T.C.
KONYA TEKNİK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

SCADA SİSTEMLERİNDE DAĞITIK HİZMET DIŞI BIRAKMA SALDIRILARININ DERİN ÖĞRENME VE MAKİNE ÖĞRENMESİ YÖNTEMLERİ İLE TESPİTİ

Ebru YAĞMUR

YÜKSEK LİSANS TEZİ

Bilgisayar Mühendisliği Anabilim Dalı

Haziran-2023
KONYA

TEZ KABUL VE ONAYI

Ebru YAĞMUR tarafından hazırlanan “SCADA SİSTEMLERİNDE DAĞITIK HİZMET DIŞI BIRAKMA SALDIRILARININ DERİN ÖĞRENME VE MAKİNE ÖĞRENMESİ YÖNTEMLERİ İLE TESPİTİ” adlı tez çalışması 01/06/2023 tarihinde aşağıdaki jüri tarafından oy birliği ile Konya Teknik Üniversitesi Lisansüstü Eğitim Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı’nda YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Jüri Üyeleri	**İmza**
Başkan Prof. Dr. Nurettin DOĞAN	……..
Danışman Prof. Dr. Halife KODAZ	……..
Üye Dr. Öğr. Üyesi Özgür ÖKSÜZ	……..

Yukarıdaki sonucu onaylarım.

Prof. Dr. Saadettin Erhan KESEN
Enstitü Müdürü

TEZ BİLDİRİMİ

Bu tezdeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edildiğini ve tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

DECLARATION PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Ebru YAĞMUR

Tarih: 01/06/2023

ÖZET

YÜKSEK LİSANS TEZİ

SCADA SİSTEMLERİNDE DAĞITIK HİZMET DIŞI BIRAKMA SALDIRILARININ DERİN ÖĞRENME VE MAKİNE ÖĞRENMESİ YÖNTEMLERİ İLE TESPİTİ

Ebru YAĞMUR

Konya Teknik Üniversitesi
Lisansüstü Eğitim Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Prof. Dr. Halife KODAZ

2023, 171 Sayfa

Jüri
Prof. Dr. Halife KODAZ
Prof. Dr. Nurettin DOĞAN
Dr. Öğr. Üyesi Özgür ÖKSÜZ

SCADA (Supervisory Control and Data Acquisition) sistemleri günümüzde kritik altyapıların kontrolünü sağlamakta önemli bir rol oynamaktadır. Bu sistemler çeşitli endüstrilerde kullanılan altyapıları, tesisleri ve makineleri kontrol etmek, izlemek ve yönetmek için tasarlanmıştır. Ancak, bu sistemlerin internete bağlanması ve diğer teknolojik gelişmelerin hızla ilerlemesiyle birlikte, SCADA sistemlerine yönelik siber saldırılar da artmaktadır. Özellikle son yıllarda SCADA sistemlerine düzenlenen DDoS (Distributed Denial of Service) saldırıları, bu sistemlerin işleyişinde ciddi aksaklıklara neden olabilmektedir. Bu tür saldırılar, hedef sistemlere aşırı miktarda trafik göndererek sistemlerin hizmet verme kapasitesini aşırı yükleyerek, normal veri akışını engelleyerek sistemleri tamamen çökertebilirler. Bu durum, kritik altyapıların işleyişini ciddi şekilde etkileyebilir ve hatta insan hayatını da tehlikeye atabilir. Bu nedenle, SCADA sistemlerinin siber güvenliği son derece önemlidir. Bu sistemlerin korunması için pek çok farklı güvenlik önlemi alınmaktadır, ancak DDoS saldırılarına karşı kesin bir çözüm henüz bulunamamıştır. Bu noktada, yapay zekâ teknolojilerinin kullanılması, SCADA sistemlerinin korunması için etkili bir araç olabilmektedir. Bu çalışmada, SCADA sistemlerine düzenlenen DDoS saldırılarından oluşan bir veri seti elde edilerek, Lojistik Regresyon (LR), Karar Ağaçları (KA), Navie Bayes (NB), K-En Yakın Komşular (KEYK), Rasgele Orman (RO), Yapay Sinir Ağları (YSA), Uzun Kısa Süreli Bellek (UKSB), Tekrarlı Sinir Ağları (TSA) ve Evrişimli Sinir Ağları (ESA) modelleri ile saldırı tespiti gerçekleştirilmiş ve modellerin performansları karşılaştırılmıştır. Ayrıca, CICDDoS2019 veri seti üzerinde de bu modeller test edilerek, sonuçlar değerlendirilmiştir. Bu çalışma, SCADA sistemlerine düzenlenen siber saldırıların tehlikesini ve bu sistemlerin korunması için yapay zekâ teknolojilerinin önemini vurgulamaktadır. Çalışma sonucunda modellerin başarılarının yüksek çıkması, yapay zekâ teknolojilerinin SCADA sistemlerinin siber güvenliği için etkili bir araç olabileceğini göstermiştir.

.

Anahtar Kelimeler: DDoS, derin öğrenme, SCADA, siber güvenlik, siber saldırı, makine öğrenmesi, veri seti.

ABSTRACT

MS THESIS

DETECTION OF DISTRIBUTED DENIAL OF SERVICE ATTACKS IN SCADA SYSTEMS WITH DEEP LEARNING AND MACHINE LEARNING METHODS

Ebru YAĞMUR

Konya Technical University
Institute of Graduate Studies
Department of Computer Engineering

Advisor: Prof. Dr. Halife KODAZ

2023, 171 Pages

Jury
Prof. Dr. Halife KODAZ
Prof. Dr. Nurettin DOĞAN
Assist. Prof. Dr. Özgür ÖKSÜZ

SCADA (Supervisory Control and Data Acquisition) systems play an important role in controlling critical infrastructures today. These systems are designed to control, monitor and manage infrastructures, facilities and machinery used in various industries. However, with the connection of these systems to the internet and the rapid progress of other technological developments, cyber attacks against SCADA systems are also increasing. Especially in recent years, DDoS (Distributed Denial of Service) attacks on SCADA systems can cause serious disruptions in the functioning of these systems. Such attacks can send an excessive amount of traffic to the target systems, overloading the systems' capacity to serve, blocking the normal data flow and completely crashing the systems. This can seriously affect the functioning of critical infrastructures and even endanger human life. Therefore, the cyber security of SCADA systems is extremely important. Many different security measures are taken to protect these systems, but a definitive solution against DDoS attacks has not been found yet. At this point, the use of artificial intelligence technologies can be an effective tool for the protection of SCADA systems. In this study, a data set consisting of DDoS attacks on SCADA systems was obtained, Logistic Regression (LR), Decision Trees (DT), Navie Bayes (NB), K-Nearest Neighbors (KNN), Random Forest (RF), Artificial Neural Network (ANN), Long Short-Term Memory (LSTM), Recursive Neural Networks (RNN) and Convolutional Neural Networks (CNN) models and the performances of the models were compared. In addition, these models were tested on the CICDDoS2019 dataset and the results were evaluated. This study emphasizes the danger of cyber attacks on SCADA systems and the importance of artificial intelligence technologies for the protection of these systems. As a result of the study, the high success of the models showed that artificial intelligence technologies can be an effective tool for the cyber security of SCADA systems.

Keywords: Cyber security, cyber attack, data set, DDoS, deep learning, machine learning, SCADA.

ÖNSÖZ

Tez çalışmam boyunca desteğini esirgemeyen, hususi olarak bilgi ve tecrübesi ile her zaman bana yol gösteren saygıdeğer danışman hocam Prof. Dr. Halife KODAZ'a;

Tezimde kullandığım veri setini oluşturmamda gerekli donanımsal desteği ve SCADA sistemleri hakkında daha fazla bilgi sahibi olmamı sağlayan Konelsis Firması çalışanı Mustafa ERSAN'a ve bu süreçte bilgi ve desteklerini esirgemeyen kıymetli meslektaşım Mustafa CAYMAZ'a;

Bilgisayar Mühendisliği Bölümü'ndeki saygıdeğer hocalarıma;

Yüksek Lisans eğitimine başlamama vesile olan anne ve babama, bu süreç boyunca sonsuz desteği ile bana güç veren değerli eşim Serdal YAĞMUR'a, çalışmalarım boyunca sabırla beni bekleyen oğlum Demir Alp YAĞMUR'a ve çalışma arkadaşlarıma sonsuz teşekkürlerimi sunarım.

Ebru YAĞMUR
KONYA-2023

İÇİNDEKİLER

ÖZET ..... **iv**

ABSTRACT ..... **v**

ÖNSÖZ ..... **vi**

İÇİNDEKİLER ..... **vii**

SİMGELER VE KISALTMALAR ..... **ix**

1. GİRİŞ **1**

1.1. Problemin Tanımı **4**
1.2. Amaç ve Hedef **4**
1.3. Tezin Organizasyonu **5**

2. KAYNAK ARAŞTIRMASI **7**

2.1. Genel DDoS Saldırıları **7**
2.2. SCADA ile İlgili Çalışmalar **15**

3. DDOS SALDIRILARI VE SCADA SİSTEMLERİ **19**

3.1. Dağıtık Hizmet Dışı Bırakma Saldırıları (DDoS) **19**
3.1.1. DDoS saldırı yöntemleri 21
3.1.1.1. Volümetrik saldırılar 22
3.1.1.2. Protokol saldırıları 23
3.1.1.3. Uygulama saldırıları 24
3.1.2. Sık kullanılan DDoS saldırı çeşitleri 25
3.1.2.1. TCP SYN flood saldırısı 25
3.1.2.2. UDP flood saldırısı 26
3.1.2.3. ICMP flood saldırısı 27
3.1.2.4. DNS amplification saldırısı 28
3.1.2.5. HTTP flood saldırısı 29
3.1.2.6. Smurf DDoS saldırısı 30
3.1.2.7. NTP amplification (kuvvetlendirmeli) DDoS saldırısı 31
3.1.2.8. SNMP amplification (kuvvetlendirmeli) DDoS saldırısı 32
3.1.2.9. LAND flood DDoS saldırısı 33
3.1.3. DDoS saldırılarının dünya geneli özeti 34
3.2. Denetleyici Kontrol ve Veri Toplama Sistemleri (SCADA) **37**
3.2.1. Modbus protokolü 40
3.2.2. Programlanabilir mantık denetleyici (PLC) sistemleri 40
3.2.3. SCADA sistemlerinde güvenlik 41
3.2.4. SCADA sistemlerine yapılan siber saldırıları örnekleri 43

4. MATERYAL VE YÖNTEM **46**

4.1. Saldırı Tespit Sistemleri **46**
4.1.1. Ağ tabanlı saldırı tespit sistemi 46

4.1.2. İmza tabanlı saldırı tespiti 47
4.1.3. Anomali tabanlı saldırı tespiti 47
4.1.4. Ana bilgisayar tabanlı saldırı tespit sistemi 48
4.1.5. Derin öğrenme tabanlı saldırı tespit sistemi 49
4.2. Kullanılan Araçlar 49
4.2.1. Docker sanallaştırma 49
4.2.2. Kali linux işletim sistemi 52
4.2.3. Wireshark 52
4.2.4. Hping3 araçları 53
4.3. Paketlerin Yakalanması 54
4.4. Paketlerin Analizi 55
4.5. Makine Öğrenmesi 56
4.5.1. Logistic regresyon (LR) 57
4.5.2. Navie bayes (NB) 57
4.5.3 K en yakın komşu (KEYK) 57
4.5.4. Karar ağaçları (KA) 57
4.5.5. Rasgele orman (RO) 58
4.6. Derin Öğrenme 58
4.6.1. Yapay sinir ağları (YSA) 59
4.6.2. Evrişimsel Sinir Ağları (ESA) 61
4.6.3. Tekrarlayan Sinir Ağları (TSA) 61
4.6.4. Uzun Kısa Süreli Bellek (UKSB) 62
4.7. Değerlendirme Metrikleri 63
4.7.1. Karmaşıklık matrisi 63
4.7.2. Performans metrikleri 64
4.8. Hazır Veri Seti 65
4.9. Oluşturulan Veri Seti 66
4.10. Veri Ön İşleme 72
4.10.1. CICDDoS2019 veri seti ön işlem 72
4.10.2. KEY2023 veri seti ön işlem 76

5. ARAŞTIRMA SONUÇLARI VE TARTIŞMA 82

5.1. Çalışma Ortamı 83
5.2. CICDDoS2019 Veri Seti Sonuçları 85
5.2.1. Çoklu sınıflandırma sonuçları 85
4.2.2. İkili sınıflandırma sonuçları 104
5.3. KEY2023 Veri Seti Sonuçları 117
5.3.1. Çoklu sınıflandırma sonuçları 117
5.3.2. İkili sınıflandırma sonuçları 132
5.4. Tartışma 146

6. SONUÇLAR VE ÖNERİLER 147

6.1 Sonuçlar 147
6.2 Öneriler 152

KAYNAKLAR 153

SİMGELER VE KISALTMALAR

Simgeler

b	: Eğilim
F	: Evrişimsel katman nöronlarının boyutu
N	: Nöron sayısı
P	: Sıfır dolgulama miktarı
γ	: Küme normalleştirmesi
β	: Hiper-parametre
α, η	: Öğrenme oranı
μB	: Düzeltilen kümenin ortalaması
σB2	: Düzeltilen küme varyansı
w	: Ağırlık
W	: Girdi boyutu
z	: Ürün

Kısaltmalar

ACK	:Onay
ADAM	:Uyarlanabilir Moment Tahmini
ADAMAX	:Uyarlanabilir Maksimum Havuzlama
BotNet	:Robot Ağı
ÇYUKSB	:Çift Yönlü Uzun Kısa Süreli Bellek
ÇYTSA	:Çift Yönlü Tekrarlayan Sinir Ağları
ESA	:Evrişimli Sinir Ağı
DAE	:Derin Oto-Kodlayıcı Ağları
DBN	:Derin İnanç Ağı
DESA	:Derin Evrişimli Sinir Ağı
DCS	:Dağıtık Kontrol Sistemi
DoS	:Hizmet Dışı Bırakma
DDoS	:Dağıtık Hizmet Dışı Bırakma
DNN	:Derin Sinir Ağı
DNS	:Alan Adı Sistemi
DÖ	:Derin Öğrenme
DVM	:Destek Vektör Makinesi
FNN	:İleri Beslemeli Sinir Ağı
GB	:Gradyan Artırma
GRU	:Geçitli Tekrarlayan Birim
HMI	:İnsan-Makine Arayüzü
HTTP	:Üst Metin Transfer Protokolü
HTTPS	:Güvenli Üst Metin Transfer Protokolü
ICMP	:İnternet Kontrol Mesajı Protokolü
STS	:Saldırı Tespit Sistemi
IoT	:Nesnelerin İnterneti
IP	:İnternet Protokolü
ISO	:Uluslararası Standardizasyon Örgütü
KA	:Karar Ağacı
KEYK	:K- En Yakın Komşular
LDA	:Doğrusal Diskriminant Analizi

LDAP :Basit Dizin Erişim Protokolü
MFB :Morfolojik Fraktal Boyutu
MLP :Çok Katmanlı Algılayıcı
MSSQL :Microsoft SQL Serverix
MÖ :Makine Öğrenmesi
NB :Naive Bayes
NETBIOS :Ağ Temel Giriş-Çıkış Sistemi
NIDS :Ağ Tabanlı Saldırı Tespit Sistemi
NDAE :Simetrik Olmayan Derin Otomatik Kodlayıcı
NTP :Ağ Zaman Protokolü
OSI :Açık Sistem Ara Bağlantısı
PLC :Programlanabilir Mantık Denetleyiciler
ReLu :Doğrultulmuş Doğrusal Birim
Rmsprop :Kök Ortalama Kare Yayılımı
RPS :Saniye Başına İstek
RO :Rasgele Orman Algoritması
SCADA :Denetleyici Kontrol ve Veri Toplama Sistemleri
SDN :Yazılım Tanımlı Ağ
SMTP :Basit Posta Aktarım Protokolü
SNMP :Basit Ağ Yönetimi Protokolü
SSDP :Basit Hizmet Keşif Protokolü
SÖS :Saldırı Önleme Sistemi
SYN :Senkronize
TCP :İletim Kontrol Protokolü
TFTP :Önemsiz Dosya Aktarım Protokolü
TSA :Tekrarlayan Sinir Ağı
UDP :Kullanıcı Datagram Protokolü
UKSB :Uzun Kısa Süreli Bellek

1. GİRİŞ

Günümüzde teknolojinin gelişmesine bağlı olarak birçok sektörde özellikle bilişim araçlarının kullanılmasında önemli ölçüde gelişmeler olmaktadır. İnsanlar birçok iş ve işlemlerini bilişim araçları sayesinde kolaylıkla yapabilmektedir. Bilişim araçları ile yapılan işlemlerin çoğu internet üzerinden yapılmaktadır. Genel olarak online ticaret ya da kurum ve kuruluşların kendilerini internet ortamında tanıtma isteği, verilerin bulut ortamlarda saklanması, sosyal medyanın günümüzde daha aktif kullanılması vb. gibi ihtiyaçlar neticesinde bu kullanım oranı günden güne artarak devam etmektedir. İnternet kullanımının artması ile birçok güvenlik sorunları meydana gelmektedir. Bunlardan günümüzde en önemli sorun olarak karşımıza çıkan siber saldırılardır. Siber Saldırı Alkan'ın tanımına göre, "hedef seçilen şahıs, şirket, kurum, örgüt ve devlet gibi yapıların bilgi ve iletim sistemlerine ve kritik altyapılarına yapılan planlı ve koordineli saldırılar" ifade edilmektedir (Alkan, 2012). Siber saldırılar türüne göre farklı işlevler göstermekle birlikte siber saldırılara maruz kalan sistemlere ve bu sistemleri kullanan ya da bu sistemlerden fayda sağlayan kişilere önemli ölçüde zarar vermektedir. Siber saldırıların artması sonucu, siber güvenliğin sağlanması ve alınması gereken önlemlerin gerekliliği son yıllarda ciddi bir şekilde artmıştır (Savaş ve Karataş, 2022). Siber saldırılardan özellikle verilen hizmetin kesintiye uğratılması firmalar için büyük bir sorun teşkil ederek maddi kayıplara sebep olmaktadır (Atasever ve ark., 2019).

Hayatın her alanında kullanılmaya başlanan internet ile birçok alanda cihazların güvenlik ihtiyaçları artmıştır. IoT cihazlar, akıllı ev sistemleri, otonom araçlar, SCADA sistemleri gibi alanlar daha da savunmasız hale gelmiştir. Bu sistemlerin belirli bir yapay zekâ alt yapısı ile oluşturulmuş güvenlik sistemlerini kullanmaları aldıkları güvenlik önlemlerinden biridir. Ayrıca kullanılan erken tespit sistemleri bu önlemleri güçlendirmiştir. Her ne kadar alınan güvenlik önlemleri fazla olsa da Dağıtık hizmet dışı bırakma (DDoS) gibi siber saldırılarda kesin bir çözüm getirilememiştir.

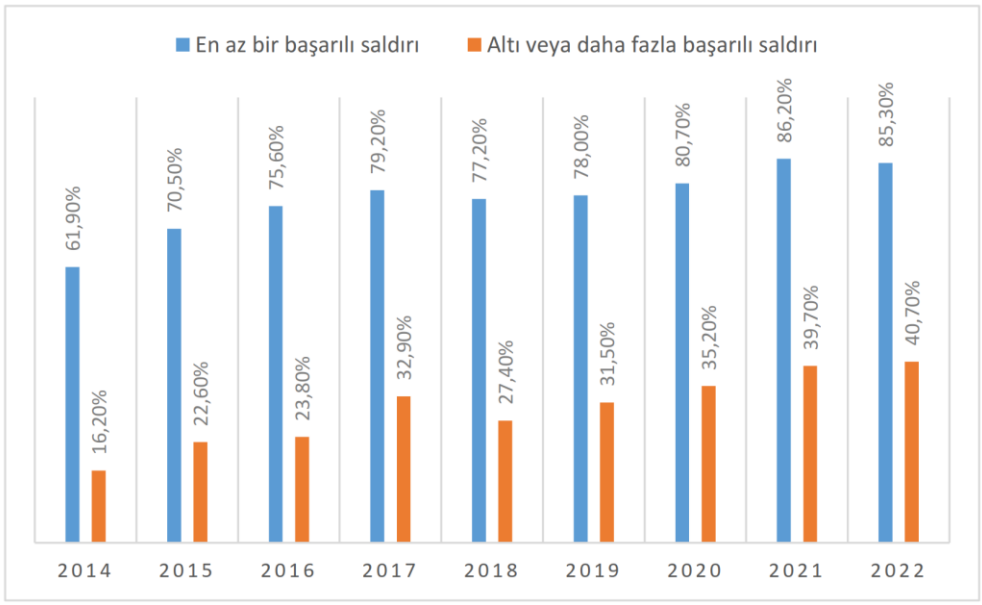
DDoS saldırılarında saldırganlar hedefledikleri cihazlara zararlı yazılımlar bulaştırmakta ve bu cihazları ele geçirerek yönetmektedir. DDoS saldırıları kurum ya da kuruluşların internet hizmetini, ağ bağlantısını kesintiye uğratmaktadır. Hizmet kesintisinden dolayı ortaya çıkabilecek zararların önlenmesi için tespit edilmesi büyük önem arz etmektedir. Günümüzde çeşitli güvenlik cihazları ve yazılımları kullanılmasına rağmen tam anlamı ile bu durumlarda da güvenlik sağlanamamaktadır. Bu yüzden sistemlerin otomatikleştirilmesi ve saldırıların tespit edilmesinde yapay zeka

yöntemlerinin kullanılması DDoS saldırılarının tespitinde önemli bir rol oynamaktadır (Efe, 2021). Yapay zekâ yöntemleri ile entegre olan güvenlik sistemleri etkili sonuçlar verebilmektedir (Şeker, 2020). Yapay zekâ, bilgisayarların insan gibi düşünme ve öğrenme yeteneklerini taklit etme yeteneğine sahip olmasıdır. Yapay zekâ ile insan zekasının birçok özelliğini taklit etmeye çalışılır, fakat insana ait özelliklerin hepsini taklit edebilme gibi bir yapısı yoktur. Yapay zekâ, makine öğrenmesi (MÖ) ve derin öğrenmeyi (DÖ) kapsayan genel bir kavramdır ve çoğunlukla veriler ve öğrenme algoritmaları kullanılarak yapılmaktadır. Günümüzde yapay zekâ birçok alanda kullanılmaktadır ve kullanımı giderek yaygınlaşmaktadır. STM Thinktech'in raporuna göre yapay zekanın en çok tercih edilen alanlarından birisi de siber güvenlik alanıdır (Thinktech, 2022). Şekil 1.1'de yapay zekânın en çok kullanıldığı 5 alan gösterilmiştir.

Şekil 1.1. Yapay zekanın en çok kullanıldığı alanlar.

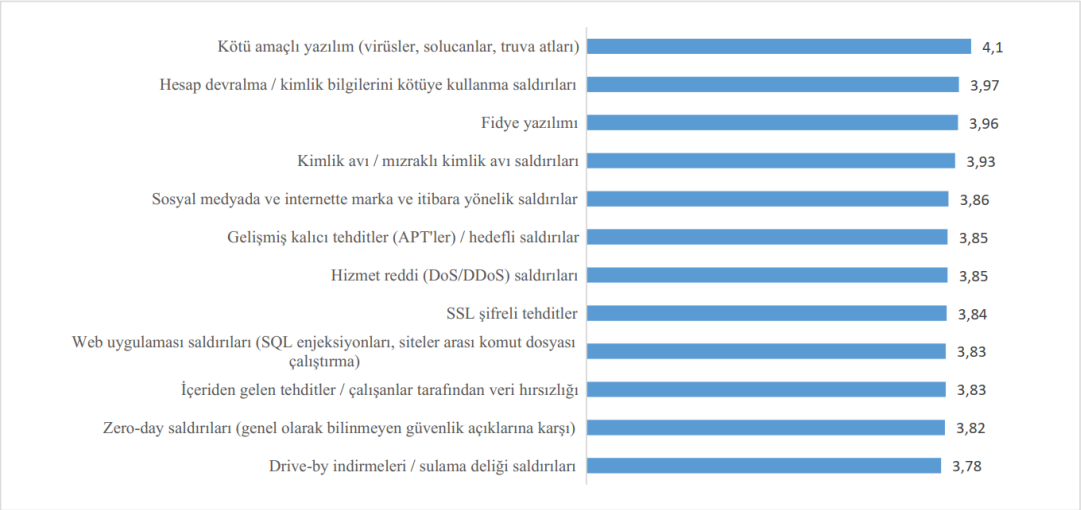
Yapılan çalışmalarda Saldırı Tespit Sistemi (STS) ve Saldırı Önleme Sistemi (SÖS) sistemlerinde yapay zekâ kullanımı son yıllarda artış göstermektedir. CyberEdge Group Research Lab'ın Son 5 yıla ait Siber Tehdit Savunma Raporu'na göre: 2022 yılında kuruluşların %90'ının makine öğrenimi ve yapay zekâ içeren SÖS, STS ve Güvenlik Duvarı (Firewall) gibi sistemleri kullanmalarına karşın; yine aynı kuruluşların %85'i bir

önceki yıl başarılı bir siber saldırıya maruz kalarak zarara uğramıştır (Cyberedge, 2022). Bu saldırılardaki artışın nedeni son yıllarda uzaktan çalışma yönteminin sağlık koşulları sebebi ile tercih edilmesi ve buna bağlı olarak internet kullanımının artmasıdır. Şekil 1.2.'ye bakıldığında son yıllar içerisindeki siber saldırıların arttığı görülmektedir.



Şekil 1.2. Cyberedge 2022 Raporu (Cyberedge, 2022).

Cyberedge 2022 Raporu'na göre siber saldırı türlerinin her biri 1 ile 5 puan üzerinden puanlanarak sıralanmış ve DDoS saldırıları Şekil 1.3.'te gösterildiği gibi 2022 yılında ilk 10 saldırı arasında yer almaktadır.



Şekil 1.3. Cyberedge 2022 Raporu Saldırı Artışı (Cyberedge, 2022)

Bu saldırı türleri yapay zekânın alt dalı olan MÖ ve DÖ yöntemleri ile günümüzde tespit edilebilmektedir. DDoS saldırıları endüstriyel otomasyon sistemlerinde çok ciddi sorunlara neden olabilmesi sebebiyle bu sistemlerde en sık kullanılan sistemlerden biri olan Denetleyici Kontrol ve Veri Toplama Sistemleri (SCADA), sistemi izler ve veri toplar. Bu aşamada kullandığı protokoller Modbus gibi siber saldırılara açık bir protokol olması sebebi ile güvenlik önlemlerinin alınması gerekmektir. Bu çalışmada SCADA sistemlerine karşı olabilecek DDoS saldırılarının tespiti amaçlanmaktadır. Öncelikle DDoS saldırılarından oluşan ağ paketlerinin kaydedilmesi ve bu paketlerin temizlenmesi ile oluşturulacak veri seti ile olası DDoS saldırılarının MÖ ve DÖ yöntemleri ile tespiti yapılmaktadır.

1.1. Problemin Tanımı

SCADA sistemleri endüstriyel otomasyon alanında sıklıkla kullanılmaktadır. Bu sistemler internet üzerinden hizmet vererek otomasyon işlemini izlenebilir olmasını sağlamaktadır. Sistemde meydana gelen değişiklikler izlenerek yaşanabilecek para veya iş gücü kaybını önlemek amaçlanmaktadır.

İnternet üzerinden hizmet veren sistemler çeşitli saldırılara uğramaktadırlar. Bu saldırıların en tipik olanı DDoS saldırılarıdır. DDoS saldırıları hizmetin cevap verememesine neden olabilmektedir. Otomasyon sistemlerinde hizmetin cevap verememesi büyük sorunlara neden olabilmektedir. Takibi yapılamayan bir otomasyon sistemi çeşitli kazalara yol açabilmektedir. Bu nedenle SCADA sistemlerinde DDoS saldırılarının tespiti hayati önem kazanmaktadır.

1.2. Amaç ve Hedef

Bu çalışmanın amacı, SCADA sistemleri gibi enerji denetim ve yönetim sistemlerine, sistem dışından gelecek olan DDoS saldırılarını MÖ ve DÖ modellerinin uygulanması ile tespit ederek sistemin korunması sağlamaktadır. Yapılan bu çalışma ile normal ve DDoS saldırıları zamanlarında elde edilen verilerin farklılıklarından yararlanılarak DÖ ile sınıflandırma algoritmaları ile DDoS saldırısı olup olmadığı ayrımın doğru bir şekilde yapılabiliyor olması amaçlanmaktadır. Bu çalışmada elde edilecek bir veri seti ile ileriki çalışmalara kaynak oluşturma ve daha önceden oluşturulmuş veri setleri ile karşılaştırmadır.

1.3. Tezin Organizasyonu

Tez altı bölümde organize edilmiştir, bu bölümlerin içeriği ve detayı aşağıda sıralanmıştır.

Birinci bölümde siber güvenliğin öneminden, DDoS saldırılarının sistemlere verebileceği zararlardan bahsedilmiştir.

İkinci bölümde literatüre yönelik kaynak araştırması iki başlıkta incelenmiştir. İlk başlıkta daha önce oluşturulmuş CICDDoS2019 veri seti ve diğer benzer veri setleri üzerindeki DDoS saldırılarının MÖ ve DÖ yöntemleri ile tespit edilmesi ve DDoS saldırılarının uygulamaları araştırılmıştır. Bu bağlamda geliştirilen modeller ve kullanılan veri setlerinden bahsedilmiştir.

Üçüncü bölümde iki başlık altında ele alınmıştır. Bunlar sıra ile; birinci bölümde DDoS saldırılarının neler olduğundan, türlerinin neler olduğu ve bu saldırıların uygulanma şekillerinden, ikinci bölümde ise SCADA sistemleri hakkında detaylı bilgi verilerek siber saldırılar karşısında sistemlerin nasıl etkilendiği detaylı olarak açıklanmıştır.

Dördüncü bölümde materyal ve yöntem on başlık altında ele alınmıştır. Bu başlıklar sıra ile; birinci bölümde saldırı tespit sistemlerinin neler olduğundan ve nasıl çalıştıklarından, ikinci bölümde veri seti oluşturma aşamasında kullanılan araçlar ve bu araçların kullanımlarından, üçüncü bölümde ağ trafiğinde paketlerin yakalanması, dördüncü bölümde ağ trafiğinde yakalanan paketlerin analizinin nasıl gerçekleştirildiği, nelere dikkat edildiği, beşinci bölümde MÖ modellerinden, altıncı bölümde DÖ modellerinden ve bu modellerin sıklıkla tercih edilen alanları ile avantajları, dezavantajlarından, yedinci bölümde çalışmalar için kullanılan değerlendirme metriklerinden, sekizinci bölümde bu çalışmada kullanılan hazır veri seti özelliklerinden, dokuzuncu bölümde bu tez çalışması kapsamında oluşturulan SCADA sistemlere düzenlenen DDoS saldırılarından oluşan veri setinin oluşturulması aşamaları ve özelliklerinden, onuncu bölümde ise hem hazır veri seti olan CICDDoS2019 veri seti hem de yeni oluşturulan veri seti üzerinde veri ön işleme adımları detaylı olarak açıklanmıştır.

Beşinci bölüm araştırma sonuçları ve tartışma başlığı altında dört kısımda incelenmiştir. İlk bölümde çalışma ortamı, ikinci bölümde CICDDoS2019 veri seti için çoklu sınıflandırma ve ikili sınıflandırmada elde edilen sonuçlar açıklanmış ve değerlendirilmiştir. Üçüncü bölümde ise bu tez kapsamında oluşturulan SCADA sistemlere düzenlenen DDoS saldırılarından oluşan veri seti için ikili sınıflandırma ve

çoklu sınıflandırma sonuçları değerlendirilmiştir. Bu değerlendirme aşaması için yapılan çalışmada kullanılan modellere ait deneysel sonuçlar verilmiştir. Dördüncü bölümde ise tartışma konusu üzerinde durulmuştur.

Altıncı bölüm sonuç ve öneriler bölümüdür. Bu bölümde tez kapsamında yapılan çalışmaların sonuçları değerlendirilerek çalışmanın geliştirilmesi adına geleceğe yönelik öneriler verilmiştir.

2. KAYNAK ARAŞTIRMASI

Kaynak araştırması 2 bölümden oluşmaktadır. Bu bölümler çalışmaların içerdiği materyal ve yöntemlere bağlı olarak ayrılmıştır. Literatürde değinilen birinci bölüm, açık erişimli veri setlerini kullanan çalışmalar, yeni veri seti oluşturulan çalışmalar ve DDoS saldırılarında DÖ çalışmalarından oluşmaktadır. İkinci bölüm ise, SCADA sistemlerine düzenlenen siber saldırılar ve DDoS saldırılarını içermektedir.

2.1. Genel DDoS Saldırıları

DDoS saldırıları üzerinde veri seti oluşturmak için laboratuvar ortamında birçok donanıma ihtiyaç duyulmaktadır. Duyulan bu gereksinimden dolayı çalışmalar açık erişimli veri setleri üzerinde yazarlar tarafından sıklıkla gerçekleştirilmiştir. Bu yüzden açık erişimli veri setleri ve yeni oluşturulan veri setleri üzerinde DDoS saldırılarının tespiti üzerine yapılan çalışmalar bu çalışmanın kaynaklarında incelenmiştir. Ayrıca, DDoS saldırılarının tespitinde derin öğrenme ile yapılan birçok çalışma bulunmaktadır. DDoS saldırıları içeren veri kümeleri ile yapılan deneyler ve derin öğrenme modelinin kullanımına yönelik çalışmalar da bu kısımda özetlenmektedir. Literatür çalışmalarını incelerken bu başlık altında yapılan çalışmaları son 6 yıla ait çalışmalar özellikle DÖ çalışmaları baz alınarak sunulmuştur.

Çatak ve Mustaçoğlu (Çatak ve Mustaçoglu, 2017) yaptıkları çalışmada DDoS saldırılarının algılanmasında derin öğrenme yöntemleri ve makine öğrenme yöntemlerini kullanarak bir model oluşturmuşlardır. Kullandıkları KDD99 veri setinden sayısal olmayan değerleri de içeren 49 özelliği çıkararak 25 özellik ile bu çalışmayı gerçekleştirmişlerdir. Önerdikleri model normal ağ trafiği ile normal olmayan ağ trafiğini sınıflandırmada %98 doğruluk oranı sağlamıştır.

Hasan ve arkadaşları (Hasan ve ark., 2018) tarafından yapılan çalışmada, Optik Anahtarlama ağındaki DDoS saldırılarının tespiti için Derin Evrişimli Sinir Ağları (DESA) modeli önerilmiştir. Deney sonuçlarına göre, sırasıyla %93, %88 ve %79 doğruluk değerlerine sahip olan K-En Yakın Komşu (KEYK), Destek Vektör Makinesi (DVM), Naive Bayes makine öğrenmesi algoritmalarına göre DESA'nin %99 doğruluk ile en yüksek başarıyı elde etmiştir.

Alzahrani ve Hong (Alzahrani ve Hong, 2018), DDoS saldırılarını tespit etmek için imza tabanlı yaklaşımla birlikte Yapay Sinir Ağı (YSA)'nın kullanımını

önermişlerdir. Deneyler sonucunda bu iki yaklaşımın birlikte kullanımının %99,98 gibi daha yüksek bir doğruluk değerine ulaştığı görülmüştür.

Zhu ve arkadaşları (Zhu ve ark., 2018), tarafından yapılan çalışmada ağ trafiğini analiz etmek ve DDoS saldırı algılamasını kullanmak için derin öğrenme modellerinden Evrişimli Sinir Ağları (ESA) ve İleri Beslemeli Sinir Ağları (FNN Feed-forward Neural Network) modelinin kullanılması önerilmektedir. NSL-KDD veri seti üzerinde yapılan deneylerde, FNN ve ESA modellerinin, makine öğrenme algoritmaları olan Naive Bayes, Rastgele Orman (RO), Karar Ağacı(J48), Rastgele Ağaç, DVM'den daha yüksek doğruluğa sahip olduğu gözlemlenmiştir.

Sharafaldin ve arkadaşları (Sharafaldin ve ark., 2019), DDoS saldırılarının makine öğrenmesi algoritmalarıyla tespiti üzerine çalışma yapmışlardır. Çalışmalarını kendi ürettikleri CICDDoS2019 veri seti ile gerçekleştirmişlerdir. Model eğitimi için üretilen saldırı verileri içerisinde NTP DDoS, DNS DDoS, LDAP DDoS, MSSQL DDoS, Network Basic Input/Output System (NetBIOS) DDoS, SNMP DDoS, SSDP DDoS, UDP DDoS, UDP-Lag DDoS, WebDDoS, SYN DDoS ve Trivial File Transfer Protocol (TFTP) DDoS saldırıları bulunmaktadır. Model testi için üretilen saldırı verileri içerisinde PortMap DDoS, NetBIOS DDoS, LDAP DDoS, MSSQL DDoS, UDP DDoS, UDP-Lag DDoS ve SYN DDoS saldırıları bulunmaktadır. Hem eğitim hem de test verileri içerisine normal trafik içeren veriler de eklenmiştir. Çalışmalarında Decision Tree algoritmasından biri olan Iterative Dichotomiser 3 (ID3), Random Forest, Naive Bayes ve Multinomial Logistic Regression algoritmalarını kullanmışlardır. Çalışmalarında en iyi sonucu veren ID3 algoritması ile %78 kesinlik değeri, %65 hatırlama değeri ve %69 F1 skor değeri elde etmişlerdir.

Krishnan ve arkadaşları (Krishnan ve ark., 2019), SDN (Yazılım Tanımlı Ağ) güvenliğini sağlamak için yazılım tanımlı ağlar için gelişmiş çok düzlemli güvenlik çerçevesi olarak adlandırdıkları "VARMAN"ı önermişlerdir. Simetrik olmayan bir derin otomatik kodlayıcı (Non-Symmetric Deep Auto-Encoder-NDAE) algoritmasını kullanmışlardır. DDoS saldırılarını tespit etmek için kullanılan modelin performansını ölçmek için NSL-KDD ve CICIDS2017 veri setleri kullanarak dengeli veri setlerine dönüştürmüşlerdir. Çalışmalarında kullandıkları NSL-KDD ve CICIDS2017 veri setlerine NDAE modeli uygulanmasıyla etiketli örneklerin yüzdesi %100 olduğunda elde edilen doğruluk değerleri sırası ile %99,60 ve %99,24 olarak ölçülmüştür.

Ahmetoğlu ve Daş (Ahmetoğlu ve Daş, 2019) yaptıkları çalışmada CICIDS2017 veri setini kullanarak saldırı tiplerini tam bağlantılı YSA ile tespitini yapmışlardır.

Çalışmalarında veri setinin tam bir analizini gerçekleştirerek ikili sınıflandırma da ve çoklu sınıflandırmada önerdikleri model başarısı %98 olarak elde ederek Saldırı Tespit Sistemi (STS) geliştirmişlerdir.

Ateş ve arkadaşları (Ateş ve ark., 2019) yaptıkları çalışmada açgözlü algoritması (Greedy Algorithm) ve destek vektör makineleri (DVM) algoritmasını kullanarak DDoS saldırıları tespit edebilmek için farklı boyutlara sahip iki olasılığın dağılımındaki mesafeyi saldırı olarak değerlendirilmiştir. DDoS saldırılarını tespitinde bu değerlerin etkili olduğunu belirtmişlerdir. Boğaziçi Üniversitesi ağından ve MIT Darpa 2000 veri setinden oluşan gerçek dünya verileri ile DDoS saldırılarında veriler arasındaki uzaklığı hesaplamak için Greedy Algoritmasını kullanıp, yanlış tespit oranını azaltmak için ise DVM modelini kullanmışlardır. Kullandıkları veri setlerinde %99 doğruluk sağlamışlardır.

Karataş (Karataş, 2020), CSE-CIC-IDS2018 veri setini kullanarak MÖ ve DÖ algoritmaları ile saldırı tespiti çalışması yapmıştır. Veri setindeki dengesizliği azaltmak için sentetik veri örnekleme modelini kullanmıştır. KA, RO, KEYK, AdaBoost, Gradyan Artırma (GB) ve Doğrusal Ayırma Analizi (LDA) makine öğrenmesi algoritmaları ve ESA, Tekrarlayan Sinir Ağları (TSA), Çift Yönlü Tekrarlayan Sinir Ağları (ÇYTSA), Uzun Kısa Süreli Bellek (UKSB), Çift Yönlü Uzun Kısa Süreli Bellek (ÇYUKSB), Evrişimli Uzun Kısa Vadeli Hafıza Ağları (ESA-UKSB), Geçitli Tekrarlayan Birim (GRU) ve Derin Oto-Kodlayıcı Ağları (DAE) derin öğrenmesi algoritmalarını kullanmıştır. Kullanılan veri setindeki dengesizliği düzeltmek için sentetik veri üretme işlemini SMOTE ve ADASYN algoritmalarını kullanarak gerçekleştirmiştir. Bu algoritmalardan SMOTE ile daha iyi sonuçlar elde edilmiştir. Makine öğrenmesi algoritmaları arasından, sentetik veri üretmeden aldığı sonuçlar içerisinde en başarılı sonucu %99,69 doğruluk değeri ile AdaBoost algoritması vermiştir. Sentetik veri üretimi yaptıktan sonra en başarılı sonucu %99,60 doğruluk, değeri ile yine AdaBoost algoritması vermiştir.

Karaman ve arkadaşları (Karaman ve ark., 2020). Çalışmalarında bir ağa saldırı olup olmadığını ve bu saldırının hangi tür olduğunu tespit etmek için CSE-CICIDS2018 veri setini kullanmışlardır. Saldırı türlerini DDoS, DoS, Botnet ve BruteForce saldırılarına göre ayırmak için veri setini bu saldırıları ifade eden en iyi özelliklerine göre 5 farklı veri setine ayırarak yapay sinir ağları (YSA) ile çalışmalarını yapmışlardır. Her bir veri setinde ayrı ayrı YSA ile eğitim sonucunda ise tehdit olup olmadığını %99,11 ile

Bot saldırısı olduğu %92.33 ile DDOS saldırısı olduğu %99.23 ile BruteForce saldırısı olduğu %99.33 ve DOS saldırısı olduğu %92.26 oranında doğru tahmin etmişlerdir.

Elsayed ve arkadaşları (Elsayed ve ark., 2020) SDN ortamlarında DDoS saldırılarına karşı bir saldırı tespit sistemi olan DDoSNet'i önermişlerdir. Bu modeli geliştirmek için TSA kullanmışlardır. CIC-DDoS2019 veri setini benign(normal) ve attack(saldırı) olarak iki sınıf kullanarak MÖ ve DÖ modellerini değerlendirmişlerdir. Değerlendirme sonucunda ise, NB %57, KA %77 Booster %84, RO %86, DVM %93, LR %95, önerilen model olan DDoSNET ise %99 başarı sağlamıştır.

Aytaç ve arkadaşları (Aytaç ve ark., 2020), çalışmasında CIC-DDoS2019 veri setini kullanarak DDoS saldırılarının tespitinde öncelikle veri setini 77 özelliğe indirgemiş ve bu özelliklerden DDoS saldırılarının tespitini sağlayan 4, 6, 8 ve 12 özelliğe göre ayrı ayrı MÖ ve DÖ algoritmalarının performansını değerlendirip karşılaştırmıştır. Bu değerlendirme sonucunda en yüksek başarı oranı KEYK, LR, NB algoritmaları elde ederken, eğitim ve test sürelerine göre DVM %99,7 oranında başarı elde etmiştir.

Assis ve arkadaşları (Assis ve ark., 2021), DDoS saldırılarını önlemek için Nesnelerin İnterneti (IoT) ile Yazılım Tanımlı Ağ (SDN) için bir savunma sistemi önerdi. İki sınıf olarak saldırıları tanımlamışlardır; DDoS ve Normal olarak. MLP, ESA, D-MLP, LR gibi yöntemleri kullanmışlardır. Eğitim ve test için SDN trafiği oluşturup ayrıca CIC-DDoS2019 veri kümesinden simüle edilmiş IP akışları toplanmıştır.

Cil ve arkadaşları (Cil ve ark., 2021), DDoS saldırılarının tespiti ve sınıflandırılması için CICDDoS2019 veri setinden bazı özellikleri çıkararak 69 özellik ile model eğitilmiştir ve iki sınıf olarak (normal ve saldırı) sınıflandırma gerçekleştirilmiştir. Derin öğrenme ile DDoS saldırılarının tespiti ve sınıflandırılmasında daha etkin kullanabilmek için CICDDoS2019 veri setini iki farklı formata Dönüştürerek kullanmışlardır. İki farklı veri setinde birincisin de normal ve saldırı türleri diğer veri setin de saldırı olmayanlar veriler çıkarılarak saldırı türleri belirlenmiştir. Veri setlerine derin öğrenme modeli uygulandığında birinci veri seti için doğruluk %99,99, ikinci veri seti için ise %94.57 oranında doğruluk elde edilmiştir.

Myneni ve arkadaşları (Myneni ve ark., 2022), çalışmalarında kaynakta ve uçta DDoS saldırılarını tespit etmeye ve hafifletmeye yönelik bir DDoS algılama ve azaltma çerçevesi olan SmartDefense'i önermişlerdir. Çalışmada CIC-DDoS2019 veri seti kullanılarak ISP uç ağına giden DDoS trafiği tarafından tüketilen gereksiz bant genişliğini azaltılmıştır. Derin öğrenme yöntemleri kullanılarak DDoS trafiğinin %90'ından

fazlasının kaynağında yakalanması ve kalan DDoS trafiğinin %97,5'inden fazlasının uçta yakalanmasıyla algılama ve azaltma oranını iyileştirmişlerdir.

Aydın ve arkadaşları (Aydın ve ark., 2022), çalışmalarında bulut ağ ortamında DDoS saldırılarının tespiti ve önlenmesi için tasarlanmış UKSB tabanlı bir sistem UKSB-CLOUD sistemini önermişlerdir. UKSB-CLOUD, algılama ve savunma olarak iki modüle sahip sistemde ilk modülü UKSB DÖ modeli ile DDoS saldırılarının oluşumunu CICDDoS2019 veri seti üzerinde %99,83 doğruluk oranı ile tespit etmişlerdir. Diğer modülün işlevi ise saldırılar tespit edildiğinde bulut sistemlerini korumak için savunma mekanizmasını çalıştırmak olarak ayarlamışlardır.

Liu ve arkadaşları (Liu ve ark., 2022), çalışmalarında SDN sistemlerinde bilgi entropisine ve derin öğrenmeye dayalı iki seviyeli bir DDoS saldırı tespit yöntemi önerilmişlerdir. Önerilen yöntemin saldırı tespit doğruluğu %98,98'e ulaşmıştır. Ayrıca altı farklı, derin öğrenme modeli ve makine öğrenmesi yöntemleri ile CICIDS2017 veri seti test edilmiştir. %98,99 ile 99,25 arasında başarı oranları çıkmıştır. ESA %99.16, DNN %95,72, PSO-BPNN %90,50, RO %95,45 DVM %93,43 olarak elde etmişlerdir.

Baldini ve Amerini (Baldini ve Amerini, 2022), çalışmalarında Morfolojik Fraktal Boyutu (MFB) ile kayan pencereye dayalı bir çevrimiçi algoritma önermişlerdir. MFB'yi CICIDS2017 veri setine uygulayarak, entropi tabanlı yaklaşımlara oranla DDoS saldırısının tespitinde önemli bir gelişme sağlamıştır. Kayan pencere boyutunun otomatik olarak tanımlanması için yeni bir algoritma da önermişlerdir. MFB'de bulunan farklı hiper parametrelerin etkisini ölçmüşlerdir. Önerilen model %99,3 başarı oranı sağlamıştır.

Akgün ve arkadaşları (Akgun ve ark., 2022), çalışmalarında DNN, ESA ve UKSB tabanlı çeşitli modelleri değerlendirmişlerdir. Önerdikleri modelde CIC-DDoS2019 veri setini kullanmışlardır. CIC-DDoS2019 veri setine birçok ön işleme tekniğini uygulamışlardır. Elde ettikleri temizlenmiş veri seti üzerinde farklı özellik seçim teknikleri kullanılmış ve Info Gain Attribute Evaluation tekniği ile bir alt veri seti tanımlanmıştır. Çalışma sonucunda ESA tabanlı başlangıç modeli kullanılarak ikili sınıf için %99,99 ve çok sınıflı doğruluk için %99,30 önerilen modeller arasında en iyi sonuçları vermiştir.

Yousuf ve arkadaşları (Yousuf ve Mir, 2022), çalışmalarında IoT'lerde DDoS saldırılarını belirlemek için SDN, OpenDayLight ve derin öğrenme yaklaşımını incelemişlerdir. Çalışmada NSL KDD veri seti kullanarak TSA modeli ile eğitilmiştir. DDoS saldırı tespiti için OpenDayLight platformunda uygulanan yeni bir algoritma olan

DALESA'yi önermişlerdir. Önerilen algoritma MLP, SMO, IBK ve J48 gibi diğer yöntemler ile karşılaştırmışlardır ve DALESA daha yüksek başarı göstermiştir. Önerilen algoritma %99,98 oranında başarı elde etmiştir.

Kumar ve arkadaşları (Kumar ve ark., 2023), DDoS saldırılarını tespit etmek için UKSB modeli oluşturmuşlardır. Çalışmalarında, bir ağ trafiği paketleri üzerinde DDoS saldırılarını belirlemek için derin bir özellik seçimi ve çıkarma algoritması içeren öğrenme yöntemi olan UKSB'yi önermişlerdir. Bu çalışma için CICDDoS2019 veri setini kullanarak KEYK, YSA ve önerdikleri UKSB yöntemlerini test etmişlerdir ve önerdikleri model %98 oranında doğruluk elde etmişlerdir.

Bu çalışmaların genel sonucunda DÖ ve MÖ gibi yöntemlerin kullanımı ile DDoS saldırılarına karşı başarılı sonuçlar elde edildiği görülmüştür. Literatür çalışmalarının karşılaştırılması Çizelge 2.1'de verilmiştir.

Çizelge 2.1. DDoS saldırılarının literatür karşılaştırması

	Makale	**Veri Seti**	**Teknikler**	**Algoritma**	**Doğruluk**
1	(Çatak ve Mustaçoglu, 2017)	KDD99	Sınıflandırma	DÖ MÖ	%98
2	(Hasan ve ark., 2018)	BHP flooding attack datasets	Sınıflandırma	NB DVM KEYK DESA	%79 %88 %93 %99
3	(Alzahrani ve Hong, 2018)	Özel	Sınıflandırma	YSA	%99,98
4	(Zhu ve ark., 2018)	NSL-KDD		ESA FNN NB RO DVM	%77.8 %80.34 %75,22 %74 %73,68
5	(Sharafaldin ve ark., 2019)	CICDDoS2019	Sınıflandırma	ID3 RO	%78-Pr, %65-Rc, %69-F1 %77-Pr, %56-Rc, %62-F1

				NB	%41-Pr, %11-Rc, %5-F1
				MLR	%25-Pr, %2-Rc, %4-F1
6	(Krishnan ve ark., 2019)	CICIDS2017 NSL-KDD	Sınıflandırma	NSAE	%99,24 %99,60
7	(Ahmetoğlu ve Daş, 2019)	CICIDS2017	Sınıflandırma	YSA	%98
8	(Ateş ve ark., 2019)	MIT Darpa 2000	Sınıflandırma	GA+ DVM	%99
9	(Karataş, 2020)	CSE-CIC-IDS2018	Sınıflandırma	ADA KA RO KEYK GB LDA NB	%99,69 %99,66 %99,21 %98,52 %99,11 %90,80 %57,11
10	(Karaman ve ark., 2020)	CSE-CICIDS2018	Sınıflandırma	YSA	%99,11
11	(Elsayed ve ark., 2020)	CIC-DDoS2019	Sınıflandırma	NB KA Booster RO DVM LR DDoSNET (Önerilen)	%57 %77 %84 %86 %93 %95 %99
12	(Aytaç ve ark., 2020)	CIC-DDoS2019	Sınıflandırma	DVM	%99,7
13	(Assis ve ark., 2021)	CIC-DDoS2019	Sınıflandırma	GRU DNN ESA UKSB DVM LR KEYK GD	%99,94 %93,66 %99,45 %99,84 %99,86 %99,84 %99,89 %99,86

14	(Cil ve ark., 2021)	CICDDoS2019	Sınıflandırma	DÖ	%99,99
15	(Myneni ve ark., 2022)	CIC-DDoS2019	Sınıflandırma	DÖ	-
16	(Aydın ve ark., 2022)		Sınıflandırma	DÖ (Önerilen UKSB-CLOUD)	%99,83
17	(Liu ve ark., 2022)	CICIDS2017	Sınıflandırma	ESA DNN PSO-BPNN RO DVM	%99,16 %95,72 %90,50 %95,45 %93,43
18	(Baldini ve Amerini, 2022)	CICIDS2017	Sınıflandırma	MFB	%99,3
19	(Akgun ve ark., 2022)	CIC-DDoS2019	İkili Sınıflandırma Çoklu Sınıflandırma	ESA ESA	%99,99 %99,30
20	(Yousuf ve Mir, 2022)	NSL-KDD		MLP SMO IBK J48 DALESA (Önerilen)	%99,5 %95,73 %97,83 %97,89 %99,98
21	(Kumar ve ark., 2023)	CICDDoS2019	Sınıflandırma	KEYK YSA UKSB (Önerilen)	%89 %93 %98

2.2. SCADA ile İlgili Çalışmalar

Kakanakov ve Spasov (Kakanakov ve Spasov, 2011), çalışmalarında DDoS saldırılarında güvenli işletim sistemi olarak Linux işletim sistemlerinin daha iyi olduğundan bahsetmişlerdir. Bunun sebebi ise, ağ da ilk SYN paketini alındığında bağlantı kurmak için ayrıca bir kaynak ayırılmamaktadır. Bunun yerine SYN bağlantısı kullanılıp ACK komutu geldiğinde kaynak ayırılmaktadır. SCADA sistemlerinde ise bu sebeple Linux işletim sistemlerinin kullanılmasının siber saldırılara karşı daha güvenli olacağını savunmaktadırlar.

Markovic ve Stojanovic (Markovic-Petrovic ve Stojanovic, 2013), çalışmalarında hidroelektrik santrallerindeki SCADA sistemindeki zayıflıkları incelemişlerdir ve kablosuz bilgi sistemlerinin altyapısını güvence altına almaya çalıştılar. Çalışma, özellikle DDoS saldırılarıyla ilgili SCADA sistemi güvenlik açıklarının simülasyon tabanlı bir analizini sağlamıştır.

Markovic-Petrovic ve Stojanovic (Markovic-Petrovic ve Stojanovic, 2013), çalışmalarında hidroelektrik santrallerdeki SCADA sistemindeki birçok zayıflıkları incelediler ve kablosuz bilgi sistemlerinin altyapısını güvence altına almaya çalışmışlardır. Çalışma, OPNET (Optimize Edilmiş Ağ Mühendisliği Aracı) kullanılarak, özellikle DDoS saldırılarıyla ilgili SCADA sistemi güvenlik açıklarının simülasyon tabanlı bir analizini sağlamıştır. Oluşturdukları simülasyonda iki senaryo üzerinden ilerlemişlerdir: ağ altyapısına saldırı olmayan bir model ve DDoS saldırısı sırasında olan bir model. Simülasyon modellerinin geliştirilmesi, uzaktan kontrol işletim servislerinin performanslarının DDoS saldırıları açısından analiz edilmesini sağlamıştır. Simülasyonun sonuçları, performansta bir bozulma ve bir eksiklik olduğunu göstermediğini belirtmiştirler.

Almalawi ve arkadaşları (Almalawi ve ark., 2014), çalışmalarında su dağıtım sistemindeki siber saldırıların tespiti için KEYK yöntemi ile bir saldırı tespit sistemi önermiştir. SCADA sistemlerindeki veriler arasındaki doğruluğu otomatik algılayan bir otomatik yakınlık algılayarak kuralları çıkarma işlemini yapan bir sistem üzerinde durmuşlardır. Bu aşamada doğruluğu belirlemede KEYK ile yoğunluğu ve tutarsızlığı hesaplamışlardır. KEYK ile kendi veri setleri ve DUWWTP veri seti üzerinde çalışmalarının sonucunda saldırı tespitinde %92,86 başarı elde etmişlerdir.

Shitharth ve Winston (Shitharth ve Winston, 2015), çalışmalarında Karışık Mod Algılama (PMD) yöntemini önermişlerdir. Önerdikleri yöntem ile güvenlik araçları

(Wireshark, tcpdump) arasındaki karşı önlem karşılaştırması, DDoS ile Sniffing (Koklama) saldırıları ile analiz etmişlerdir. Bu analizi SCADA ağına uygun güvenlik sistemi, bant genişliği tüketimi ve trafik analiz kapasitesi olarak analiz etmişlerdir. Önerdikleri simülasyon çalışmasında, bant genişliği kullanımının minimum olduğunu dolayısıyla, DDoS ve Sniffing paketlerini tespit ettikten sonra bile, hesaplama için yüksek bant genişliği kullanarak SCADA sistemini geciktirmediğini belirtmişlerdir.

Hoyos ve arkadaşları (Hoyos Ll ve ark., 2016), çalışmalarında DDoS saldırılarının tespiti için bir prototip geliştirmişlerdir. Bunun için DVM kullanmışlardır. Ağ trafiğini yakalayan, HTTP başlıklarını filtreleyen, verileri operasyonel değişkenlere göre normalleştiren Destek Vektör Makineleri (DVM) tarafından denetlenen bir öğrenme modeli kullanarak DDoS saldırılarını algılama prototipi geliştirmişlerdir. DDoS DVM prototipinin yüksek algılama doğruluğuna (%99) sahip olduğunu, geleneksel algılama modellerine kıyasla yanlış pozitif ve yanlış negatif oranlarında azalma olduğunu göstermişlerdir.

Shirazi ve arkadaşları (Shirazi ve ark., 2016), Mississippi Eyalet Üniversitesi laboratuvarındaki bir gaz boru hattı SCADA sisteminde oluşan veri setine denetimli ve denetimsiz makine öğrenmesi algoritmaları uygulayarak, özellikle anomali tespiti tekniklerini değerlendirmek için çalışmalarını gerçekleştirmişlerdir. Veri seti toplamda dört kategoriye ayrılmış ve yedi farklı türde anomali ağ trafiği içermektedir. Bu anomali türleri, "tepki enjeksiyonu", "keşif", "hizmet reddi" ve "komut enjeksiyonu" olarak dört kategori altında birleştirilmiş ve ağda saldırı olup olmadığı incelenmiştir. Ayrıca çalışmada, denetimli ve denetimsiz öğrenme algoritmaları arasında bir performans karşılaştırması yapılmıştır. Çalışma sonucunda K-Means %56.80, PCA-SVD %17.14, NB %90.36, GMM %45.16 başarı oranları elde edilmiştir.

Nazir ve arkadaşları (Nazir ve ark., 2017), çalışmalarında Modbus protokolünün siber saldırılara karşı savunmasız olduğunu belirtmişlerdir. Bu çalışmada SCADA sistemi güvenlik açıklarını ortaya çıkarmak için araçları ve tekniklerini incelemişlerdir. Buna göre çalışmada DDoS saldırılarının SCADA sistemlerine yönelik en tehlikeli ve yaygın siber saldırılar arasında yer aldığını belirtmişlerdir.

Alhaidari ve AL-Dahasi (Alhaidari ve AL-Dahasi, 2019), yaptıkları çalışmada SCADA sistemlerinin DDoS saldırılarına karşı daha güvenlikli olması için bir makine öğrenmesi yöntemlerinden KA, RO ve NB yöntemlerini kullanmışlardır. KDD'Cup99 veri setini kullanarak performansları değerlendirilmiştir. Bu veri setine ait 6 saldırı türü

kullanılmıştır. NB %99,99 oranında başarı elde etmiştir. En düşük başarıyı RO %97,74 oranında almıştır.

Yang ve arkadaşları (Yang ve ark., 2019), çalışmalarında SCADA sistemlerinin UDP taşma saldırılarına; TCP RST, SYN taşması ve DNP3 hedefli ARP spoofing saldırılarına karşı derin öğrenme tabanlı bir ağ saldırı tespit sistemi önermiştir. Bu amaçla, enerji dağıtım sistemi test yataklarından DNP3 protokolü aracılığıyla toplanan trafik verileri kullanarak veri seti oluşturmuşlardır. Çalışmalarında, Evrişimli sinir ağları (ESA) algoritmasını kullanarak analizleri gerçekleştirmişlerdir. Bu algoritma, SCADA trafiğinin zamansal kalıplarını tanımlayarak ağ saldırılarının mevcut olduğu zaman pencerelerini belirlemektedir ve ESA ile elde ettikleri başarı oranı % 99.38 olarak tespit etmişlerdir.

Marino ve Zio (Marino ve Zio, 2021), çalışmalarında karmaşık ağ modellemesi modülü ile fiziksel gaz boru hattı iletim ağını oluşturmak ve normal koşullar altında ve DDoS saldırısı altında SCADA sisteminin yanıtını simüle ederek önerilen analiz yöntemi ile, matematiksel teorik modelleri ve kritik altyapıların karmaşık fiziksel gerçekliğini ilişkilendirmeyi amaçlamışlardır ve SCADA sistemi simülasyonu üzerinde farklı modüller geliştirerek güvenilirliğini test etmişlerdir. Bu bağlamda gaz boru hattı iletim ağlarının esnekliğini analiz etmek için bütünleşmiş bir çerçeve geliştirmişlerdir.

Polat ve arkadaşları (Polat ve ark., 2022), çalışmalarında DDoS saldırılarını tespit etmek için UKSB ve GRU'nun paralel kullanıldığı derin öğrenmeye dayanan yeni bir yaklaşım önermişlerdir. Önerilen yöntem, TSA tabanlı UKSB ve GRU modellerinin eğitiminden ve eğitilen mimarilerin UKSB ve GRU katmanlarından çıkarılan özniteliklerin DVM yöntemi ile sınıflandırılmasından oluşmaktadır. Bu çalışma da deneysel ortamda toplanan bir veri setini kullanılarak, %97.62 sınıflandırma doğruluğu elde edilmiştir. Önerilen yöntem çeşitli DVM çekirdek işlevlerine sahip diğer yöntemlerden daha iyi performans gösterdiği sonucu elde edilmiştir.

Bu çalışmaların genel sonucuna bakıldığında, alınacak her önlemin SCADA sistemler için hayati önem taşıdığı görülmektedir. Kalınabilecek herhangi bir siber saldırının sistemleri kötü etkilemesi birçok kayıp ile sonuçlanmaktadır. Çalışmalar da derin öğrenme yöntemlerinin bu sistemlerde yavaş yavaş yerini almaya başlaması ve SCADA sistemlerinin siber saldırılar karşısında güvenliksiz olması bu çalışmanın ana motivasyonu olmuştur. Literatürde yapılan çalışmalardan farklı olarak SCADA sistemlerine laboratuvar ortamında düzenlenecek DDoS saldırılarından oluşturulacak bir veri seti ile ve bu veri setinin derin öğrenme yöntemleri ile analizinin yapılması

bakımından ayrılmaktadır. Çizelge 2.2'de SCADA sistemlerde siber saldırılarının literatür karşılaştırması verilmiştir.

