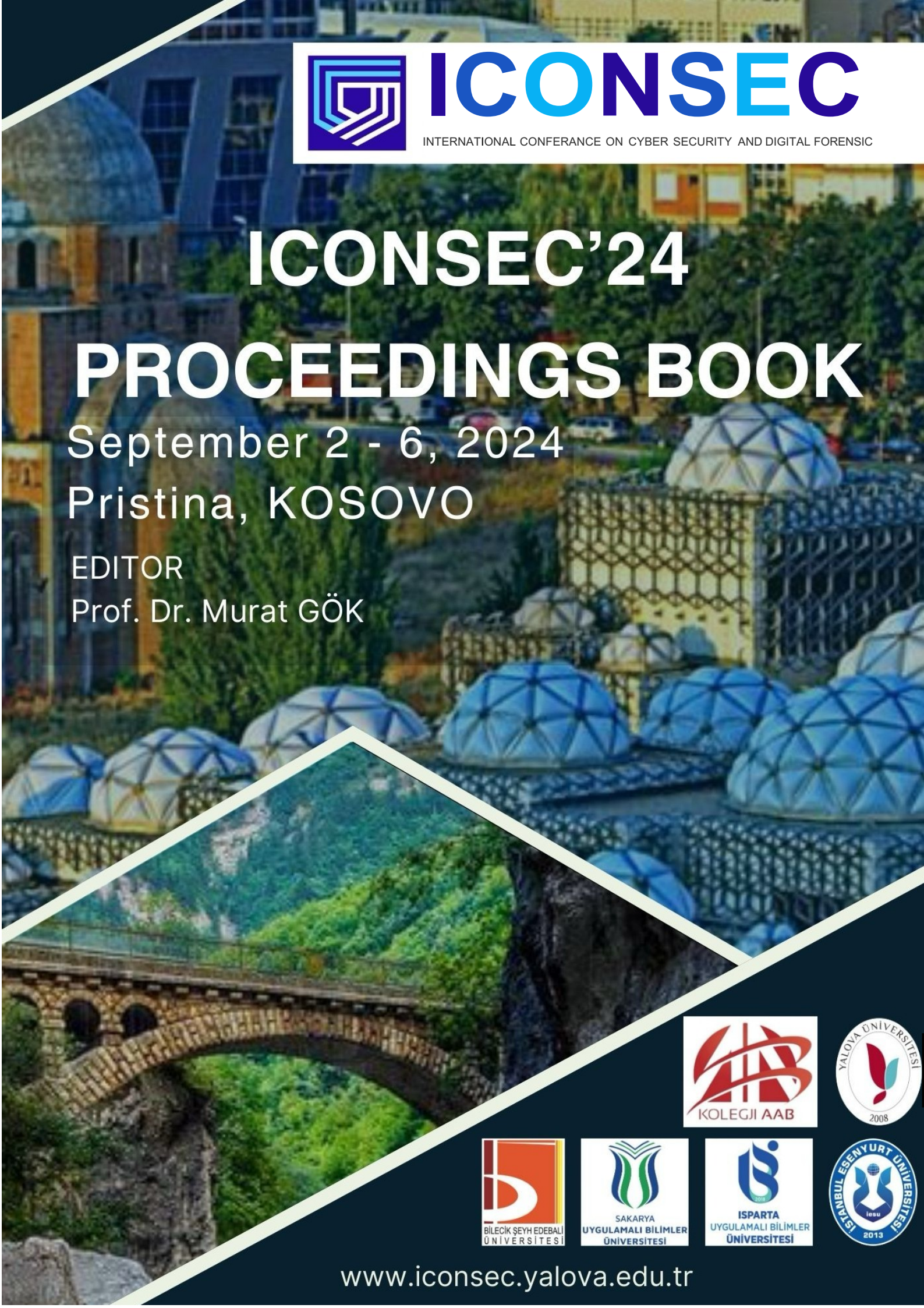


ICONSEC

INTERNATIONAL CONFERANCE ON CYBER SECURITY AND DIGITAL FORENSIC

ICONSEC'24
PROCEEDINGS BOOK

September 2 - 6, 2024

Pristina, KOSOVO

EDITOR
Prof. Dr. Murat GÖK

KOLEGJI AAB

YALOVA ÜNİVERSİTESİ 2008

BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ

SAKARYA UYGULAMALI BİLİMLER ÜNİVERSİTESİ

ISPARTA UYGULAMALI BİLİMLER ÜNİVERSİTESİ

İSTANBUL ESENYURT ÜNİVERSİTESİ 2013

www.iconsec.yalova.edu.tr

COMMITTEES

Honorable Committee

- Prof. Dr. Bujar Demjaha (Rectorr of AAB College)
- Prof. Dr. Mehmet Bahçekapılı (Rector of Yalova University)
- Prof. Dr. Zafer Asım Kaplancıklı (Rector of Bilecik Şeyh Edebali University)
- Prof. Dr. Yılmaz Çatal (Rector of Isparta University of Applied Sciences)
- Prof. Dr. Mehmet Sarıbıyık (Rector of Sakarya University of Applied Sciences)
- Prof. Dr. Süleyman Özdemir (Rector of Istanbul Esenyurt University)

Conference Chair

- Prof. Dr. Murat Gök (Yalova University)

Organizing Board

- Prof. Dr. Mehmet Büyükyıldız (Bursa Technical University, Turkey)
- Assoc. Prof. Dr. Süleyman Uzun (Sakarya University of Applied Sciences, Turkey)
- Assoc. Prof. Dr. Faruk Bulut (Istanbul Esenyurt University, Turkey)
- Assoc. Prof. Dr. Emre Dandil (Bilecik Şeyh Edebali University,Turkey)
- Assist. Prof. Dr. Sinan Demir (Isparta University of Applied Sciences, Turkey)
- Assist. Prof. Dr. İrfan Kösesoy (Kocaeli University, Turkey
- Emine Cengiz (Yalova University, Turkey)
- Sudenur Şenkal (Yalova University, Turkey)
- Fatih Buldur (Yalova University, Turkey)

Scientific Committee

- Prof. Dr. Ayhan İstanbullu (Balıkesir University, Turkey)
- Prof. Dr. Ecir Uğur Küçüksille (Süleyman Demirel University, Turkey)
- Prof. Dr. Müfit Çetin (Yalova University, Turkey)
- Prof. Dr. Ramazan Bayındır (Gazi University, Turkey)
- Prof. Dr. Naci Genç (Yalova University, Turkey)
- Prof. Dr. Yıldıray Yalman (Piri Reis University, Turkey)
- Prof. Dr. Resul Daş (Fırat University, Turkey)
- Prof. Dr. Ahmet Bedri Özer (Fırat University, Turkey)
- Prof. Dr. Ahmet Zengin (Sakarya University, Turkey)
- Prof. Dr. Atilla Elçi (Hasan Kalyoncu University, Turkey)
- Prof. Dr. Muharrem Tolga Sakallı (Trakya University, Turkey)
- Assoc. Prof. Dr. Bilgin Metin (Bogazici University, Turkey)
- Assoc. Prof. Dr. Ahmet Koltuksuz (Yaşar University, Turkey)
- Assoc. Prof. Dr. Derya Avcı (Fırat University, Turkey)
- Assoc. Prof. Dr. Sunay Türkdoğan (Yalova University, Turkey)
- Assoc. Prof. Dr. Fatih Ertam (Fırat University, Turkey)
- Assoc. Prof. Dr. Muhammed Ali Aydın (Istanbul University-Cerrahpaşa, Turkey)
- Assoc. Prof. Dr. Serdar Solak (Kocaeli University, Turkey)
- Assoc. Prof. Dr. Bünyamin Ciylan (Gazi University, Turkey)
- Assoc. Prof. Dr. Ercan Buluş (Tekirdağ Namık Kemal University, Turkey)
- Assoc. Prof. Dr. Sedat Akleylek (Ondokuz Mayıs University, Turkey)
- Assoc. Prof. Dr. Murat Arıcı (Selçuk University, Turkey)
- Assist. Prof. Dr. Mert Özarar (HAVELSAN Cyber Security Director / Ankara Science University, Turkey)
- Assist. Prof. Dr. Bülent Tuğrul (Ankara University, Turkey)
- Assist. Prof. Dr. Burcu Demirelli Okkalıoğlu (Yalova University, Turkey)
- Assist. Prof. Dr. Meltem Kurt Pehlivanoğlu (Kocaeli University, Turkey)
- Assist. Prof. Dr. Murat Ak (Akdeniz University, Turkey)
- Assist. Prof. Dr. Ahmet Albayrak (Düzce University, Turkey)
- Assist. Prof. Dr. Güneş Harman (Yalova University, Turkey)
- Assist. Prof. Dr. Murat Okkalıoğlu (Yalova University, Turkey)

- Assist. Prof. Dr. Ömer Aydın (Manisa Celal Bayar University, Turkey)
- Assist. Prof. Dr. Ömer Özgür Bozkurt (Turkish National Defense University, Turkey)
- Assist. Prof. Dr. Osman H. Koçal (Yalova University, Turkey)
- Assoc. Prof. Dr. Şebnem Özdemir (Beykent University, Turkey)
- Assist. Prof. Dr. Mustafa Coşar (Hitit University, Turkey)
- Assist. Prof. Dr. Tarık Yerlikaya (Trakya University, Turkey)
- Assist. Prof. Dr. Yunus Özen (Yalova University, Turkey)
- Assist. Prof. Dr. Kevser Ovaz Akpınar (Sakarya University, Turkey)
- Assist. Prof. Dr. Esra N. Yolaçan (Eskişehir Osmangazi University, Turkey)
- Assist. Prof. Dr. Mustafa Cem Kasapbaşı (İstanbul Commerce University, Turkey)
- Assist. Prof. Dr. Fatma Büyüksaraçoğlu Sakallı (Trakya University, Turkey)
- Assist. Prof. Dr. Atila Bostan (Ankara Science University, Turkey)
- Assist. Prof. Dr. Andaç Mesut (Trakya University, Turkey)
- Assist. Prof. Dr. Burcu Yılmazel (Eskişehir Technical University, Turkey)
- Assist. Prof. Dr. Alpay Doruk (Bandırma University, Turkey)
- Assist. Prof. Dr. Özgür Can Turna (Istanbul University-Cerrahpaşa, Turkey)
- Assist. Prof. Dr. Zeynep Gürkaş Aydın (Istanbul University-Cerrahpaşa, Turkey)
- Dr. Ahmet Ali Süzen (Isparta University of Applied Sciences, Turkey)
- Dr. Mehmet Yavuz Yağcı (Istanbul University, Turkey)
- Dr. Remzi Gürfidan (Isparta University of Applied Sciences, Turkey)
- Dr. Ömer Aslan (Siirt University, Turkey)
- Dr. Faruk Süleyman Berber (Süleyman Demirel University, Turkey)
- Dr. Semih Çakır (Zonguldak Bülent Ecevit University, Turkey)
- Dr. Gülsüm Akkuzu Kaya (Kirsehir Ahi Evran University, Turkey)
- Dr. Ahmet Karaküçük (Uludağ University, Turkey)
- Dr. Duygu Sinanç Terzi (Amasya University, Turkey)
- Dr. Mehmet Mehdi Karakoç (Ağrı University, Turkey)
- Dr. Kerime Dilşad Çiçek (Ayvansaray University, Turkey)
- Dr. Sultan Zavrak (Düzce University, Turkey)
- Dr. Maad M. Mijwil (Baghdad College of Economic Sciences University, Iraq)

CONTENTS

3rd International Conference on Cyber Security and Digital Forensics (ICONSEC) 2024

PROCEEDINGS BOOKS

Volume 1

ABSTRACT BOOK

Çocuk ve Siber Güvenlik Konulu Haberlerinin Medyada Temsili

Ayşe Hümeyra BAYRAM[1]*, Asude BAYRAM[2]

[1]*Gebze Teknik Üniversitesi, Siber Güvenlik Meslek Yüksekokulu, Kocaeli, TÜRKİYE*
[2]*Bilecik Şeyh Edebali Üniversitesi, Sağlık Bilimleri Fakültesi, Çocuk Gelişimi Bölümü, Bilecik, TÜRKİYE*

Özet

Hızla gelişen dijital çağın çocuklar üzerindeki etkisi elbette yadsınamaz. Çoğu kez erken çocukluk döneminde başlayan teknoloji kullanımı, çocuklara bilgiye erişim olanağı sunarken diğer yandan onları siber dünyada çeşitli risklerle karşı karşıya bırakmaktadır. Siber güvenlik çocukların dijital ortamlarda güvenli bir şekilde gelişmeleri için kritik bir öneme sahiptir. Çalışmada, siber güvenlik ve çocuk konulu haberlerinin medyadaki temsilinin tespiti amaçlanmıştır. Bu bağlamda, Anadolu Ajansı'nın siber güvenlik ve çocuk çerçevesinde ele aldığı; siber zorbalık, çocukların siber güvenliği, online istismar ve şifre güvenliği gibi kavramları içeren haberleri incelenmiştir. Örnekleme dahil edilen haberler, 27.12.2011-29.04.2024 tarih aralığındaki online arşiv kayıtlarından 2024 yılı Nisan ayında elde edilmiştir. Araştırma sonucunda; çalışma konusuna uyan toplam 92 haber olduğu tespit edilmiş, bu haberlerin Anadolu Ajansı kategorilerinden en fazla teknoloji, gündem ve eğitim alanında olduğu görülmüştür. Haberlerin yayınlandığı yıllar incelendiğinde, 16 haber ile 2019 yılı ilk sıradayken bunu 13 haber ile 2023 yılı takip etmektedir. Bu haberlerde ele alınan koruyucu önlemlerin en fazla hükümet kanadından gerçekleştirildiği ve bakanlıklardan en fazla MEB'in yer aldığı dikkat çekmektedir. Bu çalışma, çocukların dijital dünyada karşılaştıkları riskler konusunda farkındalık oluşturmayı ve siber güvenlik alanında alınması gereken önlemleri vurgulayarak, ebeveynler, eğitimciler ve politikacılar için değerli bilgiler sunmaktadır.

Anahtar Kelimeler: *Siber Güvenlik, Siber Zorbalık, Çocuk, Online İstismar*

*Contact email: ahbayram@gtu.edu.tr

Homomorphic Encryption for Secure Data Processing: A User-Centered Wiki Solution

Büşra PARTİGÖÇ[1]*. Ahmet ALBAYRAK[1]

[1]*Düzce Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Düzce, TÜRKİYE*

Abstract

In this study introduces a user-centered wiki web application that emphasizes the importance of homomorphic encryption technology in ensuring the security of personal data. In the digital age, protecting personal data is of critical importance. Homomorphic encryption provides a solution to protect the confidentiality of personal information by allowing data to be processed in encrypted form.

In the study, the basic principles of homomorphic encryption and popular algorithms such as RSA and Paillier were examined. The wiki application, developed using the ASP.NET Core MVC platform, allows users to experience homomorphic encryption operations using the Microsoft SEAL library. In this way, users will gain awareness about the security of their personal data and will be able to discover practical applications of this technology.

Nowadays, accurate and secure protection of personal data is of great importance for both individuals and institutions. This study aims to raise awareness on this issue by emphasizing the potential of homomorphic encryption-based solutions in ensuring personal data security.

Keywords *Homomorphic Encryption, Wiki Web Application, MVC Layered Architecture, Data Security*

*Contact email: busrap4206@gmail.com

Experimental Applications of Artificial Intelligence in Cybersecurity Training

Büşra PARTİGÖÇ[1], Ahmet ALBAYRAK[1]*

[1]*Düzce Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Düzce, TÜRKİYE*

Abstract

Cyber security is one of the most critical issues of the digital age. New technologies such as increasing internet use, cloud computing, and the Internet of Things (IoT) cause cyber threats to rapidly diversify and intensify. Cyber-attacks can lead to serious consequences such as theft of corporate/personal data, compromise of systems, and service interruptions. Therefore, it is vital to have strong cybersecurity measures in place. Artificial Intelligence (AI) is finding increasing use in the field of cybersecurity. AI-based solutions can detect and prevent cyber threats more effectively and proactively than traditional methods. Training expert personnel in the field of cyber security is of great importance because technological developments are rapidly progressing, and threats are constantly changing. In this context, it can be said that applied training has a critical role in training cyber security experts. Applied trainings enable students to face real-life scenarios by putting theoretical knowledge into practice. For example, working on virtual attack scenarios helps students develop attack detection and response skills. In addition, discovery of vulnerabilities, analysis of security vulnerabilities and improvement studies can also be carried out within the scope of applied training.

In this study, firstly, the potential usage areas of artificial intelligence in the field of cyber security are discussed. It examines how artificial intelligence-based solutions can be applied in the detection of cyber threats, simulation of attack/defense scenarios, detection of security vulnerabilities and incident response processes. Then, the process of creating an artificial intelligence-based experiment sheet developed in the study is explained in detail. This test sheet is designed to enable students to receive practical training on cyber security issues. It explains how the leaflet can be used to improve students' problem-solving, critical thinking and quick decision-making skills. Additionally, the applicability and effectiveness of the test sheet are also evaluated. Considering student feedback and results obtained, the leaflet's contributions to cyber security education and potential improvement areas are discussed.

Keywords: *Artificial Intelligence, Cyber Security, Machine Learning, Deep Learning, Laboratory Studies*

*Contact email: ahmetalbayrak@duzce.edu.tr

Audio Steganography with Stereo Audio by Using Mid/Side Processing

Ali Erdem Altınbaş[1]*, Yıldıray Yalman[2]

[1]*Kocaeli University, Faculty of Engineering, Electronics and Communication Engineering, Kocaeli, TURKIYE*
[2]*Piri Reis University, Faculty of Engineering, Computer Engineering, Istanbul, TURKIYE*

Abstract

This paper presents a novel audio steganography algorithm that utilizes music theory and audio mixing techniques. In the field of steganography, audio files are less preferred as a cover due to the sensitivity of the human auditory system. This is because the capacity for data hiding is typically diminished in steganography in order to ensure the principle of imperceptibility. The method that is presented includes an example of how music technologies can be used in audio steganography. Even when the entire cover file is used, the experimental results demonstrate that the imperceptibility principle is satisfied. With regard to robustness, which is another crucial aspect of steganography, the proposed method has been demonstrated to be robust even in the presence of the MP3 compression algorithm. MATLAB codes of the study can be accessed from this link: http://bit.ly/3R6uwZv

Keywords: *audio steganography, mid/side, data hiding, watermarking*

*Contact email: alierdemaltinbas@gmail.com

3rd International Conference on Cyber Security and Digital Forensics (ICONSEC) 2024

PROCEEDINGS BOOKS

Volume 2

FULLTEXT BOOK

Yapay Zeka Yöntemleri Kullanarak Ses Tabanlı Konuşmacı Dili Tanıma

Nazife Gizem AVCILAR[1]*, Erhan AKBAL[2]

[1,2]*Fırat Üniversitesi, Teknoloji Fakültesi,Adli Bilişim Müh. Bölümü, Elazığ, Türkiye*

Özet

Dil tanıma sistemleri, iletişimdeki dil bariyerlerini aşma ve adli bilişimde önemli bir rol oynama üzerine odaklanmıştır. Bu sistemler, kullanıcının konuştuğu dili otomatik olarak tespit ederek, iletişimdeki dil bariyerlerini kaldırmakta ve adli süreçlerde ses analizi yoluyla bilgi sağlamaktadır. Adli bilişimde, dil tanıma sistemleri güvenlik birimlerine kişinin hangi dili konuştuğu hakkında önemli bir ipucu verir ve güvenlik açısından kritik bilgiler sağlar. Dil tanımlama ve süreçlerinin tanımı yapılarak, bu tanım doğrultusunda yapay zekâ tabanlı çalışmalar incelenmiştir. Literatürdeki çalışmalarla konuşmacı dili tanımlama ve otomatik dil tanımlama alanlarında araştırma yapılmıştır. Doğruluk oranları, özellik çıkarma yöntemine, sınıflandırma yöntemine ve kullanılan veri setine bağlı olarak farklılık göstermektedir. Bu çalışmada farklı yapay zekâ yöntemlerinin performansları değerlendirilmiştir. Kullanılan sınıflandırma modellerinden Subspace k-en yakın komşuluk (KNN) ve Fine k-en yakın komşuluk (KNN) sırasıyla %96.7 ve %96.5 doğruluk oranlarına ulaşmıştır.

Anahtar Kelimeler: *Adli Bilişim, Dil Tanımlama, Dil Sınıflandırma*

Sound-Based Speaker Language Recognition Using Artificial Intelligence Methods

Abstract

Language recognition systems are focused on overcoming language barriers in communication and playing an important role in forensics. By automatically detecting the language spoken by the user, these systems remove language barriers in communication and provide information through voice analysis in forensic processes. In forensic informatics, language recognition systems give security units an important clue about the language spoken by the person and provide security-critical information. Language identification and processes are defined, and artificial intelligence-based studies are analyzed in line with this definition. Research in the fields of speaker language identification and automatic language identification has been carried out based on the studies in the literature. Accuracy rates vary depending on the feature extraction method, classification method, and data set used. In this study, the performances of different artificial intelligence methods are evaluated. Among the classification models used, Subspace k-nearest neighbor (KNN) achieved an accuracy rate of 96.7%, while Fine k-nearest neighbor (KNN) achieved 96.5%.

Keywords: *Forensics , Langauge Identification ,Language Classification*

1 Giriş

Dünyada bilinen veya bilinmeyen birçok toplum vardır [1]. Her toplum kendi dili ile iletişimini sürdürmektedir. Bilinmeyen bir dili konuşan biri ile karşılaşılırsa iletişim kurulamaz. Böyle bir durumda tercümana ihtiyaç duyulur. Ancak dili bilmeden tercüman bulmak mümkün değildir. Dil tanımlama, konuşma veya yazıya bakılarak hangi dil olduğunu belirleme sürecidir [2]. İnsanlar dil tanımlama için en iyi sistemdir [3]. Ancak dünyada pek çok dil vardır ve konuşmacının hangi dili konuştuğunu belirlemek çok zordur. Ek olarak, her dil farklı aksan ve lehçelerden oluşur. Dil tanımlama ve sınıflandırma, konuşma sinyalinin akustik özelliklerini kullanarak hedef dili yüksek

*Contact email: 222144111@firat.edu.tr

doğrulukla tanımlama işlemidir [4]. Dil tanımlama süreci, konuşma veya konuşmacı tanıma sürecinden farklıdır. Konuşmayı kullanarak dili tanımlamanın amacı, dilin metin temelli özellikleri kullanılarak üretilen seslerin özelliklerini kullanmaktır [5]. Konuşma, dilin akustik, fonetik ve prozodik özelliklerine sahiptir. Ayrıca alfabe, kelimeler, morfoloji, sözdizimi ve dilbilgisi yapısı konuşmayı etkileyen faktörlerdir [6]. Bu nedenle, diller, konuşmacıdan bağımsız olarak farklı akustik özellikler gösterir ve bilgisayar destekli otomatik dil tanımlama sistemlerine (ODTM) ihtiyaç vardır.

Adli bilişimde konuşmacıdan dil tanımlamak, hukuki süreçlerde önemli bir rol oynar. Ses tonu, vurgu, hız ve diğer ses özellikleri üzerinden yapılan analiz, şüphelilerin ve tanıkların ifadelerini değerlendirmek ve ses kayıtlarını incelemek gibi konularda bilgi sağlamak için kullanılır. Bu nedenle son zamanlarda adli konuşmacı tanıma konusunda araştırmalar yapılmaktadır [7]. Adli ses bilişim inceleme teknikleri, bilgisayar korsanlığı veya çocuk pornografisi değil aynı zamanda cinayet, terörizm, organize suç, vergi kaçakçılığı, uyuşturucu kaçakçılığı ve gasp gibi farklı suç türlerinin çözümüne de katkı sağlar[8]. Bu sistemler, güvenlik birimlerine kişinin hangi dili konuştuğu hakkında önemli bir ipucu verir ve güvenlik açısından kritik bilgiler sağlar.

1.1 Çalışmanın Amacı

Dil sınıflandırma çalışmalarının temel amacı, konuşma özelliklerini kullanarak dilin ait olduğu sınıfı yüksek doğrulukla belirlemektir. Adli bilişimde, konuşmacıdan dil tanıma alanında yapılan çalışmalar, küreselleşen dünya ve farklı toplumlar arası iletişimin arttığı bir dönemde önem kazanmaktadır. Özellikle son yıllarda yaşanan göç ve mülteci sorunları, dil tanımlama ihtiyacını artırmıştır. Bu bağlamda, dil tanımanın adli bilişimdeki rolü daha da belirgin hale gelmiş ve dil analizi teknolojilerine olan talebi artırmıştır. Bu çalışmalar, farklı dilleri konuşan bireyler arasında yapılan iletişimin yanı sıra, suç soruşturmalarında ve hukuki süreçlerde dilin belirlenmesi gereken durumlarda önemli bir rol oynamaktadır.

Bu amaçla çalışmada konuşmacı dili tanımlama konusunun kapsamı belirlenerek, yapay zeka tabanlı dil tanımlama alanında literatürdeki yöntemler araştırılmıştır. Deney için de 10 dilden oluşan bir veri seti ile sınıflandırma gerçekleştirilmiştir.

1.2 Literatür Taraması

Literatürde dil tanımlama alanında farklı amaçlarla çalışmalar yapılmaktadır. Adli konuşmacı tanıma [7], [9], konuşmacı tanımlama [5], [10], metin tabanlı dil tanımlama [11], [12], metinden bağımsız dil tanımlama [13], [14], duygu tanıma [15], [16]. Dil tanımlama alanında, veri seti, özellik çıkarma yöntemi ve kullanılan sınıflandırma modeli, doğruluk değeri açısından kritik öneme sahiptir. Özellik çıkarma yöntemleri için MFCC [17], PLP [18], LPC ve LPCC [19]. Sınıflandırma için derin sinir ağları (DNN)[20], [21], x-vectors [10], [22], [23], evrişimli sinir ağları [24], [25], destek vektör makineleri (SVM) [5], [26]. Dil tanımlama tabanlı diğer çalışmalar aşağıdaki gibidir. Literatürde, Mel-Frekans kepstrum katsayıları (MFCC), cepstral ve spektral teknikler gibi özellikler kullanılmıştır.

Nie ve arkadaşları [27] tarafından yapılan çalışmada, OLR20 altı dil içeren çok dilli bir veri kümesidir ve ortalama segment uzunluğu 5.45 saniyedir. Çince-İngilizce karışımı bir veri kümesi olan T&T, THCHS-30 (Çince) ve TIMIT (İngilizce) veri kümelerinin birleşimidir. Tüm cümlelerin sessiz olmayan kısımlarını, bir saniyelik konuşma parçalarına bölerek kısa uzunlukta bir veri kümesi oluşturulmuştur. TAL_ASR, Çince öğretilen İngilizce dersleri senaryosu altında toplanan bir veri kümesidir. İçinde Çince ve İngilizce'nin iç içe geçtiği bir yapıya sahip, birçok kod değiştiren konuşmayı içermektedir. Önerilen yöntem BERT destekli bir dil tanımlama sistemidir. BERT RCNN modeli ile OLR20 veri kümesinde % 99.21 doğruluk ve % 99.51 F1-score başarı değerlerine ulaşılmıştır.

Thukroo ve arkadaşları [28] tarafından gerçekleştirilen çalışmada, veri kümesi için JK ve Ladakh bölgelerinde konuşulan altı farklı dil türünden veri toplanmıştır. Bu diller arasında Hintçe, İngilizce, Dogri, Keşmir, Ladakhi ve Urduca bulunmaktadır. İngilizce ve Hintçe veri kümeleri IIIT H ve VoxForge standart derlemelerinden elde edilirken, diğer dil veri setleri farklı kaynaklardan manuel olarak toplanmıştır. Özellik çıkarma işlemi cepstral ve spektral tekniklerle yapılmıştır. Konuşulan dil tanımlanmasında önerilen yöntem AD-TSA-ISVM-RNN ile % 97.64 doğruluk, % 99.48 sensitivity, % 98.09 precision ve % 98.78 f1-score başarı değerlerine ulaşılmıştır.

Albadr ve arkadaşları [29] tarafında yapılan çalışmada, veri kümesi olarak sekiz farklı dil kullanılmıştır. Her dil 15 ifade içermekte olup ifadeler 30 saniye sürmektedir. Veri kümesi eğitim

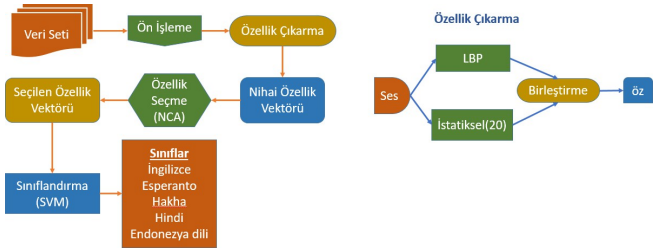
seti için %67'ye ve test seti için %33'e bölünmüştür. Diğer bir deyişle, her dildeki 10 ifade eğitim için, kalan 5 ifade ise test için kullanılmıştır. Eğitim seti, ELM ve GWO parametrelerini optimize etmek amacıyla kullanılırken, test seti ise GWO-ELM performansını ölçmek için kullanılmıştır. Özellik çıkarma için Mel Frekans Cepstral Katsayısı (MFCC), Kaydırılmış Delta Katsayısı (SDC), Gauss Karışım Modeli (GMM) ve i-vectör çerçevesi kullanılmıştır. Regresyon ve sınıflandırma için GWO-ELM ve ESA-ELM yöntemleri kullanılarak sırasıyla % 100.00 ve % 96.25 başarı değerleri elde edilmiştir.

Lu ve arkadaşları [30] tarafından yapılan çalışmada veri kümesi, Oryantal Dil Tanıma (OLR) yarışması için tasarlanan çok dilli THCHS30 ve OLR veri setlerinden alınmıştır. Bu veri kümesi, 10 farklı dil ve yaklaşık 110 bin ifade içermektedir. Farklı görevlerde iki ayrı test seti oluşturulmuştur: İlk test seti eğitim seti ile aynı 10 dili içermektedir. Her dil için 1,8 bin ifade içermekte ancak ifadelerin süresi 1 saniyedir. İkinci test seti geliştirme ve test için oluşturulmuş olup sadece 6 dil içermektedir. Konuşma dili tanımada UDA, NOT ve NPOT algoritmaları kullanılmıştır. NPOT algoritmasının diğer algoritmalara göre daha düşük bir sınıflandırma risk değeri olan 0.0503 ve daha yüksek bir doğruluk değeri olan 5.011 elde edilmiştir. Bu sonuçlar POT ve NPOT algoritmalarının etki alanı kaymasını azaltmada etkili olduğunu ve SLR'nin etkinliğini artırdığını göstermektedir.

Woods ve arkadaşları [25] tarafından yapılan çalışmada, çeşitli kaynaklardan oluşturdukları 3 dil içeren bir veri seti kullanılmıştır. Özellik çıkarma yöntemi olarak kısa süreli spektral özellikler, sınıflandırma için ise Evrişimli Sinir Ağı - Tekrarlayan Sinir Ağı (CNN-RNN) kullanılmıştır. Konuşma dili tanımlama için uygulanan model ile %95.6 doğruluk başarı değerine ulaşılmıştır.

2 Önerilen Yöntem

Yapılan çalışma için belirlenen yöntemin akış şeması Şekil 1'de detaylı bir şekilde açıklanmıştır.



Şekil 1 Konuşmacı dil tanıma için önerilen yöntemin akış şeması

Deney için ilk olarak toplanan veri seti üzerinde ön işleme adımı gerçekleştirildi. Bu aşamada gürültü azaltma ve ses düzeltme gibi uygulamalar gerçekleştirildi. İkinci aşama olan özellik çıkarım sürecinde Yerel İkili Desenler (LBP) algoritması, ses verilerinin lokal desenlerini belirlemede etkili bir rol oynamıştır. Bu sayede, sesin özgün özellikleri daha iyi anlaşılabilir hale gelmiştir. İstatistiksel özelliklerin eklenmesi, LBP'nin çıkardığı desenlere ek olarak daha yüksek seviyede bilgi sağlamıştır. Toplamda 276 özellik, ses verilerinin detaylı bir temsilini oluşturmak üzere bir araya getirilmiştir.

Ayrıca, ses verilerine uygulanan 20 seviyeli Ayrık Dalgacık Dönüşümü, frekans bileşenlerini ayırmada etkili olmuştur. Bu dönüşüm ile birlikte elde edilen 5520 özellik, ses sinyallerinin frekans ve zaman açısından geniş bir perspektifte incelenmesine imkân tanımaktadır. Özellik vektörlerinin 0-1 arasındaki MİN-MAX normalizasyonu, farklı özellik türlerinin birbirleriyle karşılaştırılabilir hale getirilmesine yardımcı olmuştur. Bu sayede, ölçek farklılıklarının etkisi minimize edilerek daha güvenilir sonuçlar elde edilmiştir. Elde edilen zengin özellik seti, her bir ses verisi için bir etiketle eşleştirilerek sınıflandırma öncesi veri seti oluşturulmuştur. Bu adım, sınıflandırma işlemi için hazırlanan veri setinin temelini oluştururken, etiketleme sayesinde modelin eğitim sürecinde doğru sonuçlar elde etmesine katkıda bulunmuştur. Denklem 1'de verilen işlem ile 5521 özellik çıkarılmıştır.

$$("(256 + 20) \times 20^* + 1) \quad (1)$$

İşlemde bulunan '+1' değeri etiketin sayısını ifade etmektedir. ReliefF özellik seçme yöntemi kullanılarak 5521 özellik içinden en anlamlı 500 özellik seçilmiştir. Sınıflandırma aşamasında MATLAB R2020a'nın classification learner aracı, bu zengin özellik seti üzerinde farklı sınıflandırma algoritmalarını değerlendirerek en uygun olanını seçme imkanı sağlamıştır. Bu aşama, ses verilerinin karmaşıklığını anlama ve farklı sınıflar arasındaki ilişkileri ortaya koyma konusunda daha derin bir

bakış açısı sunmuştur. Sınıflandırma için Karar Ağaçları, Destek Vektör Makineleri(SVM) ve k-En Yakın Komşuluk (KNN) gibi modeller kullanılmıştır.

2.1 Veri Seti

Bu araştırmada kullanılan veri seti, geniş bir dil yelpazesini içermektedir. İngilizce, Esperanto, Hakha, Hindi, Endonezya, Tatar, Telugu, Thai, Türkçe ve Ukrayna gibi farklı dil gruplarından seçilmiş olan bu diller, manuel olarak çeşitli kaynaklardan toplanmıştır. Kaynaklar arasında Mozilla Common Voice ve YouTube gibi platformlar bulunmaktadır.

Veri setinin oluşturulma sürecinde, toplanan ses dosyaları özel olarak NHC WavePad programı kullanılarak işlenmiştir. Ses dosyaları, sessiz olmayan kısımları belirlemek ve standartlaştırmak amacıyla dikkatlice incelenmiş ve bu süreçte her ses kaydı 2 saniyelik segmentlere bölünmüştür. Bu yaklaşım, veri setinin homojenliğini artırmaya ve dil özelliklerini daha etkili bir şekilde yakalamaya yönelik bir strateji olarak benimsenmiştir.

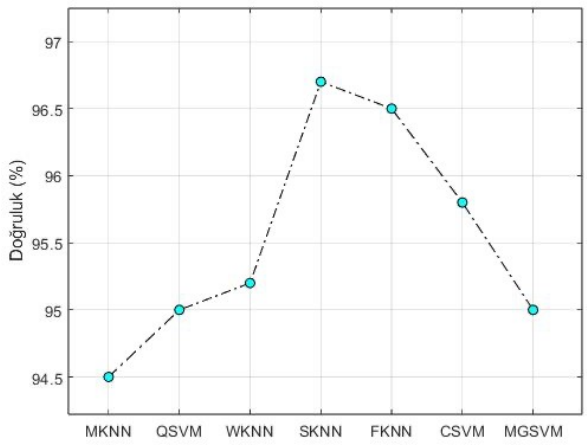
Bölünmüş olan ses segmentleri, her bir dil için ayrı klasörlerde düzenlenmiş ve WAV formatında etiketlenerek kaydedilmiştir. Bu düzenleme, veri setinin kullanıcılar ve araştırmacılar tarafından daha kolay anlaşılabilir ve erişilebilir olmasını sağlamak amacıyla yapılmıştır. Tablo 1'de verisetine ait içerik gösterilmiştir.

Tablo 1. Veri seti içeriği

No	Dil	Ses dosya sayısı (2 sn)	No	Dil	Ses dosya sayısı (2 sn)
1	İngilizce	1000	6	Tatar	1543
2	Esparanto	1045	7	Telugu	1253
3	Hakha	992	8	Thai	1565
4	Hindi	1037	9	Türkçe	1365
5	Endonezya	900	10	Ukrayna	1047

2.2 Deneysel Sonuçlar

Destek Vektör Makineleri (SVM), bir hiper düzlemle veri setini en iyi şekilde ayırmayı amaçlayan bir sınıflandırma veya regresyon modelidir. Sınıflar arasında bir hiper düzlem oluşturarak, bu düzlemi optimize eder. Veri noktalarının bu hiper düzleme olan uzaklıkları maksimum olacak şekilde ayırmaya çalışır. k-En Yakın Komşuluk (KNN), belirli bir örneği sınıflandırmak veya tahmin etmek için çevresindeki k en yakın komşusuna bakarak çalışan bir algoritmadır. Veri noktasını çevresindeki komşulara göre sınıflandırır veya tahmin eder. Sınıflandırma için genellikle çoğunluk sınıfı kullanılır. Şekil 2'de kullanılan yöntemlerin başarım oranları gösterilmiştir.



Şekil 2. Deney sonucunda sınıflandırma yöntemlerine göre doğruluk oranı

Tablo 2. Literatürde bulunan çalışmalar ve önerilen yöntem

Literatürde bulunan çalışmalar			
Veri seti	**Sınıflandırma Yöntemi**	**Özellik Çıkarma Yöntemi**	**Doğruluk Oranı**
6 dil içeren veri kümesi[27]	BERT-RCNN	-	%99.21
6 dil içeren veri kümesi[28]	AD-TSA-ISVM-RNN	Cepstral ve Spektral teknikler	%97.64
8 dil içeren veri kümesi[29]	GWO-ELM ve ESA-ELM	MFCC, SDC ve GMM	GWO-ELM: %100 ESA-ELM: %96.25
3 dil içeren veri kümesi[25]	CNN-RNN	Spektral teknikler	%95.6
Önerilen yöntem			
10 dil içeren veri kümesi	SVM ve KNN	LBP	KNN: %96.7 SVM: %95.8

3 Sonuçlar

Bu çalışma, konuşmacı dil tanınması için kısa ifadelerden dil bilgilerinin çıkarılmasına dayanan bir yöntem sunmaktadır. Önerilen yöntem, iki farklı temel derin öğrenme yöntemiyle uygulanmıştır. 5520 özellik üzerinden en anlamlı 500 özelliği kullanarak yüksek başarı değerlerine ulaşılmıştır. Deneysel sonuçlar, tüm temel ve derin öğrenme

yöntemlerinin önerilen yöntemle gerçekten iyi performans gösterdiğini göstermektedir. Sınıflandırma modelleri arasında Medium k-en yakın komşuluk (KNN), Quadratic Destek Vektör Makineleri (SVM), Weighted k-en yakın komşuluk (KNN), Subspace k-en yakın komşuluk (KNN), Fine k-en yakın komşuluk (KNN), Cubic Destek Vektör Makineleri (SVM) ve Medium Gaussian Destek Vektör Makineleri (SVM), daha iyi performans sergilemektedir. Subspace k-en yakın komşuluk (KNN) ve Fine k-en yakın komşuluk (KNN) modelleri sırasıyla %96.7 ve %96.5 doğruluk oranlarına ulaşmıştır. Bu sonuçlar, dil bilgisinin çıkarılmasının daha iyi konuşmacı tanıma oranlarına yol açtığını göstermektedir.

Kaynaklar

[1] E. Demuro ve L. Gurney, "Languages/languaging as world-making: the ontological bases of language", *Language Sciences*, c. 83, s. 101307, Oca. 2021, doi: 10.1016/j.langsci.2020.101307.

[2] J. Monteiro, J. Alam, ve T. H. Falk, "Residual convolutional neural network with attentive feature pooling for end-to-end language identification from short-duration speech", *Computer Speech & Language*, c. 58, ss. 364-376, Kas. 2019, doi: 10.1016/j.csl.2019.05.006.

[3] R. K. Das ve S. R. M. Prasanna, "Speaker Verification from Short Utterance Perspective: A Review", *IETE Technical Review*, c. 35, sy 6, ss. 599-617, Kas. 2018, doi: 10.1080/02564602.2017.1357507.

[4] J. Bora, S. Dehingia, A. Boruah, A. A. Chetia, ve D. Gogoi, "Real-time Assamese Sign Language Recognition using MediaPipe and Deep Learning", *Procedia Computer Science*, c. 218, ss. 1384-1393, Oca. 2023, doi: 10.1016/j.procs.2023.01.117.

[5] H. Li, B. Ma, ve K. A. Lee, "Spoken Language Recognition: From Fundamentals to Practice", *Proceedings of the IEEE*, c. 101, sy 5, ss. 1136-1159, May. 2013, doi: 10.1109/JPROC.2012.2237151.

[6] M. Chaiani, S. A. Selouani, M. Boudraa, ve M. Sidi Yakoub, "Voice disorder classification using speech enhancement and deep learning models", *Biocybernetics and Biomedical Engineering*, c. 42, sy 2, ss. 463-480, Nis. 2022, doi: 10.1016/j.bbe.2022.03.002.

[7] S. Saleem, F. Subhan, N. Naseer, A. Bais, ve A. Imtiaz, "Forensic speaker recognition: A new method based on extracting accent and language information from short utterances", *Forensic Science International: Digital Investigation*, c. 34, s. 300982, Eyl. 2020, doi: 10.1016/j.fsidi.2020.300982.

[8] C. Bakir ve M. Yuzkat, "A Search on the Importance of Forensic Voice Studies in Forensic and a Example Application", içinde *2022 30th Signal Processing and Communications Applications Conference (SIU)*, Safranbolu, Turkey: IEEE, May. 2022, ss. 1-4. doi: 10.1109/SIU55565.2022.9864995.

[9] R. A., S. N., ve G. K., "Forensic investigation for twin identification from speech: perceptual and gammatone features and models", *Multimed Tools Appl*, c. 80, sy 12, ss. 18301-18315, May. 2021, doi: 10.1007/s11042-021-10639-z.

[10] D. Martinez, O. Plchot, L. Burget, O. Glembek, ve P. Matejka, "Language Recognition in iVectors Space".

[11] J. Valk ve T. Alumäe, "VOXLINGUA107: A Dataset for Spoken Language Recognition", içinde *2021 IEEE Spoken Language Technology Workshop (SLT)*, Oca. 2021, ss. 652-658. doi: 10.1109/SLT48900.2021.9383459.

[12] G. R. Botha ve E. Barnard, "Factors that affect the accuracy of text-based language identification", *Computer Speech & Language*, c. 26, sy 5, ss. 307-320, Eki. 2012, doi: 10.1016/j.csl.2012.01.004.

[13] M. Sadanandam, V. K. Prasad, V. Janaki, ve A. Nagesh, "Text independent language recognition system using DHMM with new features", içinde *2012 IEEE 11th International Conference on Signal Processing*, Eki. 2012, ss. 511-514. doi: 10.1109/ICoSP.2012.6491537.

[14] A. Khosravani ve M. M. Homayounpour, "A PLDA approach for language and text independent speaker recognition", *Computer Speech & Language*, c. 45, ss. 457-474, Eyl. 2017, doi: 10.1016/j.csl.2017.04.003.

[15] M. W. Bhatti, Y. Wang, ve L. Guan, "A neural network approach for human emotion recognition in speech", içinde *2004 IEEE International Symposium on Circuits and Systems (ISCAS)*, May. 2004, s. II-181. doi: 10.1109/ISCAS.2004.1329238.

[16] A. F. Adoma, N.-M. Henry, ve W. Chen, "Comparative Analyses of Bert, Roberta, Distilbert, and Xlnet for Text-Based Emotion Recognition", içinde *2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, Ara. 2020, ss. 117-121. doi: 10.1109/ICCWAMTIP51612.2020.9317379.

[17] M. Biswas, S. Rahaman, A. Ahmadian, K. Subari, ve P. K. Singh, "Automatic spoken language identification using MFCC based time series features", *Multimed Tools Appl*, c. 82, sy 7, ss. 9565-9595, Mar. 2023, doi: 10.1007/s11042-021-11439-1.

[18] N. Dave, "Feature Extraction Methods LPC, PLP and MFCC In Speech Recognition", c. 1, 2013.

[19] H. Gupta ve D. Gupta, "LPC and LPCC method of feature extraction in Speech Recognition System", içinde *2016 6th International Conference - Cloud System and Big Data Engineering (Confluence)*, Oca. 2016, ss. 498-502. doi: 10.1109/CONFLUENCE.2016.7508171.

[20] J. Gonzalez-Dominguez, I. Lopez-Moreno, P. J. Moreno, ve J. Gonzalez-Rodriguez, "Frame-by-frame language identification in short utterances using deep neural networks", *Neural Networks*, c. 64, ss.

49-58, Nis. 2015, doi: 10.1016/j.neunet.2014.08.006.

[21] F. Richardson, D. Reynolds, ve N. Dehak, "Deep Neural Network Approaches to Speaker and Language Recognition", *IEEE Signal Processing Letters*, c. 22, sy 10, ss. 1671-1675, Eki. 2015, doi: 10.1109/LSP.2015.2420092.

[22] D. Snyder, D. Garcia-Romero, A. McCree, G. Sell, D. Povey, ve S. Khudanpur, "Spoken Language Recognition using X-vectors", içinde *The Speaker and Language Recognition Workshop (Odyssey 2018)*, ISCA, Haz. 2018, ss. 105-111. doi: 10.21437/Odyssey.2018-15.

[23] S. Kacprzak, M. Rybicka, ve K. Kowalczyk, "Spoken Language Recognition with Cluster-Based Modeling", içinde *ICASSP 2022 - 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, May. 2022, ss. 6867-6871. doi: 10.1109/ICASSP43922.2022.9747515.

[24] S. Mukherjee, N. Shivam, A. Gangwal, L. Khaitan, ve A. J. Das, "Spoken Language Recognition Using CNN", içinde *2019 International Conference on Information Technology (ICIT)*, Ara. 2019, ss. 37-41. doi: 10.1109/ICIT48102.2019.00013.

[25] N. Woods ve G. Babatunde, "A ROBUST ENSEMBLE MODEL FOR SPOKEN LANGUAGE RECOGNITION", *acs*, c. 16, sy 3, ss. 56-68, Eyl. 2020, doi: 10.35784/acs-2020-21.

[26] G. Vyas ve M. K. Dutta, "An integrated spoken language recognition system using support vector machines", içinde *2014 Seventh International Conference on Contemporary Computing (IC3)*, Ağu. 2014, ss. 105-108. doi: 10.1109/IC3.2014.6897156.

[27] Y. Nie, J. Zhao, W.-Q. Zhang, ve J. Bai, "BERT-LID: Leveraging BERT to Improve Spoken Language Identification", içinde *2022 13th International Symposium on Chinese Spoken Language Processing (ISCSLP)*, Ara. 2022, ss. 384-388. doi: 10.1109/ISCSLP57327.2022.10038152.

[28] Research Scholar, Department of Computer Science Islamic University of Science & Technology, Kashmir, I. A. Thukroo, R. Bashir, ve J. K. Giri, "Improved Support Vector-Recurrent Neural Network with Optimal Feature Selection-based Spoken Language Identification System", *IJST*, c. 16, sy 10, ss. 680-697, Mar. 2023, doi: 10.17485/IJST/v16i10.2119.

[29] M. A. A. Albadr, S. Tiun, M. Ayob, M. Z. A. Nazri, ve F. T. AL-Dhief, "Grey wolf optimization-extreme learning machine for automatic spoken language identification", *Multimed Tools Appl*, c. 82, sy 18, ss. 27165-27191, Tem. 2023, doi: 10.1007/s11042-023-14473-3.

[30] X. Lu, P. Shen, Y. Tsao, ve H. Kawai, "Neural domain alignment for spoken language recognition based on optimal transport". arXiv, 20 Ekim 2023. doi: 10.48550/arXiv.2310.13471.

Güvenli Video Kayıt Sistemi için Görüntüde Tespit Edilen Yüz Bölgelerinin Şifrelenmesi

Hakan AKTAŞ[1], Ömer KARAGÖZ[2]*

[1]haktas@ohu.edu.tr

[2]karagozo240@gmail.com

[1]Niğde Ömer Halisdemir Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, Niğde, Türkiye
[2]Niğde Ömer Halisdemir Üniversitesi, Mühendislik Fakültesi, Elektrik Elektronik Mühendisliği, Niğde, Türkiye

Özet

Video gözetim sistemlerinin internet tabanlı olması ve kamu kurumlarındaki kamera kayıtlarına sonradan erişilmesi bir takım güvenlik zafiyetlerini de beraberinde getirmektedir. Video gözetim sistemleri tarafından kaydedilen görüntüleri daha güvenilir hale getirebilmek için görüntülerin şifreli bir şekilde kaydedilmesi en güvenli yöntemlerden birisidir. Bu çalışmada video gözetim sistemlerinden elde edilen görüntülerin güvenli bir şekilde gerçek zamanlı olarak kaydedilmesi için, işlem süresini ve yükünü azaltmak adına tüm veriyi şifrelemek yerine YOLOv4 - tiny yapısı ile tespit edilen yüz bölgeleri GOST 28147-89 şifreleme algoritması ile şifrelenmiştir. Önerilen yöntem i5 işlemcili ve i9 işlemcili iki farklı donanım üzerinde test edilmiştir. İ9 işlemcili bir sistem kullanıldığında görüntü boyutundan bağımsız olmak üzere YOLO-v4-tiny yapısı ile yüz tespiti yaklaşık 25ms sürmüştür. Aynı donanım ile HD çözünürlüğündeki bir görüntüde tespit edilen 80x80 boyutundaki yüz bölgesinin şifreleme süresi 16 ms, ara işlemler 4 ms, toplam işlem süresi ise 45 ms olarak ölçülmüştür.

Anahtar Kelimeler: *Yüz Tespiti, YOLOv4-tiny, GOST 28147-89 Şifreleme Algoritması*

Encrypting Face Regions Detected on the Images for Secure Video Recording System

Abstract

The internet-based video surveillance systems and unauthorized access to security camera recordings in public institutions lead to some security vulnerabilities. In order to make the images recorded by video surveillance systems more reliable, one of the safest methods is the encryption of the recorded images. In this study, instead of encrypting whole frame output of video surveillance systems, the face regions detected with the YOLOv4 – tiny structure are encrypted with the GOST 28147-89 encryption algorithm so that the processing time and load are reduced without compromising a real time system. The proposed method has been tested on two different hardware including either an i5 processor or an i9 processor. When using a system with an i9 processor, face detection took about 25ms with the YOLO-v4-tiny structure, regardless of the image size. With the same hardware, the encryption time of the 80x80 face region detected on an image with a HD resolution took 16 ms, while other operations took 4 ms and total processing time was measured as 45 ms.

Keywords: *Face Detection, YOLOv4-tiny, GOST 28147-89 Cipher Algorithm*

**Contact email: haktas@ohu.edu.tr*

1 Giriş

Günümüzde, video gözetim sistemleri sokakta, toplu ulaşım araçlarında, istasyonlarda, iş yerlerinde, park yerlerinde, kamu kurumlarda ve hatta evlerde olmak üzere her yerde bulunmaktadır. Bu sistemlerde kameralardan gelen videoların izlenmesi ile anlık güvenlik takibinin yapılması ya da istenmedik olaylar olduğunda geçmişe yönelik kayıtların izlenmesi ile birçok güvenlik zafiyetini ortadan kaldırmak mümkün hale gelmektedir. 2020 verilerine göre video gözetim sistemleri kamera pazarı 33,99 Milyar ABD doları değerine ulaşmıştır [1]. Video gözetim sistemlerinin bu kadar yaygın olması birtakım sorunları da beraberinde getirmektedir. Mevcut kamera yayınına yapılacak bir saldırı ile anlık kamera görüntüleri ele geçirilebilmekte ya da kamera kayıtlarına ulaşıp geçmişe yönelik kayıtların bilgisayar korsanları tarafından siber saldırılar yapılarak ele geçirilmesi mümkün hale gelmektedir. Video gözetim sistemleri üzerine yapılmış bazı saldırılar şu şekildedir [2]: DoS Saldırısı, Fidye Yazılımı Saldırısı, Kaba Kuvvet Saldırısı.

Video gözetim sistemlerinden gelen görüntüler internet tabanlı sunucularda saklanmaktadır. Bu görüntülerin güvenilir bir şekilde saklanması için en uygun yöntem verilerin şifrelenmesi işlemidir [3]. Verilerin şifrelenmesi için simetrik blok şifreleme ve asimetrik şifreleme işlemleri etkin bir şekilde kullanılmaktadır. Simetrik blok şifreleme kriptografik sistemlerde en yaygın olarak kullanılan şifreleme yöntemidir [4]. Blok şifreleme sistemlerinde şifrelenmek istenen verilerin uzunluğunda bloklara bölünür ve şifreleme işlemi (bloklar halinde) gerçeklenir. En bilindik blok şifreleme algoritmalarından bazıları şunlardır: DES [5] ve AES [6] ve GOST [7] Seth ve Mishra [8] yaptıkları çalışmada DES, AES ve RSA [9] algoritmaları ile şifreleme işlemlerini zaman, hafıza kullanımı ve enerji tüketimi açısından incelemişler ve DES, AES ve RSA algoritmaları ile 500 KB bir veriyi şifreleme işlemi sırası ile 2,6 saniye , 2,4 saniye ve 24,4 saniye sürmüştür. Asimetrik şifreleme algoritmalarının işlem sürelerinin uzun olmasından dolayı CPU tabanlı gerçek zamanlı sistemlerde çok tercih edilmemektedir. Bunun yerine simetrik blok şifreleme algoritmaları daha çok tercih edilmektedir. Yine GPU gibi farklı donanımların kullanılması ile verinin paralel işlenerek şifreleme süresi önemli ölçüde kısalabilmektedir [10].

Yüz tespiti, örüntü tanıma alanındaki zorlu problemlerden bir tanesidir. 1994 yılının başlarında Vaillant ve diğerleri görüntüdeki yüzleri algılamak için yapay sinir ağlarını kullanmışlardır [11]. Geliştirilen sinir ağını eğiterek bir görüntüdeki yüzün varlığını veya yokluğunu tespit edebilecek bir model önermişlerdir. 2002 yılında Gracia vew Delakis tarafından kompleks bir görüntüde yarı ön yüzü tanımak adına bir sinir ağı geliştirilmiştir [12]. 2007 yılında Osadchy ve diğerleri poz tahmini ve yüz tespit etmek için evrişimli sinir ağı yapısı önermişlerdir [13].

Son yıllarda, derin öğrenmenin hızlı gelişimi ile birlikte, hedef tespiti çalışmalarına dayalı olarak büyük bir gelişme kaydedilmiştir. Derin öğrenmeye dayalı iki tür nesne algılama vardır: bunlardan biri bölgesel algılamaya dayılı R-CNN yapıları [14], [15] ve diğer yapılar ise SSD [16] ve YOLO [17] yapılarıdır. Bölgesel algılamaya dayalı yapılarda, her türlü potansiyel bölgesel üretici parça ve çeşitli özellik katmanları içerdiğinden dolayı, bu da yüksek işlem maliyetinden dolayı algoritmanın gerçek zamanlı sistemlerde çalışmasını zorlaştırmaktadır. Bunun yerine YOLO mimarileri daha yüksek hızlarda çalışmaktadırlar. Bu sebepten dolayı son zamanlarda YOLO mimarisi kullanılarak yüz tespiti uygulamalarının geliştirilmesi popüler hale gelmiştir [18].

Bu çalışmada video gözetim sistemlerinden gelen görüntüler kaydedilmeden önce veri güvenliği açısından şifrelenmesi ve görüntülerin şifreli bir şekilde kaydedilmesi amaçlanmıştır. İşlem süresini kısaltmak adına tüm veriyi şifrelemek yerine YOLO V4 - Tiny [19] modeli ile tespit edilen yüz (bölgesinin) verisinin şifrelenmesi hedeflenmiştir.

2 TEMEL ALINAN ALGORİTMALAR

2.1 YOLO Mimarisi

YOLO (You Look Only Once), 'Sadece Bir Kez Bak' anlamına gelmektedir. YOLO mimarisi ilk olarak Joseph Redmon ve diğerleri tarafından geliştirilmiştir. YOLO mimarisi, tek bir çerçevede birden fazla nesneyi tanıyabilen gerçek zamanlı bir nesne takibi için CNN kullanan en yaygın algoritmadır. YOLO zamanla YOLOv2 [20], YOLOv3 [21] ve YOLOv4 [22] olmak üzere daha yeni sürümlere dönüşmüştür. YOLO, önceki diğer algılama sistemlerinden tamamen farklı bir yaklaşım kullanıp; Tüm görüntüye tek bir sinir ağı uygulanmaktadır. Bu ağ, görüntüyü bölgelere ayırır ve her bölge için sınırlayıcı kutuları ve olasılıkları

tahmin eder. Bu kutulara Bounding Box denir. Bu sınırlayıcı kutular, tahmin edilen olasılıklarla ağırlıklandırılır. YOLO, girdi görüntüsünü S×S boyutundaki ızgaralara böler ve her ızgara hücresi, o ızgara hücresinde ortalanmış nesneyi tahmin etmeye çalışır. Her ızgara hücresi, B sınırlayıcı kutuları için güven puanlarını tahmin eder. Bu güven puanları, kutunun bir nesne içerdiğinden ne kadar emin olduğunu ve ayrıca kutunun tahmin ettiğinin ne kadar doğru olduğunu gösterir. YOLO her bounding box için ayrı ayrı tahmin vektörleri oluşturur. Bu vektörlerin içerisinde bahsedilen güven skoru, nesnenin koordinatları ve boyutları bulunur. YOLO modelinin sınıflandırıcı tabanlı sistemlere göre birçok avantajı vardır: Tek bir çerçevede birden fazla nesneyi tanıyabilir. Test zamanında görüntünün tamamına bakar, ayrıca R-CNN gibi tek bir görüntü için binlerce işlem gerektiren sistemlerden farklı olarak tek bir ağ değerlendirmesi ile tahminler yapar. Bu sayede R-CNN'den 1000 kat daha hızlı ve Faster R-CNN'den 100 kat daha hızlı çalışabilmektedir [23]. YOLO tasarımı, yüksek ortalama hassasiyeti korurken uçtan uca eğitim ve gerçek zamanlı sistemlerde çalışma imkânı sağlamaktadır.

2.2 YOLOv4-tiny Mimarisi

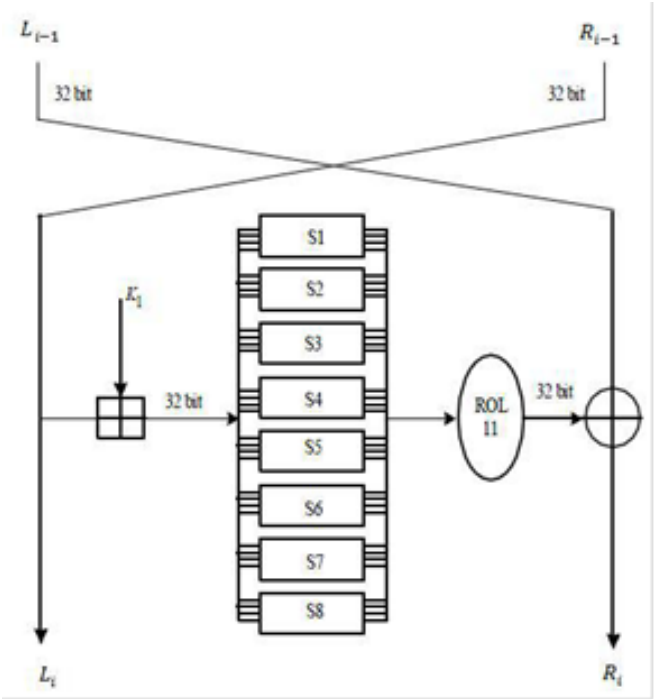
YOLOv4, YOLOv3 modelinin gelişmiş bir versiyonu olan nesne algılama algoritmasıdır. Performans olarak EfficientNet'ten iki kat daha hızlıdır. Ayrıca YOLOv4'teki AP (Ortalama Hassasiyet) ve FPS (Saniyedeki Kare Sayısı), YOLOv3'e kıyasla sırasıyla %10 ve %12 daha fazladır [22]. YOLOv4'ün mimarisi, omurga olarak CSPDarknet53, uzamsal piramit havuzlama ek modülü, PANet yol toplama boynu ve YOLOv3 kafasından oluşmaktadır.

YOLOv4-tiny, YOLOv4'ün sıkıştırılmış bir versiyonudur. Ağ yapısını daha basit hale getirmek ve parametreleri azaltmak, böylece mobil ve gömülü cihazlarda geliştirmeyi mümkün kılmak için YOLOv4'e dayalı olarak önerilmiştir. YOLOv4-tiny daha hızlı eğitim ve daha hızlı algılama için kullanabilmektedir. YOLOv4'teki üç kafanın aksine sadece iki YOLO kafasına sahiptir. Yine önceden eğitilmiş 137 konvolüsyonel katman ile eğitilmiş YOLOv4'ün aksine, önceden eğitilmiş 29 konvolüsyonel katman ile eğitilmiştir.

YOLOv4-tiny'deki FPS, YOLOv4'ün yaklaşık sekiz katıdır. Ancak, MS COCO veri kümesinde test edildiğinde YOLOv4-tiny'nin doğruluğu YOLOv4'ün 2/3'ü kadardır. YOLOv4-tiny modeli, RTX 2080Ti'de 443 FPS hızında %22,0 AP'ye (%42,0 AP50) ulaşırken, TensorRT, parti boyutu = 4 ve FP16-hassasiyeti kullanıldığında YOLOv4-tiny, 1774 FPS'ye ulaşmaktadır [24]. Gerçek zamanlı nesne algılama için YOLOv4-tiny, YOLOv4 ile karşılaştırıldığında daha iyi bir seçenektir, çünkü gerçek zamanlı nesne algılama ortamıyla çalışırken daha hızlı çıkarım süresi, hassasiyet veya doğruluktan daha önemlidir.

2.3 Gost 28147-89 Şifreleme Algoritması

GOST 28147-89, Sovyetler Birliği tarafından 1989'da geliştirilmiş bir blok şifreleme algoritmasıdır [25]. GOST 28147-89, verileri 64 bitlik yapılara bölerek 256 bitlik bir anahtar ile şifreler ve bu işlem 32 tur boyunca devam eder. GOST fiestal ağ yapısına sahip olup; bu özelliği sayesinde şifreleme ve şifre çözmede aynı algoritma kullanılır [26]. Algoritma bir tur için Şekil 1'de gösterildiği gibi çalışır.



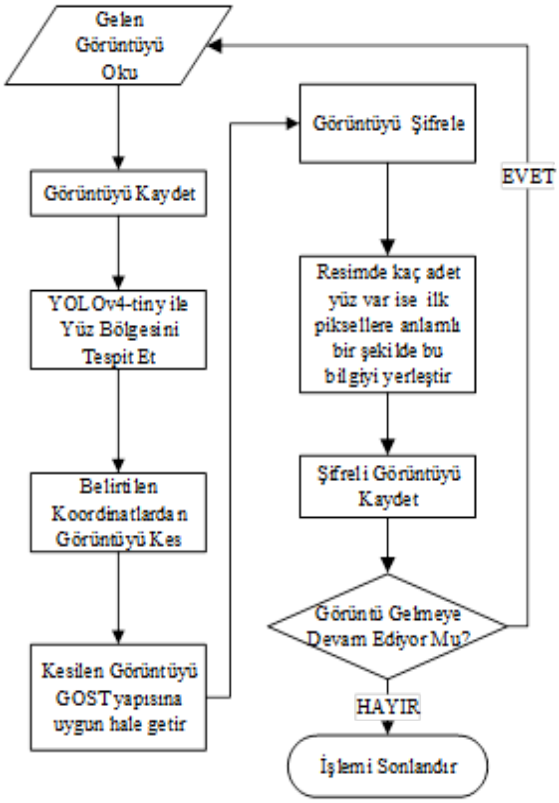
Şekil 1 . Bir turda GOST 28147-89 Şifreleme Algoritması

Anahtar uzunluğu 256 bit olup 8 adet alt anahtar vardır ve her bir alt anahtarın uzunluğu 32 bittir. GOST şifreleme işlemi 32 turlu bir yapıya sahip olup her alt anahtar bu 32 tur boyunca dörder kez kullanılır. Şifreleme işlemindeki veri karıştırma işlemi S-Box yapıları ile yapılmaktadır. Bir turda şifreleme işlemi şu şekilde gerçekleşmektedir. İlk önce şifrelenmek istenen veri 64 bitlik yapılara

bölünür. Daha sonra bu 64 bitlik veri 32 bit sağ ve 32 bit sol verisi olmak üzere ikiye ayrılır. 32 bitlik sağ verisi ilgili tura ait alt anahtar ile modulo 32 toplaması yapılır. Toplam sonucu olan 32 bitlik veri 8 eşit parçaya bölünür. Bu 8 adet 8 bitlik veri 8 adet S-Box'ın girişi olur. 32 bitlik veri S-Box'lar vasıtasıyla karıştırıldıktan sonra çıkış verisi 11 bitlik sola kaydırma operatörüne gider. 11 bitlik sola kaydırma operatörünün çıkışı ise 32 bitlik XOR işlemine gider ve bu işlemden sonra ilk tur tamamlanmış olur. Tüm bu işlemler 32 tur boyunca tekrarlanır ve böylece şifreli veri elde edilmiş olur.

3 Önerilen Yöntem

Bu çalışmada güvenlik kamera kayıtlarını ve kişisel kamera kullanımı daha güvenli getirmek adına görüntülerdeki yüzlerin tespit edilmesi ve devamında tespit edilen yüz bölgesini şifreleyen bir yöntem önerilmiştir. Önerilen yöntemin çalışması Şekil 2'deki gibidir.



Şekil 1. Önerilen Yöntem

Önerilen yöntemde ilk olarak resimdeki yüz bölgesi tespit edilmektedir. YOLOv4-tiny algoritması yüz bölgesine ait başlangıç koordinatını(x1,y1) ve bitiş koordinatını(x2,y2) vermektedir. GOST 64 bitlik blok şifreleme algoritması olup; şifreleme işleminde padding işlemi yapmamak adına şifrelenmek istenilen veri 8 pikselin (64bit) katı olarak belirlenmektedir. Yüz koordinatlarına ait uzunluk ve genişlik verisi 100, 100 ise her iki değerde 8in katı olacak şekilde bir üst sayıya çevrilecektir. Yani yeni değer 104, 104 olarak hesaplanacaktır. Hesaplanan bu yeni değere göre görüntü üzerindeki ilgili yüz bölgesi kesilecek ve devamında bu kesilen yüz bölgesi şifrelenecektir. Görüntüde birden fazla yüz olması durumunu da göz önünde bulundurarak görüntünün ilk pikseline tespit edilen yüz sayısı yazılacak, diğer piksellere de bulunan yüzlerin koordinatları yazılacaktır. Görüntü formatı 8 bitlik gri formatta görüntü olmak üzere örneğin görüntüde 3 adet yüz tespit edildi ve bu yüzlere ait koordinatlar şu şekilde ise: (100,100)/(148,148), (200,200)/(280,280), (300,300)/ (364,364) tüm bu verileri görüntü ile karşı tarafa aktarmak için ilk 8 bite 3 verisi, sonraki 16 bite 100 verisi ve devam eden her 16 piksele ilgili koordinat verileri sırası ile yazılacaktır. Yani 1 adet yüz tespit edildi ise gri formattaki bir görüntü için şifreli yüze ait verileri ilk 9 piksel, 2 adet yüz tespit edildi ise gri formattaki bir görüntü için şifreli yüze ait verileri ilk 17 piksel taşıyacaktır. Sonuç olarak gri formattaki görüntüde n adet yüz tespit edildi ise 8*n+1 adet piksel ile şifrelemeye ait veriler karşı tarafa aktarılacaktır.

4 Deneysel Sonuçlar

Yüz tespiti için laboratuvar ortamında 73 fps hızında bir renkli kamera kullanılmıştır. Test sonuçları için yazarların laboratuvar ortamındaki yüz görüntüleri kullanılmıştır. Kullanılan kameranın çözünürlüğü 1440x1080 piksel olup; bu çalışmada 1440x1080, 1280x720(HD) ve 640x480(VGA) çözünürlükleri ile 8 bitlik gri formatta görüntüler kullanılmıştır. Uygulama için iki farklı test ortamı kullanılmış olup; bunlardan ilki: i5 10400f işlemcili, 16GB DDR4, 256 GB M2SSD bir bilgisayar olup; diğer sistem ise i9 10900f işlemcili, 32GB DDR4 Ram ve 512 GB M2SSD özelliklerine sahip bilgisayar test ortamı olarak kullanılmıştır. Algoritma geliştirme ve test işlemlerini gerçeklemek için Visiul Studio 2019 derleyicisi, C++ yazılım dili ve OpenCV 3.2 görüntü işleme kütüphanesi kullanılmıştır. Yüz tespiti için wider face veri seti ile eğitilmiş [27] YOLOv4-tiny yapısı [28] kullanılmıştır.

4.1 Test Görüntüleri ile Elde Edilen Sonuçlar

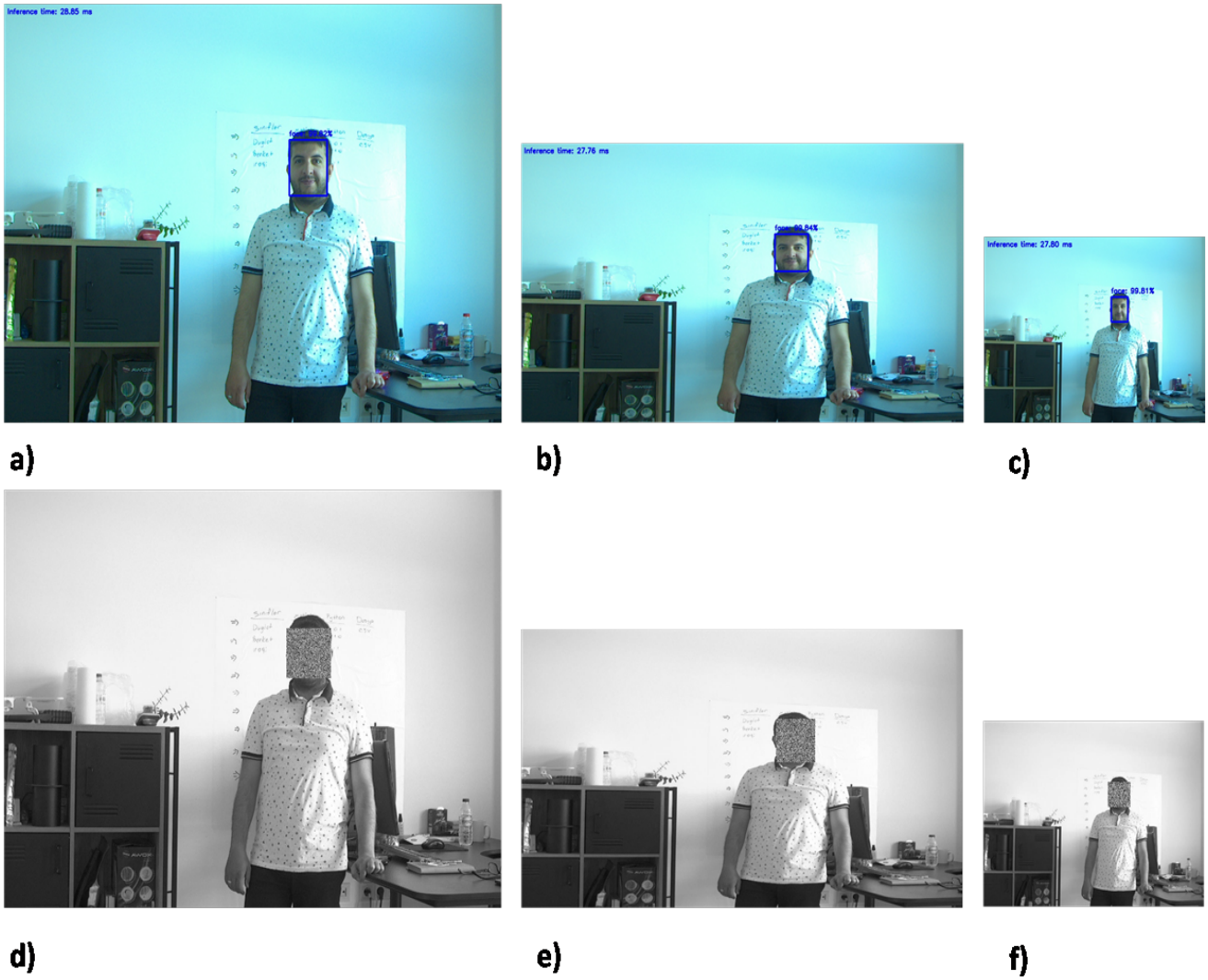
Bu çalışmada iki temel algoritma kullanılmıştır. Bunlar YOLOv4-tiny ve GOST 28147-89 Şifreleme Algoritmasıdır. Her iki algoritmada işlem yükü

yüksek algoritmalar olup; i5 işlemci üzerinde elde edilen test sonuçları Tablo 1'deki gibidir. YOLOv4-tiny modeli ile yüz tespit işlemleri sürekli değişmekle birlikte maksimum 30ms olarak tespit edilmiştir.

Tablo 1. i5 İşlemci İle Yüz Tespiti Ve Şifreleme Süreleri

Görüntü Formatı	Yüz Bölgesi	Yüz Tespit Süresi	Şifreleme Süresi	Ara İşlemler	Toplam Süre
1440x1080	128x128	30 ms	45 ms	8 ms	83 ms
1280x720	80x80	30 ms	20 ms	6 ms	56 ms
640x480	56x56	30 ms	8 ms	3 ms	41 ms

Kullanılan kameranın orijinal çözünürlüğü 1440x1080 olup; farklı çözünürlüklerde algoritmanın zaman testlerini yapabilmek adına orijinal görüntü HD ve VGA çözünürlükteki görüntülere boyutlandırılmış ve performans testleri yapılmıştır. Tablo 1' de kullanılan görüntüler ve şifreleme sonuçları Şekil 3' teki gibidir. Yüz tespit işlemi için RGB görüntüler kullanılmıştır. YOLOv4-tiny modeli ile elde edilen yüz koordinatlarına göre şifreleme işlemi ise işlem yükünü azaltmak adına gri formattaki görüntüler üzerinde yapılmıştır. Donanıma bağlı performansı ölçmek adına bir sonraki aşamada Tablo 1' deki tüm değerler i9 işlemcili bilgisayar üzerinde denenmiş ve test sonuçları Tablo 2' deki gibidir. İ9 işlemci kullanılması sonucu şifreleme süresinde ve toplam sürede ciddi bir değişiklik olmuştur.



Şekil 2. Orijinal ve Şifreli Görüntüler; a) 1440x1080 boyutundaki görüntü, b)1280x720 boyutundaki görüntü, c) 640x480 boyutundaki görüntü, d)1440x1080 boyutunda yüz bölgesi şifreli görüntü, e) 1280x720 boyutunda yüz bölgesi şifreli görüntü, f) 640x480 boyutunda yüz bölgesi şifreli görüntü

Tablo 2. İ9 İşlemci ile Yüz Tespiti ve Şifreleme Süreleri

Görüntü Formatı	Yüz Bölgesi Boyutları	Yüz Tespit Süresi	Şifreleme Süresi	Ara İşlemler	Toplam Süre
1440x1080	128x128	25 ms	39 ms	7 ms	71 ms
1280x720	80x80	25 ms	16 ms	4 ms	45 ms
640x480	56x56	25 ms	6 ms	2 ms	33 ms

Bu çalışmada tüm görüntüyü şifrelemek yerine işlemleri hızlandırmak adına sadece yüz bölgeleri şifrelenmiştir. Tüm görüntü şifrelenmek istenirse 1440x1080, 1280x270 ve 640x480 görüntüleri için şifreleme süreleri sırasıyla 4971ms, 2967ms ve 1007ms olarak hesaplanmıştır. Şifreleme işleminin tüm görüntü yerine yüz bölgesi üzerinde yapılması toplam süreyi yaklaşık olarak %90 - %95 oranında azaltmaktadır.

4.2 Sonuçların Veri Setleri ile Test Edilmesi

Bu çalışmada güvenlik kamerası kayıtlarının güvenli bir şekilde saklanabilmesi için öncelikle görüntülerdeki yüz bölgeleri YOLOV4-tiny modeli ile tespit edilmiş devamında ise tespit edilen bu yüz bölgeleri GOST 28147-89 algoritması ile şifrelenmiştir. Geliştirilen uygulama ilk olarak Şekil 3' teki görüntüler üzerinde test edilmiştir. Söz konusu görüntüler test amaçlı kullanılmış olup; sistemin gerçek bir uygulama ortamında çalışmasını test etmek adına Luber ve ark tarafından geliştirilen veri seti kullanılmıştır [29]. Kullanılan veri seti üzerinde YOLOv4-tiny modeli ile yüz tespiti %95 üzerinde bir doğruluk sağlamıştır. Şekil 4' te görüntüdeki iki kişi tespit edilmiş olup tespit işlemi 25ms, iki yüzün şifrelenmesi ise 47ms sürmüştür.