Çizelge 2.2. SCADA sistemlerde siber saldırılarının literatür karşılaştırması

	Makale	Veri Seti Öznitelikler Teknikler Açıklama	Algoritma	Doğruluk
1	(Kakanakov ve Spasov, 2011)	Linux İşletim sistemlerinin DDoS saldırılarına karşı daha güvenli olduklarını belirtmişlerdir.	-	-
2	(Almalawi ve ark., 2014)	Kendi veri setleri DUWWTP üzerinde çalışmışlardır.	KEYK	%92,86
3	(Markovic-Petrovic ve Stojanovic, 2013)	SCADA sisteminin zayıflıklarını incelemişlerdir.	OPNET	-
4	(Shitharth ve Winston, 2015)	Saldırı analizini bir simülasyon yöntemi ile yapılması üzerine çalışmışlardır.	PMD	-
5	(Hoyos Ll ve ark., 2016)	DDoS saldırı tespiti için bir prototip geliştirmişlerdir.	DVM	%99
6	(Shirazi ve ark., 2016)	Anomali tespitini farklı modeller ile gerçekleştirip performans değerlendirmesini kendi veri setlerinde yapmışlardır.	K-Means PCA-SVD NB, GMM	%56.80 %17.14 %90.36 %45.16
7	(Nazir ve ark., 2017)	Modbus protokolünün siber saldırılara karşı zayıf olduğunu incelemişlerdir.	-	-
8	(Alhaidari ve AL-Dahasi, 2019)	KDD'Cup99 veri seti kullanarak performans değerlendirilmiş, SCADA sistemlerinin güvenliğini test etmişlerdir.	KA RO NB	 %97,74 %99,99
9	(Yang ve ark., 2019)	SCADA sitemlerine karşı düzenlenen UDP taşma saldırılarına kendi veri setlerini oluşturarak derin öğrenme yöntemini denemişlerdir.	ESA	% 99.38
10	(Marino ve Zio, 2021)	DDoS saldırıları normal koşullar ve saldırı olduğu zamanda SCADA sistemini simüle edilmiştir.	-	-
11	(Polat ve ark., 2022)	UKSB ve GRU yöntemlerini paralel kullanarak özellik çıkarmışlardır.	DVM	%97,62

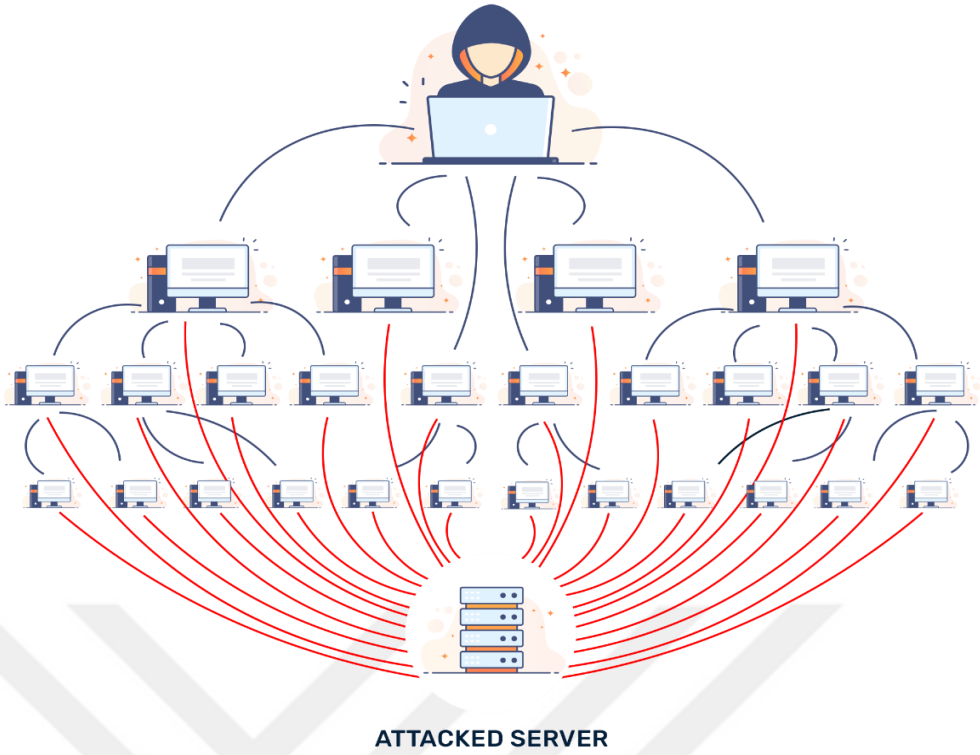
3. DDOS SALDIRILARI VE SCADA SİSTEMLERİ

Bu bölüm iki başlık altında ele alınmıştır. Bunlar sıra ile; birinci bölümde DDoS saldırılarının neler olduğundan, türlerinin neler olduğu ve bu saldırıların uygulanma şekillerinden, ikinci bölümde ise SCADA sistemleri hakkında detaylı bilgi verilerek siber saldırılar karşısında sistemlerin nasıl etkilendiği detaylı olarak açıklanmıştır.

3.1. Dağıtık Hizmet Dışı Bırakma Saldırıları (DDoS)

DDoS (Distributed Denial of Service) saldırıları, internette bir web sitesini ya da sunucuyu trafiğinin büyük kısmının bir anda gelecek olmasından dolayı kullanılamaz hale getirme amacıyla yapılan saldırılardır.

DDoS saldırıları, bir web site veya ağı kullanım dışı hale getirmek için ağ trafiğini aşırı yükleyen bir tür siber saldırı türüdür. Bu saldırılar, birçok farklı bilgisayardan aynı anda yapıldığı için "dağıtılmış" olarak adlandırılır. Bu saldırılar genellikle çok sayıda bilgisayar veya cihaz tarafından yapılmaktadır ve bu cihazların topluluğuna "botnet" adı verilmektedir. Bu cihazların bir hedef sunucuya çok sayıda istek göndermesiyle, hedef sunucuyu aşırı yüklemek ve çökertmek amaçlanmaktadır (Lau ve ark., 2000). DDoS saldırıları erişilebilirliği engellemeyi amaçlayarak genellikle hizmete bağlanması gereken kullanıcıların hizmet erişimini durmayı hedeflemektedirler. Siber saldırılara maruz kalan ağ trafiği, kullanıcıların istenen hizmetlere ulaşmasını engelleyen ağlar üzerinde olumsuz etkilere neden olmaktadır (Jasiul ve ark., 2014). Güvenlik duvarları ve saldırı tespit sistemleri, çeşitli ağ saldırılarını önlemek için yaygın olarak kullanılmaktadır. Bu tür araçlar genellikle imza tabanlı güvenlik mekanizmalarını kullanır ve yeni ağ paketi modelleri veya kötü niyetli ağ trafiği değişiklikleri ile çalışamazlar. Sınıflandırma modelleri kullanılarak saldırılar daha erken tespit edilip ayrıştırılabilir. Dağıtılmış Hizmet Reddi Saldırıları (DDoS), bir hizmetin kullanıcılar için kullanılabilirliğini önlemeye veya azaltmaya odaklanır (Catak ve Mustacoglu, 2019). DDoS saldırılarının yapısı Şekil 3.1.'de gösterilmektedir.



Şekil 3.1. DDoS saldırı yapısı (Academy, 2022)

Saldırganın bir DDoS saldırısı başlatması için, bir botnet aracılığıyla, ağdaki tüm zombilere veya botlara aynı anda, genellikle uzun bir süre boyunca hedef sunucunun IP adresine trafik gönderme komutu vermesi gerekmektedir. Bu zombiler veya botlar normal makineler olma eğiliminde olduğundan, botnet tarafından kontrol edilen trafiği normal internet trafiğinden ayırmak genellikle zordur. DDoS saldırıları, saldırının türüne göre yedi katmanlı Açık Sistemler Ara Bağlantı (OSI) modelinin farklı katmanlarında gerçekleştirilebilir. Daha yaygın saldırılardan bazıları şunlardır:

- Katman 3 (Ağ Katmanı): İnternet Kontrol Mesajlaşma Protokolü (ICMP) taşmaları
- Katman 4 (Aktarım Katmanı): SYN taşmaları ve UDP taşmaları
- Katman 7 (Uygulama Katmanı): HTTP taşmaları

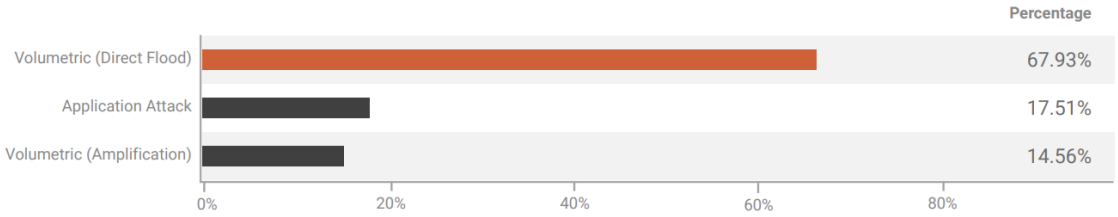
DDoS saldırıları yalnızca tek bir katmana saldırmaz, birden çok katmandaki saldırıları da birleştirir. DDoS saldırıları saldırganın amacına göre değişiklik göstermektedir. Buna bağlı olarak birçok DDoS saldırı türü mevcuttur. Bu tür saldırılarda kötü ağ yönetimi, bant genişliği ve kolayca bulunabilen saldırı araçları vb. gibi durumlar saldırganların motivasyonu olmaktadır.

3.1.1. DDoS saldırı yöntemleri

DDoS saldırılarını düzenleyen saldırganlar genel olarak üç çeşit DDoS saldırı yöntemini kullanmaktadırlar: hacimsel, protokol ve uygulama saldırıları. Bu saldırı türleri Şekil 3.2.'de gösterilmektedir.

Şekil 3.2. DDoS saldırı yöntemleri.

2022 yılında yayınlanan 2022 İlk Yarı DDoS İstatistik Raporu'na göre (Nexusguard, 2022), DDoS saldırılarının dağılımı Şekil 3.3.'te verilmiştir.



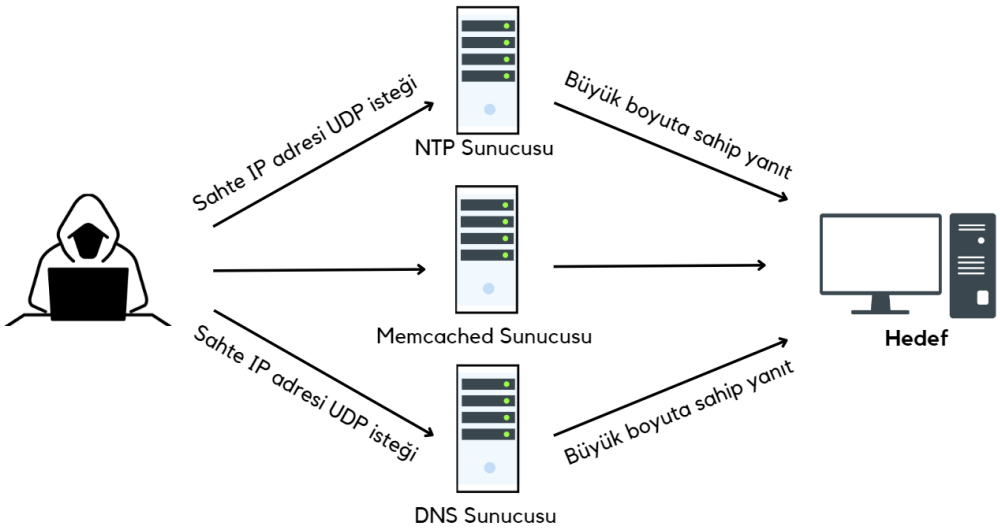
Şekil 3.3. Saldırı türleri yüzde dağılımları

Günümüzde de saldırı türleri karşılaştırıldığında 2022'nin ilk yarısında kaydedilen toplam saldırıların %67,93'ünün Volumetrik (Doğrudan Taşma / Sel) saldırılar, %17,51'i Uygulama saldırıları ve saldırıların kalan %14,56'sı hacimsel (Amplifikasyon) saldırılar olduğu Şekil 3.3.'te verilen saldırı türlerinden yine en çok volümetrik saldırıların yapıldığı görülmektedir. Saldırı yöntemleri aşağıda detaylı olarak açıklanmıştır.

3.1.1.1. Volümetrik saldırılar

Hacimsel saldırılar ya da amplification (kuvvetlendirmeli) saldırılar olarak ifade edilen volümetrik saldırılar bir web sunucusu ile İnternet arasındaki bant genişliğini tüketilmesi ile meydana gelir. Bir web sunucusu ile İnternet arasındaki tüm bant genişliği, kötü niyetli bir volümetrik saldırı tarafından tükendiğinde, normal ağ trafiği için artık kullanılabilir bir bant genişliği kalmaz.

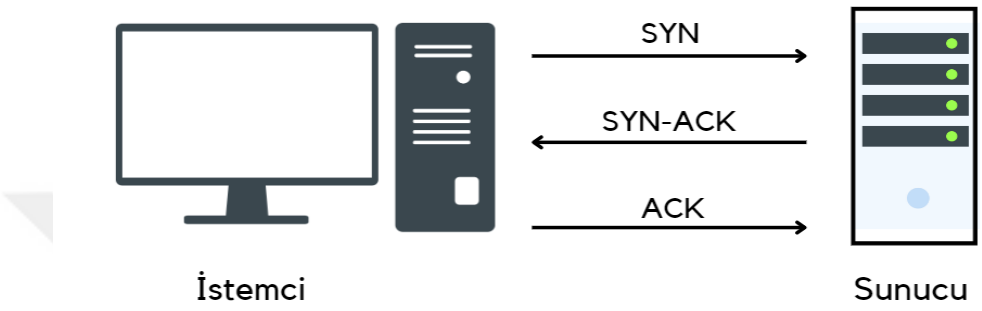
DNS (Domain Name Server- Alan Adı Sistemi) Amplification saldırıları, volümetrik saldırıların en yaygın türlerinden biridir. Bir saldırgan, bir zombi makinesi kullanarak bir DNS sunucusunu sorgulamak için hedef sunucusunun IP adresini taklit eder. DNS sunucuları, hedef sunucusu gerçekte bir istekte bulunmamış olsa bile yanıtları hedef sunucusunun IP adresine gönderir. Saldırgan, bir botnet'e komut vererek DNS sorgularını büyük ölçüde artırabilir, hedef sunucusunu büyük miktarlarda istenmeyen DNS yanıtlarıyla doldurabilir ve web sunucusu ile İnternet arasındaki bant genişliğini tüketerek performansını bozabilmektedir. Volümetrik saldırılara; TCP/UDP Flood, DNS/NTP/Mamcached Amplifikasyonu saldırıları örnek olarak verilebilir. Şekil 3.4'te volümetrik saldırı yapısı gösterilmiştir.



Şekil 3.4. Volümetrik saldırı yapısı

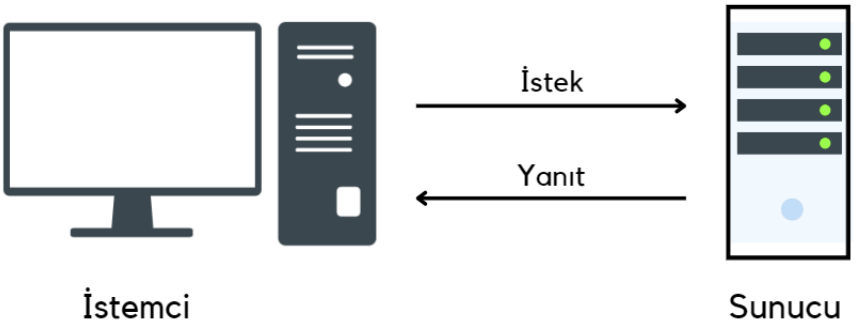
3.1.1.2. Protokol saldırıları

Protokol saldırıları genel olarak OSI referans modelinin 3. Katmanı Ağ katmanını ve 4. Transfer katmanlarını hedeflemektedir. Örneğin, bir SYN flood saldırısı, bir iletim kontrol protokolü (TCP) bağlantısı kurmak için gereken üç yollu el sıkışma sürecinden yararlanmaktadır.



Şekil 3.5. SYN flood saldırısı yapısı.

Zombi makineler, bir SYN paketi göndererek el sıkışma işlemini başlatır (Şekil 3.5). Ancak, zombi makineler anlaşma sürecini tamamlamaya devam etmez, portları meşgul ve meşru istekleri işleyemez durumda bırakarak sunucuyu sürekli meşgul eder. Bir UDP taşma saldırısında, zombi makineler hedef sunucudaki rastgele bağlantı noktalarına büyük miktarda UDP datagramı gönderir. Şekil 3.6'da UDP bağlantısı gösterilmektedir.

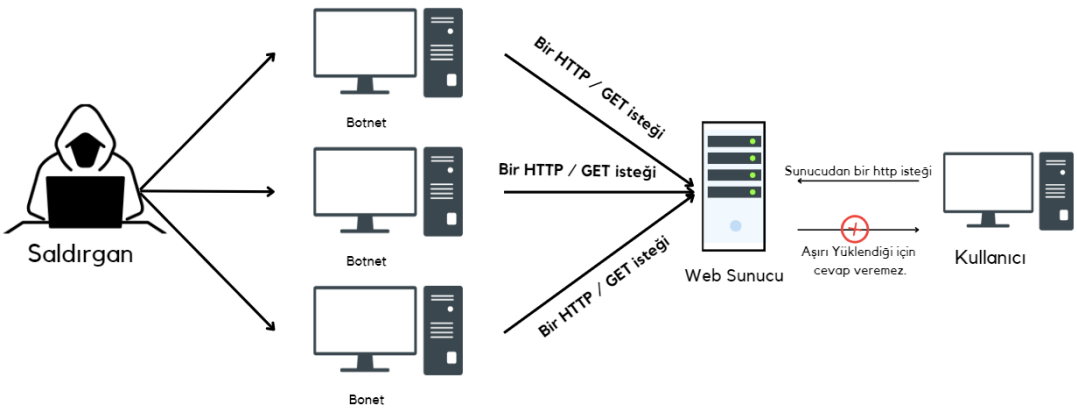


Şekil 3.6. UDP bağlantısı yapısı

Şekil 3.6'da gösterilen yapıya göre bu, web sunucusunun o anda çalışmakta olan ve bu datagramları bu bağlantı noktalarında alması gereken uygulamaları aramasına neden olur. Datagramlar web sunucusunda çalışan bir uygulama tarafından talep edilmediğinden, sunucu, göndericiye hedefin ulaşılamaz olduğunu bildirmek için bir ICMP paketi ile yanıt verecektir. Yeterince büyük miktarda gelen UDP datagramı ile sunucu, ICMP paketleriyle yanıt vererek kendini tüketerek ve böylece sunucuyu felce uğratmaktadır. Protokol saldırılarına; SYN/SYN-ACK/ACK Flood, Ping of Death gibi saldırılar örnek olarak verilebilir.

3.1.1.3. Uygulama saldırıları

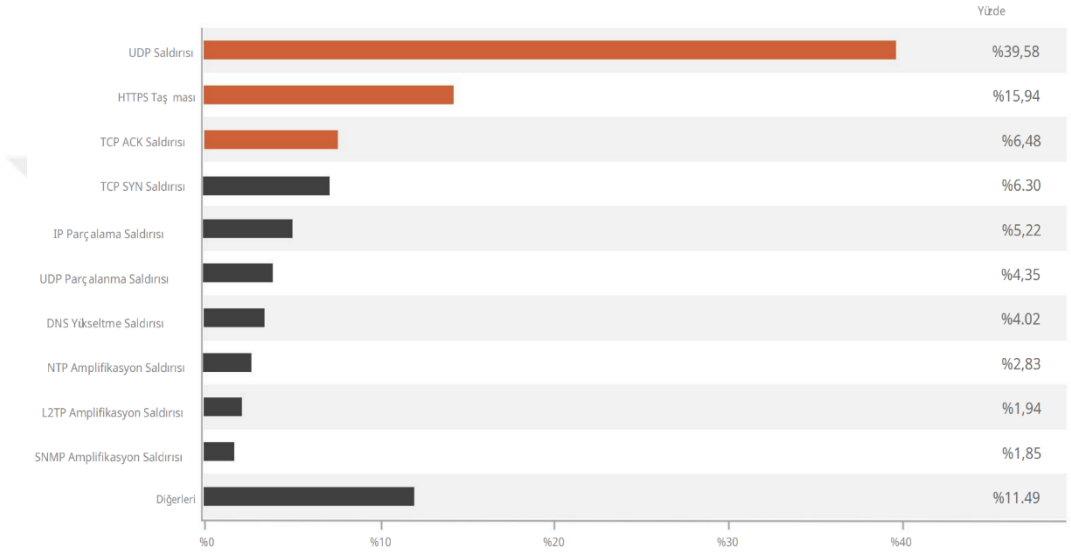
Uygulama saldırıları genellikle HTTP isteklerinin gönderilmesi yoluyla gerçekleştirilirler. Bir kullanıcı bir web uygulamasından bir web sayfası istediğinde, web sunucusunun genellikle talebi yerine getirmek için birkaç komut dosyası yürütmesi ve veritabanı sorguları çalıştırması gerekir. Bir web sunucusunun bir HTTP isteğini yerine getirmesi, bir istemcinin HTTP isteği yapmasından zahmetlidir. Saldırganlar, bir botnet'i kontrol ederek, sunucudaki bir web uygulamasını HTTP istekleri göndermelerini sağlayarak bir web sunucusunun hesaplama kaynağını daha kolay alt edebilmektedir. Temel olarak, HTTP saldırıları, birçok kullanıcının bir web tarayıcısındaki yenile düğmesine birden çok kez basmasına eşdeğerdir. Şekil 3.7'de bir http saldırısı yapısı gösterilmektedir. Uygulama saldırılarına; HTTP, HTTPS, DNS ve SMTP servislerine yapılan taşma saldırıları örnek olarak verilebilir.



Şekil 3.7. Bir HTTP saldırısı yapısı

3.1.2. Sık kullanılan DDoS saldırı çeşitleri

DDoS saldırılarında en çok flood yani sel saldırıları, yansıma saldırıları ve kuvvetlendirmeli saldırıları yer almaktadır. Aşağıda siber saldırılarda en çok kullanılan DDoS saldırı çeşitleri açıklanmıştır. Nexusguard'ın 2022 1.Yarı DDoS Saldırı İstatistikleri Raporu'na (Nexusguard, 2022) göre, DDoS Saldırı türlerinin 2022'de artış oranları gösterilmiştir (Şekil 3.8).



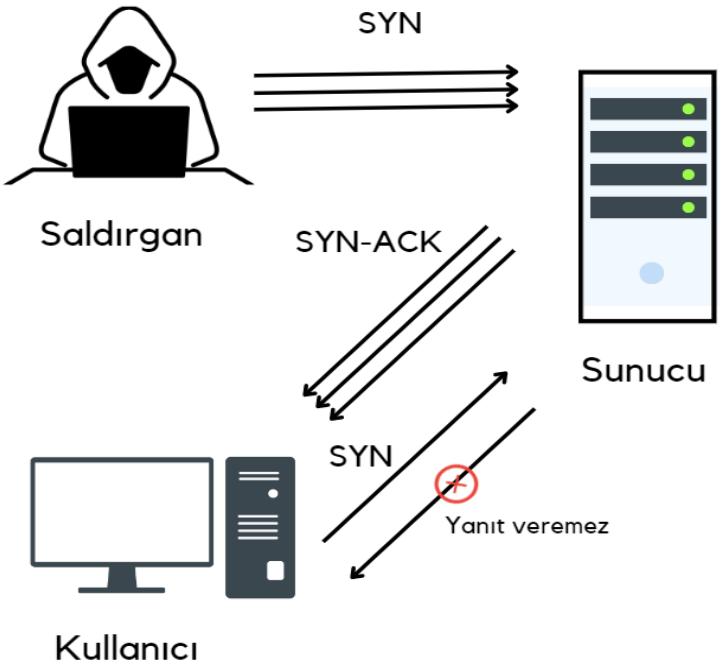
Şekil 3.8. 2022 Yılı ilk yarısı DDoS saldırı türleri oranları

Günümüzde sıklıkla tercih edilen DDoS saldırı türleri UDP, HTTP Flood, TCP ACK, TCP SYN saldırıları olarak ilk sıralarda olduğu görülmektedir (Şekil 3.8). Rapora göre, 2022'nin ilk yarısında sırasıyla %39,58 ve %15,94 ile UDP saldırısı ve HTTPS taşma saldırısı baskın iki saldırı türü olurken, TCP ACK saldırıları %6,48 ile üçüncü sırada yer almıştır.

3.1.2.1. TCP SYN flood saldırısı

Bu tür bir saldırı, hedef sisteme gönderilen fazla sayıda TCP (Transmission Control Protocol) bağlantı isteği ile yapılır. TCP haberleşmelerinde sunucu ile istemci arasında veri alışverişinden önce 3 yollu el sıkışma (3-way handshake) olayı gerçekleşmektedir. Buradaki amaç güvenilir bir bağlantı üzerinden verilerin transferini sağlamaktır. Syn seli saldırısı bu el sıkışmasında araya girer ve saldırı bu şekilde başlar

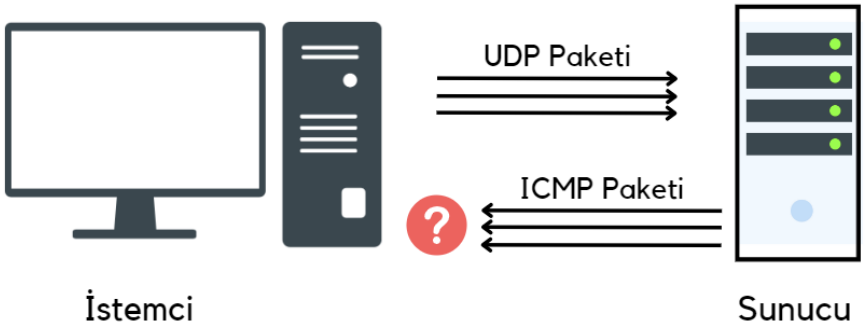
(Imperva, 2023a). Syn seli saldırı atağında temel amaç sunucuya aynı anda çok sayıda isteği cevap vermesini beklemeden göndererek bağlantı sağlamasını önlemektir (Şekil 3.9). Syn seli saldırısı bir DoS (Denial of Service) saldırısı olduğundan eğer tedbir alınmazsa sistemde sorunlara yol açabilmektedir (Prakash ve Priyadarshini, 2018). Sistem, bu istekleri yanıtlayamayacağı için tüm bağlantı noktalarının kullanımını engeller.



Şekil 3.9. SYN flood DDoS saldırı

3.1.2.2. UDP flood saldırısı

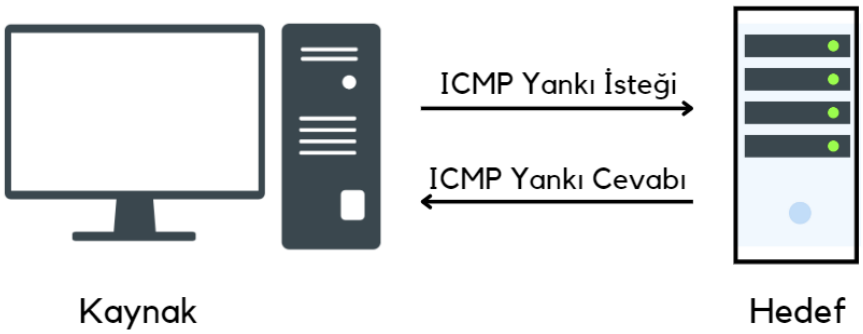
Bu saldırı, hedef sisteme rastgele veya yanıtlama gerektirmeyen UDP paketlerinin gönderilmesi ile yapılır. UDP paketlerinin gönderilmesinde TCP bağlantısındaki gibi 3 yollu el sıkışma işlemi olmadığından paketlerin karşı tarafa teslim edilip edilmediği bilgisi alınmaz (Imperva, 2023b). Sistem, bu paketlerin işlenmesi için yeterli kaynağa sahip olmayacağından performansını yavaşlatabilir veya tamamen bozabilir. Şekil 3.10'da UDP seli saldırı yapısı gösterilmektedir.



Şekil 3.10. UDP flood DDoS saldırısı

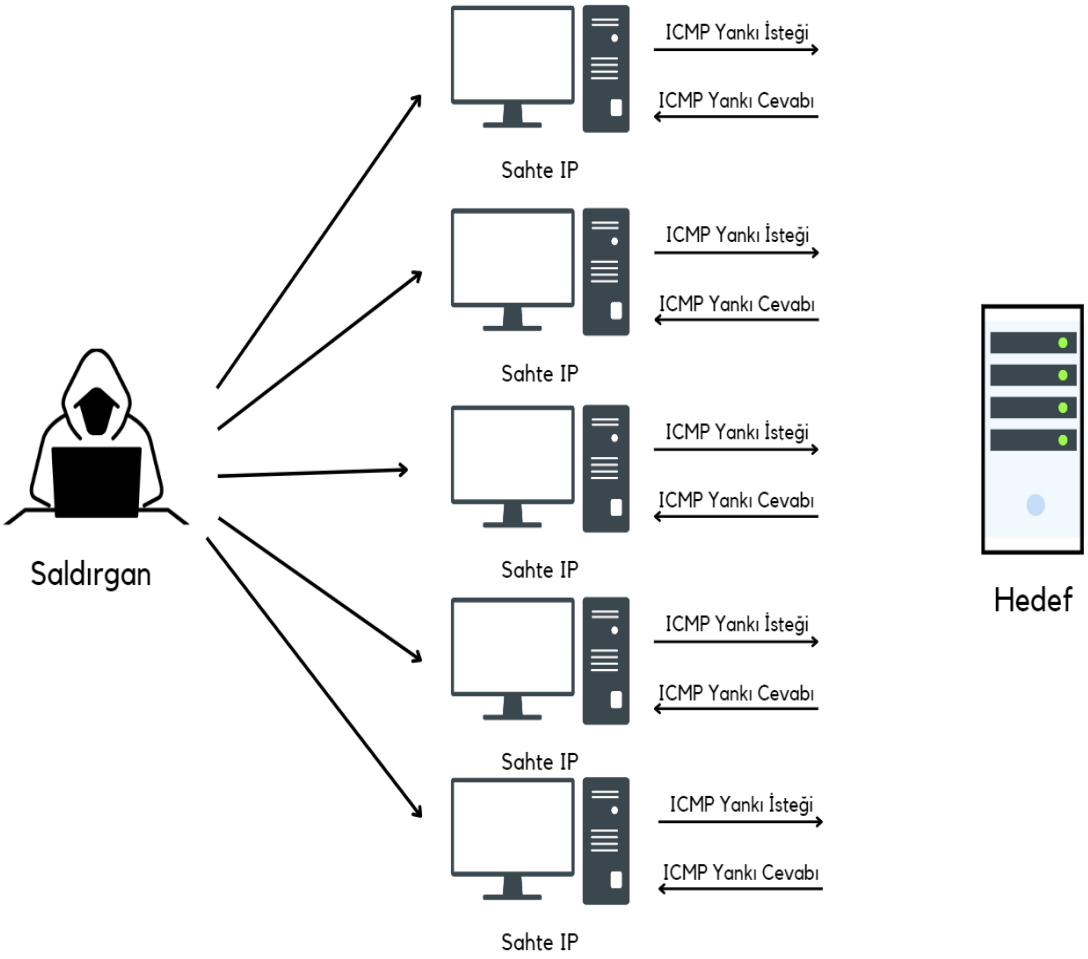
3.1.2.3. ICMP flood saldırısı

Bu saldırı, hedef sisteme fazla sayıda ICMP (yankı isteği- ping) paketinin gönderilmesi ile yapılır (Şekil 3.11). Bir sunucuya ping isteği gönderildiğinde ICMP paketleri devreye girer. Sistem, bu paketlerin yanıtlanması için yeterli kaynağa sahip olmayacağından performansını yavaşlatabilir veya tamamen bozabilir.



Şekil 3.11. ICMP paketlerinin işleyişi

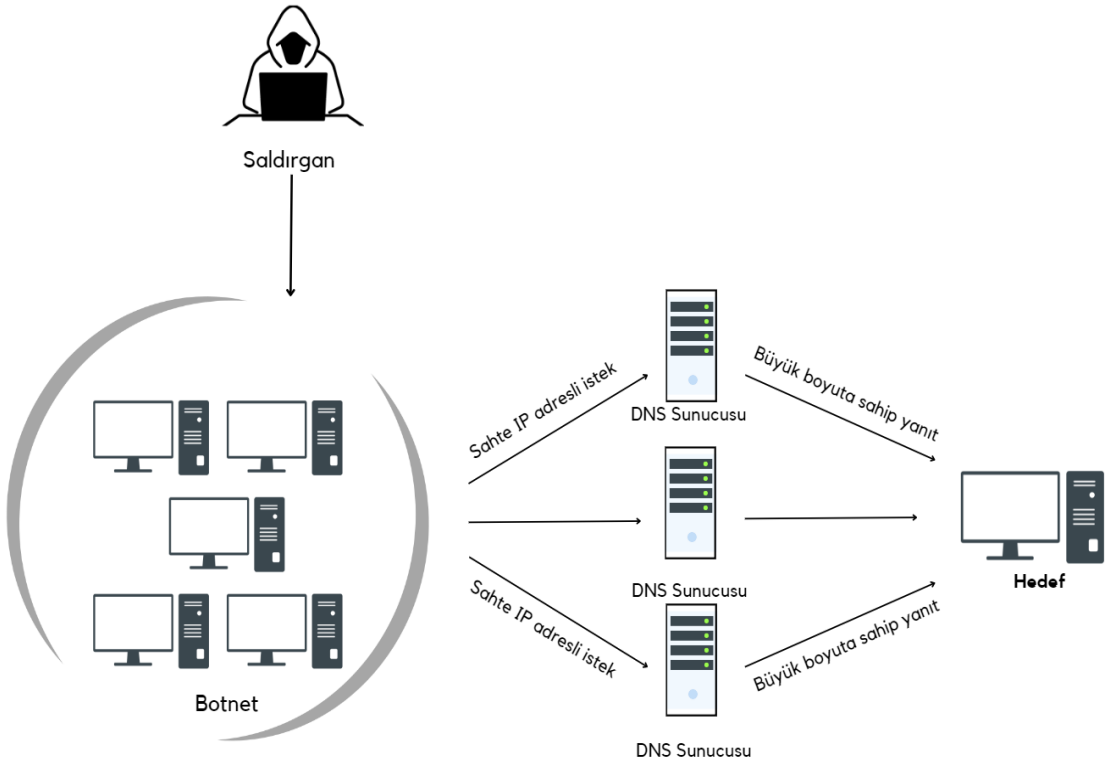
ICMP Flood saldırısı, çok fazla sayıda IP adresi kaynakları kullanılarak birçok sahte ICMP paketi gönderilerek oluşturulan bir saldırıdır. Bu saldırıdaki amaç, ağa ICMP yankı istekleri ile doldurulup cevap vermesinin engellenmesidir (Şekil 3.12). Hedef sunucu gelen sahte ICMP paketi isteklerine yanıt vermeye çalıştığından kaynaklarını tüketerek sunucunun performansı bu şekilde düşürülmüş olur (Akamai, 2023). ICMP Flood saldırısında saldırganlar hedef IP adresinin sanki kaynak adresi gibi gösterildiğinden dolayı çok sayıda IP paketi gönderilmesinden dolayı ağın bant genişliği tüketilir ve bu yüzden gerçek paketlerin de hedeflerine ulaşması önlenir.



Şekil 3.12. ICMP DDoS saldırı yapısı

3.1.2.4. DNS amplification saldırısı

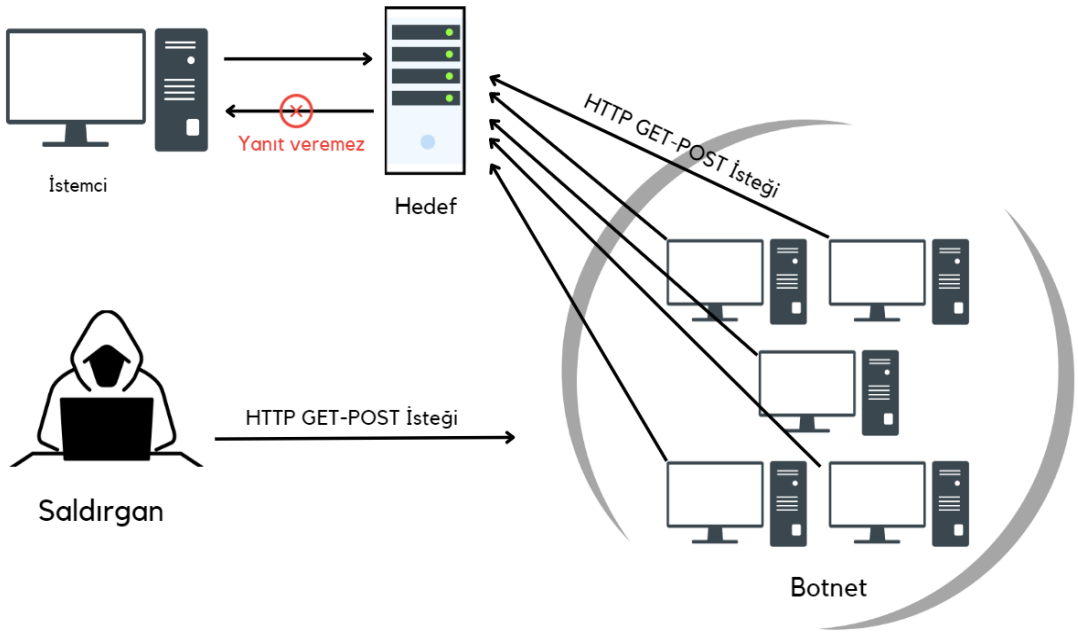
DNS Amplification saldırısı, hedef sistem üzerinde bulunan bir DNS sunucusunun güçsüz tarafından kullanılır. Saldırganın açık DNS sunucularını manipüle ederek kullandığı iki adımlı bir DDoS saldırısıdır. Saldırgan, DNS sunucularına sahte IP adresleri kullanarak büyük istekler gönderir. DNS sunucusu daha sonra isteğe yanıt vererek hedefe bir saldırı oluşturur (Netscout). Bu saldırıların boyutu sahte istekten daha büyüktür ve hedef sunucuya büyük miktarda trafik gitmesiyle sonuçlanır (MacFarland ve ark., 2017). Şekil 3.13'te DNS amplification saldırısının yapısı gösterilmektedir. Bu şekilde hedefteki verilere erişim ve kullanımı engellenmiş olmaktadır.



Şekil 3.13. DNS kuvvetlendirmeli DDoS saldırısı yapısı

3.1.2.5. HTTP flood saldırısı

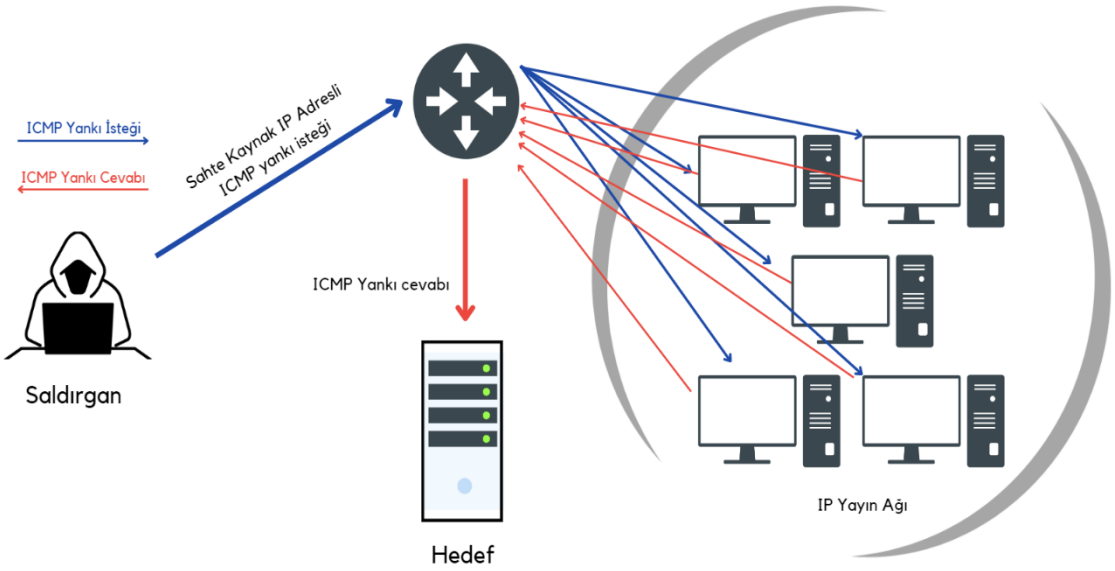
Bu tür saldırı, hedef sistem üzerindeki bir web sunucusunu hedef almaktadır. Genel olarak, HTTP flood saldırılarının amacı, bir web sunucusunu aşırı yüklemek ve web sunucusunu yavaşlatmaktır. Saldırganlar, normal kullanıcılar gibi davranan trafik oluşturmak için botnet'leri kullanır. İletim hızlarının ve istek sayılarının genellikle gerçek kullanıcıların isteklerinden daha yüksek olduğu, normal ve kötü niyetli trafiği sınıflandırmayı zorlaştıran bağlantılar oluşturur. Bu şekilde bant genişliği gibi sunucu kaynaklarının normalden fazla tüketilmesine neden olur. Sisteme erişmeye çalışan kullanıcıların bağlantılarının zarar görmesi, sunucunun isteklere yeterince yanıt vermemesine ve bu yüzden hizmetin kullanılamaz hale getirmesine neden olmaktadır (do Nascimento ve ark., 2021). Saldırganın botnet ağı oluşturarak bu botnet ağının hedef sunucuda çok fazla HTTP GET-POST isteklerine yetişemediğinden kullanıcının gerçek isteğine yanıt veremez ve hizmet engelli saldırgan tarafından gerçekleştirilmektedir (Şekil 3.14).



Şekil 3.14. HTTP DDoS flood saldırısı yapısı

3.1.2.6. Smurf DDoS saldırısı

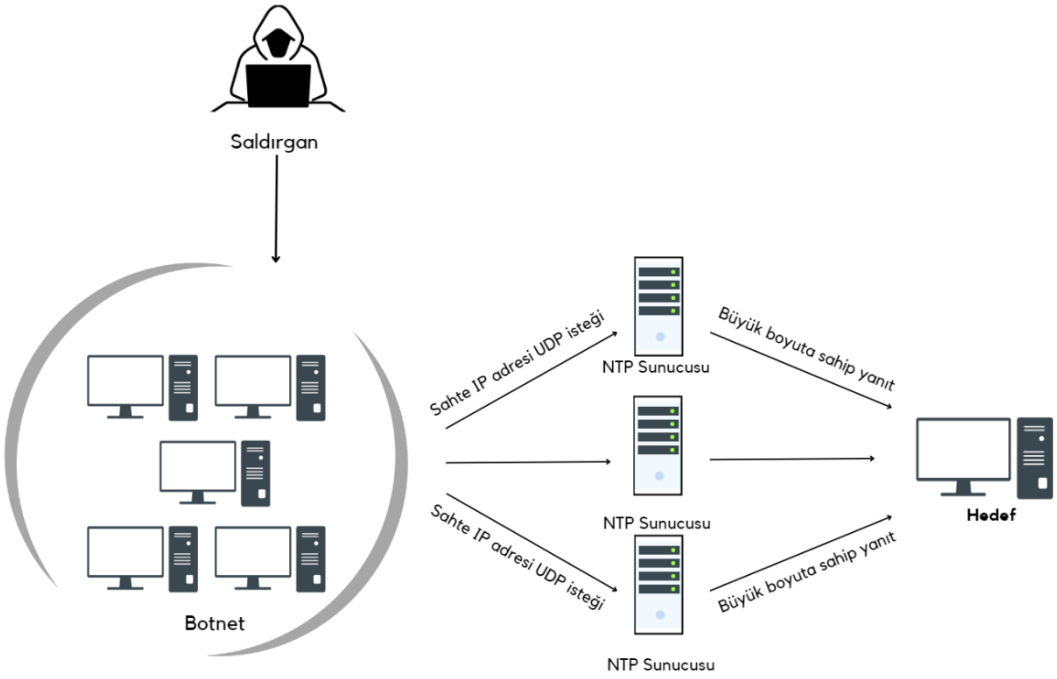
Smurj saldırısı, saldırganın IP yayın adresine büyük miktarda ICMP yankı isteği göndermesini içermektedir. ICMP yankı paketleri, hedefin kaynak adresi ile belirtilir ve IP yayın ağındaki bilgisayarlar, ICMP yankı isteklerini kabul ederek ve hedefe bir yankı yanıtıyla yanıt vermektedir. Bu, trafiği yanıt veren ana bilgisayar sayısıyla çarpıp IP yayın ağında, potansiyel olarak her bir ICMP paketine yanıt verecek yüzlerce makine oluşturulabilmektedir (Lau ve ark., 2000). Bu tür saldırılardan zarar gören iki taraf yönlendiriciler ve hedef zarar görmektedir. Şekil 3.15'te saldırgan tarafından sahte kaynak IP adresinden gönderilen ICMP yankı isteği ile IP yayın ağına istek gönderildiği ve geri gelen istekleri yönlendiricinin sunucuya göndermesi ile sunucunun bu isteklere cevap verilemediği gösterilmektedir. Bu saldırının sonucunda hedefin sunucunun yanıt veremeyeceği sayıda ping isteği olacağından dolayı hedef sunucu hizmet dışı kalacaktır.



Şekil 3.15. Smurf DDoS saldırısı yapısı

3.1.2.7. NTP amplification (kuvvetlendirmeli) DDoS saldırısı

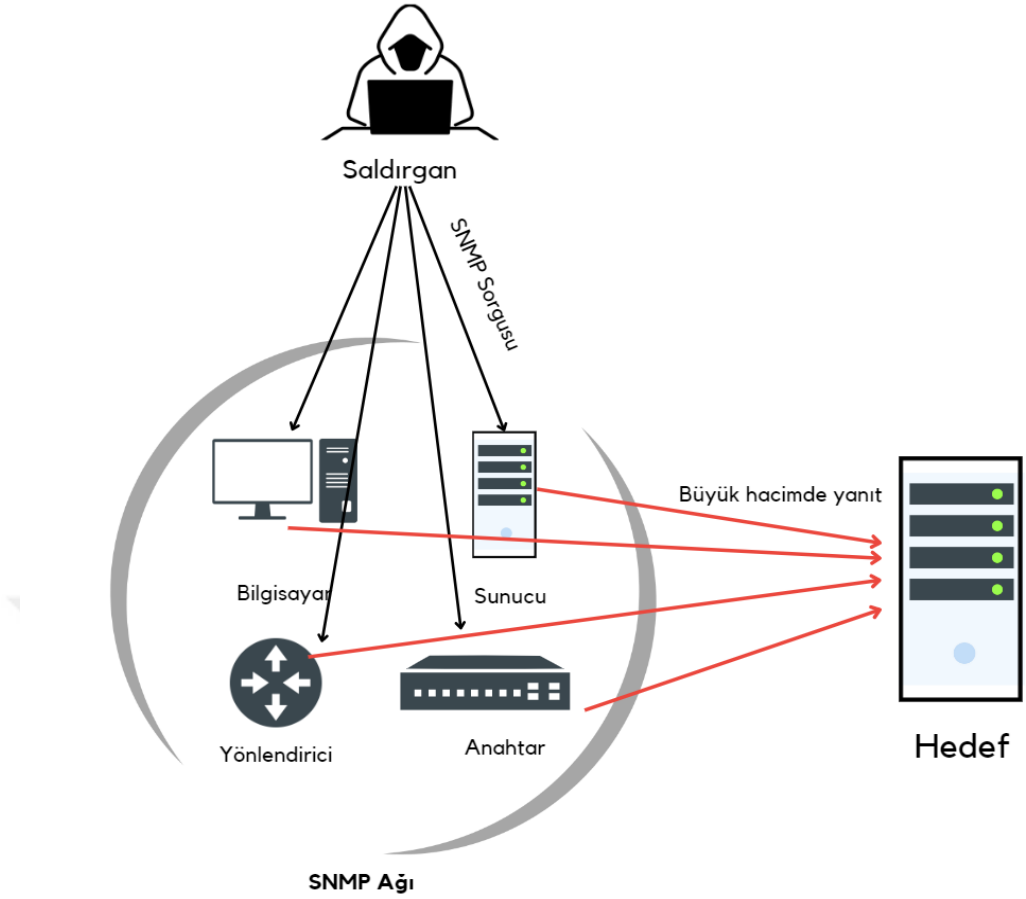
Bir Ağ Zaman Protokolü (NTP) Amplifikasyon saldırısı, kurban bir sistemi UDP trafiğiyle boğmak için genel olarak erişilebilen NTP sunucularının kullanımına dayanan, bir DDoS saldırısıdır (Alert, 2020). NTP hizmeti, yöneticilerin bağlı istemcilerin trafik sayımları için sunucuyu sorgulamasına izin veren bir izleme hizmetini destekler. Temel saldırı tekniği, bir saldırganın savunmasız bir NTP sunucusuna, kurbanın adresiymiş gibi davranan kaynak adresiyle bir "tek listeye alma" isteği göndermesinden oluşur. Ek olarak, yanıtlar geçerli sunuculardan gelen meşru veriler olduğundan, bu tür saldırıları engellemek özellikle zordur. NTP ve diğer tüm UDP tabanlı yükseltme saldırıları, kaynak IP adresi sahteciliğine dayanmaktadır (Cloudflare). Şekil 3.16'da NTP kuvvetlendirmeli DDoS saldırılarının yapısı gösterilmektedir.



Şekil 3.16. NTP kuvvetlendirmeli DDoS saldırısı

3.1.2.8. SNMP amplification (kuvvetlendirmeli) DDoS saldırısı

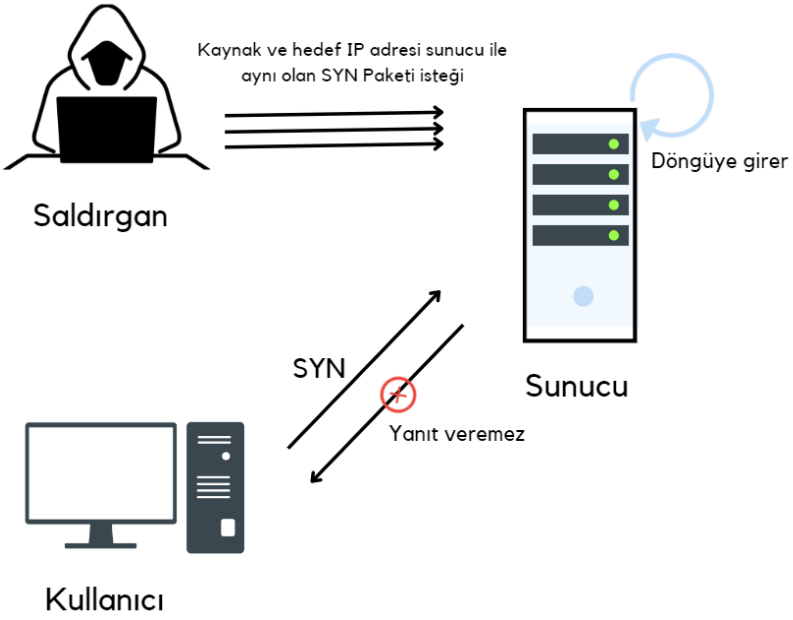
SNMP (Basit Ağ Yönetim Protokolü) (Case ve ark., 1989), ağa bağlı olan cihazların modem, sunucu, anahtar, yönlendirici gibi yönetim ve takibinin yapmayı sağlayan uygulama katmanı protokolüdür. SNMP, ağ yönetimi ve ağ izleme gibi işlemlerde sıklıkla kullanılmaktadır. SNMP'de mesajlar durum bilgisi olmayan bir UDP paketleri üzerinden iletilmekte ve alınmaktadır (Brahanyaa ve Anbarasi, 2018). SNMP amplification saldırısında bir sahte IP adresine karşı fazla boyutta yanıt ortaya koyulmasını hedeflenir. SNMP amplification saldırısında, saldırgan sahte bir IP'ye sahip çok sayıda SNMP sorgusunu ağ üzerindeki tüm cihazların yanıtlaması için gönderir. Ağda bulunan cihazlardan hedefteki sunucuya büyük boyutlarda yanıtlar iletilir. SNMP iletilen yanıtlarının hedef ağda hepsinin hacmi düşürülünceye kadar, bu sürede daha fazla cihaz yanıtladıkça saldırı hacmi büyür. Saldırı ise basit bir sorgu ile başlayıp (Şekil 3.17) hedef sunucu ağı üzerinde fazla bir trafik oluşturarak ağ bant genişliğinin taşmasıyla sonuçlanır.



Şekil 3.17. SNMP kuvvetlendirmeli DDoS saldırısı

3.1.2.9. LAND flood DDoS saldırısı

Land Flood saldırısı TCP bağlantı protokolüne bağlı açıklardan yararlanır. Şekil 3.18'de gösterilen saldırıda saldırgan, kaynak IP adresi ve bağlantı noktası, hedef adres ve bağlantı noktası ile aynı olacak şekilde ayarlanacak şekilde TCP SYN paketi oluşturulur ve bu da kurbanın makinesindeki açık bir bağlantı noktasına işaret edecek şekilde ayarlanır. Savunmasız bir makine, böyle bir mesajı alır ve paketi sonsuz bir döngüde yeniden işlenmek üzere etkili bir şekilde göndererek hedef adrese yanıt verir. Bu nedenle, kurban makinenin kilitlenmesine hatta çökmesine neden olur (Radware, 2022).



Şekil 3.18. LAND flood saldırısı

3.1.3. DDoS saldırılarının dünya geneli özeti

DDoS saldırılarının tarihçesi, internetin ortaya çıkışına kadar uzanır. İnternetin ilk yıllarında, bu tür saldırılar genellikle tek bir bilgisayardan yapılırdı. Ancak 1990'lı yıllarda, bu saldırıların dağıtılmış olma özelliği ortaya çıktı ve bu tür saldırıların yapılabilmesi için ağa bağlı birden fazla bilgisayar kullanılmaya başlandı (Atasever ve ark., 2019).

DDoS saldırılarının en önemli özelliği, saldırganın saldırıyı yaparken kendisinin anonim kalmasıdır. Bu nedenle, bu tür saldırılar genellikle küçük gruplar tarafından yapılır ve saldırganların kimliği çoğu kez bulunamamaktadır. DDoS saldırılarının yapılma amacı ise genellikle rekabete dayalıdır ve saldırıların hedefi genelde rakiplerin web siteleri veya ağ üzerinden çalışan otomasyon sistemleridir.

1999 tarihinde ortaya çıkan DDoS saldırılarının günümüze kadar bilinen saldırıları aşağıda listelenmiştir (Sağıroğlu, 2021).

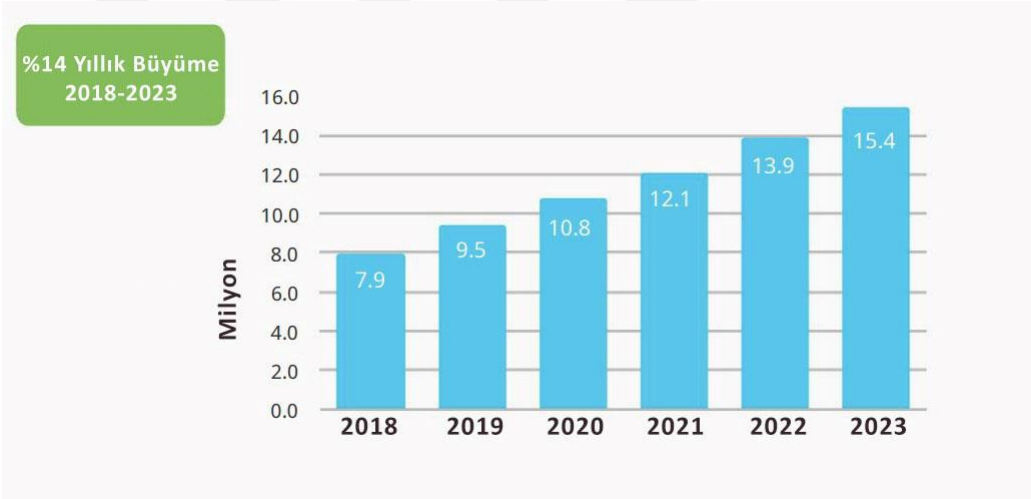
1. 2000 yılında, The Register adlı bir teknoloji haber sitesine yapılan DDoS saldırısı, o dönemde bilinen en büyük DDoS saldırısı olmuştur.
2. 2002 yılında, Microsoft'a yapılan DDoS saldırısı, saldırının yapıldığı gün içinde Microsoft'un web sitelerini tamamen durdurmuştur.

3. 2007 yılında, Estonian Government'a yapılan DDoS saldırısı, Estonian Government'ın internet erişimini etkilemiş ve ülke genelinde birçok web sitesine erişim engellenmiştir.
4. 2010 yılında, Wikileaks'e yapılan DDoS saldırısı, Wikileaks'in web sitesini yavaşlatmış ve erişimini zorlaştırmıştır.
5. 2013 yılında, Spamhaus adlı bir e-posta spam engelleme servisine yapılan DDoS saldırısı, Spamhaus'un web sitesini yavaşlatmış ve çeşitli ağları etkilemiştir.
6. 2016 yılında, Dyn adlı bir DNS hizmet sağlayıcısına yapılan DDoS saldırısı, ABD'nin birçok bölgesinde internet erişimini etkilemiş ve ülke genelinde birçok web sitesine erişim engellenmiştir (Wikipedia, 2016).
7. 2018 yılında, GitHub adlı bir kod depolama ve yönetim platformuna yapılan DDoS saldırısı, platformun web sitesini yavaşlatmış ve çeşitli ağları etkilemiştir (Kotey ve ark., 2019).
8. 2018 yılında, Akamai Technologies adlı bir internet hizmet sağlayıcısına yapılan DDoS saldırısı, DDoS saldırıları tarihinde bilinen en büyük saldırı olmuştur ve ağın yavaşlamasına sebep olmuştur.
9. 2019 yılında Çin'deki bir büyük teknoloji şirketinin web sitesine yapılan DDoS saldırısı gerçekleştirilmiştir.
10. 2020 yılında ABD ve Avrupa'daki birçok banka ve finansal kuruluşun web sitelerine yapılan Revil ransomware tarafından yapılan DDoS saldırıları gerçekleştirilmiştir.
11. Amazon Web Services (AWS), Şubat 2020'de kaydedilen 2,3 Tb/sn'lik büyük bir DDoS saldırısıyla sarsıldı. AWS'ye yapılan saldırı, diğer tüm toplu saldırılardan %44 daha büyüktü (Crane, 2020).
12. 2021 yılında Japonya ve Güney Kore'deki birçok e-ticaret ve teknoloji şirketinin web sitelerine yapılan Egregor ransomware tarafından yapılan DDoS saldırıları gerçekleştirilmiştir.
13. 2021 yılı ortalarında, hükümet ve parlamento web siteleri de dahil olmak üzere Belçika genelinde 200'den fazla kuruluş DDoS saldırılarına maruz kalmıştır.
14. Eylül 2021'de Yandex, 21,8 milyon RPS (Saniye Başına İstek) ile DDoS saldırısına maruz kaldı. Yapılan bu saldırı 7 Ağustos 2021'den kaydedildi (Raza, 2021).
15. Kaspersky DDoS saldırıları 2021 4. Çeyrek raporunda, 2021 yılı sonlarına doğru DDoS saldırılarının, Amerika Birleşik Devletleri'nde %43,55, Çin yüzde %9,96,

Hong Kong %8,80, Almanya %4,85 ve Fransa'da %3,75 olduğu belirtilmiştir (Kyspersky, 2021).

16. 2022 yılında Avrupa, Orta Doğu ve Afrika'daki birçok enerji ve enerji üretimi şirketinin SCADA sistemlerine yapılan Trickbot malware tarafından yapılan DDoS saldırıları meydana gelmiştir.

Cisco (2018-2023) Yıllık Raporu'na göre; DDoS Saldırıları, dünya çapında 2023 yılına kadar ikiye katlanarak 15,4 milyona ulaşacağını belirtmiştir. Bu rapora göre; DDoS Saldırı Boyutu ve Frekans Artışı, En yüksek saldırı boyutu, her yıl %63 oranında artış göstermiştir. 100 Gb/sn ile 400 Gb/sn arasında yıllık saldırılarda %776 artış gözlendiği belirtilmiştir. DDoS saldırılarının küresel sıklığı her yıl %39 oranında arttığı ve ortalama DDoS saldırılarının boyutunun 1 Gb/sn ve çoğu kuruluşu tamamen çevrimdışı duruma getirmeye yeterli olduğunu vurgulamıştır (Cisco, 2022). Şekil 3.19'da 2018 yılı ile 2023 arasındaki saldırıların artış oranları gösterilmiştir.



Şekil 3.19. Cisco (2018-2023) Yıllık Raporu (Cisco, 2022)

NESCOUT'un DDoS Tehdit İstihbarat 2022 İlk Çeyrek Raporuna göre, DDoS saldırılarının 2021'in sonlarında azalma olmasına karşın 2022'nin başlarında arttığını belirtmişlerdir. DDoS saldırılarını düzenleyen saldırganların TCP tabanlı doğrudan yol saldırıları başlatmak için güçlü "botnet"leri daha fazla kullandıklarını belirtmişlerdir. Bu saldırıları genel olarak toplumsal olaylara bağlamışlardır. Saldırganlar bu süreçte yeniliklere giderek yeni saldırı yöntemleri denemişlerdir. Rapora göre yapılan saldırılar bölgelere ayrılmıştır ve Türkiye'nin dahil olduğu

EMEA olarak kısaltılan; Avrupa, Orta Doğu ve Afrika saldırılar %7'lik bir artış göstermiştir (Netscout, 2022) .

Rapora göre saldırı sayısına göre 2022'nin 1. Çeyreğinde en çok hedeflenen dikey sektörler listelenmektedir (Şekil 3.20).