!" #"

Şekil 3. Veri seti test sonuçları a) Görüntü üzerinden tespit edilen yüzler b) Tespit edilen yüzlerin şifrelenmesi

Ara işlemler ile birlikte toplam işlem süresi 77ms sürmüştür. Görüntüler RGB formatta olup şifrelenmeden önce görüntü gri formata çevrilmiştir.

5 Sonuçlar ve Gelecek Çalışmalar

Bu çalışmada yüz verilerinin güvenli bir şekilde ağ üzerinde kaydedilmesi için YOLOv4-tiny ile yüz bölgesinin tespit edilmesi ve GOST şifreleme algoritmasının efektif bir şekilde kullanıldığı bir yöntem önerilmiştir. Önerilen yöntemin gerçek zamanlı sistemlere uygun hale getirilmesi için tüm resmi şifrelemek yerine görüntü üzerinde tespit edilen yüz bölgeleri şifrelenerek şifreleme işlemi daha kısa sürelerde gerçekleştirilmiştir. Yine işlem sürelerinin farklı donanımlarda ne kadar sürede gerçeklendiğini ölçmek adına i5 ve i9 işlemciye sahip iki farklı bilgisayar kullanılmıştır. HD görüntülerde yüz bölgesinin tespit edilmesi ve tespit edilen yüzün şifreleme işlemleri i5 ve i9 işlemcileri için sırasıyla 56 ms ve 45 ms sürmüştür.

Elde edilen sonuçlar güvenlik kamerası kayıtlarının gerçek zamanlı olarak HD çözünürlükte ve düşük fps değerlerinde şifreli bir şekilde kaydedilmesine olanak sağlayacak seviyededir. Gelecek çalışmalarda şifreleme işlemlerinin işlemci üzerindeki iş parçacıkları ile paralel bir şekilde yapılması ya da GPU üzerinde gerçeklenmesi sayesinde daha yüksek fps değerlerinde yapılması hedeflenmektedir. Bu çalışmada sadece gri formattaki görüntüler şifrelenmiş olup gelecek çalışmalarda RGB formatındaki verilerinde şifrelenmesi işlemleri yapılacaktır. Yine gelecek çalışmalarda önerilen yöntemin daha da geliştirilerek online toplantı platformlarında gerçek zamanlı olarak çalıştırılması hedeflenmektedir. Bu sayede kamu ve özel sektördeki kritik öneme sahip görüşmelerin güvenli bir şekilde yapılması hedeflenmektedir.

Kaynaklar

[1] Grand View Research 2022,, https://www.grandviewresearch.com/industry-analysis/surveillance-camera-market-report#:~:text=Report%20Overview,10.7%25%20from%202023%20to%202030,son erişim tarihi, 11 Şubat 2023

[2] P. Vennam, T. C. Pramod, B. M. Thippeswamy, Y. G. Kim, and B. N. Pavan Kumar, "Attacks and preventive measures on video surveillance systems: A review," Appl. Sci., vol. 11, no. 12, doi: 10.3390/app11125571., 2021.

[3] X. Zhang, S. H. Seo, and C. Wang, "A Lightweight Encryption Method for Privacy Protection in

Surveillance Videos," IEEE Access, vol. 6, pp. 18074–18087, doi: 10.1109/ACCESS.2018.2820724., 2018.

[4] D. R. Stinson, "Cryptography Theory and Practice, Second Edition. Chapman and Hall/CRC, 2005.

[5] M. E. Smid and D. K. Branstad, "Data Encryption Standard: past and future," in Proceedings of the IEEE, vol. 76, no. 5, pp. 550-559, , doi: 10.1109/5.4441., May 1988.

[6] "Advanced Encryption Standard (AES)", Federal Information Processing Standards, doi:10.6028/NIST.FIPS.197,2001.

[7] G. S. GOST ,". Cryptographic protection for data processing systems," Government Committee of the USSR for Standards. 28147-89,1989.

[8] S. M. Seth and R. Mishra, "Comparative Analysis Of Encryption Algorithms For Data Communication," Ijcst, vol. 2, no. 2, pp. 292–294, 2011.

[9] L. Rivest, R. L., Shamir, A. and Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21.2, 1978.

[10] J. P. D'Amato, and M Venere., "Encrypting video streams using OpenCL code on-demand ",2011.

[11] R. Vaillant, C. Monrocq, and Y. Lecun, "Original approach for the localisation of objects in images," IEEE Proceedings on Vision, Image, and Signal Processing, vol. 4, 1994.

[12] C. Garcia and M. Delakis, "A neural architecture for fast and robust face detection," IEEE Trans. Pattern Anal. Mach. Intell., vol. 26, no.11, pp. 1408–1423, 2004.

[13] M. Osadchy, Y. Le Cun, and M. L. Miller, "Synergistic Face Detection and Pose Estimation with Energy-Based Models," Journal of Machine Learning Research, vol. 8, pp. 1197-1215, 2007.

[14] R. Girshick, "Fast R-CNN," Proc. IEEE International Conference on Computer Vision, ICCV 2015, pp. 1440–1448, 2015.

[15] S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: towards realtime object detection with region proposal networks," Proceedings of the 28th International Conference on Neural Information Processing Systems - Volume 1. MIT Press, pp. 91–99, 2015.

[16] W. Liu, D. Anguelov ,D. Erhan ,C. Szegedy, S. Reed, S.,C. Y. Fu and A. C. Berg, Ssd: Single shot multibox detector. 9905th ed., IEEE ECCV, pp. 21-37., 2016.

[17] J. Redmon, S. Divvala, R. Girshick and A. Farhadi., You only look once: Unified, real-time object detection, IEEE CVPR, pp. 779-788., 2016.

[18] D. Garg, P. Goel, S. Pandya, A. Ganatra and K. Kotecha, "A Deep Learning Approach for Face Detection using YOLO," IEEE Punecon, pp. 1-4, doi: 10.1109/PUNECON.2018.8745376. 2018.

[19] Z. Jiang, L. Zhao, S. Li, and Y. Jia, Real-time object detection method based on improved YOLOv4-tiny. arXiv:2011.04244, 2020.

[20] J. Redmon and A. Farhadi, YOLO9000: better, faster, stronger. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 7263-7271).2017.

[21] J. Redmon and A. Farhadi,Yolov3: An incremental improvement. arXiv:1804.02767, 2018.

[22] A. Bochkovskiy, C. Y. Wang and H. Y. M. Liao, Yolov4: Optimal speed and accuracy of object detection. arXiv:2004.10934, 2020.

[23] https://viso.ai/deep-learning/object-detection/ , erişim tarihi 06.06.2022

[24] C. Y. Wang, A. Bochkovskiy and H. Y. M. Liao, Scaled-yolov4: Scaling cross stage partial network. In Proceedings of the IEEE/cvf conference on computer vision and pattern recognition ,(pp. 13029-13038).2021.

[25] V. V. Shorin, V. V. Jelezniakov, and E. M. Gabidulin, "Linear and differential cryptanalysis of Russian GOST," Electron. Notes Discret. Math., vol. 6, no. April 2001, pp. 1–10, 2000.

[26] H. Aktaş, "Implementation of GOST 28147-89 Encryption and Decryption Algorithm on FPGA," International Conference on Cyber Security and Computer Science (ICONCS'18), Safranbolu, Turkey, 2018.

[27] S. Yang, P. Luo, C. C. Loy and X. Tang. WIDER FACE: A Face Detection Benchmark ,IEEE Conference on Computer Vision and Pattern Recognition (CVPR),2016.

[28] https://github.com/ltkhang/face-detection-yolov4-tiny, erişim tarihi 07.06.2022.

[29] M. Luber, L. Spinello and K. O. Arras, People Tracking in RGB-D Data With On-line Boosted Target Models. *IEEE Int. Conf. on Intelligent Robots and Systems (IROS)*, 2011.

Cloud App Data Privacy to Comply with GDPR

Eugene Alooeff[1]*

[1]*ATEK, R&D Department, Wroclaw, Poland*

Abstract

In this paper we analyzed current law for data protection, requirements and trends in cybersecurity. We developed the data schema and algorithms to let the cloud applications comply with data protection regulations in the European Union. This solution had practical implementation on the health center cloud infrastructure. Security assessment has been passed and the system was successfully launched in production.

Keywords: *GDPR, PII, Data Privacy, Security, Compliance.*

1 Introduction

The EU General Data Protection Regulation (GDPR) is enforced across all EU Members from 2018, is a landmark in the evolution of the European privacy framework [1]. This law covers the personal data of all EU residents, regardless of their processing location. Personal data is information that, directly or indirectly, can identify an individual and specifically includes online identifiers such as IP addresses, location data. GDPR aims to bring a single standard for data protection among all EU member states, and applies to entities that operate in the EU or deal with the data of any EU resident, regardless of where the data is processed. This is much wider than the concept of personally identifiable information (PII) in US privacy law [2].

Depending on where your organization operates and what data stores, you may need to adhere to location-specific privacy laws. For example, if your organization operates in Turkey, you are subject to the Law on the Protection of Personal Data [3] and Regulation on Deletion, Destruction or anonymization of Personal data [4].

Globally, there are two types of privacy laws: comprehensive (applicable to all industries and sectors) and sectoral (applicable to specific industries or sectors). In the US, the federal government has historically taken a sectoral approach. For example, there's the Health Insurance Portability and Accountability Act (HIPAA) [5], which is the US healthcare privacy law protecting data that reveals the health status of an individual.

Cybersecurity compliance involves meeting various controls to protect the confidentiality, integrity, and availability of data. Regulatory compliance insists that the organizations should follow local, state, federal, and international laws and regulations relevant to its business function.

Many existing cloud operators process data submitted by customers for the purpose of providing online services to them. To fulfill these purposes, cloud operators may access the data to provide the services, to correct and adress technical issues. To show the compliance to the law, the can implement the Data Privacy Framework (DPF) program and publish the notice of certification under it [6].

2 Apply data privacy principles

There are many key privacy principles. In this work we take into account some of them:

Security principle - Anonymization technique - the process of protecting private or sensitive information by erasing, obfuscating (masking), or encrypting it. It removes all identifiers associated with a person [7]. If data is truly anonymized, then the data does not constitute personal data under the GDPR. However, the bar to be considered anonymous is high: It must be impossible for any individual to be identified from the data by any further processing or by combining it with other information.

Data Deletion and Retention - Organizations should only store personal data for as long as it's required and for the originally intended purpose. Organizations should not keep any personal data for an indefinite period even if it may be used in the future. Clear time frames should be established for when data is deleted with rationale for why the data

*Contact email: alooeff@gmail.com

is retained for that length of time. For example, you may need to retain security log files for certain periods of time to identify and track malicious adversary behaviors. However, the period still must remain finite, with supporting rationale. You should also be aware of data retention laws for specific types of data, such as legal documents, within the country where your organization provides that service.

3 GDPR and privacy by design

Privacy by Design is a key concept of the GDPR and is made a legal requirement. Privacy by Design means thinking about data privacy and its implications when you're developing products, features, even marketing campaigns based on personal data. It also means encouraging employees to ask themselves questions before collecting or using data:

- Do I need all the data I'm collecting here?
- Could I do this work without using personal data at all?
- Am I using the data in a way a user may not expect?
- And do I have a plan to delete this data once myself or my team no longer need it?

The GDPR also encourages organizations to document key privacy decisions they make around the collection, use and storage of personal data. Documenting compliance with the GDPR may be one of the most challenging and time consuming aspects of this law. There are several ways an organization can demonstrate and document compliance. Your organization may need to complete a privacy review process of products or features to ensure GDPR compliance before they go live [8].

This is often referred to as a data protection impact assessment or DPIA. DPIA's help document key decisions within an organization that have a privacy impact. companies should also inventory the personal data it stores and collects. Also companies should. update its existing policies and procedures or develop new ones that outline how personal data will be protected, deleted and processed.

4 Purpose

Since companies work with customer's data, they are personal data processors. They perform such operations on personal data, as collection, storage, alteration, retrieval, erasure or destruction. From the moment when any personal data gets uploaded to the company databases, they become a Processor of personal data. Under the GDPR, it is also mandatory for processors to designate a Data Protection Offices (DPO) [9].

To let Processors to comply with security requirements, we developed objects schema and the algorithms, implemented and tested them on practice.

5 Algorithm

To let Processors to comply with security requirements, we developed objects and the methods and tested them on practice.

Developed algorithm and objects can be implemented either as a part of internal system or as external system and work through API. To implement GDPR requirements in part of data retention and deletion / anonymization, we have to use 2 objects:

- Wipeout Policy object to store policies for each object in the database we have to apply the logic.
- Wipeout Policy Count object to store the history of the number of records affected by Wipeout Policy.

The records in the first object (Table 1) are being created and updated by the system administrator in accordance with the current database used in company and do not depend on the IT infrastructure.

Table 1. Wipeout Policy object definition.

Field Name	Type	Value Example
Name	text	Customer wipeout policy
Query	text	CLEAR UserName, Phone, Email FROM Appointment WHERE (Status = 'Closed') AND End < LAST_N_DAYS:180 AND End > LAST_RUN
Object Name	text	Customer
Wipeout Action	picklist	Clear_Fields / Deletion
Fields	Text	Name, Phone, Email, Priority
Values	text	null, null, null, normal
Retention Period	number	180
Wipeout Criteria	text	Status = 'Closed'
Active	boolean	true
Bypass Trigger	boolean	true

Each record is a rule, used by wipeout logic and corresponds to one Object (**Object Name** field). If

Wipeout Action is 'Clear_Fields', then the '**Fields**' and '**Values**' have text (comma separated values) about what object fields should be cleared (filled with null or blank values) or set to default value in case of picklist. If **Wipeout Action** is 'Deletion', then the records are being deleted. '**Wipeout Criteria**' field stores the rule to select the processing records by specific criteria. For example, for closed accounts, finished orders or paid bills. The format of this criteria should be just the WHERE condition for SQL query. In addition, '**Retention Period**' field shows the period when object records should remain unwiped. It needs to have the ability to control or audit closed deals for retention periods. **Query** field is generated on the policy criteria and retention period in SQL style. It is used on the dashboard to show how the set of records is selected. Finally, '**Bypass Trigger**' field shows whether the object trigger should be switched off during the object record processing (deleting or updating operation) to avoid additional logic run, as standard field validation or sending notifications.

The records in the second object (Table 2) are being created by Wypeout Scheduler and updated by Wypeout Batch. Each record is information about the daily run of Wipeout Batch and the result of its work. **Query** field is a copy of Wipeout Policy Query field in the moment of running the Wipeout Batch for future analysis if needed. **Before Count** and **After Count** fields show the number of fields in the **Query** before wipeout action and after. In the ideal situation (when there are no any errors) **After Count** should be always zero. **Start Time** field allows to keep the last run time to eliminate processing the records already processed previously. Dashboard uses the information from this object to show the history of batches that were run for the last days and create a chart for brief overview.

Table 2. Wipeout Policy Count object definition.

Field Name	Type	Value Example
Name	text	Customer wipeout policy
Policy Id	Id	
Batch Job Id	Id	
Query	text	CLEAR UserName, Phone, Email FROM Appointment WHERE (Status = 'Closed') AND End < LAST_N_DAYS:180 AND End > LAST_RUN
Object Name	text	Customer
Wipeout Action	picklist	Clear_Fields / Deletion
Before Count	number	1234
After Count	number	0
Start Time	datetime	
End Time	datetime	

To implement GDPR/HIPAA requirements in part of data retention and deletion / anonymization, we use 2 code blocks.

Wipeout Scheduler is the algorithm, which is scheduled to run daily. It gets all the active Wipeout Policies, and do such steps for all of them:

- Find the newest record in 'Wipeout Policy Count' object for current policy Id. Record should have Batch Job Id and Run Time End value.
- Create filter for the records to process by merging the criteria in 'Wipeout Policy' with the Start Time in 'Wipeout Policy Count' record.
- Get the current number of records in the DB which match the policy criteria.
- Create a new 'Wipeout Policy Count' record with 'Query', 'Before Count' and 'After Count' values, received in the previous step.
- Run Wipeout Batch for current policy.
- Repeat the logic for the next policy

Wipeout Batch is the algorithm, which process records in the next steps:

- Get the chunk of records based on policy and retention period criteria.
- Deactivate object trigger if needed by policy.
- Run the logic depending on Wipeout Action (clear fields or delete records). – Get 'Wipeout Policy Count' record related to this Batch Job Id.
- Update 'Run Time End' field with actual date/time and 'After Count' field with the number of the records failed during clearing or deleting.
- Repeat the logic for the next chunk of records.

6 Results

System administrator has access to the dashboard (Fig. 1), which shows the list of wipeout policies with SQL to retrieve the record to process (Description field) and the chart for the last month. On this chart we can see 2 graphs for 'Before Count' and 'After Count' values. In an ideal situation, the last graphs should always show zero values (all the records were processed successfully).

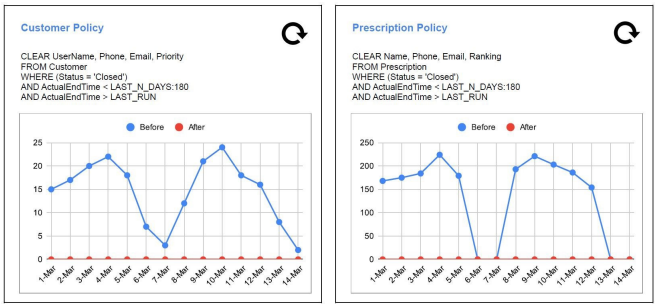


Fig.1. Dashboard

Retention period and Fields for wiping out are easily accessible to updating by system administrator and there is no need to change or reschedule the code logic. Being scheduled once, Wipeout Scheduler runs Wipeout Batches daily and puts the result into the Wipeout Policy Count object for easy monitoring by Dashboard.

7 Implementation in practice

Using a cybersecurity assessment and a structured approach to identifying regulations and implementing controls we have successfully implemented algorithms described above and tested them on the Health Care center. Internal audit of implementation and half-a-year run showed that after the retention period all obsolete sensitive information in the company database is being erased successfully in accordance with the internal documents related to GDPR. Dashboard shows the number of records processed and is easy to read and monitor the work of algorithms. As a result, implemented solution meets cybersecurity regulations and safeguard customers against cybersecurity attacks.

8 Trends in cybersecurity compliance

Trends in cybersecurity compliance and regulation are affecting organizations everywhere. Today's regulatory environment is more challenging than ever.

Cybersecurity Compliance Is Not Just an Information Technology Issue. Many fear cybersecurity compliance as an amorphous issue that only the information technology department handles. The reality is that the financial, legal, and reputational ramifications that arise from a data breach affect the entire organization.

If standards, regulations, or rules are too burdensome, organizations and their employees may engage in insecure workarounds to meet business needs. It's important to communicate to staff how to attain security without compromising business goals.

As guidance and regulations evolve quickly, organizations may not have the resources to keep up with changes year over year. Cybersecurity is a fast-moving sector, as both attackers and security providers vie to outsmart each other.

Gone are the days where organizations used a spreadsheet to document their controls and then had to copy, paste, and repeat against other regulations. Today, organizations use automation to document once, and then comply against many different standards. They use automated tools to collect evidence—such as vulnerability scan results and analysis, log correlation, and more—to assess their security posture, add workflow to task out items such as patching, and report to senior executives.

Automation helps streamline compliance especially with engineers using compliance as code where they design system and products to automatically meet control objectives. One example of automating compliance is the National Institute of Standards and Technology's (NIST's) Open Security Controls Assessment Language (OSCAL) [10].

The recruitment, retention, and training of the right security personnel to help meet compliance requirements is key. Ideally a combination of compliance analysts, security operations specialists, and software engineers make up these teams. Because the burden of regulatory compliance on organizations can be huge, organizations need to create focused cybersecurity teams that work in tandem with their internal risk teams. Organizations must hire more staff who are well-trained on the security aspects related to their industry.

With the economic effects of the COVID-19 pandemic still in full force, organizations are looking to contain costs by working with third-party vendors and partners on an ongoing basis.

One area organizations may look to outsource is compliance. This may be especially true to help perform gap assessments and meet reporting requirements, particularly if a company is small, doesn't have the right staff in house, or needs a small increase in effort for a short time to meet a new regulation or answer a point-in-time audit. As outsourcing compliance becomes more prevalent, frameworks and vendor assessments will also need

to raise the bar for third-party vetting to ensure a degradation in security doesn't occur [11].

References

[1] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[2] Guidance on the Protection of Personal Identifiable Information https://www.dol.gov/general/ppii

[3] Law on the Protection of Personal Data N 6698 https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law

[4] KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VEYA ANONİM HALE GET?R?LMES? HAKKINDA Y?NETMEL?K ttps://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm

[5] Health Insurance Portability and Accountability Act https://www.hhs.gov/hipaa/index.html

[6] Data Privacy Framework (DPF) Program https://www.dataprivacyframework.gov

[7] Anonymization. Imperva Learning Center https://www.imperva.com/learn/data-security/anonymization/

[8] Nishant Bhajaria. Data Privacy. A runbook for engineers. 2022 https://www.manning.com/books/data-privacy

[9] Guidelines on Data Protection Officers https://ec.europa.eu/newsroom/article29/items/612048

[10] OSCAL: the Open Security Controls Assessment Language https://pages.nist.gov/OSCAL/

[11] Forbes: Cybersecurity Compliance Trends in a Post-Pandemic World https://www.forbes.com/sites/forbestechcouncil/2020/05/11/cybersecuritycompliance-trends-in-a-post-pandemic-world/?sh=4a62bd6f4ae2

Siber Güvenlik Meslek Yüksekokulları Özelinde 2023 Yılında Türkiye'de Açılan Tüm Yeni Programların Betimsel Analizi

Ayşe Hümeyra Bayram[1]*

[1]*Gebze Teknik Üniversitesi, Siber Güvenlik Meslek Yüksekokulu, Kocaeli, TÜRKİYE*

Özet

Türkiye'de Yükseköğretim Kurulu Başkanlığı ile T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı'nın 5 Ekim 2022 tarihinde imzaladıkları iş birliği protokolü çerçevesinde Siber Güvenlik Meslek Yüksekokulları (SGMYO) açılmasına karar verilmiş ve 2023 yılında bu karar uygulamaya geçmiştir. SGMYO çatısı altında Siber Güvenlik Analistliği ve Operatörlüğü adındaki ön lisans programı dört farklı üniversitede kurulmuştur. Farklı alanlarda yeni programların da aynı yıl öğrencilere kapılarını ilk kez açtığı tespit edilmiştir. YÖK Atlasta yer alan toplam sekiz yeni programın ilk yerleşim verilerinin betimsel analizinin yapıldığı bu çalışmada; SGMYO'nun açılması kararını aldıran ilgili protokolün, öğrenci tercih davranışlarına nasıl yansıdığının tespit edilmesi ve SGMYO tercihleri ile diğer yeni programların yerleşme sonuçlarının karşılaştırmalı olarak değerlendirilmesi amaçlanmıştır.

Çalışmada; 2023 yılında ilk kez öğrenci alan toplam sekiz programın başarı sıralaması ve taban puanları, bu programlara yerleşen öğrencilerin eğitim durumları, demografik özellikleri yanı sıra mezuniyet başarıları, yerleşme sıralamaları gibi kriterler de analiz edilmiştir.

Sonuç olarak; çalışma, Türkiye'de yükseköğretimdeki yeni eğilimleri ve SGMYO'nun açılmasının öğrenci tercihlerine etkisini anlamak için önemli bir kaynak sunmaktadır. Devlet politikası gereği açılan SGMYO'nun diğer yeni programlara kıyasla başarı seviyesi yüksek yeni öğrencileri, geleceğin siber güvenlik operatörlerinin akademik başarısına bir örneklik sunmaktadır.

Anahtar Kelimeler: *Siber Güvenlik Meslek Yüksekokulu, Siber Güvenlik Operatörlüğü, Siber Güvenlik Analistliği, YÖK Atlas, Betimsel Analiz, T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi*

Descriptive Analysis Of All New Programs Opened In Turkey In 2023, Specifically For Cybersecurity Vocational Schools

Abstract

In Turkey, the Presidency of the Council of Higher Education and the Republic of Turkey. In the framework of the cooperation protocol signed by the Presidential Digital Transformation Office on 5 October 2022, it was decided to open Cyber Security Vocational Schools (CSVS) and this decision was implemented in 2023. Under the umbrella of CSVS, an associate degree section called Cyber Security Analyst and Operator was established in four different universities. It has been found that new parts of different regions opened their doors for the first time in the same year. A descriptive analysis of the first placement data of a total of eight new programs in the YÖK Atlas was made, how the relevant protocol that determines the opening distribution of SGMYO reflects student preferences, and a comparative evaluation of the SGMYO preferences and the starting results of other new programs.

The study analysed criteria such as the success rankings and baseline scores of a total of eight programmes accepting students for the first time in 2023, the educational status of students placed in these programs, their demographic characteristics, as well as their graduation success and placement rankings. As a result; the study provides an important resource for integrating student preferences into the opening of new programmes and CSVS in higher education in Turkey. The new success of

*Contact email: ahbayram@gtu.edu.tr

CSVS, where the government policy is implemented, has a high level of success compared to other new programs and provides an example of the academic success of future cyber security operators.

Keywords: *Cyber Security Vocational School, Cyber Security Analyst, Cyber Security Operator, YÖK Atlas, Descriptive Analysis,T.R. Presidential Office for Digital Transformation*

1 Giriş

Dijital çağın gelişimiyle birlikte, bireysel kullanımdan, kurumsal ve ticari kullanıma kadar her sektör ve alanda siber tehditlerle karşılaşılmaktadır. Tehditlere sebep aktörler, kamu ve özel sektördeki hedeflerine yönelik saldırılarını gerçekleştirmek için taktik, teknik ve prosedürlerini her geçen gün geliştirmekte, bu durum siber güvenlik pozisyonlarındaki açıkların artmasına ve siber güvenlik becerilerindeki eksikliklerin büyümesine yol açmaktadır (1). Yıllardır artan siber güvenlik yeteneklerine yönelik iş gücü talebi karşısında; pedagojik yaklaşımın öngördüğü, en çok talep gören teknik bilgi, beceri ve yetenekler için müfredat belirleme ve oluşturma yaklaşımı (2), Türkiye'de de çözüm yolu olarak benimsenmiştir. Bu doğrultuda 2022 yılında Yükseköğretim Kurulu (YÖK) Başkanlığı ile T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (DDO) Başkanlığı tarafından SGMYO açılmasına karar verilen bir iş birliği protokolü imzalanmış ve bir yıl sonra Siber Güvenlik Analistliği ve Operatörlüğü ön lisans programı dört farklı üniversitede kurulmuştur.

Ülkelerin kültürel mirasları, geleneksel dokuları, bölgesel ihtiyaçları ve teknik bilgi ve becerilere sahip nitelikli işgücü açığı, akademinin bu yönde planlama yaparak ilgili alanlarda yeni programların açılmasına sebep olabilmektedir. Bazen de devlet politikası olarak belirli alanlarda açılan programla teşvik edilmiş, desteklenmiş ve ön plana çıkarılmıştır (3) (4).

2 Yeni programlar hakkında bilgi

Çalışmada ele alınan 2023 yılında ilk kez öğrenci yerleştirmesi yapılan sekiz yeni pozisyonun tamamı aynı saha ve alanda olmayıp öğrencilerine farklı teknik bilgi ve Yetenekleri kazandırmayı hedefleyen programlardan oluşmaktadır (bk. Tablo 1). Siber Güvenlik Analistliği ve Operatörlüğü ile Sanal ve Artırılmış Gerçeklik programları teknoloji ve bilişim alt yapılarıyla öne çıkan iki program olarak dikkat çekerken Bağcılık ve Bağ Ürünleri Teknolojisi programı tarım ve doğa bilimleri ile ilişkilidir. Diğer yeni programlar ise geleneksel ve uygulamalı zanaatlarla ilgili olup, biri Kenevir Dokuma Tezgahtarlığı, diğeri ise Bıçakçılık ve El Aletleri üretimi teknolojisi adında iki programı içermektedir.

2.1 Bağcılık ve bağ ürünleri teknolojisi

Ankara Üniversitesi Kalecik Meslek Yüksekokulunda 2023 yılında açılan Bağcılık ve Bağ Ürünleri Teknolojisi ön lisans programı, bağcılık ve bağda üretilen tarım ürünlerinin üretim aşamaları ile yetiştirilme süreçlerini tüm yönleriyle ele almaktadır. Bu alanda; insana, topluma ve doğaya duyarlı; yüksek mesleki becerilere sahip; sorumluluk bilinci taşıyan; sürekli gelişimi benimseyen; bilgi ve iletişim teknolojilerini ustalıkla kullanan; üretken ve çözüm odaklı teknik uzmanlar yetiştirilmesi hedeflenmektedir. Program boyunca, asma morfolojisi, üretim teknikleri, toprak bilgisi, bağ hastalık ve zararlıları gibi bağcılıkla alakalı temel derslerin yanı sıra, İş sağlığı ve güvenliği, bilgi ve iletişim teknolojisi, işletme hijyeni ve sanitasyon gibi genel uzmanlık dersleri de sunulmaktadır. Programdan başarıyla mezun olan öğrenciler; gıda, organik tarım veya bağcılık işletmelerinde; tohum, fide, fidan ve süs bitkileri yetiştiriciliği yapan sektörlerde; danışmanlık firmalarında; özel ve kamuya bağlı laboratuvarlarda kariyer yapma olanağına sahiptirler (5).

Tablo 1. 2023 yılında ilk defa öğrenci alan programlar.

Program	Üniversite	MYO	Şehir	Üniversite Türü
Bağcılık ve Bağ Ürünleri Teknolojisi	Ankara Üniversitesi	Kalecik Meslek Yüksek Okulu	Ankara	Devlet
Bıçakçılık ve El Aletleri Üretim Teknolojisi	Pamukkale Üniversitesi	Serinhisar Meslek Yüksek Okulu	Denizli	Devlet
Kenevir Dokuma Tezgahtarlığı	19 Mayıs Üniversitesi	Ladik Meslek Yüksek Okulu	Samsun	Devlet
Sanal ve Artırılmış Gerçeklik	İstanbul Üniversitesi Cerahpaşa	Teknik Bilimler Meslek Yüksek Okulu	İstanbul	Devlet
Siber Güvenlik Analistliği ve Operatörlüğü	Ankara Üniversitesi	Siber Güvenlik Meslek Yüksek Okulu	Ankara	Devlet
Siber Güvenlik Analistliği ve Operatörlüğü	Ege Üniversitesi	Siber Güvenlik Meslek Yüksek Okulu	İzmir	Devlet
Siber Güvenlik Analistliği ve Operatörlüğü	Gebze Teknik Üniversitesi	Siber Güvenlik Meslek Yüksek Okulu	Kocaeli	Devlet
Siber Güvenlik Analistliği ve Operatörlüğü	İstanbul Teknik Üniversitesi	Siber Güvenlik Meslek Yüksek Okulu	İstanbul	Devlet

2.2 Bıçakçılık ve El Aletleri Üretim Teknolojisi

Pamukkale Üniversitesi Serinhisar Meslek Yüksekokulunda 2023 yılında açılan ve ilk öğrencilerini kabul eden Bıçakçılık ve El Aletleri Üretim Teknolojisi Programı, alanında nitelikli teknikerler yetiştirmeyi amaçlamaktadır. Program, malzeme bilgisi, yenilikçi tasarım ve sürdürülebilir üretim süreçleri üzerine odaklanmaktadır. Öğrenciler, bilgisayar destekli tasarım, malzeme teknolojisi, temel kalıpçılık teknolojisi, bilgisayar destekli üretim ve imalat işlemleri gibi sektörel derslerin yanı sıra girişimcilik, internet ve pazarlama gibi temel derslerden oluşan kapsamlı bir eğitim almaktadır. Ayrıca, atölye çalışmalarıyla teorik bilgilerini pratiğe dökme fırsatı bulmaktadırlar. Bu programı tamamlayan öğrenciler, bıçakçılık ve el aletleri üretim teknolojisi teknikeri olarak hem kamu hem de özel sektörde görev alabilmektedirler. Kendi işyerini kurmayı hedefleyen mezunlar ise programda edindikleri teorik bilgi ve uygulamalı deneyimler sayesinde az bir bütçe ile bıçakçılık ve ev aletleri üretimi yapan bir firmada işveren olma olanağına sahiptirler. Bunun yanı sıra, bakım ve onarım hizmetlerinde görev alabilir, makine çizimlerine uygun olarak parçaların doğru yerleştirilmesini sağlayabilir veya makine mühendislerinin tasarladığı makinelerle ilgili teknik resim üzerinde çalışabilirler (6).

2.3 Kenevir Dokuma Tezgahtarlığı

Ondokuz Mayıs Üniversitesi Ladik Meslek Yüksekokulu bünyesinde 2023 yılında açılan Kenevir Dokuma Tezgahtarlığı adındaki ön lisans programı, yün fanila ve halı dokumacılığında öne çıkan Ladik ilçesinde kenevir dokumacılığının daha yaygın hale gelmesine, bu alanda yetkin eleman yetiştirilmesine ve geleneksel dokuma kültürünün canlı kalmasına katkı sağlamaktadır. Program, halı ve kilim dokumacılığı alanında bölgede istihdam ihtiyacını karşılayacak zanaatkarlar yetiştirmeyi amaçlamaktadır. Geleneksel kültürel dokuların, modern teknoloji ile harmanlanarak yeni nesillere aktarımı hedeflenmektedir. Program kapsamında öğrencilere dokuma temel bilgileri, dokuma teknikleri, motif ve tasarım dersleri gibi teorik bilginin yanı sıra atölye ve proje çalışmaları ile uygulama imkânı da sunulmaktadır. Programın açılmasında hızlandırıcı bir etken olarak, 2019 yılında yüksekokula yaklaşık 60 km uzaklıkta bulunan Vezirköprü ilçesinin Cumhurbaşkanı Recep Tayyip Erdoğan tarafından "Türkiye'nin Kenevir Ekim Merkezi" olarak ilan edilmesi gösterilmektedir. Ondokuz Mayıs Üniversitesi'nin (OMÜ) stratejik öncelik olarak belirlediği bu alan sayesinde, ilgili ürünün endüstriyel bir nitelik kazanması sağlanmıştır. Geçmişte yaklaşık 350 dönümlük bir alanda gerçekleştirilen kenevir ekimi, günümüzde alım garantisi ve sözleşmeli tarım avantajlarıyla 7 bin dönümlük bir alana ulaşmaktadır. Kenevirin yalnızca lifi değil, endüstriyel bir ürüne dönüştürülmesi, ekonomik değer yaratmanın temel koşulu olarak görülmektedir (7) (8) (9).

2.4 Sanal ve Artırılmış Gerçeklik

İstanbul Üniversitesi- Cerrahpaşa Teknik Bilimler Meslek Yüksekokulunda 2023 yılında açılan Sanal ve Artırılmış Gerçeklik programı; sanal gerçeklik (VR), artırılmış gerçeklik (AR), genişletilmiş gerçeklik (XR) ve karma gerçeklik (MR) gibi hem güncel hem de gelecekteki teknolojilere odaklanan bir eğitim sunmaktadır. Müfredat; bu alanlarda uygulama geliştirme becerilerini kazandırmayı amaçlayan Bilgi Teknolojileri Kullanımı, Tasarım, Modelleme,

Veri Tabanı Yönetim Sistemleri, Programlama gibi derslerden oluşmaktadır. Ayrıca, sanal ve artırılmış gerçeklik uygulamalarını tasarlamak ve geliştirmek için gerekli olan tasarım, uygulama ve laboratuvar dersleri de müfredatın bir parçasıdır. Bu ön lisans programından başarıyla mezun olan öğrenciler; VR, AR, XR uygulama geliştiricisi, mobil uygulama geliştiricisi, oyun programcısı, web uygulama geliştiricisi, yazılım geliştirici olarak kariyerlerini geliştirme olanağına sahiptirler. Ayrıca İstanbul Kalkınma Ajansı katkısıyla geliştirilen bir proje ile oluşturulan Yenilikçi XR Teknolojileri Araştırma ve Geliştirme Merkezi'nde (YETAM-XR) bulunan deneyim atölyeleri, programdaki öğrencilerin ilgili teknoloji içerikli ders uygulamalarında kullanılmaktadır (10) (11).

2.5 Siber Güvenlik Analistliği ve Operatörlüğü

2023-2024 öğretim yılında Ankara Üniversitesi, Ege Üniversitesi, Gebze Teknik Üniversitesi ve İstanbul Teknik Üniversitesinde açılan SGMYO Siber Güvenlik Analistliği ve Operatörlüğü ön lisans programı siber güvenlik alanında uzman ve nitelikli işgücü yetiştirmeyi amaçlamaktadır. SGMYO'larının kurulması için atılan ilk adım, 05.10.2022 tarihinde YÖK Başkanlığı ile T.C. Cumhurbaşkanlığı DDO Başkanlığı arasında gerçekleştirilen iş birliği protokolünün imzalanmasıyla gerçekleştirilmiştir. Bu okullarda, gerek kamu gerekse özel sektörün ihtiyaçlarına uygun siber güvenlik uzmanlık alanlarına yönelik eğitim programlarının oluşturulması ve "Ara Eleman değil Aranan Eleman" profiline sahip bireylerin yetiştirilmesi amaçlanmaktadır. Bu hedef doğrultusunda, programı başarıyla tamamlayan öğrenciler; siber güvenlik olay analisti, siber tehdit istihbarat analisti, siber güvenlik operasyon merkezi (SGOM) ve Siber Olaylara Müdahale Ekibi (SOME) 1. Seviye Destek Elemanı veya siber güvenlik sistemleri operatörü gibi uzmanlık alanlarında kariyer fırsatlarına sahip olabileceklerdir. Programın eğitim dili %30 İngilizce olup program 1 yıl İngilizce hazırlık ile birlikte toplam 6 dönem olarak uygulanmaktadır. Mezuniyetten hemen önceki son eğitim dönemini kapsayan staj eğitimi için yüksekokulların bulunduğu teknoparklarda yer alan şirketlerde veya Türkiye Siber Güvenlik Kümelenmesine üye firmalarda sahada mesleki eğitim fırsatlarının sağlanması öngörülmektedir. Programdan mezun olanlar 12.09.2012 tarihli Yükseköğretim Yürütme Kurulunun kararlarına dayanan güncel mevzuat gereği "tekniker" unvanını kullanacaklardır (12) (13).