RÜTBE	DİKEY	SIKLIK	MAKSİMUM SALDIRI	MAKSİMUM ETKİ	ORTALAMA SÜRE
1	Kablolu Telekomünikasyon Taşıyıcıları	453	12,8 Gb/sn	1.45 Mp/sn	91 Dakika
2	Özel Bilgisayar Programlama Hizmetleri	68	204,71 Gb/sn	47.39 Dakika	24 Dakika
3	Kablosuz Telekomünikasyon Taşıyıcıları (Uydu hariç)	48	5.32 Gb/sn	1.73 Mp/sn	11 Dakika
4	Veri İşleme Barındırma ve İlgili Hizmetler	16	4,55 Gb/sn	1.18 Dakika	30 dakika
5	İşe Yerleştirme Ajansları	9	25,24 Gb/sn	6.55 Dakika	27 Dakika
6	Tarifeli Yolcu Hava Taşımacılığı	1	1,28 Gb/sn	0.12 Dakika	6 Dakika

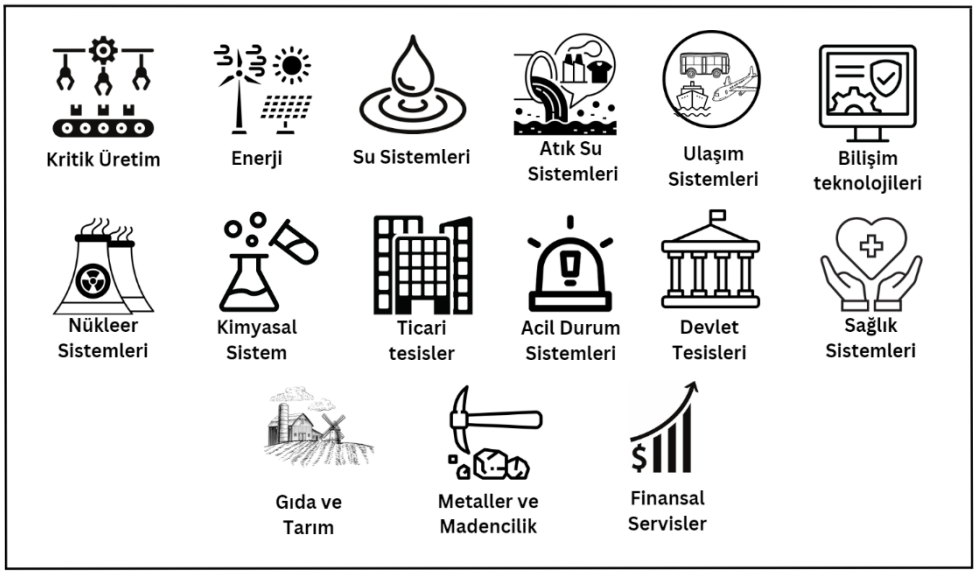
Şekil 3.20. NETSCOUT 2022 1. çeyrek DDoS saldırılarının endüstriyel dikey dağılımı (Netscout, 2022)

Raporda belirtilen Dikey endüstriyel dağılımdaki alanların hepsi genel olarak Siber Saldırılara açık alanlardır. 4. Sırada bulunan "Veri İşleme Barındırma ve İlgili Hizmetler" bir sonraki bölümde açıklayacağımız SCADA sistemler için önem teşkil etmektedir.

3.2. Denetleyici Kontrol ve Veri Toplama Sistemleri (SCADA)

Denetleyici Kontrol ve Veri Toplama Sistemleri (SCADA), birçok sistemi izler ve veri toplar. SCADA sistemleri, geniş bölgelerde bulunan birimlerin merkez bilgisayar ile kontrol edilmesi, izlenmesi, denetlenmesi birimlere ait eski verilerin saklanmasını sağlayan sistemlere verilen genel bir isimdir (Mohamed Najeh, 2017). SCADA tesislerin denetim düzeyine odaklanmaktadır. Genel olarak programlanabilir mantık denetleyicileri (PLC'ler) ile arabirim oluşturduğu donanımın üzerine yerleştirilmiş tamamen bir yazılım paketidir (Daneels ve Salter, 1999). SCADA sistemleri ayrıca, uzaktan erişim ve yönetim işlemlerini de destekler. Kritik altyapı olarak adlandırılan elektrik, su ve gaz gibi üretimi iletimi dağıtımında SCADA sistemleri kullanılmaktadır (Söğüt ve Erdem, 2020). Aslında, kritik altyapıların ve endüstriyel otomasyonun birbirine bağlı fiziksel ve siber

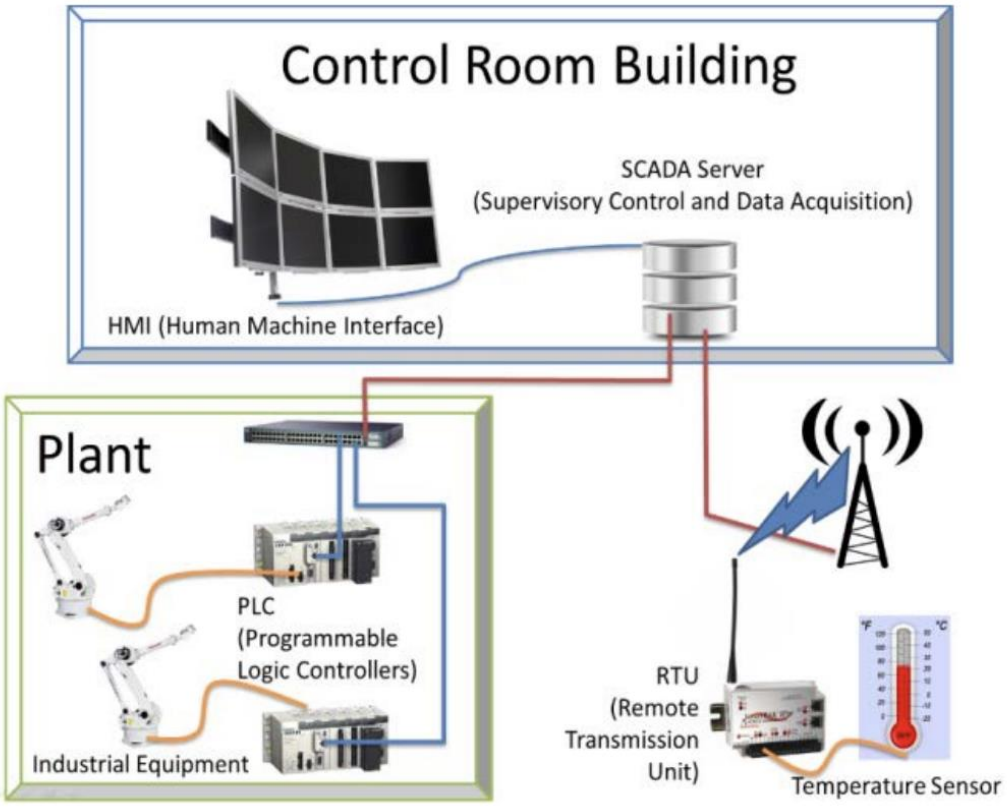
tabanlı kontrol sistemlerine artan bağımlılığı, SCADA ve dağıtılmış kontrol sistemlerine (DCS'ler) yönelik artan ve önceden tahmin edilemeyen bir siber güvenlik tehdidi ile sonuçlanmıştır (Mohamed Najeh, 2017). DCS ise, bir tesis veya bir fabrika gibi kontrol alanı içerisinde bulunan coğrafi olarak dağıtılmış kontrol döngülerini kullanan bir otomatik endüstriyel kontrol sistemidir (Nwoba ve ark., 2022). Dağıtılan bu kontrol döngülerinden oluşan DCS'ler sensörler, bilgisayarlar ve kontrollerden oluşmaktadır (Nwoba ve ark., 2022). SCADA sistemlerine benzer yapıları bulunmaktadır fakat SCADA sistemleri kontrolü tek olmasına rağmen DCS'ler kontrol edilecek makine grubuna göre özel bir kontrol sistemi kullanmaktadır. Bu yüzden de DCS'ler genel olarak proses odaklıdır, SCADA ise veri toplama odaklıdır. SCADA sürekli veri kontrolü işlemi gerçekleştirmeden veri tabanına kaydetmiş olduğu değişen verilere göre işlemlerini sürdürür. SCADA sistemleri; enerji sistemleri, ulaşım sistemleri, nükleer sistemler gibi kritik alt yapı sistemlerinde yani daha geniş alanlarda kullanılan sistemlerden birisidir (Şekil 3.21).



Şekil 3.21. SCADA sistemlerinin uygulama alanları

SCADA sistemlerinin uygulama alanı çok geniştir. Şekil 3.21'de bu alanlar gösterilmiştir (Alanazi ve ark., 2022). SCADA sistemlerinde açık haberleşme ve kapalı haberleşme protokolleri mevcuttur. Burada kapalı haberleşme protokolleri, üretici firmanın kendi ürünleri aralarında bazı özel protokoller vasıtasıyla haberleşmesini sağlayan, açık haberleşme protokolleri ise üretici firmaya bağlı olmadan haberleşmedir (Taşdelen, 2022). Modbus protokolü SCADA sistemlerinde haberleşmede en sık

kullanılan açık sistem haberleşme protokollerinden birisidir (Sharma ve ark., 2022). Diğer kullanılan açık sistem haberleşme protokolleri ise; AS-i protokolü, CANBus, DeviceNet, Fieldbus, Profibus, HART ve INTERBUS protokolleridir. Bir SCADA sisteminin yapısı Şekil 3.22'de gösterilmektedir.



Şekil 3.22. SCADA örnek sistem yapısı (Mohamed Najeh, 2017).

SCADA sistemleri, endüstriyel süreçleri otomatikleştirme ve izleme için kullanılan karmaşık bir sistemdir. SCADA sistemleri genellikle üç ana bileşen içerir:

- **SCADA Ana Bilgisayar (Master Station):** SCADA sistemi üzerindeki tüm verileri toplayan ve analiz eden ana bilgisayar. Bu bilgisayar, veri tabanlarına ve kontrol merkezine bağlı çalışan bir yazılımdır.
- **RTU (Remote Terminal Unit):** SCADA sistemine bağlı olan sensör ve aktüatörleri kontrol eden cihazdır. Bu cihazlar, veri toplama, işleme ve kontrol için kullanılan çok sayıda giriş ve çıkış noktasına sahiptir.
- **İletişim Ağı:** SCADA sistemi bileşenleri arasında veri iletişimini sağlayan ağdır. Bu ağlar genellikle Ethernet, Profibus, Modbus, DNP3 ve ICCP gibi protokoller kullanır. Verilerin iletilmesi için kablosuz veya kablolu ağlardan da yararlanılabilir.

SCADA sistemleri, birçok bileşenin yanı sıra veri toplama, işleme ve kontrol işlemlerini yöneten yazılımların entegre edilmesiyle oluşturulur. Diğer bileşenler arasında, PLC'ler, SCADA İnsan-Makine Arayüzü (HMI) yazılımı, grafiksel kullanıcı arayüzleri, tarihsel veri tabanları, alarm ve olay yönetimi yazılımları bulunabilir.

3.2.1. Modbus protokolü

Modbus, 1979 yılında Modicon tarafından geliştirilmiş bir açık sistem haberleşme protokolüdür (Wingpath, 2014-2023). Akıllı cihazlar arasında istemci-sunucu (TCP) iletişimi kurmak için kullanılır. PLC'ler ile kullanılmak üzere tasarlanıp daha sonra bir evrensel olarak kabul edilen bir protokol haline gelmiştir. PC'ler ve HMI'lar kullanarak saha cihazlarını izlemek için kullanılır. Modbus protokolü, kablosuz haberleşmede RTU uygulamaları için uygun bir protokol olması sebebiyle de en çok tercih edilen iletişim protokolüdür. Modbus-TCP ise, Modbus protokolünün Ethernet TCP/IP'nin üzerinde kullanıldığını göstermektedir (Mehta ve Reddy, 2014). Modbus, iletişim için 502 TCP Port Numarasını kullanmaktadır. Bilinen port numarası sebebiyle de özellikle SCADA sistemlerde kullanılan Modbus protokolü, siber saldırılara açık bir protokoldür (Bhatia ve ark., 2014).

Bu sebeple SCADA sistemlerine düzenlenen DDoS saldırılarında direk port numarası üzerinden flood saldırıları gerçekleştirilmektedir. Bu çalışmada port numarası üzerinden gerçekleştirilen saldırılar ile SCADA sistemlerinde hizmet kesintisi sağlanmış ve sistem devre dışı bırakılmıştır.

3.2.2. Programlanabilir mantık denetleyici (PLC) sistemleri

PLC'ler, otomatik sistemleri kontrol edebilen, tek işlemcili ve elektrikli merdiven diyagramının mantığında çalışan bilgisayar tabanlı cihazlardır (Alphonsus ve Abdullah, 2016). Bir diğer ifade ile PLC, endüstriyel otomasyonda kullanılan programlanabilir mantık denetleyicidir (Patel, 2018). Genel olarak tesislerin üretim faaliyetlerini kontrol etmek için geliştirilmiştir. PLC sistemleri; Merkezi işlem birimi, bellek birimi, giriş birimi ve çıkış birimlerini içermektedir (Zimmerman, 2008). PLC'ler de herhangi bir ağ saldırısına karşı savunma sistemi bulunmamaktadır. Bu sebeple kullandığı Modbus ve DNS3 protokolleri vasıtası ile saldırılara açık bir sistemdir (Ahmed ve ark., 2017). SCADA sistemlerinde PLC donanımları kullanılmaktadır.

3.2.3. SCADA sistemlerinde güvenlik

SCADA sistemleri siber saldırılara karşı çok savunmasızdır. Bu sistemler genellikle eski ve zayıf işletim sistemleri ve yazılımları kullanırlar, bu nedenle güncel güvenlik önlemleri uygulanmayan sistemler tehlikelere daha açık hale gelmektedir. Bu sistemler, ethernet, fiber optik kablolama, uydu veya radyo dahil olmak üzere farklı iletim ortamlarının kullanımı vasıtası ile bağlantı sağlanır ve bu bağlantılardan kablosuz bağlantı, SCADA sistemlerini siber saldırılara açık hale getirmektedir (Ayaburi ve Sobrevinas, 2015). Bu sistemlerde özel ağlar üzerinde çalışan ve internete bağlı olmayanlarında saldırganların erişmesi zordur. Ancak, saldırganlar özel ağların güvenlik açıklarını kullanarak SCADA sistemlerine erişebilmektedirler. Fakat geniş alanlarda kullanılan SCADA sistemleri internete bağlı olarak çalışmaktadır ve siber saldırıların odağı haline gelmektedir.

SCADA sistemlerini internete bağlamak, artan düzeyde kolaylık sağlarken, aynı zamanda onları arabellek taşması, bellek ve Hizmet Reddi (DoS), DDoS saldırıları gibi çeşitli siber saldırılara maruz bırakır (Samtani ve ark., 2016). Akıllı şebekelerde, kontrol merkezi ve son kullanıcılar arasında veri alışverişi önemlidir. Dolayısıyla bu akıllı şebekenin verimli ve güvenilir çalışmasını sağlar. İletişim protokolleri bilgisine sahip bir saldırgan birçok siber saldırı gerçekleştirebilir; DoS, DDoS DNS spoofing saldırısı, kimlik doğrulama sunucusu saldırısı, ortadaki adam (MITM) gibi bir siber saldırıları çok kolay bir şekilde gerçekleştirebilir. Siber saldırıların tüm olası sonuçları arasında ağ gecikmesi en sık karşılaşılan konulardan birisidir (Chen ve ark., 2014).

Bu sistemlerde karşılaşılabilecek bir siber saldırı sonucunda hem sisteme hem de sistemi kullanan kişilere ciddi zararlar verebilmektedir (Onyeji ve ark., 2014). SCADA sistemlerine yapılan DDoS saldırıları genellikle sistemin güvenliğini tehlikeye düşürmek veya sistemin çalışmasını bozmak amacıyla gerçekleştirilir. Bu da sistemin hizmet dışı kalarak ağ gecikmesinin yaşanmasına neden olmaktadır.

SCADA sistemlerinde siber saldırıların önlenmesi için, sistemlerinin güncel işletim sistemleri ve yazılımları kullanması, güncel güvenlik önlemleri uygulanması ve sistemlerin sürekli olarak izlenmesi ve denetlenmesi önemlidir.

SCADA sistemleri, üretim tesislerinin en önemli bileşenlerinden biridir ve bu nedenle, SCADA sistemlerinin güvenliği büyük önem taşımaktadır. SCADA sistemleri için özel olarak tasarlanmış birçok farklı güvenlik çözümü bulunmaktadır. İşte bazı örnekler:

- **Ağ Güvenlik Duvarı:** Ağ güvenlik duvarları, tesis ağının SCADA ağına erişimini sınırlandırarak, kötü niyetli saldırılardan koruma sağlar. Ağ güvenlik duvarları, saldırıları tespit etmek ve engellemek için gerekli filtreleme, güvenlik politikaları ve erişim kontrolü sağlar.
- **Sanal Özel Ağ (VPN):** Sanal özel ağlar, farklı yerlerdeki SCADA sistemlerine erişim sağlamak için kullanılır. Bu sistemler, internet üzerinden veri aktarımı yaparken, güvenliği artırmak için VPN kullanılır. VPN, verileri şifreleyerek ve güvenli bir tünel oluşturarak, SCADA sistemlerine erişimi sınırlandırır.
- **Antivirüs ve Güvenlik Yazılımı:** SCADA sistemleri için özel olarak tasarlanmış antivirüs ve güvenlik yazılımları, zararlı yazılımları tespit etmek ve engellemek için kullanılır. Bu yazılımlar, SCADA sistemleri için özel olarak tasarlanmıştır ve tesislerin ihtiyaçlarına uygun olarak yapılandırılabilir.
- **Güvenlik Analiz Araçları:** Güvenlik analiz araçları, SCADA sistemlerine yönelik saldırıları tespit etmek ve engellemek için kullanılır. Bu araçlar, ağ trafiğini izleyerek, anormallikleri tespit eder ve güvenlik ekibine bildirir. Bu sayede, saldırılar hızlı bir şekilde engellenebilir.
- **Fiziksel Güvenlik:** SCADA sistemlerine fiziksel erişimi sınırlandırmak, saldırıları engellemenin en önemli yollarından biridir. Bu nedenle, SCADA sistemleri, güvenli bir şekilde korunmak için uygun bir alanda saklanmalıdır.

Bu güvenlik çözümleri, SCADA sistemlerinin güvenliği için önerilen bazı yöntemlerdir. Ancak, her tesisin ihtiyaçları farklıdır ve bu nedenle, güvenlik çözümleri de farklı olabilir. SCADA sistemlerinde derin öğrenme yöntemleriyle yapılmış güvenlik çözümleri geliştirilmektedir. Derin öğrenme, makine öğrenmesi alanında geliştirilen bir teknoloji olup, yapay sinir ağları kullanılarak yüksek seviyede öğrenme ve veri analizi sağlar.

SCADA sistemleri için derin öğrenme yöntemleri kullanılarak geliştirilen güvenlik çözümleri, saldırıların tespit edilmesi, önceden tahmin edilmesi ve önlenmesi amacıyla kullanılır. Bu sistemler, ağ trafiğini izler ve anomali durumları tespit ederek, saldırıları önceden tahmin etmeye çalışır. Örneğin, saldırganların tespit edilmesi, kimlik doğrulama işlemlerinde yapılan hataların tespit edilmesi ve zararlı yazılımların tespit edilmesi için kullanılabilir.

Derin öğrenme teknikleri kullanılarak geliştirilen SCADA güvenlik çözümleri, büyük veri kümelerinin analizi için uygun olan yapay sinir ağları ve benzeri yöntemlerle

çalışır. Bu yöntemler, tesislerdeki ağ trafiğini analiz ederek, anormal durumları tespit eder ve güvenlik sorunlarına erken müdahale edilmesini sağlar. Bununla birlikte, derin öğrenme yöntemleriyle yapılmış SCADA güvenlik çözümleri halen geliştirme aşamasındadır ve bu teknolojilerin kullanımı, uygun şekilde planlanıp uygulanması gerekmektedir. Bu nedenle, SCADA sistemleri için güvenlik çözümleri seçilirken, çözümün mevcut tesisin ihtiyaçlarına uygun olduğundan emin olmak önemlidir.

3.2.4. SCADA sistemlerine yapılan siber saldırıları örnekleri

SCADA sitemlerinin internet ağı üzerinden veri iletimi sağlanması ile oluşan en önemli siber saldırılar hizmet yavaşlatma saldırılarıdır. Bunlar genel olarak DoS ve DDoS saldırılarıdır. SCADA sistemlerine yapılan büyük DDoS saldırıları, bu sistemleri hedef alan geniş kapsamlı saldırılardır. Bu saldırıların amacı, üretim ve endüstriyel tesislerin otomasyon sistemlerini etkisiz hale getirerek, üretimi durdurmak veya işletmeleri ciddi şekilde hasara uğratmak olabilir. SCADA sistemlerine düzenlenen DDoS ve faklı yapıda olan saldırılarından bazıları şunlarıdır:

Ukraine Power Grid Saldırısı, 2015 yılında gerçekleştirilmiş ve Ukrayna'daki bir enerji şirketinin SCADA sistemine yapılan DDoS saldırısıdır. Saldırganlar, SCADA sistemlerine zarar vermek ve Ukrayna'nın elektrik altyapısını etkisiz hale getirmek için çeşitli teknikler kullanmışlardır (Wired, 2016).

Dragonfly 2.0 Saldırısı ise, 2017 yılında gerçekleştirilmiş ve enerji şirketlerini hedef almıştır (Paganini, 2017). Saldırganlar, SCADA sistemlerine saldırarak, endüstriyel tesislerin üretim süreçlerini etkisiz hale getirmeye çalışmışlardır (Bitchkei, 2017).

TRITON/ TRISIS Saldırısı (Öztürk, 2018), 2017 yılında Suudi Arabistan'daki bir petrokimya tesisi için kullanılan Triconex kontrol sistemine yönelik bir siber saldırıdır. Bu saldırı, Triconex kontrol sistemlerini etkileyen özel bir kötü amaçlı yazılım (malware) kullanarak gerçekleştirildi. TRITON/TRISIS saldırısının amacı, Triconex kontrol sistemleri üzerinde kontrol sağlamaktı. Bu sistemler, endüstriyel işletmelerde kullanılan önemli bir SCADA teknolojisidir ve enerji, petrol ve gaz, kimya gibi sektörlerde kullanılır. Saldırı, sistemin güvenlik açığından yararlanarak Triconex kontrolörlerine kötü amaçlı bir yazılım yükledi ve böylece operatörlerin erişimini engelleyen bir saldırı gerçekleştirildi. TRITON/TRISIS saldırısı, endüstriyel kontrol sistemleri için oldukça sofistike bir saldırıydı ve siber güvenlik açısından önemli bir dönüm noktası olarak kabul

edilir. Saldırı, endüstriyel işletmelerin SCADA sistemlerine yönelik güvenlik önlemlerinin artırılması gerektiğini vurgulamıştır.

2018 yılında Ukrayna'daki bir enerji şirketinin SCADA sistemlerine yapılan NotPetya malware saldırısı, son derece yıkıcı bir saldırıdır ve birçok şirketi etkilemiştir (Kaspersky, 2018). NotPetya, bir fidye yazılımı olarak tanımlanmaktadır. Saldırı, dünya genelinde birçok şirketi, hükümeti ve kuruluşu etkilemiştir. NotPetya, bilgisayarları ele geçirdikten sonra verileri şifrelemiş ve şifreleme karşılığında fidye talep etmiştir. Ancak, saldırganlar verileri geri vermeyi hiçbir zaman garanti etmediler ve fidye ödeyen şirketler bile verilerini kurtaramadılar. Ayrıca, NotPetya, sadece verileri şifrelemekle kalmamıştır, aynı zamanda sistemin başlatılmasını engellemiş ve hatta sabit sürücüleri fiziksel olarak hasar vermiştir. Saldırı, özellikle Ukrayna'daki enerji şirketlerini hedef almıştır ve bu şirketlerin operasyonlarını felç etmiştir. Saldırı ayrıca, Rusya'ya yönelik yaptırımları uygulamaya çalışan birçok Batı şirketini hedef aldı ve bu şirketlerin operasyonlarını durdurmuştur. NotPetya saldırısı, siber güvenlik dünyasında önemli bir dönüm noktası olarak kabul edilmektedir. Bu saldırı, birçok şirketin ve kuruluşun güvenlik önlemlerini gözden geçirmesine ve iyileştirmesine yol açtı. Ayrıca, saldırı, siber saldırılara karşı daha iyi hazırlanmak için yeni protokoller ve yöntemlerin geliştirilmesini de sağladı.

Bad rabbit ransomware saldırısı, 2020 yılında Rusya'daki bir petrol ve gaz şirketinin SCADA sistemlerine yapılan bir siber saldırıydı. Saldırı, şirketin enerji üretim ve dağıtım sistemlerine zarar vermek amacıyla gerçekleştirildi. Bad Rabbit, bir fidye yazılımı olarak tasarlanmıştır ve sisteme bulaştığında, verileri şifreleyerek kullanıcıların dosyalarına erişimini engellemektedir. Saldırganlar daha sonra kurbanlardan fidye talep etmek için iletişim kuruyorlardı. Bad Rabbit saldırısı, özellikle enerji sektörü gibi kritik altyapıları hedef alan bir saldırıydı ve bu nedenle son derece ciddi bir tehdit olarak değerlendirilmiştir. Saldırı, şirketin SCADA sistemlerine sızarak üretim ve dağıtım işlemlerine müdahale etmek için tasarlanmıştı. Eğer saldırı başarılı olsaydı, bu şirketin üretim ve dağıtım faaliyetlerini durdurması ve hatta enerji arzını kesmesi mümkün olmaktaydı.

Bu tür saldırılar, üretim tesislerinin SCADA sistemlerine erişerek, cihazları veya verileri etkisiz hale getirerek, üretim hatlarını bozarak veya üretim tesislerinin verimliliğini azaltarak, önemli hasarlara neden olabilmektedir. Bu nedenle, SCADA sistemlerine yapılan siber saldırılara karşı koruma sağlamak için, ağ güvenliği cihazlarının kullanılması, düzenli güncelleme ve yamaların uygulanması, ağ trafiğinin izlenmesi, ağdaki cihazların doğrulanması ve erişim kontrollerinin uygulanması gibi bir

dizi önleyici tedbir alınmalıdır. Bunun yanı sıra DÖ yöntemleri ile saldırıların önceden tespit edilmesi büyük önem arz etmektedir.

4. MATERYAL VE YÖNTEM

Bu bölümde materyal ve yöntem on dört başlık altında ele alınmıştır. Bunlar sıra ile; birinci bölümde saldırı tespit sistemlerinin neler olduğundan, ikinci bölümde veri seti oluşturma aşamasında kullanılan araçlardan, üçüncü bölümde paketlerin yakalanması, dördüncü bölümde paketlerin analizinin nasıl gerçekleştirildiği, nelere dikkat edildiği, dördüncü bölüm ile dokuzuncu bölümlerde MÖ modellerinden, onuncu bölümde DÖ modelinden, on birinci bölümde değerlendirme metriklerinden, on ikinci bölümde hazır veri seti özelliklerinden, on üçüncü bölümde bu tez çalışması kapsamında oluşturulan SCADA sistemlere düzenlenen DDoS saldırılarından oluşan veri setinin oluşturulması aşamaları ve özelliklerinden, on dördüncü bölümde ise hem hazır veri seti olan CICDDoS2019 veri seti hem de yeni oluşturulan veri seti üzerinde veri ön işleme adımları detaylı olarak açıklanmıştır.

4.1. Saldırı Tespit Sistemleri

Saldırı Tespit Sistemi (STS), ağ üzerinden bilgisayar sistemlerine yapılabilecek olan saldırılara karşı, ağın izlenerek tehdit unsuru bulunduran durumların analiz edilmesi süreçlerini ifade etmektedir (Baykara ve Resul, 2019). Genellikle gerçek zamanlı olarak, bilgisayar sistemlerinin izinsiz ve kötüye kullanımını tespit edilmesinde kullanılan sistemlerdir. Yaygın kullanılan STS'lere bu bölümde değinilmiştir.

4.1.1. Ağ tabanlı saldırı tespit sistemi

Ağ tabanlı saldırı tespit sistemi (NIDS- Network-based Intrusion Detection System), Ağ üzerindeki trafiği izleyerek, ağa yapılan saldırıları tespit etmek ve raporlamak için tasarlanmış bir sistemdir. NIDS, ağ üzerindeki trafiği analiz ederek, normal ağ trafiğinden farklı olan davranışları tespit eder ve potansiyel saldırıları belirler (İtübidb, 2013). NIDS'in ana görevi, saldırıları tespit etmek ve siber güvenliği sağlamak için ağ trafiğini sürekli olarak izlemek ve analiz etmektir. Bu işlem, ağ üzerindeki tüm paketleri izleyen bir sensör aracılığıyla gerçekleştirilir. Sensör, ağ üzerindeki tüm paketleri analiz eder ve tespit edilen herhangi bir anomaliyi bir uyarı olarak rapor eder. NIDS, iki farklı şekilde çalışabilir;

- **Signature-Based Detection:** Bu yöntem, bilinen saldırı imzaları veya belirtileri ile karşılaştırma yaparak saldırıları tespit eder. Eğer ağ üzerindeki trafikte bilinen bir saldırı imzası tespit edilirse, NIDS bunu belirterek uyarma yapar.
- **Anomaly-Based Detection:** Bu yöntem, normal ağ trafiğini öğrenerek, normal davranışlardan farklı olan davranışları tespit ederek saldırıları belirler. Bu yöntem, bilinmeyen saldırılar için daha iyi bir koruma sağlar. NIDS, saldırı tespitinde etkili bir yöntemdir, ancak tespit edilen saldırıların analizi ve raporlanması için insan müdahalesi gerektirebilir.

4.1.2. İmza tabanlı saldırı tespiti

İmza tabanlı saldırı tespiti, bilgisayar sistemleri ve ağlarındaki güvenlik açıklarını ve kötü amaçlı yazılımları tespit etmek için kullanılan bir tekniktir. Bu yöntem, önceden belirlenmiş bilinen saldırıların imzalarını kullanarak kötü amaçlı faaliyetleri tespit etmeye çalışır. İmza tabanlı saldırı tespiti, kötü amaçlı yazılımın belirli bir kalıbı izlemesi ve belirli özelliklere sahip olması gerektiğinden, etkili bir tespit yöntemi olarak kabul edilebilir (Kaynar ve ark., 2018). Bu kalıplar ve özellikler, saldırıları tespit etmek için kullanılan imzalar olarak adlandırılır ve bilinen kötü amaçlı yazılım örneklerinden elde edilen bilgilerden türetilir. Ancak, imza tabanlı saldırı tespiti yöntemi yalnızca bilinen saldırıları tespit edebilir ve yeni veya daha önce görülmemiş saldırılara karşı savunmasız kalabilir. Bu nedenle, imza tabanlı saldırı tespiti, diğer tespit yöntemleriyle birlikte kullanılmalı ve güvenlik açıklarının tespit edilmesi için sürekli bir izleme ve güncelleme gerektirir.

Bu teknik, bilgisayar sistemleri ve ağlarındaki güvenlik açıklarını tespit etmek için yaygın olarak kullanılan bir yöntemdir. Bununla birlikte, imza tabanlı saldırı tespiti tek başına yeterli değildir ve diğer tespit yöntemleriyle birlikte kullanılmalıdır. Bu sayede, bilinmeyen saldırıların tespit edilmesi ve güvenlik açıklarının önceden engellenmesi mümkün olabilir. Sonuç olarak, bilgisayar sistemleri ve ağlarındaki güvenlik açıklarının tespiti için sürekli bir izleme ve güncelleme yapılması önemlidir.

4.1.3. Anomali tabanlı saldırı tespiti

Anomali tabanlı saldırı tespiti, bilgisayar sistemlerinde ve ağlarda kötü amaçlı faaliyetleri tespit etmek için normal davranış kalıplarından sapmaları tespit etmek üzere

kullanılan bir tekniktir. Bu teknik, önceden belirlenmiş bir imza veya kalıp kullanmak yerine, normal davranış kalıplarını öğrenerek anomali (normalden sapma) tespit eder. Anomali tabanlı saldırı tespiti, genellikle makine öğrenimi veya yapay zekâ teknikleri kullanılarak normal davranış kalıplarının öğrenilmesine dayanır. Bu teknikler, ağ ve sistem verilerinin analiz edilmesi yoluyla algoritmalara normal davranış kalıplarını öğrenmek için öğrenme süreci sağlar (Ahmed ve ark., 2016). Öğrenilen bu normal davranış kalıpları daha sonra gerçek zamanlı olarak izlenir ve herhangi bir sapma durumunda alarm verilir. Anomali tabanlı saldırı tespiti, önceden belirlenmiş imzaların kullanılmaması nedeniyle imza tabanlı tespit yöntemlerine göre daha esnek ve yeni veya daha önce görülmemiş saldırılara karşı daha koruyucu olabilir. Ancak, normal davranış kalıplarının öğrenilmesi süreci yanlış pozitif veya yanlış negatif sonuçlar üretebilir. Bu nedenle, anomali tabanlı saldırı tespiti sürekli bir izleme, öğrenme ve geliştirme süreci gerektirir.

4.1.4. Ana bilgisayar tabanlı saldırı tespit sistemi

Ana bilgisayar tabanlı saldırı tespit sistemleri, kötü amaçlı yazılımların ve saldırıların tespit edilmesi amacıyla kullanılan bir tekniktir ve bu amaçla ana bilgisayarın faaliyetlerini izlerler. Bu tespit yöntemi, ana bilgisayarın kayıtlarını takip ederek normal davranış kalıplarından sapmaları belirleyerek kötü amaçlı yazılımları ve saldırıları tespit eder. Ana bilgisayar tabanlı saldırı tespit sistemleri, ana bilgisayarın dosya sistemini, bellek kullanımını ve ağ bağlantılarını sürekli olarak izlerler. Sistem, çalışan tüm uygulamaların başlangıç zamanlarını, bellek kullanımlarını, hangi dosyaları veya ağ kaynaklarını kullandıklarını takip eder ve bu bilgiler normal davranış kalıplarının belirlenmesi için kullanılır (Takaoğlu ve Özer, 2019). Bu yöntem önceden belirlenmiş bir imza veya kalıp kullanmadığından, yeni veya daha önce görülmemiş kötü amaçlı yazılımları ve saldırıları tespit edebilir. Ancak, normal davranış kalıplarının belirlenmesi ve öğrenilmesi süreci zaman alabilir ve doğruluğu, bu kalıpların doğru bir şekilde tanımlanmasıyla ilgilidir. Ana bilgisayar tabanlı saldırı tespit sistemi, diğer tespit yöntemleriyle birlikte kullanılabilir ve birlikte çalışarak daha kesin sonuçlar üretebilir. Ancak, tek başına kullanıldığında bile, herhangi bir anormal aktiviteyi tespit ederek bilgisayarın güvenliğini artırmak için etkili bir yöntemdir.

4.1.5. Derin öğrenme tabanlı saldırı tespit sistemi

Derin öğrenme temelli saldırı tespit sistemleri, bilgisayar sistemleri ve ağlardaki kötü amaçlı yazılımları ve saldırıları tespit etmek için kullanılan bir tekniktir. Bu yöntem, öğrenme süreci boyunca daha karmaşık özellikleri algılayabilen derin öğrenme algoritmalarını kullanır. Derin öğrenme tabanlı saldırı tespit sistemleri, öncelikle ağ ve sistem verilerini toplar ve işler. Daha sonra, bu veriler, derin öğrenme algoritmaları gibi yapay sinir ağları kullanılarak analiz edilir. Bu algoritmalar, ağdaki anormallikleri tespit etmek için öğrenirler ve normal davranış kalıplarından sapmaları tespit ederek kötü amaçlı yazılımları ve saldırıları tespit ederler. Derin öğrenme tabanlı saldırı tespit sistemleri, diğer tespit yöntemlerine göre daha karmaşık ve daha doğru sonuçlar verebilir. Ancak, veri işleme ve öğrenme süreci, diğer yöntemlere göre daha fazla zaman ve işlem gücü gerektirir. Derin öğrenme tabanlı saldırı tespit sistemleri, diğer tespit yöntemleriyle birlikte kullanılabilir ve daha kesin sonuçlar üretmek için birlikte çalışabilirler.

DDoS saldırılarına karşı, ağ trafiği izleme, filtreleme, anormallik tabanlı izinsiz giriş tespit sistemleri ve imza tabanlı algılama gibi izinsiz giriş önlemleri uygulanmaktadır. Ağ trafiği anormal trafikten arındırılsa da, güncellemeler belirli aralıklarla gerçekleştirilir ve bu da ani saldırılara karşı ağı savunmasız bırakabilmektedir (Mall ve ark., 2023).

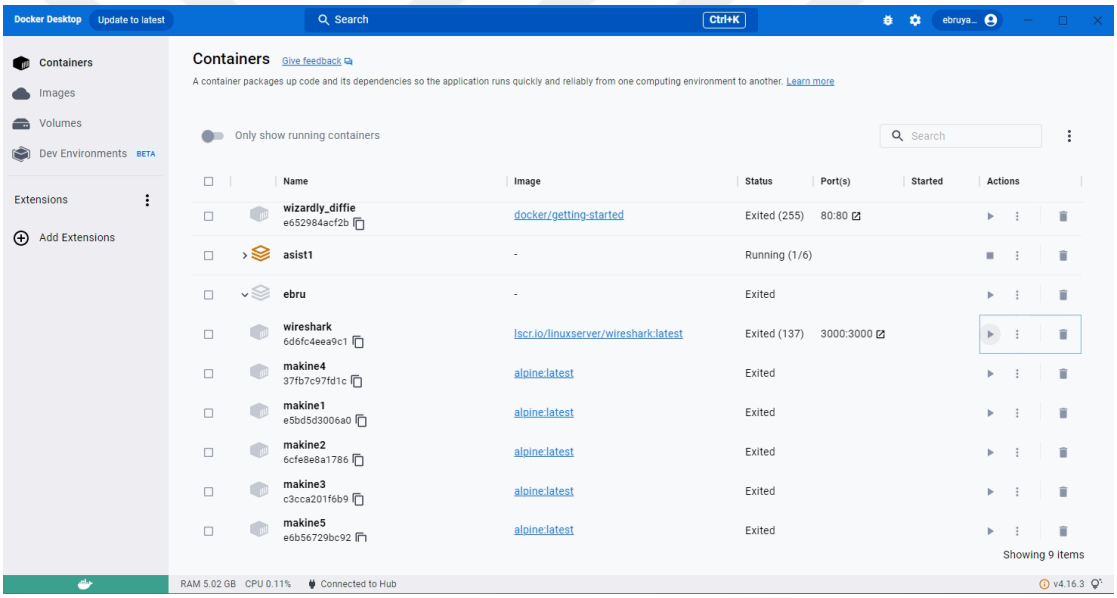
4.2. Kullanılan Araçlar

Bu bölümde veri seti oluşturma aşamasında kullanılan araçlar detaylı olarak açıklanmıştır. Bir ağa saldırı yapabilmek için farklı materyal ve yöntemler bulunmaktadır.

4.2.1. Docker sanallaştırma

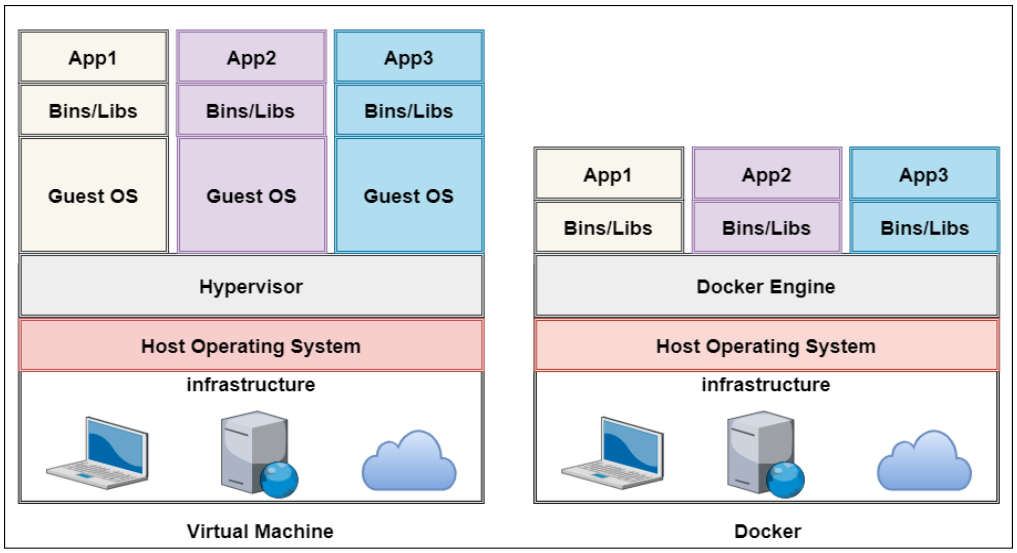
Açık kaynaklı bir sanallaştırma platformu olarak oluşturulan yapıya Docker ismi verilmiştir. Docker ile işletim sistemleri üzerinde istenilen sanal Container'ler (makineler) çalıştırılabilmektedir. Bu sanal makineler Linux, Microsoft ya da MacOs işletim sistemleri ya da herhangi bir program parçacığı olabilmektedir. Bu platform sayesinde birçok makine tek seferde oluşturulabilmekte, programlar kolaylıkla kurulup kullanılabilmektedir.

Docker sanallaştırma platformlarında sıklıkla bahsedilen Container yapısı ismini, birçok makineyi içerisinde barındırabilmesi ve her makinenin bir klonunu oluşturmak çok kolay olduğundan dolayı deniz taşımacılığına benzetilip oradan almıştır. Bu yapı program geliştiricileri ya da sistem yöneticileri için kullanım kolaylığı, az yer kaplaması, direk sistem image'larını container içerisinden rahatlıkla çalıştırılabilmesi gibi avantajlardan dolayı birçok sorunu ortadan kaldırmaktadır. Docker kendisine ayrılan kaynağı kullanır ve en düşük seviyede kaynak paylaşımı gerçekleştirebilmektedir. Docker ile oluşturulan Container'ler birbirinden bağımsız çalışabilmektedir ve başka ortamlarda da rahatlıkla sorunsuz bir şekilde çalışmaktadır. Geliştiriciler, geliştirme ortamlarını gerekli ayarları yaparak başka ortamlara aktarabilmektedir. Docker arayüzü ise kullanımı kolay ve ulaşılabilirdir (Şekil 4.1).



Şekil 4.1. Docker arayüzü

Docker, işletim sistemlerini Images'ını Container'ler vasıtası ile kullanılabilir hale getirmektedir. Kurulan Images'lar klonlanabilir ya da baştan yeni Images'leri oluşturmaya imkân veren dinamik bir yapısı vardır. Dockerfile talimat dosyalarından da yararlanılarak manuel müdahaleye gerek kalmadan da kullanılabilmektedir. Docker sanallaştırma, klasik Virtual Machine (Sanal Makineler)'den mimari yapısı ile farklıdır ve bu yüzden geliştiricilerin son zamanlarda tercih ettiği sanallaştırma uygulamalarından biri olmuştur (Şekil 4.2).



Şekil 4.2. VM ve docker karşılaştırması

Sanal makineler (VM'ler) her bir işletim sistemi ya da sunucu için tam bir işletim sistemine sahiptir. Docker ise işletim sisteminin tamamının yerine boyut olarak indirgenmiş Images'leri kullanmaktadır (Combe ve ark., 2016). İşletim sisteminin tüm kütüphaneleri paylaşımlı olarak kullanılabilmesine imkân vermektedir. Ancak bu yapı Docker'i sistem kaynak tüketim konusunda avantajını gösterirken, izolasyon seviyesini de düşürmektedir. Docker ve VM'ler için kullanım açısından değerlendirildiğinde (Çizelge 4.1) Docker'ın daha avantajlı olduğu görülmektedir. Docker, hız, taşınabilirlik, ölçeklenebilirlik, hızlı teslimat ve yoğunluk gibi avantajlara sahiptir (Rad ve ark., 2017).

Çizelge 4.1. Docker ve VM karşılaştırması

Kıyas türü	**VM**	**Docker**
OS	Tam işletim sistemi	Küçültülmüş işletim sistemi imajı
İzolasyon	Yüksek	Daha düşük
Çalışır hale gelmesi	Dakikalar	Saniyeler
Versiyonlama	Yok	Yüksek
Kolay paylaşılabilirlik	Düşük	Yüksek

4.2.2. Kali linux işletim sistemi

Kali Linux işletim sistemi, BackTrack tarafından 2013 yılında Linux işletim sisteminin siber güvenlik için oluşturulmuş olan bir Debian tabanlı işletim sistemidir ve sızma test ortamları ve güvenlik denetimleri için kullanılmaktadır (Linux, 2020).
Kali işletim sistemi içerisinde kullanılabilir araçlar çok çeşitlidir: Bilgi toplama, Güvenlik açığı analizi, Kablosuz saldırılar, Web uygulamaları, İstismar araçları, Adli tıp araçları, Stres testi, Sniffing ve Sızdırma, Parola saldırıları, Bakım saldırılar, Tersine mühendislik, Donanım korsanlığı ve Raporlama araçları gibi araçlar içerisinde hazır olarak gelmektedir. Diğer Linux işletim sistemlerinden ayıran noktalardan birisi bu araçların hazır olarak gelmesidir. Fakat diğer Linux işletim sistemlerine de bu araçlar tek tek kurulabilmektedir. Ayrıca Kali Linux, Nmap (bağlantı noktası tarayıcı), Wireshark (paket analizcisi), John The Ripper (şifre kırıcı), Aircrack-ng (kablosuz LAN'lara sızma testi için yazılım paketi), Nikto (web sunucusu tarayıcı), Sqlmap (SQL enjeksiyon kusurlarını tespit etmek ve kullanmak ve veri tabanı sunucularını devralmak için araç), OwaspZap (web uygulamalarındaki güvenlik açıklarını bulmak), Metasploit Çerçevesi (sömürü) ve diğer araçları içermektedir (Cisar ve Pinter, 2019).

Özellikle siber güvenlik alanında çalışanların kolaylıkla ulaşabileceği araçlar işletim sistemi içerisinde hazır gelmektedir.

4.2.3. Wireshark

Wireshark programı ağ trafiğinin, bir grafik arayüz üzerinden izlenmesini ve analiz edilmesine olanak sağlayan, ağ trafiğinde birçok önemli özelliğe sahip bir programdır(Wang ve ark., 2010). Wireshark programının kurulu olduğu bilgisayar üzerinden anlık olarak ağ trafiği izlenebilmekte ayrıca daha önceden kaydedilmiş dosyaların incelenmesi amacı ile de kullanılabilen ücretsiz ve açık kaynaklı bir paket yakalama programıdır. Wireshark, gerçek zamanlı ağ paketlerini yakalamak için pcap kütüphanesinden yararlanmaktadır (Munz ve Carle, 2008). Bu program siber güvenlik alanında çalışanlar için çok kullanışlı bir programdır. Bunun sebebi ağa gönderilen ve ağa gelen paketler pcap dosyaları olarak kaydedilebilir ayrıca kaydedilen bu pcap dosyalarını analiz etmek için kullanır. Zararlı yazılım analizinde kullanıldığı için bu çalışmada tercih edilmiştir. Wireshark Kali Linux İşletim Sisteminde kurulu olarak gelmektedir. Fakat kurulu gelmeyen Linux sistemlerini kurulum yapılması çok kolaydır, “sudo apt install

Wireshark" kodu terminal ekranında çalıştırıldığında program internet üzerinden otomatik olarak Linux sistemlere kurulumu gerçekleşmektedir.

4.2.4. Hping3 araçları

Hping, ağ paket oluşturma ve ağ paket analizi için kullanılan bir TCP/IP komut satırı aracıdır. TCP/IP paket çözümleyicisi olarak da bilinmektedir. Klasik Ping komutundan daha gelişmiş bir komut satırı tabanlı bir araçtır ve rastgele kaynaklarla büyük ölçekli DDOS saldırıları oluşturmak için en sık kullanılan araçlardan birisidir (Gandhi ve Kansal, 2019). TCL dilinde kodlanan Hping3, veri paketlerinin ikili veya dize gösterimini tanımlayarak veri paketlerini alan veya gönderen bir paket oluşturma aracıdır. Hping'i tüm özellikleriyle kullanabilmek, çıktılarını yorumlayabilmek için TCP/IP bilgisi gerekmektedir. Çünkü Hping3 TCP/IP komut satırı aracıdır. Hping3 komutu ile ping komutu gibi hedef IP adresine ya da hedef porta ağ paketleri gönderilir. Hping3 uygulaması, Linux tabanlı işletim sistemlerinin bazılarında (Kali işletim sistemi gibi) kurulu olarak gelen bir güvenlik uygulamasıdır. Kurulu olmayan sistemlere kurulumu kolaydır. Bu araç ile istenilen saldırı türüne göre paketler oluşturulabilir ve bu paketler hedef IP adresine gönderilir. Bu şekilde ağ testleri, Anti-DDoS Cihazları, Firewall ve IP adreslerine saldırılar için kullanılmaktadır. Hping3'ü komut satırında kullanmak için aldığı birtakım parametreler vardır. Bu parametrelerden birkaçı listelenmiştir (Çizelge 4.2).

Çizelge 4.2. Hping3 ile ilgili parametreler

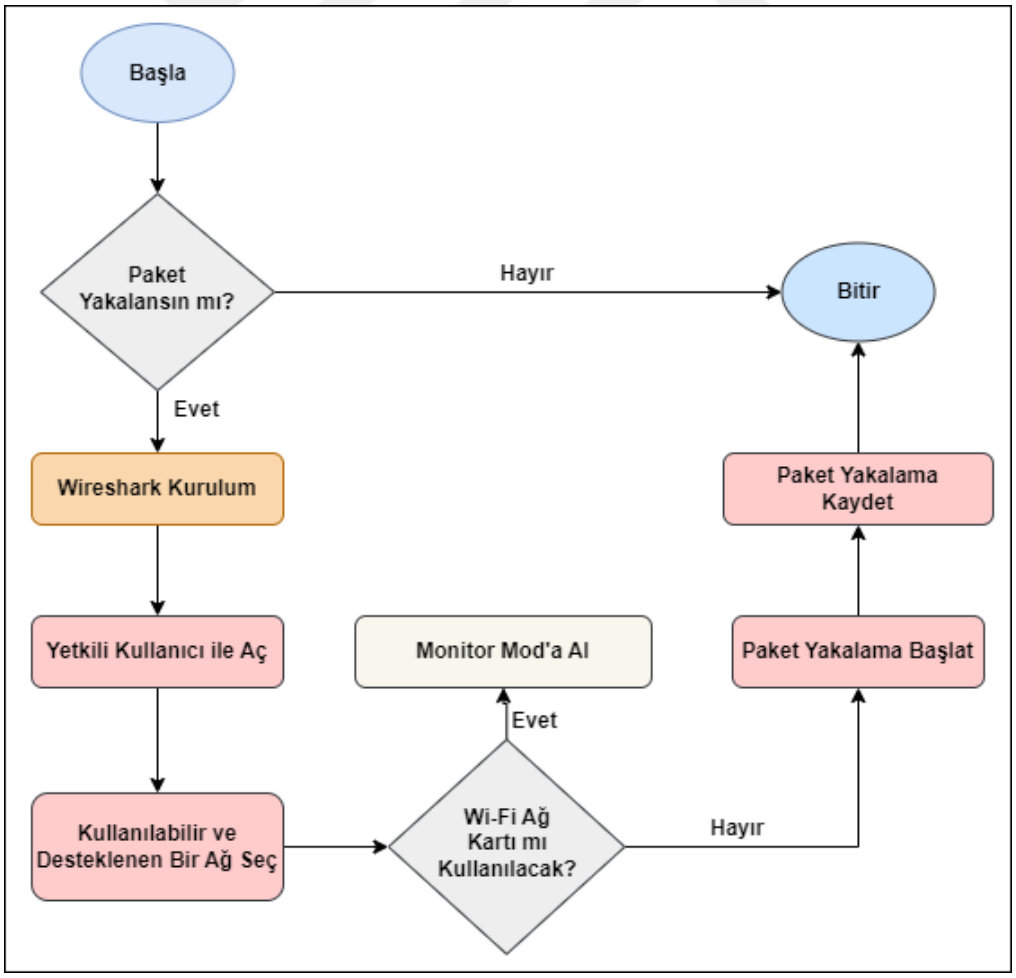
Parametre	***Açıklama***
-s	Syn paketi gönderir
-p	Hedef port numarası
-c	Gönderilecek paket sayısı
-d	Gönderilecek veri boyutu
–udp	Udp protokolünde paket yollar
–tcp	Tcp protokolünde paket yollar
–fast	Saniyede 10 paket gönderir
–faster	Saniyede 100 paket gönderir
–flood	Paketleri hızlı bir şekilde gönderir.
-a	Sahte IP adreslerinde paketler gönderir.
–rand-source	Rastgele IP adresleri üzerinden paketler gönderir.

Bu çalışmada hping3 aracı Kali Linux işletim Sistemi üzerinden kullanılarak SCADA sistemlere DDoS saldırıları düzenlenmiştir. Flood saldırıları en çok yapılan saldırılardır. Bu bağlamda protokol saldırılarından UDP, ICMP Flood ve TCP SYN saldırıları Nexusguard'ın Raporuna dikkat edilerek seçilmiştir.

DDoS saldırılarından UDP, TCP SYN ve ICMP flood saldırıları Hping3 kullanılarak oluşturulmuştur.

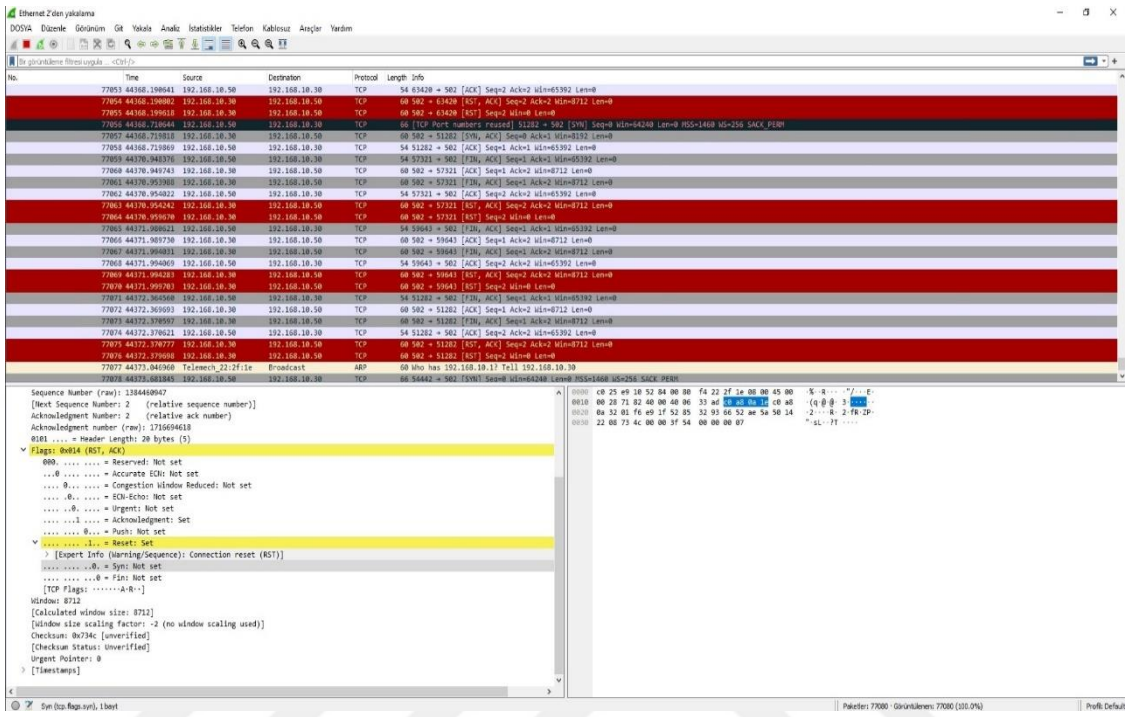
4.3. Paketlerin Yakalanması

Ağ paketleri farklı programlar, scriptler vs. ile kaydedilebilmektedir. Bu çalışmada ağ trafiğini izlemek ve ağdaki paketleri yakalamak için Wireshark programı kullanılmıştır. Wireshark ile ".pcap" dosyası formatında kaydedilen normal trafik verileri ve DDoS saldırısı olduğunda kaydedilen veriler 84 özellik alanından oluşmaktadır. Şekil 4.3'te Wireshark ile paket yakalama diyagramı gösterilmektedir.



Şekil 4.3. Wireshark ile paket yakalama diyagramı

Paket yakalama işlemi ağ analizi için, ağı değerlendirmek için önem arz etmektedir. Şekil 4.4'te hping3 saldırısı altında bulunan SCADA sistemine ait ağ trafiği gösterilmektedir.

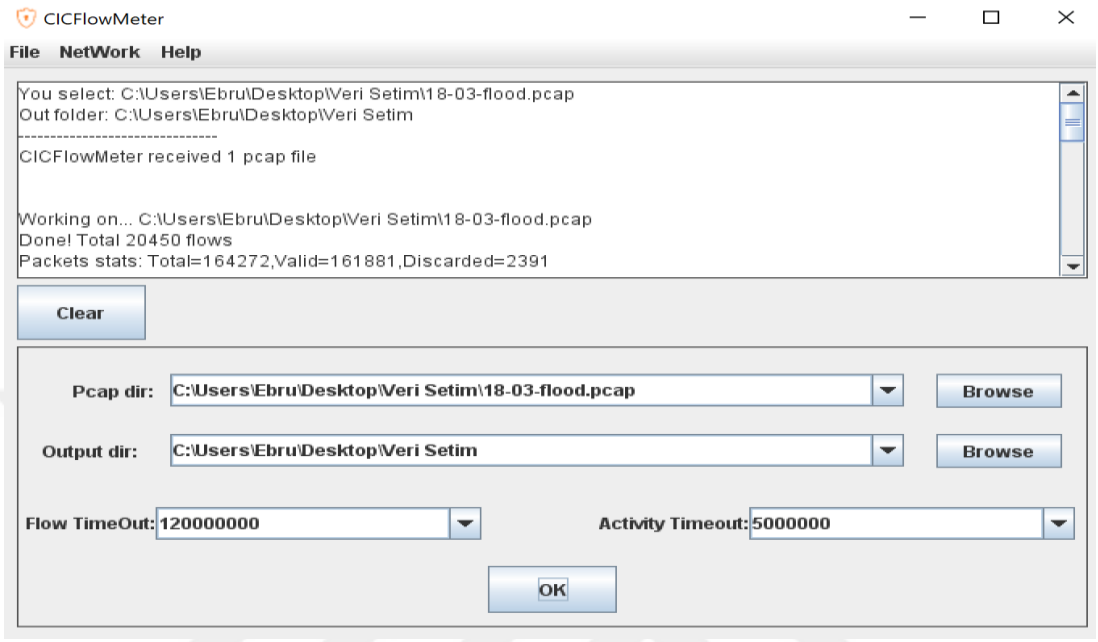


Şekil 4.4. Wireshark ile paket yakalama

4.4. Paketlerin Analizi

Ağ paketlerinin analizi ve görüntülenmesi işlemi için kullan Canadian Institute for Cybersecurity tarafından geliştirilen açık kaynak kodlu yazılım olan CICFlowMeter aracı kullanılmıştır. Wireshark ile yakalanan normal ağ trafiği verileri ile, DDoS saldırıları altındayken yakalanan ağ paketleri ".pcap" dosya formatından ML ve DÖ algoritmalarında işlenmesi için CICFlowMeter-4.0 (Cybersecurity, 2017) ile ".csv" uzantılı dosya formatına dönüştürülmüştür. Bu sayede en sık kullanılan 84 özellik alanı incelenmiş ve analizi gerçekleştirilmiştir. Çıkarılan özellikler Çizelge 4.6'da detaylı olarak gösterilmiştir. Paket analizinde faklı programlar kullanılmaktadır fakat en yaygın tercih edilen programlardan birisi olması nedeniyle bu çalışmada CICFlowMeter-4.0 tercih edilmiştir. Kullanılan programın arayüzü şekildeki gibidir (Şekil 4.5). Bu program ayrıca paket yakalama için de kullanılmaktadır. Bunun için sistemde bulunan ağ kartlarının yüklenmesi ve paket yakalama işlemine başlatılması gerekmektedir. Bu

çalışmada Wireshark ile elde edilen dosyaların format dönüştürülmesi amacı ile ofline modunda kullanılmıştır. Yüksek miktarda veri içeren dosyalarda hızlı dönüştürme işlemi gerçekleştirdiği için tercih edilmektedir.



Şekil 4.5. CICFlowMeter programı arayüzü

Öneriler bölümünde kaydedilen ".pcap" uzantılı ham verilere başka çalışmalarda kullanılması amacıyla kamuya açık platformalarda paylaşılması önerilmiştir.

4.5. Makine Öğrenmesi

Makine öğrenmesi, yapay zekânın kapsadığı alanlardan birisi olmak ile beraber birçok problemin çözümünde kullanılan çeşitli algoritmalar içermektedir. Bu tez kapsamında beş farklı MÖ algoritması ile veri setleri üzerinde ikili ve çoklu sınıflandırma işlemi gerçekleştirilmiştir. Kullanılan MÖ algoritmaları: Logistic regresyon, Navie Bayes, K en yakın komşu, karar ağaçları ve rasgele orman algoritmalarıdır. Bu algoritmalar kısaca açıklanarak, avantaj dezavantajları Çizelge 4.3'te de karşılaştırmaları incelenmiştir.

4.5.1. Logistic regresyon (LR)

Lojistik regresyon, yeni bir örneğin hedef sınıflardan birine ait olup olmama olasılığını tahmin etmek için veri kümesinin özelliklerinden faydalanarak ikili veri sınıflandırmasında sıklıkla kullanılan makine öğrenmesi algoritmasıdır.

4.5.2. Navie bayes (NB)

Naive Bayes algoritması, bir sınıflandırma algoritmasıdır. Naive Bayes algoritması, her özelliğin sınıflandırılmış veriyle olan ilişkisini hesaplar. Bu ilişki, Bayes teoremi kullanılarak belirlenir. Bayes teoremi, bir olayın gerçekleşme olasılığını, o olayın meydana gelmesine katkıda bulunan faktörlere bağlı olarak hesaplayan bir teoremdir (Webb ve ark., 2010). Naive Bayes algoritması, basit ve hızlı çalışması, veri kümesinin boyutuna göre ölçeklenebilir olması, az miktarda veri kullanarak doğru sonuçlar verebilmesi gibi avantajlara sahiptir.

4.5.3 K en yakın komşu (KEYK)

K en Yakın Komşu algoritması, sınıflandırılacak örnek veri noktasının olduğu sınıfın ve en yakın komşu elemanının, k değerine göre belirlendiği bir makine öğrenme yöntemi olarak ifade edilmektedir. KEYK algoritması benzer sınıflara sahip örneklerin birbirlerine yakın olması gerekir varsayımına dayanır. Bu varsayıma göre, her örnek kendisine en yakın k adet örnekten en fazla hangi örneğin sınıfına benziyorsa o örnekle ilişkilendirilir. Örnekler arasındaki uzaklık ilişkisi Öklid, Minkowski, Manhattan gibi yöntemlerle bulunabilir.

4.5.4. Karar ağaçları (KA)

Karar ağacı algoritması, sınıflandırma algoritmalarından birisidir. Önceden belirlenmiş sınıf değişkenine sahiplerdir. Yapıları itibariyle yukarıdan aşağıya inen bir yöntem sunmaktadırlar (Kantardzic, 2011). Bu ağaçtaki iç düğümler öznitelik değerine göre karşılaştırılırlar ve düğümün altındaki dallar farklı öznitelik değerlerine göre değerlendirilir (Zhong, 2016). Nihai sonuç, yaprak düğümlerinden elde edilebilir. Tüm süreç, yeni düğümde kök ağacın alt öğesi olarak tekrarlanmaktadır. Bir karar ağacı, çok

sayıda örnek içeren bir veri setini, bir takım karar kuralları uygulayarak bölme işlemi gerçekleştirerek sınıflandırma yapan yöntemdir.

4.5.5. Rasgele orman (RO)

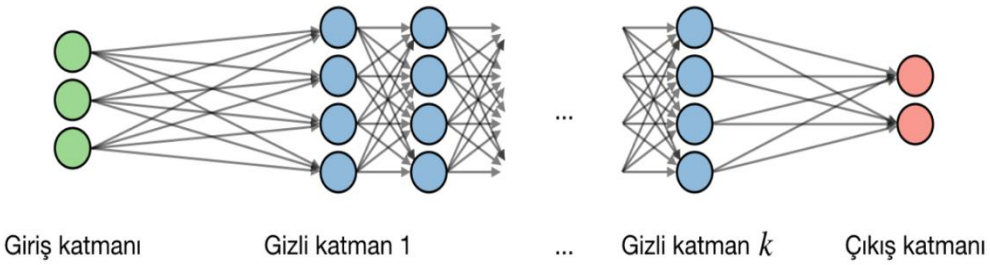
Rastgele Orman (Random Forest) 2001 yılında Leo Breiman tarafından geliştirilen sınıflama ve regresyon algoritmasıdır (Biau ve Scornet, 2016). Rasgele orman algoritması aslında birkaç rasgele karar ağacının sonundaki sınıf tahminlerini ortalama alarak ortak bir sonuca ulaşılmasıdır. Birkaç rasgele karar ağacını birleştiren ve tahminlerini ortalama alarak toplayan yaklaşım, değişken sayısının gözlem sayısından çok daha fazla olduğu durumlarda iyi sonuçlar vermektedir.

4.6. Derin Öğrenme

Derin öğrenme, arka arkaya gelen katmanların verileri işlenirken daha da artan şekilde kullanışlı gösterimler elde edilebilen makine öğrenmesinin bir alt dalıdır (Chollet, 2021). Bir diğer deyişle derin öğrenme, kullanılan verilerin sonucunda faydalı çıkarımlar elde edebilen matematiksel bir araç olarak ifade de edilebilir. DÖ'de oluşturulan modelde katman sayısı kavramı modelin derinliği ifade etmektedir. Birçok katmandan oluşan DÖ modelleri oluşturulabilmektedir. Kullanılacak verinin çeşidi DÖ'yi MÖ'ne göre daha avantajlı kılmaktadır. Bu yapıdan kaynaklı arka arkaya gelen katmanlar sinir ağı olarak ifade edilir ve sinir ağları sayesinde modeller öğrenme davranışını gösterir (Chollet, 2021). Aslında DÖ kullanılan verilerden yararlı sonuçlar elde edebilen matematiksel bir araç olarak ifade de edilebilir. DÖ ile MÖ'nin karşılaştığı zor verilerden başarılı sonuçlar elde edilebilmektedir. Bunlar: görüntü sınıflandırma, el yazısı tanıma, ses tanıma, metin verilerinden ses oluşturma, hedef kitle tespiti, metin verilerinden duygu analizi vb. gibi daha birçok alanda sıralanabilir. En çok kullanılan derin öğrenme kütüphaneleri ise TensorFlow ve Keras'tır. TensorFlow, ilk olarak Google'ın Makine Zekâsı araştırma kuruluşu bünyesinde Google Beyin Ekibi tarafından geliştirilmiştir. TensorFlow, ML de araştırmayı kolaylaştırmak ve prototiplerden üretim sistemine geçişi sağlamak için tasarlanmıştır (Abadi ve ark., 2016). Keras, Python'da yazılmış ve TensorFlow üzerinde çalışabilen üst düzey bir sinir ağları uygulama programlama ara yüzüdür.

4.6.1. Yapay sinir ağları (YSA)

Yapay sinir ağları (YSA'lar), katmanlarla oluşturulan bir modeller sınıfıdır. Biyolojik sinir ağlarından ilham alan YSA'lar, çok sayıda ara bağlantıya sahip çok sayıda basit işlemciden oluşan büyük ölçüde paralel bilgi işlem sistemleridir. YSA'lar, doğal nöronlardan ilham alan bir hesaplama modelidir ve YSA'ların işlevi bilgiyi işleme amacı ile kullanıldığı için daha çok mühendislik alanlarında tercih edilmektedir (Gupta, 2013). Gerçek sinir ağlarını modellemek ve makinelerde davranışı incelemek için kullanılan çok çeşitli YSA'lar vardır ve YSA'ların en çok kullanılan yöntemleri ise; evrişimsel sinir ağları (ESA) ve tekrarlayan sinir ağlarıdır (TSA). YSA'lar genel olarak katmanlı mimariden oluştuğu için giriş katmanı, çıkış katmanı ve arada gizli katmanlar bulunmaktadır (Şekil 4.6). YSA, karmaşık doğrusal olmayan ilişkileri modelleme yeteneğine sahiptir. YSA ayrıca mükemmel hata toleransına sahiptir ve paralel işleme ile hızlı ve yüksek düzeyde ölçeklenebilirdir.

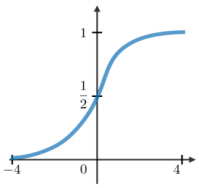
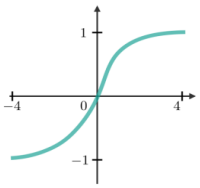
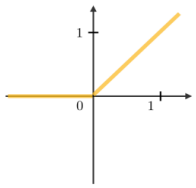
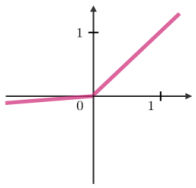


Şekil 4.6. Yapar sinir ağı modeli (Amidi ve Amidi)

Matematiksel olarak YSA'ların yapısında ağın *i*. Sırasındaki katmana *i* ve *j*. Sırasındaki gizli birim *j* ile ifade edildiğinde, (4.1) denklemi elde edilir. Bu denklemde *z*, *w*, *b* değerleri sırasıyla ürün, ağırlık ve eğilimi ifade etmektedir.

$$z_j^{[i]} = {w_j^{[i]}}^T x + b_j^{[i]} \tag{4.1}$$

Sinir ağlarında aktivasyon fonksiyonları kullanılmaktadır. Aktivasyon fonksiyonları gizli birimlerin sonunda, modele doğrusal olmayan karmaşıklıklar eklemek için kullanılır (Amidi ve Amidi). Yaygın olarak modellerde kullanılan aktivasyon fonksiyonları Şekil 4.7'de listelenmiştir:

Sigmoid	Tanh	ReLU	Leaky ReLU
$g(z) = \frac{1}{1+e^{-z}}$	$g(z) = \frac{e^{z}-e^{-z}}{e^{z}+e^{-z}}$	$g(z) = \max(0,z)$	$g(z) = \max(\epsilon z, z)$ ile $\epsilon \ll 1$
			

Şekil 4.7. Aktivasyon fonksiyonları (Amidi ve Amidi)

Çapraz entropi kaybı L(z,y) ise YSA'lar içerisine, sıklıkla kullanılır ve denklem 4.2'deki gibi formüle edilmiştir:

$$L(z,y) = -\Big[y\log(z) + (1-y)\log(1-z)\Big] \tag{4.2}$$

Öğrenme oranı ise genellikle α veya η olarak belirtilir, ağırlıkların hangi tempoda güncellendiğini göstermektedir. Bu derece sabit veya uyarlamalı olarak değişebilmektedir (Gupta, 2013). Yaygın olarak kullanılan yöntemler Adam ve RMSprop olarak ifade edilen ve öğrenme oranını ayarlayan yöntemlerdir.

Geri yayılım ise sinir ağındaki ağırlıkları güncellemek için kullanılan ve gerçek sonuç ile beklenilen sonucun arasındaki mesafeyi hesaplayan bir yöntemdir (Chollet, 2021). Ağırlık w değerine göre türev, zincir kuralı kullanılarak hesaplatılan denklemi 4.3'te verilmiştir:

$$\frac{\partial L(z,y)}{\partial w} = \frac{\partial L(z,y)}{\partial a} \times \frac{\partial a}{\partial z} \times \frac{\partial z}{\partial w} \tag{4.3}$$

Sonuç olarak, ağırlık güncellenmesi aşağıdaki denklem 4.4'teki gibidir:

$$w \longleftarrow w - \eta \frac{\partial L(z,y)}{\partial w} \tag{4.4}$$

Bir YSA'nın ağırlıkları güncellenirken Amidi ve Amidi'ye göre sırası ile yapılacak işlemler şu şekildedir:

• 1. İşlem: Bir eğitim veri seti alınır.

• 2. İşlem: Denk gelen kaybı elde etmek için, ileri yayılım gerçekleştirilir.

• 3. İşlem: Gradyanları elde etmek için kayba geri yayılım uygulanır.

• 4. İşlem: Ağın ağırlıklarını güncellemek için gradyanlar kullanılır (Amidi ve Amidi).

Bırakma ise, eğitim verisinin aşırı uymasını engellemek için YSA'daki nöronları azaltma yoluyla uygulanan bir tekniktir. Pratikte, nöronlar ya p olasılığıyla azaltılır ya da 1 – p olasılığıyla tutulmaktadır.

4.6.2. Evrişimsel Sinir Ağları (ESA)

Evrişimsel Sinir Ağları (ESA), birçok farklı uygulama alanında kullanılan, özellikle görüntü işlemede sıkça kullanılan derin öğrenme modelleridir. Yapay sinir ağlarındaki bir alt sınıf olarak kabul edilen ESA'lar, verilerin önceden belirlenmiş birçok katmanda işlenmesini ve bu şekilde özelliklerin tanınmasını sağlarlar (O'Shea ve Nash, 2015). Bu katmanlar, önceki katmanların çıktılarına dayanarak, nesnelerin daha karmaşık özelliklerini tanımlamak için daha yüksek seviyeli özellikleri çıkarabilirler (Albawi ve ark., 2017). ESA'lar ayrıca, dil işleme ve siber güvenlik gibi diğer uygulama alanlarında da kullanılmaktadır. ESA'lar, genellikle ağ trafiği analizi ve sınıflandırma problemlerinde kullanılırlar. Bu nedenle, DDoS saldırıları gibi ağ trafiğini etkileyen durumlarda kullanılan bir modeldir. Bu nedenle DDoS saldırılarına karşı savunma amaçlı kullanılabilirler.

4.6.3. Tekrarlayan Sinir Ağları (TSA)

Tekrarlayan Sinir Ağları (TSA), sıralı verilerle çalışan derin öğrenme modelleridir. Girdiler arasındaki zaman bağımlılığını modellemek için kullanılırlar. Bu nedenle, doğal dil işleme, konuşma tanıma ve zaman serileri analizi gibi alanlarda yaygın olarak kullanılmaktadırlar. TSA'lar, girdilerin önceden belirlenmiş bir sayıda dönüşümden geçtiği ardışık katmanlardan oluşur. Her katman, önceki adımların çıktılarına dayanarak bir sonraki adımın çıktısını hesaplamak için tekrar kullanılır (Chen, 2016). DDoS saldırıları, genellikle ağ trafiği üzerinde birçok farklı örüntü üretirler.

TSA'lar, bu örüntüleri tanımlamak ve saldırıları tespit etmek için kullanılan DÖ modellerinden birisidir.

4.6.4. Uzun Kısa Süreli Bellek (UKSB)

Uzun Kısa Süreli Bellek (UKSB), DÖ yöntemleri arasında sıkça kullanılan bir yapay sinir ağıdır. Bu yöntem, diğer sinir ağı modellerindeki aşırı öğrenme ve gradiyent kaybı sorunlarını da çözebilen bir yapıya sahiptir. UKSB, her hücrede bulunan üç anahtar bileşen olan "unutma kapısı", "güncelleme kapısı" ve "çıkış kapısı" aracılığıyla verileri işler. Bu bileşenler sayesinde, UKSB, geçmiş verileri hafızasında tutarak gelecekteki tahminlerini geliştirebilir (Van Houdt ve ark., 2020). UKSB, doğal dil işleme, ses tanıma ve otomatik çeviri gibi birçok alanda başarılı sonuçlar veren bir modeldir.

UKSB, siber güvenlik alanında da önemli bir rol oynamaktadır. Özellikle DDoS saldırılarına karşı savunmada kullanılan bir yöntemdir. UKSB, DDoS saldırılarına karşı, ağdaki trafiği analiz ederek anomali davranışları tespit edebilir ve hedef sistemlerin korunmasına yardımcı olabilir. UKSB, geçmiş trafik verileriyle eğitilerek, normal ağ trafiği desenlerini öğrenir ve ağda anormal davranışlar tespit edildiğinde, bu davranışları engelleyerek saldırıyı önleyebilir.

Çizelge 4.3. MÖ modelleri karşılaştırması

Algoritma	Açıklama	Avantajlar	Dezavantajlar
Logistic Regresyon (LR)	İkili veya çoklu sınıflandırma problemleri için kullanılır.	Basit ve hızlı bir algoritmadır.	Yüksek boyutlu veri setleri için performans sorunu olabilir.
Navie Bayes (NB)	Olasılık temelli bir sınıflandırma algoritmasıdır.	Hızlı ve düşük bellek kullanımı gerektirir.	Bağımsızlık varsayımı gerçek hayatta her zaman geçerli olmayabilir.
Karar Ağaçları (KA)	Karar ağaçlarından oluşan bir sınıflandırma veya regresyon modelidir.	Kolay anlaşılır ve yorumlanabilir modeller üretir.	Veriye aşırı uyum sağlama (overfitting) eğilimi vardır.
Rasgele Orman (RO)	Birçok karar ağacının birleşimiyle oluşturulan bir ensemle modelidir.	Yüksek boyutlu veri setlerinde iyi performans gösterir.	Büyük veri setlerinde eğitim süresi uzun olabilir.
K En Yakın Komşu (KEYK)	Sınıflandırma veya regresyon problemleri için kullanılır.	Basit ve hızlı bir algoritmadır.	Veri seti büyüdükçe hesaplama maliyeti artar.

Çizelge 4.4. DÖ modelleri karşılaştırması

Algoritma	Açıklama	Avantajlar	Dezavantajlar
Yapay Sinir Ağları (YSA)	Sinir hücrelerinden oluşan bir ağ yapısıdır.	Büyük ve karmaşık veri setlerinde güçlü performans gösterir.	Eğitim süreci zaman alabilir ve yüksek hesaplama gücü gerektirebilir.
Evrişimsel Sinir Ağları (ESA)	Görüntü veya ses gibi verileri işlemek için kullanılır.	Görüntü ve sese özgü özellik çıkarımında etkilidir.	Derin ağ yapısı nedeniyle aşırı öğrenme riski vardır.
Tekrarlayan Sinir Ağları (TSA)	Zaman serileri veya dil modelleri gibi sıralı verileri işlemek için kullanılır.	Geçmiş bilgiyi hatırlama yeteneği vardır.	Eğitim süreci zaman alabilir ve aşırı öğrenme eğilimi vardır.
Uzun Kısa Süreli Bellek (UKSB)	Tekrarlayan sinir ağlarına benzer, daha gelişmişmiş bir hafıza mekanizmasıdır. Daha uzun süreli bağımlılıkları işlemek için kullanılır.	Uzun süreli bağımlılıkları başarılı bir şekilde işleyebilir.	Daha karmaşık bir yapıya sahip olduğu için eğitim ve hesaplama maliyeti daha yüksektir.

Bu tez çalışmasında kullanılan MÖ ve DÖ modelleri Çizelge 4.3 ve Çizelge 4.4'te karşılaştırmalı olarak verilmiştir.

4.7. Değerlendirme Metrikleri

Bu çalışmada DÖ yöntemlerinden DDoS saldırılarının sınıflandırma işlemi için YSA, UKSB, TSA ve ESA yöntemleri, MÖ yöntemlerinden LR, RO, KA, NB ve KEYK kullanılmış ve modelin başarısı karmaşıklık matrisi ve diğer performans metriklerine göre değerlendirilmiştir.

4.7.1. Karmaşıklık matrisi

Kullanılan sınıflandırma algoritmaları performans metriklerine göre değerlendirilmiştir. Performans özetlemek için ise karmaşıklık matrisi kullanılmıştır.

Çizelge 4.5. Karmaşıklık matrisi

		Gerçek Sınıf	
		Pozitif	**Negatif**
Tahmin Edilen Sınıf	**Pozitif**	Doğru Pozitif (TP)	Yanlış Pozitif (FP)
	Negatif	Yanlış Negatif (FN)	Doğru Negatif (TN)

Çizelge 4.5'te gösterilen karmaşıklık matrisi parametreleri açıklanacak olursa sırası ile;

- Doğru Pozitif (TP) : Doğru sınıflandırılan durumların sayısını verir.
- Yanlış Pozitif (FP) : Yanlışlıkla doğru sınıflandırılan durumların sayısını verir.
- Doğru Negatif (TN) : Doğru sınıflandırılan negatif durumların sayısını verir.
- Yanlış Negatif (FN) : Yanlışlıkla negatif sınıflandırılan durumların sayısını verir.

TP & TN : Sınıfların doğru tahmin edildiği rakamını vermektedir.

FN & FP : Sınıfların birbirleri ile olan yanlış tahmin adetlerini vermektedir (Pushpa Singh, 2021).

4.7.2. Performans metrikleri

Değerlendirme ölçütü olarak karmaşıklık matrisi ile diğer metriklerde kullanmak modelin başarısı hakkında detaylı bilgi almayı sağlar. Bu nedenle matristen elde edilen veriler kullanılarak bazı ölçüm parametrelerine ihtiyaç duyulmaktadır.

- Doğruluk (Accuracy): Model başarısının ölçülmesinde basit ve popüler bir yöntem olan değerinden faydalanılabilir. Doğru sınıflandırılmış örnek sayısının toplam örnek sayısına oranı olarak denklem 4.5'te ifade edilmektedir.

$$Accuracy(\ Doğruluk) = \frac{(\ TP + TN)}{(\ TP + FP + FN + TN)} \tag{4.5}$$

- Kesinlik (Precision) : Bu değeri belirleyen faktör ise doğru sınıflandırılmış verinin o sınıfa ait tüm örneklerine oranı olarak hesaplanmaktadır (Denklem 4.6). Doğru tahmin edilen değerlerin, yanlış tahmin edilen değerlerden fazla olması kesinlik değerinin yüksek olduğunu ifade etmektedir ve bu değerin %100'e yakın olması önemlidir (Sokolova ve Lapalme, 2009).

$$Precision(\ Kesinlik) = \frac{TP}{TP + FP} \tag{4.6}$$

- Duyarlılık (Recall): Doğru olarak sınıflandırılan pozitif örneklerin diğer tüm pozitif örnekler sayısına oranı olarak ifade edilmektedir (Denklem 4.7).

$$Recall(\ Duyarlılık) = \frac{TP}{TP + FN} \tag{4.7}$$

- F1-Score : Kesinlik ve duyarlılık ölçütlerinin harmonik ortalaması olarak ifade edilmektedir (Denklem 4.8).

$$F1 - Score = \frac{2 \times (\ precision \times recall)}{precision + recall} \tag{4.8}$$

Bu çalışma da DÖ tabanlı saldırı tespit sistemleri için bir model geliştirilmiştir ve modelin saldırıları tespit etmedeki başarısı diğer çalışmalar ile karşılaştırılmıştır.

Literatürde yapılan çalışmalar incelendiğinde sık kullanılan ve güncel olan hazır veri seti tercih edilmiştir. Bu çalışmada da hazır veri seti olan CIC-DDoS2019 veri seti ve SCADA sistemlerine düzenlenen DDoS saldırılarından elde edilen deneysel veri seti kullanılmıştır. Veri seti oluşturma ve bu süreçte kullanılan araçlardan bahsedilmiştir.

4.8. Hazır Veri Seti

Bu çalışmada kullanılan veri seti DDoS saldırılarından oluşan CICDDoS2019 veri setidir (Sharafaldin ve ark., 2019). Bu veri seti, yazarlar tarafından günlük olarak düzenlenen bir veri setidir. CICFlowMeter-V3 kullanılarak 80'den fazla trafik özelliğini çıkarılmıştır. Her bir makine başına bir .csv dosyası olarak kaydedilmiştir.

CICDoS2019 veri seti, verileri iki güne ayırır. İlki, DNS, LDAP, MSSQL, NTP, NetBIOS, SYN, SNMP, SSDP, TFTP, UDP-Lag, UDP ve WebDDoS olmak üzere 12 tür farklı DDoS saldırısını içeren bir eğitim günüdür. İkincisi, LDAP, MSSQL, NetBIOS, SYN, UDP ve UDP-Lag ve olmak üzere 7 farklı DDoS saldırısı türünü içeren bir test günü olarak kaydedilmiştir.

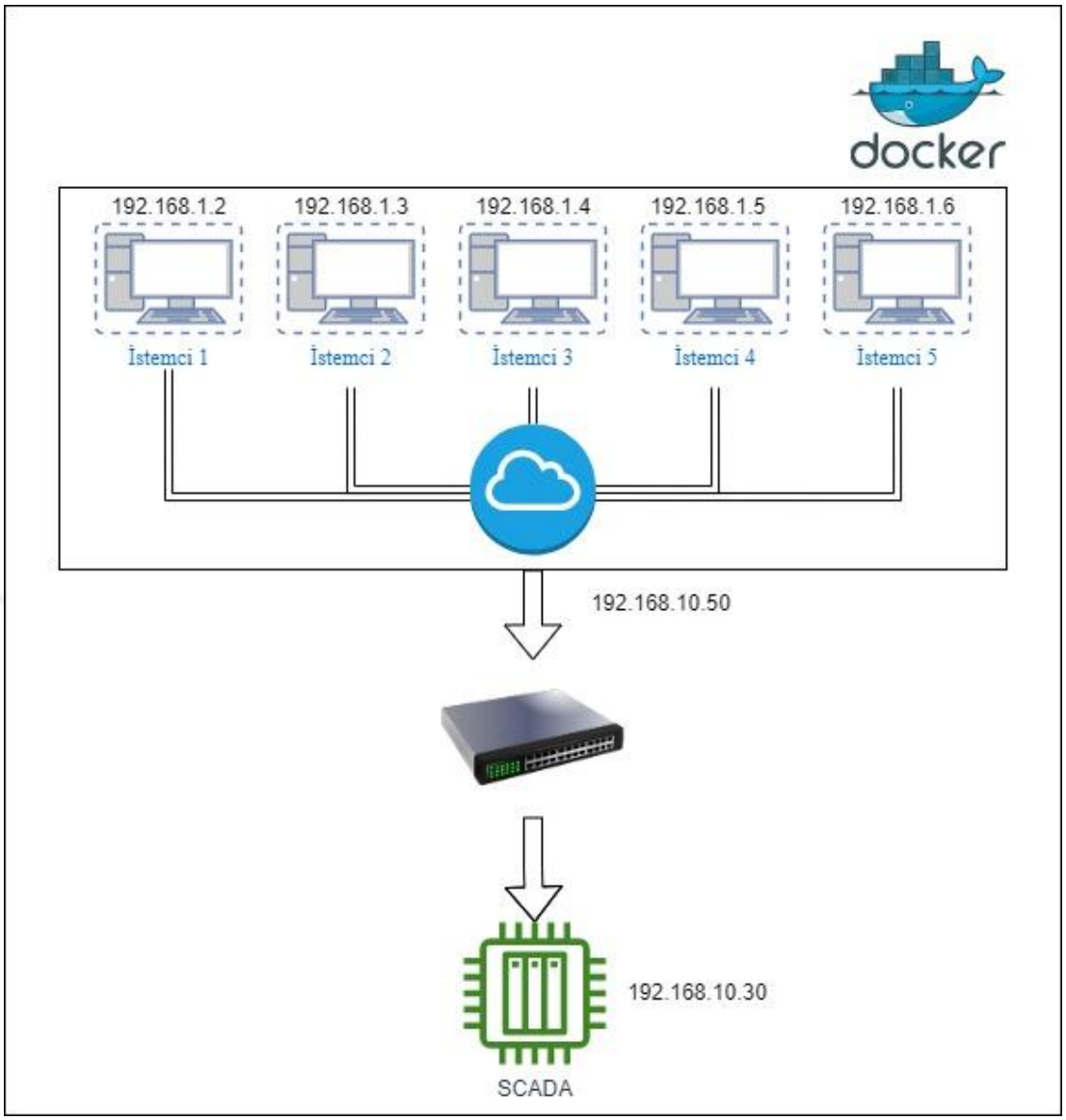
Bu veri seti, kaynak IP, hedef IP adresleri, bağlantı noktaları, kullanılan protokoller, bayraklar, sayaçlar ve akış tanımlama özellikleri gibi IP Akış özelliklerine sahip veriler sağlamaktadır.

4.9. Oluşturulan Veri Seti

Veri seti oluşturmak için öncelikle farklı günlerde saldırı olmadan SCADA sistemleri üzerinde 5 makineden veri okuması başlanmıştır. Bu işlem sırasında aktif olarak gelen giden paketler izlenmiş ve sisteme müdahale edilmemiştir. Saldırı olmadan toplanan veriler ".pcap" uzantılı dosyalar olarak kaydedilmiştir. Daha sonra bu veriler ".csv" uzantılı dosyalara dönüştürülerek veri seti özellikleri incelenmiştir.

Ağ paketi analizi yapıldığında çıkarılan özellikler açıklamaları ile Çizelge 4.6'da detaylı olarak verilmiştir.

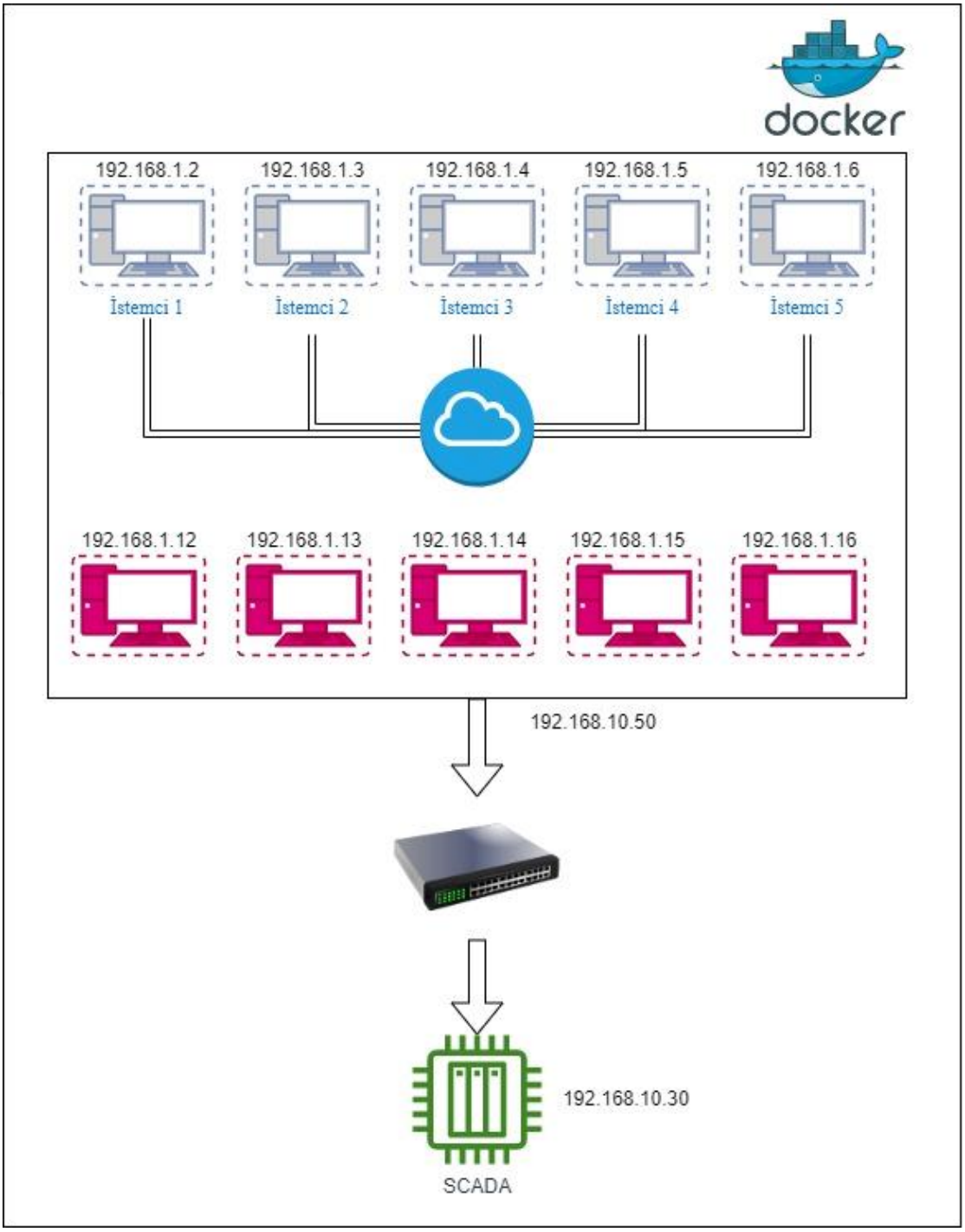
Veri toplamak için SCADA sistemine saldırı olmaksızın veri toplamak için oluşturulan ağ topolojisi Şekil 3.30'da gösterilmektedir. Burada Docker sanallaştırma ile oluşturulan 5 makine üzerinden SCADA sisteminde ağ paketlerinin okunması gerçekleştirilmiş ve sisteme herhangi bir müdahale edilmemiştir.



Şekil 4.8. Saldırı olmaksızın veri toplama için oluşturulan ağ topolojisi

Oluşturulan topolojide (Şekil 4.8), Docker sistemi üzerine kurulan IP adresleri sırasıyla 192.168.1.2 – 192.168.1.6 arasında olan 5 sanal makineden SCADA sisteminden veri alışverişi gerçekleştirilmiştir. Bu işlem sırasında kurulan ağın çıkış IP adresi 192.168.10.50'dir ve IP adresi 192.168.10.30 olan SCADA sistemi ile iletişim sağlanmıştır. Bu sayede 24 saat boyunca Wireshark programı ile veriler kaydedilmiştir. Veri toplamanın bir diğer aşamasında SCADA sistemine 3 ayrı DDoS saldırısı düzenlenmiştir. Bu saldırılar gerçekleştiği anda sistemi devre dışı hale getirirken toplanan veriler de ayrı ayrı .pcap dosyaları olarak kaydedilmiştir ve daha sonra .csv uzantılı dosyalara çevrilmiştir. Saldırı anında botnetler kullanılarak DDoS saldırıları

gerçekleştirilerek aktif olarak çalışan sistem hizmet dışı bırakılmıştır. Örnek olarak saldırı anında SCADA sistemlerindeki ağ topolojisi görülmektedir (Şekil 4.9).



Şekil 4.9. Saldırı anında veri toplama için oluşturulan ağ topolojisi

Çizelge 4.6. Elde edilen verilerin özellik ve açıklamaları

	Özellik Adı	Açıklaması		Özellik Adı	Açıklaması
1	**Flow ID**	Akışı tekil olarak tanımlayan ID	**43**	**Fwd Pkts/s**	İleri yöndeki akıştaki paket hızı
2	**Src IP**	Akışın kaynak IP adresi	**44**	**Bwd Pkts/s**	Geri yöndeki akıştaki paket hızı
3	**Src Port**	Kaynak IP adresinin kullanarak gönderdiği veri paketinin kaynak bağlantı noktası numarası	**45**	**Pkt Len Min**	Tüm paketlerin minimum uzunluğu
4	**Dst IP**	Akışın hedef IP adresi	**46**	**Pkt Len Max**	Tüm paketlerin maksimum uzunluğu
5	**Dst Port**	Hedef IP adresinin kullanarak gönderdiği veri paketinin hedef bağlantı noktası numarası.	**47**	**Pkt Len Mean**	Tüm paketlerin ortalama uzunluğu
6	**Protocol**	Akıştaki veri paketleri için kullanılan protokol numarası.	**48**	**Pkt Len Std**	Tüm paketlerin standart sapması
7	**Timestamp**	Akışın oluştuğu zaman damgası (milisaniye cinsinden).	**49**	**Pkt Len Var**	Tüm paketlerin varyansı
8	**Flow Duration**	Akışın başlangıcından sonuna kadar geçen süre (mikro saniye cinsinden).	**50**	**FIN Flag Cnt**	Tüm akışlardaki FIN bayraklarının sayısı
9	**Tot Fwd Pkts**	İleri doğru yönlendirilen toplam veri paketi sayısı.	**51**	**SYN Flag Cnt**	Tüm akışlardaki SYN bayraklarının sayısı
10	**Tot Bwd Pkts**	Geri doğru yönlendirilen toplam veri paketi sayısı	**52**	**RST Flag Cnt**	Tüm akışlardaki RST bayraklarının sayısı
11	**TotLen Fwd Pkts**	İleri doğru yönlendirilen toplam veri paketlerinin toplam boyutu (byte cinsinden).	**53**	**PSH Flag Cnt**	Tüm akışlardaki PSH bayraklarının sayısı
12	**TotLen Bwd Pkts**	Geri doğru yönlendirilen toplam veri paketlerinin toplam boyutu (byte cinsinden)	**54**	**ACK Flag Cnt**	Tüm akışlardaki ACK bayraklarının sayısı
13	**Fwd Pkt Len Max**	İleri doğru yönlendirilen en büyük veri paketi boyutu (byte cinsinden)	**55**	**URG Flag Cnt**	Tüm akışlardaki URG bayraklarının sayısı

14	**Fwd Pkt Len Min**	İleri doğru yönlendirilen en küçük veri paketi boyutu (byte cinsinden)	**56**	**CWE Flag Count**	Tüm akışlardaki CWE bayraklarının sayısı
15	**Fwd Pkt Len Mean**	İleri doğru yönlendirilen veri paketlerinin ortalama boyutu (byte cinsinden)	**57**	**ECE Flag Cnt**	Tüm akışlardaki ECE bayraklarının sayısı
16	**Fwd Pkt Len Std**	İleri doğru yönlendirilen veri paketlerinin standart sapması (byte cinsinden)	**58**	**Down/Up Ratio**	İleri ve geri yöndeki akışlardaki veri oranı
17	**Bwd Pkt Len Max**	Geri doğru yönlendirilen en büyük veri paketi boyutu (byte cinsinden)	**59**	**Pkt Size Avg**	Tüm paketlerin ortalama boyutu
18	**Bwd Pkt Len Min**	Geri doğru yönlendirilen en küçük veri paketi boyutu (byte cinsinden)	**60**	**Fwd Seg Size Avg**	İleri yöndeki akıştaki segmentlerin ortalama boyutu
19	**Bwd Pkt Len Mean**	Geri doğru yönlendirilen veri paketlerinin ortalama boyutu (byte cinsinden)	**61**	**Bwd Seg Size Avg**	Geri yöndeki akıştaki segmentlerin ortalama boyutu
20	**Bwd Pkt Len Std**	Geri doğru yönlendirilen veri paketlerinin standart sapması (byte cinsinden)	**62**	**Fwd Byts/b Avg**	İleri yöndeki akıştaki bayt/saniye hızının ortalama değeri
21	**Flow Byts/s**	Akışın aktarım hızı (byte/saniye cinsinden)	**63**	**Fwd Pkts/b Avg**	İleri yönde iletilen her paketin ortalama bayt sayısı
22	**Flow Pkts/s**	Akışın paket hızı (paket/saniye cinsinden)	**64**	**Fwd Blk Rate Avg**	İleri yönde iletilen bloke edilen paketlerin ortalama oranı
23	**Flow IAT Mean**	Ardışık veri paketleri arasındaki ortalama zaman aralığı (milisaniye cinsinden)	**65**	**Bwd Byts/b Avg**	Geri yönde iletilen her byte'ın ortalama paket sayısı
24	**Flow IAT Std**	Ardışık iki paket arasındaki zaman aralığının standart sapması (milisaniye cinsinden)	**66**	**Bwd Pkts/b Avg**	Geri yönde iletilen her paketin ortalama byte sayısı
25	**Flow IAT Max**	Ardışık veri paketleri arasındaki en büyük zaman aralığı (milisaniye cinsinden)	**67**	**Bwd Blk Rate Avg**	Geri yönde iletilen bloke edilen paketlerin ortalama oranı

26	**Flow IAT Min**	Ardışık veri paketleri arasındaki en küçük zaman aralığı (milisaniye cinsinden)	**68**	**Subflow Fwd Pkts**	İleri yönde iletilen alt akış paket sayısı
27	**Fwd IAT Tot**	İleri doğru yönlendirilen veri paketleri arasındaki toplam zaman aralığı (milisaniye cinsinden)	**69**	**Subflow Fwd Byts**	İleri yönde iletilen alt akış bayt sayısı
28	**Fwd IAT Mean**	İleri doğru yönlendirilen veri paketleri arasındaki ortalama zaman aralığı (milisaniye cinsinden)	**70**	**Subflow Bwd Pkts**	Geri yönde iletilen alt akış paket sayısı
29	**Fwd IAT Std**	İleri doğru yönlendirilen veri paketleri arasındaki standart sapma (milisaniye cinsinden)	**71**	**Subflow Bwd Byts**	Geri yönde iletilen alt akış bayt sayısı
30	**Fwd IAT Max**	İleri doğru yönlendirilen veri paketleri arasındaki en büyük zaman aralığı (milisaniye cinsinden)	**72**	**Init Fwd Win Byts**	İleri yönde başlatılan pencere boyutu (byte)
31	**Fwd IAT Min**	İleri doğru yönlendirilen veri paketleri arasındaki en küçük zaman aralığı (milisaniye cinsinden)	**73**	**Init Bwd Win Byts**	Geri yönde başlatılan pencere boyutu (byte)
32	**Bwd IAT Tot**	Geri yöndeki akıştaki aralıkların toplamı	**74**	**Fwd Act Data Pkts**	İleri yönde aktif veri paketi sayısı
33	**Bwd IAT Mean**	Geri yöndeki akıştaki aralıkların ortalaması	**75**	**Fwd Seg Size Min**	İleri yönde en küçük TCP segment boyutu
34	**Bwd IAT Std**	Geri yöndeki akıştaki aralıkların standart sapması	**76**	**Active Mean**	Bağlantı başına ortalama aktif süre (saniye)
35	**Bwd IAT Max**	Geri yöndeki akıştaki aralıkların maksimumu	**77**	**Active Std**	Bağlantı başına standart sapma aktif süre (saniye)
36	**Bwd IAT Min**	Geri yöndeki akıştaki aralıkların minimumu	**78**	**Active Max**	Bağlantı başına maksimum aktif süre (saniye)
37	**Fwd PSH Flags**	İleri yöndeki akıştaki PSH bayraklarının sayısı	**79**	**Active Min**	Bağlantı başına minimum aktif süre (saniye)

38	**Bwd PSH Flags**	Geri yöndeki akıştaki PSH bayraklarının sayısı	**80**	**Idle Mean**	Bağlantı başına ortalama boşta kalma süresi (saniye)
39	**Fwd URG Flags**	İleri yöndeki akıştaki URG bayraklarının sayısı	**81**	**Idle Std**	Bağlantı başına standart sapma boşta kalma süresi (saniye)
40	**Bwd URG Flags**	Geri yöndeki akıştaki URG bayraklarının sayısı	**82**	**Idle Max**	Bağlantı başına maksimum boşta kalma süresi (saniye)
41	**Fwd Header Len**	İleri yöndeki akıştaki başlık uzunluğu	**83**	**Idle Min**	Bağlantı başına minimum boşta kalma süresi (saniye)
42	**Bwd Header Len**	Geri yöndeki akıştaki başlık uzunluğu	**84**	**Label**	Ağ trafiği sınıflandırması

4.10. Veri Ön İşleme

Bu tez çalışması kapsamında CICDDoS2019 veri seti ve SCADA sistemlerine düzenlenen saldırılardan bu tez çalışması için oluşturulan veri seti kullanılmıştır. Veri setleri üzerinde uygulama gerçekleştirilmeden önce CICDDoS2019 veri seti ilk gün verilerinden oluşan 6 farklı ".csv" dosyasında bulunan veriler ve KEY2023 (Konelsis-Ebru Yağmur 2023) olarak adlandırılan veri seti, MÖ ve DÖ modelleri ile eğitilebilmesi için Python programlama dili kullanılarak veri ön işlemi uygulanmıştır.

4.10.1. CICDDoS2019 veri seti ön işlem

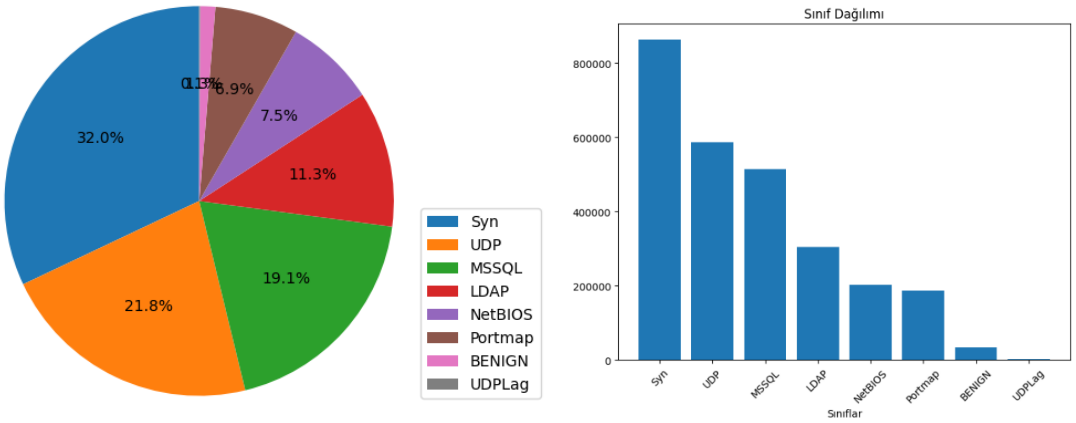
CICDDoS2019 veri setinde bu çalışmada kullanılan saldırı sınıfları ve bu sınıflara ait veri sayıları gösterildiği gibidir (Çizelge 4.7).

Çizelge 4.7. CICDDoS2019 veri setinde bulunan saldırı çeşitlerine göre veri sayısı

Normal	***Veri Sayısı***
BENIGN	30036
Saldırı Türü	***Veri Sayısı***
LDAP	303733
MSSQL	513714
NetBIOS	202919
Portmap	186960

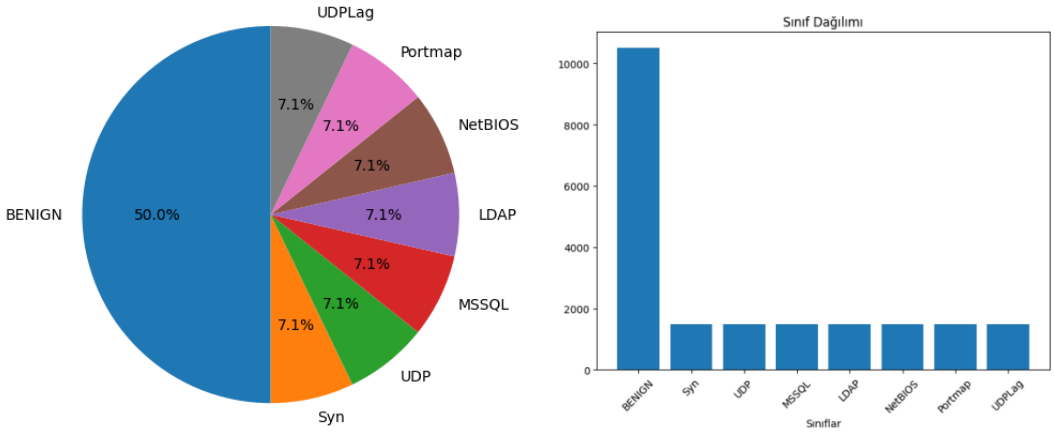
Syn	862107
UDP	586330
UDPLag	1873

CICDDoS2019 veri setinde bulunan özellikler KEY2023 veri setinde bulunan özellikler ile aynı olmasının yanında, "Fwd Header Length.1, Inbound ve SimillarHTTP" özelliklerini de içermektedir. Bu veri seti 86 özellik ve Label alanından oluşmaktadır. Veri setine ait sınıflar Şekil 4.10'da gösterildiği gibi dağılmaktadır.



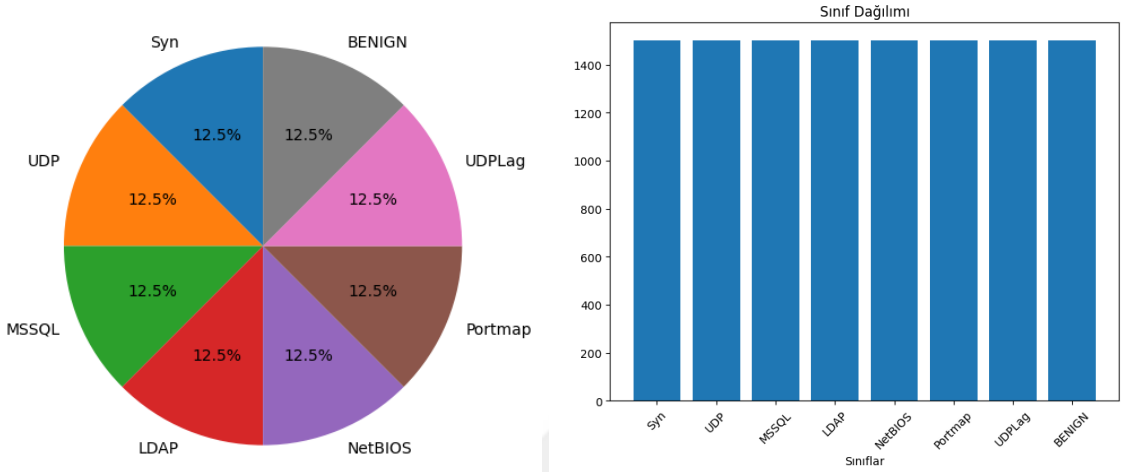
Şekil 4.10. CICDDoS2019 veri seti alanların dağılımı grafikleri

Veri setindeki dengesizlik farkının çok olduğu (Çizelge 4.7) görülmektedir. Bu çalışmada ikili sınıflandırma yapılabilmesi için verilerin dengesinin sağlanması gerekmektedir. Bunun için aşağı örnekleme yöntemi kullanılarak veri sayıları eşitlenmiştir (Şekil 4.11).



Şekil 4.11. CICDDoS2019 veri seti ikili sınıflandırma eşitlenen alanlar

Bu çalışma da çoklu sınıflandırma ile model performansları da değerlendirileceği için veri setinde bulunan alanlar eşit bir şekilde de dağıtılıp sınıflandırma yapmaya uygun hale getirilmiştir.



Şekil 4.12. CICDDoS2019 çoklu sınıflandırma için veri seti eşitlenen alanlar grafiği

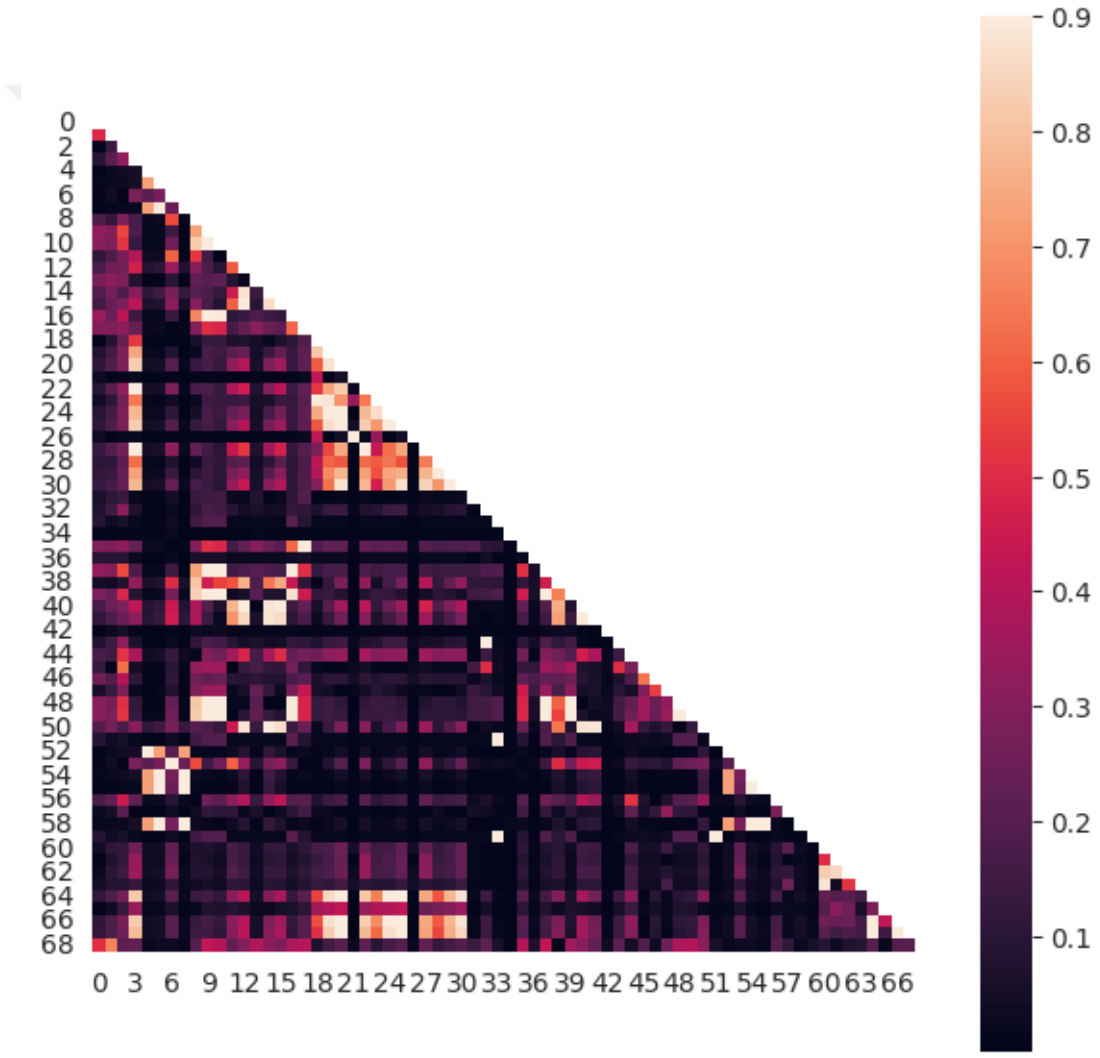
Veri setinde sınıflar, sınıflandırma modeline göre eşitlendikten sonra (Şekil 4.12) veri setinde bulunan bazı özelliklerin sınıflandırma performansına etkisi değerlendirilmiştir. Buna göre sonsuz değer içeren (infinity), boş değer içeren, tamamen negatif değer içeren ve değişmeyen özellikler veri setinden çıkarılmıştır. Çıkarılan alanlar Çizelge 4.8.'de gösterilmektedir.

Çizelge 4.8. CICDDDoS2019 veri setinden çıkarılan özellikler

Özellik	***Açıklaması***
Flow ID	Akışı tekil olarak tanımlayan ID
Source IP	Akışın kaynak IP adresi
Destination IP	Akışın hedef IP adresi
Timestamp	Akışın oluştuğu zaman damgası (milisaniye cinsinden)
SimillarHTTP	Ağ trafiğindeki HTTP akışlarının benzerliği
Bwd PSH Flags	Geri yöndeki akıştaki PSH bayraklarının sayısı
Fwd URG Flags	İleri yöndeki akıştaki URG bayraklarının sayısı
Bwd URG Flags	Geri yöndeki akıştaki URG bayraklarının sayısı
FIN Flag Count	Tüm akışlardaki FIN bayraklarının sayısı
PSH Flag Count	Tüm akışlardaki PSH bayraklarının sayısı
ECE Flag Count	Tüm akışlardaki ECE bayraklarının sayısı
Fwd Avg Bytes/Bulk	İleri yöndeki akıştaki bayt/saniye hızının ortalama değeri

Fwd Avg Packets/Bulk	İleri yönde iletilen her paketin ortalama bayt sayısı
Fwd Avg Bulk Rate	İleri yönde iletilen bloke edilen paketlerin ortalama oranı
Bwd Avg Bytes/Bulk	Geri yönde iletilen her byte'ın ortalama paket sayısı
Bwd Avg Packets/Bulk	Geri yönde iletilen her paketin ortalama byte sayısı
Bwd Avg Bulk Rate	Geri yönde iletilen bloke edilen paketlerin ortalama oranı

Ayrıca sınıflandırma performansının artırılması için yüksek korelasyona sahip özellikler hesaplanmış ve veri setinden çıkarılmıştır. Index numarasına göre Şekil 4.13'te korelasyon ilişkisi, Çizelge 4.9'da özellikler listelenmektedir.



Şekil 4.13. Yüksek korelasyona sahip özellikler

Çizelge 4.9. Yüksek korelasyona sahip özellik isimleri

Yüksek Korelasyona Sahip Özellik İsimleri		
Total Length of Bwd Packets	Fwd Packets/s	Subflow Fwd Packets
Fwd Packet Length Mean	Min Packet Length	Subflow Fwd Bytes
Bwd Packet Length Std	Packet Length Mean	Subflow Bwd Packets
Fwd IAT Total	Packet Length Std	Subflow Bwd Bytes
Fwd IAT Mean	Packet Length Variance	act_data_pkt_fwd
Fwd IAT Std	RST Flag Count	min_seg_size_forward
Fwd IAT Max	Average Packet Size	Idle Mean
Fwd IAT Min	Avg Fwd Segment Size	Idle Max
Bwd IAT Total	Avg Bwd Segment Size	Idle Min
Bwd IAT Std	Fwd Header Length.1	

Veri setinde bulunan kategorik veri türüne sahip Protocol, Source Port ve Destination Port alanları "one hot encoding" uygulandıktan sonra, veri setinde bulunan özellikler MÖ ve DÖ modelleri ile eğitime hazır hale getirmek için "z-score normalization" uygulanmıştır. Bu şekilde hazır veri seti olan CICDDoS2019 veri seti hem çoklu sınıflandırma hem de ikili sınıflandırma için hazır hale gelmiştir. Ayrıca çoklu sınıflandırma için etiket değerleri Çizelge 4.10'da gösterilmektedir. İkili sınıflandırma için ise BENIGN ve Attack şeklinde etiketlenmiştir.

Çizelge 4.10. CICDDoS2019 veri seti etiket değerleri

Etiket Adı	***Değeri***
BENIGN	0
NetBIOS	1
LDAP	2
MSSQL	3
Portmap	4
Syn	5
UDP	6
UDPLag	7

4.10.2. KEY2023 veri seti ön işlem

SCADA sistemlerine Modbus/TCP protokolü üzerinden düzenlenen DDoS saldırı verileri ve normal ağ trafik verilerinden oluşan bir veri seti elde edilmiştir. Öncelikle toplanan veriler ayrı dosyalardan ".pcap" dosya formatından ".csv" dosya formatına dönüştürülüp daha sonra tek bir ".csv" dosyasında birleştirilmiştir. Veri setinde yapılan

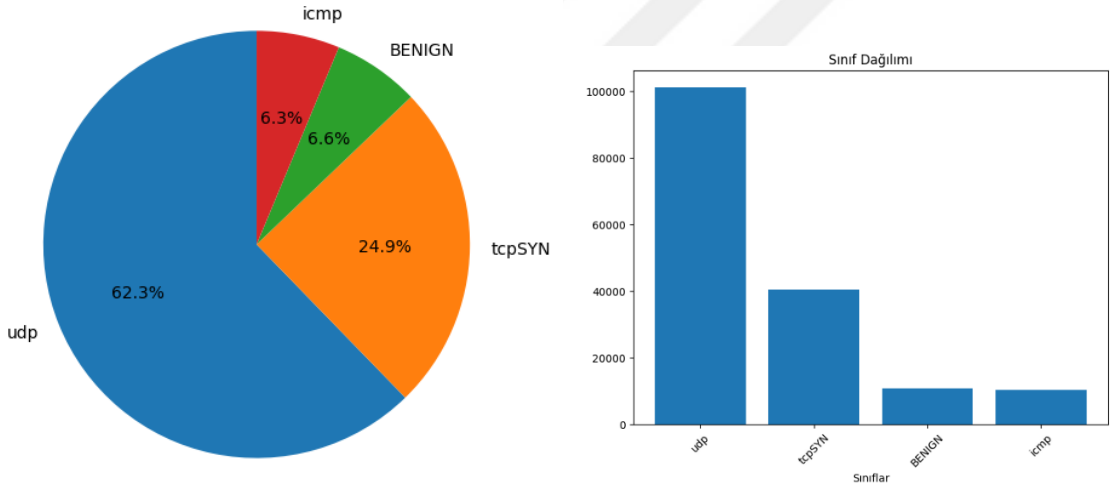
saldırı türlerine göre “Label” alanı saldırı türlerini ifade edecek şekilde sırasıyla Çizelge 4.11 ve 4.12’de gösterildiği gibi etiketlenerek veri sayıları kontrol edilmiştir.

Çizelge 4.11. KEY2023 veri setinde bulunan normal veri sayısı

Normal	***Veri Sayısı***
BENIGN	10668

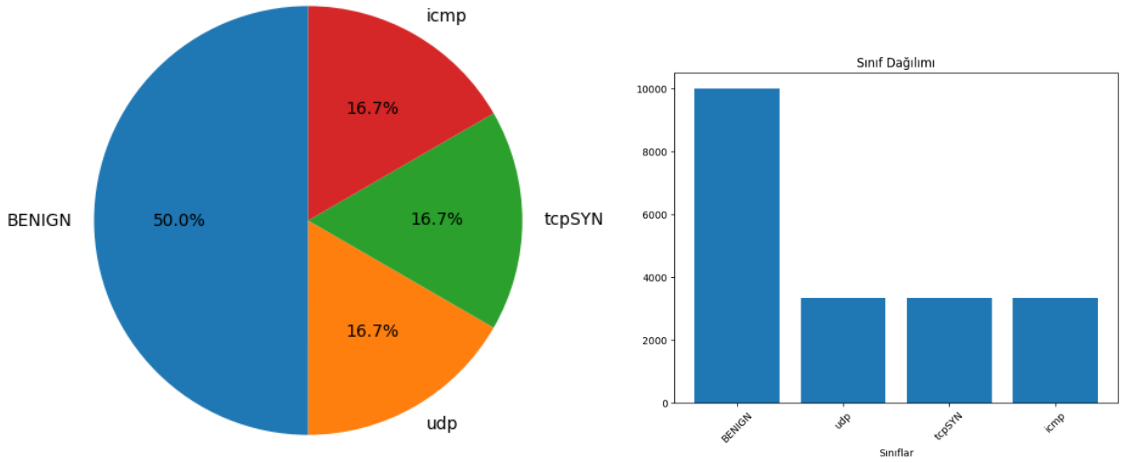
Çizelge 4.12. KEY2023 veri setinde bulunan saldırı çeşitlerine göre veri sayısı

Saldırı Türü	***Veri Sayısı***
TCP SYN Flood	40354
ICMP Flood	10228
UDP Flood	101103



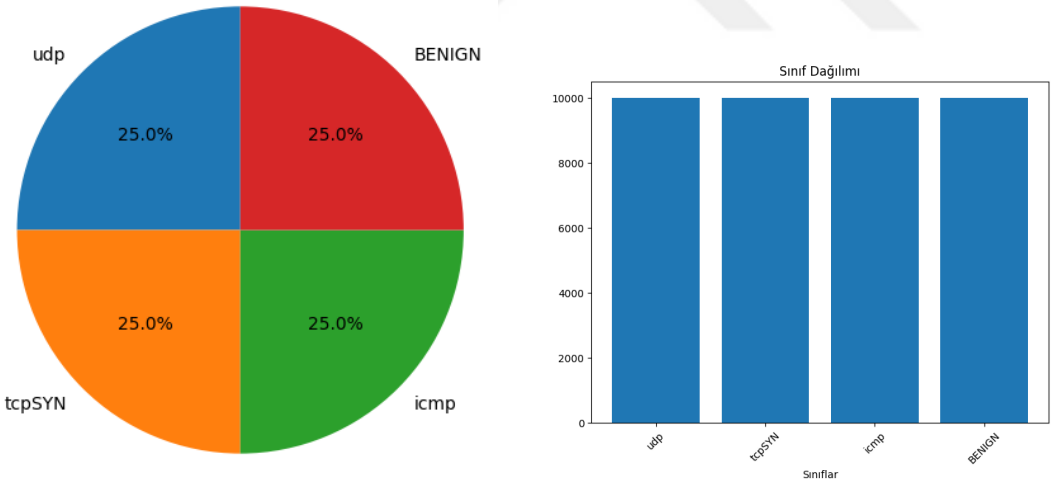
Şekil 4.14. KEY2023 veri seti etiket dağılımı grafikleri

Şekil 4.14’te görüldüğü gibi sınıf dağılımı dengesiz olarak veri setinde yer almaktadır. Bunun nedeni yapılan saldırılar sırasında toplanan paket sayısının saldırıya göre değişmesinden kaynaklanmaktadır. Bu durumu düzeltmek için hem çoklu sınıflandırma için az veri sayısına sınıf etiketi sayısı baz alınarak aşağı örnekleme yapılarak diğer sınıflar eşitlenmiştir. İkili sınıflandırma için veri setinde bulunan benign ve diğer sınıflar benign sınıfında bulunan veri sayısına göre her saldırı çeşidinden eşit sayıda veri alınarak eşitlenmiştir (Şekil 4.15). Burada amaç saldırı türünün tespiti değil, saldırı var mı yok mu bunu tespit edebilmektir. Bu yüzden iki sınıf benign ve attack olarak alınmıştır.



Şekil 4.15. KEY2023 ikili sınıflandırma eşitlenen verilerin grafikleri

Çoklu sınıflandırma için bütün veri etiket değerleri şekilde görüldüğü gibi eşitlenmiştir. Ayrıca veri setinin ikili sınıflandırmada da performansının değerlendirilip karşılaştırılabilmesi için "benign" sınıfının diğer sınıflar ile eşit olarak dağılımı da Şekil 4.16'da gösterildiği gibi eşitlenmiştir.



Şekil 4.16. KEY2023 veri seti çoklu sınıflandırma için eşitlenen alanlar

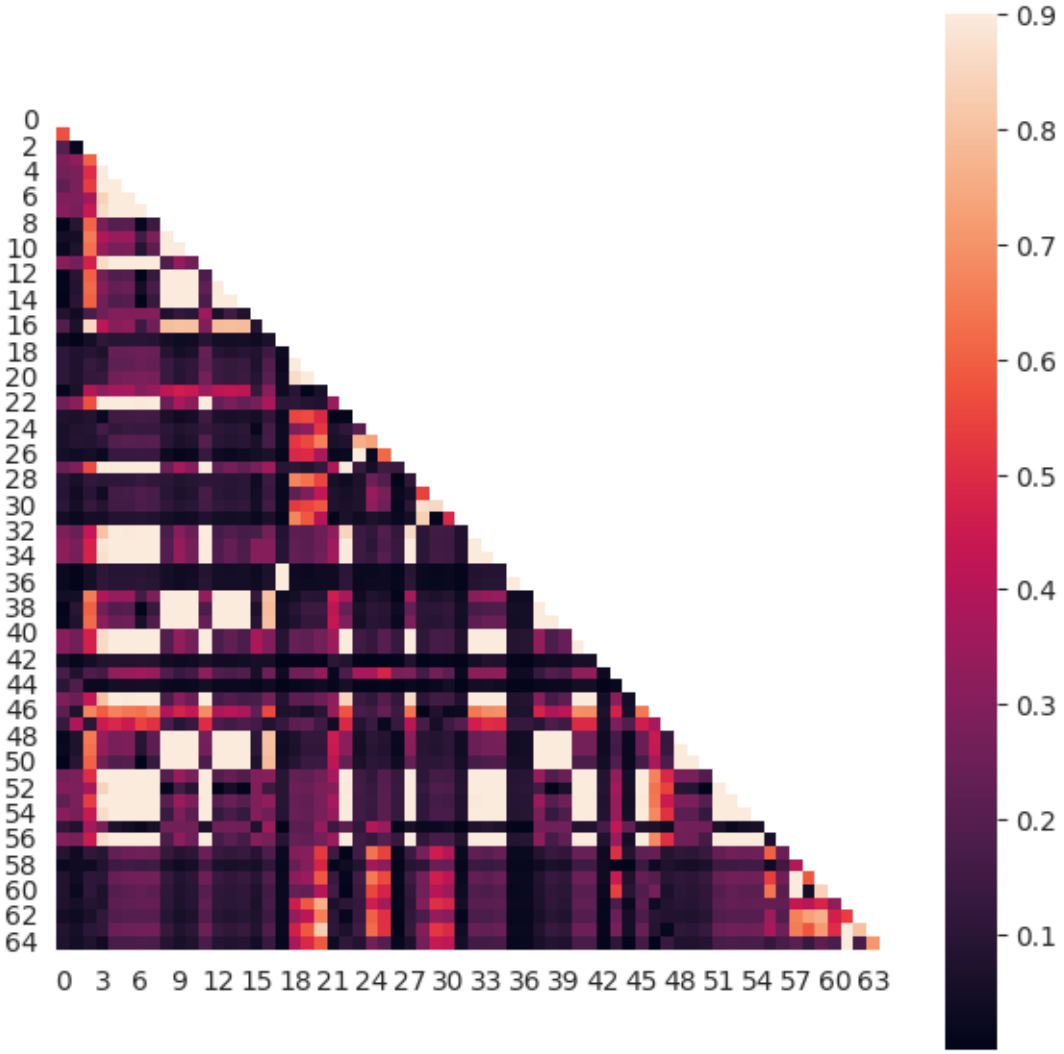
Çalışmada kullanılan KEY2023 veri setinde ham hali ile 83 özellik ve 1 etiket alanı bulunmaktadır. Bu 83 özellik içerisinde, Flow ID alanı incelenerek tekrar eden ve anlamsız olan veriler bu alana göre çıkarılmıştır. Veri setinde bulunan Flow ID, Src IP ve Dst IP özellikleri modellerin tahmin performansını arttırmak için çıkarılmıştır. Bunun sebebi aynı değerlere sahip olmalarından dolayı aşırı ezberleme gerçekleşmesini

önlemektir. Ayrıca zaman değerinin bir önem arz etmemesinden dolayı Timestamp özelliği de çıkarılmıştır. KEY2023 veri setinde içerisinde "NaN" bulunan veriler 0 ile doldurulmuş, tamamen -1 değerleri ve infinity(sonsuz) değer içeren özellikler ve değişmeyen özellikler veri setinden çıkarılarak veri seti modellerin uygulanabilir olması için hazır hale getirilmiştir (Çizelge 4.13). Bunun sebebi içerisindeki verilerin değişmemesinden dolayı sonuca herhangi bir etki sağlayamayacaklarındandır.