2.5.1 Ankara Üniversitesi Siber Güvenlik Analistliği ve Operatörlüğü

Ankara Üniversitesi SGMYO, 2023 yılında kurulan dört okuldan biridir. Bu üniversitedeki Siber Güvenlik Analistliği ve Operatörlüğü ön lisans programı; müfredat, içerik ve amaç bakımından diğer 3 üniversitede bulunan eşdeğer programlar ile uyumlu bir şekilde yürütülmektedir. Okulda öğrencilerin kendilerini geliştirme ve pratik yapma imkânı bulacağı 27 adet bilgisayarlı bir laboratuvar bulunmaktadır. Bu bilgisayarlarda, sanal ağlar, sanal makineler ve çeşitli güvenlik yazılımları ile deneyim kazanan öğrencilere gerçek dünyadaki senaryoları modelleyerek bulut güvenliği, ağ güvenliği, zafiyet analizi, dijital inceleme ve kriptoloji gibi siber güvenlik alanlarında derinlemesine bilgi ve beceri edinme imkânı sunulmaktadır (14) (15).

Üniversite SGMYO bünyesinde belirli periyotlarla düzenlenen "Siber Güvenlik Sohbetleri" etkinliği, sektörde ileri gelen uzman kişilerle öğrencileri buluşturma ve bu profesyonellerin tecrübelerinden gençlerin istifade etmesi sağlanmaktadır. Bu etkinlikler ile siber güvenlik alanında uzman olan kişilerle etkileşime giren öğrencilerin sektördeki yenilikleri yakından takip etmeleri ve güncel teknolojilere dair bilgi edinmeleri hedeflenmektedir. Her bir sohbet etkinliğinin öğrencilere bir diğer kazanımı ise onların mesleki ağlarını zenginleştirmekte ve önemli bağlantılar kurma fırsatı sunmaktadır (16).

2.5.2 Ege Üniversitesi Siber Güvenlik Analistliği ve Operatörlüğü

T.C. Cumhurbaşkanlığı DDO Başkanlığı ile YÖK Başkanlığı arasında imzalanan işbirliği protokolünün neticesi olarak Ege Üniversitesi'nde açılan SGMYO Siber Güvenlik Analistliği ve Operatörlüğü ön lisans programı; ulusal siber güvenliğin sağlanmasına yönelik olarak teknik altyapıyı ve organizasyon yapısını güçlendirmek için gerekli teknolojiyi üreten, geliştiren ve yöneten nitelikli insan gücünün yetiştirmesi vizyonunun hayata geçirilmesinde önemli bir rol oynamaktadır. 2023 yılında bu amaç doğrultusunda belirlenen dört pilot

okuldan biri olan Ege Üniversitesi SGMYO, sektörle entegre ve sektörden beslenen bir programla öğrencilerin uygulama alanındaki pratiklerini gerçek dünyadaki deneyimlerle pekiştirmeyi amaçlamaktadır (17).

2.5.3 Gebze Teknik Üniversitesi Siber Güvenlik Analistliği ve Operatörlüğü

Gebze Teknik Üniversitesi SGMYO bünyesinde Bilgisayar Teknolojileri bölümü altında Siber Güvenlik Analistliği ve Operatörlüğü adında bir adet program bulunmaktadır. 2023 yılında ilk defa öğrenci alan bu program ile; siber güvenlik alanında nitelikli ve yetkin işgücü yetiştirilmesi, bu alanın gençler için çekici bir kariyer seçeneği haline getirilmesi, siber güvenlik uzmanlığının kavramsal gelişimine katkıda bulunarak bu mesleğe özgü yetkinliklerin kazandırılması amaçlanmaktadır. Programın akademik kanadından; kişisel mahremiyetin korunması, ulusal ve küresel savunma kapasitelerinin muhafaza edilmesi, hem ekonomik hem de sosyal iletişimin sağlıklı bir şekilde sürdürülmesi ve kurumsal güvenliğin tesis edilmesi gibi dijital alanda gerçekleşen süreçler açısından siber güvenliğin taşıdığı kritik önemin altı çizilmektedir. Bu doğrultuda çalışmalarını sürdüren programın ilk yerleşen öğrencileri, danışman akademisyenlerin rehberliğinde, Türkiye Bilimsel ve Teknik Araştırma Kurumu (TÜBİTAK) Bilim İnsanı Destek Programları Başkanlığı (BİDEB) tarafından yürütülen 2209-A Üniversite Öğrencileri Araştırma Projeleri Destekleme Programı kapsamında iki ayrı proje kabulü alarak, kayda değer çalışmalara imza atma potansiyellerini göstermektedirler (18) (19). Müfredat; Temel Programlama, Bilişim ve Ağ Teknolojisi, Veri Tabanı Uygulamaları ve Güvenliği, İşletim Sistemleri ve Güvenliği gibi bilgisayar bilimleri alan derslerine ek olarak siber güvenlik alanında Sızma Testi, Siber Olay Yönetimi, Siber Güvenlik Yönetişimi gibi daha birçok mesleki ders ve Kriptoloji, Bilişim Hukuku, Adli Bilişim gibi seçmeli alan derslerini de içermektedir (20).

2.5.4 İstanbul Teknik Üniversitesi Siber Güvenlik Analistliği ve Operatörlüğü

İçerik, amaç, yola çıkma şekli ve kurulma tarihi bakımında birbiriyle eşdeğer toplam dört okuldan biri olan İstanbul Teknik Üniversitesi SGMYO Bilgisayar Teknolojileri Bölümüne bağlı Siber Güvenlik Analistliği ve Operatörlüğü ön lisans programı, siber saldırılara ve kötü amaçlı yazılımlara karşı 'Siber Vatan'ın muhafızları' olarak bilinen beyaz şapkalı hackerlar, yani iyi niyetli siber güvenlik uzmanı yetiştirmeyi amaçlamaktadır. Programda, siber güvenlik alanının temel konularının yanı sıra ağ güvenliği, güvenlik teknolojileri, veri analizi ve sızma testi gibi konularda eğitim verilmektedir. Programın akademik kanadı tarafında; dijitalleşen dünyada artık birçok cihaz ve makinenin internet bağlantısına sahip olduğu göz önüne alındığında, bu cihazların hem bireysel hem de devlet ölçeğinde korunmasının önemi vurgulanmaktadır. Ayrıca, bu koruma süreçlerinin yerli uzman iş gücü ve yazılımlarla gerçekleştirilmesinin gerekliliği ifade edilmekte ve bu hedef doğrultusunda programın gerekli insan gücünün sağlanmasına yönelik katkısı öne çıkarılmaktadır. Diğer yandan, bu alanda çalışacak adayların yetiştirildiği programda, her türlü zafiyetlerin ve açığın tespitine yönelik bilgi ve becerilerin kazanımı sağlanırken, etik çizgiden ayrılmamanın önemi de vurgulanmaktadır (21) (22).

3 Yöntem

Bu çalışmada 2023 yılında açılan ve aynı yıl ilk kez öğrenci kabulüne başlayan sekiz yeni programın betimsel (tanıtsal) analizi gerçekleştirilmiş, YÖK Atlas web sitesinden elde edilen bu programlara yerleşen öğrencilere ait veriler özetlenmiş ve bu programlara yönelik mevcut durumun belirlenmesine yönelik bir değerlendirme yapılmıştır. Verilerin özetlenmesi, tanımlayıcı analizler kapsamında görselleştirme, grafik ve tablolama yöntemleriyle gerçekleştirilmiştir (23) (24). Bu sayede, verilerin değerlendirilmesi ve denetimi kolaylaşmış, analiz ve yorumlama süreçlerinde de verimlilik sağlanmıştır (25). Çalışmada kullanılan veriler, resmi kayıtlar, raporlar ve istatistiksel verilere dayanan YÖK Atlas web sitesinden elde edilen ikincil veri kaynağı niteliğindedir (26). Yeni açılan programların tamamı ön lisans programı olduğu için, YÖK Atlas web sitesindeki YÖK ön lisans atlası kısmından verilere erişim sağlanmıştır (27).

4 Bulgular ve Tartışma

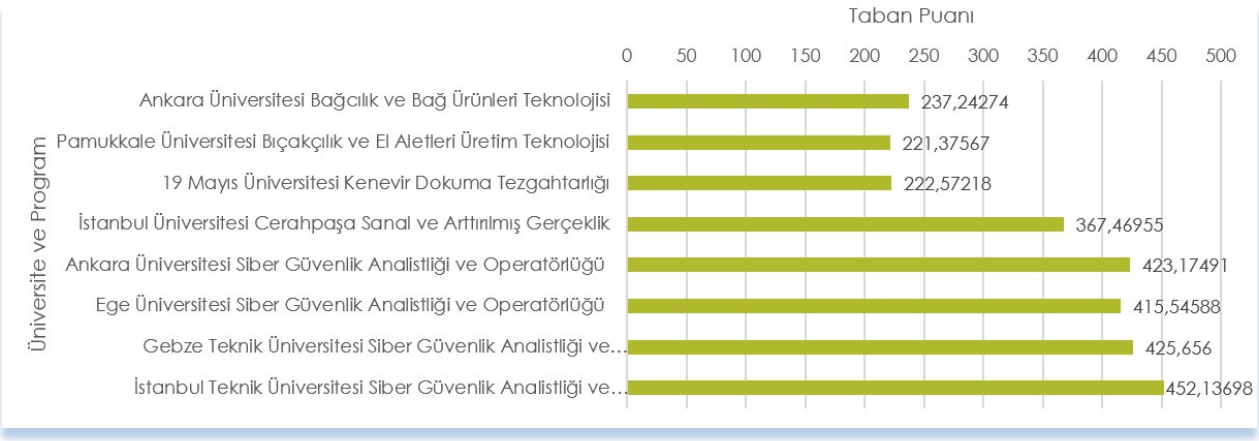
2023 yılında ilk kez öğrenci alan programlara ilişkin veriler bu araştırmanın amacı doğrultusunda değerlendirilerek elde edilen bulgular aktarılarak yorumlanmıştır.

Tablo 2'de; sekiz yeni programın tümünde toplam kontenjan sayısına göre %100 yerleşme oranlarına ulaşıldığı gözlemlenmiştir. Bununla birlikte dikkat çeken bir diğer husus, okul birinciliği kontenjanlarının tabloda yer alan ilk üç programda dolmamış olmasıdır.

Tablo 2. 2023 yılında ilk defa öğrenci alan programların kontenjan ve yerleşme bilgileri.

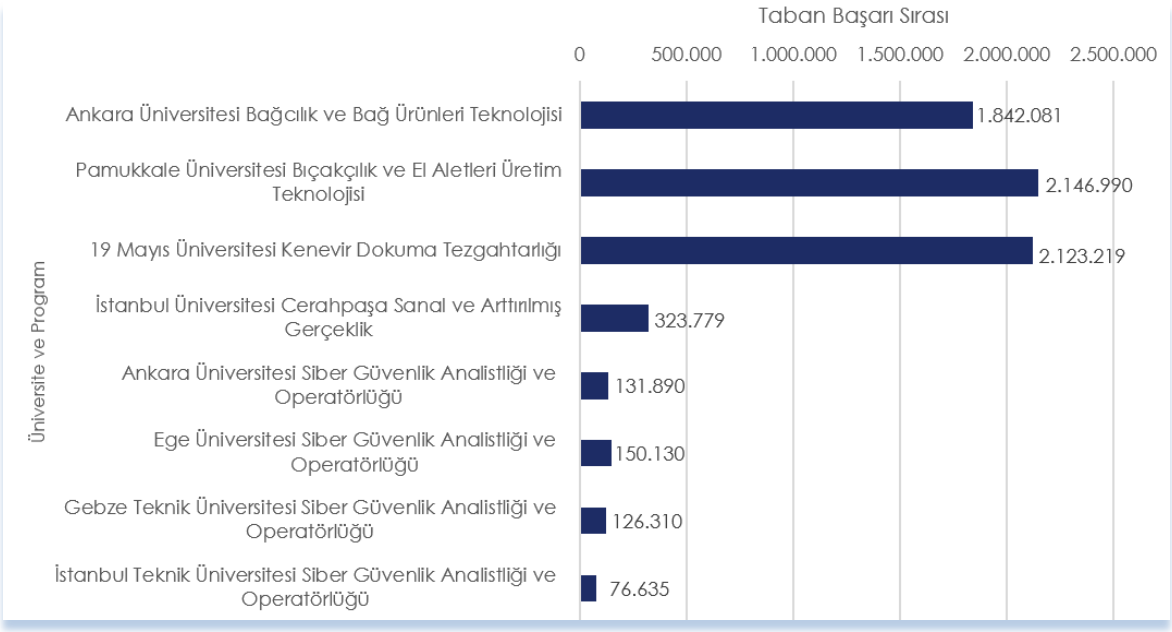
		Kontenjan			Yerleşme		
Program	Üniversite	Genel	Okul Birincisi	Toplam	Genel	Okul Birincisi	Toplam
Bağcılık ve Bağ Ürünleri Teknolojisi	Ankara Üniversitesi	30	1	32	31	0	32
Bıçakçılık ve El Aletleri Üretim Teknolojisi	Pamukkale Üniversitesi	30	1	32	30	0	32
Kenevir Dokuma Tezgahtarlığı	19 Mayıs Üniversitesi	25	1	27	26	0	27
Sanal ve Arttırılmış Gerçeklik	İstanbul Üniversitesi Cerahpaşa	25	1	27	25	1	27
Siber Güvenlik Analistliği ve Operatörlüğü	Ankara Üniversitesi	25	1	27	25	1	27
Siber Güvenlik Analistliği ve Operatörlüğü	Ege Üniversitesi	25	1	27	25	1	27
Siber Güvenlik Analistliği ve Operatörlüğü	Gebze Teknik Üniversitesi	25	1	27	25	1	27
Siber Güvenlik Analistliği ve Operatörlüğü	İstanbul Teknik Üniversitesi	25	1	27	25	1	27

Şekil 1'de yeni programlara yerleşen son öğrencilerin 0,12 katsayı ile hesaplanmış temel yeterlilik testi (TYT) puanları grafik ile gösterilmiştir. İlk dört sırayı Siber Güvenlik Analistliği ve Operatörlüğü programı oluştururken hemen ardından Sanal ve Artırılmış Gerçeklik programı gelmektedir.



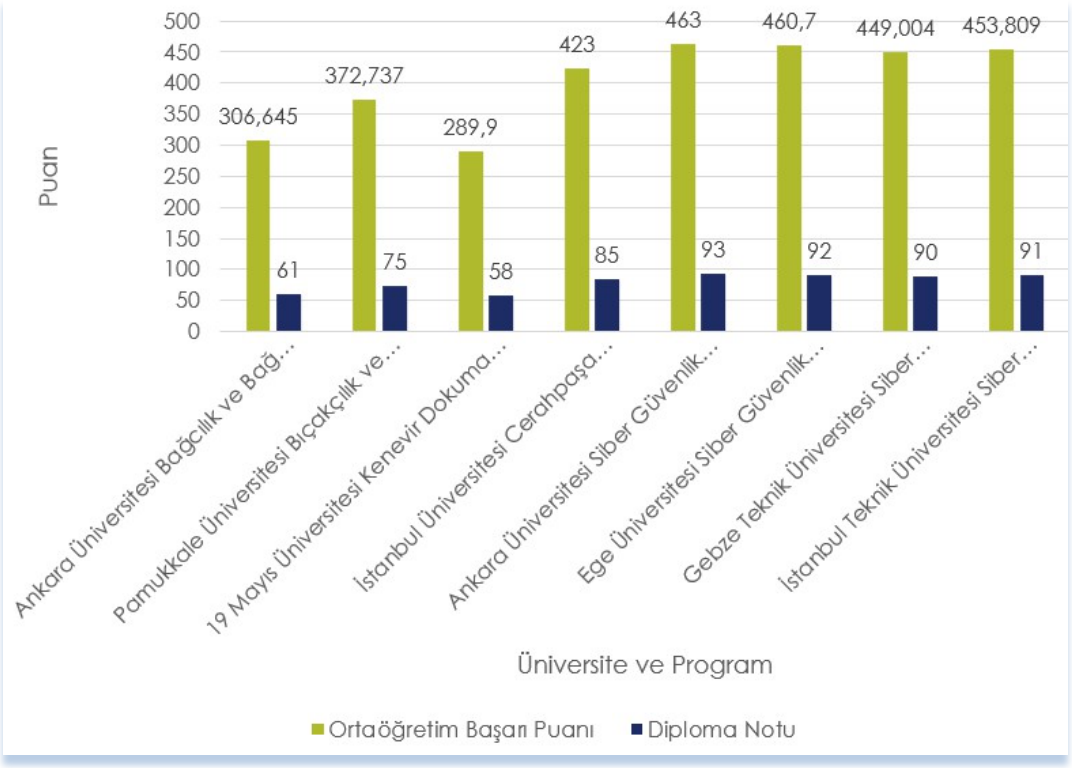
Şekil 1. 2023 yılında ilk defa öğrenci alan programlara yerleşen öğrencilerin taban puanları

Şekil 2'de, yeni programlara yerleşen son öğrencilerin 0,12 katsayısı ile hesaplanmış taban başarı sıralamaları grafiksel olarak sunulmuştur. En düşük başarı sıralamasına sahip programlar arasında 76.635-150.130 bandında yer alan Siber Güvenlik Analistliği ve Operatörlüğü programları öne çıkarken, Sanal ve Artırılmış Gerçeklik programı 323.779 başarı sırasıyla, Siber Güvenlik Analistliği ve Operatörlüğü programının oldukça gerisinde kalmıştır. Kenevir, bıçakçılık ve bağcılıkla ilgili yeni programlar ise çok daha geride yer almıştır.



Şekil 2. 2023 yılında ilk defa öğrenci alan programlara yerleşen öğrencilerin taban başarı sırası

Şekil 3'te, 2023 yılında ilk defa öğrenci alan programlara yerleşen son öğrencilerin lise başarı durumları grafiksel olarak sunulmaktadır. Lise başarı durumu göstergesi olarak, ortaöğretim başarı puanı (OBP) ve diploma notu değişkenleri değerlendirilmiştir. 90-93 aralığındaki diploma notuna sahip öğrenciler Siber Güvenlik Analistliği ve Operatörlüğü programına yerleşirken, Sanal ve Artırılmış Gerçeklik programı öğrencileri 85 diploma notu sınırında yer almaktadır. Diğer üç programın diploma notu ortalamaları ise 58-75 aralığında kalmaktadır. OBP kriterine bakıldığında ise bu sıralama ve dağılımın değişmediği görülmektedir.



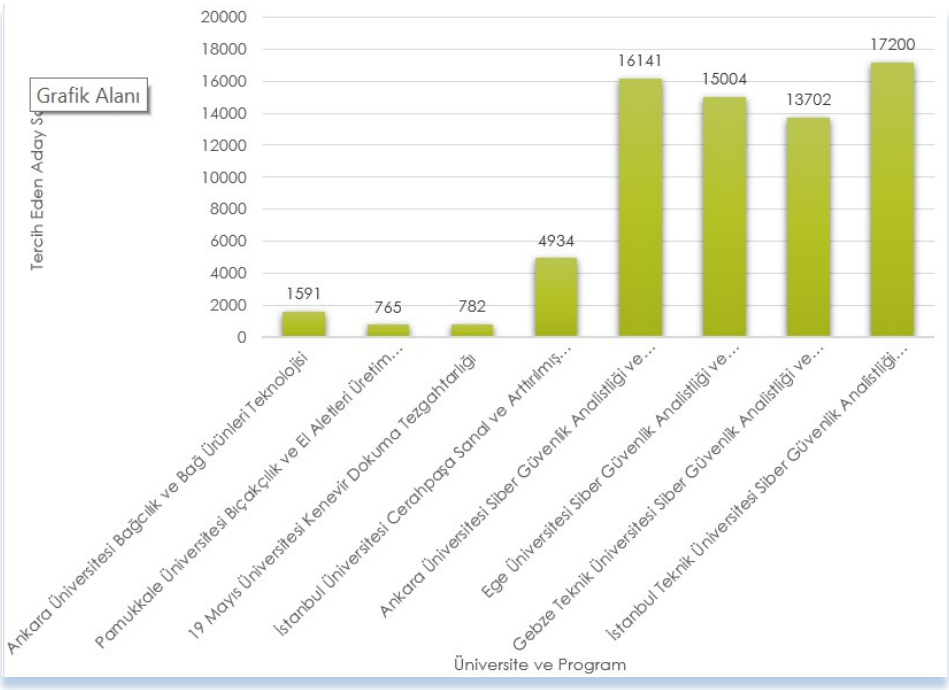
Şekil 3. 2023 yılında ilk defa öğrenci alan programlara yerleşen öğrencilerin lise başarı durumu

Tablo 3. 2023 yılında ilk defa öğrenci alan programlara yerleşen öğrencilerin öğrenim durumları.

Program	Üniversite	Liseden yeni mezun, YKS ye ilk defa girdi	Liseden mezun, daha önce hiç üniversiteye yerleşmemişti	Üniversitede öğrenci iken sınava girip buraya yerleşti	Bir üniversiteden daha önce mezun olmuş	Diğer	Toplam
Bağcılık ve Bağ Ürünleri Teknolojisi	Ankara Üniversitesi	0	17	2	13	0,00	32
Bıçakçılık ve El Aletleri Üretim Teknolojisi	Pamukkale Üniversitesi	2	22	2	3	3,00	32
Kenevir Dokuma Tezgahtarlığı	19 Mayıs Üniversitesi	4	12	2	6	3,00	27
Sanal ve Arttırılmış Gerçeklik	İstanbul Üniversitesi Cerahpaşa	4	6	6	10	1,00	27
Siber Güvenlik Analistliği ve Operatörlüğü	Ankara Üniversitesi	9	12	3	2	1,00	27
Siber Güvenlik Analistliği ve Operatörlüğü	Ege Üniversitesi	8	10	4	4	1,00	27
Siber Güvenlik Analistliği ve Operatörlüğü	Gebze Teknik Üniversitesi	5	14	6	2	0,00	27
Siber Güvenlik Analistliği ve Operatörlüğü	İstanbul Teknik Üniversitesi	2	5	19	1	0,00	27
Toplam		34	98	44	41	9	226

Tablo 3'te, çalışmaya konu olan sekiz programa yerleşen toplam 226 öğrencinin öğrenim durumlarına ilişkin istatistikler sunulmaktadır. Bu bilgiler arasında dikkat çeken bir ayrıntı, 44 öğrencinin hâlihazırda üniversite öğrencisi iken bu programa yerleşmiş olmaları ve bu öğrencilerden 32'sinin Siber Güvenlik Analistliği ve Operatörlüğü programına girmiş olmasıdır. Ayrıca, 41 öğrencinin daha önce bir üniversiteden mezun olduğu ve 2023 yılında 10'unun Sanal ve Artırılmış Gerçeklik programına, 22'sinin ise kenevir, bıçakçılık ve bağcılıkla ilgili yeni programlara yerleştiği görülmektedir.

Şekil 4'te, 2023 yılında ilk kez öğrenci alan sekiz programa tercih yapan aday sayıları görülmektedir. Diğer programlara kıyasla, dört üniversitedeki Siber Güvenlik Analistliği ve Operatörlüğü programlarının tümü açık ara farkla en çok tercih edilen programlar olmuştur.



Şekil 4. 2023 yılında ilk defa öğrenci alan programların tercih edilme durumu

Tablo 4. 2023 yılında ilk defa öğrenci alan programların tercih sıralama istatistikleri.

Program	Üniversite	Üniversite ve Bölüm	Ortalama Tercih Edilme sırası	Yerleşenler Ortalama Kaçıncı Tercihlerinde Yerleşti
Bağcılık ve Bağ Ürünleri Teknolojisi	Ankara Üniversitesi	Ankara Üniversitesi Bağcılık ve Bağ Ürünleri Teknolojisi	11,2	5,4
Bıçakçılık ve El Aletleri Üretim Teknolojisi	Pamukkale Üniversitesi	Pamukkale Üniversitesi Bıçakçılık ve El Aletleri Üretim Teknolojisi	12,7	7,7
Kenevir Dokuma Tezgahtarlığı	19 Mayıs Üniversitesi	19 Mayıs Üniversitesi Kenevir Dokuma Tezgahtarlığı	13,3	7,1
Sanal ve Arttırılmış Gerçeklik	İstanbul Üniversitesi Cerahpaşa	İstanbul Üniversitesi Cerahpaşa Sanal ve Arttırılmış Gerçeklik	6,9	4,5
Siber Güvenlik Analistliği ve Operatörlüğü	Ankara Üniversitesi	Ankara Üniversitesi Siber Güvenlik Analistliği ve Operatörlüğü	5,1	3,1
Siber Güvenlik Analistliği ve Operatörlüğü	Ege Üniversitesi	Ege Üniversitesi Siber Güvenlik Analistliği ve Operatörlüğü	5,2	4,1
Siber Güvenlik Analistliği ve Operatörlüğü	Gebze Teknik Üniversitesi	Gebze Teknik Üniversitesi Siber Güvenlik Analistliği ve Operatörlüğü	5,3	3,9
Siber Güvenlik Analistliği ve Operatörlüğü	İstanbul Teknik Üniversitesi	İstanbul Teknik Üniversitesi Siber Güvenlik Analistliği ve Operatörlüğü	4,4	1,6

Çalışmaya konu olan sekiz programın tüm adaylar tarafından ortalama kaçıncı sırada tercih edildikleri Tablo 4'te sunulmaktadır. Siber Güvenlik Analistliği ve Operatörlüğü programlarının tercih edilme sırası ortalama 4,4 ile 5,3 aralığında iken, Sanal ve Artırılmış Gerçeklik programının ortalama tercih edilme sırası 6,9 olarak görülmektedir. Kenevir, bıçakçılık ve bağcılıkla ilgili yeni programların ortalama tercih edilme sırası ise 11'in üzerindedir. Aynı tabloda, bu sekiz yeni programa yerleşen öğrencilerin ortalama kaçıncı tercihlerine yerleştikleri ile ilgili bilgiler de yer almaktadır. Bu bilgiler ışığında, Siber Güvenlik Analistliği ve Operatörlüğü programına yerleşenler ortalama 1,6 ile 4,1 aralığındaki tercihlerine yerleşirken, hemen ardından 4,5 ortalama tercih sırasıyla Sanal ve Artırılmış Gerçeklik programı gelmektedir. Diğer üç programın yerleşen öğrencileri de 5,4 ile7,7 aralığında tercih sıralamasına sahiptir.

Tablo 5'te, 2023-2024 öğretim yılı yükseköğretim istatistiklerine göre kayıtlı öğrenci bilgileri ve bu öğrencilerin cinsiyet bilgilerine yer verilmiştir. Bilgilerin yorumlanmasını kolaylaştırmak adına, tabloda toplam yerleşme bilgileri ile kayıtlı öğrenci bilgileri bir arada sunulmuştur. Yerleştiği halde kesin kayıt yaptırmayan öğrenciler ve ek yerleştirme ile kayıt yaptıran öğrenciler dikkate alınmış ancak bu detaylara tabloda yer verilmemiştir. Bunun yerine, bu çalışma için anlamlı bir bilgi olarak, nihai kayıtlı öğrenci sayısı ile bu sayının toplam yerleşen öğrenci sayısına yüzdelik oranı hesaplanmış ve tabloda sunulmuştur. Bu bilgiler ışığında Siber Güvenlik Analistliği ve Operatörlüğü programına yerleşen öğrenci sayısının ve kayıtlı öğrenci sayısına eşit olduğu ve dolayısıyla %100 kayıtlı öğrenci oranının oluştuğu görülmektedir Diğer bölümlerde bu oran %87,5 ile %90,63 arasında değişiklik göstermektedir.

Tablo 5. 2023 yılında ilk defa öğrenci alan programlara kayıtlı öğrenci bilgileri.

			2023-2024 Öğretim Yılı Yükseköğretim İstatistikleri			
Program	Üniversite	Toplam Yerleşme	Toplam Kayıtlı Öğrenci	Kayıtlı Kız Öğrenci	Kayıtlı Erkek Öğrenci	Kayıtlı Öğrenci Oranı*
Bağcılık ve Bağ Ürünleri Teknolojisi	Ankara Üniversitesi	32	28	9	19	87,50
Bıçakçılık ve El Aletleri Üretim Teknolojisi	Pamukkale Üniversitesi	32	29	8	21	90,63
Kenevir Dokuma Tezgahtarlığı	19 Mayıs Üniversitesi	27	26	13	13	96,30
Sanal ve Arttırılmış Gerçeklik	İstanbul Üniversitesi Cerahpaşa	27	26	12	14	96,30
Siber Güvenlik Analistliği ve Operatörlüğü	Ankara Üniversitesi	27	27	5	22	100,00
Siber Güvenlik Analistliği ve Operatörlüğü	Ege Üniversitesi	27	27	9	18	100,00
Siber Güvenlik Analistliği ve Operatörlüğü	Gebze Teknik Üniversitesi	27	27	7	20	100,00
Siber Güvenlik Analistliği ve Operatörlüğü	İstanbul Teknik Üniversitesi	27	27	3	24	100,00
Toplam		226	217	66	151	96,02

5 Sonuç ve Öneriler

Bu çalışmada, 2023 yılında açılan ve ilk kez öğrenci alımı gerçekleştiren sekiz yeni üniversite programının yerleşme verileri incelenmiş ve betimsel analiz yöntemiyle elde edilen bulgular değerlendirilmiştir. Bu sekiz yeni pozisyonun dört tanesi aynı programın farklı üniversitelerdeki eşdeğerleri olduğundan, analiz toplamda beş yeni programını kapsamaktadır.

Çalışmada ele alınan programların tamamı ön lisans düzeyinde olup, Siber Güvenlik Analistliği ve Operatörlüğü programını dışındakilerin eğitim dili Türkçe ve eğitim süreleri iki yıl olarak belirlenmiştir. Siber Güvenlik Analistliği ve Operatörlüğü programı ise, %30 İngilizce eğitim verilmesi ve toplam eğitim süresinin İngilizce hazırlık ile birlikte üç yıl olması bakımından diğerler programlardan ayrılmaktadır. Bu farklılık, programın kurulum aşamasındaki beklentiler, üstlendiği misyon ve siber güvenlik alanındaki talep açığı gibi çeşitli faktörlerle de kendini göstermektedir. Zira, programın kritik öneme sahip bir meslek için eleman yetiştirmesi ve ülkemizin stratejik eylem planının bir parçası olması, bu programı diğerlerinden büyük ölçüde farklı ve önemli kılmaktadır. Yerleşme verileri değerlendirildiğinde, bu farkın öğrenci tercihleri açısından da desteklendiği ve tercih sonuçlarına yansıdığı ifade edilebilir. Bu düşünceyi destekleyen bulgular arasında, okul birincilerinin bu programı tercih etmeleri, yerleşen öğrencilerin yüksek başarı puanlarına ve düşük başarı sıralamalarına sahip olmaları örnek gösterilebilir. Özellikle, Siber Güvenlik Analistliği ve Operatörlüğü programını tercih eden öğrenci sayısındaki belirgin fazlalık, bu programın öğrenciler arasında ne kadar revaçta olduğunun bir göstergesidir. Tercih edilme istatistiklerine bakıldığında, öğrencilerin bu programı ortalama ilk 5,3'üncü tercih sırasından sonraya bırakmadıkları, yerleşenlerin ise en iyi ortalama ile 1,6'ncı tercihlerine yerleştiği, en düşük sıralama ortalamasıyla ise 4,1'inci tercihten programa yerleştiği görülmüştür. Bu veriler, programın yüksek talep gördüğünü ve öğrenciler tarafından öncelikli tercih edildiğini ortaya koymaktadır. Bu programa yerleşen öğrenci sayısının korunması ve kayıtlı öğrenci sayısında herhangi bir düşüş yaşanmaması da bu talebi desteklemektedir.

2024 yılında da benzer şekilde yeni açılan ve öğrenci alacak olan programlar ilan edilmiş olup bunlarla ilgili olarak akademik çalışmalar yapılabilir.

Kaynaklar

[1] Wagner P, Alharthi D. "Leveraging VR/AR/MR/XR Technologies to Improve Cybersecurity Education, Training, and Operations*". Journal of Cybersecurity Education, Research and Practice*, (1), 7, 2024.

[2] Sussman L L, Leavitt Z S. "Creating a Repeatable Nontechnical Skills Curriculum for the University of Southern Maine (USM) Cybersecurity Ambassador Program (CAP)". *ACIG*, 2(1), 1-25, 2023

[3] T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. "2023 Yılı Cumhurbaşkanlığı Yıllık Programı". https://cbddo.gov.tr/siber-guvenlik-stratejisi/ (20.08.2024).

[4] T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı. "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023)". https://www.sbb.gov.tr/wp-content/uploads/2022/11/2023-Yili-Cumhurbaskanligi-Yillik-Programi.pdf (20.08.2024).

[5] Ankara Üniversitesi. "Bağcılık ve Bağ Ürünleri Teknolojisi Kalecik Meslek Yüksekokulu". https://www.ankara.edu.tr/programlar/1/467/4505-2147 (18.08.2024).

[6] Pamukkale Üniversitesi. "Serinhisar Meslek Yüksekokulu Bıçakçılık ve el Aletleri Üretim Teknolojisi Programı". https://www.pau.edu.tr/serinhisarmyo/tr/sayfa/bicakcilik-ve-el-aletleri-uretim-teknolojisi-programi (18.08.2024).

[7] Ondokuz Mayıs Üniversitesi. "Ladik Meslek Yüksekokulu Kenevir Dokumacılığı Programı". https://ladikmyo.omu.edu.tr/tr/akademik/akademik-birimler/tekstil-giyim-ayakkabi-ve-deri-bolumu/kenevir-dokumaciligi-programi (19.08.2024).

[8] Ondokuz Mayıs Üniversitesi. "Kenevir Dokumacılığında Geleneksel İle Modern Üniversitelilerin Elinde Birleşecek". https://www.omu.edu.tr/tr/icerik/haber/kenevir-dokumaciliginda-geleneksel-ile-modern-universitelilerin-elinde-birlesecek (19.08.2024).

[9] Ondokuz Mayıs Üniversitesi. "Ladik Meslek Yüksekokulu Kenevir Dokumacılığı Programı Ders Programları". https://ladikmyo.omu.edu.tr/tr/ogrenci/ders-programlari/KENEV%C4%B0R.pdf (19.08.2024).

[10] İstanbul Üniversitesi. "Türkiye'nin ilk ve tek Sanal ve Artırılmış Gerçeklik Önlisans Programı

yeni öğrencilerini bekliyor". https://sanalgerceklikteknikbilimlermyo.iuc.edu.tr/tr/duyuru/turkiyenin-ilk-ve-tek-sanal-ve-artirilmis-gerceklik-onlisans-programi-yeni-ogren-57006A006500590031006800300043003900 6B005F00390079007000460062006100410 04F003200370077003200 (19.08.2024).

[11] İstanbul Üniversitesi. "Sanal ve Artırılmış Gerçeklik Programı Teknik Bilimler Meslek Yüksekokulu". https://sanalgerceklikteknikbilimlermyo.iuc.edu.tr/tr/content/hakkimizda/program-hakkinda#6A00620042005100560006B007500 36004E004D0073003100 (19.08.2024).

[12] T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. "Siber Güvenlik Meslek Yüksekokulları". https://cbddo.gov.tr/sss/siber-myo/(19.08.2024).

[13] T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. " Siber Güvenlik Meslek Yüksekokulları tanıtım broşürü". https://cbddo.gov.tr/SharedFolderServer/Genel/File/SGMYO_Tanitim_Brosuru.pdf (19.08.2024).

[14] Ankara Üniversitesi "Siber Güvenlik Meslek Yüksekokulu". https://sgmyo.ankara.edu.tr/laboratuvar/ (20.08.2024).

[15] Ankara Üniversitesi. "Siber Güvenlik Meslek Yüksekokulu". https://www.ankara.edu.tr/dizin/myo/siber-guevenlik-meslek-yueksekokulu (20.08.2024).

[16] Ankara Üniversitesi Siber Güvenlik Meslek Yüksekokulu. "Siber Güvenlik Sohbetleri". https://sgmyo.ankara.edu.tr/siber-guvenlik-sohbetleri/ (20.08.2024).

[17] Ege Üniversitesi Kariyer Planlama ve Başarı Koordinatörlüğü. "Siber Güvenlik MYO, Ege Üniversitesi'nde Gün Sayıyor". https://kariyer.ege.edu.tr/a-681238/siber_guvenlik_myo__ege_universitesinde_gun_sayiyor.html (20.08.2024).

[18] Gebze Teknik Üniversitesi. "Siber Güvenlik Meslek Yüksek Okulu". https://www.gtu.edu.tr/kategori/5233/0/display.aspx (20.08.2024).

[19] Gebze Teknik Üniversitesi. "GTÜ Öğrenci Projelerine TÜBİTAK Desteği". https://www.gtu.edu.tr/icerik/8/21620/display.aspx (20.08.2024).

[20] Gebze Teknik Üniversitesi. "Siber Güvenlik Analistliği ve Operatörlüğü Önlisans Ders Kataloğu". https://abl.gtu.edu.tr/ects/?duzey=ucuncu&modul=onlisans_derskatalogu&bolum=820123&tip=onlisans (20.08.2024).

[21] İstanbul Teknik Üniversitesi. "İTÜ'de "beyaz şapkalı" hackerlar yetişiyor". https://sgmyo.itu.edu.tr/haber-detay/2024/05/30/i-t%C3%BC'de-beyaz-%C5%9Fapkal%C4%B1-hackerlar-yeti%C5%9Fiyor (20.08.2024).

[22] İstanbul Teknik Üniversitesi. "Siber Güvenlik Meslek Yüksekokulu". https://sgmyo.itu.edu.tr/hakkimizda (20.08.2024).

[23] Alptekin E, Özdemir Y A, Şahin Tekin S T. *Çözümlü Örneklerle Örnekleme Yöntemlerine Giriş.* İkinci Baskı. Ankara, Türkiye, Seçkin, 2019.

[24] Özdamar K. *Modern Bilimsel Araştırma Yöntemleri*. Birinci baskı. Eskişehir, Türkiye, Kaan, 2003

[25] İslamoğlu A H. *Bilimsel Araştırma Yöntemleri*. İkinci baskı. İstanbul, Türkiye, Beta, 2003

[26] Karasar N. *Bilimsel Araştırma Yöntemi*. On beşinci baskı. Ankara, Türkiye, Nobel, 2005

[27] Yükseköğretim Program Atlası . "YÖK Ön Lisans Atlası". https://yokatlas.yok.gov.tr/onlisans-anasayfa.php (20.06.2024).