Çizelge 4.13. KEY2023 veri setinden çıkarılan değişmeyen özellikler

Özellik	***Açıklaması***
Flow ID	Akışı tekil olarak tanımlayan ID
Src IP	Akışın kaynak IP adresi
Dst IP	Akışın hedef IP adresi
Timestamp	Akışın oluştuğu zaman damgası (milisaniye cinsinden).
Fwd PSH Flags	İleri yöndeki akıştaki PSH bayraklarının sayısı
Fwd URG Flags	İleri yöndeki akıştaki URG bayraklarının sayısı
Bwd URG Flags	Geri yöndeki akıştaki URG bayraklarının sayısı
URG Flag Cnt	Tüm akışlardaki URG bayraklarının sayısı
CWE Flag Count	Tüm akışlardaki CWE bayraklarının sayısı
ECE Flag Cnt	Tüm akışlardaki ECE bayraklarının sayısı
Fwd Byts/b Avg	İleri yöndeki akıştaki bayt/saniye hızının ortalama değeri
Fwd Pkts/b Avg	İleri yönde iletilen her paketin ortalama bayt sayısı
Fwd Blk Rate Avg	İleri yönde iletilen bloke edilen paketlerin ortalama oranı
Bwd Byts/b Avg	Geri yönde iletilen her byte'ın ortalama paket sayısı
Bwd Pkts/b Avg	Geri yönde iletilen her paketin ortalama byte sayısı
Bwd Blk Rate Avg	Geri yönde iletilen bloke edilen paketlerin ortalama oranı
Init Fwd Win Byts	İleri yönde başlatılan pencere boyutu (byte)
Fwd Seg Size Min	İleri yönde en küçük TCP segment boyutu

Uygulanacak modellerin performansını arttırmak için veri setlerinde bulunan özelliklerin korelasyonları incelenmiş ve yüksek korelasyona sahip veriler de veri setinden çıkarılmıştır. Yüksek korelasyona sahip özellikler Şekil 4.17'de gösterilmiştir ve çıkarılan özellikler Çizelge 4.14'te yer almaktadır.



Şekil 4.17. KEY2023 veri seti yüksek korelasyona sahip özellikler grafiği

Çizelge 4.14. KEY2023 veri seti yüksek korelasyona sahip özellikler

Yüksek Korelasyona Sahip Özellik İsimleri			
Tot Fwd Pkts	Flow IAT Std	Pkt Len Min	Subflow Fwd Byts
Tot Bwd Pkts	Flow IAT Max	Pkt Len Max	Subflow Bwd Pkts
TotLen Fwd Pkts	Fwd IAT Tot	Pkt Len Mean	Subflow Bwd Byts
TotLen Bwd Pkts	Fwd IAT Min	Pkt Len Std	Fwd Act Data Pkts
Fwd Pkt Len Min	Bwd IAT Tot	Pkt Len Var	Active Max
Fwd Pkt Len Mean	Bwd PSH Flags	PSH Flag Cnt	Active Min
Fwd Pkt Len Std	Fwd Header Len	Pkt Size Avg	Idle Max
Bwd Pkt Len Max	Bwd Header Len	Fwd Seg Size Avg	Idle Min
Bwd Pkt Len Min	Fwd Pkts/s	Bwd Seg Size Avg	
Bwd Pkt Len Mean	Bwd Pkts/s	Subflow Fwd Pkts	

Ayrıca KEY2023 veri setinde etiket değerleri Çizelge 4.15'te olduğu gibi yeniden adlandırılmıştır.

Çizelge 4.15. KEY2023 etiket değerleri

Etiket Adı	***Değeri***
BENIGN	0
tcpSYN	1
İcmp	3
udp	4

Veri ön işlem adımlarını sıra ile özetlenirse;

- Sınıf dağılımları incelenerek çalışma türüne göre veri dağılımı yapılmıştır.
- Veri setlerindeki verilere göre aşağı örnekleme yapılmıştır.
- Sonsuz ve boş değerler veri setlerinden çıkarılmıştır.
- Veri setlerinde bulunan değişmeyen özellikler çıkarılmıştır.
- Veri setlerinde bulunan önem arz etmeyen veriler çıkarılmıştır.
- Yüksek korelasyona sahip özellikler çıkarılmıştır.
- Veri setlerinde içerisinde çok fazla negatif olan değerler değiştirilmiştir.
- Kategorik veri tipine sahip özelliklere encoding işlemi uygulanmıştır.
- Veri setlerine eğitimden önce z-score normalizasyon yapılmıştır.
- Veri setleri modellerin tahmin performansını ölçmek için hazır hale gelmiştir.

5. ARAŞTIRMA SONUÇLARI VE TARTIŞMA

Çalışmada MÖ ve DÖ modelleri ile SCADA sistemlerde DDoS saldırı tespiti sınıflandırılması hedeflenmiştir. DÖ yönteminin başarısını değerlendirmek için MÖ algoritmalarının da DDoS saldırılarını sınıflandırmasının da incelemesi yapılmıştır. Bu bölümde hem MÖ algoritmaları ile elde edilen sonuçlar hem de önerilen DÖ modeli ile elde edilen sonuçlara karşılaştırmalı olarak yer verilmiştir. Bu çalışmalar her iki veri seti için ayrı ayrı elde edilmiştir. Uygulanan adımlar Şekil 5.1'de gösterildiği gibidir. Veri ön işleme adımlarında veri seti temizlenerek modellerin eğitimi için hazır hale getirilmiştir. DÖ modelleri için çoklu sınıflandırmada eğitim kısmında en uygun fonksiyonu oluşturmak için, Adam optimizasyonu ve sparse categorical crossentropy kayıp fonksiyonu, sınıflandırma için softmax fonksiyonu kullanılmıştır. İkili sınıflandırma için ise Adam optimizasyonu, binary crossentropy kayıp fonksiyonu ve sınıflandırma için sigmoid fonksiyonu kullanılmıştır. Her iki sınıflandırma çalışması için 100 adım sayısı(epoch) ve bach size (adım sayısı) 64 olarak seçilmiştir. Ayrıca, modelin doğruluğu arttıkça eğitimi durdurmak için erken çağırma fonksiyonu (early callback) kullanılmıştır. Veri setleri %70 eğitim, %30 test verisi olarak ayrılmıştır. Bu çalışmalar CICDDoS2019 veri seti için ikili sınıflandırma ve çoklu sınıflandırma, KEY2023 veri seti için ikili sınıflandırma ve çoklu sınıflandırma şeklinde gerçekleştirilmiştir. YSA modeli, 11 katmandan oluşmaktadır. Bu katmanlar; bir giriş katmanı, altı tam bağlantılı gizli katman, üç Dropout katmanı, bir BatchNormalization katmanı ve bir çıkış katmanıdır. Aktivasyon fonksiyonu olarak ara katmanlarda ReLU kullanılmıştır. UKSB modelinde ise beş katman bulunmaktadır: 1. Bidirectional UKSB katmanı, 2-4 arası UKSB katmanları ve bir tam bağlantılı (Dense) katman. Dördüncü UKSB katmanının ardından bir Dropout katmanı eklenmiştir. TSA modeli, 4 SimpleRNN katmanı ve 1 tam bağlantılı (Dense) katmandan oluşmaktadır. ESA modeli ise tek bir giriş katmanına ve üç tam bağlantılı katmana sahiptir. Aktivasyon fonksiyonu olarak ara katmanlarda ReLU kullanılmıştır.

5.1. Çalışma Ortamı

Deneysel sonuçlar Python programlama dili kullanılarak Keras / Tensorflow'da uygulanmıştır. Performansı ölçmek için uygulamalar, Google Colab'da test edilmiştir. SCADA sisteminin bulunduğu bilgisayar özellikleri Çizelge 5.1'de gösterilmiştir.

Çizelge 5.1. SCADA sistemi bulunan donanım özellikleri

Donanım	***Özellikler***
CPU	İntel Xeon CPU E3-1245 3.50GHz (8 CPUs)
İşletim Sistemi	Windows 10 Pro 64-bit
Grafik Kartı	AMD Radeon HD7400 6GB
Ram	16 GB

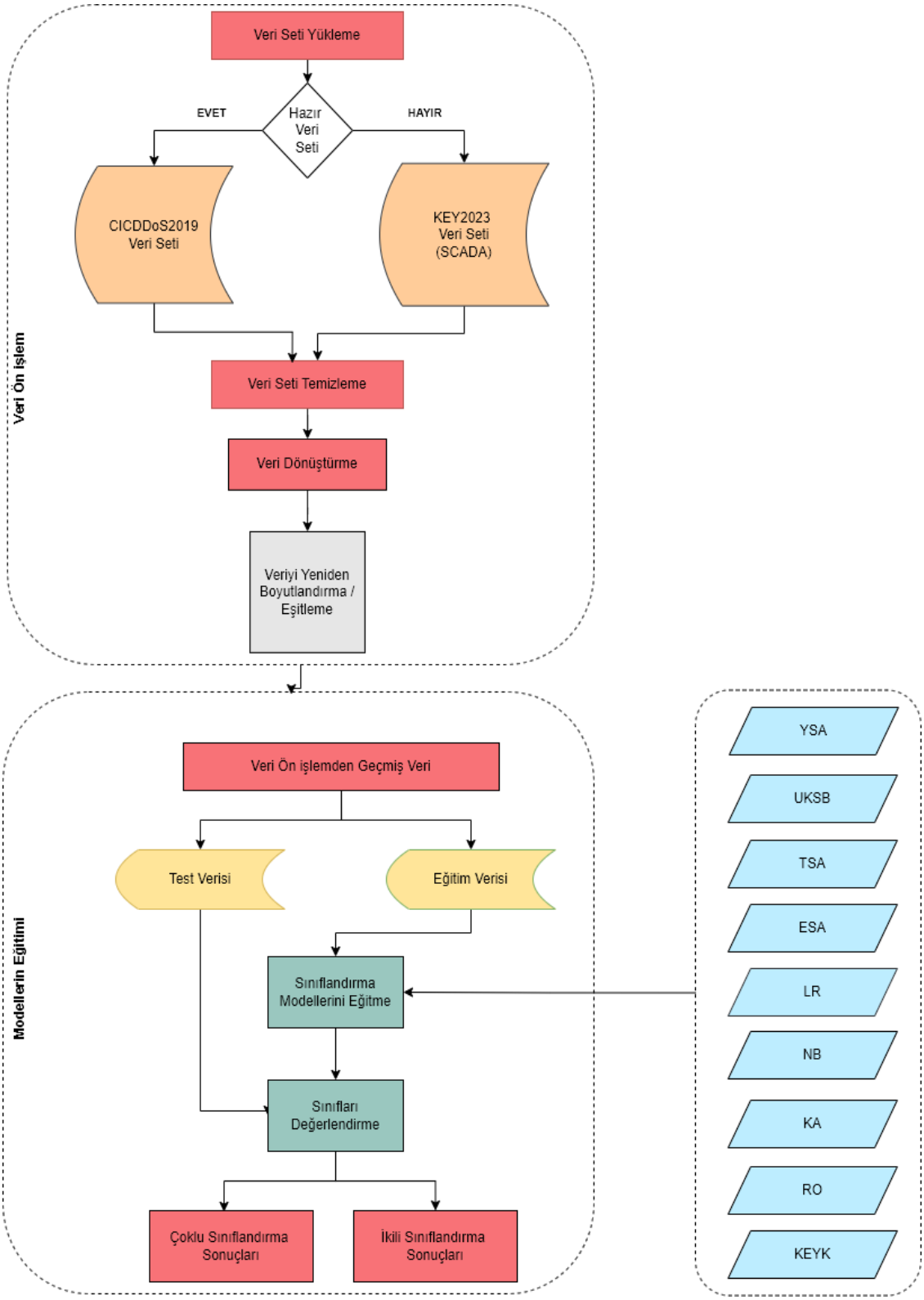
Çalışmalar Çizelge 5.2'de gösterilen bilgisayarda gerçekleştirilmiştir.

Çizelge 5.2. Çalışma alanı

Donanım	***Özellikler***
CPU	i7-11370H 3.30GHz (8 CPUs)
İşletim Sistemi	Windows 10 Education 64-bit
Grafik Kartı	NVIDIA GeForce RTX 3050Ti 6GB
Ram	16 GB

DÖ modelinin test aşamasında daha güçlü GPU gereksiniminden dolayı çalışmalar Google Colab ortamında gerçekleştirilmiştir.

Bu tez çalışmasında DÖ modellerinden YSA, UKSB, TSA ve ESA, MÖ modellerinden LR, RO, KA, NB ve KEYK modelleri ile test gerçekleştirilmiştir. DÖ modellerinde performansı artırmak için farklı özellikler, adım sayısı ve katman derinliği gibi farklı çalışmalar yapılmıştır. DÖ ile yapılan çalışma 100 epoch'da gerçekleştirilmiştir.



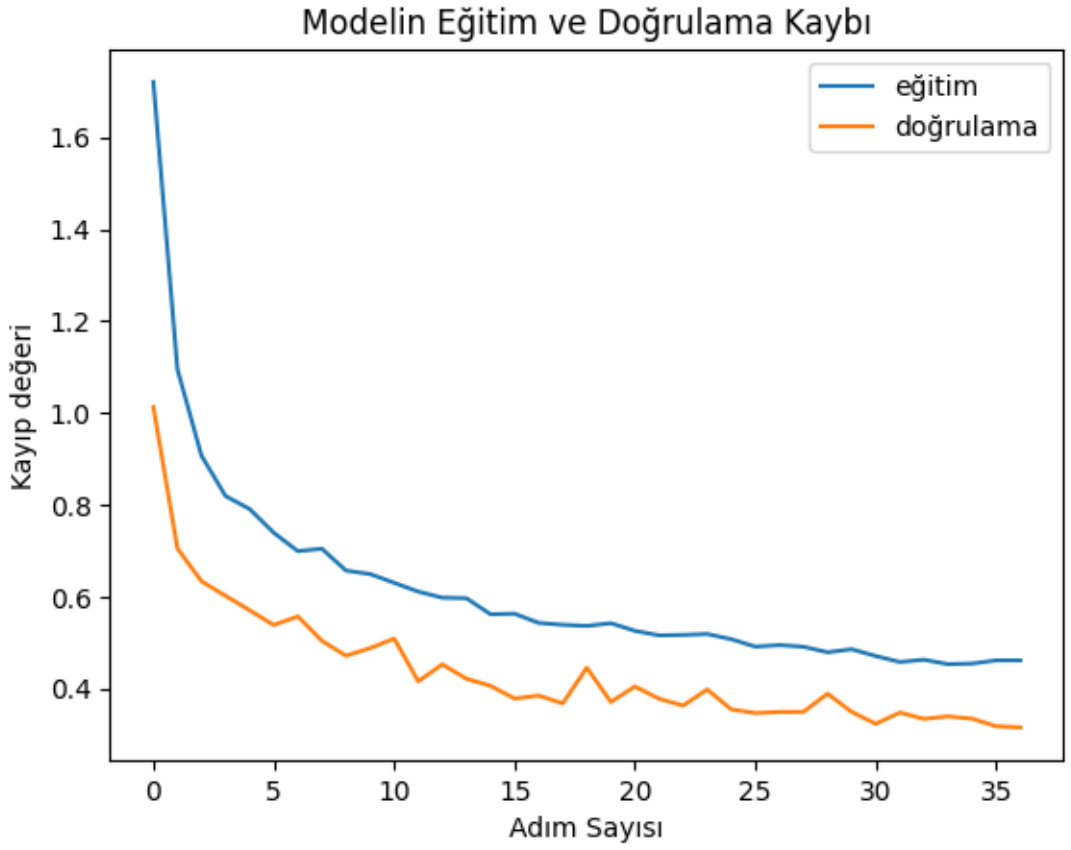
Şekil 5.1. Çalışma adımları

5.2. CICDDoS2019 Veri Seti Sonuçları

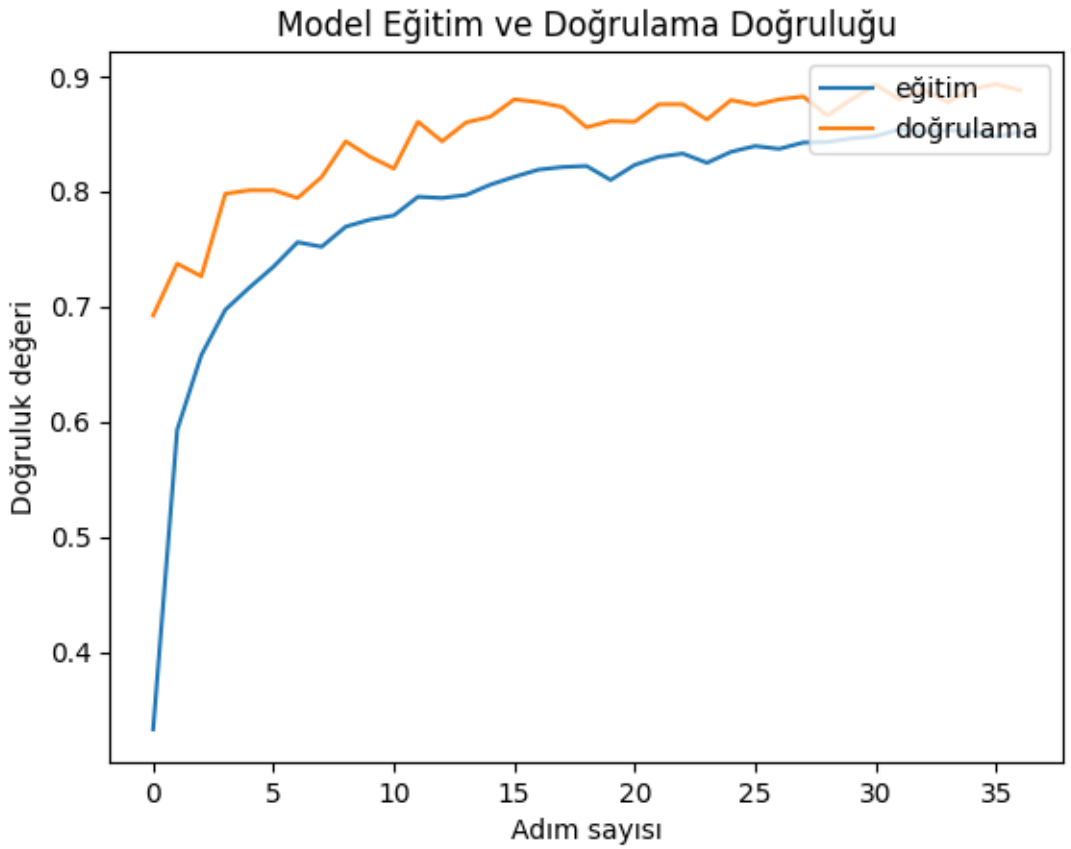
Hazır veri seti ile yapılan çalışmada modellerin ikili sınıflandırma ve çoklu sınıflandırma performansları değerlendirilmiştir. Buna göre veri ön işlemden geçen veri seti ile elde edilen sonuçlar iki başlık halinde incelenmiştir.

5.2.1. Çoklu sınıflandırma sonuçları

Uygulanan YSA modelinin eğitim ve doğrulama kaybı grafiğinde (Şekil 5.2) eğitim kaybı, modelin eğitim verilerine ne kadar iyi uyduğunu ölçerken, doğrulama kaybı, modelin test verilerinde ne kadar iyi performans gösterdiğini ölçmektedir. Grafikteki eğrilerin adım sayısı arttıkça düştüğünü görülmektedir, bu da modelin eğitim verilerine ve test verilerine uygun şekilde uyum sağladığını göstermektedir.



Şekil 5.2. YSA modelinin eğitim ve doğrulama grafiği



Şekil 5.3. YSA modelinin eğitim ve doğrulama doğruluğu grafiği

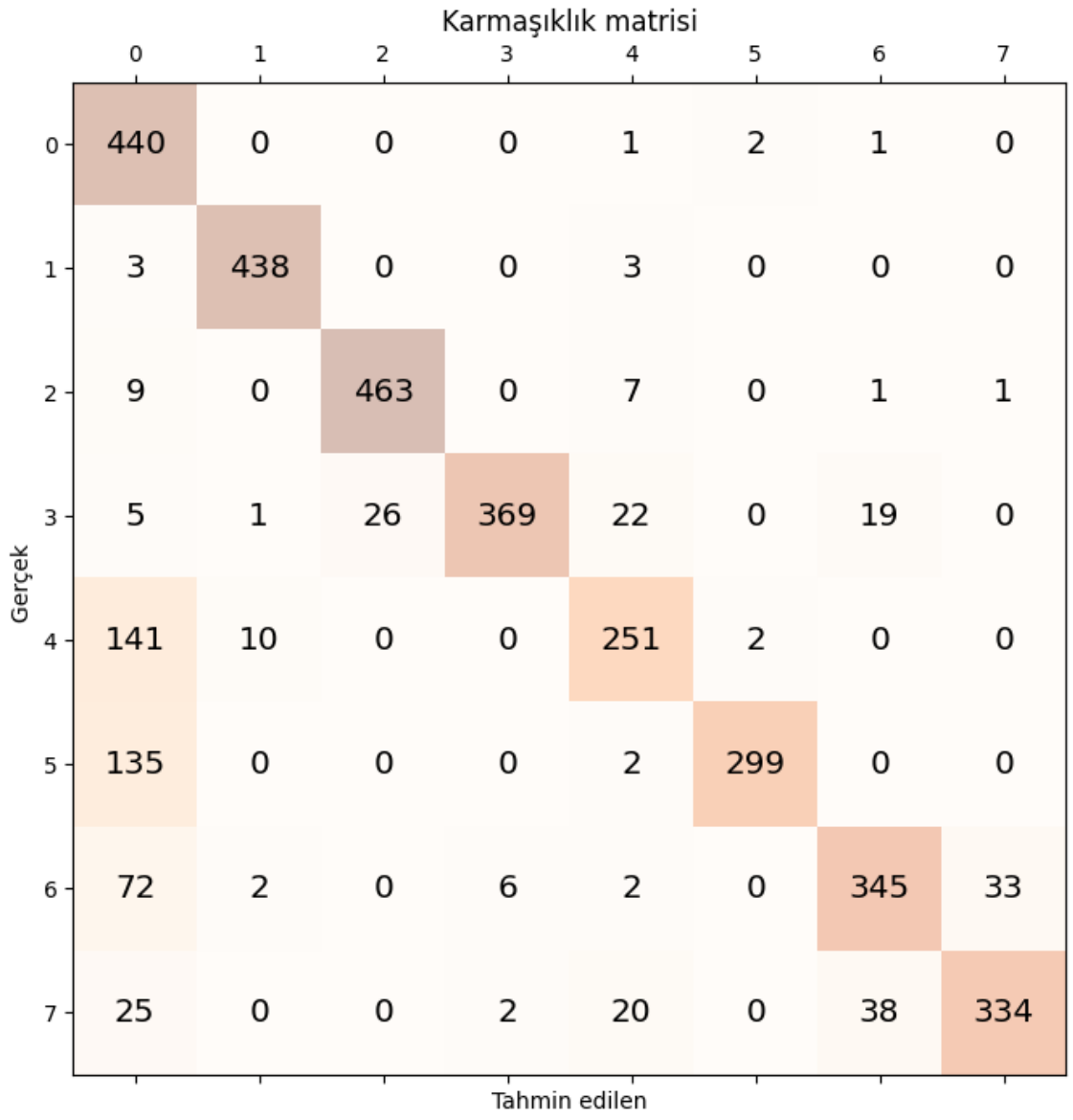
YSA modelinin eğitim ve doğrulama doğruluğu grafiği (Şekil 5.3), modelin eğitim verilerindeki doğruluğu her adım sayısında artarken, doğrulama verilerindeki doğruluğun da arttığı göstermektedir.

Modelin karmaşıklık matrisinde (Şekil 5.4), 8 sınıfın karşılaştırmaları gösterilmektedir. Şekil 5.4'te gösterilen sınıfların çoğunun doğru sınıflandırıldığı görülmektedir. Ancak, Portmap sınıfı örnekleri tahmin edilirken daha fazla yanlış sınıflandırılmıştır. Ayrıca, Syn sınıfı için de diğer sınıflara göre fazla oranda yanlış sınıflandırma vardır. Modelin bu sınıfları öğrenmedeki performansının düşük olduğu görülmektedir.

YSA modelinin diğer performans metrikleri incelendiğinde modelin doğruluğu %83.25'tir. Sınıfların kesinlik, duyarlılık ve f1-Skor değerleri sınıfların doğru bir şekilde tahmin edilip edilmediğini ve bu sınıfların hassasiyetlerini ölçmek için kullanılır.

Çizelge 5.3'teki sonuçlara göre, NetBIOS sınıfı için en yüksek kesinlik %97, duyarlılık %99 ve f1-Skor %98 değerleri elde edilmiştir. MSSQL sınıfı için de yüksek kesinlik %98 değeri elde edilmiştir ancak recall değeri daha düşük %83 olduğundan f1-

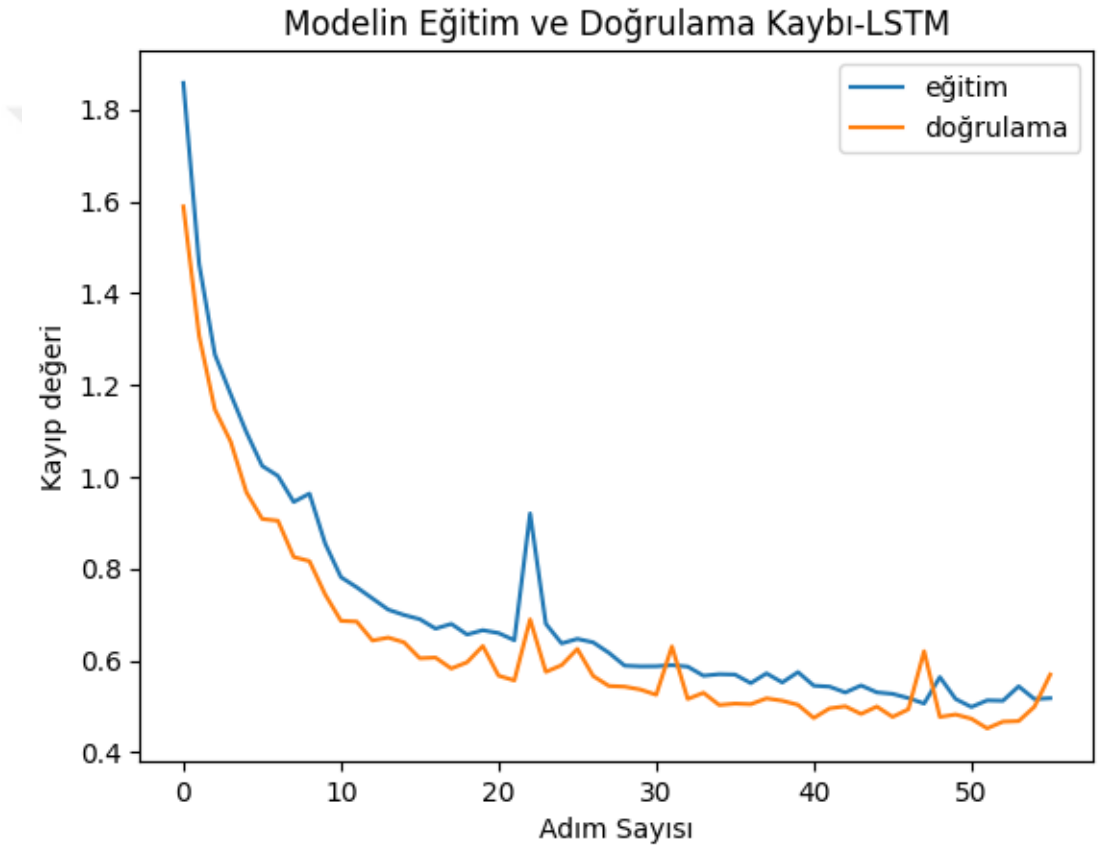
Skor değeri %90 civarındadır. Syn sınıfı için kesinlik %99 değeri oldukça yüksekken recall %69 daha düşüktür, bu nedenle f1-Skor değeri %81 diğer sınıflara göre daha düşüktür. Portmap sınıfı için duyarlılık değeri diğer sınıflara göre daha düşük %62 olduğundan, f1-Skor değeri de diğer sınıflara göre daha düşüktür %71. UDP ve UDPLag sınıflarının kesinlik, duyarlılık ve f1-Skor değerleri sırasıyla %85, %75, %80 ve %91, %80, %85'tir. Bu değerler, modelin bu sınıfları diğer sınıflara göre daha az başarıyla sınıflandırdığını göstermektedir. Portmap sınıfı için, recall değeri düşük olduğundan, modelin bu sınıfı doğru bir şekilde sınıflandırmakta zorlandığı görülmektedir.



Şekil 5.4. YSA modeli karmaşıklık matrisi

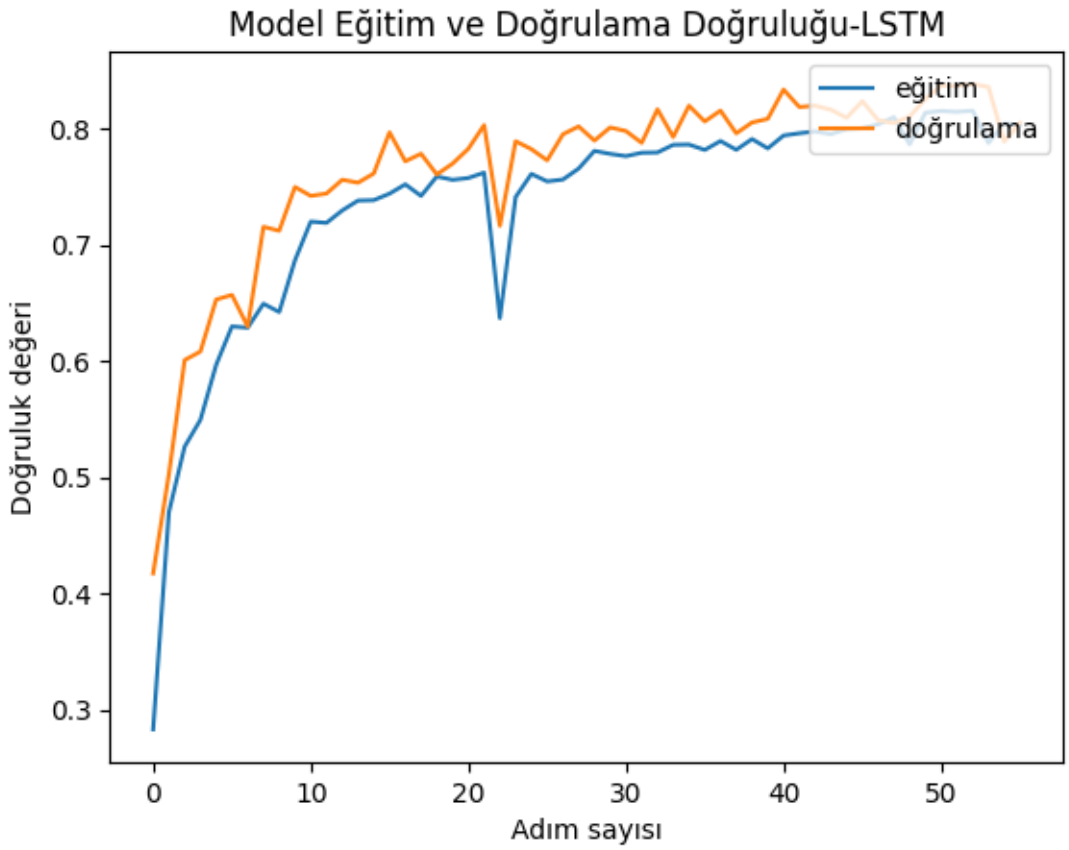
Çizelge 5.3. YSA için performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 53	% 99	% 69
1	**NetBIOS**	% 97	% 99	% 98
2	**LDAP**	% 95	% 96	% 95
3	**MSSQL**	% 98	% 83	% 90
4	**Portmap**	% 81	% 62	% 71
5	**Syn**	% 99	% 69	% 81
6	**UDP**	% 85	% 75	% 80
7	**UDPLag**	% 91	% 80	% 85
Modelin Accuracy (Doğruluğu) %		% 83,25		



Şekil 5.5. UKSB modelinin eğitim ve doğrulama kaybı grafiği

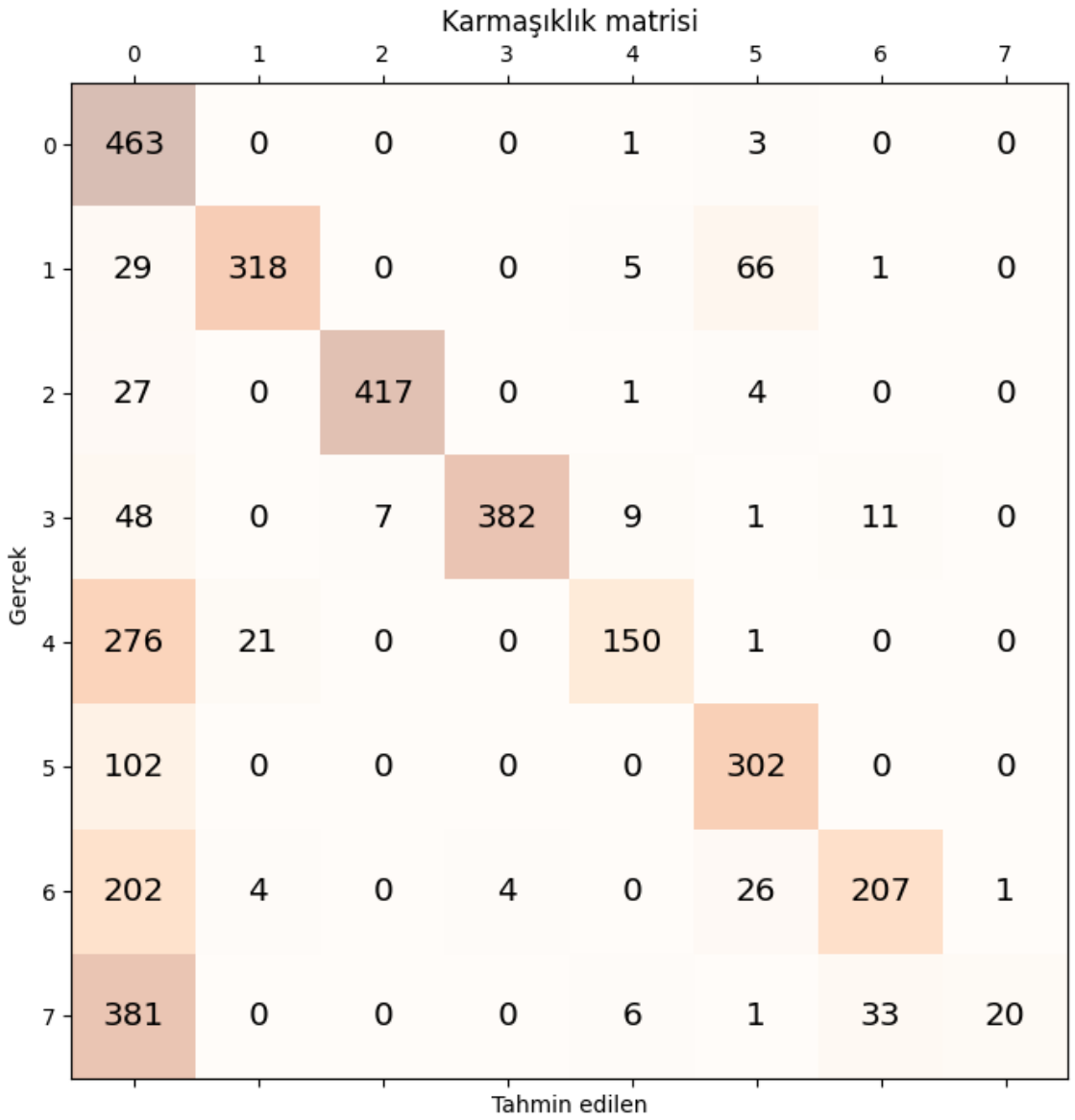
Veri setine uygulanan UKSB modelinin eğitim ve doğrulama kaybı grafiği Şekil 5.5'te verilmiştir. Grafikteki eğrilerin adım sayısı arttıkça düştüğünü görülmektedir, fakat bu düşüşte bazı adımlarda dalgalanmalar meydana gelmiştir. Bu da modelin eğitim verilerine ve test verilerine uyum sağlamaya çalıştığını göstermektedir.



Şekil 5.6. UKSB modelinin eğitim ve doğrulama doğruluğu grafiği

UKSB modelinin doğrulama doğruluğu grafiği de Şekil 5.6'da verilmiştir. UKSB modelinin eğitim ve doğrulama doğruluğu grafiğinde modelin eğitim verilerindeki doğruluğu her adım sayısında artarken, doğrulama verilerindeki doğruluğun da arttığı göstermektedir. Yaklaşık 24. Adımda grafikte bir düşüş gözlenmiştir fakat daha sonra tekrar yükselmiştir.

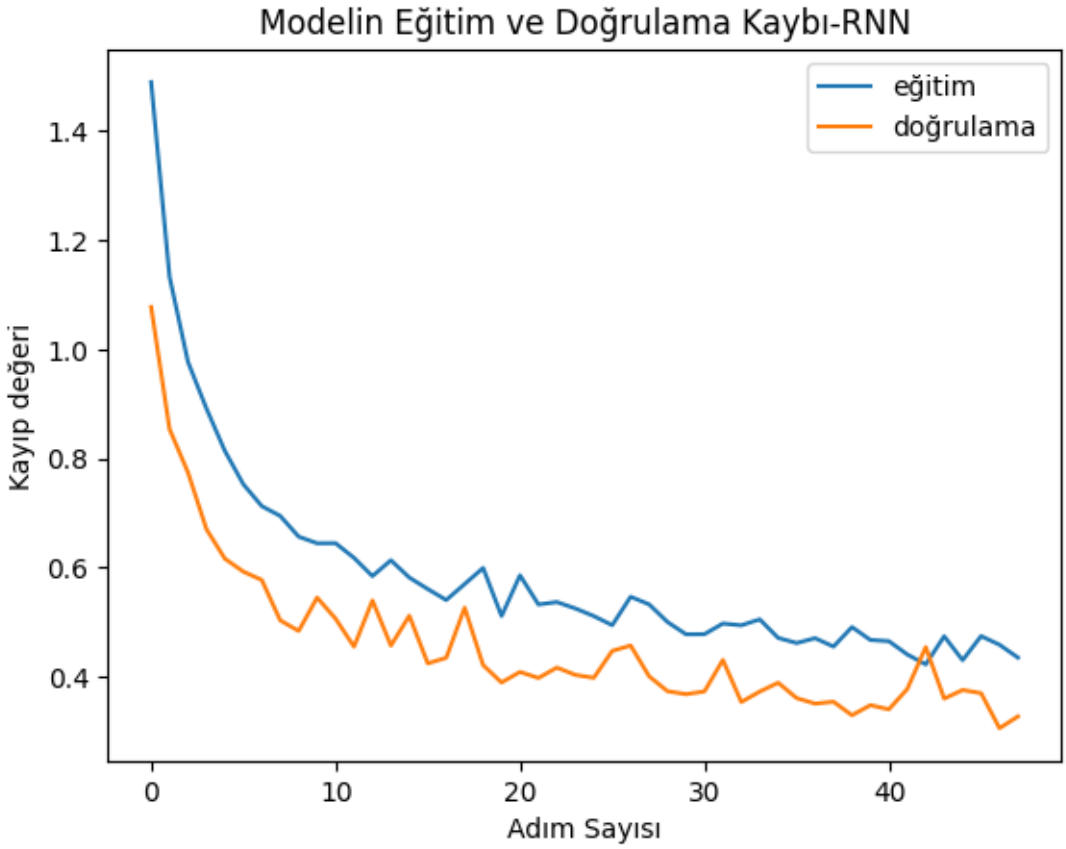
UKSB modelinin performans metrikleri Çizelge 5.4'te verilmiştir. Buna göre, modelin başarısının %63,99 olduğu görülmektedir. Diğer sınıflar incelendiğinde LDAP sınıfı için duyarlılık %93 olarak belirtilmiş, bu da LDAP sınıfına ait doğru tahmin edilenlerin %93'ünün doğru şekilde tahmin edildiğini göstermektedir. UKSB modelin BENIGN, Portmap, Syn ve UDP sınıflarını düşük bir kesinlik ve duyarlılıkla tahmin ettiği görülmektedir. Ayrıca UDPLag sınıfı için de düşük bir duyarlılık ve f1-skor değeri gözlemlenmiştir. Diğer sınıflar için ise kesinlik, duyarlılık ve f1-skor değerleri yüksek seviyelerdedir. Genel olarak, modelin performansı iyi değil, ancak bazı sınıflarda başarılı olduğu görülmektedir. Şekil 5.7'de verilen modelin karmaşıklık matrisinde modelin sınıflandırmada sınıfları yanlış tahmin ettiği görülmektedir.



Şekil 5.7. UKSB modeli karmaşıklık matrisi

Çizelge 5.4. UKSB için performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 30	% 99	% 46
1	**NetBIOS**	% 93	% 76	% 83
2	**LDAP**	% 98	% 93	% 96
3	**MSSQL**	% 99	% 83	% 91
4	**Portmap**	% 87	% 33	% 48
5	**Syn**	% 75	% 75	% 75
6	**UDP**	% 82	% 47	% 59
7	**UDPLag**	% 95	% 5	% 9
Modelin Accuracy (Doğruluğu) %		% 63,99		

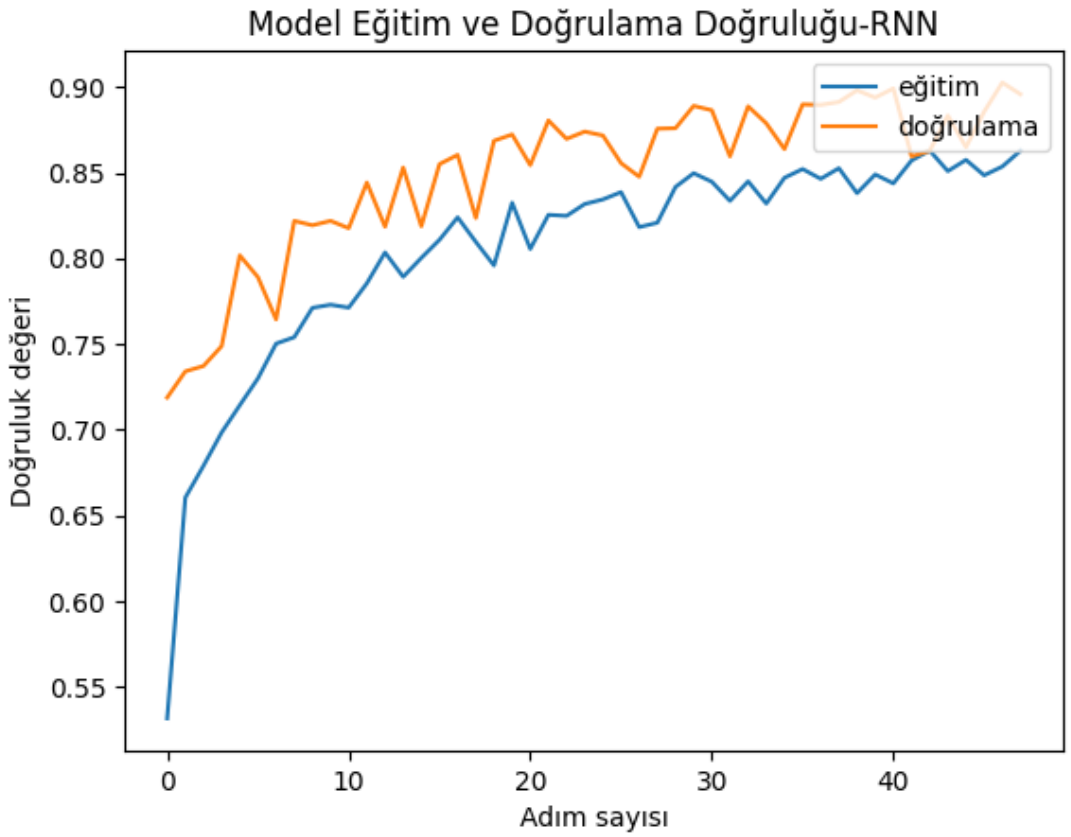


Şekil 5.8. TSA modelinin eğitim ve doğrulama kaybı grafiği

TSA modelinin eğitim ve doğrulama kaybı grafiği Şekil 5.8'de verilmiştir. Bu grafiğe göre adım sayısı arttıkça modelin eğitim ve doğrulama kayıplarının her ikisi de eğitim süreci boyunca düzenli bir şekilde azaldığı görülmektedir.

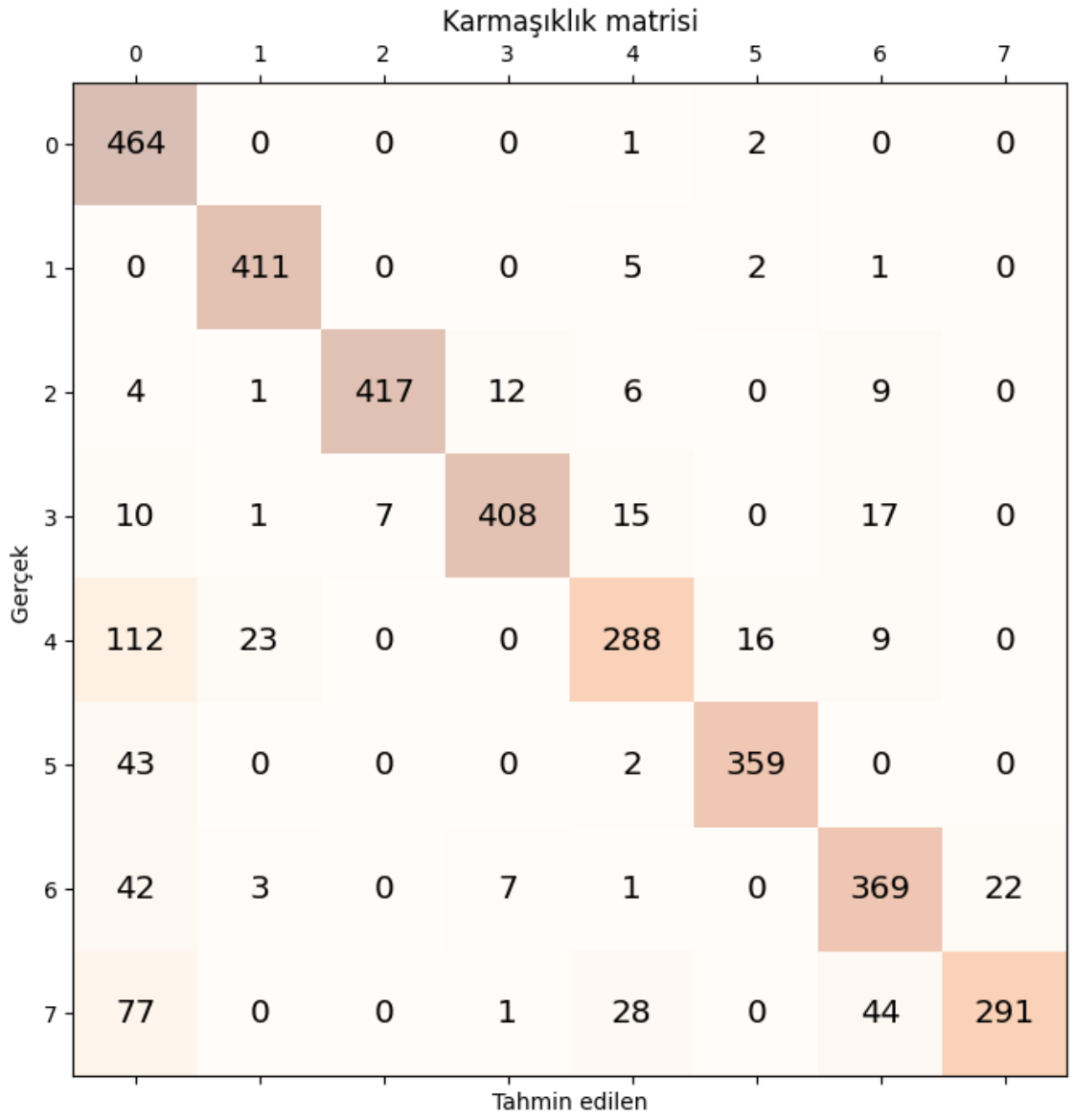
TSA modelinin Şekil 5.9'da verilen doğrulama doğruluğu grafiğinde, eğitim süreci boyunca, eğitim doğruluğu artarken, doğrulama doğruluğu da artmıştır ancak belirli bir noktadan sonra artış yavaşlamıştır hatta doğrulama doğruluğunda hafif bir düşüş gözlemlenmiştir.

Modelin karmaşıklık matrisi Şekil 5.10'da verilmiştir. Karmaşıklık matrisi incelendiğinde, Portmap ve UDPLag sınıflarının sınıflandırma performansının diğer sınıflara göre düşük olduğu gözlemlenmektedir.



Şekil 5.9. TSA modelinin eğitim ve doğrulama doğruluğu grafiği

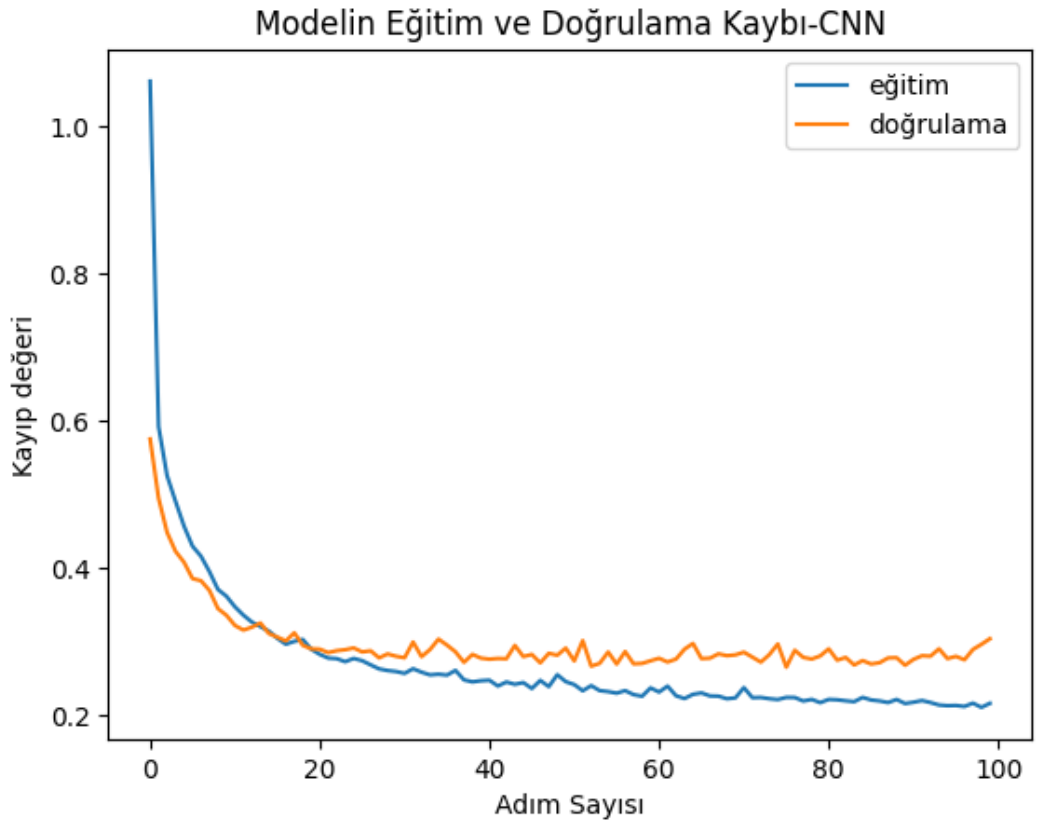
TSA modelinin diğer performans metrikleri Çizelge 5.5'te verilmiştir. Bu metriklerin sonuçlara göre, NetBIOS, LDAP ve Syn sınıfları için yüksek bir kesinlik ve duyarlılık elde edilmiştir. Diğer sınıflar için de genel olarak iyi sonuçlar elde edilmiştir, ancak Portmap sınıfı için duyarlılık %64, UDPLag sınıfı için ise %66 olarak hesaplanmıştır, bu da bu sınıfların belirlenmesinde modelin düşük performans gösterdiğini gösterir. Modelin doğruluğu %85,18'dir, yani model, tüm sınıfların doğru bir şekilde sınıflandırılması için kullanıldığında %85,18 başarı oranına sahiptir. Genel olarak sınıflandırma başarısı iyi bir modeldir.



Şekil 5.10. TSA modeli karmaşıklık matrisi

Çizelge 5.5. TSA için performans metrikleri

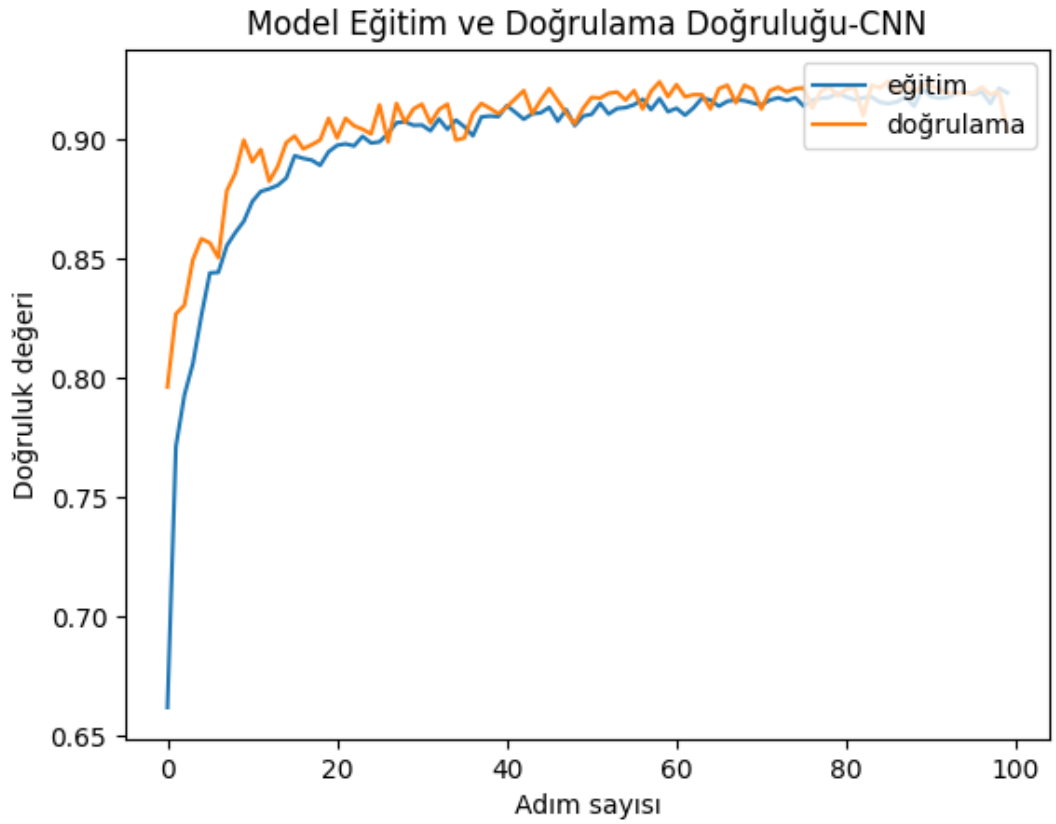
Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 62	% 99	% 76
1	**NetBIOS**	% 94	% 98	% 96
2	**LDAP**	% 98	% 93	% 96
3	**MSSQL**	% 95	% 89	% 92
4	**Portmap**	% 83	% 64	% 73
5	**Syn**	% 95	% 89	% 92
6	**UDP**	% 82	% 83	% 83
7	**UDPLag**	% 93	% 66	% 77
Modelin Accuracy (Doğruluğu) %		% 85,18		



Şekil 5.11. ESA modelinin eğitim ve doğrulama kaybı grafiği

Veri setine uygulanan ESA modelinin eğitim ve doğrulama kaybı grafiği Şekil 5.11'de verilmiştir. Bu grafiğe göre, eğitim kaybı ve doğrulama kaybı arasındaki fark eğitim süresince düzenli şekilde azalmaktadır. Ancak doğrulama kaybı, eğitim kaybından daha yüksek kalmaktadır. Sonuç olarak, bu grafik, iyi bir eğitim sonucu elde edildiğini ve modelin iyi performans göstermesi beklenilebileceğini göstermektedir.

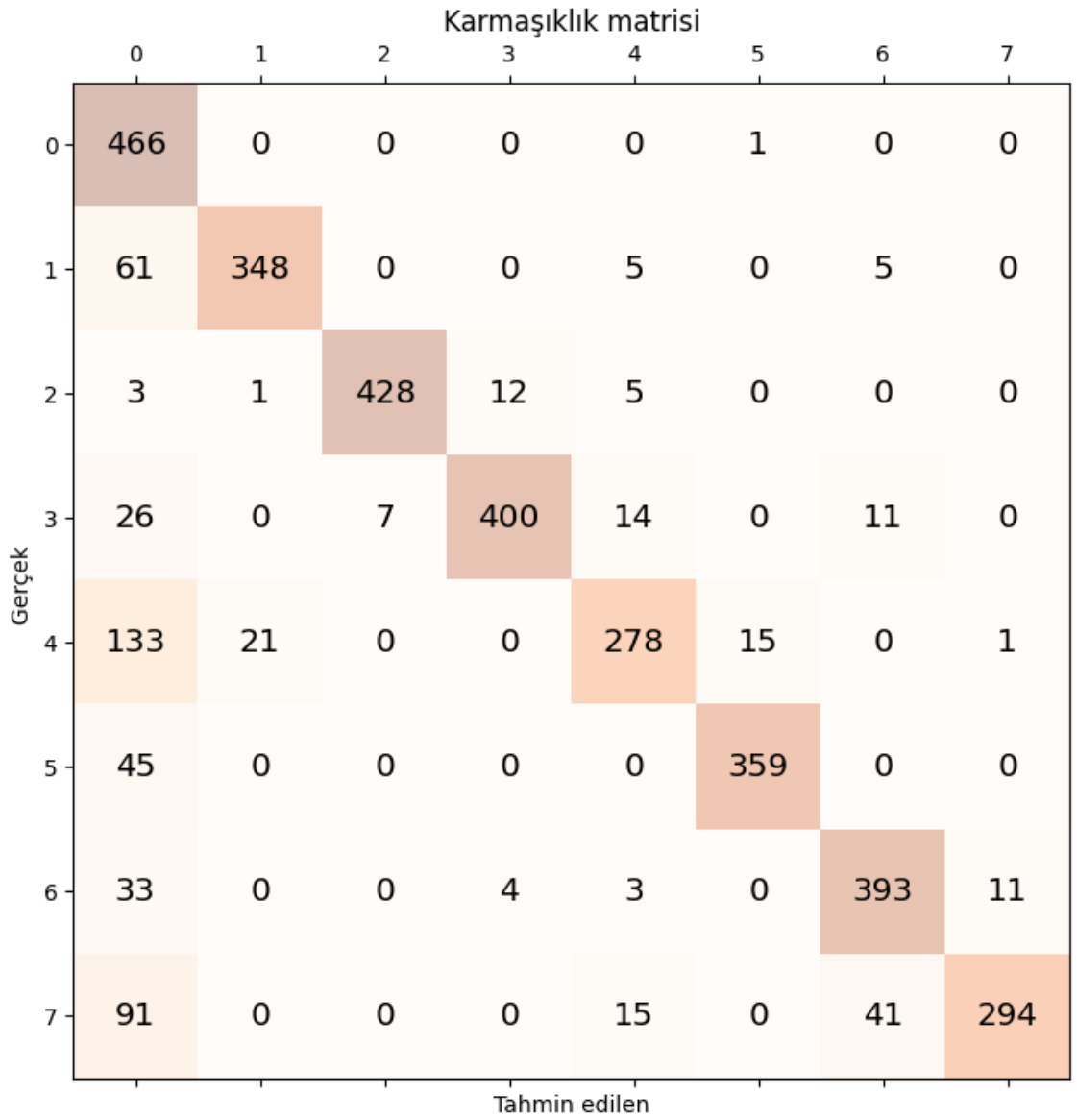
ESA modelinin eğitim ve doğrulama doğruluğu grafiği Şekil 5.12'ye göre, modelin başlangıçta düşük bir doğruluk değeriyle başladığını, ancak eğitim adımları ilerledikçe doğruluğun arttığını göstermektedir. Bu grafiğe bakarak, modelin eğitim sürecinin başarılı olduğu ve doğruluk oranının arttığını görülmektedir.



Şekil 5.12. ESA modelinin eğitim ve doğrulama doğruluğu grafiği

ESA modeline ait performans metrikleri incelendiğinde (Çizelge 5.6), BENIGN sınıfı için kesinlik %54, duyarlılık %100 ve f1-skoru %70 olarak ölçülmüştür. NetBIOS, LDAP, MSSQL, Syn ve UDP sınıfları için kesinlik, duyarlılık ve F1 skoru oldukça yüksektir (%87 ve üzeri). Ancak, Portmap ve UDPLag sınıfları için duyarlılık düşük olduğundan, bu sınıfları doğru bir şekilde sınıflandırmada sorun yaşanmaktadır. Modelin doğruluğu %84,02 olarak ölçülmüştür, bu da modelin sınıflandırma yaparken doğru sonuçları verme oranının iyi düzeyde olduğunu göstermektedir.