Executing and Analysis of Keylogger and Local Account Discoverer Monitoring System

Arda Bozdoğan, Burak Can Ödemiş, Emre ATLIER OLCA

Maltepe University, Faculty of Eng. and Natural Sci., Computer Engineering, İstanbul,Türkiye

Maltepe University, Faculty of Eng. and Natural Sci., Computer Engineering, İstanbul, Türkiye

Maltepe University,Faculty of Eng. and Natural Sci., İstanbul, Türkiye

Abstract

Our project aims to execute 2 attacks on a remote computer by using PowerShell scripts. The first script is designed to capture keystrokes, providing us the users input. The second script focuses on enumerating local accounts, giving us a overview of all user accounts on the system. We have a dashboard that helps us to monitoring the results, attack that have been done, their times and captured data's. Our dashboard is connected to the database where we store all the information. The primary aim of this project we are trying to identify and understand security vulnerabilities through a controlled testing environment.

Keywords: *Cyber Security, Keylogger, Enumerate Account*

1. Introduction

Our project works with three platforms working with combinations. These are client application, database and dashboard. With the client application we will select and execute which attack will be executed. After the attacks the results will be transferred to the database. Dashboard pulls the data's from database and admins can be able to see the result of these attacks. Our main objective in this project is to understand and test these vulnerabilities through executing and analyzing key capture and enumerating local account attacks. We have selected Input Capture: Keylogging which is used for capturing users keystrokes and Account We have selected Input Capture: Keylogging which is used for capturing users keystrokes and Account Discovery: Enumerate Account to gather information about existing accounts on the system.

2. Related Works

A lot of projects with diverse ways have contributed to cyber security field and Keyloggers but there are not any works have been done about Local Account Discovery. In this part, projects about the same purposes with us will be discussed. Same purpose with different implementation and injection style has been used [1] in this study that published in 2020 3rd International Conference on Computer and Informatics Engineering (IC2IE), In this project, Keylogger was injected to and Windows device as same as we have done but for injection with running a PowerShell Script using a USB to activate and this script was embedded in a Arduino device and results were taken via email. In our project we are injecting without Arduino device, and we take result via our own created database. In this project [2] that published in the 2023 2nd International Conference on Automation, Computing and Renewable Systems(ICACRS), Compared to us; Python has been used for creating an efficient software based keylogger that collects data advanced features like keystrokes, clipboard information like image or text, screenshots and system information's but they have the same purposes with us but they have done with different way. For results they were taken via email we are taking the data via our own created Database. The study [3] published at the 2021 5th International Conference on Information Systems and Computer Networks (ISCON) is so similar to our project with even the coding language(C#) and operates on Windows. But for data storage they have used a server that refreshes every hour and for extra they have recorded victim's IP address, MAC Address and it re-launches every time that system starts. That study[4] published at the 2021 5th International Conference on Information Systems and Computer Networks (ISCON) has been done with different purposes (parental control and employee monitoring, result testing and experimenting) but the same logic as our project. With that project also they have been checking the ethical responsibilities with legal frameworks,

highlighting the potential advantages of children and organizations' safety.

3. The System

The project has three parts: Client Application, Database and Dashboard. Client Application: We are going to infect the selected computer through a USB that will carry this application. The application has a simple design. It will be used for selecting which attacks will execute and transfer the data to the our own created database. Database: Database is where we store the attacks' results. Both the app and the dashboard will have access to the database. The application will transfer the results of the attacks to Database. The Dashboard will pull these results from here and let the admins to analyze them. Dashboard: The Dashboard will be the main way to see the results. The Database is connected to Dashboard for monitoring every information of the attacks for the admins. Admin users will access the dashboard to review and analyze the outputs of the attacks.

4. System Architecture

The project has three parts: Client Application, Database and Dashboard. Client Application: We are going to infect the selected computer through a USB that will carry this application. The application has a simple design. It will be used for selecting which attacks will execute and transfer the data to the our own created database. Database: Database is where we store the attacks' results. Both the app and the dashboard will have access to the database. The application will transfer the results of the attacks to Database. The Dashboard will pull these results from here and let the admins to analyze them. Dashboard: The Dashboard will be the main way to see the results. The Database is connected to Dashboard for monitoring every information of the attacks for the admins. Admin users will access the dashboard to review and analyze the outputs of the attacks.

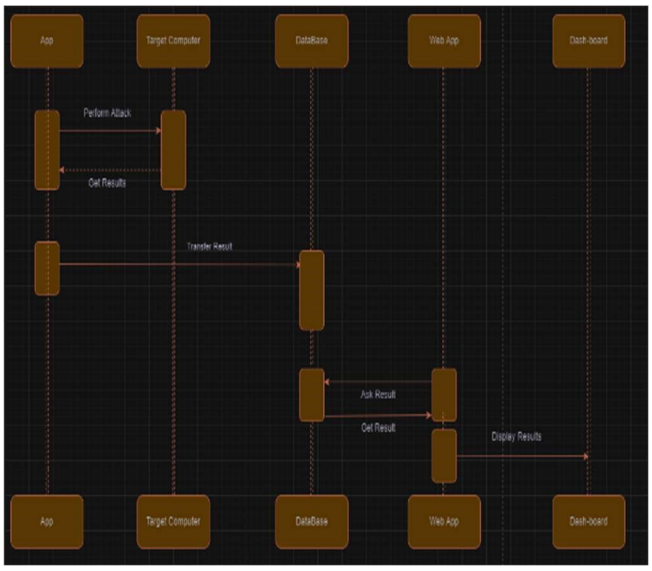


Fig. 1. The Squence Diagram

In figure 2; we represent the High-Level Diagram of our project. This diagram shows the operations that the system does step by step, serves the illustrations of main components, relations and interactions of main components and the data flow among these components. The diagram helps us to understand how the app executes these attacks. Which is then results transferred to the database for storege. Then the collected data transferred to the website. At the website if the user is an admin, they can review the results 2 at the dashboard.

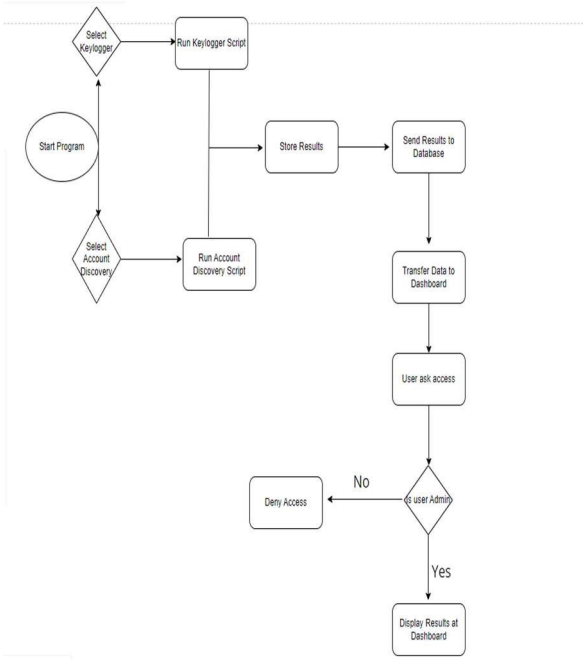


Fig. 2. High-Level Diagram

4.1. Client Application

The client app is the one of the main components of our system that executes the PowerShell Scripts so executes our MITRE Attacks to Victim and also connected with our Database so this app does the data transfer job about the data that we displayed on our Dashboard. This App was coded in C#, has a basic working principle executes scripts of Keylogger and Local Account Discoverer. While executing the Scripts of Keylogger it also uses the similar script methods with RokRat[5][6] and Sandworm Team[7], with coded language; Client App has similar features with BabyShark[8] and our App is PowerShell based so has similar mechanics with Kimsuky[9][10][11][12] while logging keystrokes. For Local Account Discoverer option of our Client App we execute the part of Local Account Discoverer Part of Scripts on Victim's computer.

4.2. DataBase

In Database part of our system we have shown the relations and features of our databases with ER diagram. We created our Database with MsSql Server Management Studio 19. We have optional 2 Attacks so we created 2 Tables which are not related with themselves but includes the required output features for the chosen attack and the pushable data's for our Dashboard.

Fig. 3. Database Diagram

4.3. Dashboard

For our Dashboard we have used HTML, CSS and JavaScript coding languages for the front-end section, C# for the back-end parts with MVC Templates and the Entity Frameworks for the Database connection. With Dashboard admin users can monitor the results of the attacks and their datetimes on our own created localhost website.

5. Conclusion

In this project, we executed two different attacks on a controlled environment. In result of these attack, we have captured user keystrokes and local account information. This result was captured and with the app and then transferred to the database. The dashboard will get the data and admins will be able to analyze the result of these attacks. In the future we aim to remotely execute the scripts in a test environment and add encryption algorithms so that security of the stored data will be protected.

References

[1] Annisa DwiayuRamadhanty, Avon Budiono and Ahmad Almaarif, "Implementation and Analysis of Keyboard Injection Attack using USB Devices in Windows Operating System", 2020 3rd International Conference on Computer and Informatics Engineering (IC2IE), 2020, 10.1109/IC2IE50715.2020.9274631 doi:

[2] Jerin Joy, V Rajaram, A R Aditya and V. Pandimurugan, "Developing Advanced Software Keylogger using Python and Creating Awareness of their Functionalities", 2023, 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), 10.1109/ICACRS58579.2023.10404996 doi:

[3] Mayank Srivastava, Anjali Kumari, Krishan Kant Dwivedi, Sakshit Jain, Vrishti Saxena, "Analysis and Implementation of Novel Keylogger Technique", 2021, 2021 5th International Conference on 3 Information Systems and Computer Networks (ISCON) doi:10.1109/ISCON52037.2021.9702433

[4] Aditya Shirke, Radhika Pawar, Mandar Bivalkar, Harsh Waghela and Zenith Shah, "Advance Keylogger – Capturing Keystrokes", 2023, 2023 6th International Conference on Advances in Science and Technology (ICAST), doi: 10.1109/ICAST59062.2023.10455057

[5] https://blog.talosintelligence.com2017/04/introducing-rokrat.html

[6]https://www.volexity.com/blog/2021/08/24/n orth-korean-bluelight-special-inkysquid-deploys rokrat/

[7]https://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/

[8]https://unit42.paloaltonetworks.com/babyshark-malware-part-two-attacks-continue-using kimjongrat-and-pcrat/

[9] https://securelist.com/the-kimsuky-operation a-north-korean-apt/57915

[10] https://us-cert.cisa.gov/ncas/alerts/aa20-301a

[11] https://blog.talosintelligence.com/2021/11/k i msuky-abuses-blogs-delivers-malware.html

[12] https://blog.alyac.co.kr/2234

Siber tehditlere karşı derin öğrenme ile bellek analizi kullanarak kötü amaçlı yazılım tespiti

Havvanur BOZÖMEROĞLU[1]*, Zeynep GÜRKAŞ AYDIN[1], Ebu Yusuf GÜVEN[1], Muhammed Ali AYDIN[1]

[1]İstanbul Üniversitesi-Cerrahpaşa, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, İstanbul, TÜRKİYE

Özet

Son yıllarda kötü amaçlı yazılım tehditleri, teknolojinin ilerlemesiyle birlikte katlanarak artmıştır. Bu çalışma, bellek analizi ve çok katmanlı Evrişimsel Sinir Ağı (ESA) kullanarak kötü amaçlı yazılım tespitini geliştirmeyi amaçlamaktadır ve CIC MALMEM 2022 veri setine odaklanmaktadır. Windows 10 sistemlerinden alınan bellek dökümlerini analiz ederek, hem ikili hem de çoklu sınıflandırma görevleri gerçekleştirilmiştir. Modelin eğitimi için kullanılan çok katmanlı ESA mimarisi, bellek dökümlerinden özellikleri otomatik olarak öğrenir ve bu özellikler üzerinden sınıflandırma yapar. SMOTE kullanılarak veri seti dengelenmiş ve model, sınıf dengesizliklerinden etkilenmeden daha iyi performans göstermiştir. İkili sınıflandırmada model, zararsız ve zararlı yazılım örneklerini %100 doğrulukla ayırt ederken, çoklu sınıflandırmada truva atı, casus yazılım ve fidye yazılımı gibi farklı kötü amaçlı yazılım kategorileri arasında %85 doğruluk oranına ulaşılmıştır. Bu çalışma, bellek analizi ile çok katmanlı ESA kullanarak kötü amaçlı yazılım tespitinde yüksek doğruluk oranları elde edilmesini sağlayarak, bellek dökümleri üzerinden kötü amaçlı yazılımların tespitine yönelik literatüre önemli bir katkı sağlamaktadır.

Anahtar Kelimeler: *Kötü Amaçlı Yazılım, Derin Öğrenme, CIC MALMEM 2022, İkili Sınıflandırma, Çoklu Sınıflandırma*

Detection of malware using deep learning with memory analysis against cyber threats

Abstract

In recent years, malware threats have exponentially increased with the advancement of technology. This study aims to enhance malware detection using memory analysis and a multi-layer Convolutional Neural Network (CNN), focusing on the CIC MALMEM 2022 dataset. By analyzing memory dumps from Windows 10 systems, both binary and multi-class classification tasks were performed. The multi-layer CNN architecture used for model training automatically learns features from memory dumps and classifies them. The dataset was balanced using SMOTE, allowing the model to perform better without being affected by class imbalances. In binary classification, the model achieved 100% accuracy in distinguishing benign and malicious software samples. In multi-class classification, it reached an accuracy rate of 85% in differentiating between various malware categories such as Trojans, spyware, and ransomware. This study significantly contributes to the literature on detecting malware through memory dumps by achieving high accuracy rates using memory analysis with multi-layer CNN.

Keywords: *Malware, Deep Learning, CIC MALMEM 2022, Binary Classification, Multi-Class Classification*

*Contact email: alooeff@gmail.com

1 Giriş

Kötü amaçlı yazılım, bilgisayar sistemlerine sızmak ve zarar vermek için özel olarak tasarlanmış kötü niyetli yazılım anlamına gelir[1]. Bu kötü amaçlı programlar, virüsler, solucanlar, Truva atları, fidye yazılımları, casus yazılımlar ve daha fazlası gibi birçok farklı biçimde olabilir. Kötü amaçlı yazılımlar genellikle gizlice çalışır ve önemli hasarlar meydana gelene kadar tespit edilmez, kişisel bilgileri, finansal verileri ve kritik altyapıyı tehlikeye atar[2]. Teknoloji ilerledikçe, kötü amaçlı yazılım geliştiricilerinin kullandığı teknikler ve stratejiler de gelişir, bu da bu tehditlerin tespiti ve önlenmesini giderek daha zor hale getirir.

Dijital cihazların sayısının artması ve internet bağlantısına olan bağımlılık, kötü amaçlı yazılım saldırılarında patlama yaşanmasına neden olmuştur. Bu kötü niyetli faaliyetlerdeki artış, hem bireyler hem de kuruluşlar için önemli bir tehdit oluşturur. Son raporlar, her yıl milyarlarca kötü amaçlı yazılım saldırısı gerçekleştiğini ve geleneksel tespit yöntemlerinden kaçınmak için tasarlanmış karmaşık gizleme tekniklerinde belirgin bir artış olduğunu göstermektedir[3]. Örneğin, SonicWall'a göre, 2022'nin ilk yarısında 2.8 milyar kötü amaçlı yazılım saldırısı yaşanmış olup, bu bir önceki yıla göre %11'lik bir artışı işaret etmektedir. Bu artış, daha gelişmiş ve etkili kötü amaçlı yazılım tespit stratejilerine duyulan acil ihtiyacı vurgulamaktadır.

Kötü amaçlı yazılım tehdidine yanıt olarak, derin öğrenme, siber güvenlik cephaneliğinde güçlü bir araç olarak ortaya çıkmıştır[4]. Birden fazla katmana sahip sinir ağlarını içeren derin öğrenme teknikleri, kötü amaçlı yazılımla ilişkili karmaşık kalıpları ve davranışları tanımada büyük umut vaat etmektedir. Bu yöntemler, büyük miktarda veriyi analiz edebilir ve geleneksel tespit sistemlerinin gözden kaçırabileceği ince göstergeleri öğrenebilir. Derin öğrenmeden yararlanan araştırmacılar, yeni ve gelişen kötü amaçlı yazılım tehditlerine uyum sağlayabilen daha sağlam modeller geliştirebilirler[5].

Bu çalışma, bellek analizi kullanarak bulanıklaştırılmış kötü amaçlı yazılımların tespiti ve sınıflandırılmasını geliştirmek için CIC MALMEM 2022 veri setini kullanmaktadır. Bu veri seti, Windows 10 sisteminden alınan bellek dökümlerinin dengeli bir koleksiyonunu sağlayarak hem iyi huylu hem de kötü amaçlı örnekleri içermektedir. Kötü amaçlı örnekler, fidye yazılımları, casus yazılımlar ve Truva atları gibi çeşitli kötü amaçlı yazılım ailelerini içerirken, iyi huylu örnekler normal kullanıcı etkinlikleri aracılığıyla üretilmiş ve SMOTE kullanılarak dengelenmiştir. Bu çalışmanın amacı, çok katmanlı Evrişimsel Sinir Ağı (ESA) kullanarak bulanıklaştırılmış kötü amaçlı yazılımların tespiti ve sınıflandırılmasında bu modelin etkinliğini değerlendirmektir. ESA modeli, konvolüsyonel katmanlar aracılığıyla bellek dökümlerinden önemli özellikleri otomatik olarak öğrenir ve sınıflandırma yapar. Modelin yüksek doğruluk oranları ve düşük kayıp değerleri, bellek analizi ile kötü amaçlı yazılım tespitinde etkili olduğunu göstermektedir. Bu çalışma, daha dayanıklı siber güvenlik önlemlerinin geliştirilmesine katkıda bulunmayı amaçlamaktadır.

Bu makalenin yapısı şu şekilde organize edilmiştir: Bölüm II'de, kötü amaçlı yazılım tespiti ve sınıflandırma teknikleri üzerine yapılan ilgili çalışmalar ve bu alandaki derin öğrenme uygulamalarının evrimi ve mevcut durumu tartışılmaktadır. Bölüm III, bu çalışmada kullanılan veri ön işleme, özellik çıkarma ve ESA modelinin tasarımı dahil olmak üzere metodolojiyi detaylandırmaktadır. Bölüm IV, deneysel sonuçları sunarak modelin CIC MALMEM 2022 veri seti üzerindeki performansının kapsamlı bir değerlendirmesini sağlar. Bölüm V, bulguların tartışılması, bunların sonuçları ve çalışmanın potansiyel sınırlamalarını içermektedir. Son olarak, Bölüm VI, katkıların bir özetini sunar ve gelecekteki araştırmalar için yön önerileri getirir, tespit doğruluğunu artırmaya ve analiz kapsamını diğer kötü amaçlı yazılım davranışlarını da içerecek şekilde genişletmeye odaklanır.

2 Literatür Taraması

Kötü amaçlı yazılımların artan karmaşıklığına yanıt olarak, araştırmacılar siber güvenlik çabalarını güçlendirmek için yenilikçi yaklaşımlar keşfetmeye devam etmektedir. Gelişmiş tekniklerin, özellikle makine öğrenimi algoritmalarının ve davranış analizinin kullanımı, kötü amaçlı yazılım tespitinin doğruluğunu ve verimliliğini artırmada umut vaat etmektedir.

Khan ve arkadaşları[6], yapay sinir ağları (YSA) kullanarak gizlenmiş kötü amaçlı yazılımların tespitini ele almıştır. Bu çalışma, YSA modelini kullanarak statik ve dinamik analiz yöntemleri ile kötü amaçlı yazılımları tespit etmiş ve modelin yüksek doğruluk sağladığını göstermiştir. Benkerroum ve arkadaşları[7], dijital adli analiz

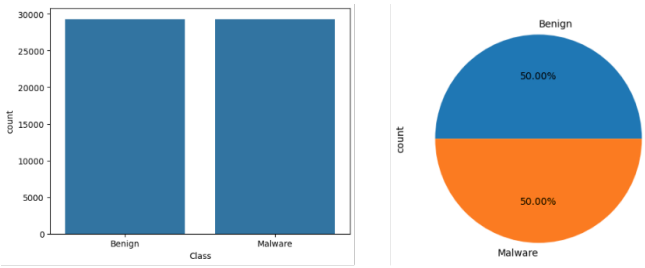
sürecini makine öğrenimi tabanlı yaklaşımla otomatikleştirmiştir. Çalışmada, CIC-MalMem-2022 veri seti kullanılarak Rastgele Orman ve Gradyanla Güçlendirilmiş Ağaç algoritmalarının bellek taramaları yoluyla kötü amaçlı yazılım tespitinde üstün performans sergilediği bulunmuştur. Salem ve arkadaşları[8], karar ağaçları sınıflandırıcılarını kullanarak kötü amaçlı yazılım tespiti için veri madenciliği tekniklerini araştırmışlardır. CIC-MalMem-2022 veri setini kullanarak, kötü amaçlı yazılımları ve bunların çeşitli ailelerini tespit etmek için özellik çıkarma ve bağımsız bileşen analizi yöntemlerini uygulamışlardır. Sonuçlar, bu yöntemlerin kötü amaçlı yazılımları yüksek doğrulukla tespit etmede etkili olduğunu göstermiştir. Mezina ve arkadaşları[9], genişletilmiş evrişimsel ağlar kullanarak kötü amaçlı yazılım tespitinde yeni bir yaklaşım önermiştir. Bu çalışmada, bellek tabanlı kötü amaçlı yazılım tespiti için CIC-MalMem-2022 veri seti kullanılmış ve önerilen modelin yüksek doğruluk oranları sağladığı gösterilmiştir. Smith ve arkadaşları[10], gözetimli ve gözetimsiz öğrenme tekniklerinin kötü amaçlı yazılım veri setleri üzerindeki performansını değerlendirmiştir. CIC-MalMem-2022 veri seti üzerinde yapılan bu çalışma, derin öğrenme tabanlı yöntemlerin kötü amaçlı yazılım tespitinde etkinliğini vurgulamaktadır. Balasubramanian ve arkadaşları[11], CIC-MalMem-2022 veri setinden elde edilen bellek verilerini kullanarak, makine öğrenimi yöntemleri ile yüksek doğrulukla kötü amaçlı yazılım tespiti yapılmıştır. Çeşitli makine öğrenimi modelleri ve performans metrikleri incelenmiş ve karşılaştırılmıştır. Özellikle, bellek analizi yoluyla disk izi bırakmayan ve bellek içinde çalışan kötü amaçlı yazılımlar gibi atipik kötü amaçlı yazılımların tespitine odaklanılmıştır. Louk ve arkadaşları[12], PE kötü amaçlı yazılımın analizinde kullanılan çeşitli ağaç tabanlı topluluk öğrenme yöntemleri karşılaştırılmıştır. Rastgele Ağaçlar, XGBoost, CatBoost, GBM ve LightGBM gibi teknikler, BODMAS, Kaggle ve CIC-MalMem-2022 gibi veri setleri kullanılarak performans ölçütleriyle değerlendirilmiştir. Sonuçlar, tüm ağaç tabanlı toplulukların iyi performans gösterdiğini ve hiperparametreleri uygun şekilde ayarlandığında algoritmalar arasındaki performans farklarının istatistiksel olarak anlamlı olmadığını göstermiştir. Dener ve arkadaşları[13], CIC-MalMem-2022 veri seti kullanılarak bellek verileriyle kötü amaçlı yazılım tespiti yapılmıştır. Pyspark ve Apache Spark platformlarında, çeşitli derin öğrenme ve makine öğrenme algoritmaları kullanılarak ikili sınıflandırma gerçekleştirilmiştir. Bellek analizi ile en yüksek başarı, %99.97 doğrulukla Lojistik Regresyon algoritmasıyla elde edilmiştir.

Bu literatür incelemesi, makine öğrenimi ve derin öğrenme tekniklerinin kötü amaçlı yazılım tespiti ve sınıflandırmasında nasıl kullanıldığını ve bu yöntemlerin etkinliğini artırmak için hangi stratejilerin uygulandığını göstermektedir. Bu çalışmalar, hem statik hem de dinamik analiz yöntemlerinin yanı sıra bellek analizine dayalı tespit tekniklerinin önemini vurgulamaktadır. Literatürdeki bu bulgular, makine öğrenimi tabanlı modellerin kötü amaçlı yazılımları yüksek doğrulukla tespit etme potansiyelini ortaya koymaktadır ve bu da bu çalışmanın temelini oluşturmaktadır.

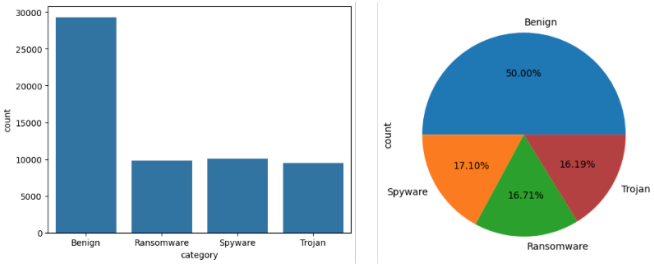
3 Metodoloji

3.1 Veri Kümesi

Bu çalışmada kullanılan veri seti, CIC MALMEM 2022 veri setidir. Bu veri seti, Windows 10 sisteminden alınan bellek dökümlerini içermekte olup, hem kötü amaçlı hem de iyi huylu örnekleri kapsamaktadır. Kötü amaçlı örnekler, fidye yazılımları (ransomware), casus yazılımlar (spyware) ve Truva atları (trojans) gibi çeşitli kötü amaçlı yazılım ailelerinden toplanmıştır. Toplamda 58,596 örnek içeren veri setinin 29,298'i kötü amaçlı yazılımlardan, 29,298'i ise iyi huylu yazılımlardan oluşmaktadır. Şekil 1'de kötü yazılım ve kötü olmayan yazılım verisinin grafikleri gösterilmiştir. Kötü amaçlı yazılımın kategori bazında dağılımı Şekil 2'de gösterilmiştir. Veri setinin dengelenmesi için SMOTE kullanılmıştır, böylece sınıflar arasında eşit dağılım sağlanmıştır.



Şekil 1. Zararsız ve zararlı kötü yazılım verisinin dağılım grafikleri

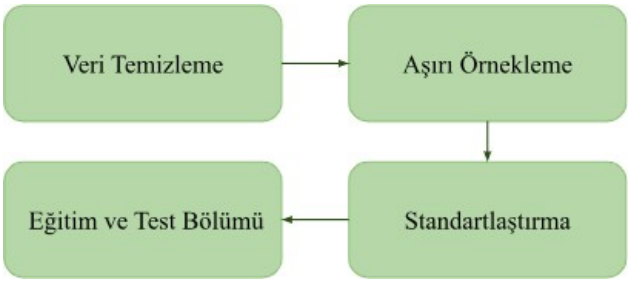


Şekil 2. Kötü amaçlı yazılımın grafik dağılımı

3.2 Veri Ön İşleme

Veri ön işleme adımları, modelin doğru ve etkili bir şekilde eğitilmesi için kritik öneme sahiptir. Bu çalışmada, veri seti üzerinde birkaç önemli ön işleme adımı uygulanmıştır. İlk olarak, veri seti eğitim ve test veri setleri olarak ikiye ayrılmıştır. Eğitim veri seti, veri setinin %80'ini, test veri seti ise %20'sini oluşturmaktadır. Bu adım, modelin performansının bağımsız olarak değerlendirilmesine olanak tanır. Daha sonra, veriler StandardScaler kullanılarak ölçeklendirilmiştir. Bu ölçeklendirme işlemi, verilerin belirli bir aralıkta normalize edilmesini sağlayarak modelin daha hızlı ve etkili bir şekilde öğrenmesine yardımcı olmaktadır. Normalizasyon, veriler arasındaki farklılıkları azaltarak modelin performansını artırır.

Son olarak, eğitim veri setine SMOTE yöntemi uygulanmıştır. SMOTE, azınlık sınıflarına ait örneklerin sayısını artırarak veri setini dengeler ve böylece modelin dengeli bir şekilde öğrenmesini sağlar. Bu yöntem, veri setindeki sınıf dengesizliğini giderir ve modelin her sınıfı da etkin bir şekilde öğrenmesini sağlar. SMOTE, azınlık sınıflarının temsilini artırarak modelin genel doğruluğunu ve sınıflandırma performansını iyileştirir. Bu ön işleme adımları, modelin daha sağlam ve güvenilir sonuçlar üretmesini sağlamak için kritik öneme sahiptir. Ön işleme adımları Şekil 3'te gösterilmiştir.



Şekil 3. Ön işlem adımları

3.3 Model Mimarisi

Evrişimsel Sinir Ağı modeli, farklı konvolüsyonel ve tam bağlantılı katmanlardan oluşan derin bir yapıya sahiptir ve her bir katman belirli bir işlevi yerine getirir. Modelin başlangıcında, giriş verisi bir konvolüsyonel katmana geçirilir. Bu katman, görüntüdeki yerel özellikleri yakalamak amacıyla 64 adet 3x1 boyutunda filtre kullanır. ReLU aktivasyon fonksiyonu, negatif değerleri sıfıra çevirerek doğrusal olmayan bir dönüşüm sağlar. Konvolüsyonel katmanın ardından gelen max-pooling katmanı, özellik haritalarının boyutunu küçültürken önemli bilgileri korur ve fazlalıkları azaltır. Daha sonra, özelliklerin daha derin ve daha karmaşık temsillerini öğrenmek için ikinci ve üçüncü konvolüsyonel katmanlar devreye girer. İkinci katman, 128 filtre ve üçüncü katman ise 256 filtre kullanır. Her iki katmanda da max-pooling işlemi, veri boyutunu küçültmeye ve modelin hesaplama verimliliğini arttırmaya yardımcı olur. Konvolüsyonel katmanlar ve max-pooling işlemleri tamamlandıktan sonra, veri düzleştirilir ve tam bağlantılı katmanlara aktarılır. İlk tam bağlantılı katman, 512 nöron içerir ve yine ReLU aktivasyon fonksiyonu kullanır. Bu katmanı takip eden batch normalization katmanı, her mini-batch'ten sonra aktivasyonları normalize eder, böylece öğrenme sürecinin hızlanmasına ve stabilize olmasına yardımcı olur. Dropout katmanı ise aşırı öğrenmeyi (overfitting) önlemek için belirli nöronları rastgele devre dışı bırakır. İkinci ve üçüncü tam bağlantılı katmanlar sırasıyla 256 ve 128 nöron içerir ve her ikisi de ReLU aktivasyon fonksiyonu kullanır. Bu katmanlar da batch normalization ve dropout katmanları ile desteklenir, böylece modelin daha genel hale gelmesi sağlanır.

Son olarak, çıkış katmanı, softmax aktivasyon fonksiyonu ile 4 nörondan oluşur. Bu katman, modelin her bir giriş örneği için dört sınıf olasılıkları üretmesini sağlar. Model, sınıflandırma görevini yerine getirirken bu olasılıklar üzerinden karar verir. Bu ESA modeli, konvolüsyonel ve tam bağlantılı katmanları bir araya getirerek veri kümesindeki karmaşık ve hiyerarşik özellikleri öğrenir ve bunları sınıflandırma amacıyla kullanır. Batch normalization ve dropout gibi teknikler, modelin daha hızlı ve verimli öğrenmesini, aynı zamanda genel performansının artmasını sağlar.

4 Deneysel Sonuçlar

Modelin eğitimi ve doğrulanması için 5 katlı çapraz doğrulama (KFold) kullanılmıştır. Bu yöntem, veri setinin farklı bölümlerinin eğitim ve doğrulama

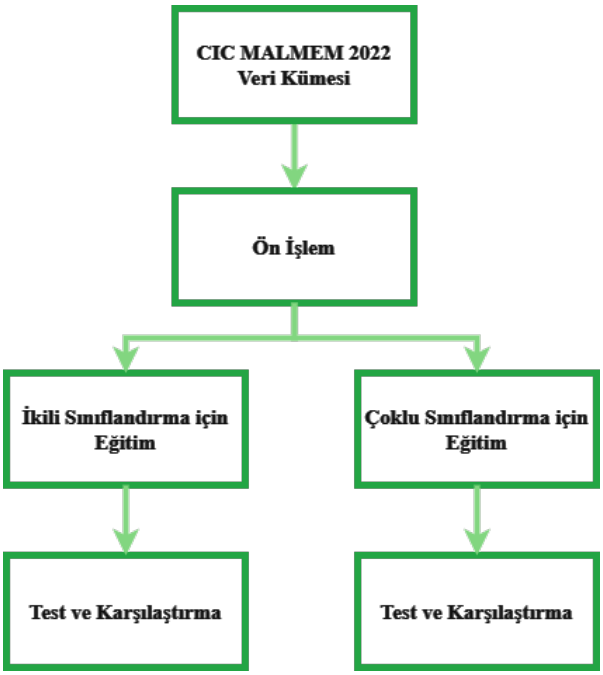
süreçlerinde kullanılmasını sağlar ve modelin genel performansını değerlendirir. Bu bölümde, modelin eğitim ve doğrulama süreçleri detaylı bir şekilde açıklanmaktadır.

Eğitim sürecinde, model 300 epoch boyunca eğitilmiştir. Epoch, modelin tüm eğitim veri seti üzerinden bir kez geçiş yapmasını ifade eder. Her epoch sırasında model, eğitim veri setindeki veriler üzerinde öğrenme işlemi gerçekleştirir. Modelin eğitim sürecinde aşırı öğrenmeyi önlemek ve genel performansı artırmak için erken durdurma tekniği kullanılmıştır. Erken durdurma, modelin doğrulama kaybına göre eğitimin durdurulmasını sağlar. Doğrulama kaybı, modelin doğrulama veri seti üzerindeki tahmin hatasını temsil eder. Eğitim sürecinde, doğrulama kaybı sürekli olarak izlenir ve eğer belirli bir süre boyunca (bu çalışmada 10 epoch) doğrulama kaybında bir iyileşme görülmezse, eğitim süreci durdurulur. Bu, modelin en iyi performansı gösterdiği noktada eğitimin sonlandırılmasını sağlar ve aşırı öğrenmeyi engeller. Öğrenme oranı, modelin her adımda ağırlıklarını ne kadar değiştirdiğini belirleyen önemli bir hiper parametredir. Bu çalışmada, doğrulama kaybına göre dinamik olarak ayarlanan öğrenme oranı zamanlama tekniği kullanılmıştır. ReduceLROnPlateau adı verilen bu teknik, doğrulama kaybında bir iyileşme görülmediğinde öğrenme oranını yarıya indirir. Tablo 1'de, modelin eğitiminde kullanılan hiper parametrelerin bir özetini sunar ve her bir hiper parametrenin değerini ve amacını açıklar. Bu şekilde, modelin nasıl yapılandırıldığını ve hangi parametrelerin kullanıldığını kolayca görebilirsiniz.

Eğitim ve test veri setlerinin oluşturulması süreci ve bu veri setlerinin oranları ile dağılımları açıklanmıştır. Eğitim ve test veri setleri, CIC-MalMem-2022 veri setinden elde edilen bellek dökümleri kullanılarak oluşturulmuştur. Veri kümesi, %80 eğitim ve %20 test oranında bölünmüştür. Eğitim veri seti, modelin öğrenme sürecinde kullanılmış, test veri seti ise modelin performansını değerlendirmek için ayrılmıştır. Eğitim ve test veri kümelerinin dengeli ve homojen bir dağılıma sahip olması, modelin genel performansını artırmak amacıyla sağlanmıştır. Çalışma akışı Şekil 5'te gösterilmiştir.

Hiper Parametre	Değer
Epoch sayısı	300
Batch boyutu	32
Öğrenme oranı	0.0001
Dropout oranı	0.5
Aktivasyon fonksiyonu	ReLU
Çıktı aktivasyon fonksiyonu	Softmax
Erken durdurma sabrı	20
ReduceLROnPlateau sabrı	20

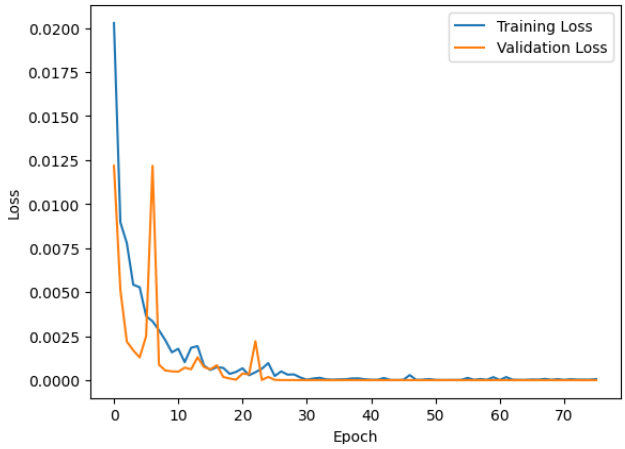
Tablo 1. Hiper parametreler



Şekil 5. Çalışma akışı

4.1 İkili Sınıflandırma

İkili sınıflandırmada elde edilen %100 doğruluk oranı, modelin tüm zararsız ve zararlı yazılım örneklerini doğru bir şekilde ayırt edebildiğini göstermektedir. Bu mükemmel sonuç, modelin bellek dökümleri üzerinden iki sınıfı da son derece etkin bir şekilde öğrenip ayırt edebildiğini kanıtlamaktadır. İkili sınıflandırma için bu kadar yüksek bir doğruluk oranı, modelin basit ve belirgin özellikleri başarılı bir şekilde öğrendiğini ve ayırt ettiğini göstermektedir. Bu sonuç, siber güvenlik uygulamalarında yüksek güvenilirlik ve etkinlik sunarak, potansiyel tehditlerin hızlı ve doğru bir şekilde tespit edilmesini sağlar.



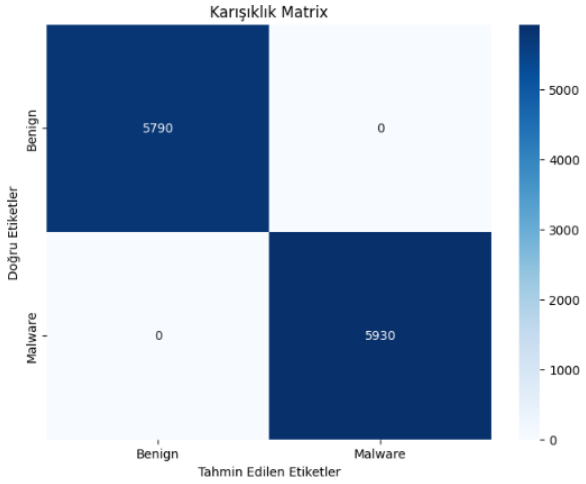
Şekil 6. İkili sınıflandırmada eğitim ve test kayıp değeri grafiği

Şekil 6'daki grafikte, modelin eğitim ve doğrulama süreçlerinde kayıp değerlerinin nasıl değiştiği gösterilmektedir. Eğitim süreci boyunca her iki kayıp değeri de hızla düşmekte ve düşük bir seviyede stabilize olmaktadır. Eğitim ve doğrulama kayıpları başlangıçta oldukça yüksek, ancak ilk birkaç epoch içinde hızlı bir şekilde düşüyor. Bu durum, modelin hızla öğrenmeye başladığını ve hem eğitim hem de doğrulama veri setlerinde hata oranını hızla azaldığını gösterir.