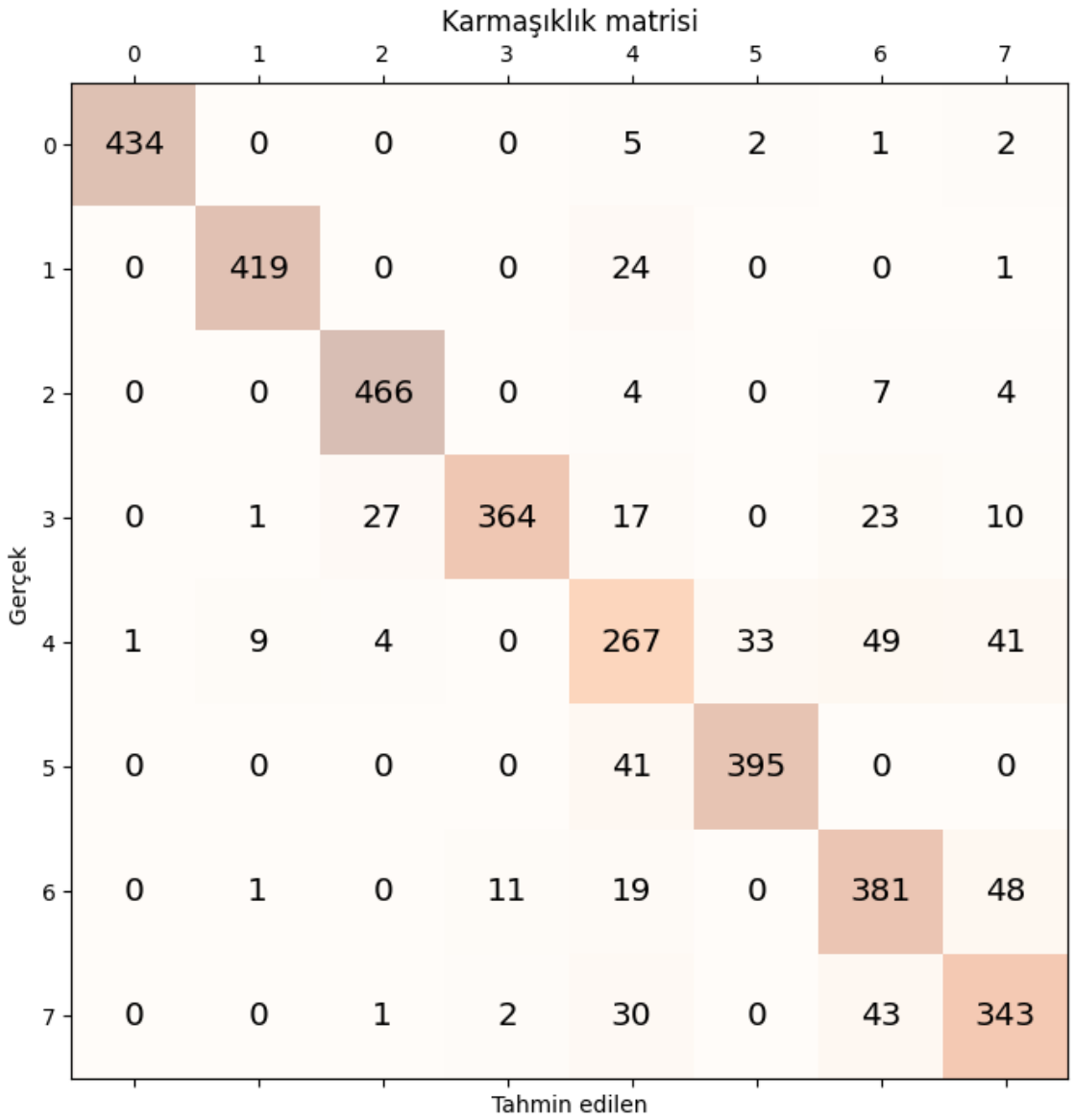
Karmaşıklık matrisi incelendiğinde (Şekil 5.13), Portmap ve UDPLag sınıflarının yanlış sınıflandırma sayısının diğer sınıflara göre daha fazla olduğu görülmektedir. Model bu sınıfları sınıflandırmada yeterince başarılı olamamıştır.



Şekil 5.13. ESA modeli karmaşıklık matrisi

Çizelge 5.6. ESA için performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 54	% 100	% 70
1	**NetBIOS**	% 94	% 83	% 88
2	**LDAP**	% 98	% 95	% 97
3	**MSSQL**	% 96	% 87	% 92
4	**Portmap**	% 87	% 62	% 72
5	**Syn**	% 96	% 89	% 92
6	**UDP**	% 87	% 89	% 88
7	**UDPLag**	% 96	% 67	% 79
Modelin Accuracy (Doğruluğu) %		% 84,02		



Şekil 5.14. LR modeli karmaşıklık matrisi

Çizelge 5.7. LR için performans metrikleri

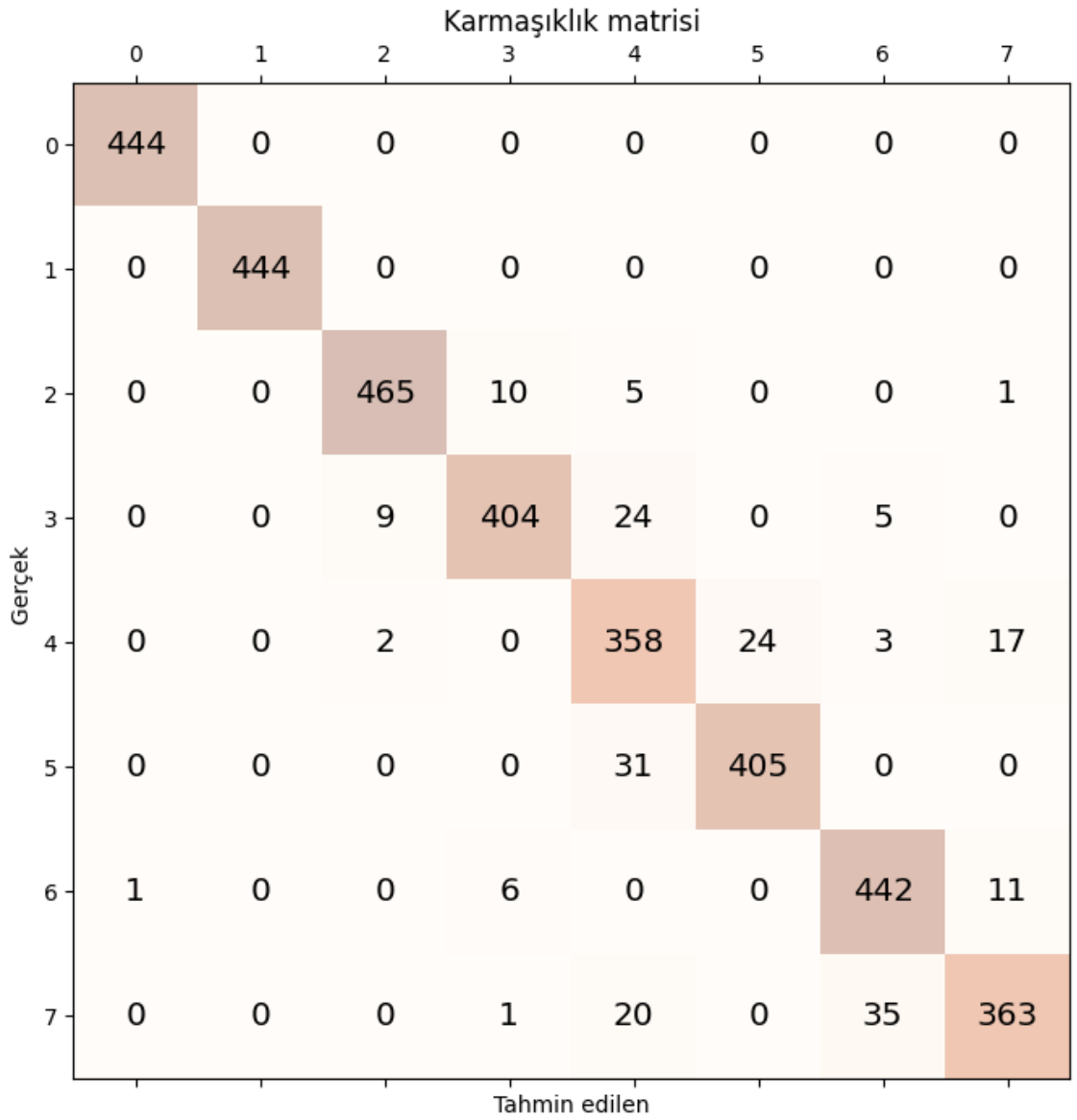
Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 100	% 98	% 99
1	**NetBIOS**	% 97	% 94	% 96
2	**LDAP**	% 94	% 97	% 95
3	**MSSQL**	% 97	% 82	% 89
4	**Portmap**	% 66	% 66	% 66
5	**Syn**	% 92	% 91	% 91
6	**UDP**	% 76	% 83	% 79
7	**UDPLag**	% 76	% 82	% 79
Modelin Accuracy (Doğruluğu) %		% 86,94		

LR modelinin performansına bakıldığında, modelin doğruluğu % 86,94'tür. Çizelge 5.7'teki sınıflandırma metriklerine göre, modelin en yüksek kesinlik oranı % 100 ile BENIGN sınıfında, en yüksek duyarlılık oranı % 97 ile LDAP sınıfında elde edilmiştir. En yüksek F1-Skor oranı ise % 99 ile BENIGN sınıfında elde edilmiştir.

Karmaşıklık matrisi grafiğine (Şekil 5.14) baktığımızda, modelin en yüksek yanlış tahmin oranının Portmap sınıfında olduğunu görülmektedir. Bu sınıfta yanlış pozitif ve yanlış negatif tahminler yapmıştır. Bu sınıfın sınıflandırılması model için zor olduğu tespit edilmiştir.

RO modeli için sınıflandırma metrikleri oldukça yüksek kesinlik, duyarlılık ve f1-Skor oranları göstermektedir (Çizelge 5.8). Tüm sınıflar için kesinlik, duyarlılık ve f1-Skor oranları % 82'nin üzerindedir. BENIGN ve NetBIOS sınıfları için % 100 kesinlik, duyarlılık ve f1-Skor oranları elde edilmiştir. RO modelinin doğruluğu % 94,19'dur, bu da oldukça yüksek bir değerdir.

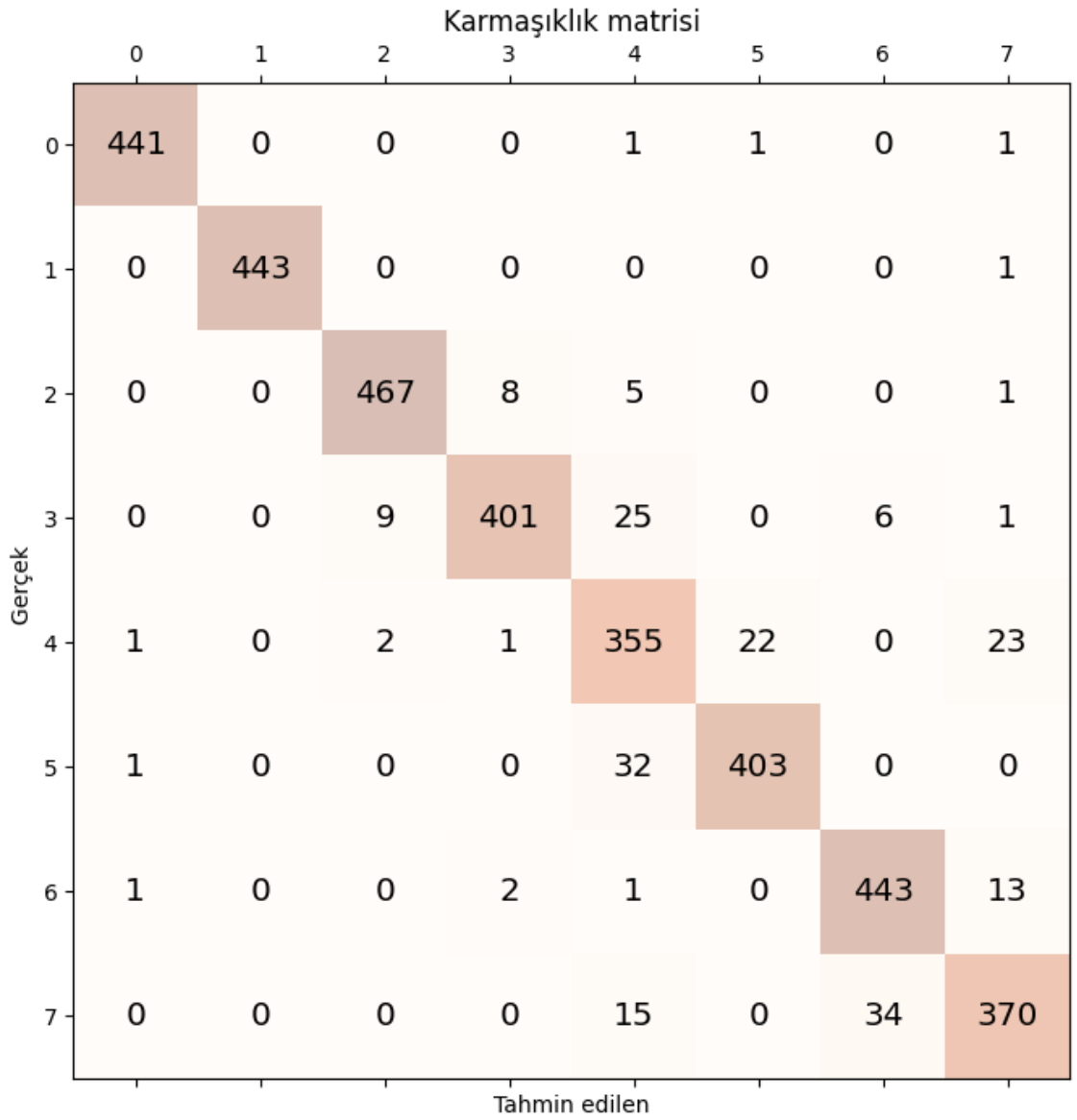
Karmaşıklık matrisine (Şekil 5.15) bakıldığında, modelin yanlış tahminlerinin çoğunlukla UDPLag ve Portmap sınıflarında olduğunu görülmektedir. UDPLag sınıfı için yanlış pozitif tahminler yapılmıştır, Portmap sınıfı için ise hem yanlış pozitif hem de yanlış negatif tahminler yapılmıştır. Ancak tüm sınıfların altında görülen sayılar oldukça düşüktür, bu nedenle modelin sınıflandırma performansı genel olarak iyi olarak değerlendirilmektedir.



Şekil 5.15. RO modeli karmaşıklık matrisi

Çizelge 5.8. RO için performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 100	% 100	% 100
1	**NetBIOS**	% 100	% 100	% 100
2	**LDAP**	% 98	% 97	% 97
3	**MSSQL**	% 96	% 91	% 94
4	**Portmap**	% 82	% 89	% 85
5	**Syn**	% 94	% 93	% 94
6	**UDP**	% 91	% 96	% 94
7	**UDPLag**	% 93	% 87	% 90
Modelin Accuracy (Doğruluğu) %		% 94,19		

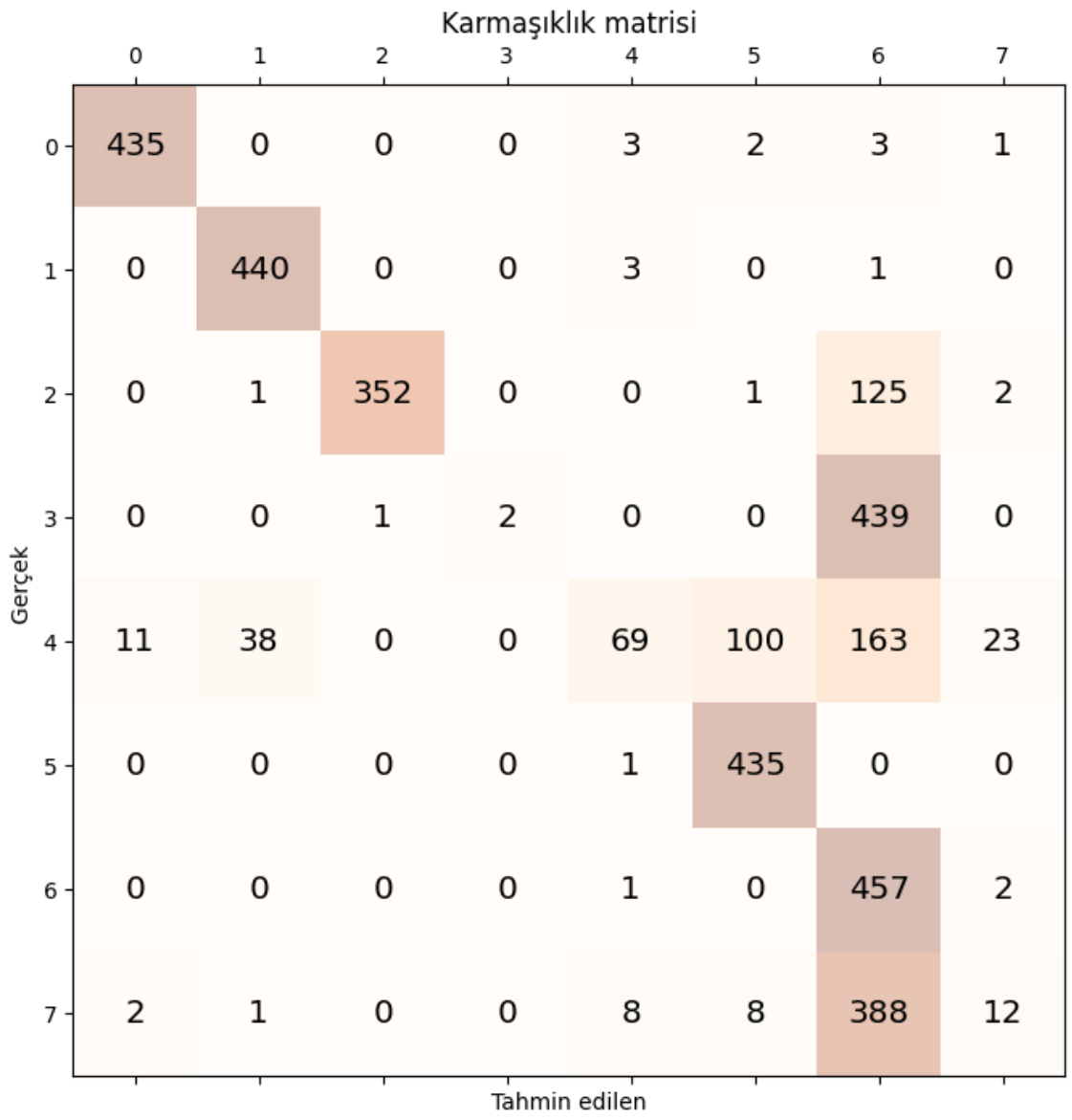


Şekil 5.16. KA modeli karmaşıklık matrisi

Çizelge 5.9. KA için performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 99	% 99	% 98
1	**NetBIOS**	% 100	% 100	% 100
2	**LDAP**	% 98	% 97	% 97
3	**MSSQL**	% 97	% 91	% 94
4	**Portmap**	% 82	% 88	% 85
5	**Syn**	% 95	% 92	% 94
6	**UDP**	% 92	% 96	% 94
7	**UDPLag**	% 90	% 88	% 89
Modelin Accuracy (Doğruluğu) %		% 94,13		

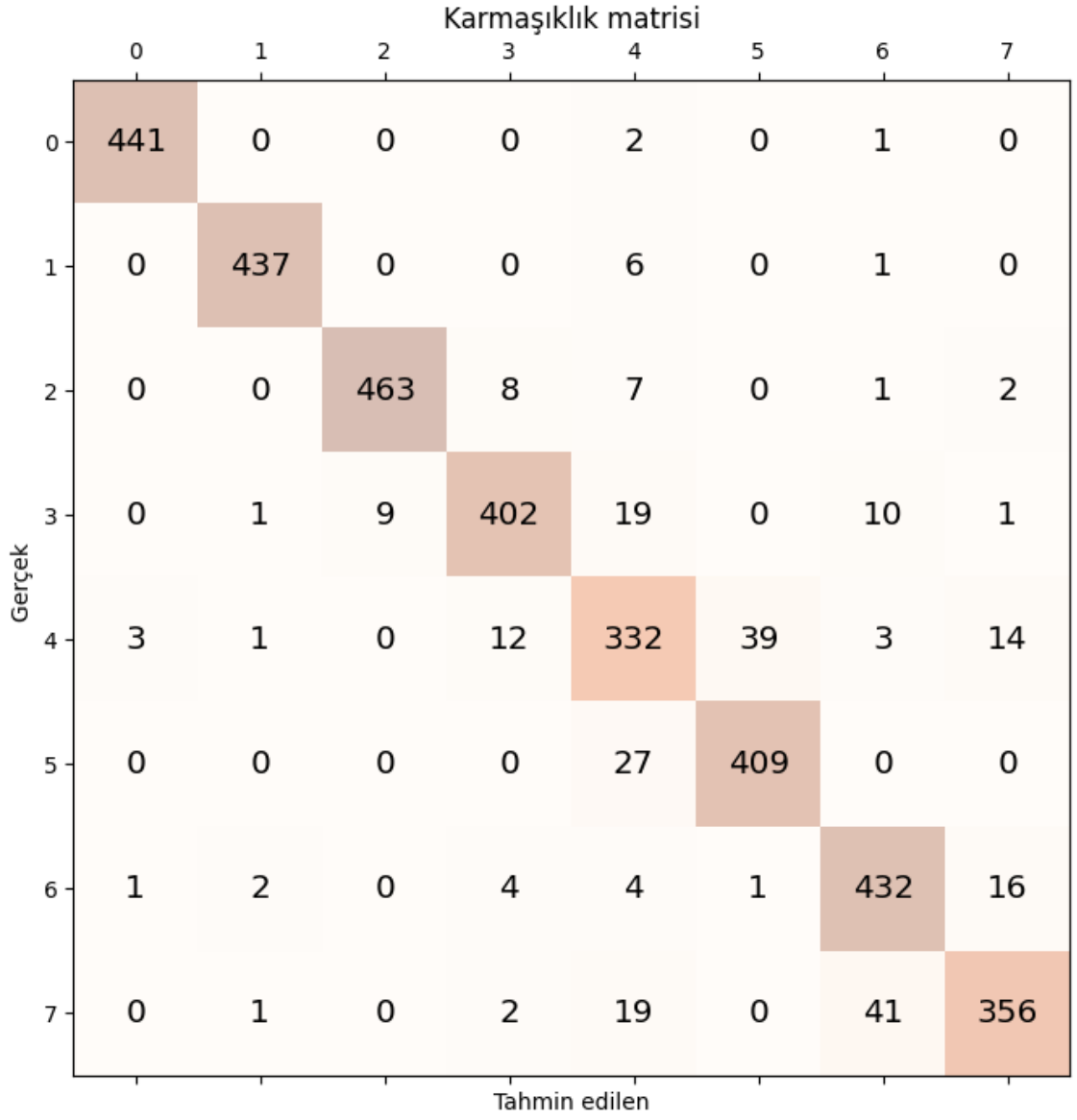
KA modeli için sınıflandırma performansı oldukça iyi olduğu görülmektedir. Karmaşıklık matrisinde (Şekil 5.16) de görülebileceği gibi, model genellikle sınıfları doğru tahmin etmiştir. Ancak, bazı sınıflarda hatalar yapılmıştır. Özellikle Portmap ve UDPLag sınıfları için modelin duyarlılık değerleri biraz düşüktür. Portmap sınıfı ve UDPLag sınıfı için duyarlılık değerleri % 88'dir. Bu, bu sınıflardaki bazı örneklerin yanlış etiketlendiği anlamına gelmektedir. Çizelge 5.9'da gösterildiği gibi, modelin doğruluğu %94,13'tür ve diğer sınıfların kesinlik, duyarlılık ve f1-Skor değerleri oldukça yüksektir. Özellikle NetBIOS sınıfı için %100 kesinlik, duyarlılık ve f1-Skor değerleri dikkat çekicidir. Bu nedenle, bu modelin genel olarak iyi performans gösterdiği tespit edilmiştir.



Şekil 5.17. NB modeli karmaşıklık matrisi

Çizelge 5.10. NB için performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 97	% 98	% 98
1	**NetBIOS**	% 92	% 99	% 95
2	**LDAP**	% 100	% 73	% 84
3	**MSSQL**	% 100	% 1	% 1
4	**Portmap**	% 81	% 17	% 28
5	**Syn**	% 80	% 100	% 89
6	**UDP**	% 29	% 99	% 45
7	**UDPLag**	% 30	% 3	% 5
	Modelin Accuracy (Doğruluğu) %	% 62,37		



Şekil 5.18. KEYK modeli karmaşıklık matrisi

Çizelge 5.11. KEYK için performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık)%	F1-Score (F1-Skor) %
0	**BENIGN**	% 99	% 99	% 99
1	**NetBIOS**	% 99	% 98	% 99
2	**LDAP**	% 98	% 96	% 97
3	**MSSQL**	% 94	% 91	% 92
4	**Portmap**	% 80	% 82	% 81
5	**Syn**	% 91	% 94	% 92
6	**UDP**	% 88	% 94	% 91
7	**UDPLag**	% 92	% 85	% 88
Modelin Accuracy (Doğruluğu) %		% 92,69		

NB modelinin performans metriklerine (Çizelge 5.10) göre, modelin performansının oldukça düşük olduğu görülmektedir. Kesinlik ve duyarlılık değerlerinin çoğu sınıf için düşük olduğu görülmekte ve f1-Skorları da genellikle düşük çıkmıştır. Modelin doğruluğu da %62.37, yani bu modele göre model sınıflandırma yaparken oldukça hatalı olduğu tespit edilmiştir. Ayrıca, MSSQL sınıfı için duyarlılık değeri %1 olduğu için bu sınıfı doğru bir şekilde sınıflandırmada başarısız olmuştur. Benzer şekilde, UDPLag sınıfı için de kesinlik ve duyarlılık değerleri oldukça düşük olduğundan doğru sınıflandırma yapmakta başarılı bir model olmamıştır.

NB modelinin karmaşıklık matrisi (Şekil 5.17) incelendiğinde, modelin LDAP, MSSQL, Portmap ve UDPLag sınıfları için zayıf kaldığını göstermektedir. Bu durum, modelin sınıflandırma performansının iyi olmadığını göstermektedir.

KEYK modelinin performans metrikleri (Çizelge 5.11) oldukça iyi sonuçlar vermiştir. Kesinlik ve duyarlılık değerleri genellikle yüksek ve f1-Skor değerleri de iyi bir seviyededir. Ancak, Portmap ve UDPLag sınıfları için kesinlik ve duyarlılık değerleri biraz daha düşüktür. KEYK modeli için karmaşıklık matrisi de (Şekil 5.18) genel olarak iyi sonuçlar vermiştir, ancak Portmap ve UDPLag sınıfları için bazı yanlış sınıflandırmalar olduğu görülmektedir. Bununla birlikte, KEYK modelinin doğruluk değeri %92,69 ile oldukça iyi bir seviyede ve modelin sınıflandırma performansının iyi olduğu görülmektedir.

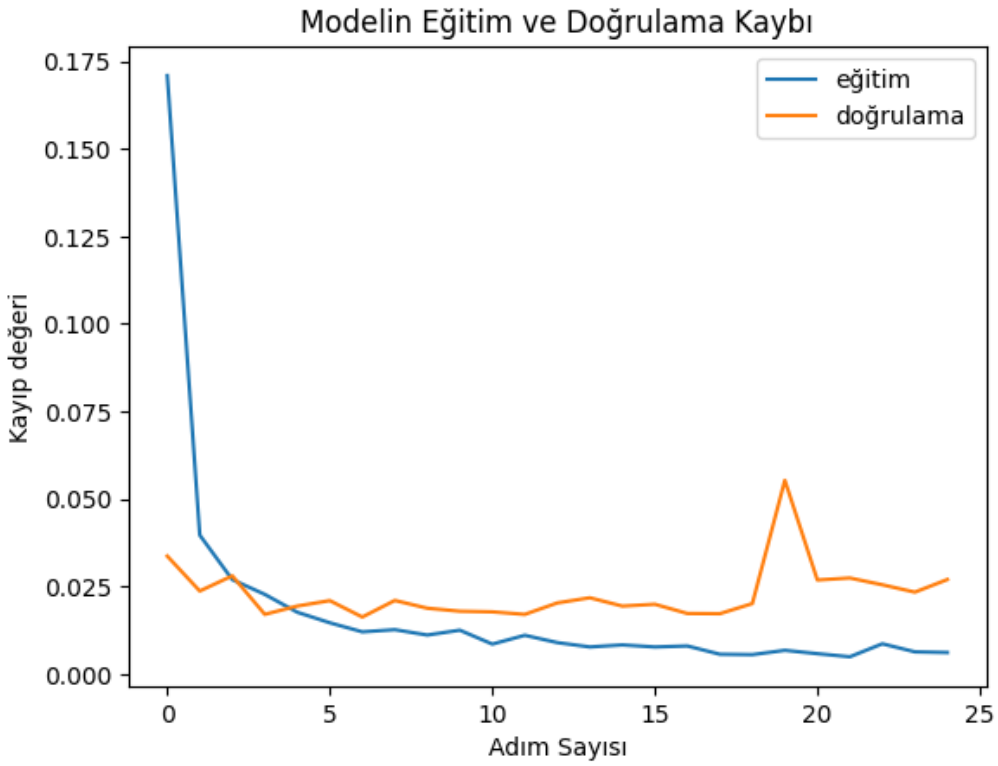
Bu tez çalışmasında CICDDoS2019 veri seti ile çoklu sınıflandırmada modellerin eğitim süreleri de hesaplanmıştır (Çizelge 5.12). Buna göre, KEYK modeli en hızlı, TSA modeli en yavaş sürede eğitimi tamamlamıştır. TSA modelinin diğer modellere göre uzun sürmesinin nedeni ise katmanlı mimariye sahip olmasındandır. Genel olarak modellerin eğitim sürelerinin iyi olduğu görülmektedir. Çoklu sınıflandırmada sonuç olarak RO

%94,19 ile en iyi sınıflandırma performansına sahip model, NB ise %62,37 oranı ile en düşük sınıflandırma performansına sahip model olarak tespit edilmiştir.

Çizelge 5.12. CICDDoS2019 çoklu sınıflandırma modellerin eğitim zamanları

Model	*Zaman(ms)*
YSA	49515
UKSB	133818
TSA	1200903
ESA	64768
LR	337
RO	104
KA	41
NB	7
KEYK	1

4.2.2. İkili sınıflandırma sonuçları

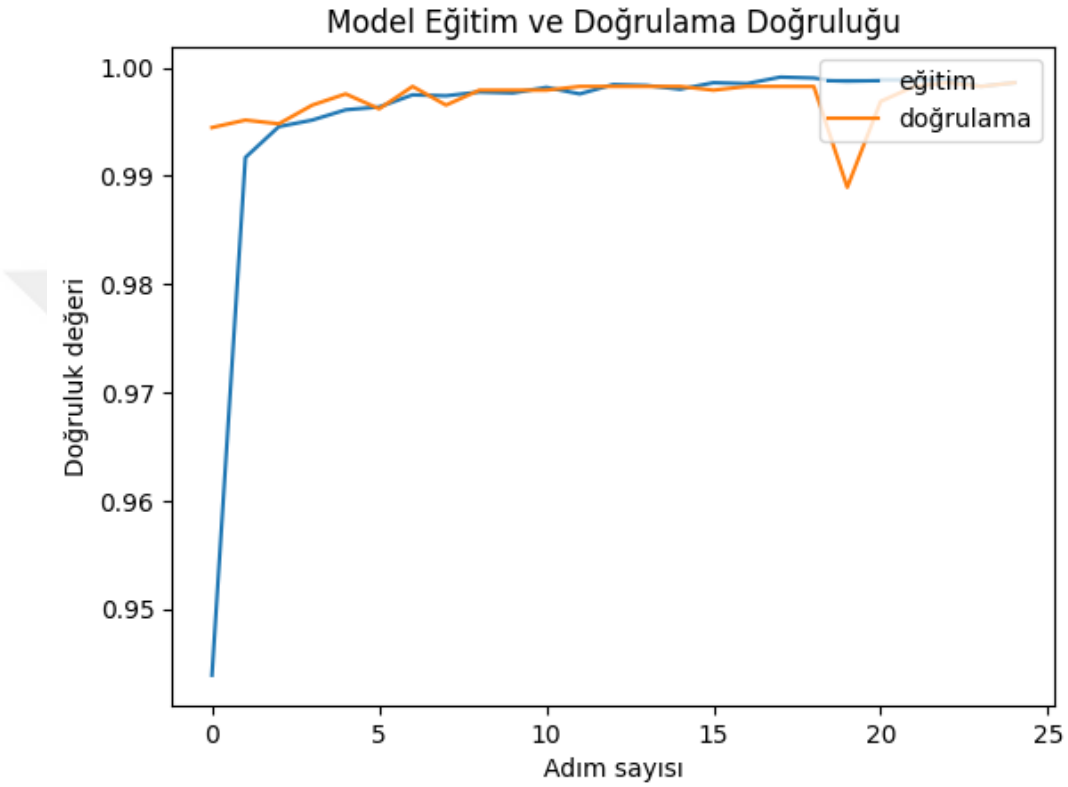


Şekil 5.19. YSA modeli ikili sınıflandırma eğitim ve doğrulama kaybı grafiği

YSA modelinin eğitim ve doğrulama kaybı grafiği (Şekil 5.19) incelendiğinde, başlangıçta eğitim ve doğrulama kayıplarının yüksek olduğu görülmektedir. Ancak, eğitim adımlarının sayısı arttıkça kayıp değerlerinin azaldığı ve eğitim setinde kayıp değerinin azaldığı gözlenmektedir. Doğrulama kaybı da benzer bir şekilde, eğitim

adımlarının artmasıyla azalmaktadır, ancak eğitim kaybı kadar hızlı azalmamaktadır. Bu, modelin overfitting (aşırı uyum) eğilimi göstermediğini göstermektedir.

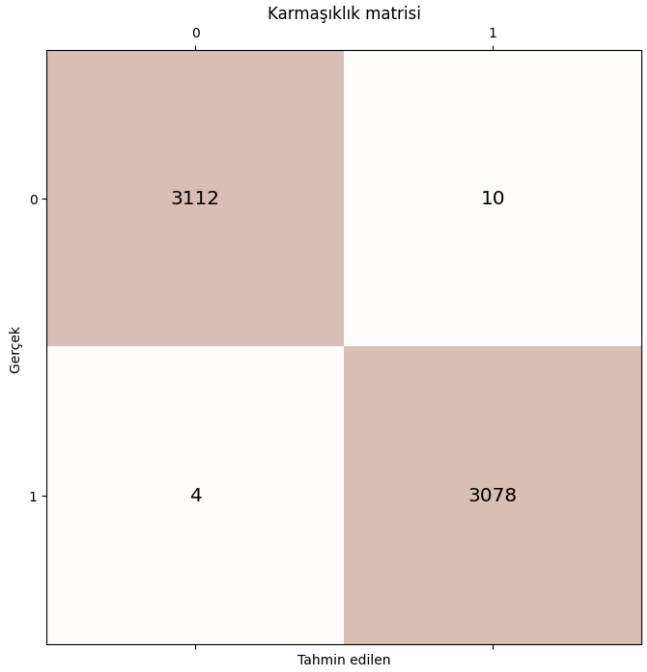
Genel olarak, modelin eğitim ve doğrulama kayıplarının düşük olduğu ve benzer bir şekilde azaldığı gözlenmektedir, bu da modelin iyi bir performans sergilediğini göstermektedir.



Şekil 5.20. YSA modeli ikili sınıflandırma eğitim ve doğrulama doğruluğu grafiği

YSA modelinin doğrulama doğruluğu grafiği (Şekil 5.20) incelendiğinde, doğrulama doğruluğunun da benzer şekilde, eğitim adımlarının artmasıyla birlikte artmaktadır, ancak eğitim doğruluğuna kıyasla daha yavaş bir artış oranı göstermektedir. Bu durum, modelin eğitim verilerine overfitting eğilimi göstermediğini göstermektedir.

Sonuç olarak, eğitim ve doğrulama doğruluğu değerlerinin yüksek olduğu ve benzer bir şekilde arttığı görülmektedir. Bu, modelin ikili sınıflandırmada iyi bir performans sergilediğini ve sınıflandırma görevini başarıyla yerine getirdiğini göstermektedir.



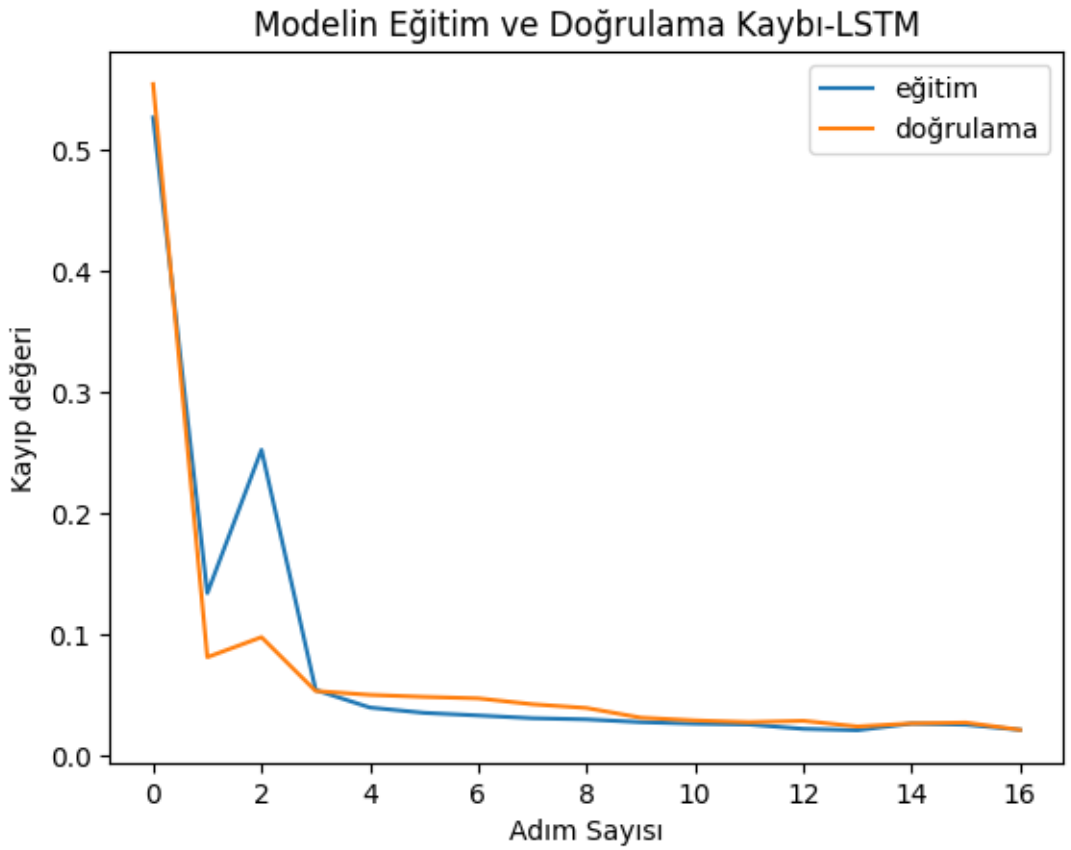
Şekil 5.21. YSA modeli iki sınıflı karmaşıklık matrisi

Çizelge 5.13. YSA için performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 100	% 100	% 100
1	**ATTACK**	% 100	% 100	% 100
Modelin Accuracy (Doğruluğu) %		% 99,77		

YSA modelinin doğruluğu Çizelge 5.13'te verildiği gibi %99,77, yani verilerin %99,77'sinin doğru bir şekilde tahmin edildiği anlamına gelmektedir. Kesinlik %100 ve duyarlılık %100 olarak elde edilmiştir, bu da modelin hem BENIGN sınıfını hem de ATTACK sınıfını %100 doğru şekilde tahmin ettiği anlamına gelmektedir. F1-Skor %100 oranında, bu da modelin hem kesinlik hem de duyarlılık metriklerinin eşit derecede iyi performans gösterdiği anlamına gelmektedir.

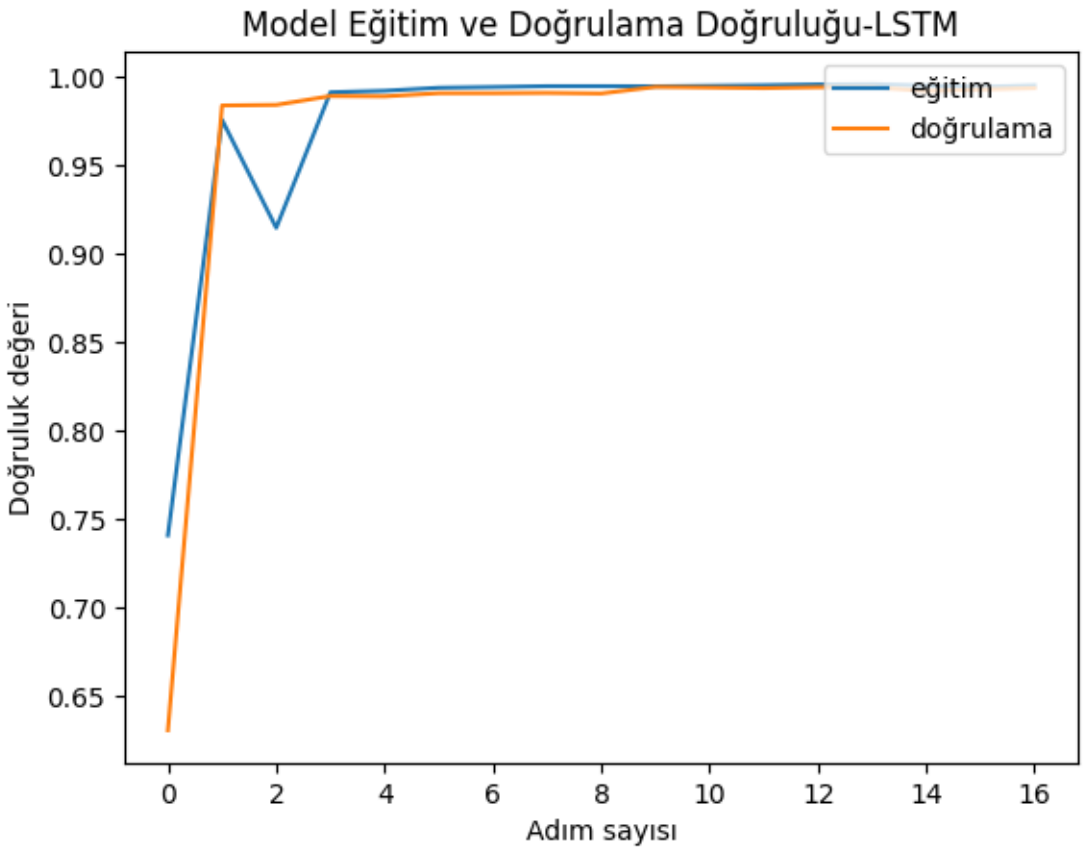
Karmaşıklık matrisi (Şekil 5.21) incelendiğinde, model her iki sınıf için de doğru tahminler yapmıştır. Sonuç olarak, YSA modeli oldukça başarılı ve verilerin büyük bir kısmını doğru bir şekilde tahmin edebilmektedir.



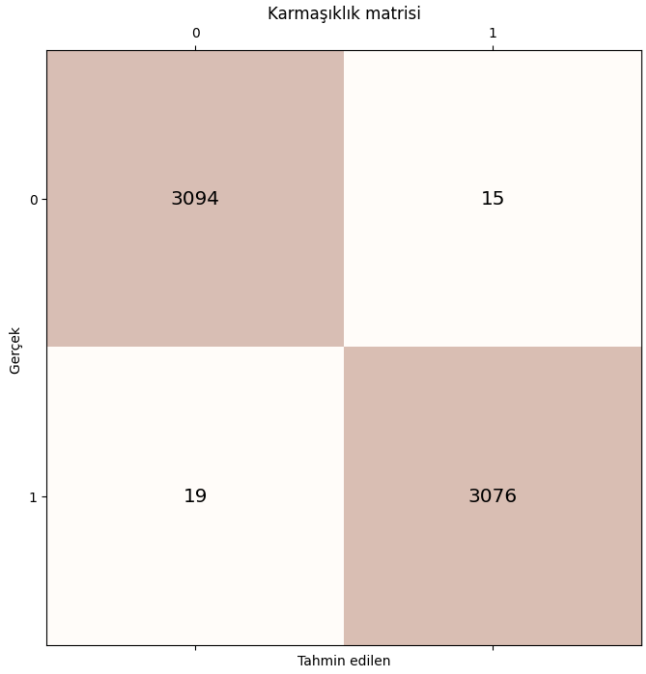
Şekil 5.22. UKSB modelinin eğitim ve doğrulama kaybı grafiği

UKSB modelinin ikili sınıflandırmada Şekil 5.22'ye bakıldığında, eğitim kaybının ve doğrulama kaybının zamanla azaldığı görülmektedir, bu da modelin öğrenme sürecinin iyi olduğunu ve overfitting'in (aşırı uydurma) meydana gelmediğini göstermektedir. Şekil 5.23'te de modelin eğitim ve doğrulama doğruluğu grafiği verilmiştir.

UKSB modelinin karmaşıklık matrisi Şekil 5.24'te verilmiştir. Buna göre modelin sınıflandırma da yanlış sınıflandırma sayıları oldukça düşüktür. Çizelge 5.14'te verilen performans metriklerine göre, BENIGN sınıfına ait kesinlik, duyarlılık ve f1-skor değerleri sırasıyla %99, %100, %99; Attack sınıfına ait kesinlik, duyarlılık ve f1-skor değerleri sırasıyla %100, %99 ve %99'dur. Modelin başarısı %99,45 olarak ölçülmüştür. Sonuç olarak UKSB modeli ikili sınıflandırmada oldukça yüksek bir başarı göstermiştir.



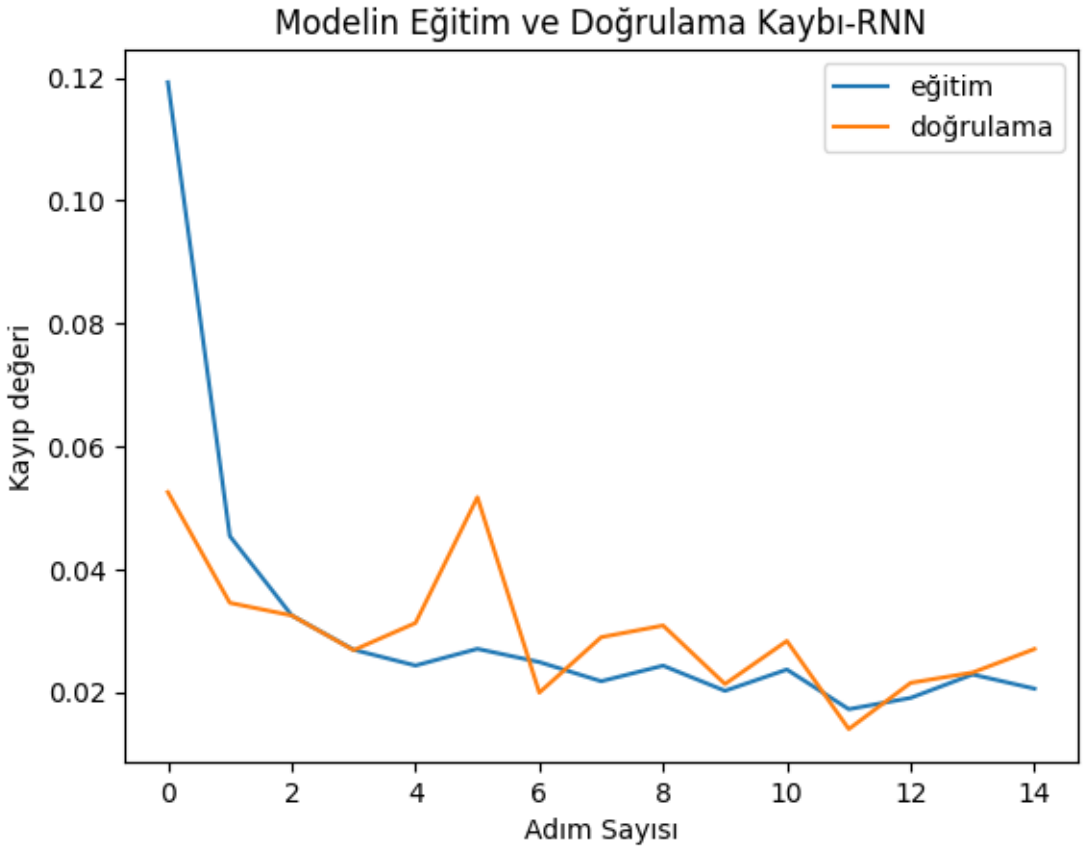
Şekil 5.23. UKSB modelinin eğitim ve doğrulama doğruluğu grafiği



Şekil 5.24. UKSB modeli karmaşıklık matrisi

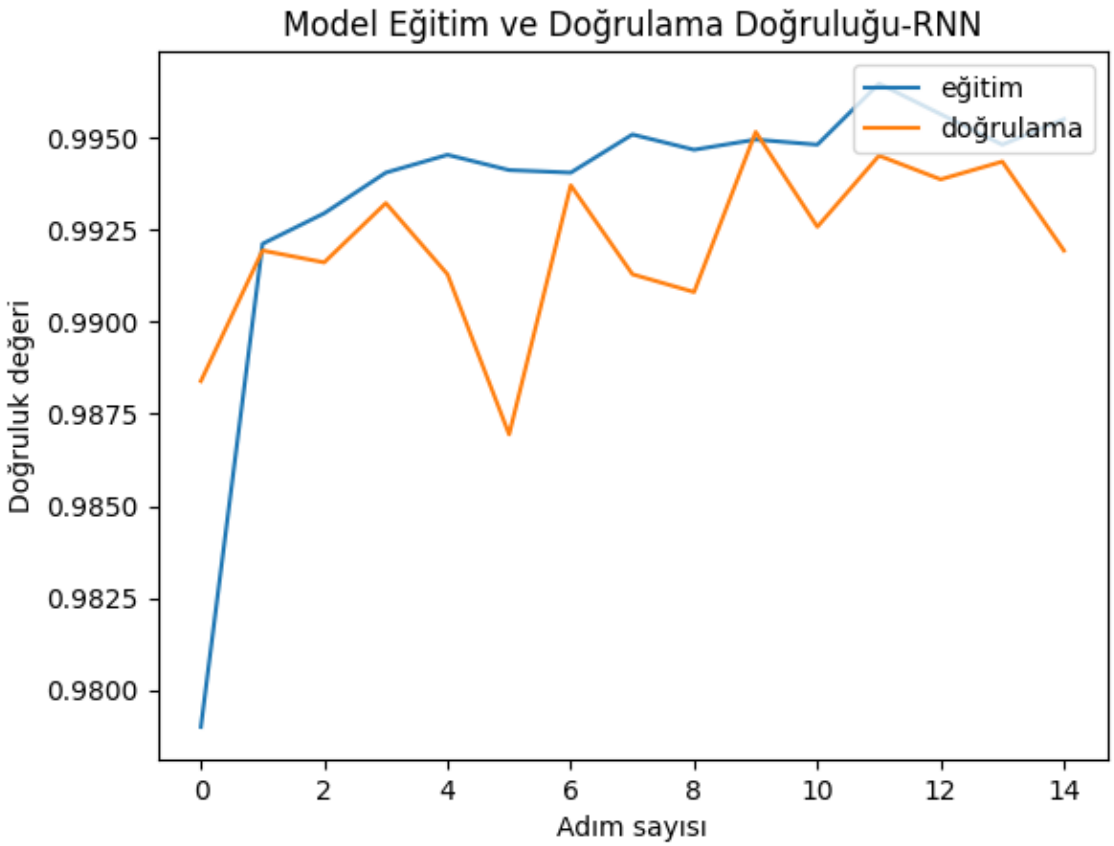
Çizelge 5.14. UKSB için performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 99	% 100	% 99
1	**ATTACK**	% 100	% 99	% 99
Modelin Accuracy (Doğruluğu) %		% 99,45		

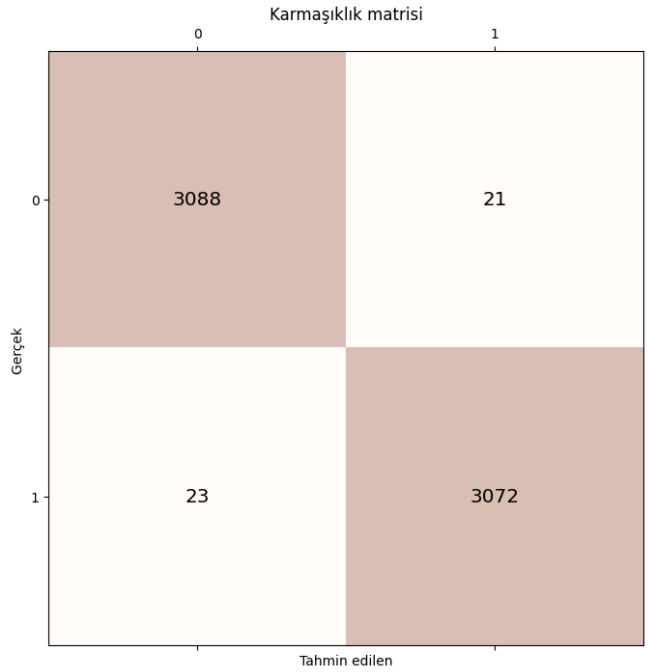


Şekil 5.25. TSA modelinin eğitim ve doğrulama kaybı grafiği

TSA modeline ait eğitim ve doğrulama grafiği ikili sınıflandırma için Şekil 5.25'te verilmiştir. Bu grafiğe göre, ilk başta, her iki kayıp da oldukça yüksektir, ancak model eğitildikçe kayıplar azalmaya başlamıştır ve sonunda yaklaşık olarak eşitlenmektedir. Modelin eğitim veri setindeki kaybı düşüktür ve doğrulama veri setindeki kayıp, eğitim veri setindeki kayıptan biraz daha yüksektir, ancak bu makul bir farktır. Şekil 5.26'da TSA modelinin eğitim ve doğrulama doğruluğu grafiği de gösterilmektedir. Şekil 5.27'de verilen karmaşıklık matrisi incelendiğinde modelin sınıfları doğru sınıflandırmadaki kaybının da az olduğu görülmektedir



Şekil 5.26. TSA modelinin eğitim ve doğrulama doğruluğu grafiği

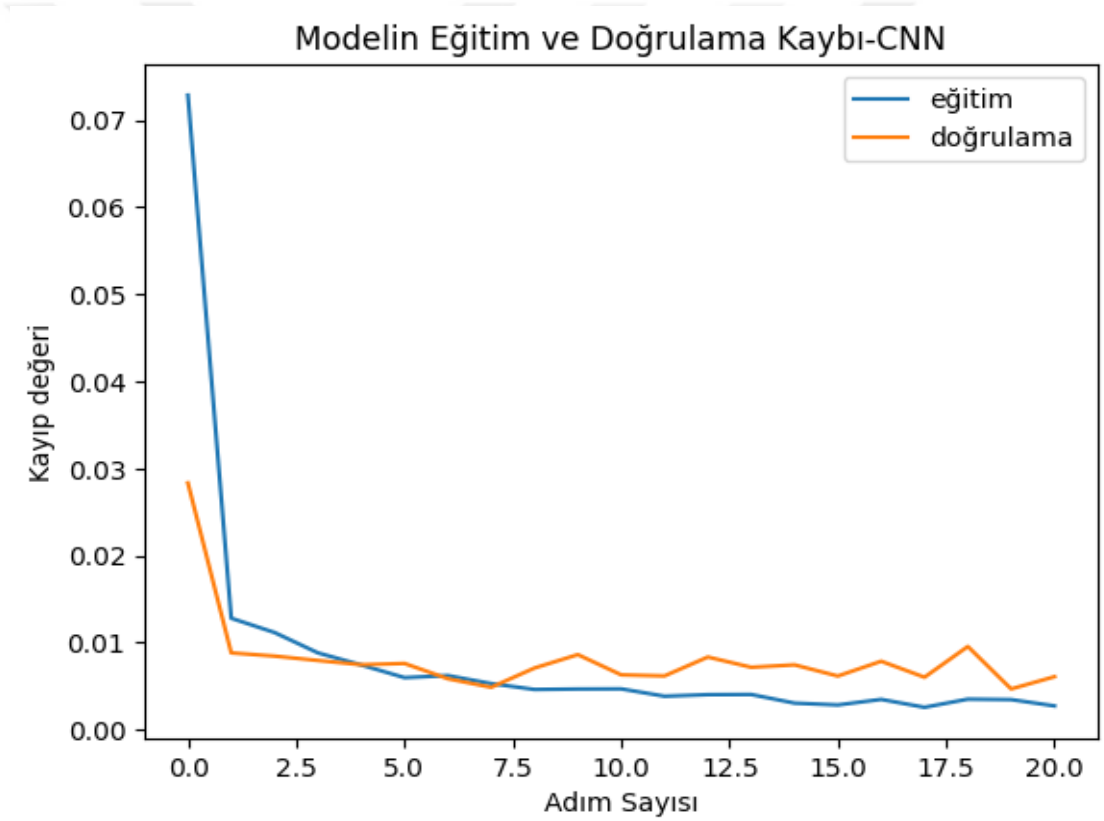


Şekil 5.27. TSA modeli karmaşıklık matrisi

Çizelge 5.15. TSA için performans metrikleri

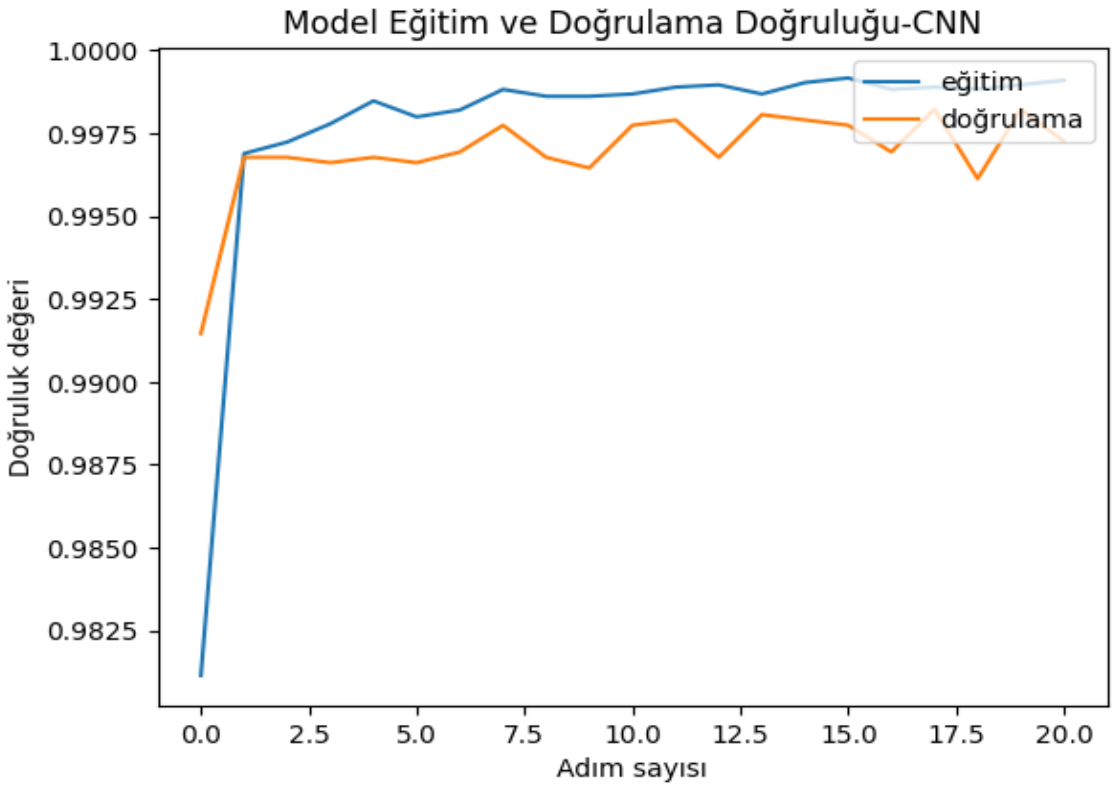
Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 99	% 99	% 99
1	**ATTACK**	% 99	% 99	% 99
Modelin Accuracy (Doğruluğu) %		% 99,29		

TSA modeline ait performans metrikleri Çizelge 5.15'te verilmiştir. Buna göre, BENIGN sınıfına ait kesinlik, duyarlılık ve f1-skor değerleri sırasıyla %99, %99, %99; Attack sınıfına ait kesinlik, duyarlılık ve f1-skor değerleri sırasıyla %99, %99 ve %99'dur. Modelin başarısı %99,29 olarak ölçülmüştür. Sonuç olarak TSA modeli ikili sınıflandırmada oldukça yüksek bir başarı göstermiştir.

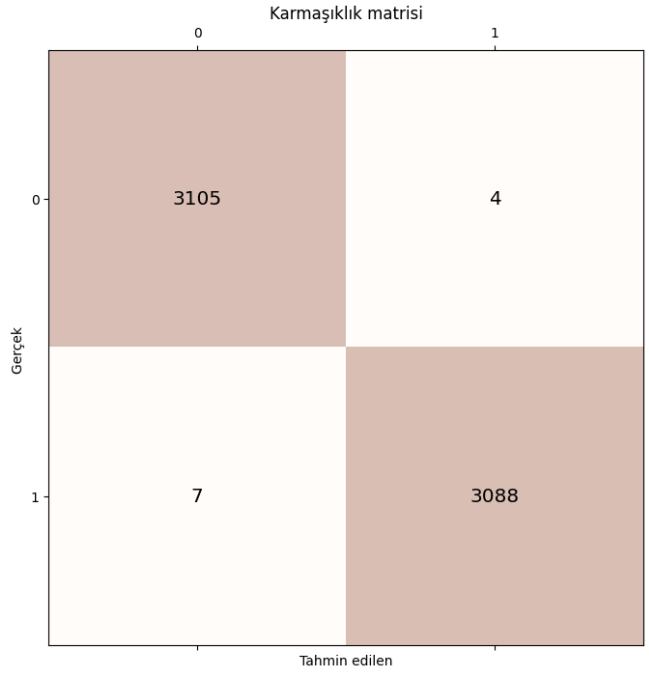


Şekil 5.28. ESA modelinin eğitim ve doğrulama kaybı grafiği

Veri setine uygulanan ESA modeline ait eğitim ve doğrulama kaybı grafiği Şekil 5.28'de, eğitim ve doğrulama doğruluğu grafiği Şekil 5.29'da verilmiştir. Grafikler incelendiğinde, modelin iyi uyum sağladığı görülmektedir. ESA modeline ait karmaşıklık matrisi Şekil 5.30'da da görüldüğü gibi sınıflar doğru bir şekilde sınıflandırılmıştır ve model %99,80 ile yüksek bir başarı elde etmiştir (Çizelge 5.16).