Eğitim kaybı, yaklaşık 20. epoch'tan sonra çok düşük ve sabit bir seviyeye ulaşmaktadır. Bu, modelin eğitim veri setindeki hataları minimize ettiğini ve öğrenmenin büyük ölçüde tamamlandığını gösterir. Doğrulama kaybında bazı dalgalanmalar görülmektedir. Ancak genel trend, doğrulama kaybının da azaldığını ve düşük bir seviyede sabit kaldığını göstermektedir. Bu dalgalanmalar, doğrulama veri setindeki bazı örneklerin eğitim veri kümelerindekilerden farklı olabileceğini ve modelin bu örneklerde bazen hata yapabildiğini gösterir. Eğitim ve doğrulama kayıplarının benzer seviyelerde olması, modelin aşırı öğrenme yapmadığını gösterir. Eğer doğrulama kaybı eğitim kaybına göre önemli ölçüde daha yüksek olsaydı, modelin aşırı öğrenme yaptığı düşünülebilirdi. Bu grafikte görülen düşük ve stabilize olmuş kayıplar, modelin genel olarak hem eğitim hem de doğrulama veri setlerinde iyi performans gösterdiğini ve etkili bir şekilde öğrendiğini göstermektedir.

Şekil 7'deki karmaşıklık matrisi, modelin sınıflandırma performansını detaylı bir şekilde değerlendirir. Bu özel matriste, modelin mükemmel bir performans gösterdiği görülmektedir. Model, 5790 zararsız yazılım örneğini ve 5930 zararlı yazılım örneğini doğru şekilde sınıflandırmıştır. Bu, modelin %100 doğrulukla çalıştığını ve tüm örnekleri doğru sınıflandırıldığını gösterir. Matristen görülebileceği gibi, model hiçbir örneği yanlış sınıflandırmamıştır (0 yanlış pozitif ve 0 yanlış negatif). Bu, modelin hem zararsız hem de zararlı yazılım örneklerini mükemmel bir doğrulukla ayırt edebildiğini göstermektedir.

Bu sonuçlar, modelin son derece etkili olduğunu ve bellek dökümlerinden elde edilen verilerle kötü amaçlı yazılımları doğru bir şekilde tespit edebildiğini göstermektedir. Modelin böyle yüksek bir doğrulukla çalışması, özellikle siber güvenlik alanında önemli bir başarı olarak değerlendirilebilir.



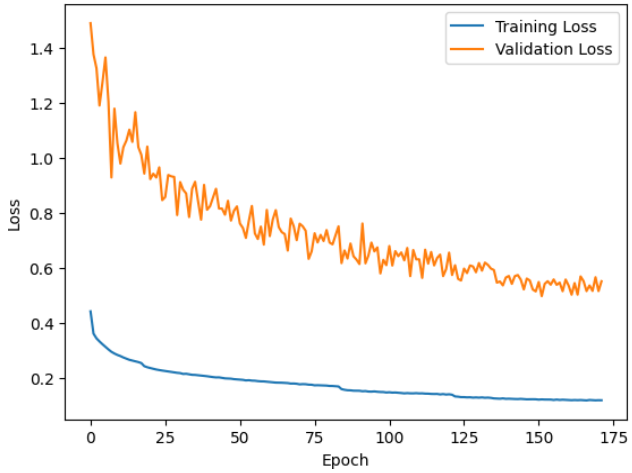
Şekil 7. İkili sınıflandırmada karmaşıklık matrisi

4.2 Çoklu Sınıflandırma

Çoklu sınıflandırmada elde edilen %85 doğruluk oranı, modelin Trojan, Spyware ve Ransomware gibi farklı kötü amaçlı yazılım kategorilerini ayırt etme kapasitesinin yeterli olduğunu ancak mükemmel olmadığını göstermektedir. Bu doğruluk oranı, modelin çoğu örneği doğru sınıflandırıldığını, ancak bazı sınıflar arasında karışıklıklar yaşadığını göstermektedir. Özellikle Spyware sınıfında daha fazla yanlış sınıflandırma yapıldığı göz önüne alındığında, modelin bu sınıfta daha fazla zorlandığı anlaşılmaktadır. Çoklu sınıflandırmadaki bu sonuç, modelin daha karmaşık ve ince ayırt edici özellikleri öğrenmede zorlandığını, bu nedenle bazı sınıfları karıştırabileceğini gösterir. Ancak %81 doğruluk oranı hala kabul edilebilir bir seviyedir ve modelin genel performansının iyi olduğunu göstermektedir. Bu sonuçlar, modelin eğitim sürecinde bazı iyileştirmeler yapılarak doğruluk oranının

artırılabileceğini ve belirli sınıfların daha iyi ayırt edilebileceğini işaret etmektedir.

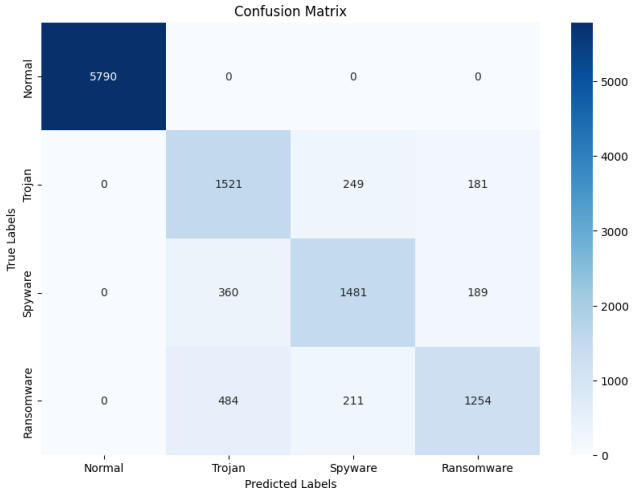
Eğitim ve doğrulama kayıplarının epoch sayısına göre değişimini gösteren Şekil 8'deki grafikte, eğitim kaybının başlangıçtan itibaren düzenli bir şekilde azaldığı ve sonlarda oldukça düşük bir seviyeye ulaştığı gözlemlenmektedir. Bu durum, modelin eğitim verisi üzerindeki hatalarını giderek azaldığını ve başarılı bir eğitim süreci geçirdiğini göstermektedir. Doğrulama kaybı ise başlangıçta yüksek değerlerde seyretmekte, ancak epoch sayısı arttıkça azalmakta ve düşük seviyelerde stabilize olmaktadır. Doğrulama kaybında zaman zaman dalgalanmalar görülse de genel olarak düşük seviyelerde sabitlenmesi, modelin doğrulama veri setinde de etkili bir şekilde performans sergilediğine işaret etmektedir.



Şekil 8. Çoklu sınıflandırmada eğitim ve test kayıp değeri grafiği

Modelin test veri seti üzerindeki performansı değerlendirildiğinde, test kaybının 0.3984 ve test doğruluğunun %85.7 olduğu görülmektedir. Bu, modelin test veri setinde yüksek bir doğruluk oranı ile çalıştığını ve hatalarını minimize ettiğini göstermektedir. Ancak, karışıklık matrisine bakıldığında, modelin belirli sınıflar arasında bazı karışıklıklar yaşadığı anlaşılmaktadır. Özellikle Trojan, Spyware ve Ransomware gibi kötü amaçlı yazılım kategorileri arasında karışıklıklar yaşanmış, Spyware sınıfında daha fazla yanlış sınıflandırma yapılmıştır.

Şekil 9'daki karmaşıklık matrisine göre model, zararsız yazılımları %100 doğrulukla sınıflandırırken, kötü amaçlı yazılım kategorileri arasında bazı karışıklıklar yaşamaktadır. Trojan, Spyware ve Ransomware sınıflarında doğru sınıflandırma oranları yüksek olmasına rağmen, özellikle Trojan ve Ransomware sınıfları arasında belirgin yanlış sınıflandırmalar dikkat çekmektedir.



Şekil 9. Çoklu sınıflandırmada karmaşıklık matrisi

Spyware sınıfında da önemli miktarda karışıklık yaşanmış ve bazı örnekler Trojan veya Ransomware olarak yanlış sınıflandırılmıştır. Bu sonuçlar, modelin zararsız yazılım tespitinde mükemmel performans gösterdiğini, ancak belirli kötü amaçlı yazılım sınıflarını ayırt etmede zorlandığını göstermektedir. Bu durumu iyileştirmek için daha çeşitli ve dengeli veri setleriyle eğitim, özellik mühendisliği, farklı derin öğrenme mimarilerinin denenmesi ve hiper parametre optimizasyonu gibi yöntemler önerilebilir. Bu iyileştirmeler, modelin genel performansını artırarak, kötü amaçlı yazılım tespitinde daha güvenilir ve etkin bir siber güvenlik aracı olmasını sağlayacaktır.

5 Tartışma

İkili sınıflandırmada, modelin zararsız ve zararlı yazılım örneklerini %100 doğrulukla ayırt edebildiği görülmektedir. Eğitim ve doğrulama kayıpları zamanla azalmakta ve düşük seviyede stabilize olmaktadır, bu da modelin her iki veri setinde de etkili bir şekilde öğrendiğini göstermektedir. Bu sonuçlar, modelin bellek dökümlerinden kötü amaçlı yazılım tespitinde son derece başarılı olduğunu göstermektedir. Çoklu sınıflandırmada (Trojan, Spyware, Ransomware), modelin genel olarak yüksek bir doğrulukla çalıştığı ancak bazı sınıflar arasında karışıklıklar yaşadığı görülmektedir. Özellikle Trojan ve Ransomware sınıflarında doğru sınıflandırma oranları yüksekken, Spyware sınıfında daha fazla yanlış sınıflandırma yapılmıştır. Eğitim ve doğrulama kayıpları bu durumda da zamanla azalmakta, ancak

doğrulama kaybında bazı dalgalanmalar gözlenmektedir.

Model, çok katmanlı ESA mimarisi kullanılarak eğitilmiştir. ESA yapısı, giriş verilerinden önemli özellikleri otomatik olarak öğrenerek sınıflandırma işlemini gerçekleştirmektedir. Modelin güçlü yönleri arasında, ikili sınıflandırmada mükemmel doğrulukla çalışması ve hiçbir yanlış sınıflandırma yapmaması bulunmaktadır. Eğitim ve doğrulama süreçlerinde düşük ve stabilize olmuş kayıp değerleri, modelin genel olarak iyi performans gösterdiğini ve aşırı öğrenme yapmadığını göstermektedir. Ayrıca, çoklu sınıflandırmada da yüksek doğruluk oranları, modelin farklı kötü amaçlı yazılım kategorilerini ayırt etme kapasitesini göstermektedir.

Ancak, modelin zayıf yönleri de vardır. Çoklu sınıflandırmada, özellikle Spyware sınıfında daha fazla yanlış sınıflandırma yapılması, modelin bazı sınıflarda zorlandığını göstermektedir. Doğrulama kaybındaki dalgalanmalar, modelin doğrulama veri seti üzerindeki performansının zaman zaman değişken olduğunu göstermektedir. Bu, modelin belirli sınıflar arasında net bir ayrım yapmada zorlandığını ve daha fazla iyileştirme gerektirdiğini işaret eder.

Genel olarak, ikili sınıflandırmada elde edilen mükemmel sonuçlar, modelin temel kötü amaçlı yazılım tespit görevlerinde son derece başarılı olduğunu göstermektedir. Çoklu sınıflandırmada ise, modelin karmaşık kategorileri ayırt etme kapasitesinin artırılması gerekmektedir. Bu amaçla, modelin daha fazla veriyle eğitilmesi, farklı derin öğrenme mimarilerinin denenmesi ve özellikle zayıf performans gösteren sınıflar için daha özel özellik mühendisliği yapılması önerilebilir. Ayrıca, modelin doğruluk oranını artırmak için hiper parametre optimizasyonu ve düzenleme teknikleri gibi iyileştirme yöntemleri de uygulanabilir. Özellikle çok katmanlı ESA yapısının daha derinlemesine incelenmesi ve gerektiğinde katman sayısı veya filtre boyutları gibi hiper parametrelerin optimize edilmesi faydalı olabilir. Bu iyileştirmeler, modelin genel performansını artırarak daha güvenilir ve etkin bir siber güvenlik aracı olmasını sağlayacaktır.

6 Sonuç

Bellek analizi ve derin öğrenme teknikleri kullanılarak kötü amaçlı yazılımların tespit edilmesi, geleneksel yöntemlere göre daha detaylı ve etkili bir yaklaşım sunar. Bu çalışma, bellek verilerinden elde edilen bilgilerin, bilgisayar belleğinde çalışan ve diskte iz bırakmayan kötü amaçlı yazılımların tespitinde önemli bir rol oynadığını göstermektedir. Derin öğrenme, büyük veri setlerini analiz ederek karmaşık kalıpları tanıyabilme kapasitesiyle siber güvenlik sistemlerini daha dayanıklı hale getirmektedir. Çok katmanlı ESA modeli, özellikle yüksek boyutlu ve karmaşık verilerde üstün performans göstererek, zararlı yazılımların bellek dökümleri üzerinden tespit edilmesini sağlamıştır.

Bu çalışma, CIC MALMEM 2022 veri setini kullanarak bellek dökümleri üzerinden kötü amaçlı yazılımların tespiti ve sınıflandırılmasını hedeflemiştir. İkili ve çoklu sınıflandırma yöntemleri kullanılarak, modelin zararsız ve zararlı yazılım örneklerini, ayrıca Trojan, Spyware ve Ransomware gibi farklı kötü amaçlı yazılım kategorilerini ayırt etme performansı değerlendirilmiştir. Bu amaçla, çok katmanlı Evrişimsel Sinir Ağı mimarisi kullanılarak model eğitilmiştir. Eğitim ve doğrulama süreçlerinde düşük ve stabilize olmuş kayıp değerleri, modelin her iki veri setinde de etkili bir şekilde öğrendiğini göstermiştir. İkili sınıflandırmada model %100 doğrulukla çalışırken, çoklu sınıflandırmada bazı sınıflar arasında karışıklıklar yaşanmış ancak genel olarak yüksek doğruluk oranları elde edilmiştir. Bu bulgular, modelin bellek dökümleri üzerinden kötü amaçlı yazılım tespitinde son derece başarılı olduğunu göstermektedir.

7 Gelecek Çalışmalar

Gelecekteki çalışmalar, derin öğrenme modellerinin bulanıklaştırılmış kötü amaçlı yazılım tespitindeki etkinliğini daha da artırmak amacıyla birkaç yönde ilerleyebilir. İlk olarak, farklı derin öğrenme mimarilerinin, özellikle Transformer ve Recurrent Neural Networks (RNN) gibi modellerin, ESA ile karşılaştırılması yapılarak tespit doğruluğunun artırılması araştırılabilir. Ayrıca, zaman serisi analizleri ve bellek dökümlerinin dinamik özelliklerini yakalamak için zaman-temelli derin öğrenme yaklaşımlarının entegrasyonu değerlendirilebilir. Veri kümesi çeşitliliğini artırmak için, farklı işletim sistemlerinden ve farklı kötü amaçlı yazılım ailelerinden daha geniş ve dengeli veri setleri toplanabilir. Bu da modelin genelleme kabiliyetini artırabilir ve daha geniş bir yelpazede kötü amaçlı yazılımları tespit etmesini sağlayabilir. Ayrıca, modelin gerçek zamanlı saldırılara karşı performansını değerlendirmek için daha fazla deney yapılabilir ve modelin hesaplama verimliliğini artırmaya yönelik optimizasyon teknikleri geliştirilebilir. Son olarak, tespit edilen

kötü amaçlı yazılımların otomatik olarak analiz edilmesi ve raporlanması için akıllı sistemlerin geliştirilmesi, güvenlik uzmanlarına daha hızlı ve etkili müdahale imkanları sunabilir.

Kaynaklar

[1] Akhtar MS, Feng T. "Evaluation of Machine Learning Algorithms for Malware Detection". Sensors, 23(2), 946, 2023. https://doi.org/10.3390/s23020946

[2] Majid, Al-Ani & Alshaibi, Ahmed & Kostyuchenko, Evgeny & Shelupanov, Alexander. "A review of artificial intelligence based malware detection using deep learning". Materials Today: Proceedings, 10.1016/j.matpr.2021.07.012, 2021.

[3] Djenna A, Bouridane A, Rubab S, Marou IM. "Artificial Intelligence-Based Malware Detection, Analysis, and Mitigation". Symmetry, 15(3), 677, 2023. https://doi.org/10.3390/sym15030677

[4] Brown, Austin & Gupta, Maanak & Abdelsalam, Mahmoud. "Automated machine learning for deep learning based malware detection". Computers & Security, 137, 103582, 2023. 10.1016/j.cose.2023.103582.

[5] Gaurav, Akshat & Gupta, Brij & Panigrahi, Prabin. "A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system". Enterprise Information Systems, 17, 1-25, 2022. 10.1080/17517575.2021.2023764.

[6] Khan LP. "Obfuscated Malware Detection Using Artificial Neural Network (ANN)". 2023 Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT), Erode, India, 2023, pp. 1-5. doi: 10.1109/ICECCT56650.2023.10179639.

[7] Benkerroum, Samira & Chougdali, Khalid. "Enhancing Forensic Analysis Using a Machine Learning-based Approach". 2023, 1-6. 10.1109/CommNet60167.2023.10365260.

[8] Salem, Israa & Al-Saedi, Karim. "Intensive Malware Detection Approach based on Data Mining". Journal of Applied Engineering and Technological Science (JAETS), 5, 414-424, 2023. 10.37385/jaets.v5i1.2865.

[9] Mezina, Anzhelika & Burget, Radim. "Obfuscated malware detection using dilated convolutional network". 2022, 110-115. 10.1109/ICUMT57764.2022.9943443.

[10] Smith, Daryle & Khorsandroo, Sajad & Roy, Kaushik. "Supervised and Unsupervised Learning Techniques Utilizing Malware Datasets". 2023, 1-7. 10.1109/ICAIC57335.2023.10044169.

[11] Balasubramanian, Karthik & Vasudevan, Shri & Kumar, T. & T, Gireesh & Srinivasan, Kartik & Tibrewal, Anjali & Vajipayajula, Sulakshan. "Obfuscated Malware detection using Machine Learning models". 2023, 1-8. 10.1109/ICCCNT56998.2023.10307598.

[12] Louk, Maya & Adhi Tama, Bayu. "Tree-Based Classifier Ensembles for PE Malware Analysis: A Performance Revisit". Algorithms, 15, 332, 2022. 10.3390/a15090332.

[13] Dener, Murat & Ok, Gökçe & Orman, Abdullah. "Malware Detection Using Memory Analysis Data in Big Data Environment". Applied Sciences, 12, 23, 2022. 10.3390/app12178604.

[14] Hasan, S. M. R., & Dhakal, A. "Obfuscated Malware Detection: Investigating Real-world Scenarios through Memory Analysis". arXiv preprint arXiv:2404.02372, 2024.

Nesnelerin interneti güvenliğinde yapay zeka ikilemi: Saldırganların güç kazandığı noktalar

The artificial intelligence dilemma in internet of things security: Points Where Attackers Gain Power

Hatice Yüsra *KAYA*[1]*, Zeynep *GÜRKAŞ AYDIN*[2], Ebu Yusuf *GÜVEN*[3], Muhammed Ali *AYDIN*[4]

[1]*İstanbul Üniversitesi-Cerrahpaşa, Mühendislik Fakültesi, Bilgisayar Mühendisliği, İstanbul, TÜRKİYE*
haticeyusrakaya@ogr.iuc.edu.tr
[2]*İstanbul Üniversitesi-Cerrahpaşa, Mühendislik Fakültesi, Bilgisayar Mühendisliği, İstanbul, TÜRKİYE*
zeynepg@iuc.edu.tr
[3]*İstanbul Üniversitesi-Cerrahpaşa, Mühendislik Fakültesi, Bilgisayar Mühendisliği, İstanbul, TÜRKİYE*
eyguven@iuc.edu.tr
[4]*İstanbul Üniversitesi-Cerrahpaşa, Mühendislik Fakültesi, Bilgisayar Mühendisliği, İstanbul, TÜRKİYE*
aydinali@iuc.edu.tr

Özet

Günümüzün hızla dijitalleşen dünyasında, Nesnelerin İnterneti (IoT), evlerimizden endüstriyel tesislere kadar geniş bir yelpazede kullanılmaya başlandı. IoT cihazlarının yaygınlaşması, hayatımızı kolaylaştırmakla birlikte, beraberinde ciddi güvenlik tehditlerini de getirdi. Bu tehditlere karşı alınması gereken önlemler konusunda yapay zeka hem bir çözüm hem de potansiyel bir sorun kaynağı olarak karşımıza çıkıyor. Bu makalede, yapay zekanın IoT güvenliğinde nasıl bir rol oynadığını, saldırganların bu teknolojiyi nasıl kullandığını ve güvenlik stratejilerinin bu yeni tehditlere karşı nasıl evrilmesi gerektiğini inceledik. Ana bulgularımız, yapay zekanın IoT cihazları için hem güçlü bir savunma mekanizması oluşturabileceğini hem de yeni saldırı vektörleri yaratabileceğini göstermektedir. Bu çerçevede, IoT güvenliğinde yenilikçi ve adaptif güvenlik yaklaşımlarının benimsenmesi gerektiği vurgulanmaktadır. Amacımız, IoT ekosisteminde yapay zekanın sağladığı fırsatlar ve yarattığı riskler arasında dengeli bir bakış açısı sunarak, bu alandaki güvenlik stratejilerine katkıda bulunmaktır.
Anahtar Kelimeler: *Nesnelerin İnterneti Güvenliği, Düşman Yapay Zeka, Makine Öğrenmesi*

Abstract

In today's rapidly digitizing world, the Internet of Things (IoT) has begun to be used in a wide range of applications, from our homes to industrial facilities. While the proliferation of IoT devices has made our lives easier, it has also brought serious security threats. Artificial intelligence (AI) emerges as both a solution and a potential problem in addressing these threats. In this article, we examined the role of AI in IoT security, how attackers leverage this technology, and how security strategies need to evolve to counter these new threats. Our main findings indicate that AI can create both a strong defense mechanism for IoT devices and new attack vectors. In this context, the adoption of innovative and adaptive security approaches in IoT security is emphasized. Our aim is to contribute to security strategies in this field by presenting a balanced perspective on the opportunities and risks posed by AI in the IoT ecosystem.
Keywords: *IoT Security, Adversarial AI, Machine Learning*

*Contact email: 222144111@firat.edu.tr

1 Giriş

Nesnelerin İnterneti (IoT), çeşitli nesneler ve sistemler arasında kesintisiz bağlantı ve iletişimi mümkün kılarak, günlük yaşamımızın birçok yönünü önemli ölçüde etkilemiştir. Ancak, verilerin iletimi ve işlenmesi sırasında gizliliğini ve bütünlüğünü sağlamak için, bu bağlantılı cihazların neden olduğu birçok güvenlik sorununu ele almak gereklidir. Geleneksel güvenlik yöntemleri, IoT cihazlarının değişken tehdit ortamına ve sınırlı özelliklerine uyum sağlamakta zorlanmaktadır. Bu cihazlar, genellikle sınırlı işlemci hızı, bellek boyutu ve enerji kaynaklarına sahip olmaktadır.

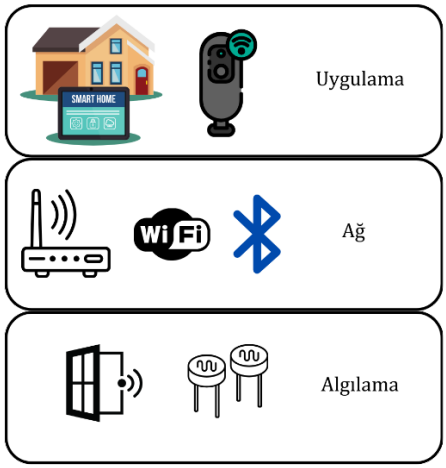
IoT güvenliğini sağlamak için yenilikçi yaklaşımlar gerekmektedir. Yapay Zeka (AI), büyük miktarda veriyi değerlendirme, kalıpları belirleme ve güvenlik tehditlerini proaktif olarak tespit etme yeteneği sayesinde bu alanda önemli bir potansiyele sahiptir. AI tabanlı çözümler, IoT güvenlik çerçevelerine entegre edilerek, değişen saldırılara karşı gerçek zamanlı tepkileri, anomali tespitini ve proaktif tehdit tanımlama ve azaltmayı iyileştirmektedir. Ancak, AI teknolojilerinin bu alandaki kullanımının artması, aynı zamanda siber saldırganlara da güç kazandırmaktadır. Yapay zeka, saldırganların IoT sistemlerinde güvenlik zafiyetlerini daha etkili bir şekilde tespit etmelerini ve bu zafiyetlerden yararlanmalarını sağlamaktadır.

Bu makale, IoT güvenliğinde AI'nın sunduğu fırsatlar ve oluşturduğu riskler arasındaki dengeyi incelemektedir. AI'nın IoT güvenliğine getirdiği avantajlar, saldırganların bu teknolojiyi kullanarak nasıl güç kazandıklarıyla birlikte değerlendirilmektedir. AI'nın sağladığı veri analizi yetenekleri, saldırganların tehdit azaltma trendleri hakkında istihbarat oluşturmalarına, hedef profillemelerine ve geniş ölçekte zafiyet kütüphaneleri oluşturmalarına olanak tanımaktadır. Bu ikilem, IoT güvenliğinde yeni bir dinamiği ortaya çıkarıyor: Yapay zeka, savunma ve saldırı yöntemlerinde bir yarış haline geliyor. Bu bağlamda, AI destekli çözümlerle IoT sistemlerinin güvenliğini artırmak ve siber saldırganların AI kullanarak oluşturduğu tehditlere karşı etkili stratejiler geliştirmek için kapsamlı bir bakış açısı sunulmaktadır.

2 Nesnelerin İnterneti

Statistica 2023 yılı verilerine göre [1], Dünya genelinde Nesnelerin İnternetine bağlı cihaz sayısı 15 milyarı geçmiştir. Bu sayının 2030 yılına kadar 30 milyara ulaşması beklenmektedir. Bu istatistikler, IoT'nin hayatımızın her alanında hızla yayıldığını ve giderek artan bir etki alanına sahip olduğunu göstermektedir. Farkında olmasak da günlük hayatımız Nesnelerin İnterneti örnekleri ile doludur. Bu teknoloji, insan müdahalesi olmadan veri alışverişi yapabilen nesnelerin oluşturduğu bir ağı temsil eder. IoT'nin temelinde, herhangi bir cihazın, veri toplama ve iletimi yeteneği olan herhangi bir tür sensörle donatılmış olması yatar. Bu, çevresel faktörlerle etkileşime girebilen ve bu bilgiyi kullanarak kararlar verebilen cihazlar demektir.

IEEE Communication Magazine'de tanımlanan ifadeyle [2], IoT'nin amacı, her şeyin internet üzerinde bir temsili ve varlığı olmasıyla, fiziksel ve sanal dünyalar arasında köprüler kurarak yeni uygulamalar ve hizmetler sunmaktır. Makine-Makine (M2M) iletişimi, Nesnelerin İnterneti'ndeki temel iletişimdir ve bu iletişim, nesnelerle bulut tabanlı uygulamalar arasındaki etkileşimleri mümkün kılar.



Şekil 1. Üç katmanlı IoT mimarisi

2.1 Nesnelerin İnterneti Ağlarına Yönelik Güvenlik Tehditleri

Nesnelerin İnterneti teknolojisi, hayatımızı kolaylaştıran faydalarının yanında göz ardı edilmemesi gereken riskler ve güvenlik tehditleriyle birlikte gelir. Sistemlerinin tasarımı nedeniyle IoT cihazlarına geleneksel güvenlik yaklaşımları doğrudan uygulanamaz. Çok sayıda cihazın bu sınırlı kaynaklarla birlikte çalışması, heterojenlik ve ölçeklenebilirlik sorunlarını

beraberinde getirir. Bu nedenle, sistemin beklenen ve beklenmeyen risklerle başa çıkabilecek kadar güçlü ve esnek olması gerekmektedir. Ayrıca, uygun algoritmalar ve protokolleri uygulayabilmek için güvenlik mekanizmalarının IoT ile entegrasyonunu sağlamak kritik bir öneme sahiptir.

IoT cihazları arasındaki veri alışverişi kablosuz iletişimle gerçekleştirildiğinden, bu durum birden fazla saldırı ve gizlilik ihlali için temel bir yöntem olarak kabul edilir. Bu nedenle, değiş tokuş edilen veriler için sıkı koruma önlemleri almak önemlidir. Mevcut koşullar altında, güvenlik ve gizlilik gerçek bir meydan okuma olmaya devam etmektedir. IoT cihazlarına yönelik saldırılar, cihazların güvenlik açıklarından faydalanarak çeşitli yollarla gerçekleştirilebilir. Bu saldırılar, cihazların donanım ve yazılım bileşenlerinden ağlarına kadar geniş bir yelpazede gerçekleşir. Aşağıda, IoT cihazlarına yönelik en yaygın saldırı yöntemleri detaylandırılmıştır.

2.1.1 İlk Keşif

Saldırganlar, hedefledikleri IoT cihazlarının zayıf noktalarını belirlemek için bu cihazları piyasadan satın alır ve tersine mühendislik ile analiz ederler. Bu süreçte, cihazın yazılımını ve donanımını inceleyerek olası saldırı yollarını tespit ederler.

2.1.2 Fiziksel Saldırılar

Bu tür saldırılar, cihazların fiziksel bileşenlerine zarar vererek veya manipüle ederek gerçekleştirilir. Örnekler arasında cihazların işlevini engellemek için ağa erişimi kesmek, fiziksel olarak zarar vermek, USB yoluyla zararlı enjekte etmek ve sinyal bozucular kullanmak yer alır.

2.1.3 Ortadaki Adam Saldırıları

Ortadaki adam saldırıları, iki iletişim noktası arasındaki verileri yakalamak ve manipüle etmek için gerçekleştirilir. IoT cihazları genellikle bu tür saldırılara karşı savunmasızdır çünkü standart güvenlik önlemlerinden yoksundurlar.

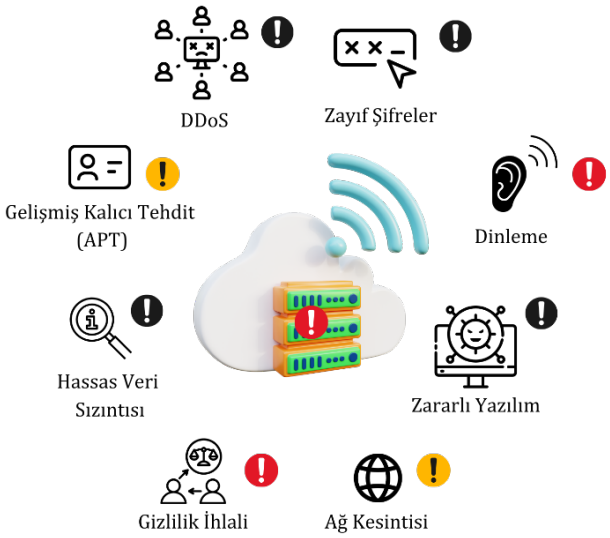
2.1.4 Botnetler

Botnet saldırıları, birçok IoT cihazının ele geçirilerek bir ağ üzerinden koordineli bir şekilde hizmet engelleme saldırıları düzenlenmesiyle gerçekleştirilir. Mirai botnet gibi örnekler, IoT cihazlarını ele geçirerek büyük ölçekli saldırılar yapabilmektedir.

2.1.5 Hizmet Engelleme Saldırıları

Hizmet engelleme saldırıları ya da bilinen adıyla Denial of Service Attack (DoS) bir hizmeti meşru kullanıcılar için erişilmez hale getirmek amacıyla gerçekleştirilen saldırılardır.

IoT cihazlarına yönelik güvenlik tehditleri, donanım, ağ ve uygulama katmanlarındaki çeşitli zayıflıklarla ilişkilendirilebilir. Örneğin, ağ katmanında çalışan açık portlar ve iletişim protokolleri üzerindeki güvenlik açıkları IoT cihazlarını siber saldırılara karşı savunmasız hale getirerek risk oluşturur. Uygulama katmanındaki zayıf kimlik doğrulama mekanizmaları kimlik avı, fidye yazılımı veya kişisel bilgi hırsızlığı gibi çeşitli siber suçlar için potansiyel bir fırsat yaratır. Bu tehditler, IoT ekosisteminin güvenliği için kapsamlı bir yaklaşımın benimsenmesini ve hem donanım hem de yazılım düzeyinde güvenlik önlemlerinin uygulanmasını gerektirir. Aşağıdaki figürde IoT ağlarına yönelik başlıca tehditler ve etki düzeyleri görselleştirilmiştir. Siyah, kırmızı ve sarı işaretler sırasıyla kritik, yüksek ve orta etki düzeylerini belirtmektedir.



Şekil 2. IoT tehditleri ve etki düzeyleri

3 Nesnelerin interneti güvenliğinde yapay zekanın rolü

Yapay zekadaki son gelişmeler, birçok sektörde inovasyonun ve otomasyonun gelişmesini etkilemiştir. Siber güvenlik de bu durumdan istisna değildir. Makine ve derin öğrenme, doğal dil işleme, bilgi, tahmin ve veri analizi gibi yapay zeka teknikleri, geleneksel saldırılara karşı savunmaları güçlendirmek için bir araç olarak kullanılmaktadır [3]. Nesnelerin İnterneti, daha fazla bağlı cihazı içerecek şekilde genişledikçe, hassas verilerin güvenliğini ve gizliliğini korumak daha da

zorlaşmaktadır. Bu bağlamda, yapay zeka, Nesnelerin İnterneti cihazlarının güvenliğini artırmak için güçlü bir araç haline gelmiştir. IoT cihazları, yukarıda da bahsedildiği gibi, çeşitli siber güvenlik tehditlerine karşı savunmasızdır. Bu tehditlerle başa çıkabilmek için, AI yaklaşımlarının IoT güvenlik çerçevelerine dahil edilmesi, değişen saldırılara gerçek zamanlı tepkileri, proaktif tehdit tespitini ve önlemeyi iyileştirmiştir. Yapay zeka, IoT cihazlarına yönelik bilinen saldırı vektörlerini analiz eder ve bu tür saldırıları tespit etmek için modeller oluşturur. AI tabanlı sistemler, IoT cihazlarını gerçek zamanlı olarak izleyerek, kötü amaçlı yazılım faaliyetlerini hızlı bir şekilde tespit eder ve müdahale eder.

Yapay zeka, özellikle izinsiz giriş tespiti alanında siber güvenlikte paha biçilmez bir varlık haline gelmiştir [4].

Makine öğrenimi teknikleri, IoT cihazları, ağlar ve insan etkileşimleri tarafından üretilen büyük miktarda veriyi analiz edebilir. Karar ağaçları, en yakın komşu algoritması (KNN), destek vektör makineleri (SVM) ve yapay sinir ağları (ANN) gibi yapay zeka algoritmaları, Trafik kalıplarını değerlendirerek ve şüpheli faaliyetleri belirleyerek, siber güvenlik sistemlerinin IoT ortamlarını koruma yeteneklerini artırır. Örneğin, bir IoT cihazının normal çalışma sırasında gönderdiği veri miktarını öğrenerek, bu miktarın dışında gerçekleşen faaliyetleri anomali olarak işaretleyebilir.

Anomali tespiti, kötü amaçlı yazılım tespiti, kimlik doğrulama, otomatik yanıt ve veri gizliliği gibi alanlarda Yapay Zeka, IoT cihazlarının güvenliğini önemli ölçüde artırabilir. Öte yandan, Yapay zekanın IoT siber güvenliğindeki ilerlemeleri, yeni zorlukları da beraberinde getirmektedir. Yapay zeka geliştikçe, siber suçluların kullandığı yöntemler de gelişmektedir. Adversarial AI (düşman yapay zeka), güvenlik önlemlerini atlatmak için AI algoritmalarını kullanan saldırganların yarattığı büyüyen tehlikeye işaret eder. Bu nedenle, gelişen tehditlerin önünde kalabilmek için AI tabanlı siber güvenlik çözümleri üzerine sürekli araştırma yapılması gereklidir. Bu, Yapay Zeka'nın hem saldırı hem de savunma alanlarında kritik bir rol oynadığını gösterir.

4 Literatür araştırması

Mevcut literatürde IoT alanında yapılmış çoğu çalışma, IoT ağlarında güvenliği sağlamak için gerçekleştirilmiş ve IoT teknolojilerindeki güvenlik açıklarını belirleyip, bu açıkları azaltmak için çözümler önermiştir. Örneğin, Reza ve Binod [5], IoT sistemlerindeki güvenlik açıklarını ve bu açıkların hassas veriler için oluşturduğu potansiyel riskleri vurguladılar. Ayrıca güvenlik önlemlerinin uygulanmasının ve iletişim kanallarının bütünlüğünün korunmasının önemini belirttiler.

Kumari ve Sharma [6], IoT ağlarında port tarama saldırılarını tespit etmek için yapay zeka destekli tehdit tespit teknikleri önerdi.

Yusuf ve diğerleri [7], IoT sistemlerinin güvenliğini sağlamak için makine öğrenimi tabanlı çözümler önererek veri kümelerinin standartlaştırılmasının ve makine öğreniminin siber saldırılara karşı etkili olma potansiyelini vurguladı.

Zhang ve diğerleri ise [8] EdgeAI destekli yaklaşımlar kullanarak IoT cihazlarındaki gizli saldırgan davranışlarını tespit etmeyi önerdi.

Vasileios ve Kontas [9], yapay zeka destekli hibrit honeypot ağlarını kullanarak potansiyel botnet varlığını tahmin etmeyi ve bu tür saldırıları tespit etmeyi önerdi.

Moustafa ve diğerleri [10], IoT güvenliğinde yapay zeka destekli anomali tespitinin olası tehditleri belirlemek için etkili olduğunu, derin öğrenme kullanarak gösterdi.

Markus ve diğerleri [11], IoT Sentinel isimli bir sistem önerdiler. IoT Sentinel'in, riskli cihazları otomatik olarak tanımladığını ve diğer cihazları korumak için bu cihazlardan kaynaklanan tehditlere karşı uygun trafik filtreleme kurallarını uyguladığını belirtti.

Amit ve diğerleri [12], yapay zeka ve blockchain teknolojilerinin IoT güvenliği ve gizlilik koruması için entegrasyonunu tartışarak, bu teknolojilerin potansiyelleri hakkında içgörüler sundu.

Olne ve Viyecheslav ise [13], yapay zeka tabanlı tehditlerin/saldırıların tespiti, sınıflandırılması ve analizi üzerine odaklandı. Güvenlik sistemlerinin yeni tehdit türlerine uyum sağlayacak şekilde geliştirilmesinin gerekmekte olduğunu vurguladı.

Miles ve diğerleri [14], yapay zekanın kötü niyetli kullanımına ilişkin bazı varsayımsal senaryolar kullanarak fiziksel, dijital ve politik güvenlik alanlarında uyarılarda bulundu.

Benzer şekilde, bu çalışmada da yapay zekanın IoT güvenliğinde nasıl hem bir tehdit hem de bir savunma aracı olarak kullanılabileceğini ele aldık. Çoğu çalışma, yapay zekanın güvenlik savunma mekanizmalarındaki rolünü incelerken, bu çalışma yapay zekanın saldırganların lehine de

kullanılabileceğini vurgulamakta ve farkındalık oluşturmayı amaçlamaktadır. Yapay zekanın kötü niyetli kullanımlarına dair senaryoları ve bu tür saldırılara karşı alınabilecek karşı önlemleri detaylı olarak analiz etmektedir. Bu perspektif, AI ve IoT güvenliği literatürüne yeni bir bakış açısı kazandırmaktadır.

5 Yapay zekanın kötüye kullanımı

Yapay zekanın sunduğu birçok fayda ve güvenlik çözümlerine rağmen bu teknolojiler yalnızca savunma amaçlı kullanılmamaktadır; siber suçlular da bu teknolojileri saldırılarını güçlendirmek için kullanmaktadır. Düşman yapay zeka (Adversarial AI), siber saldırıları daha etkili hale getirmek için kötü niyetli aktörler tarafından benimsenmeye başlamıştır. Bu teknik, özellikle IoT cihazlarında izinsiz giriş tespit algoritmalarını engellemek veya yapay zekayı kendi sistemleri için çalışacak şekilde manipüle etmek amacıyla gerçekleştirilmektedir. Adversarial AI saldırısının temel fikri oldukça basittir. Bir saldırgan, bir veri kümesinde insan gözüyle algılanamayacak şekilde küçük değişiklikler yaparak, yapay zeka sisteminin çıktısında büyük değişiklikler meydana getirebilir. Adversarial AI, makine öğrenimi modellerinin kendisine sunulan veri girdilerini yanlış yorumlamasına neden olur. Sonuç olarak, modelin saldırganın lehine davranmasını sağlar.

Beklenmedik davranışlar üretmek için, saldırganlar "düşman örnekler" yaratır. Bu örnekler genellikle normal girdilere benzer, ancak modelin performansını bozacak şekilde titizlikle optimize edilmiştir. Saldırganlar genellikle bu düşman örnekleri, bir yapay zeka sisteminin veri girdilerine tekrar tekrar küçük değişiklikler yapabilen modeller geliştirerek oluştururlar. Bu saldırılar genellikle "zehirleme saldırıları" olarak bilinir [15].

Zehirleme saldırılarının önemli sonuçlara yol açabileceği iyi bir örnek, görüntü sınıflandırma sistemleridir. Bir saldırgan, eğitimli bir sınıflandırıcının sonuçlarını tamamen değiştiren rastgele gürültüleri giriş görüntü veri kümelerine ekleyebilir. Daha kötü bir senaryoda, saldırganlar otonom araçları hedef alarak, araçların 'dur' işaretlerini başka bir trafik işareti olarak algılamasını sağlamak amacıyla yanıltıcı etiketler kullanabilir [15].

5.1 Saldırganların Güç Kazandığı Noktalar ve AI Destekli Saldırılar

AI ve IoT'nin birleşmesi, IoT cihazlarının akıllıca çalışmasını ve verilerine ve deneyimlerine dayalı kararlar almasını sağlar [16]. Saldırganlar da bu ilerlemelerden yararlanarak IoT cihazları ve ağlarına sofistike saldırılar başlatmak için yapay zeka yeteneklerini kullanır [17]. Bu saldırılar, AI sistemlerini kontrol etmeyi ve davranışlarını kötü niyetli bir şekilde değiştirmeyi amaçlar.

5.1.1 Güvenlik açıklarının tespiti için otomasyon

Makine öğrenimi, bir sistemdeki güvenlik açıklarını keşfetmek için kullanılabilir. Bu, sistemi güvence altına almaya çalışanlar için, yamanması gereken güvenlik açıklarını akıllıca aramak adına faydalı olabilir. Ancak saldırganlar da bu teknolojiyi, hedef sistemlerindeki güvenlik açıklarını bulmak ve istismar etmek için kullanmaktadır. Teknolojinin, özellikle düşük güvenlik standartlarına sahip IoT cihazları gibi teknolojilerin, kullanımının artmasıyla, saldırganların istismar edebileceği güvenlik açıklarının sayısı da artmıştır; buna sıfır gün (zero-day) açıkları da dahildir. Saldırganlar, güvenlik açıklarını hızlı bir şekilde belirlemek amacıyla genellikle AI kullanır ve bu açıkları, geliştiricilerin düzeltmelerinden çok daha hızlı bir şekilde istismar ederler. Geliştiriciler de bu tespit araçlarını kullanabilir, ancak bir sistemi veya cihazı güvence altına almak söz konusu olduğunda dezavantajlı durumdadırlar; potansiyel olarak var olabilecek her bir güvenlik açığını bulup düzeltmek zorundadırlar, oysa saldırganların sadece bir tanesini bulmaları yeterlidir. Bu nedenle otomatik tespit, saldırganlar için değerli bir araçtır.

5.1.2 Girdi Saldırıları

Bir saldırgan, bir AI sisteminin girdisini, AI'nin arızalanmasına veya yanlış bir çıktı vermesine neden olacak şekilde değiştirdiğinde, buna girdi saldırısı denir. Girdi saldırıları, girişe bir saldırı deseni ekleyerek gerçekleştirilir. Dikkat çekici bir şekilde, girdi saldırısı gerçekleştirmek için AI algoritmasının veya güvenliğinin tehlikeye atılması gerekmez, yalnızca saldırganın çıktıyı bozmak istediği girdinin değiştirilmesi yeterlidir.

5.1.3 Veri zehirleme

Veri zehirleme saldırıları ve girdi saldırıları oldukça benzerdir, ancak girdi saldırılarının amacı yalnızca etkilenen girdinin çıktısını değiştirmekken, veri zehirlemenin amacı, yapay zekanın analiz ettiği verilerde uzun vadeli değişiklikler yaparak, yapay

zekanın temel olarak hatalı hale gelmesini sağlamaktır. Bu nedenle, veri zehirleme genellikle yapay zeka henüz eğitim aşamasındayken gerçekleştirilir. Birçok durumda, yapay zeka, saldırganın belirlediği spesifik girdilerde başarısız olacak şekilde eğitilir. Örneğin, bir askeri güç, yapay zeka kullanarak uçakları tespit ediyorsa, düşman askeri güç, yapay zekayı belirli uçak türlerini, örneğin insansız hava araçlarını tanımaması için zehirleyebilir. Veri zehirleme ayrıca, sürekli olarak öğrenen ve veri analiz eden yapay zekalar üzerinde de kullanılabilir [18]. Saldırganların yapay zekayı zehirlemek için kullanabileceği üç ana yöntem vardır.

5.1.3.1 Veri kümesi zehirleme

Bir yapay zekanın veri kümesini zehirlemek, veri zehirlemenin en doğrudan yöntemlerinden biridir. Yapay zeka, sağlanan eğitim veri kümelerinden öğrendiği için, bu veri kümelerindeki herhangi bir hata yapay zekanın bilgisini de hatalı hale getirir [18]. Örneğin, eğitim veri setinin önemli bir kısmının bozulmuş olması, sonuçta ortaya çıkan makine öğrenme modelinin hatalı çalışmasına neden olur. Veri kümesi zehirleme, hedef veri kümesine yanlış veya yanıltıcı bilgi ekleyerek gerçekleştirilir. Yapay zekalar, veri kümelerindeki desenleri tanıyarak öğrendiklerinden, zehirlenmiş veri kümeleri bu desenleri bozabilir veya yeni yanlış desenler oluşturabilir, bu da yapay zekanın girdileri yanlış tanımasına veya yanlış sınıflandırmasına yol açar [18]. Birçok veri kümesi çok büyük olduğundan, bu tür zehirlenmiş verileri tespit etmek zor olabilir. Örneğin, trafik desenlerini analiz eden bir yapay zekayı hedef alan bir saldırgan, veri kümesi etiketlerini değiştirerek yapay zekanın dur işaretlerini tanımamasına veya kırmızı ışığı yeşil ışık olarak sınıflandırmasına neden olabilir.

5.1.3.2 Algoritma zehirleme

Algoritma zehirleme saldırıları, yapay zekanın öğrenme algoritmasındaki zayıflıklardan faydalanır. Bu tür saldırılar, özellikle kullanıcıların veri gizliliğini koruyarak makine öğrenimini eğitme yöntemi olan federe öğrenme ile yaygınlaşır.

Federe öğrenme, kullanıcıların potansiyel olarak hassas verilerini tek bir veri kümesinde toplamak yerine, küçük modelleri doğrudan kullanıcıların cihazlarında eğitir ve ardından bu modelleri birleştirerek nihai modeli oluşturur [18]. Kullanıcıların verileri cihazlarından ayrılmadığı için daha güvenlidir; ancak, bir saldırgan bu algoritmanın veri aldığı kullanıcılardan biri olduğunda, kendi verilerini manipüle ederek modeli zehirleyebilir. Zehirlenmiş algoritma, diğer algoritmalarla birleştirildiğinde nihai modeli bozma veya içine bir arka kapı ekleme potansiyeline sahiptir [18].

Örneğin, IoT tabanlı akıllı ev sistemlerinde, çeşitli sensörlerden (ısı, nem, enerji tüketimi vb.) gelen veriler kullanılarak enerji verimliliğini optimize eden bir makine öğrenimi modeli oluşturulur. Federe öğrenme yöntemiyle, her sensör kendi verilerini yerel olarak işler ve yalnızca model güncellemelerini merkezi sunucuya gönderir, böylece kullanıcıların verileri güvende kalır. Ancak, bir saldırgan, kendi IoT cihazındaki verileri manipüle ederek merkezi modelin performansını bozabilir veya modele kötü amaçlı bir arka kapı ekleyebilir. Bu durum, federe öğrenme yönteminin sunduğu gizlilik avantajlarına rağmen güvenlik açıklarını ortaya çıkarır. Bu, algoritma zehirlemenin nispeten masum bir örneği olsa da, federe öğrenmenin IoT'de artmasıyla birlikte potansiyel zararlı uygulamaları da artacaktır.

5.1.3.3 Model zehirleme

Model zehirleme, yapay zekanın doğrudan kendisini hedef alan bir saldırı türüdür. Bu saldırıda, saldırgan önceden hazırlanmış kötü niyetli bir modeli, meşru bir model ile değiştirir. Saldırganın bu değişikliği yapabilmesi için modelin depolandığı sisteme erişim sağlaması yeterlidir [18]. Alternatif olarak, saldırgan eğitilmiş model dosyasındaki denklemleri ve verileri manipüle edebilir. Bu yöntem oldukça tehlikelidir çünkü modelin eğitimli olup olmadığının çift kontrol edilmesine ve verilerin zehirlenmemiş olduğunun doğrulanmasına rağmen, saldırgan modelin dağıtım sürecinin çeşitli noktalarında modeli hala değiştirebilir [18]. Örneğin, model bir IoT cihazına yerleştirilmek üzere şirket ağı içinde beklerken veya bireysel bir IoT cihazına dağıtıldıktan sonra saldırıya uğrayabilir [29].

Öte yandan, derin öğrenmedeki gelişmeler, saldırganların tanınmış politikacılar, CEO'lar, ünlüler ve diğer önemli kişilerin sahte ses veya videolarını oluşturmak için sentetik araçlar geliştirmelerine olanak tanımıştır. Bu araçlar, bireylerin seslerini veya videolarını başarılı bir şekilde taklit etmeyi öğrenir [20]. Gizli Markov modeli (HMM) tabanlı konuşma sentezleyiciler, konuşma tanıma modellerinden elde edilen standart model uyarlama tekniklerine dayanarak,

diğer konuşmacılardan elde edilen arka plan modellerini değiştirebilir ve yeni konuşma modelleri oluşturabilir [21]. Örneğin, bir AI botunun belirli bir mağduru hedef alacak şekilde programlandığını düşünelim. Bu bot, sosyal medya verilerini kullanarak mağdurun bir meslektaşını arayabilir ve meslektaşının sesini ses sentezi "deepfake" teknikleriyle taklit ederek mağduru kandırabilir [22].

Bilinen konuşma sentezi saldırılarından biri, İngiltere merkezli bir enerji şirketinin yönetim direktörünün, patronunun sesini taklit eden bir telefon aramasıyla dolandırılması olayıdır. Direktör, patronunun talimatı üzerine büyük bir miktar parayı bir Macar tedarikçi hesabına transfer etti. Ancak daha sonra paranın aslında bir Alman hesabına yönlendirildiğini fark etti [23].

Akıllı hoparlörler, örneğin Amazon Alexa ve Google Home, ve birçok IoT cihazı ses kontrollü sistemler olarak kabul edilir ve bu nedenle ses sahteciliği veya klonlama saldırılarına karşı savunmasızdır. Özellikle COVID-19 pandemisinden sonra, bu tür cihazlara yönelik saldırılar artmıştır. Derin öğrenme algoritmaları, sentetik ses komutlarının oluşturulmasını kolaylaştırır [24].

Bu saldırılar, ses klonlama veya ses tekrar saldırıları şeklinde olabilir. Bir tekrar saldırısı, saldırganın güvenli bir ağ iletişimini dinleyip, mesajları keserek ve yeniden oynatarak alıcıyı yanıltması veya geciktirmesi durumunda meydana gelir [25]. Bu tür saldırılar, ağdaki cihazların normal çalışma düzenlerini bozarak, istenmeyen işlemler gerçekleştirmelerine veya sonuçların saldırganın lehine yönlendirilmesine neden olabilir.

6 Sonuç

Nesnelerin İnterneti güvenliğinde yapay zekanın rolünü ve bu teknolojinin sağladığı fırsatlar ile yarattığı riskleri kapsamlı bir şekilde ele alan bu makalede, IoT cihazlarının hızlı yayılımının hayatı kolaylaştıran pek çok faydayı beraberinde getirdiği, ancak ciddi güvenlik tehditlerini de artırdığı vurgulanmaktadır. 2023 yılı itibarıyla dünya genelinde 15 milyardan fazla IoT cihazı bulunmakta ve bu sayının 2030 yılına kadar 30 milyara ulaşması beklenmektedir. Geleneksel güvenlik yöntemleri, IoT cihazlarının sınırlı işlemci hızı, bellek boyutu ve enerji kaynakları nedeniyle yetersiz kalmakta, bu da yenilikçi güvenlik yaklaşımlarını zorunlu kılmaktadır. Yapay zeka, büyük veri setlerini analiz etme, kalıpları tanıma ve güvenlik tehditlerini proaktif olarak tespit etme yeteneği sayesinde IoT güvenliğinde önemli bir potansiyele sahiptir. Yapay zeka tabanlı çözümler, IoT güvenlik çerçevelerine entegre edilerek, değişen saldırılara karşı gerçek zamanlı tepkileri, anomali tespitini ve tehdit azaltmayı iyileştirmektedir.

Yapay zeka, yalnızca savunma için değil, saldırganlar tarafından da güvenlik açıklarını tespit etmek ve istismar etmek amacıyla kullanılmaktadır. Adversarial AI teknikleri, yapay zeka sistemlerini yanıltmak veya bozmak için kullanılır ve bu teknikler arasında veri zehirleme, girdi saldırıları ve model manipülasyonu yer almaktadır. Saldırganlar, yapay zekayı kullanarak IoT sistemlerinde güvenlik zafiyetlerini daha etkili bir şekilde tespit edebilir ve bu zafiyetlerden yararlanabilirler. Bu durum, AI'nın IoT güvenliğinde hem bir savunma aracı hem de bir saldırı aracı olarak çift yönlü bir rol oynadığını göstermektedir.

Makale, AI tabanlı siber güvenlik çözümleri üzerinde sürekli araştırma ve geliştirme çalışmaları yapılması gerektiğini vurgulamakta ve bu çözümlerin gelişen tehditlere karşı daha dayanıklı hale getirilmesi gerektiğini belirtmektedir. IoT cihazlarının güvenliğini artırmak için hem donanım hem de yazılım düzeyinde güvenlik önlemleri alınmalı ve AI algoritmalarının güvenilirliğini artırmak ile adversarial saldırılara karşı dirençli hale getirmek için yeni teknikler geliştirilmelidir. Sonuç olarak, bu makale, yapay zekanın IoT güvenliğinde sağladığı fırsatlar ve yarattığı riskler arasındaki dengeyi incelemekte ve bu alandaki güvenlik stratejilerine katkıda bulunmayı amaçlamaktadır. AI'nın hem savunma hem de saldırı tekniklerinde nasıl kullanıldığını anlamak, IoT ekosisteminin güvenliğini sağlamak için kritik öneme sahiptir.

Gelecekteki çalışmalarda AI ve IoT güvenliği alanında kapsamlı bir test ve değerlendirme çerçevesi geliştirerek, bu teknolojilerin güvenilirliğini ve etkinliğini artırmayı amaçlıyoruz. Adversarial AI'ya karşı dirençli algoritmaların geliştirilmesi, IoT güvenliğinde devrim niteliğinde bir adım olacaktır. Yapay zekanın IoT güvenliğinde daha etkili bir şekilde kullanılabilmesi için multidisipliner iş birliği ve sürekli yenilik şarttır.

Kaynaklar

[1] Statista, "Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030 (in billions)."
https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/}. [Accessed: June 7, 2024].

[2] K. Doppler, "M2M Communications and the Internet of Things," in \textit{IEEE Wireless Communications and Networking Conference (WCNC)}, IEEE, 2017. Available: \url{https://wcnc2017.ieee-wcnc.org/workshop/m2m-communications-and-internet-things.html}.

[3] Sarker, I.H., Furhad, M.H. & Nowrozy, R. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. SN COMPUT. SCI. 2, 173 (2021). https://doi.org/10.1007/s42979-021-00557-0

[4] DevikrishnaK, S. "An Artificial Neural Network based Intrusion Detection System and Classification of Attacks." (2013).

[5] Hosenkhan, Reza & Pattanayak, Binod. (2020). Security Issues in Internet of Things (IoT): A Comprehensive Review. 10.1007/978-981-13-9330-3_36.

[6] Kumari and I. Sharma, "Securing the Internet of Things using AI-Enabled Detection of Attacks via Port Scans in IoT Networks", 2023 International Conference on Power, Energy, Environment Intelligent Control (PEEIC), 2023.

[7] Alkali, Yusuf & Routray, Indira & Whig, Pawan. (2022). Study of various methods for reliable, efficient and Secured IoT using Artificial Intelligence. SSRN Electronic Journal. 10.2139/ssrn.4020364.

[8] J. Zhang et al., "AntiConcealer: Reliable Detection of Adversary Concealed Behaviors in EdgeAI-Assisted IoT," in IEEE Internet of Things Journal, vol. 9, no. 22, pp. 22184-22193, 15 Nov.15, 2022, doi: 10.1109/JIOT.2021.3103138.

[9] V. A. Memos and K. E. Psannis, "AI-Powered Honeypots for Enhanced IoT Botnet Detection," 2020 3rd World Symposium on Communication Engineering (WSCE), Thessaloniki, Greece, 2020, pp. 64-68, doi: 10.1109/WSCE51339.2020.9275581.

[10] N. Moustafa, N. Koroniotis, M. Keshk, A. Y. Zomaya and Z. Tari, "Explainable Intrusion Detection for Cyber Defences in the Internet of Things: Opportunities and Solutions," in IEEE Communications Surveys & Tutorials, vol. 25, no. 3, pp. 1775-1807, thirdquarter 2023, doi: 10.1109/COMST.2023.3280465.

[11] M. Miettinen et al., "IoT Sentinel Demo: Automated Device-Type Identification for Security Enforcement in IoT," 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 2017, pp. 2511-2514, doi: 10.1109/ICDCS.2017.284.

[12] Tyagi, A.K.; Dananjayan, S.; Agarwal, D.; Thariq Ahmed, H.F. Blockchain—Internet of Things Applications: Opportunities and Challenges for Industry 4.0 and Society 5.0. Sensors 2023, 23, 947. https://doi.org/10.3390/s23020947.

[13] O. Veprytska and V. Kharchenko, "AI powered attacks against AI powered protection: classification, scenarios and risk analysis," 2022 12th International Conference on Dependable Systems, Services and Technologies (DESSERT), Athens, Greece, 2022, pp. 1-7, doi: 10.1109/DESSERT58054.2022.10018770.

[14] Miles Brundage, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe, Paul Scharre, Thomas Zeitzoff, Bobby Filar, et al. 2018. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv preprint arXiv:1802.07228 (2018).

[15] "Adversarial AI," DSEI, June 8, 2024, https://www.dsei.co.uk/news/adversarial-ai.

[16] Vinugayathri, "AI and IoT Blended- What It Is and Why It Matters?," www.clariontech.com. https://www.clariontech.com/blog/ai-and-iot-blended-what-it-isand-why-it-matters.

[17] A. Pandse, "Transforming cybersecurity with AI and ML: View - ET CISO," ETCISO.in, Feb. 11, 2019. https://ciso.economictimes.indiatimes.com/news/transforming-cybersecurity-with-ai-and-ml/67899197 (accessed Dec. 04, 2023).

[18] Comiter M. Attacking artificial intelligence. Belfer Center for Science and International Affairs, Belfer Center for Science and International Affairs. http://www.belfercenter.org/sites/default/files/2019-08/AttackingAI/AttackingAI.pdf.

[19] Kuzlu, M., Fair, C. & Guler, O. Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. Discov Internet Things 1, 7 (2021). https://doi.org/10.1007/s43926-020-00001-4.

[20] AlBadawy, Ehab A. et al. "Detecting AI-Synthesized Speech Using Bispectral Analysis." CVPR Workshops (2019).

[21] M. Sahidullah et al., "Introduction to Voice Presentation Attack Detection and Recent Advances," Jan. 2019, [Online] Available: http://arxiv.org/abs/1901.01085.

[22] Y. Mirsky et al., "The Threat of Offensive AI to Organizations," Jun. 2021, [Online]. Available: http://arxiv.org/abs/2106.15764.

[23] Alakeel F, Alfallaj R, HA, Almousa A. AI-based Cybersecurity Attacks and Countermeasures in IoT Environment: A Survey. JE&AS. 2023; 10(2): 61-89. doi:10.5455/jeas.2023110105.

[24] A. Javed, K. M. Malik, A. Irtaza, and H. Malik, "Towards protecting cyber-physical and IoT systems from singleand multi-order voice spoofng attacks," Applied Acoustics, vol. 183, Dec. 2021.

[25] G. Sharma, S. Vidalis, N. Anand, C. Menon, and S. Kumar, "A survey on layer-wise security attacks in IoT: Attacks, countermeasures, and open-issues," Electronics (Switzerland), vol. 10, no. 19. MDPI, Oct. 01, 2021.

Makine ve derin öğrenme teknikleriyle IoT ağları üzerinde saldırı tespiti: LightGBM, XGBoost, Stacking ve Self-Attention modellerinin performans analizi

Behice BAKIR[1]*, Zeynep GÜRKAŞ AYDIN[1], Ebu Yusuf GÜVEN[1], Muhammed Ali AYDIN[1]

[1]*İstanbul Üniversitesi-Cerrahpaşa, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, İstanbul, TÜRKİYE*

Özet

IoT ağları, siber güvenlik tehditlerine karşı savunmasız olmaları nedeniyle güvenilir ve etkili Saldırı Tespit Sistemleri (IDS) geliştirilmesini gerektirmektedir. Bu çalışma, IoTID20 veri seti kullanılarak, çeşitli makine öğrenimi ve derin öğrenme yöntemleri ile IoT ağlarında saldırı tespiti yapmayı amaçlamaktadır. Araştırmada, LightGBM, XGBoost, Stacking Classifier ve Self-Attention Mechanism gibi yöntemler kullanılmış; Mutual Information Feature Selection (MIFS) ve Recursive Feature Elimination (RFE) gibi özellik seçimi teknikleri ile Synthetic Minority Over-sampling Technique (SMOTE) ile veri dengeleme işlemleri gerçekleştirilmiştir. Sonuçlar, LightGBM modelinin MIFS ve SMOTE ile birlikte kullanıldığında %96.58 doğruluk oranı ile en yüksek performansı gösterdiğini ortaya koymuştur. XGBoost ve Stacking Classifier da benzer şekilde yüksek doğruluk oranları elde etmiştir. Self-Attention Mechanism ile geliştirilen derin öğrenme modeli ise %92.06 doğruluk oranı ile diğer modellere göre daha düşük performans sergilemiştir. Bu sonuçlar, makine öğrenimi ve derin öğrenme tekniklerinin, özellikle doğru özellik seçimi ve veri dengeleme yöntemleri ile birleştirildiğinde, IoT ağlarında etkili bir saldırı tespit sistemi geliştirilmesinde büyük potansiyele sahip olduğunu göstermektedir. Bu çalışma, IoT ağlarının güvenliğini artırmak ve siber tehditlere karşı koruma sağlamak için etkili IDS çözümleri geliştirilmesine önemli katkılar sunmaktadır.

Anahtar Kelimeler: *Saldırı Tespit Sistemi, Makine Öğrenmesi,* IoTID20

Attack detection on IoT networks with machine and deep learning techniques: performance analysis of LightGBM, XGBoost, Stacking and Self-Attention models

Abstract

IoT networks are vulnerable to cybersecurity threats, necessitating the development of reliable and effective Intrusion Detection Systems (IDS). This study aims to detect attacks in IoT networks using various machine learning and deep learning methods with the IoTID20 dataset. In the research, techniques such as LightGBM, XGBoost, Stacking Classifier, and Self-Attention Mechanism were utilized; data balancing was performed using Mutual Information Feature Selection (MIFS) and Recursive Feature Elimination (RFE) techniques along with the Synthetic Minority Over-sampling Technique (SMOTE). The results revealed that the LightGBM model, when used in conjunction with MIFS and SMOTE, achieved the highest performance with an accuracy rate of 96.58%. XGBoost and Stacking Classifier also achieved similarly high accuracy rates. However, the deep learning model developed with the Self-Attention Mechanism showed a lower performance with an accuracy rate of 92.06% compared to the other models. These results demonstrate that machine learning and deep learning techniques, especially when combined with appropriate feature selection and data balancing methods, have great potential in developing effective IDS for IoT networks. This

*Contact email: behice.bakir@ogr.iuc.edu.tr

research makes significant contributions to enhancing the security of IoT networks and providing protection against cyber threats by developing effective IDS solutions.

Keywords: *Intrusion Detection, Machine Learning,* IoTID20

1 Giriş

Nesnelerin İnterneti (IoT) alanındaki hızlı gelişmeler, akıllı evler, sağlık, tarım ve endüstriyel otomasyon gibi çeşitli sektörlerde devrim yaratmıştır. Son araştırmalara göre, 2025 yılına kadar IoT cihazlarının sayısının 4,1 milyarı aşması beklenmektedir, bu da bu cihazların günlük yaşamda ne kadar yaygınlaştığını göstermektedir[1]. Ancak, bu geniş bağlantılılık, bu cihazları çeşitli siber saldırılara karşı savunmasız hale getirerek önemli güvenlik risklerine maruz bırakmaktadır. Bu saldırılar arasında Dağıtılmış Hizmet Reddi (DDoS) saldırıları, veri ihlalleri ve yetkisiz erişimler yer almaktadır. Bu güvenlik risklerini azaltmak için Saldırı Tespit Sistemleri (IDS) kritik bir rol oynamaktadır. IDS'ler, ağ trafiğini sürekli izleyerek şüpheli faaliyetleri tespit eder. Geleneksel IDS yöntemleri, genellikle imza tabanlı tespit üzerine kurulu olup, IoT ortamlarının dinamik ve değişken doğası için yetersiz kalmaktadır. Bu nedenle, IDS'nin tespit yeteneklerini artırmak için makine öğrenimi (ML) ve derin öğrenme (DL) tekniklerinin kullanılması giderek daha fazla ilgi görmektedir.

Son çalışmalar, IoT IDS için çeşitli ML ve DL yaklaşımlarını araştırmıştır. Örneğin, Derin Öğrenme tabanlı bir IDS, Konvolüsyonel Sinir Ağları (CNN) kullanarak IoT ağlarındaki saldırıları yüksek doğruluk ve kesinlikle tespit etmiştir[2]. Başka bir çalışma, ağ trafiği verileri ve IoT sensörlerinin telemetri verilerini birleştirerek, Transformer tabanlı bir model kullanarak yeni bir IDS çerçevesi önermiştir. Bu yaklaşım, saldırıların davranışlarını ve etkilerini etkili bir şekilde öğrenmiş ve ToN_IoT veri seti üzerinde son teknoloji performans elde etmiştir[7].

Özellik seçimi teknikleri de IDS'nin performansını artırmada önemli bir rol oynamaktadır. Bir çalışmada IoT botnet saldırılarını tespit etmek için CNN ve Tekrarlayan Sinir Ağları (RNN) entegre eden hibrit bir derin öğrenme modeli kullanmış ve geleneksel yöntemlere göre üstün performans sergilemiştir[4]. Bu gelişmeler, ML ve DL tekniklerinin etkili özellik seçimi ve veri dengeleme yöntemleri ile birleştirilmesinin, IoT ağları için sağlam IDS'lerin geliştirilmesinde büyük potansiyele sahip olduğunu göstermektedir. Bu tekniklerin entegrasyonu, IDS'nin doğruluk, kesinlik ve geri çağırma oranlarını önemli ölçüde artırarak, IoT ortamlarının dinamik ve heterojen doğasına daha iyi uyum sağlamalarını sağlar.

Bu bağlamda, çalışmamız, IoTID20 veri setini kullanarak IoT ağları için bir IDS geliştirmeyi amaçlamaktadır. LightGBM, XGBoost, Stacking Classifier ve Self-Attention Mechanism yöntemlerini, Mutual Information Feature Selection (MIFS) ve Recursive Feature Elimination (RFE) gibi özellik seçimi teknikleri ve veri dengeleme için Synthetic Minority Over-sampling Technique (SMOTE) ile birlikte kullanıyoruz. Bu modellerin performansını değerlendirerek, IoT ortamlarında saldırı tespiti için en etkili yaklaşımı belirlemeyi ve IoT ağlarını gelişen siber tehditlere karşı güvence altına alma çabalarına katkıda bulunmayı amaçlıyoruz.

2 İlgili Çalışmalar

Son yıllarda, Nesnelerin İnterneti (IoT) teknolojisinin hızlı gelişimi, siber güvenlik alanında birçok yeni araştırma yapılmasını sağlamıştır. IoT ağlarındaki güvenlik açıkları ve siber saldırılar, bu teknolojinin yaygınlaşmasıyla birlikte daha da önem kazanmıştır. Bu bağlamda, çeşitli saldırı tespit sistemleri geliştirilmiştir.

Al-Emari ve arkadaşları çalışmalarında, IoT ağlarında saldırı tespiti için Mutual Information Feature Selection (MIFS) ve Light Gradient-Boosting Machine (LightGBM) algoritmalarının birleşimini tanıtmışlardır. Bu çalışma, IoTID20 veri seti üzerinde test edilmiştir ve önerilen metodoloji, doğruluk ve F1-skorda üstün performans göstermiştir. Özellikle, 11 özellikli model en yüksek performansı sergilemiştir, bu da etkili özellik seçiminin model

performansını artırmada kritik olduğunu göstermektedir[5].

Bajpai ve arkadaşları çalışmalarında IoT ağları için gelişmiş bir saldırı tespit sistemi tasarlamakta ve Particle Swarm Optimization (PSO) ile Extreme Gradient Boosting (XGB) algoritmalarını kullanmaktadır. IoTID20 veri seti üzerinde yapılan testler, bu sistemin siber tehditleri etkili bir şekilde tespit ettiğini ve IoT ağlarının güvenliğini artırdığını göstermiştir. Özellikle PSO ve XGB'nin birlikte kullanılması, optimum özellik vektörlerinin seçilmesini sağlamış ve bu da model performansını artırmıştır[6].

Endüstriyel IoT Ağları için Kendi Kendine Dikkat Tabanlı Derin Konvolüsyonel Sinir Ağları ile Saldırı Tespiti başlıklı çalışma, IIoT ağlarında saldırı tespiti için self-attention mekanizmasına dayalı derin konvolüsyonel sinir ağları (CNN) kullanmaktadır. Bu yöntem, dengesiz veri setlerinde bile yüksek doğruluk ve düşük yanlış pozitif oranları göstermiştir. Dikkat mekanizmaları, önemli özelliklerin vurgulanmasında ve gereksiz bilgilerin filtrelenmesinde etkili olmuştur[15].

Hibrit Özellik Azaltma ve Veri Dengeleme Teknikleri ile IoT Ağları için Etkili Derin Öğrenme Tabanlı Saldırı Tespit Sistemi başlıklı çalışma, IoT ağlarında saldırı tespiti için derin öğrenme tabanlı bir sistem önermekte ve özellik azaltma ile veri dengeleme tekniklerini kullanmaktadır. Bu yöntem, veri setindeki dengesizlikleri gidermiş ve saldırı tespitinde yüksek doğruluk sağlamıştır[11].

Başka bir çalışmada, afet yönetim sistemlerinde IoT ve Makine Öğrenimi (ML) tabanlı BİT çözümlerinin entegrasyonu ele alınmıştır. Bu çalışma, hibrit bir derin sinir ağı modeli kullanarak IoT ağlarındaki saldırıları tespit etmektedir ve CICIDS2017 ile IoTID20 veri setleri üzerinde yüksek doğruluk oranları elde etmiştir[7].

Natarajan ve arkadaşları çalışmasında, IoT saldırı tespiti için makine öğrenimi modellerinin performansını artırmayı amaçlayan yeni bir özellik seçim yöntemini tanıtmaktadır. Bu yöntem, çeşitli makine öğrenimi modelleri kullanılarak test edilmiş ve performans artışı sağlamıştır[8].

Hammood ve arkadaşı çalışmasında, IoT saldırı tespit sistemleri için topluluk makine öğrenimi yaklaşımını önermektedir. Logistic regression, naive bayes, karar ağaçları, ekstra ağaçlar, rastgele ormanlar ve gradyan artışı algoritmalarını birleştiren bu yöntem, çeşitli veri setlerinde yüksek doğruluk oranları elde etmiştir[13].

Parfenov ve arkadaşlarının çalışması, IoT ağlarındaki anormal faaliyetleri tespit etmek için kullanılan makine öğrenimi modellerine yönelik saldırıların etkinliğini araştırmaktadır. Bu çalışma, veri sızıntısına dayalı saldırıların makine öğrenimi modellerinin doğruluğunu önemli ölçüde etkilediğini bulmuştur[10].

Elmahfoud ve arkadaşlarının çalışması da, IoT ağlarında saldırıları tahmin etmek ve tespit etmek için çeşitli makine öğrenimi algoritmalarının performansını analiz etmektedir. Bu çalışma, farklı veri setlerinde makine öğrenimi algoritmalarının performansını karşılaştırarak en etkili modelleri belirlemiştir[12].

Bu çalışmalar, IoT ağlarının güvenliğini sağlamak için çeşitli yöntemler ve algoritmalar önermektedir. Özellik seçimi ve optimizasyon teknikleri, saldırı tespit sistemlerinin doğruluk ve etkinliğini artırmada önemli bir rol oynamaktadır. Bu bağlamda, kendi çalışmamız da IoT ağlarında saldırı tespitini geliştirmek için benzer teknikler kullanmakta ve mevcut literatüre katkıda bulunmaktadır. Özellikle, makine öğrenimi ve derin öğrenme modellerinin entegrasyonu, siber tehditlerin etkili bir şekilde tespit edilmesi ve önlenmesi için büyük bir potansiyel sunmaktadır.

3 Veri Seti

Saldırı Tespit Sistemlerinin performansını belirleyebilmek için en zorlu aşama geçerli ve uygun veri kümelerinin elde edilmesidir veya bulunmasıdır. Bu çalışmada IEEE Veri Portundan toplanan ve Huy Kang Kim tarafından sunulan açık kaynaklı bir veri kümesi olan yeni IoT botnet veri kümesi yani

IoTID20 veri kümesi kullanıldı. IoTID20 veri kümesi halka açık birkaç IoT saldırı tespit veri kümesinden biridir[13]. IoTID20 veri seti, IoT ağlarında oluşan çeşitli trafik türlerini ve saldırılarını içeren kapsamlı bir veri setidir. Bu veri seti, çeşitli normal ve anormal trafik kayıtlarını içermekte olup, özellikle Saldırı Tespit Sistemleri geliştirme ve test etme amacıyla kullanılmaktadır. Veri seti, etiketli verilerden oluşur ve her bir kayıt, belirli bir saldırı türü veya normal trafik olarak sınıflandırılmıştır. IoTID20 veri seti, hem normal hem de anormal ağ trafiği kayıtlarını içerir. Anormal trafik, çeşitli saldırı türlerini temsil ederken, normal trafik, IoT ağlarındaki standart veri akışlarını temsil eder. Veri seti, çeşitli saldırı türlerini içerir. Bunlar arasında DDoS (Distributed Denial of Service), MitM (Man-in-the-Middle), port taraması, kimlik avı ve diğer siber saldırılar yer alır. Bu çeşitlilik, IDS modellerinin geniş bir yelpazede saldırı tespit yeteneklerini değerlendirmeye olanak tanır[10]. IoTID20 veri seti, her bir trafik kaydı için bir dizi özellik içerir. Bu özellikler arasında akış süresi, ileri ve geri paket sayıları, paket uzunlukları, bayt sayıları, paketler arasındaki zaman aralıkları ve diğer ağ trafiği metrikleri bulunur. Bu özellikler, ağ trafiğinin detaylı analizine olanak tanır ve saldırıların tespiti için gerekli bilgileri sağlar[8]

4 Yöntem

Bu çalışmada, IoTID20 veri seti kullanılarak IoT ağları üzerinde bir Saldırı Tespit Sistemi (IDS) geliştirilmiştir. IDS geliştirme sürecinde, LightGBM, XGBoost, Stacking Classifier ve Self-Attention Mechanism kullanılmıştır. Bu bölümde, kullanılan yöntemler ve teknikler ayrıntılı olarak açıklanacaktır. IoTID20 veri seti, IoT ağlarında oluşan çeşitli trafik türlerini ve saldırılarını içeren bir veri setidir. Bu veri seti, çeşitli normal ve anormal trafik kayıtlarını içermekte olup, IDS geliştirme sürecinde modelin eğitim ve test edilmesi için kullanılmaktadır. Veri seti, etiketli verilerden oluşur ve her bir kayıt, belirli bir saldırı türü veya normal trafik olarak sınıflandırılmıştır. IoTID20 veri seti, ağ trafiği analizlerinde yaygın olarak kullanılır ve saldırı tespiti araştırmalarında önemli bir kaynak olarak kabul edilir. Öncelikle veri seti, eksik değerler ve gürültülü verilerden arındırılarak temizlenmiştir. Ardından, veri setinin dengesizliğini gidermek için SMOTE (Synthetic Minority Over-sampling Technique) uygulanmıştır. Bu yöntem, azınlık sınıfındaki örneklerin sayısını artırarak veri setindeki sınıf dengesizliğini azaltmayı amaçlar. SMOTE, özellikle IoT veri setlerinde yaygın olarak kullanılır ve etkili sonuçlar verir[10].