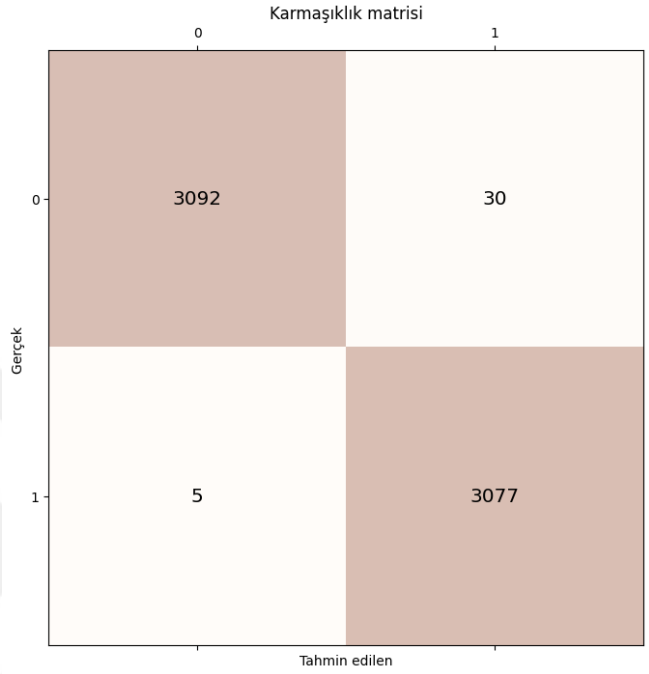
Şekil 5.29. ESA modelinin eğitim ve doğrulama doğruluğu grafiği



Şekil 5.30. ESA modeli karmaşıklık matrisi

Çizelge 5.16. ESA için performans metrikleri

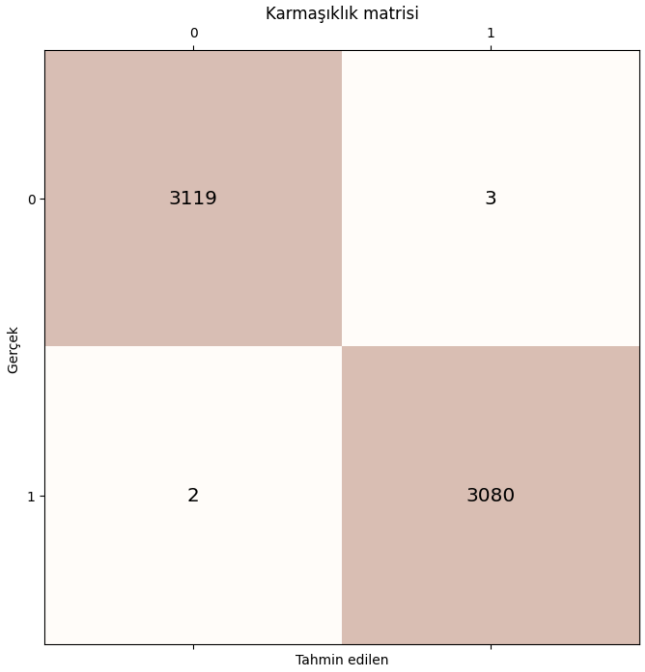
Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 100	% 100	% 100
1	**ATTACK**	% 100	% 100	% 100
Modelin Accuracy (Doğruluğu) %		% 99,82		



Şekil 5.31. LR modeli iki sınıflı karmaşıklık matrisi

Çizelge 5.17. LR için performans metrikleri

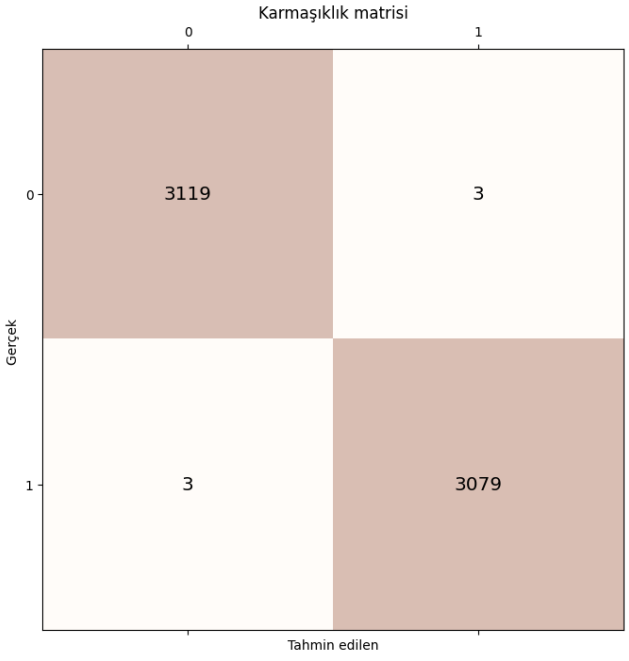
Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 100	% 99	% 99
1	**ATTACK**	% 99	% 100	% 99
Modelin Accuracy (Doğruluğu) %		% 99,43		



Şekil 5.32. RO modeli iki sınıflı karmaşıklık matrisi

Çizelge 5.18. RO için performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 100	% 100	% 100
1	**ATTACK**	% 100	% 100	% 100
Modelin Accuracy (Doğruluğu) %		% 99,80		

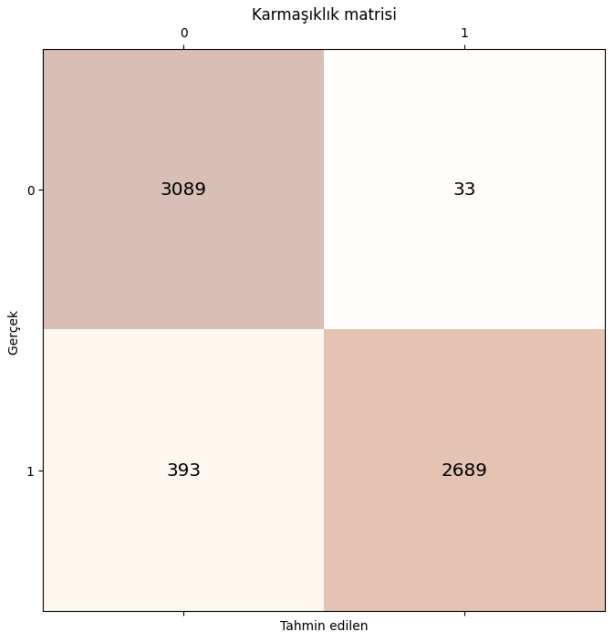


Şekil 5.33. KA modeli iki sınıflı karmaşıklık matrisi

Çizelge 5.19. KA için performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 100	% 100	% 100
1	**ATTACK**	% 100	% 100	% 100
Modelin Accuracy (Doğruluğu) %		% 99,90		

CICDDoS2019 veri setine ikili sınıflandırma için model uygulandığında, modellerin karmaşıklık matrisleri LR için Şekil 4.31, RO için Şekil 5.32, KA için Şekil 5.33'te görüldüğü gibi modellerin sınıflandırma performansları iyi derecede başarılı olarak çıkmıştır. LR modelinde BENIGN sınıfından yanlış sınıflandırılan veri sayısının diğer modellere göre biraz fazla olduğu görülmektedir. Çizelge 5.17'de LR modeli başarı oranı %99,43 olduğu görülmekte ve diğer metriklerin de oranlarının yüksek olduğu görülmektedir. Çizelge 5.18'de RO modelinin başarı oranı %99,80, Çizelge 5.19'te KA modelinin başarı oranı %99,90 olarak elde edilmiştir. Bu modellerin diğer metrikleri de incelendiğinde gayet başarılı sonuçlar verdiği görülmektedir.

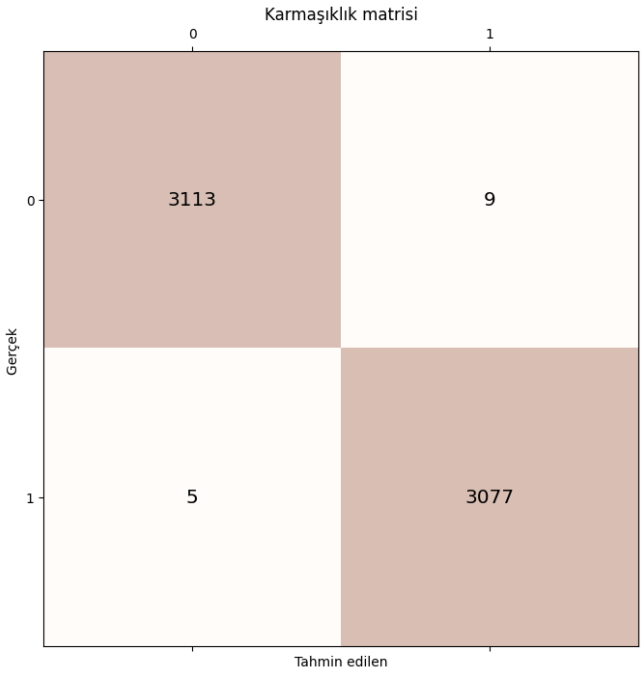


Şekil 5.34. NB modeli iki sınıflı karmaşıklık matrisi

Çizelge 5.20. NB için performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 89	% 99	% 94
1	**ATTACK**	% 99	% 87	% 93
Modelin Accuracy (Doğruluğu) %		% 93,13		

NB modeli verilerin %93,13'ünü doğru bir şekilde tahmin etmiştir. Çizelge 5.20'de görüldüğü gibi, kesinlik ve duyarlılık metrikleri BENIGN sınıfı için %89 kesinlik, %99 duyarlılık ve %94 f1-Skor olarak elde edilmiştir. ATTACK sınıfı için ise %99 kesinlik, %87 duyarlılık ve %93 f1-Skor oranı elde edilmiştir. NB modeli için karmaşıklık matrisi (Şekil 5.34) incelendiğinde, model BENIGN sınıfını nispeten iyi tahmin ederken, ATTACK sınıfı için daha düşük bir tahmin performansı sağladığı görülmektedir. Sonuç olarak NB modeli ikili sınıflandırmada iyi bir performans elde etmiştir.



Şekil 5.35. KEYK modeli iki sınıflı karmaşıklık matrisi

Çizelge 5.21. KEYK için performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 100	% 100	% 100
1	**ATTACK**	% 100	% 100	% 100
Modelin Accuracy (Doğruluğu) %		% 99,77		

KEYK modeli ile, %99,77 oranında başarılı bir sonuç elde edilmiştir. Çizelge 5.21'de verilen performans metriklerinde her iki sınıf içinde kesinlik, duyarlılık ve f1-Skor değerleri %100 oranındadır. Karmaşıklık matrisi (Şekil 5.35) incelendiğinde ise, modelin BENIGN ve ATTACK sınıflarını sınıflandırmada başarılı olduğu görülmektedir.

Modellerin eğitim performanslarının yanı sıra eğitim zamanları (Çizelge 5.22) incelendiğinde, KEYK modeli en kısa sürede eğitim performansı göstermiştir.

Çizelge 5.22. Modellerin eğitim zamanları

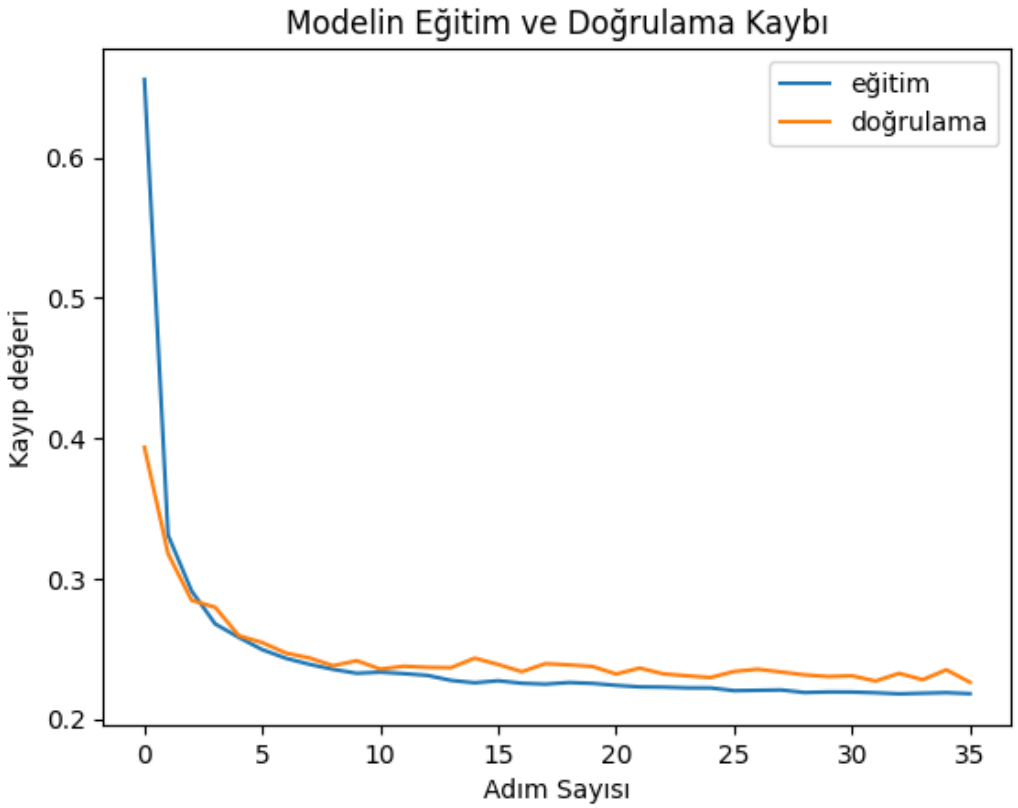
Model	*Zaman(ms)*
YSA	62543
UKSB	489141
TSA	237381
ESA	17329
LR	195
RO	156
KA	80
NB	10
KEYK	3

5.3. KEY2023 Veri Seti Sonuçları

Bu tez çalışması için oluşturulan KEY2023 veri seti ile yapılan çalışmada da modellerin ikili sınıflandırma ve çoklu sınıflandırma performansları değerlendirilmiştir. Buna göre veri ön işlemden geçen KEY2023 veri seti ile elde edilen sonuçlar iki başlık halinde incelenmiştir.

5.3.1. Çoklu sınıflandırma sonuçları

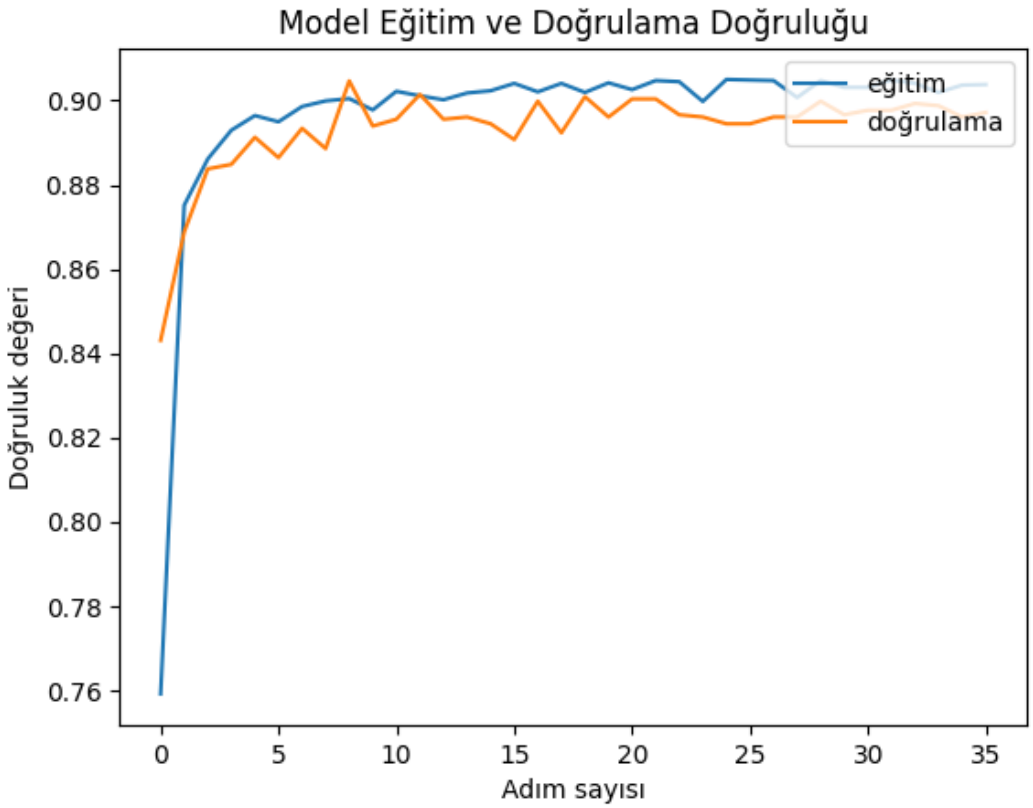
Uygulanan YSA modelinin eğitim ve doğrulama kaybı grafiğinde (Şekil 5.36), eğrilerin adım sayısı arttıkça düştüğünü görülmektedir, bu da modelin eğitim verilerine ve test verilerine uygun şekilde uyum sağladığını göstermektedir.



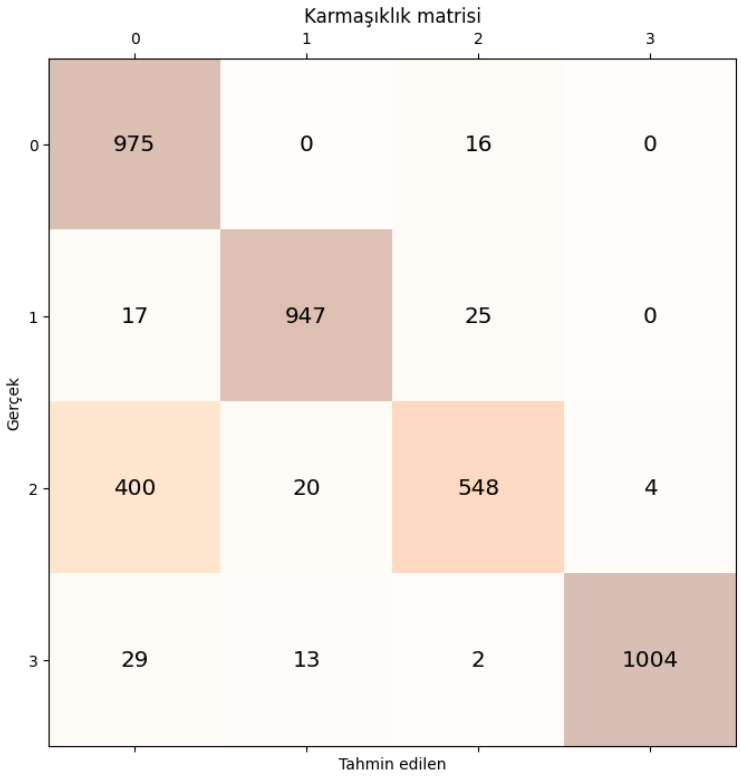
Şekil 5.36. KEY2023-YSA modelinin eğitim ve doğrulama kaybı grafiği

YSA modeli için eğitim ve doğrulama doğruluğu grafiğinde gördüğü gibi, eğitim doğruluğu adım sayısı arttıkça hızlı bir şekilde artmaktadır (Şekil 5.37). Ancak, doğrulama doğruluğu da başlangıçta artmaktadır, ancak daha sonra bir noktadan itibaren artış hızı yavaşlamaktadır. Genel olarak model performansı iyi olarak değerlendirilebilmektedir.

Bu YSA modelinin performans metriklerine göre (Çizelge 5.23), modelin doğruluğu % 87 olarak hesaplanmıştır. Kesinlik, duyarlılık ve f1-skoru gibi diğer performans metrikleri, sınıf bazında incelenmiştir. BENIGN sınıfı için, modelin kesinliği %69, duyarlılığı %98 ve f1-skoru %81 olarak hesaplanmıştır. TcpSYN sınıfı için, modelin kesinliği %96, duyarlılığı %96 ve f1-skoru %96 olarak hesaplanmıştır. İcmp sınıfı için, modelin kesinliği %93, duyarlılığı %56 ve f1-skoru %69 olarak hesaplanmıştır. Udp sınıfı için, modelin kesinliği %99, duyarlılığı %97 ve f1-skoru %98 olarak hesaplanmıştır. Bu sonuçlara göre karmaşıklık matrisi de (Şekil 5.38) incelendiğinde, BENIGN ve udp sınıfları için modelin performansı oldukça iyi iken, icmp sınıfı için düşük duyarlılık oranı nedeniyle daha düşük bir f1-skoru elde edilmiştir. TcpSYN sınıfı için de oldukça yüksek bir f1-skoru elde edilmiştir.



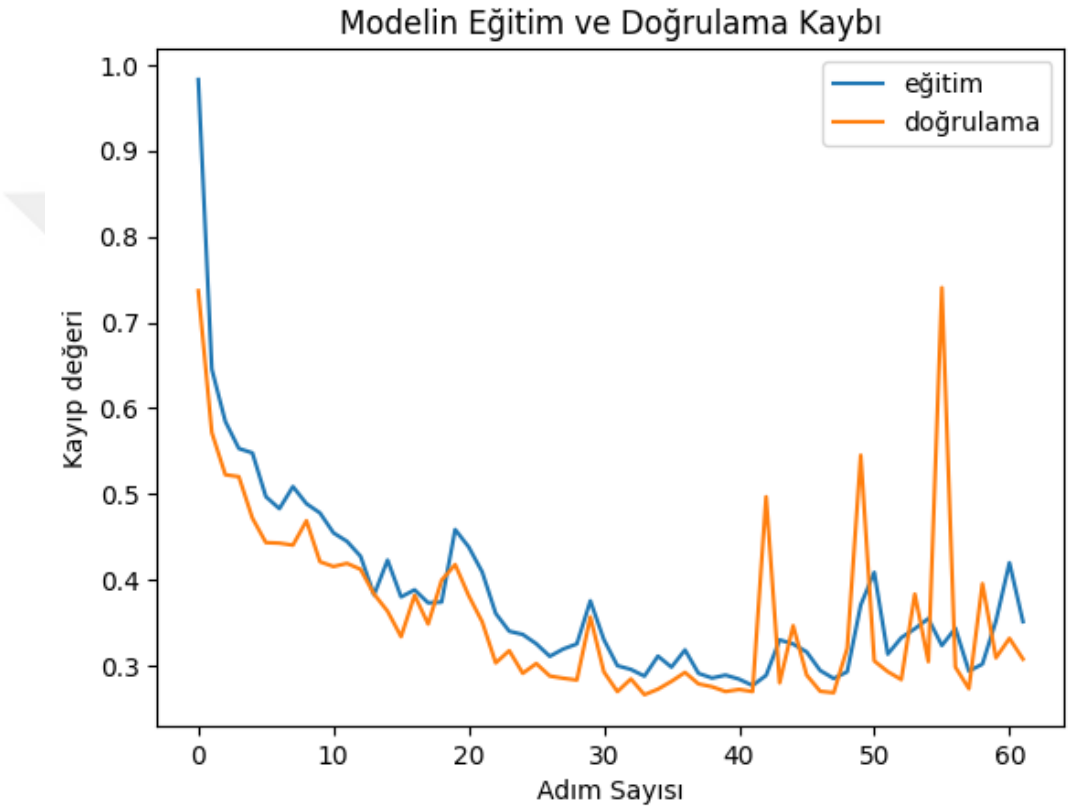
Şekil 5.37. KEY2023-YSA modelinin eğitim ve doğrulama doğruluğu grafiği



Şekil 5.38. KEY2023-YSA karmaşıklık matrisi

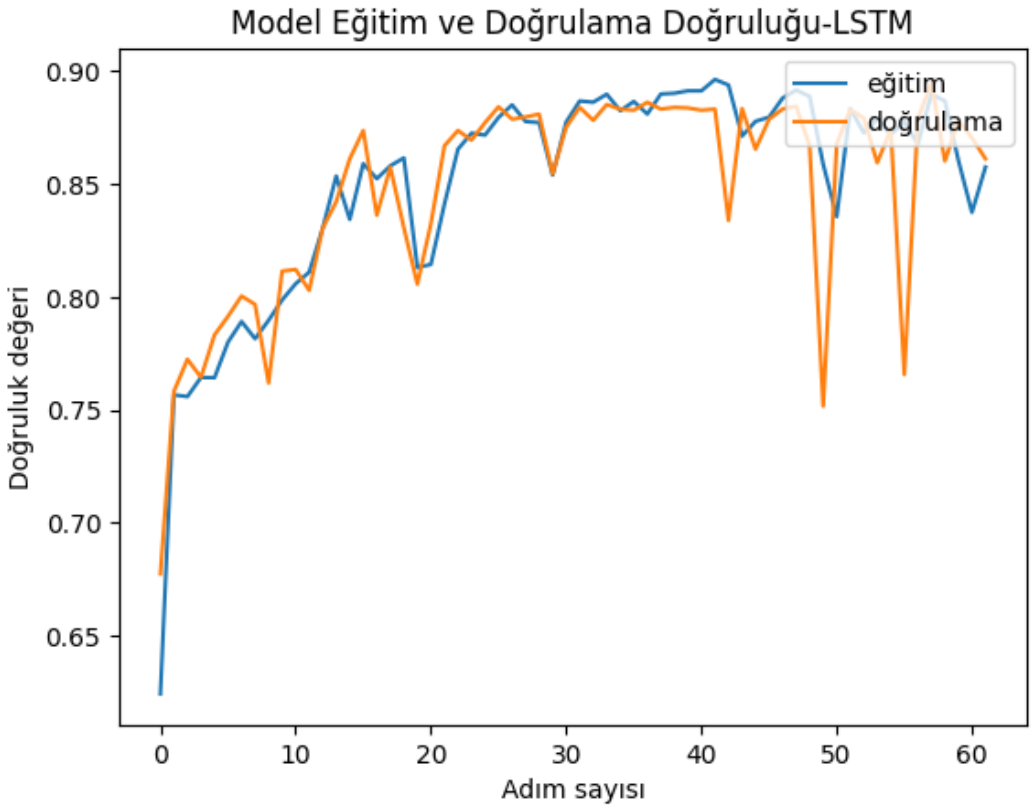
Çizelge 5.23. KEY2023-YSA için performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 69	% 98	% 81
1	**tcpSYN**	%96	% 96	% 96
2	**İcmp**	%93	% 56	% 69
3	**udp**	% 99	% 97	% 98
	Modelin Accuracy (Doğruluğu) %	% 87		

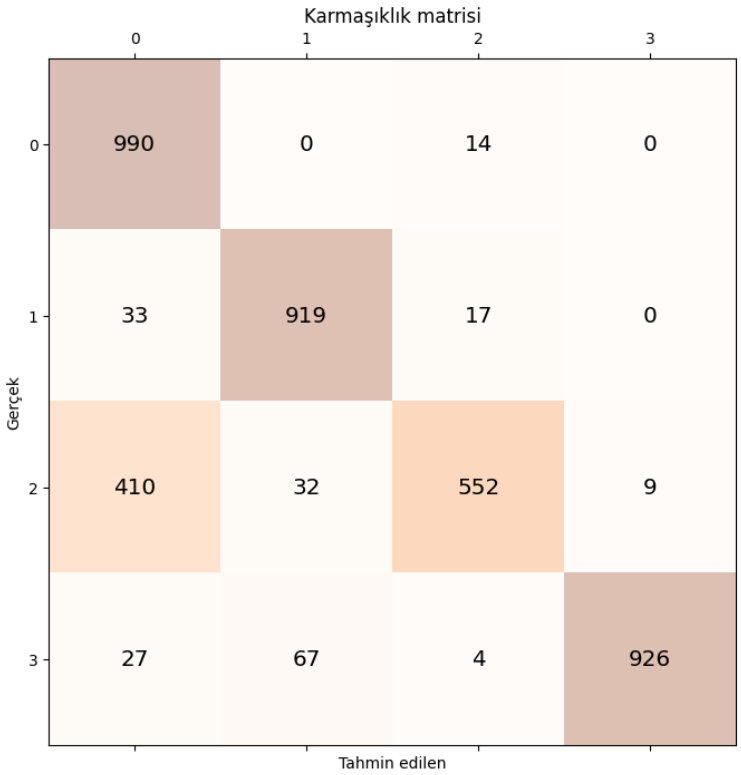


Şekil 5.39. KEY2023-UKSB modelinin eğitim ve doğrulama kaybı grafiği

UKSB modeli için eğitim ve doğrulama kaybı grafiği Şekil 5.39'da eğitim ve doğrulama kaybı adım sayısı arttıkça azalmaktadır. Fakat doğrulama kaybında 55. adımda hızlı bir artış görülmesine rağmen adım sayısı arttıkça bu kayıpta azalmaktadır. Şekil 5.40'ta eğitim ve doğrulama doğruluğu grafiği verilmiştir. Bu grafiğe göre de doğrulama doğruluğunda yine aynı adım aralığında bir düşüş meydana gelmiştir. Sonuç olarak model eğitim verilerine ve test verilerine uygun şekilde uyum sağladığı görülmektedir.



Şekil 5.40. KEY2023-UKSB modelinin eğitim ve doğrulama doğruluğu grafiği

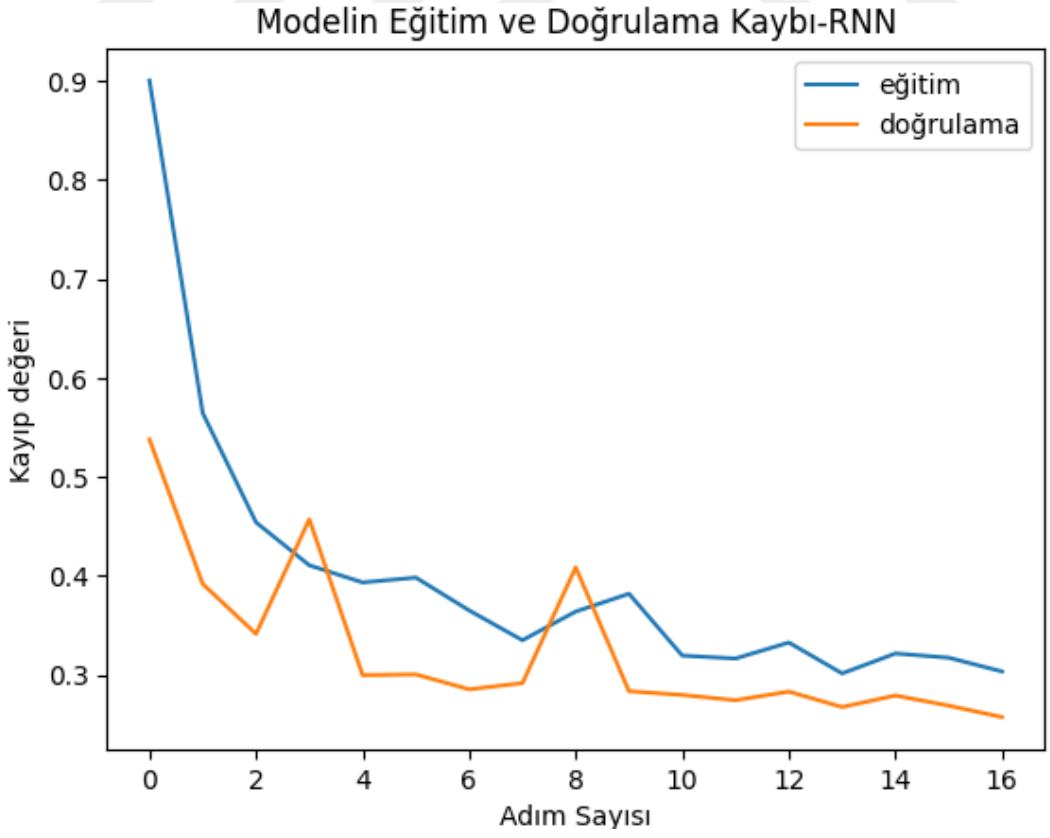


Şekil 5.41. KEY2023-UKSB modeli karmaşıklık matrisi

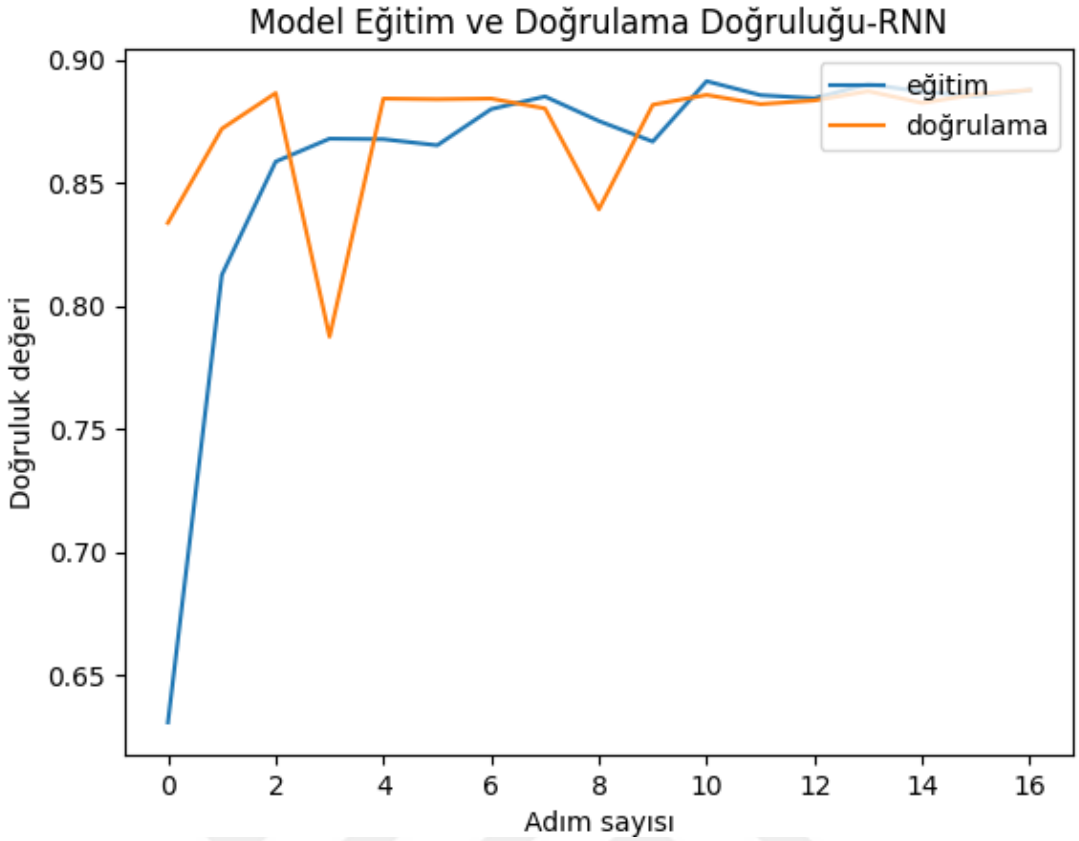
Çizelge 5.24. KEY2023-UKSB için performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 68	% 99	% 80
1	**tcpSYN**	% 90	% 95	% 93
2	**İcmp**	% 94	% 55	% 69
3	**udp**	% 99	% 90	% 95
	Modelin Accuracy (Doğruluğu) %	% 84,67		

UKSB modelinin performans metriklerine göre (Çizelge 5.24), modelin doğruluğu % 84,67 olarak hesaplanmıştır. Kesinlik, duyarlılık ve f1-skoru gibi diğer performans metrikleri, sınıf bazında incelenmiştir. BENIGN sınıfı için, modelin kesinliği %68, duyarlılığı %90 ve f1-skoru %80 olarak hesaplanmıştır. TcpSYN sınıfı için, modelin kesinliği %90, duyarlılığı %95 ve f1-skoru %93 olarak hesaplanmıştır. İcmp sınıfı için, modelin kesinliği %94, duyarlılığı %55 ve f1-skoru %69 olarak hesaplanmıştır. Udp sınıfı için, modelin kesinliği %99, duyarlılığı %90 ve f1-skoru %95 olarak hesaplanmıştır. Bu sonuçlara göre karmaşıklık matrisi de (Şekil 5.41) incelendiğinde, icmp sınıfı için düşük duyarlılık oranı nedeniyle daha düşük bir f1-skoru elde edilmiştir. Udp sınıfı için de oldukça yüksek bir f1-skoru elde edilmiştir.



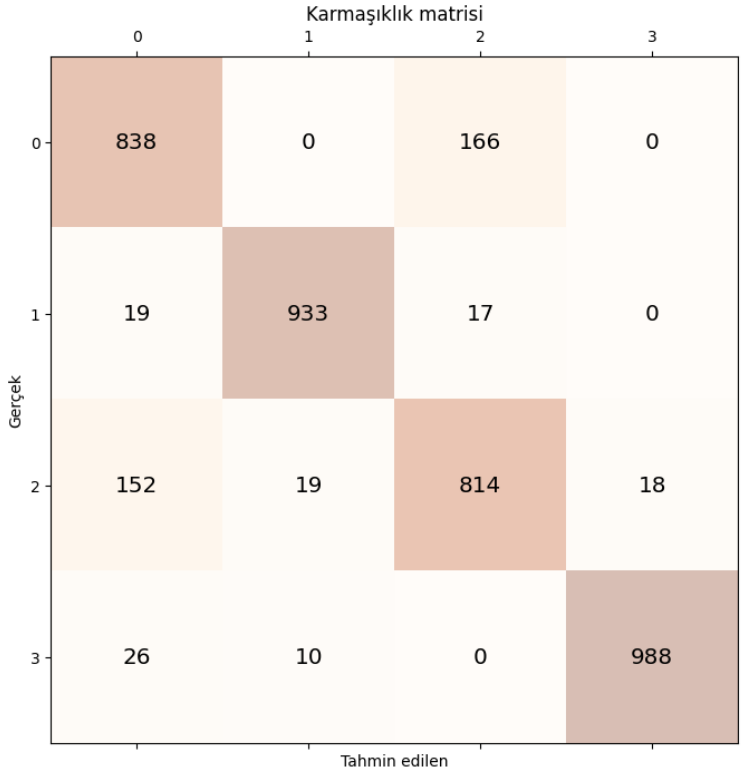
Şekil 5.42. KEY2023-TSA modelinin eğitim ve doğrulama kaybı grafiği



Şekil 5.43. KEY2023-TSA modelinin eğitim ve doğrulama doğruluğu grafiği

TSA modeli için eğitim ve doğrulama kaybı grafiği Şekil 5.42'de verilmiştir. Eğitim ve doğrulama kaybı adım sayısı arttıkça azalmaktadır. Şekil 5.43'te eğitim ve doğrulama doğruluğu grafiği verilmiştir. Bu grafiğe göre de doğrulama doğruluğu adım sayısı arttıkça aynı seviyeye gelmektedir. Sonuç olarak modelin, eğitim verilerine ve test verilerine uygun şekilde uyum sağladığı görülmektedir.

Modele ait karmaşıklık matrisi Şekil 5.44'te verilmiştir. Karmaşıklık matrisi incelendiğinde, icmp sınıfına ait verilerin yanlış sınıflandırılma sayısının diğer sınıflardan daha fazla olduğu görülmektedir. Çizelge 5.25'te verilen performans metriklerine göre, modelin doğruluğu % 89,32 olarak hesaplanmıştır. BENIGN sınıfı için, modelin kesinliği %81, duyarlılığı %83 ve f1-skoru %82 olarak hesaplanmıştır. TcpSYN sınıfı için, modelin kesinliği %97, duyarlılığı %96 ve f1-skoru %97 olarak hesaplanmıştır. İcmp sınıfı için, modelin kesinliği %82, duyarlılığı %81 ve f1-skoru %81 olarak hesaplanmıştır. Udp sınıfı için, modelin kesinliği %98, duyarlılığı %96 ve f1-skoru %97 olarak hesaplanmıştır. Model genel olarak başarılı sonuçlar vermiştir.

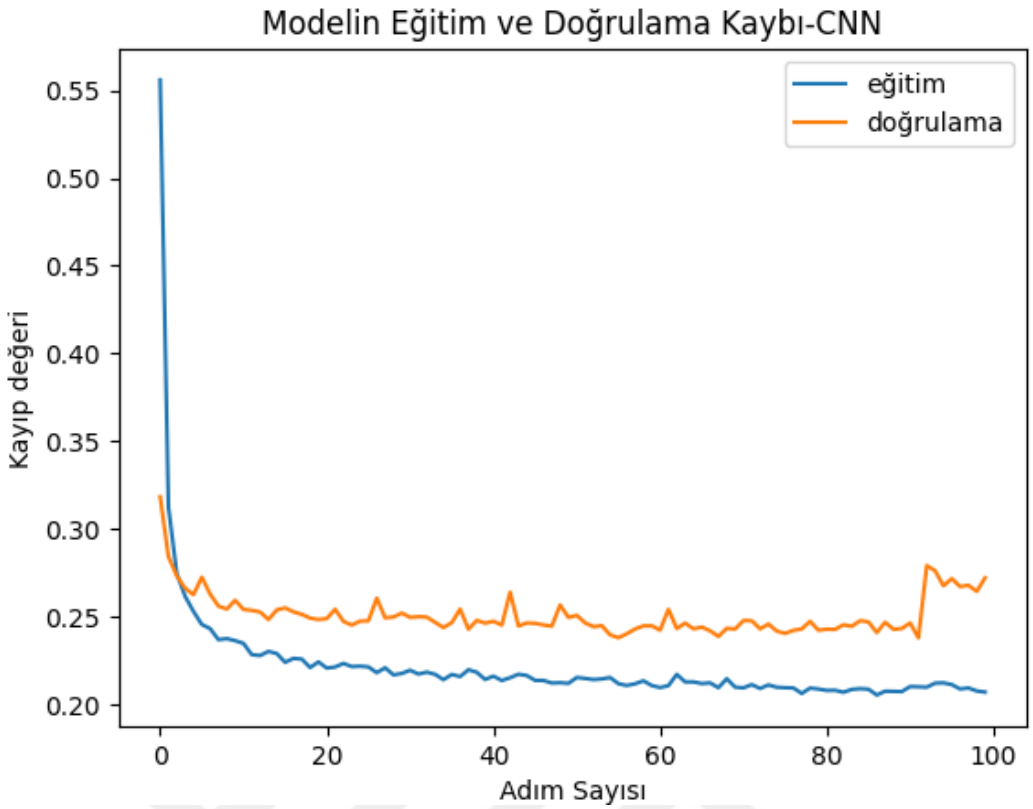


Şekil 5.44. KEY2023-TSA modeli karmaşıklık matrisi

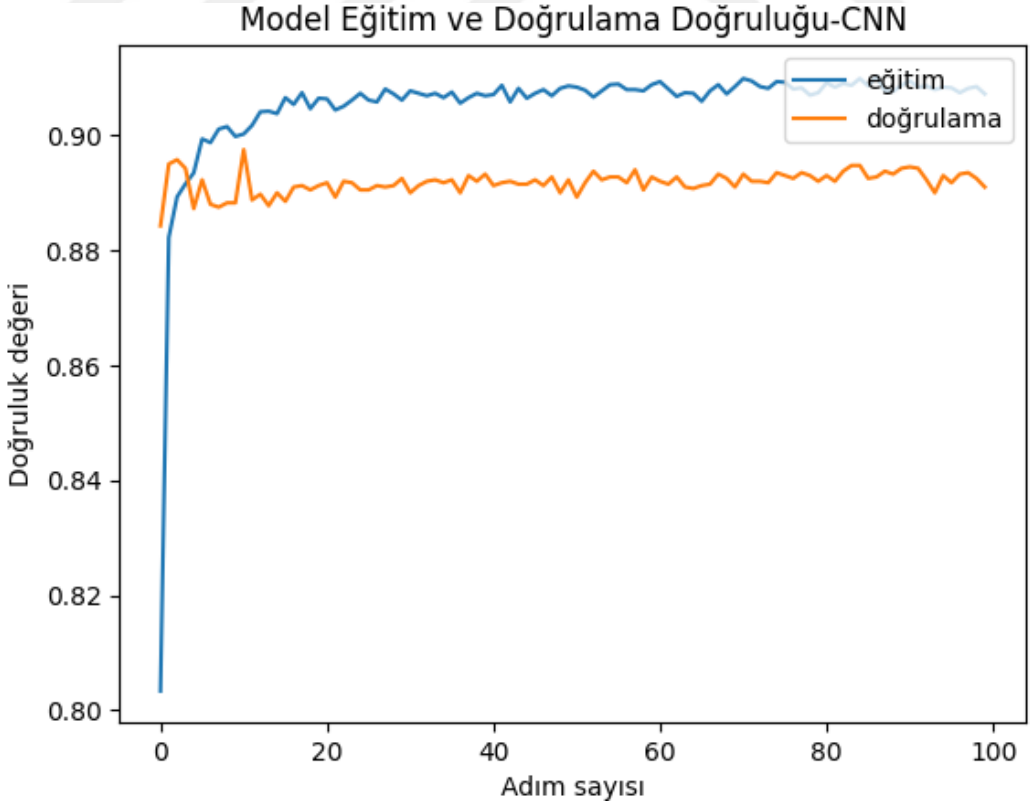
Çizelge 5.25. KEY2023-TSA için performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 81	%83	% 82
1	**tcpSYN**	% 97	% 96	% 97
2	**İcmp**	% 82	% 81	%81
3	**udp**	% 98	% 96	%97
	Modelin Accuracy (Doğruluğu) %	% 89,32		

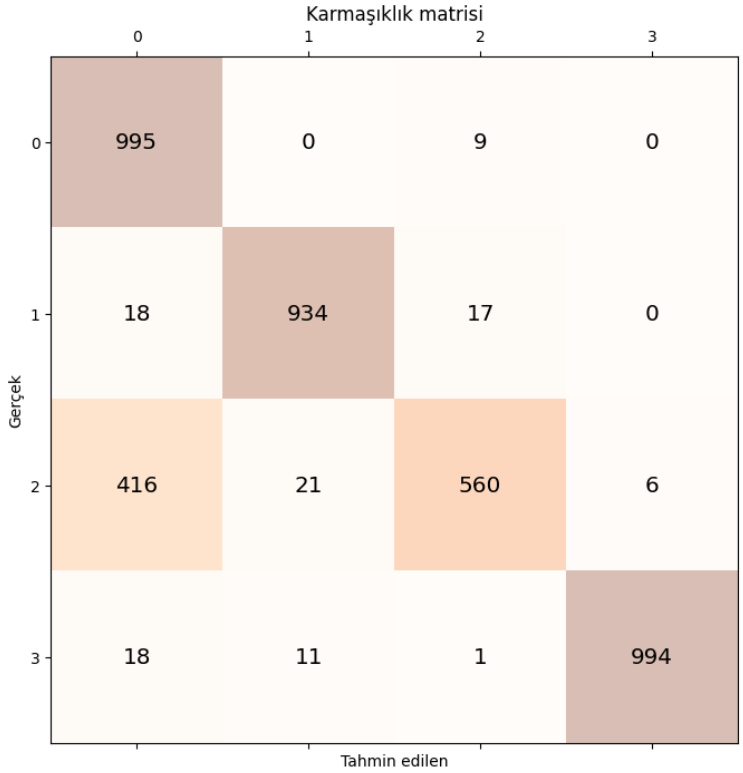
ESA modeline ait eğitim ve doğrulama kaybı grafiği Şekil 5.45'te verilmiştir. Eğitim ve doğrulama değerleri başta yüksek iken adım sayısı arttıkça düşüş göstermektedir. Şekil 5.46'da eğitim ve doğrulama doğruluğu grafiğinde ise doğrulama verileri eğitim verilerinden biraz daha düşük seviyede devam etmiştir. Genel olarak model iyi bir eğitim sürecinden geçmiştir. Şekil 5.47'de modele ait karmaşıklık matrisi verilmiştir. Bu karmaşıklık matrisine göre icmp sınıfı yanlış tahmin sayısı diğer sınıflara göre çok daha fazla olduğu görülmektedir. ESA modeli icmp sınıfını ayırmakta güçlük çekmiştir.



Şekil 5.45. KEY2023-ESA modelinin eğitim ve doğrulama kaybı grafiği



Şekil 5.46. KEY2023-ESA modelinin eğitim ve doğrulama doğruluğu grafiği

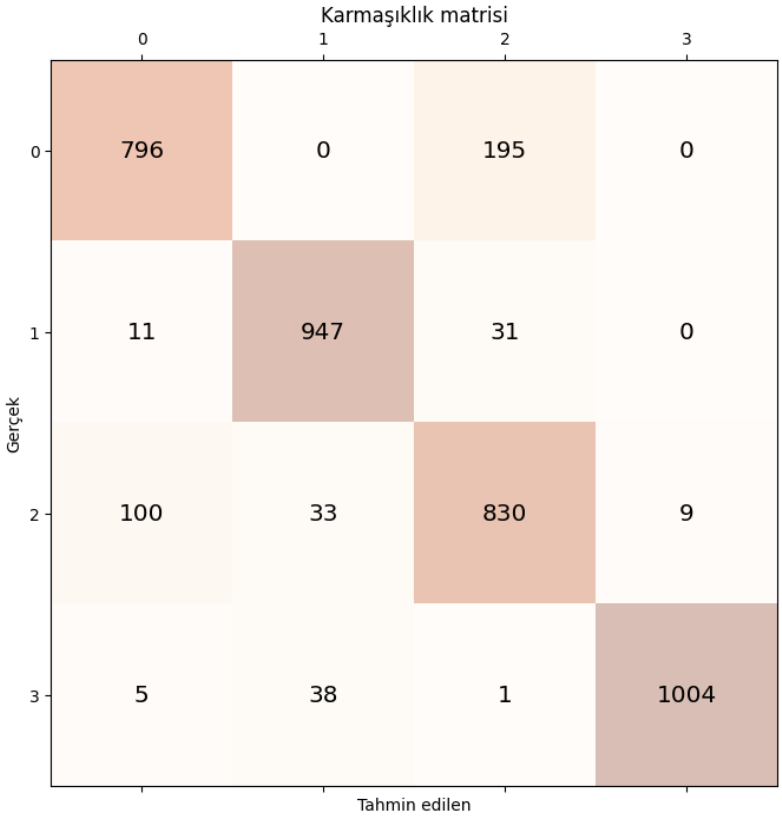


Şekil 5.47. KEY2023-ESA modeli karmaşıklık matrisi

Çizelge 5.26. KEY2023-ESA için performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 69	% 99	% 81
1	**tcpSYN**	% 97	% 96	% 97
2	**İcmp**	% 95	% 56	% 70
3	**udp**	% 99	% 97	% 98
	Modelin Accuracy (Doğruluğu) %	% 87,07		

ESA modeline ait diğer performans metrikleri Çizelge 5.26'da gösterildiği gibi, BENIGN sınıfı için, modelin kesinliği %69, duyarlılığı %99 ve f1-skoru %81 olarak hesaplanmıştır. TcpSYN sınıfı için, modelin kesinliği %97, duyarlılığı %96 ve f1-skoru %97 olarak hesaplanmıştır. İcmp sınıfı için, modelin kesinliği %95, duyarlılığı %56 ve f1-skoru %70 olarak hesaplanmıştır. Udp sınıfı için, modelin kesinliği %99, duyarlılığı %97 ve f1-skoru %98 olarak hesaplanmıştır. Modelin doğruluğu % 87,07 olarak hesaplanmıştır ve model genel olarak başarılı sonuçlar vermiştir.



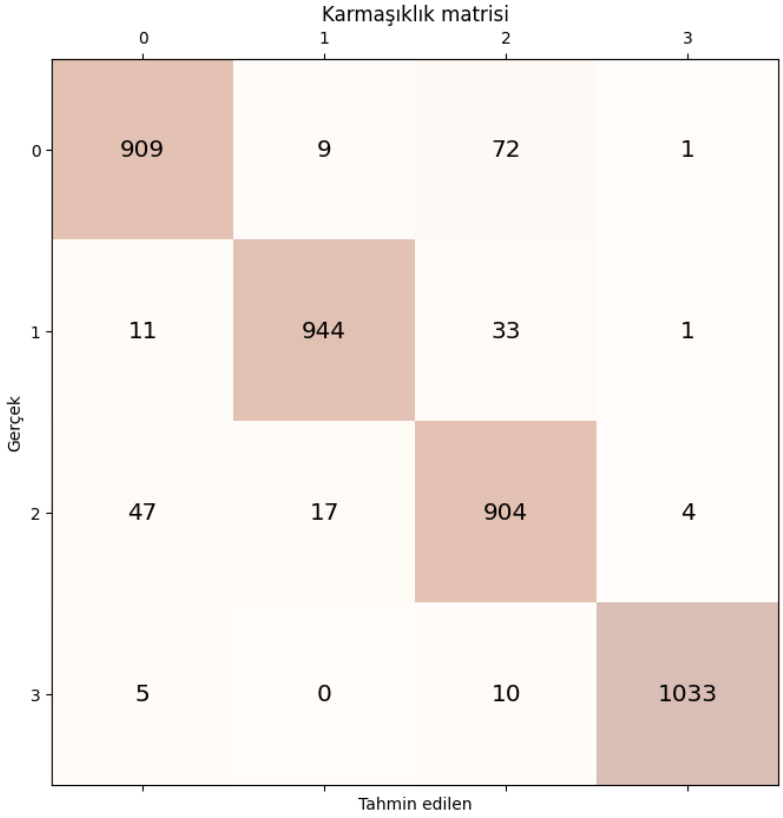
Şekil 5.48. KEY2023-LR karmaşıklık matrisi

Çizelge 5.27. KEY2023-LR için performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 87	%80	% 84
1	**tcpSYN**	% 93	% 96	% 94
2	**İcmp**	% 79	% 85	%82
3	**udp**	% 99	% 96	%97
	Modelin Accuracy (Doğruluğu) %	% 89,42		

LR modelinin performans metriklerine (Çizelge 5.27) göre, tcpSYN ve udp sınıfları için modelin performansı oldukça yüksek bir kesinlik, duyarlılık ve f1-skoru ile ölçülmüştür. Ancak BENIGN ve icmp sınıfları için kesinlik, duyarlılık ve f1-skoru biraz daha düşüktür. BENIGN sınıfı için modelin kesinliği %87, duyarlılığı %80 ve f1-skoru %84 olarak hesaplanmıştır. İcmp sınıfı için modelin kesinliği %79, duyarlılığı %85 ve f1-skoru %82 olarak hesaplanmıştır. TSA modelinin performansına kıyasla, LR modelinin performansı daha yüksek doğruluk oranı değeri göstermektedir. Ancak, her iki modelin de sınıf bazında performanslarının farklı olduğu görülmektedir. LR modelinin karmaşıklık matrisi (Şekil 5.48) incelendiğinde, doğru sınıflandırılan örneklerin sayısı

oldukça yüksektir. Ancak, İcmp sınıfı ve BENIGN sınıfı için yapılan tahminlerin bir kısmı hatalıdır. Bununla birlikte, tcpSYN ve udp sınıfları için oldukça az hatalı tahmin yapılmıştır.



Şekil 5.49. KEY2023-RO karmaşıklık matrisi

Çizelge 5.28. KEY2023-RO için performans metrikleri

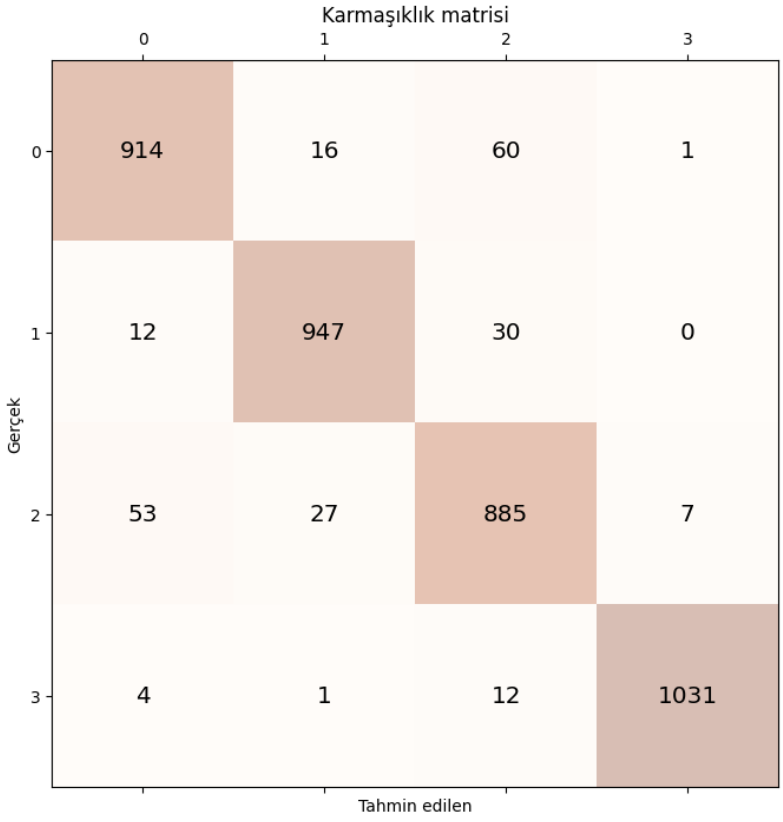
Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 94	% 92	% 93
1	**tcpSYN**	% 97	%95	% 96
2	**İcmp**	% 89	% 93	% 91
3	**udp**	% 99	% 99	% 99
	Modelin Accuracy (Doğruluğu) %	% 94,75		

RO modelinin performansı Çizelge 5.28 incelendiğinde oldukça yüksek olduğu görülmektedir. BENIGN sınıfı için modelin kesinliği %94, duyarlılığı %92 ve f1-skoru %93 olarak, tcpSYN sınıfı için modelin kesinliği %97, duyarlılığı %95 ve f1-skoru %96 olarak, icmp sınıfı için modelin kesinliği %89, duyarlılığı %93 ve f1-skoru %91 olarak, udp sınıfı için modelin kesinliği %99, duyarlılığı %99 ve f1-skoru %99 olarak

hesaplanmıştır. Ayrıca, modelin doğruluğu %94,75 olarak hesaplanmıştır, bu da modelin tüm sınıfların sınıflandırılmasında oldukça başarılı olduğunu göstermektedir.

Karmaşıklık matrisi incelendiğinde (Şekil 5.49), BENIGN ve icmp sınıflarında hatalı sınıflandırmanın diğer sınıflara göre biraz daha fazla olduğu görülmektedir. Fakat genel olarak RO modeli için, her sınıf yüksek kesinlik, duyarlılık ve f1-skor değerleri elde edilmiştir. Bu durum, modelin her sınıfı doğru bir şekilde sınıflandırabildiğini göstermektedir.

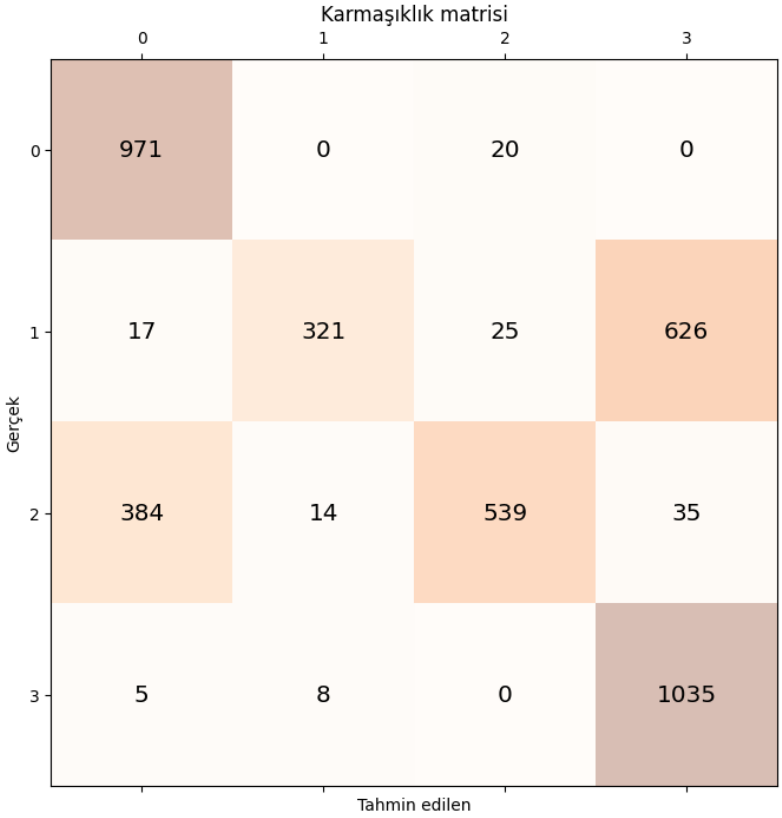
KA modelinin performans metrikleri Çizelge 5.29 incelendiğinde yüksek olarak hesaplandığı görülmektedir. Tüm sınıflar için yüksek kesinlik, duyarlılık ve f1-skorları elde edilmiştir. BENIGN sınıfında %93, tcpSYN sınıfında %96, icmp sınıfında %90 ve udp sınıfında %99 kesinlik elde edilmiştir. Duyarlılık değerleri ise BENIGN sınıfında %92, tcpSYN sınıfında %96, icmp sınıfında %91 ve udp sınıfında %98 olarak hesaplanmıştır. Ayrıca, modelin doğruluğu %94,42 olarak hesaplanmıştır. Karmaşıklık matrisi (Şekil 5.50) incelendiğinde de modelin tüm sınıflarda yüksek performans gösterdiği görülmektedir. Bu sonuçlar, KA modelinin bu veri setinde iyi bir sınıflandırma performansı sergilediğini göstermektedir.



Şekil 5.50. KEY2023-KA karmaşıklık matrisi

Çizelge 5.29. KEY2023-KA için performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 93	%92	% 93
1	**TcpSYN**	% 96	%96	% 96
2	**İcmp**	% 90	%91	% 90
3	**udp**	% 99	%98	% 99
	Modelin Accuracy (Doğruluğu) %	% 94,42		



Şekil 5.51. KEY2023-NB karmaşıklık matrisi

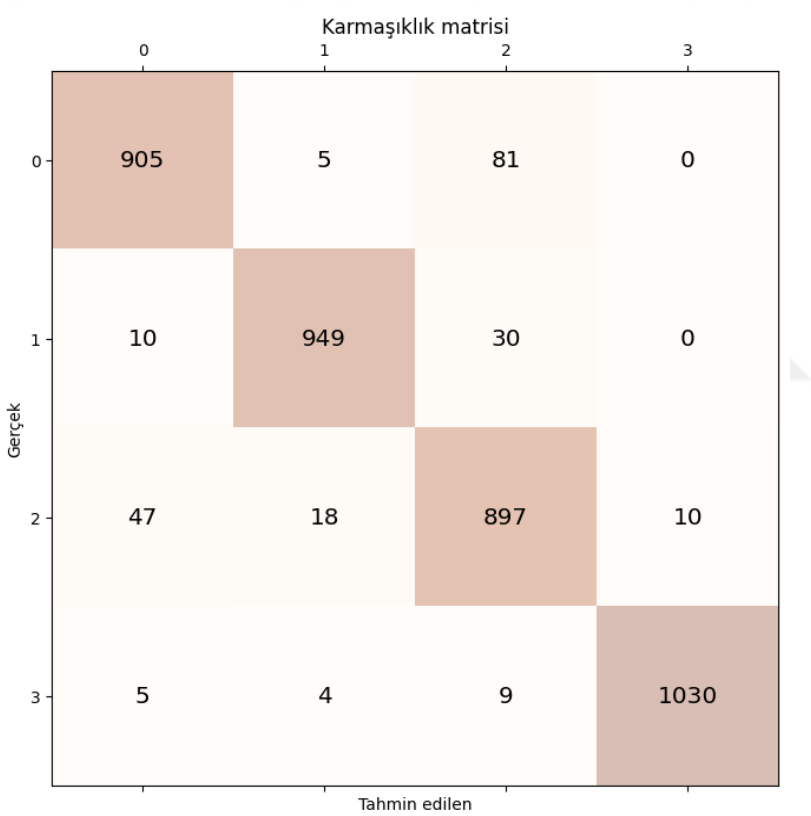
Çizelge 5.30. KEY2023-NB için performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 71	% 98	% 82
1	**TcpSYN**	% 94	% 32	% 48
2	**İcmp**	% 92	% 55	% 69
3	**udp**	% 61	% 99	% 75
	Modelin Accuracy (Doğruluğu) %	% 71,65		

NB modeli performans metrikleri (Çizelge 5.30) incelendiğinde, diğer modellerden daha düşük performansa sahip olduğu görülmektedir. Özellikle tcpSYN sınıfı için düşük duyarlılık oranı %32 ve f1-skoru oranı % 48 dikkat çekicidir. Ancak,

karmaşıklık matrisinde (Şekil 5.51) de görüldüğü gibi, modelin hatalı sınıflandırma yapma oranı oldukça yüksektir. Özellikle tcpSYN ve icmp sınıflarını sınıflandırmada yetersiz kalmıştır.