Makine öğrenimi çalışmalarında özellik seçimi, modelin performansını artırmak ve hesaplama maliyetini azaltmak için önemli bir adımdır. Bu çalışmada, Mutual Information Feature Selection (MIFS) ve Recursive Feature Elimination (RFE) yöntemleri kullanılarak en bilgilendirici özellikler seçilmiştir. MIFS, özellikler arasındaki bağımsız bilgi miktarını ölçerek en önemli özellikleri belirlerken[9], RFE ise iteratif olarak özellikleri çıkararak model performansını optimize eder[8].

Model eğitimi ve değerlendirmesi için dört farklı yöntem kullanılmıştır: LightGBM, XGBoost, Stacking Classifier ve Self-Attention Mechanism.

LightGBM (Light Gradient Boosting Machine), hızlı ve hafif bir gradient boosting algoritmasıdır. Büyük veri setlerinde ve yüksek boyutlu verilerde etkili performans göstermesi ile bilinir. LightGBM, CPU ve GPU üzerinde yüksek verimlilikle çalışabilir ve büyük veri setlerinde hızlı eğitim süreleri sağlar[9]. Bu çalışmada, LightGBM modeli hiperparametre optimizasyonu ile eğitilmiş ve doğruluğu artırılmıştır. LightGBM, özellikle sınıflandırma ve regresyon görevlerinde yüksek performans göstermesiyle bilinir ve geniş bir uygulama yelpazesinde kullanılmaktadır.

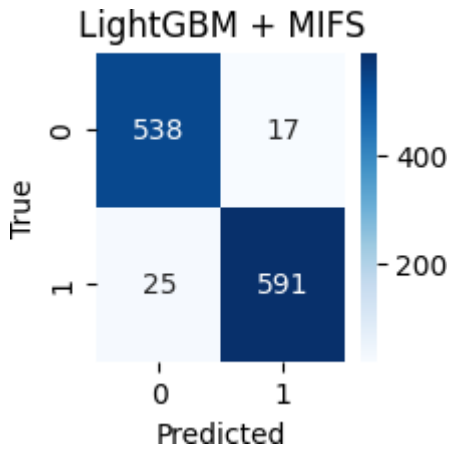
XGBoost (Extreme Gradient Boosting), optimize edilmiş bir gradient boosting algoritmasıdır. Genellikle yüksek doğruluk ve verimlilik sağlar. XGBoost, düzenli hale getirilmiş öğrenme süreci ve hızlı hesaplama yetenekleri ile bilinir. Ayrıca, overfitting'i azaltma ve genel model performansını artırma konularında etkilidir[11]. Bu çalışmada, XGBoost modelinin hiperparametreleri Grid Search kullanılarak optimize edilmiştir. XGBoost, çeşitli veri setlerinde üstün performans göstermiş ve özellikle büyük veri setlerinde etkili olmuştur.

Stacking Classifier, farklı makine öğrenimi modellerini birleştirerek genel performansı artırmayı hedefler. Bu yöntem, farklı modellerin güçlü yanlarından yararlanarak daha doğru tahminler yapmayı amaçlar. Stacking, genellikle birden fazla baz modelin (örneğin, Random Forest, Decision Tree) birleştirilmesi ve bu modellerin tahminlerinin bir meta-model (örneğin, Logistic Regression) ile birleştirilmesi ile gerçekleştirilir[13]. Bu çalışmada, Stacking Classifier kullanılarak farklı modellerin güçlü yanlarından yararlanılmış ve genel performans artırılmıştır. Stacking, çeşitli çalışmalarda yüksek doğruluk ve verimlilik sağlamış ve farklı veri setlerinde etkili olmuştur[14].

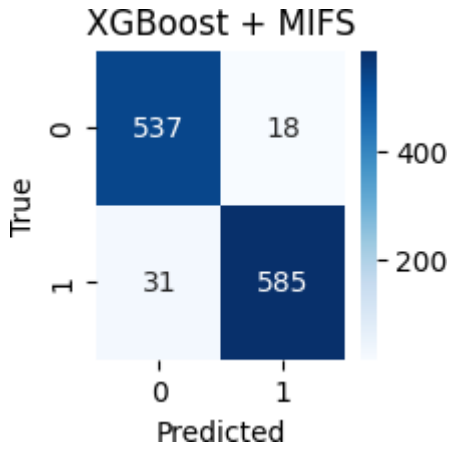
Self-Attention Mechanism, özellikle karmaşık veri yapıları ve zaman serisi verilerinde etkilidir. Bu mekanizma, modelin dikkatini önemli özelliklere yönlendirerek daha doğru tahminler yapmasını sağlar. Self-attention mekanizması, özellikle LSTM ve Transformer modellerinde yaygın olarak kullanılır ve bu modellerin doğruluğunu ve verimliliğini artırır[15]. Bu çalışmada, LSTM ve Attention katmanları kullanılarak bir derin öğrenme modeli oluşturulmuş ve eğitilmiştir. Derin öğrenme modelleri, özellikle büyük veri setlerinde ve karmaşık veri yapılarında yüksek performans göstermektedir[16].

5 Testler

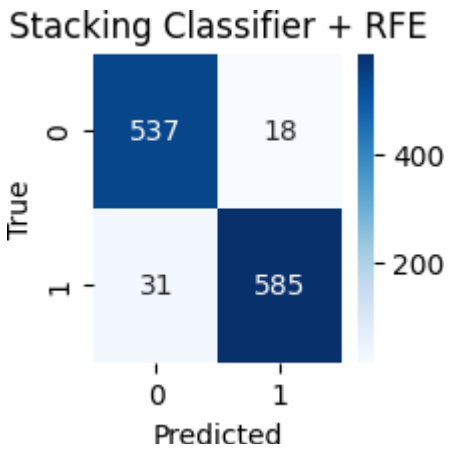
Bu çalışmada, IoTID20 veri seti kullanılarak IoT ağları üzerinde bir Saldırı Tespit Sistemi (IDS) geliştirilmiş ve LightGBM, XGBoost, Stacking Classifier ve Self-Attention Mechanism olmak üzere dört farklı makine öğrenimi ve derin öğrenme yöntemi kullanılarak değerlendirilmiştir. Özellik seçimi için Mutual Information Feature Selection (MIFS) ve Recursive Feature Elimination (RFE) yöntemleri uygulanmış, veri dengesizliğini gidermek amacıyla SMOTE (Synthetic Minority Over-sampling Technique) kullanılmıştır. LightGBM modeli, MIFS ve SMOTE teknikleriyle birlikte kullanıldığında %96.58 doğruluk oranı ile en yüksek performansı göstermiştir. Bu sonuç, LightGBM'in hızlı ve hafif yapısı sayesinde büyük veri setlerinde etkili olduğunu ortaya koymaktadır. XGBoost modeli, %96.07 doğruluk oranı ile ikinci sırada yer almış ve optimize edilmiş gradient boosting algoritması olarak yüksek doğruluk ve verimlilik sağlamıştır. Stacking Classifier, RFE ve SMOTE ile birlikte kullanıldığında da %96.07 doğruluk oranına ulaşmış, farklı modellerin güçlü yanlarını birleştirerek genel performansı artırmıştır. Self-Attention Mechanism ile geliştirilmiş derin öğrenme modeli ise, %92.06 doğruluk oranı ile diğer modellere göre daha düşük bir performans sergilemiş olmasına rağmen, karmaşık veri yapıları ve zaman serisi verilerinde etkili olmuştur. Bu sonuçlar, LightGBM'in IoT ağları üzerindeki saldırı tespiti için güçlü bir aday olduğunu ve XGBoost ile Stacking Classifier'ın da yüksek performans sunduğunu göstermektedir. Derin öğrenme modelinin performansı nispeten düşük olsa da, karmaşık veri yapılarındaki potansiyeli göz ardı edilmemelidir. Çalışma sonuçları aşağıdaki grafiklerde verilmiştir.



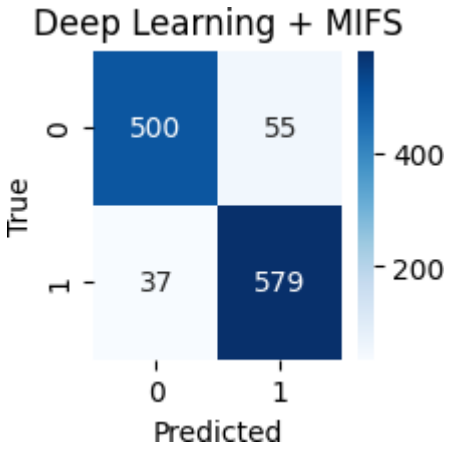
Şekil 1. LightGBM MIFS Confusion Matrisi



Şekil 2. XGBoost MIFS Confusion Matrisi



Şekil 3. Stacking Classifier RFE Confusion Matrisi



Şekil 4. Deep Learning MIFS Confusion Matrisi

Genel olarak, bu çalışma, farklı makine öğrenimi ve derin öğrenme yöntemlerinin IoT ağlarında saldırı tespiti için nasıl kullanılabileceğini ve hangi durumlarda daha etkili olabileceklerini ortaya koyarak, bu alandaki mevcut yaklaşımların etkinliğini göstermekte ve yeni yöntemlerin geliştirilmesine olanak tanımaktadır. Gelecekteki çalışmalar, daha büyük ve çeşitli veri setleri üzerinde bu tekniklerin daha fazla optimize edilmesi ve gerçek zamanlı uygulamalarda test edilmesi yönünde ilerleyebilir.

6 Sonuç

Bu çalışma, IoTID20 veri seti kullanılarak IoT ağları üzerinde bir Saldırı Tespit Sistemi (IDS) geliştirmiş ve dört farklı makine öğrenimi ve derin öğrenme yönteminin performansını değerlendirmiştir: LightGBM, XGBoost, Stacking Classifier ve Self-Attention Mechanism. Özellik seçimi için Mutual Information Feature Selection (MIFS) ve Recursive Feature Elimination (RFE) teknikleri uygulanmış, veri dengesizliğini gidermek için SMOTE (Synthetic Minority Over-sampling Technique) kullanılmıştır. LightGBM modeli, MIFS ve SMOTE teknikleriyle birlikte kullanıldığında en yüksek doğruluk oranı olan %96.58'i elde etmiş ve büyük veri setlerinde hızlı ve etkili performans göstermiştir. XGBoost modeli %96.07 doğruluk oranı ile yüksek doğruluk ve verimlilik sağlamış, Stacking Classifier da aynı doğruluk oranını yakalayarak farklı modellerin güçlü yanlarını birleştirme avantajını göstermiştir. Self-Attention Mechanism ile geliştirilen derin öğrenme modeli %92.06 doğruluk oranı ile diğer modellere göre daha düşük performans sergilemiş olsa da, karmaşık veri yapıları ve zaman serisi verilerinde önemli bir potansiyele sahiptir. Bu çalışma, farklı makine öğrenimi ve derin öğrenme yöntemlerinin IoT ağlarında saldırı tespiti için nasıl kullanılabileceğini ve hangi durumlarda daha etkili olabileceklerini ortaya koyarak, IoT güvenliği alanında önemli katkılar sunmaktadır. Gelecekteki çalışmalar, bu tekniklerin daha büyük ve çeşitli veri setleri üzerinde daha fazla optimize edilmesi ve gerçek zamanlı uygulamalarda test edilmesi yönünde ilerleyebilir. Bu araştırma, IoT ağlarında güvenlik ve saldırı tespiti için etkili yöntemlerin geliştirilmesine olanak tanımaktadır.

1. Kaynaklar

[1] Xu B, Sun L, Mao X, Ding R, Liu C. IoT Intrusion Detection System Based on Machine Learning. *Electronics*. 2023; 12(20):4289. https://doi.org/10.3390/electronics12204289

[2] Alosaimi, Shema & Almutairi, Saad. (2023). An Intrusion Detection System Using BoT-IoT. Applied Sciences. 13. 5427. 10.3390/app13095427.

[3] Wang, Minxiao & Yang, Ning & Weng, Ning. (2023). Securing a Smart Home with a Transformer-Based IoT Intrusion Detection System. Electronics. 12. 2100. 10.3390/electronics12092100.

[4] Alsoufi, Muaadh & Razak, Shukor & Siraj, Maheyzah & Ali, Abdulalem & Nasser, Maged & Abdo, Salah. (2021). Anomaly Intrusion Detection Systems in IoT Using Deep Learning Techniques: A Survey. 10.1007/978-3-030-70713-2_60.

[5] Al-Emari, Salam & Sanjalawe, Yousef & Alsmadi, Duha & Alduweib, Eman & Alharbi, Alyaa. (2024). Employing Mutual Information Feature Selection and LightGBM for Intrusion Detection in IoT. ICIC Express Letters. 18. 597-606. 10.24507/icicel.18.06.597.

[6] Bajpai, Soumya & Sharma, Kapil & Chaurasia, Brijesh. (2024). A Hybrid Meta-heuristics Algorithm: XGBoost-Based Approach for IDS in IoT. SN Computer Science. 5. 10.1007/s42979-024-02913-2.

[7] I. U. Khan, M. Y. Ayub, A. Abdollahi and A. Dutta, "A Hybrid Deep Learning Model-Based Intrusion Detection System for Emergency Planning Using IoT-Network," 2023 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM), Cosenza, Italy, 2023, pp. 1-5, doi: 10.1109/ICT-DM58371.2023.10286954.

[8] B. Natarajan, S. Bose, N. Maheswaran, G. Logeswari and T. Anitha, "A New High-Performance Feature Selection Method for Machine Learning-Based IOT Intrusion Detection," 2023 12th International Conference on Advanced Computing (ICoAC), Chennai, India, 2023, pp. 1-8, doi: 10.1109/ICoAC59537.2023.10249916.

[9] I. U. Khan, M. Y. Ayub, A. Abdollahi and A. Dutta, "A Hybrid Deep Learning Model-Based Intrusion Detection System for Emergency Planning Using IoT-Network," 2023 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM), Cosenza, Italy, 2023, pp. 1-5, doi: 10.1109/ICT-DM58371.2023.10286954.

[10] Parfenov, Denis & Grishina, Lubov & Zhigalov, Artur & Parfenov, Anton. (2024). Investigation of the impact effectiveness of adversarial data leakage attacks on the machine learning models. ITM Web of Conferences. 59. 10.1051/itmconf/20245904011.

[11] Karamollaoğlu, Hamdullah & Doğru, İbrahim & Yucedag, Ibrahim. (2024). An Efficient Deep Learningbased Intrusion Detection System for Internet of Things Networks with Hybrid Feature Reduction and Data Balancing Techniques. Information Technology and Control. 53. 243-261. 10.5755/j01.itc.53.1.34933.

[12] Ennaji Elmahfoud, Salah Elhajla, Yassine Maleh, Soufyane Mounir, Machine Learning Algorithms for Intrusion Detection in IoT Prediction and Performance Analysis, Procedia Computer Science, Volume 236, 2024, Pages 460-467, ISSN 1877-0509.

[13] Hammood, Baseem & Sadiq, Ahmed. (2023). ENSEMBLE MACHINE LEARNING APPROACH FOR IOT INTRUSION DETECTION SYSTEMS. Iraqi Journal for Computers and Informatics. 49. 93-99. 10.25195/ijci.v49i2.458..

[14] Qingmei Zhang, Peishun Liu, Xue Wang, Yaqun Zhang, Yu Han, Bin Yu, StackPDB: Predicting DNA- binding proteins based on XGB-RFE feature optimization and stacked ensemble classifier, Applied Soft Computing, Volume 99, 2021, 106921, ISSN 1568-4946.

[15] Alshehri, Mohammed & Saidani, Oumaima & Alrayes, Fatma & Abbasi, Saadullah & Ahmad, Jawad. (2024). A Self-Attention-Based Deep Convolutional Neural Networks for IIoT Networks Intrusion Detection. IEEE Access. PP. 1-1. 10.1109/ACCESS.2024.3380816.

[16] Zegarra Rodríguez D, Daniel Okey O, Maidin SS, Umoren Udo E, Kleinschmidt JH. Attentive transformer deep learning algorithm for intrusion detection on IoT systems using automatic Xplainable feature selection. PLoS One. 2023 Oct 16;18(10):e0286652. doi: 10.1371/journal.pone.0286652. PMID: 37844095; PMCID: PMC10578588.

Coverless Image Steganography: A Comparative Study

Ali Erdem Altınbaş[1]*, Yıldıray Yalman[2]

[1]*Kocaeli University, Faculty of Engineering, Electronics and Communication Engineering, Kocaeli, TURKIYE*
[2]*Piri Reis University, Faculty of Engineering, Computer Engineering, Istanbul, TURKIYE*

Abstract

This paper offers a comparative study of coverless image steganography, a technique that improves the security of digital communications without modifying the cover image. The study focuses on both mapping-based and generation-based methods. It analyzes their methodologies, robustness, capacity, and computational complexities. The first part of the study presents the basics of undisclosed steganography. The second section compares recent work in the field. The third section performs a Big-O complexity analysis to explore the competition between these approaches and predicts their future applications. The final results suggest that, with advances in deep learning, generation-based methods may become more common in high-security steganography. This study contributes to the growing body of literature on the topic of coverless image steganography, while also pointing to the potential for further developments in this field of study.

Keywords: *coverless steganograph, coverless image steganography, data hiding*

1 Introduction

In recent years, the security of digital communication, particularly the protection of confidential information, has become a significant concern. In this context, steganography is an important method for hiding confidential information in an undetectable way [1]. While traditional steganographic methods embed secret messages in a carrier (e.g., an image), their fundamental vulnerability is that they can be susceptible to steganalysis attacks due to the statistical alterations that occur in the carrier[2]. In light of these limitations, recent years have seen a focus on coverless image steganography (CIS), which offers greater resistance to steganalysis techniques and does not rely on a closed carrier [3].

Typically, coverless image steganography relies on matching secret information directly to the features of an image, thereby enabling secret communication without any addition or subtraction. This method is viewed as more secure than traditional steganography techniques because it is highly challenging for steganalysis tools to detect the secret information, given that no modifications are made to the carrier image [4].

The present paper reviews recent research in the field of coverless image steganography and analyzes the methodologies developed in this area. In particular, classical methods such as Scale-Invariant Feature Transform (SIFT) and Discrete Cosine Transform (DCT), as well as methods developed using modern deep learning techniques such as DenseUNet, and Generative Adversarial Networks (GANs) were analyzed. In an overall sense, these methods are designed to enhance robustness against both geometric and non-geometric attacks.

While the concept of coverless image steganography was first introduced by Zhou et al. in 2015, numerous innovative contributions have been made to the literature in recent years [5]. Figure 1 presents a chronological list of recent publications that have made a significant contribution to the body of knowledge in this field.

*Contact email: alierdemaltinbas@gmail.com

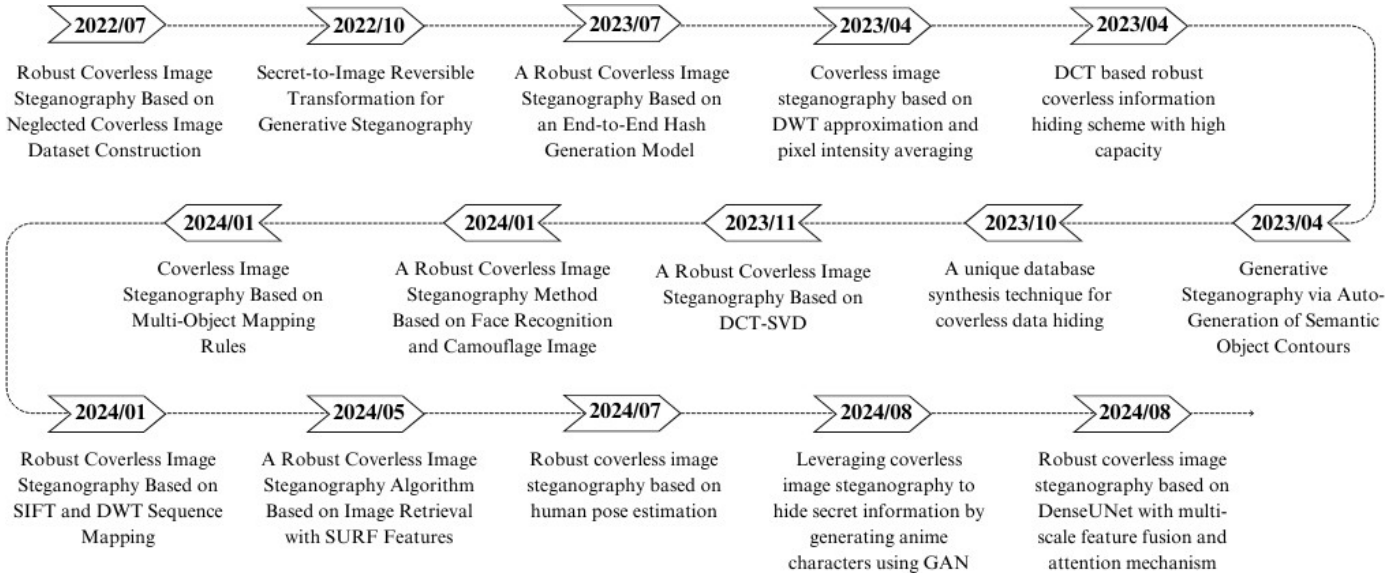


Figure 1. Coverless image steganography studies in recent years

2 Coverless Image Steganography in the Literature

The technique of coverless steganography, also known as steganography without embedding, has seen significant development over the past five years. This does not indicate that the cover is not utilized; rather, it suggests that the cover is not modified [6]. Indeed, it formulates a mapping relationship between data to be hidden and cover. As the cover remains without modification in coverless steganography, it can avoid identification by steganalysis algorithms at the fundamental level, which establishes coverless steganography as a more secure method for data hiding in comparison to "modification" steganography [7].

The development of coverless steganography may be traced to mapping-based methods, with research in this field centering on feature transformations. The work by *Jiao et. al.*, which was based on the combination of DCT and singular value decomposition (SVD), provided a powerful feature mapping using DCT and SVD [8]. This approach was further advanced by *Biswas et. al.*, which employed transformations such as DWT and pixel intensity averaging [9]. Then, *Lu et. al.*, concentrated on a more secure method of data hiding using face recognition and camouflage images [10]. *Tan et. al.*, presented an innovative approach in this field by developing a method that maps hidden messages by recognizing human body positions [11].

In the mapping-based work developed by *Zou. et al.*, the diversity and security of the coverless image dataset is increased, and a method that offers a wider range of applications is developed [12]. *Meng et. al.* developed a high-capacity and robust steganography method using an end-to-end hash generation model [13]. In their study, *Li et. al.* proposed a method based on matching secret messages with available images using SURF (Speeded-Up Robust Features). This approach represents a further advancement in secure data hiding techniques by mapping image features [14].

The integration of deep learning and neural network techniques is also a significant area of focus in the context of mapping-based methodologies. The DenseUNet-based method developed by *Li et. al.* [15] was found to enhance robustness against both geometric and non-geometric attacks through the utilisation of multi-scale feature combination and an attention mechanism. Similarly, *Chiu et al.* proposed a method that increases the range of features by mapping with a combination of SIFT and DWT [16]. The multi-object mapping rules developed by *Liang et al.* provided a flexible and comprehensive approach to steganography in this area [17].

The field of generation-based steganography has advanced considerably with the introduction of sophisticated techniques such as the hash generation model and GAN. The object contour generation approach developed by *Zhou et. al.* presented a methodological framework for

representing hidden messages by automatically generating semantic object contours [18]. *Rehman et al.* developed a methodology that generates anime characters using GAN and embeds hidden messages within these characters [19].

Kulkarni et. al. developed a high-capacity and robust steganographic method using a hash generation model [20]. Furthermore, *Majumder et al.* developed a unique database synthesis method to generate private images and provide a more reliable steganographic method [21]. *Zhou et. al.* developed a reversible method for transforming hidden messages into an image. This method employs a bidirectional transformation between a high-dimensional latent vector and the image domain, utilizing the Glow model. This approach enables the storage of hidden messages at high capacity and the accurate retrieval of the majority of the original information [22].

The techniques, brief descriptions, and most distinctive characteristics of the generation-based methods outlined in this chapter can be found in Table 1.

Table 1. Summary of the Generation-based Coverless Steganography Methods

Authors	Year	Technique	Brief Description	Distinctive Characteristics
Zhou et. al. [22]	2022	Reversible Image Conversion	The process of steganography utilises the transformation of hidden messages into images, which can subsequently be reversed.	The method has the capacity to achieve over 4 bpp hiding capacity and accurate information extraction while maintaining the desired anti-detectability and imperceptibility.
Meng et. al. [13]	2023	End-to-end Hash Generation	Hash strings representing secret messages are generated and utilized in the process of steganography.	It provides robust steganographic functionality with high data capacity.
Majumder et. al. [21]	2023	Database Generation	In order to create special images representing hidden messages, database synthesis is employed.	It is characterized by high accuracy and reliability, as well as the synthesis of a specialized database.
Zhou et. al. [18]	2023	Automatic Object Contour Generation	The generation of semantic object contours enables the production of images that represent hidden messages.	The automatic generation of object contours provides a high degree of accuracy and diversity.
Rehman et. al. [19]	2024	GAN (Generative Adversarial Network)	The generation of anime characters utilizing GAN allows for the generation of images that represent hidden messages.	The process of steganography is achieved through the creation of realistic and diverse anime characters.

Given the high costs and complexity of generation-based methods, there has been a notable increase in the use of mapping-based methods in recent years. For an overview of these methods, a summary is provided in Table 2.

Table 2. Summary of the Mapping-based Coverless Steganography Methods

Authors	Year	Technique	Brief Description	Distinctive Characteristics
Zou et. al. [12]	2023	Dataset Construction and Categorization	A coverless image dataset is created and used to increase the diversity and security of secret message mapping.	Increases dataset diversity and security, offering broader application areas.
Jiao et. al. [8]	2023	DCT and SVD	Secret messages are mapped using image features extracted via DCT and SVD.	Provides robust steganography through strong feature mapping methods.
Biswas et. al. [9]	2023	DWT and Pixel Intensity Averaging	Secret messages are mapped using DWT and pixel intensity averaging.	Provides high robustness with low-frequency components.

Kulkarni et. al. [20]	2023	DCT	Secret messages are mapped using DCT-based features, providing high capacity and robustness.	The method securely transmits data using DC coefficients and XOR, enhancing robustness and capacity.
Li et. al.[14]	2024	SURF	Secret messages are mapped to existing images using SURF features.	The method preprocesses images, creates sub-CIDs, maps hash sequences, embeds secret data, and retrieves images using SURF for secret extraction.
Lu et. al. [10]	2024	Face Recognition and Camouflage Images	Secret messages are mapped using face recognition algorithms and camouflage images.	High accuracy in extracting secret information without auxiliary data
Liang et. al. [17]	2024	Multi-Object Mapping Rules	Secret messages are mapped using multiple object recognition and mapping rules.	Offers extensive steganography with object recognition and flexible mapping rules.
Li et. al. [15]	2024	DenseUNet, Multi-Scale Feature Fusion, Attention Mechanism	Multi-scale features are extracted using DenseUNet and mapped to secret messages.	Resists both geometric and non-geometric attacks through multi-scale feature fusion and attention mechanisms.
Tan et. al. [11]	2024	Human Pose Estimation	Secret messages are mapped by recognizing human body poses in existing images.	Human pose estimation network to generate robust hash sequences from categorized pose points (facial and limb)
Chiu et. al. [16]	2024	SIFT and DWT	Double feature sequences are created using SIFT and DWT, and secret messages are mapped.	Offers high robustness and diversity with low-frequency components.

By addressing different issues related to coverless steganography, these studies have contributed to significant advances in data security and privacy.

3 Comparison of the Coverless Image Steganography Techniques

In coverless steganography, the main goal is to improve robustness and capacity. Computational cost is often considered secondary. To explore this, the study used Big-O complexity notation. This method evaluates the computational complexity of algorithms. As shown in Table 3, Big-O notation ranks computational methods in order from simple to complex [23]:

Table 3. Big-O Notations

Big-O	Description
O(1)	Constant time
O(log n)	Logarithmic
O(n)	Linear
O(n × logn)	Log-Linear
O($n^{!}$)	Quadratic
O($n^{"}$)	Polynomial
O(n!)	Factorial

In this context, the big-O complexity values of the analyzed studies are presented in Table 4.

Table 4. Big-O Notations

Paper Title	Dominant Operations	Big-O Complexity
A Robust Coverless Image Steganography Based on an End-to-End Hash Generation Model* [13]	Hash computation	O(n × log(n))
A Unique Database Synthesis Technique for Coverless Data Hiding* [21]	Database creation, data hiding	O(n × m)
Generative Steganography via Auto-Generation of Semantic Object Contours* [18]	Contour generation, object detection	O(n × log(n))
Secret-to-Image Reversible Transformation for Generative Steganography* [22]	GAN training, image generation	O(n × m)

Leveraging Coverless Image Steganography to Hide Secret Information by Generating Anime Characters Using GAN* [19]	GAN training, image synthesis	O(n × m)
DCT Based Robust Coverless Information Hiding Scheme with High Capacity [20]	DCT on 8x8 sub-blocks, XOR operation with secret message	O(n × log(m))
A Robust Coverless Image Steganography Algorithm Based on Image Retrieval with SURF Features [14]	Feature extraction, image comparison	O(n × log(n))
A Robust Coverless Image Steganography Based on DCT-SVD [8]	DCT and SVD computation	O($n^{\#}$)
A Robust Coverless Image Steganography Method Based on Face Recognition and Camouflage Image [10]	Face detection, image camouflage	O($n^{\$}$)
Robust Coverless Image Steganography Based on SIFT and DWT Sequence Mapping [16]	SIFT feature extraction, DWT sequence mapping	O(n × log(n))
Robust Coverless Image Steganography Based on DenseUNet with Multi-Scale Feature Fusion and Attention Mechanism [15]	DenseUNet feature extraction, hash sequence generation	O(n × log(m))
Robust Coverless Image Steganography Based on Human Pose Estimation [11]	Pose estimation, image matching	O($n^{\$}$)
Robust Coverless Image Steganography Based on Neglected Coverless Image Dataset Construction [12]	Clustering, feature extraction	O($n^{\$}$)
Coverless Image Steganography Based on DWT Approximation and Pixel Intensity Averaging [9]	DWT application, pixel intensity averaging	O(n × log(n))
Coverless Image Steganography Based on Multi-Object Mapping Rules [17]	Image sequence index construction using Faster RCNN	O(n × m)

**: generation-based coverless image steganography*

A preliminary examination of the data suggests that generation-based models may not be as computationally complex as initially assumed. However, this assessment does not account for the training costs in the context of big data and GAN applications. Consequently, it is probable that generation-based coverless image staganography methods will become more widely used in the coming years, if the training of GANs is accelerated and made more efficient.

4 Conclusion

This comparative study provides a comprehensive overview of recent advancements in coverless image steganography, with a focus on both mapping-based and generation-based techniques. The analysis demonstrates that while mapping-based methods have historically held a dominant position due to their lower computational complexity and robust feature extraction capabilities, generation-based methods are becoming increasingly competitive, particularly with the growth of deep learning and generative adversarial networks (GANs). These generation-based approaches, although potentially more resource-intensive, offer significant advantages in terms of security, capacity, and flexibility.

The study's Big-O complexity analysis indicates that numerous mapping-based methods are both efficient and well-suited for current applications. However, as GANs and other deep learning models continue to evolve, it is probable that the computational gap between these two categories will diminish. As training efficiency improves, generation-based methods may become the standard for high-security steganographic applications. In conclusion, this study highlights the importance of selecting an appropriate steganographic method based on the specific needs of the application, whether it be efficiency, robustness, or security. As the field progresses, the integration of deep learning into steganography is expected to play a key role in shaping future developments.

References

[1] T. Qin, B. Feng, B. Chen, Z. Peng, Z. Xia, and W. Lu, “Moiré pattern generation-based image steganography,” *Journal of Information Security and Applications*, vol. 82, May 2024, doi: 10.1016/j.jisa.2024.103753.

[2] D. R. I. M. Setiadi, S. Rustad, P. N. Andono, and G. F. Shidik, “Digital Image Steganography

Survey and Investigation (Goal, Assessment, Method, Development, and Dataset)," May 01, 2023, *Elsevier B.V.* doi: 10.1016/j.sigpro.2022.108908.

[3] B. Song, P. Wei, S. Wu, Y. Lin, and W. Zhou, "A survey on Deep-Learning-based image steganography," Nov. 15, 2024, *Elsevier Ltd*. doi: 10.1016/j.eswa.2024.124390.

[4] Y. Lin, P. Luo, Z. Zhang, J. Liu, and X. Yang, "AI-generated video steganography based on semantic segmentation," *IET Image Process*, 2024, doi: 10.1049/ipr2.13154.

[5] H. and H. R. and C. X. and S. X. Zhou Zhili and Sun, "Coverless Image Steganography Without Embedding," in *Cloud Computing and Security*, X. and L. J. and W. J. Huang Zhiqiu and Sun, Ed., Cham: Springer International Publishing, 2015, pp. 123–132.

[6] L. Meng, X. Jiang, and T. Sun, "A review of coverless steganography," Jan. 21, 2024, *Elsevier B.V.* doi: 10.1016/j.neucom.2023.126945.

[7] L. Meng, X. Jiang, Z. Zhang, Z. Li, and T. Sun, "A robust coverless video steganography based on maximum DC coefficients against video attacks," *Multimed Tools Appl*, vol. 83, no. 5, pp. 13427–13461, Feb. 2024, doi: 10.1007/s11042-023-15697-z.

[8] Y. Jiao, Z. Zhang, X. Yang, Y. Li, F. Mei, and Z. Li, "A Robust Coverless Image Steganography Based on DCT-SVD," in *2023 3rd International Conference on Computer Science and Blockchain, CCSB 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 59–63. doi: 10.1109/CCSB60789.2023.10398826.

[9] S. Biswas, S. Debnath, and R. K. Mohapatra, "Coverless image steganography based on DWT approximation and pixel intensity averaging," in *7th International Conference on Trends in Electronics and Informatics, ICOEI 2023 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 1554–1561. doi: 10.1109/ICOEI56765.2023.10125935.

[10] S. Y. Lu and C. Y. Lin, "A Robust Coverless Image Steganography Method Based on Face Recognition and Camouflage Image," in *Proceedings - 2024 4th Asia Conference on Information Engineering, ACIE 2024*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 52–57. doi: 10.1109/ACIE61839.2024.00016.

[11] Y. Tan, X. Xiang, J. Qin, and Y. Tan, "Robust coverless image steganography based on human pose estimation," *Knowl Based Syst*, vol. 296, Jul. 2024, doi: 10.1016/j.knosys.2024.111873.

[12] L. Zou, J. Li, W. Wan, Q. M. J. Wu, and J. Sun, "Robust Coverless Image Steganography Based on Neglected Coverless Image Dataset Construction," *IEEE Trans Multimedia*, vol. 25, pp. 5552–5564, 2023, doi: 10.1109/TMM.2022.3194990.

[13] L. Meng, X. Jiang, Z. Zhang, Z. Li, and T. Sun, "A Robust Coverless Image Steganography Based on an End-to-End Hash Generation Model," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 33, no. 7, pp. 3542–3558, Jul. 2023, doi: 10.1109/TCSVT.2022.3232790.

[14] F. Li, C. Liu, Z. Dong, Z. Sun, and W. Qian, "A Robust Coverless Image Steganography Algorithm Based on Image Retrieval with SURF Features," *Security and Communication Networks*, vol. 2024, pp. 1–22, May 2024, doi: 10.1155/2024/5034640.

[15] X. Li, Q. Zhang, and Z. Li, "Robust coverless image steganography based on DenseUNet with multi-scale feature fusion and attention mechanism," *Signal Image Video Process*, Aug. 2024, doi: 10.1007/s11760-024-03468-8.

[16] S. H. Chiu and C. Y. Lin, "Robust Coverless Image Steganography Based on SIFT and DWT Sequence Mapping," in *Proceedings - 2024 4th Asia Conference on Information Engineering, ACIE 2024*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 41–45. doi: 10.1109/ACIE61839.2024.00014.

[17] S. W. Liang and C. Y. Lin, "Coverless Image Steganography Based on Multi-Object Mapping Rules," in *Proceedings - 2024 4th Asia Conference on Information Engineering, ACIE 2024*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 46–51. doi: 10.1109/ACIE61839.2024.00015.

[18] Z. Zhou *et al.*, "Generative Steganography via Auto-Generation of Semantic Object Contours," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2751–2765, 2023, doi: 10.1109/TIFS.2023.3268843.

[19] H. A. Rehman, U. I. Bajwa, R. H. Raza, S. Alfarhood, M. Safran, and F. Zhang, "Leveraging coverless image steganography to hide secret information by generating anime characters using GAN," *Expert Syst Appl*, vol. 248, Aug. 2024, doi: 10.1016/j.eswa.2024.123420.

[20] T. Kulkarni, S. Debnath, J. Kumar, and R. K. Mohapatra, "DCT based robust coverless information hiding scheme with high capacity," in *7th International Conference on Trends in Electronics and Informatics, ICOEI 2023 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 358–364. doi: 10.1109/ICOEI56765.2023.10126072.

[21] A. Majumder, S. Kundu, and S. Changder, "A unique database synthesis technique for coverless data hiding," *J Vis Commun Image Represent*, vol. 96, Oct. 2023, doi: 10.1016/j.jvcir.2023.103911.

[22] Z. Zhou *et al.*, "Secret-to-Image Reversible Transformation for Generative Steganography," *IEEE Trans Dependable Secure Comput*, vol. 20, no. 5, pp. 4118–4134, Sep. 2023, doi: 10.1109/TDSC.2022.3217661.

[23] S. Phalke, Y. Vaidya, and S. Metkar, "Big-O Time Complexity Analysis Of Algorithm," in *2022 International Conference on Signal and Information Processing, IConSIP 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ICoNSIP49665.2022.10007469.