KEYK modelinin doğruluğu % 94.52 oranında oldukça yüksektir ve performans metrikleri (Çizelge 5.31) de genel olarak yüksek değerlere sahiptir. KEYK modelinde, udp sınıfını %99 kesinlik, %98 duyarlılık ve %99 f1-Skor oranıyla daha iyi tahmin edebilirken, icmp sınıfını daha düşük oranda tahmin edebilmiştir. KEYK modeli, tcpSYN ve udp sınıfları için yüksek F1-Skor değerleri vermektedir. Karmaşıklık matrisi (Şekil 5.52) incelendiğinde KEYK modeli, icmp sınıfını diğer sınıflara göre sınıflandırmada başarısı düşüktür.



Şekil 5.52. KEY2023-KEYK karmaşıklık matrisi

Çizelge 5.31. KEY2023-KEYK için performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	% 94	% 91	% 92
1	**TcpSYN**	% 97	% 96	% 97
2	**İcmp**	% 88	% 92	% 90
3	**udp**	% 99	% 98	% 99
	Modelin Accuracy (Doğruluğu) %	% 94,52		

KEY2023 veri setinde modellerin eğitim zamanları kıyaslandığında Çizelge 5.32'de gösterildiği gibi en hızlı KEYK modeli, en yavaş UKSB modeli olarak tespit edilmiştir.

Çizelge 5.32. KEY2023 veri seti modellerin çoklu sınıflandırma eğitim zamanları

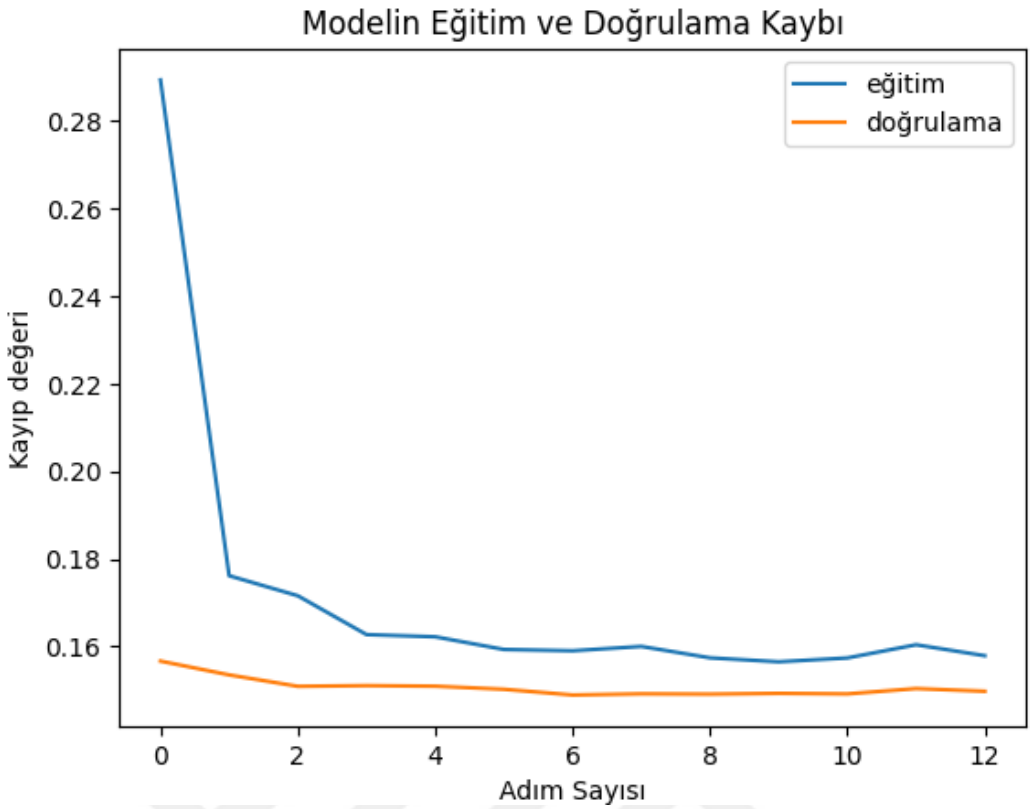
Model	*Zaman(ms)*
YSA	16395
UKSB	733216
TSA	111197
ESA	44109
LR	325
RO	185
KA	114
NB	8
KEYK	2

5.3.2. İkili sınıflandırma sonuçları

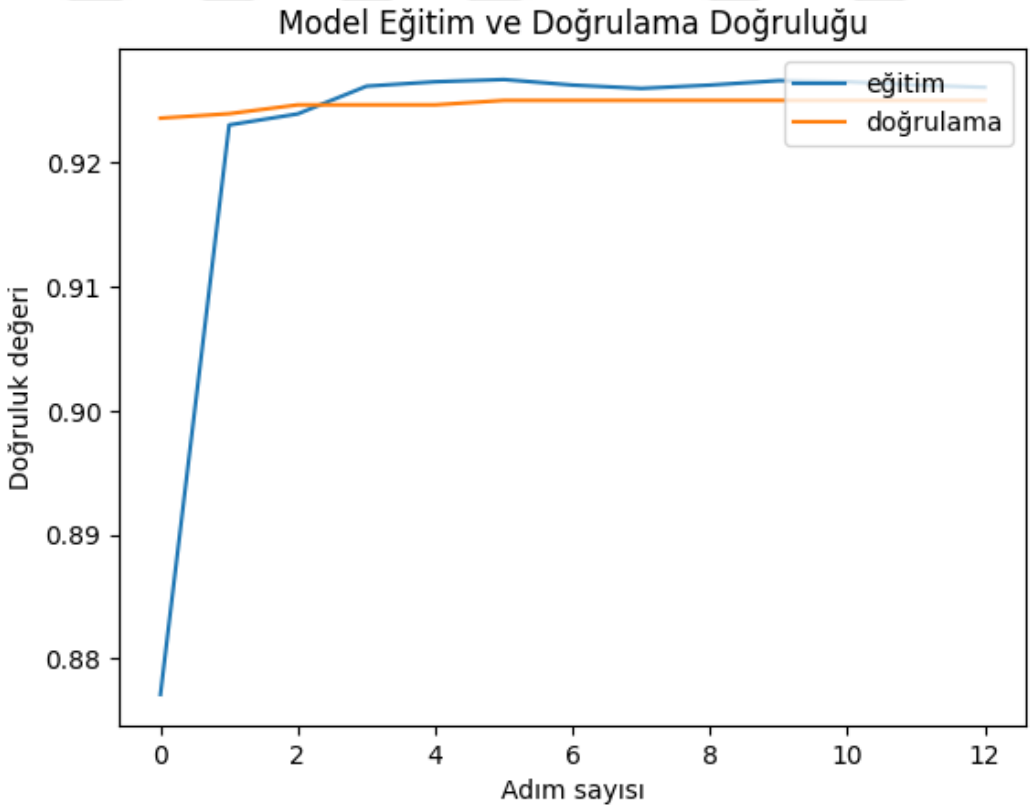
KEY2013 veri setine uygulanan YSA modelinin eğitim ve doğrulama kaybı grafiğinde (Şekil 5.53), eğrilerin adım sayısı arttıkça düştüğü görülmektedir, bu da modelin eğitim verilerine ve test verilerine uygun şekilde uyum sağladığını göstermektedir.

YSA modelinin doğrulama doğruluğu grafiği (Şekil 5.54) incelendiğinde, doğrulama doğruluğunun da benzer şekilde, eğitim adımlarının artmasıyla birlikte artmaktadır, ancak eğitim doğruluğuna kıyasla daha yavaş bir artış oranı göstermektedir. Bu durum, modelin eğitim verilerine overfitting eğilimi göstermediğini göstermektedir.

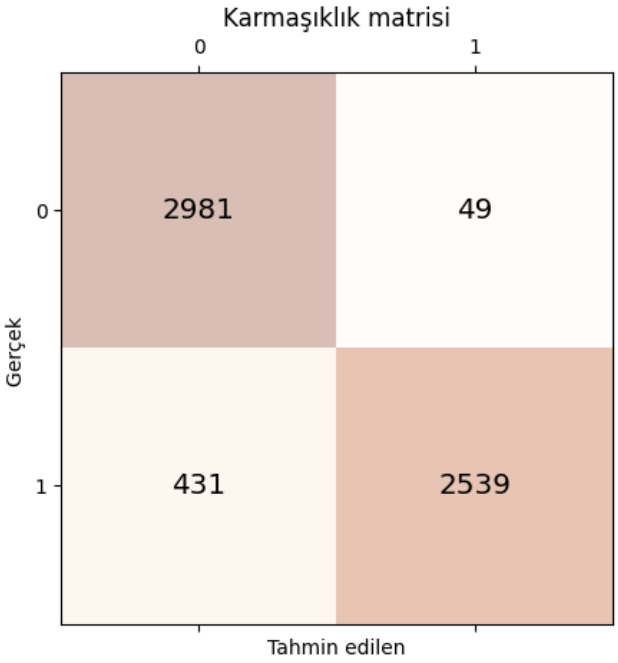
Sonuç olarak, eğitim ve doğrulama doğruluğu değerlerinin yüksek olduğu ve benzer bir şekilde arttığı görülmektedir. Bu, modelin ikili sınıflandırmada iyi bir performans sergilediğini göstermektedir.



Şekil 5.53. KEY2023- YSA modeli ikili sınıflandırma eğitim ve doğrulama kaybı grafiği



Şekil 5.54. KEY2023-YSA modeli ikili sınıflandırma eğitim ve doğrulama doğruluğu grafiği



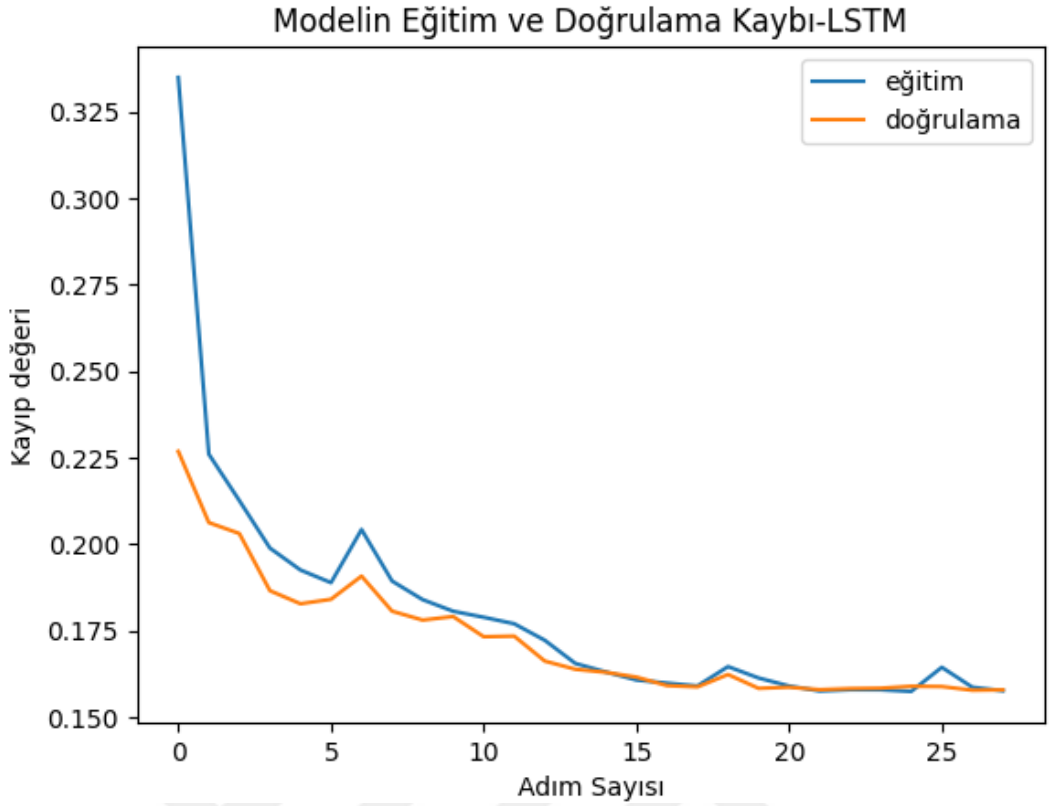
Şekil 5.55. KEY2023-YSA modeli ikili sınıflandırma karmaşıklık matrisi

Çizelge 5.33. KEY2023-YSA ikili sınıflandırma performans metrikleri

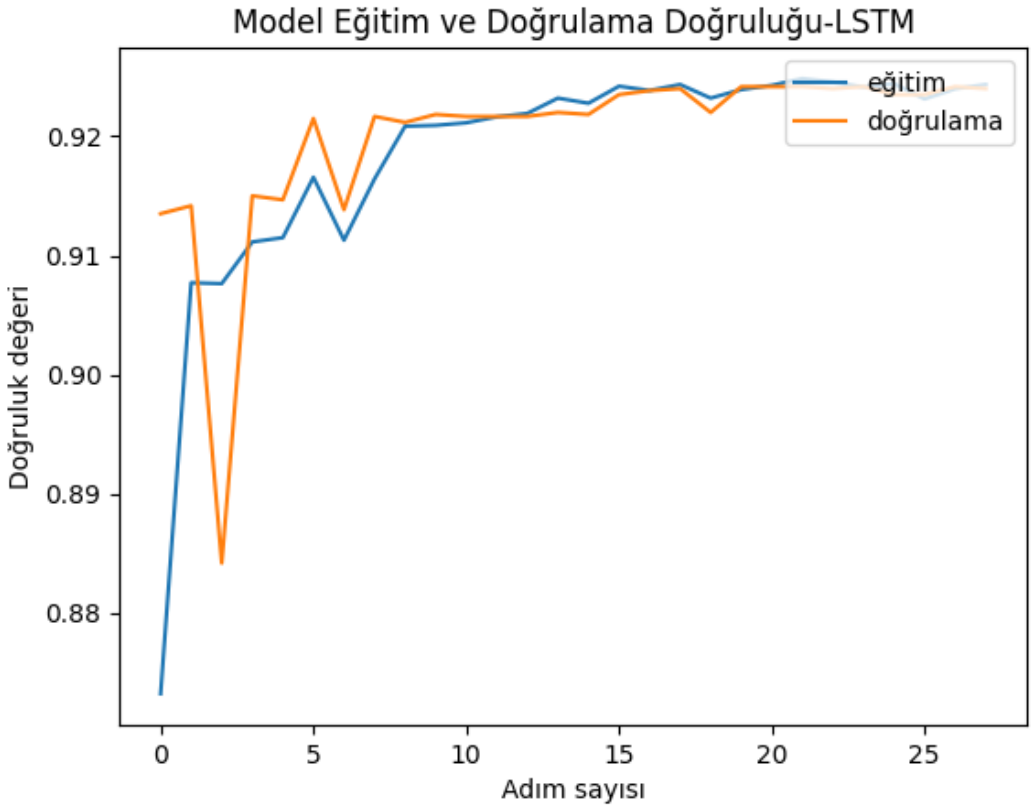
Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	%87	%98	%93
1	**Attack**	%98	%85	%91
	Modelin Accuracy (Doğruluğu) %	%92,26		

YSA modelinin performans metrikleri ikili sınıflandırmada (Çizelge 5.33) incelendiğinde, modelin doğruluğu %92,26 olarak ölçülmüştür, yani modelin doğru sınıflandırma oranı oldukça yüksektir.

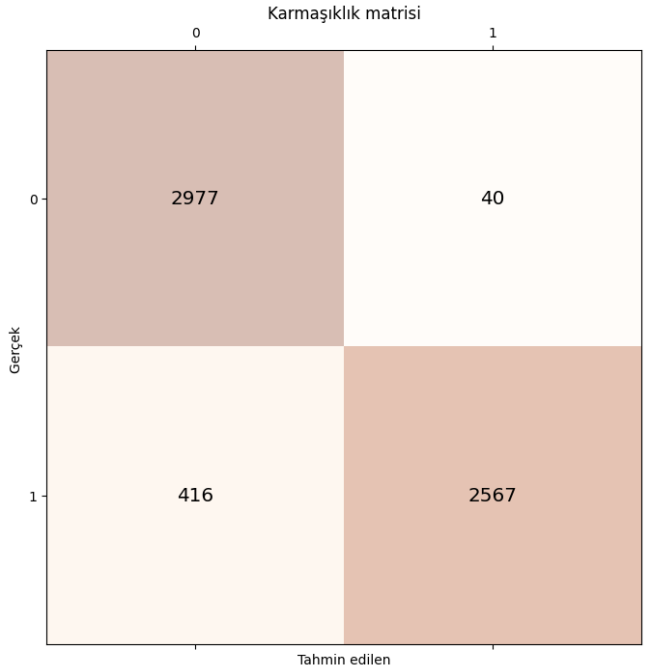
Kesinlik ve duyarlılık metriklerine baktığımızda, BENIGN sınıfı için kesinlik %87, duyarlılık %98 ve f1-Skor %93 olarak ölçülmüştür. Attack sınıfı için ise kesinlik %98, duyarlılık %85 ve f1-Skor %91 olarak ölçülmüştür. Bu sonuçlar, modelin BENIGN sınıfını oldukça iyi bir şekilde sınıflandırdığını, ancak Attack sınıfını biraz daha zorlandığını göstermektedir. Karmaşıklık matrisi (Şekil 5.55) incelendiğinde, Attack sınıfının yanlış tahmin sayısının fazla olduğu görülmektedir.



Şekil 5.56. KEY2023-UKSB modelinin ikili sınıflandırma eğitim ve doğrulama kaybı grafiği



Şekil 5.57. KEY2023-UKSB modelinin ikili sınıflandırma eğitim ve doğrulama doğruluğu grafiği

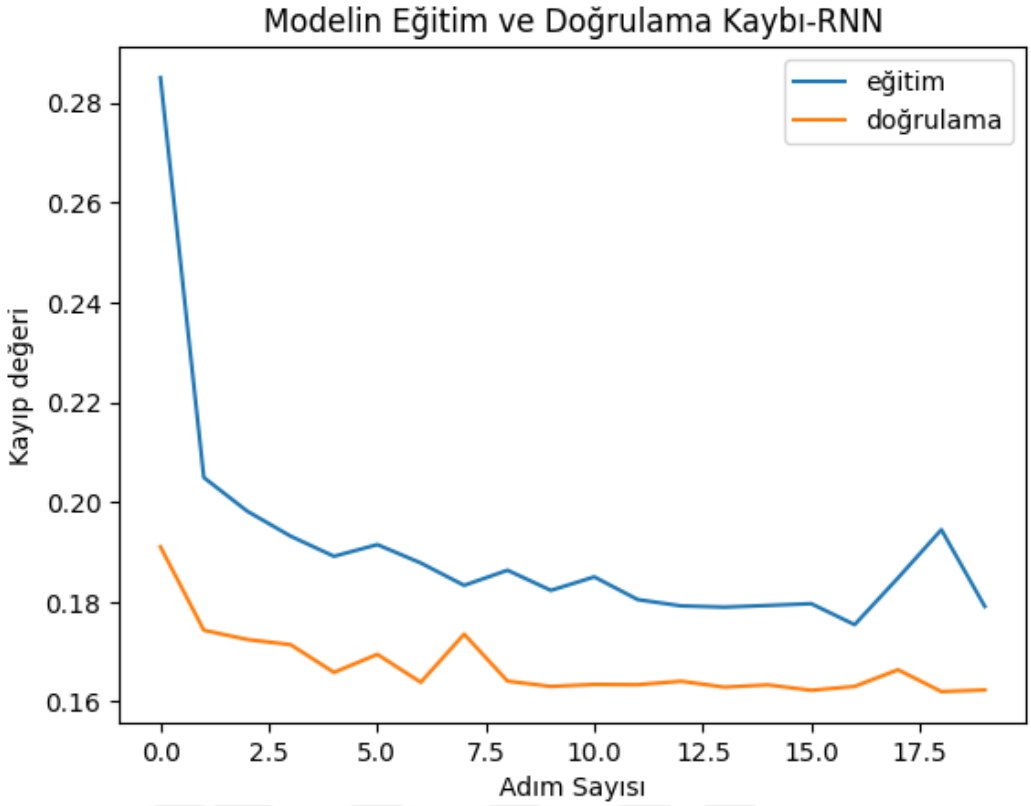


Şekil 5.58. KEY2023-UKSB modeli ikili sınıflandırma karmaşıklık matrisi

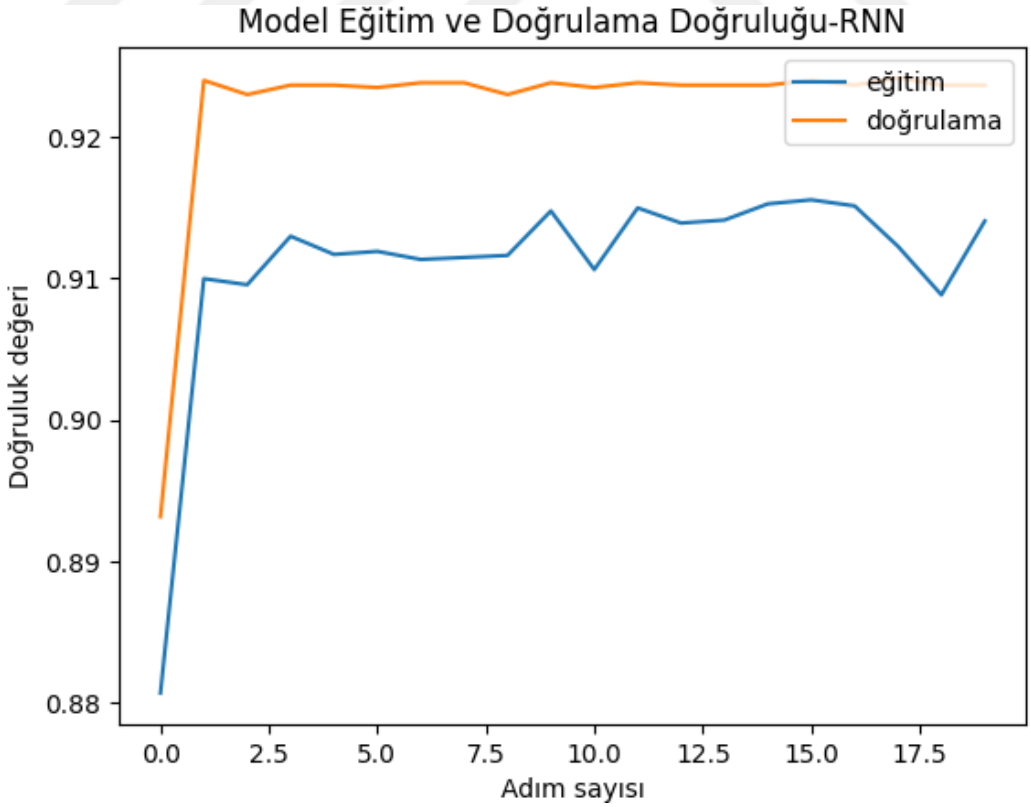
Çizelge 5.34. KEY2023-UKSB modeli ikili sınıflandırma performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	%88	%99	%93
1	**Attack**	%98	%86	%92
	Modelin Accuracy (Doğruluğu) %	%92,40		

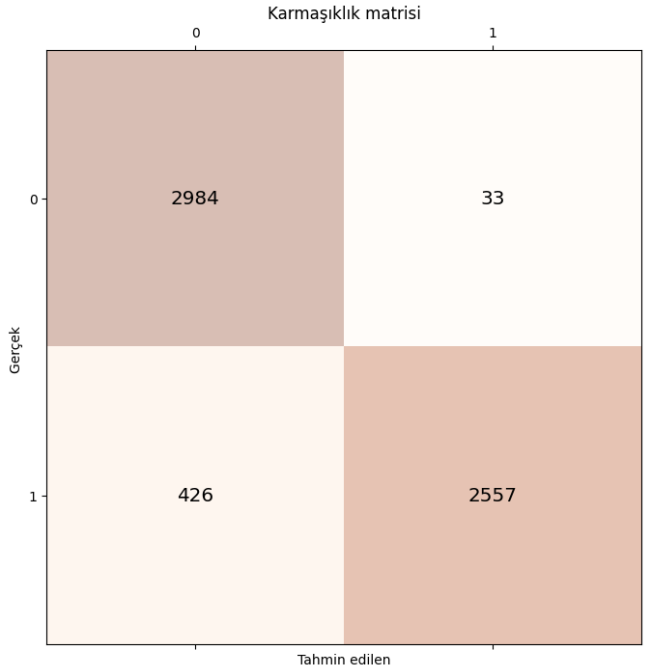
UKSB modelinin eğitim ve doğrulama kaybı grafiğinde (Şekil 5.56), eğrilerin adım sayısı arttıkça düştüğü görülmektedir, bu da modelin eğitim verilerine ve test verilerine uygun şekilde uyum sağladığını göstermektedir. UKSB modelinin doğrulama doğruluğu grafiği (Şekil 5.57) incelendiğinde, doğrulama doğruluğunun da benzer şekilde, eğitim adımlarının artmasıyla birlikte artmaktadır. Bu durum, modelin eğitim verilerine overfitting eğilimi göstermediğini göstermektedir. Şekil 5.58'de verilen karmaşıklık matrisinde Attack sınıfına ait verilerin BENIGN sınıfı olarak sınıflandırılma sayısının fazla olduğu görülmektedir. Çizelge 5.34'te verilen performans metriklerine göre, model %92,40 oranında başarı elde etmiştir. Modele ait kesinlik, duyarlılık ve f1-skor değerleri her iki sınıf için de oldukça iyi değerdedir. Model ikili sınıflandırmada çoklu sınıflandırmaya göre daha başarılı sonuçlar elde etmiştir.



Şekil 5.59. KEY2023-TSA modelinin ikili sınıflandırma eğitim ve doğrulama kaybı grafiği



Şekil 5.60. KEY2023-TSA modelinin ikili sınıflandırma eğitim ve doğrulama doğruluğu grafiği

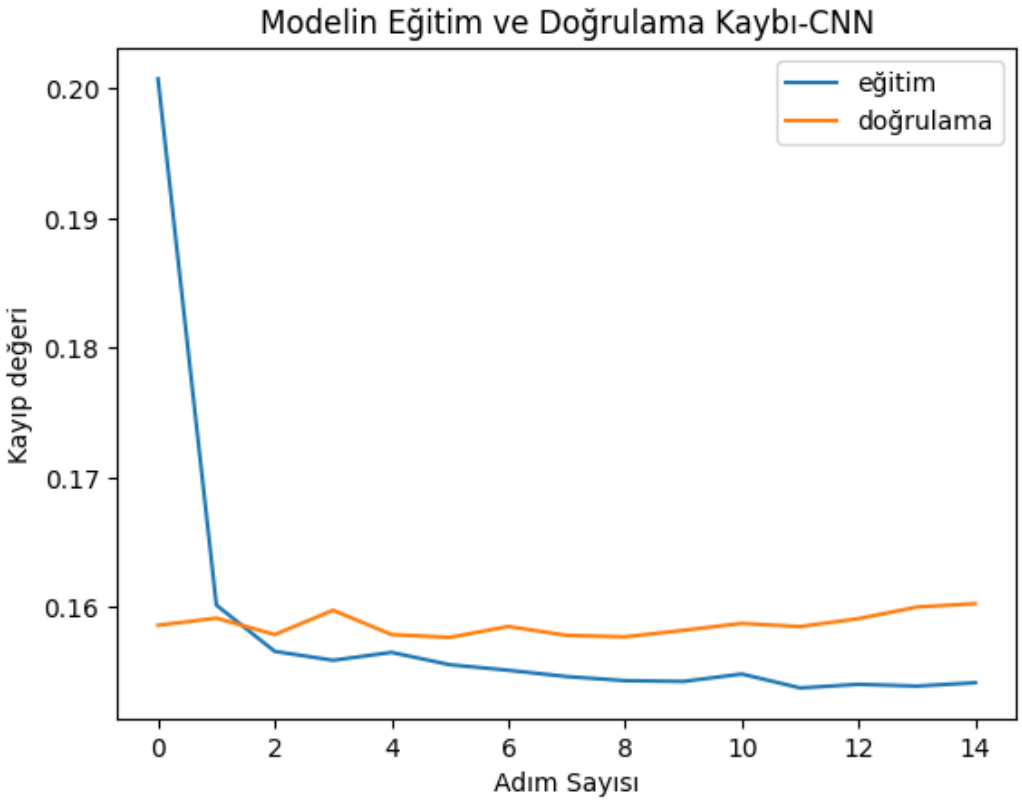


Şekil 5.61. KEY2023-TSA modeli ikili sınıflandırma karmaşıklık matrisi

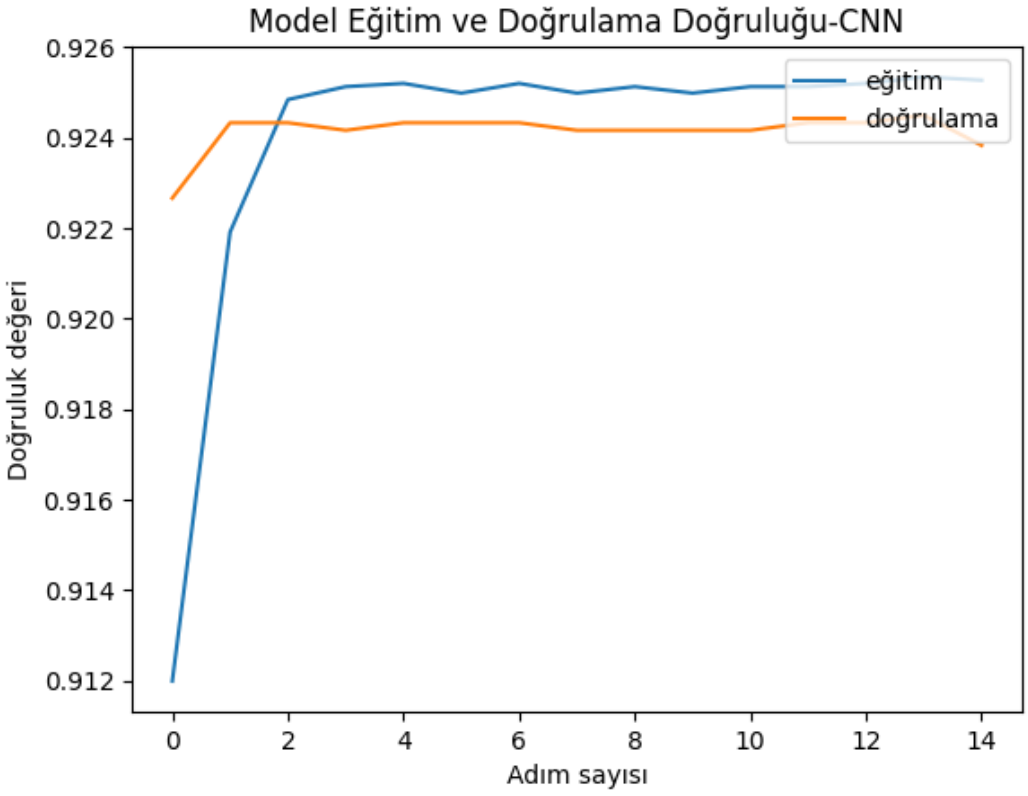
Çizelge 5.35. KEY2023-TSA modeli ikili sınıflandırma performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	%88	%99	%93
1	**Attack**	%99	%86	%92
	Modelin Accuracy (Doğruluğu) %	%92,35		

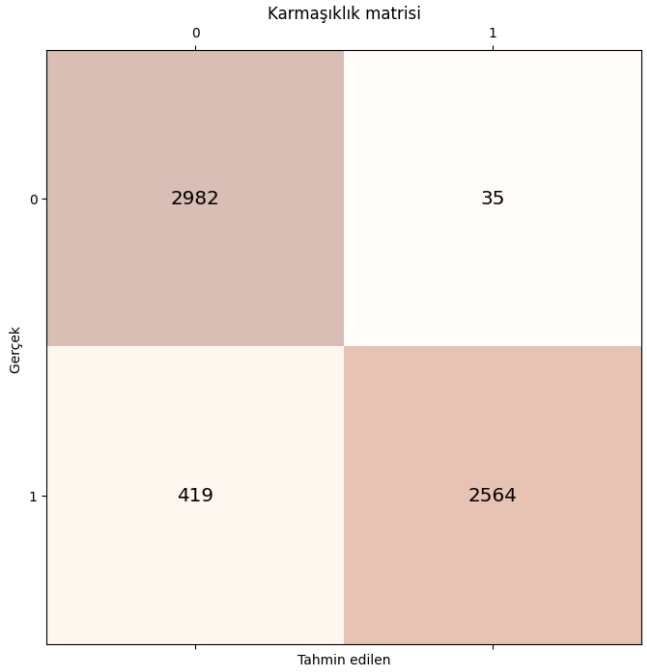
TSA modelinin eğitim ve doğrulama kaybı grafiğinde (Şekil 5.59), eğrilerin adım sayısı arttıkça düştüğü görülmektedir. TSA modelinin doğrulama doğruluğu grafiği (Şekil 5.60) incelendiğinde, doğrulama doğruluğunun da benzer şekilde, eğitim adımlarının artmasıyla birlikte artmaktadır. Fakat doğrulama verilerindeki artış eğitim verilerinden daha fazladır. Şekil 5.61'de verilen karmaşıklık matrisinde Attack sınıfına ait verilerin BENIGN sınıfı olarak sınıflandırılma sayısının fazla olduğu görülmektedir. Çizelge 5.35'te verilen performans metriklerine göre, model %92,35 oranında başarı elde etmiştir. Modele ait kesinlik, duyarlılık ve f1-skor değerleri her iki sınıf için de oldukça iyi değerdedir. Fakat Attack sınıfına ait duyarlılık değeri diğer değerlerden düşük çıkmıştır. Model ikili sınıflandırmada çoklu sınıflandırmaya göre daha başarılı sonuçlar elde etmiştir.



Şekil 5.62. KEY2023-ESA modelinin ikili sınıflandırma eğitim ve doğrulama kaybı grafiği



Şekil 5.63. KEY2023-ESA modelinin ikili sınıflandırma eğitim ve doğrulama doğruluğu grafiği



Şekil 5.64. KEY2023-ESA modeli ikili sınıflandırma karmaşıklık matrisi

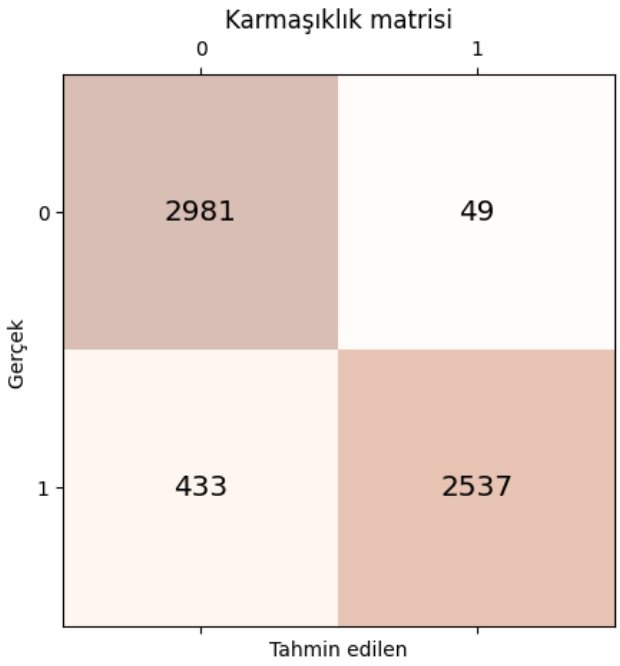
Çizelge 5.36. KEY2023-ESA modeli ikili sınıflandırma performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	%88	%99	%93
1	**Attack**	%99	%86	%92
	Modelin Accuracy (Doğruluğu) %	%92,43		

ESA modelinin eğitim ve doğrulama kaybı grafiğinde (Şekil 5.62), eğrilerin adım sayısı arttıkça düştüğü görülmektedir. ESA modelinin doğrulama doğruluğu grafiği (Şekil 5.63) incelendiğinde, doğrulama doğruluğunun da benzer şekilde, eğitim adımlarının artmasıyla birlikte artmaktadır. Fakat doğrulama verilerindeki artış eğitim verilerinden daha fazladır. Şekil 5.64'te verilen karmaşıklık matrisinde Attack sınıfına ait verilerin BENIGN sınıfı olarak sınıflandırılma sayısının fazla olduğu görülmektedir. Çizelge 5.36'da verilen performans metriklerine göre, model %92,43 oranında başarı elde etmiştir. Modele ait kesinlik, duyarlılık ve f1-skor değerleri her iki sınıf için de oldukça iyi değerdedir. Fakat Attack sınıfına ait duyarlılık değeri diğer değerlerden düşük çıkmıştır. Model ikili sınıflandırmada çoklu sınıflandırmaya göre daha başarılı sonuçlar elde etmiştir.

LR modelinin performans metriklerine (Çizelge 5.37) bakıldığında, doğruluğu %91,96 olarak ölçülmüştür, yani modelin doğru sınıflandırma oranı yine oldukça yüksek seviyededir.

Kesinlik, duyarlılık ve f1-Skor metriklerine baktığımızda, BENIGN sınıfı için kesinlik %87, duyarlılık %98 ve f1-Skor %93 oranında, Attack sınıfı için ise kesinlik %98, duyarlılık %85 ve f1-Skor %91 oranında hesaplanmıştır. Bu sonuçlar, LR modelinin de BENIGN sınıfını oldukça iyi bir şekilde sınıflandırdığını ve Attack sınıfını sınıflandırmada biraz daha zorlandığını göstermektedir. Şekil 5.65'te karmaşıklık matrisinde Attack sınıfında yanlış tahminler olduğu görülmektedir.



Şekil 5.65. KEY2023-LR modeli ikili sınıflandırma karmaşıklık matrisi

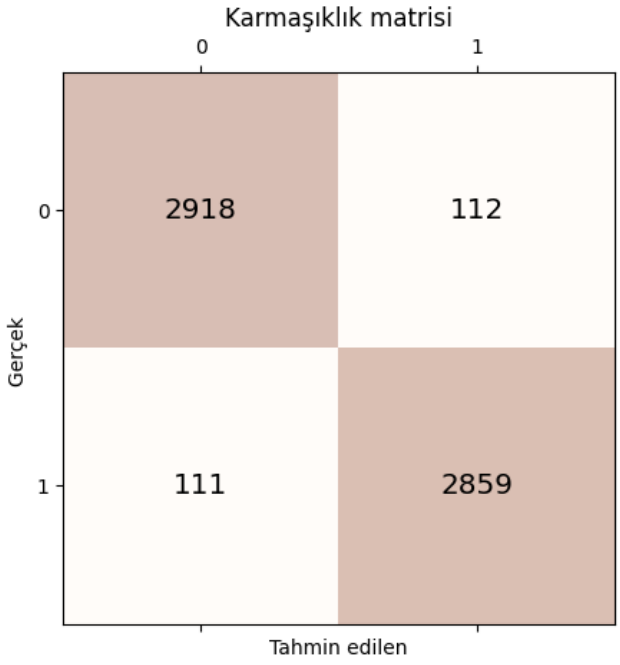
Çizelge 5.37. KEY2023-LR ikili sınıflandırma performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	%87	%98	%93
1	**Attack**	%98	%85	%91
	Modelin Accuracy (Doğruluğu) %	%91.96		

RO modelinin performans metriklerine (Çizelge 5.38) göre, modelin doğruluğu %96,28 olarak hesaplanmıştır, bu da modelin doğru sınıflandırma oranı oldukça yüksek olduğunu göstermektedir.

Kesinlik, duyarlılık ve f1-Skor metriklerine baktığımızda, BENIGN sınıfı için kesinlik %96, duyarlılık %96 ve f1-Skor %96 oranında, Attack sınıfı için ise kesinlik %96, duyarlılık %96 ve f1-Skor %96 oranında hesaplanmıştır. Bu sonuçlar, RO modelinin BENIGN ve Attack sınıflarını eşit derecede iyi bir şekilde sınıflandırdığını göstermektedir.

RO modelinin ikili sınıflandırma için karmaşıklık matrisine (Şekil 5.66) bakıldığında, BENIGN ve Attack sınıflarından da eşit sayıda doğru ve yanlış sınıflandırma yaptığı görülmektedir.



Şekil 5.66. KEY2023-RO modeli ikili sınıflandırma karmaşıklık matrisi

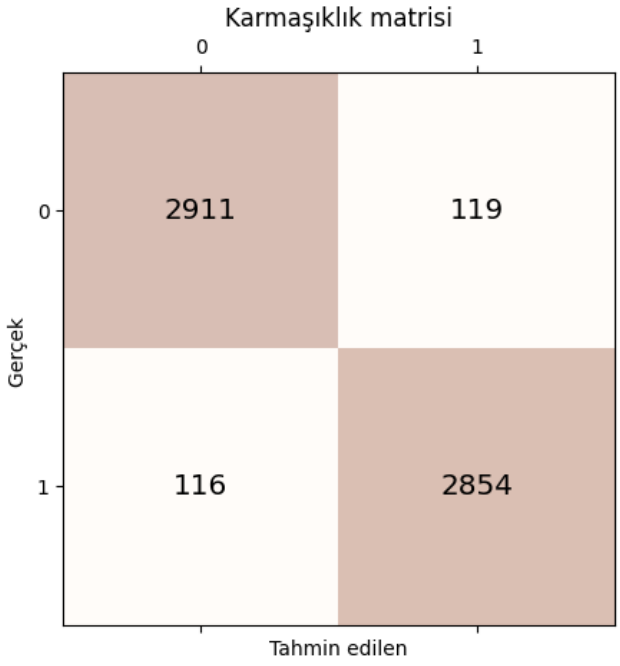
Çizelge 5.38. RO ikili sınıflandırma performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	%96	%96	%96
1	**Attack**	%96	%96	%96
	Modelin Accuracy (Doğruluğu) %	%96,28		

KA modelinin performans metrikleri (Çizelge 5.39) incelendiğinde, sınıflandırma performansı oldukça yüksek bir doğruluk oranı elde etmiştir %96,08. Modelin BENIGN ve Attack sınıflarında da %96'lık bir kesinlik, duyarlılık ve F1-skoru başarısı göstermesi, modelin iyi bir performans sergilediğini göstermektedir. Bu, modelin toplam

sınıflandırma kararlarının %96,08'inin doğru olduğu anlamına gelmektedir. Ayrıca, BENIGN sınıfı için modelin %96 kesinlik, %96 duyarlılık ve %96 f1-Skor başarısı gösterdiği, aynı şekilde Attack sınıfı için de %96 kesinlik, %96 duyarlılık ve %96 f1-Skor başarısı gösterdiği anlamına gelir.

KA modelinin karmaşıklık matrisinde (Şekil 5.67) de, BENIGN ve Attack sınıflarının eşit oranda doğru ve yanlış sınıflandırıldığı görülmektedir.



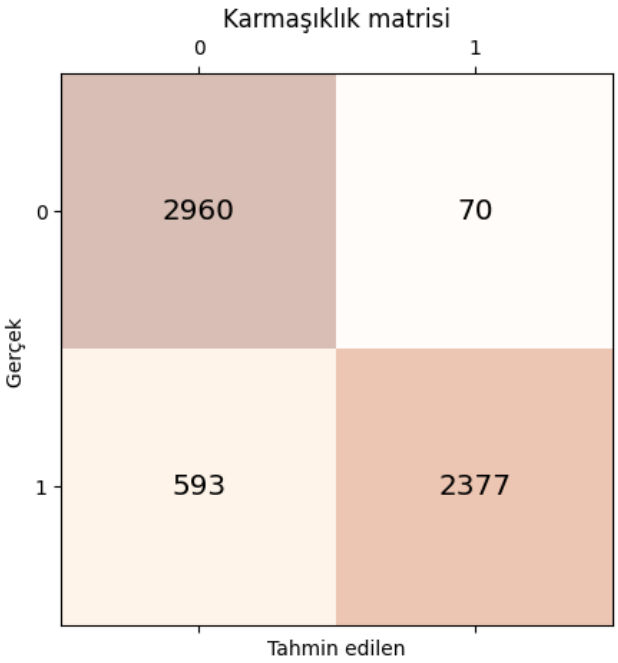
Şekil 5.67. KEY2023-KA modeli ikili sınıflandırma karmaşıklık matrisi

Çizelge 5.39. KEY2023-KA ikili sınıflandırma performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	%96	%96	%96
1	**Attack**	%96	%96	%96
	Modelin Accuracy (Doğruluğu) %	%96,08		

NB modeli iki sınıflandırma metriklerine göre (Çizelge 5.40), farklı başarı oranları elde etmiştir. BENIGN sınıfı için %83 kesinlik, %97 duyarlılık ve %90 f1-Skoru başarısı göstermiştir. Attack sınıfı için ise %97 kesinlik, %80 duyarlılık ve %88 f1-Skoru başarısı hesaplanmıştır. Modelin doğruluğu %88,95 oranında, iki sınıf arasında bir denge sağlamaktadır, ancak BENIGN sınıfının duyarlılığı daha yüksek olduğu için modelin BENIGN sınıfını tespit etme becerisi daha yüksektir.

Sonuç olarak, NB modeli BENIGN sınıfı için biraz daha düşük bir kesinlikle, ancak daha yüksek bir duyarlılık ve f1-skoru başarısı elde etmiştir. Attack sınıfı için ise NB modeli KA modelinden daha iyi bir kesinlik, ancak daha düşük bir duyarlılık ve f1-skoru başarısı göstermiştir. Karmaşıklık matrisinde (Şekil 5.68) sınıfların yanlış tahmin sayıları Attack sınıfının sınıflandırmada iyi olmadığını göstermektedir.



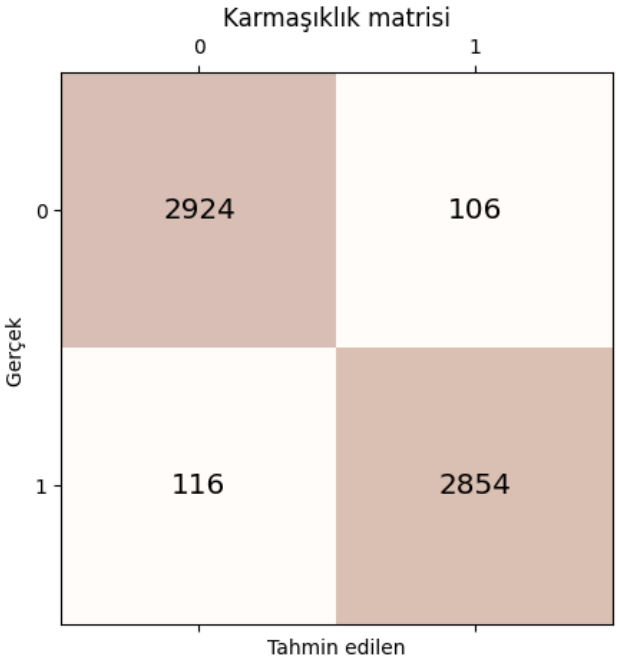
Şekil 5.68. KEY2023-NB modeli ikili sınıflandırma karmaşıklık matrisi

Çizelge 5.40. KEY2023-NB ikili sınıflandırma performans metrikleri

Etiket Değeri	Class (Sınıf)	Pecision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	%83	%98	%90
1	**Attack**	%97	%80	%88
	Modelin Accuracy (Doğruluğu) %	%88,95		

Çizelge 5.41'e göre, KEYK modeli iki sınıflandırma da %96 kesinlik, %97 duyarlılık ve %96 f1-Skoru başarısı hesaplanmıştır. Modelin doğruluğu %96,30'dur.

Bu sonuçlar, KEYK modelinin iki sınıf arasında dengeli bir performans gösterdiğini ve BENIGN sınıfını tespit etme becerisinin Attack sınıfını tespit etme becerisiyle aynı olduğunu göstermektedir. Sonuç olarak, KEYK modeli oldukça başarılı sonuçlar elde etmiştir ve iki sınıf arasında dengeli bir performans sergilemiştir ve karmaşıklık matrisinde (Şekil 5.69) de bu denge görülmektedir.



Şekil 5.69. KEY2023-KEYK modeli ikili sınıflandırma karmaşıklık matrisi

Çizelge 5.41. KEY2023-KEYK ikili sınıflandırma performans metrikleri

Etiket Değeri	Class (Sınıf)	Precision (Kesinlik) %	Recall (Duyarlılık) %	F1-Score (F1-Skor) %
0	**BENIGN**	%96	%97	%96
1	**Attack**	%96	%96	%96
	Modelin Accuracy (Doğruluğu) %	%96,30		

KEY2023 veri setinde ikili sınıflandırmada da modellerin eğitim zamanları kıyaslandığında Çizelge 5.42'de gösterildiği gibi en hızlı KEYK modeli, en yavaş TSA modeli olarak tespit edilmiştir.

Çizelge 5.42. KEY2023 veri seti modellerin ikili sınıflandırma eğitim zamanları

Model	***Zaman(ms)***
YSA	32409
UKSB	130889
TSA	950304
ESA	22809
LR	153
RO	170
KA	103
NB	8
KEYK	2

5.4. Tartışma

Bu tez çalışmasında Konelsis Kontrol Sistemleri Firmasından 2023 Mart ayında belirli zamanlarda normal ve saldırı verileri Hidroelektrik Santrallerini denetleyen ve kontrol eden SCADA sistemlerinden toplanmıştır. Sistem DDoS saldırıları ile yavaşlatılmış ve hizmet vermesi bu zaman aralıklarında engellenmiştir. Veriler alınarak oluşturulan ve KEY2023 (Konelsis-Ebru Yağmur -2023) olarak isimlendirilen bu veri seti üzerinde MÖ ve DÖ modelleri çalıştırılarak veri seti test edilip modellerin doğrulukları değerlendirilerek karşılaştırılmıştır. Modellere ait performans metrikleri hesaplanmıştır. DÖ modellerinin giriş verisi tek boyutlu dizi kanalında, optimizasyon algoritması Adam, aktivasyon fonksiyonu olarak ara katmanlarda ReLU, çıkış katmanında CICDDoS2019 veri seti için 8 çıkışlı softmax fonksiyonu, KEY2023 veri seti için ise 4 çıkışlı softmax fonksiyonu ve 100 epochda (adım sayısında) eğitilmiştir. İkili sınıflandırmada her iki veri seti için 1 çıkışlı sigmoid fonksiyonu kullanılmıştır. Genel olarak çoklu sınıflandırma başarılarında NB modelinin yetersiz kaldığı CICDDoS2019 veri seti için Çizelge 5.10 ve KEY2023 veri seti için Çizelge 5.30'da görülmektedir. Bu veri setleri üzerinde NB modelinin çoklu sınıflandırma başarısı yeterli olmadığı için diğer modellerin kullanılması gerektiği yorumlanmıştır.

6. SONUÇLAR VE ÖNERİLER

Bu bölümde yapılan çalışmalar değerlendirilmiştir ve elde edilen sonuçlara değinilerek öneriler verilmiştir.

6.1 Sonuçlar

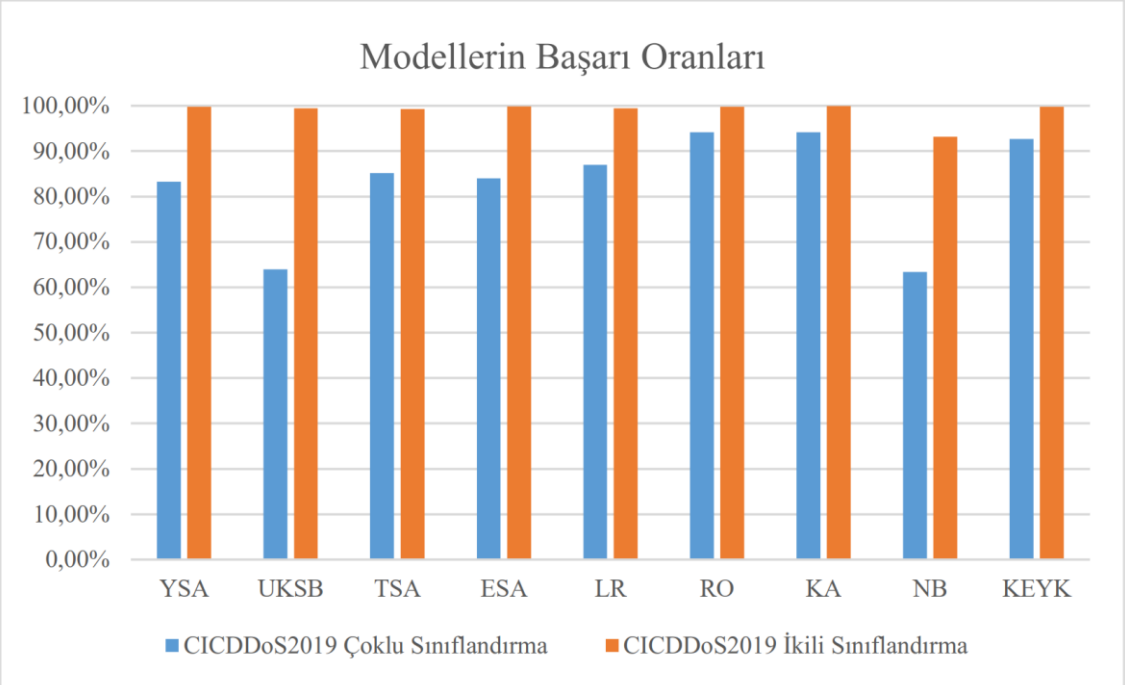
SCADA sistemlerine yapılan saldırılarla ilgili çalışmalar, Çizelge 6.1'de listelenmiştir. Listelenen çalışmalar, yazarların kendi oluşturdukları veri setleri üzerinde yaptıkları çalışmalardan oluşmaktadır. Her çalışmada farklı makine öğrenimi ve derin öğrenme modelleri uygulanmış ve başarılı sonuçlar elde edilmiştir. Bu çalışmada ise SCADA sistemlerine düzenlenen DDoS saldırıları verilerini içeren KEY2023 veri seti üzerinde ikili ve çoklu sınıflandırma makine öğrenimi ve derin öğrenme yöntemleri uygulanmıştır. Ayrıca CICDDoS2019 hazır veri setinde de modeller uygulanmıştır ve başarı oranları hesaplanmıştır. KEY2023 veri setinde, en yüksek başarı oranı ikili sınıflandırmada MÖ modellerinden KEYK modeliyle %96,30 ve DÖ modellerinden UKSB modeli ile %92,40 olarak elde edilmiştir. Çoklu sınıflandırmada ise MÖ modellerinden RO modeli %94,75 ve DÖ modellerinden TSA modeli %89,32 başarı oranları elde edilmiştir. Literatürdeki çalışmaların çoğu, SCADA sistemlerinde saldırı olup olmadığını ikili sınıflandırma ile analiz etmişlerdir. Bu çalışmada ise, bir DDoS saldırısı varsa bu saldırının hangi tür DDoS saldırısı olduğu araştırılmış ve model performansları literatüre göre başarılı sonuçlar vermiştir. Bu açıdan bakıldığında çoklu sınıflandırmada literatüre katkı sağlamıştır. Çoklu sınıflandırma sonuçları ikili sınıflandırmaya göre biraz daha düşük olsa da özellikle saldırı türünü tespit etmek istendiğinde bir saldırı tespit sistemi içinde entegre edilebilir olduğu belirlenmiştir.

Çizelge 6.1. SCADA çalışmalarının karşılaştırılması

Sıra	Yazar	Veri Seti Öznitelikler Teknikler Açıklama	Algoritma		Doğruluk
1	(Almalawi ve ark., 2014)	Kendi veri setleri DUWWTP üzerinde çalışmışlardır.	KEYK		%92,86
2	(Hoyos Ll ve ark., 2016)	DDoS saldırı tespiti için bir prototip geliştirmişlerdir.	DVM		%99
3	(Shirazi ve ark., 2016)	Anomali tespitini farklı modeller ile gerçekleştirip performans değerlendirmesini kendi veri setlerinde yapmışlardır.	K-Means PCA-SVD NB, GMM		%56.80 %17.14 %90.36 %45.16
4	(Yang ve ark., 2019)	SCADA sitemlerine karşı düzenlenen UDP taşma saldırılarına kendi veri setlerini oluşturarak derin öğrenme yöntemini denemişlerdir.	ESA		% 99.38
5	(Polat ve ark., 2022)	UKSB ve GRU yöntemlerini paralel kullanarak kendi oluşturdukları veri seti üzerinde özellik çıkarmışlardır.	DVM		%97,62
6	Bu çalışma	SCADA sistemlerine düzenlenen protokol saldırılarından oluşturulan veri seti kullanılmıştır.		*İkili*	*Çoklu*
			YSA	%92,26	%87
			UKSB	%92,40	%84,67
			TSA	%92,35	%89,32
			ESA	%92,43	%87,07
			LR	%91.96	%89.42
			RO	%96,28	%94,75
			KA	%96,08	%94,42
			NB	%88,95	%71,65
			KEYK	%96,30	%94,52

Bu çalışmalarda, yazarlar kendi veri setleriyle çalışmalarını gerçekleştirmişlerdir. Bu nedenle, bu tez çalışmasında elde edilen performans tam anlamıyla diğer çalışmalarla karşılaştırılamamıştır. Fakat modellerin performansına bakılarak bir karşılaştırma yapılmıştır. Almalawi ve arkadaşları (Almalawi ve ark., 2014) tarafından yapılan çalışmada KEYK modeli %92,86 oranında doğruluğa sahiptir ve bu çalışmada ikili

sınıflandırmada KEYK %96,30 oranında başarı ile iyi bir sonuç vermiştir. Bu sonuçların değişmesi veri setlerinde bulunan özelliklere bağlıdır. Bu tez çalışmasında DÖ modellerine odaklanılmıştır. DÖ modellerinden ESA ile Yang ve arkadaşlarının (Yang ve ark., 2019) yaptığı çalışmada UDP taşma saldırıları ve normal veriler üzerinden %99,38 oranında başarı elde edilirken, bu tez çalışmasında DÖ modellerinden ESA modeli ile, üç farklı DDoS saldırı ile oluşan Attack sınıfı ile normal verilerden ikili sınıflandırma başarısı %92,43 oranında elde edilmiştir. Tek tür DDoS saldırısı ile normal verilerin ikili sınıflandırmasında daha başarılı sonuçlar elde edilebileceği sonucuna ulaşılmıştır. Ayrıca literatüre KEY2023 veri seti eklenerek, daha başarılı sonuçlar elde etmek ve veri seti performansının daha verimli bir şekilde değerlendirilmesi için karşılaştırmalı sonuçlar sağlanabileceği sonucuna varılmıştır. Şekil 6.1'de CICDDoD2019 veri seti modellerin başarı oranları grafiği gösterilmiştir.



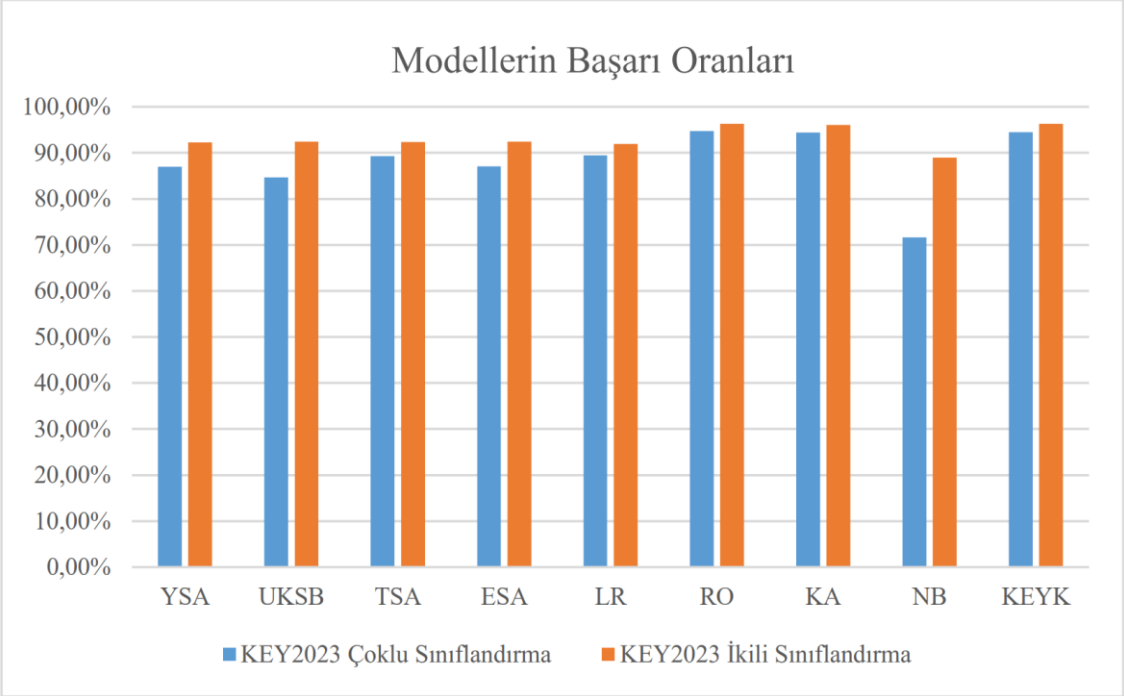
Şekil 6.1. CICDDoS2019 veri seti modellerin başarı oranları grafiği

Bu tez çalışmadı kapsamında hazır veri seti ile modeller değerlendirilmiş ve başarılı sonuçlar elde edilmiştir. CICDDoS2019 veri setinden ikili sınıflandırmada elde edilen en iyi sonuç %99,90 oranında KA modelinden elde edilmiştir. Sınıflandırma başarısı en düşük olan model ise %93,13 oranı ile NB modelidir. Çoklu sınıflandırma başarısına bakıldığında ise, %94,19 oranı ile RO modeli en başarılı model, %63,37 oranı

ile NB en düşük başarı oranına sahip modeldir. Çizelge 6.2'de bu veri setine ait başarı oranları verilmiştir.

Çizelge 6.2. CICDDoS2019 veri seti modellerin başarı oranları

Model	*Çoklu Sınıflandırma*	*İkili Sınıflandırma*
YSA	%83,25	%99,77
UKSB	%63,99	%99,45
TSA	%85,18	%99,29
ESA	%84,02	%99,82
LR	%86,94	%99,43
RO	%94,19	%99,80
KA	%94,13	%99,90
NB	%63,37	%93,13
KEYK	%92,69	%99,77



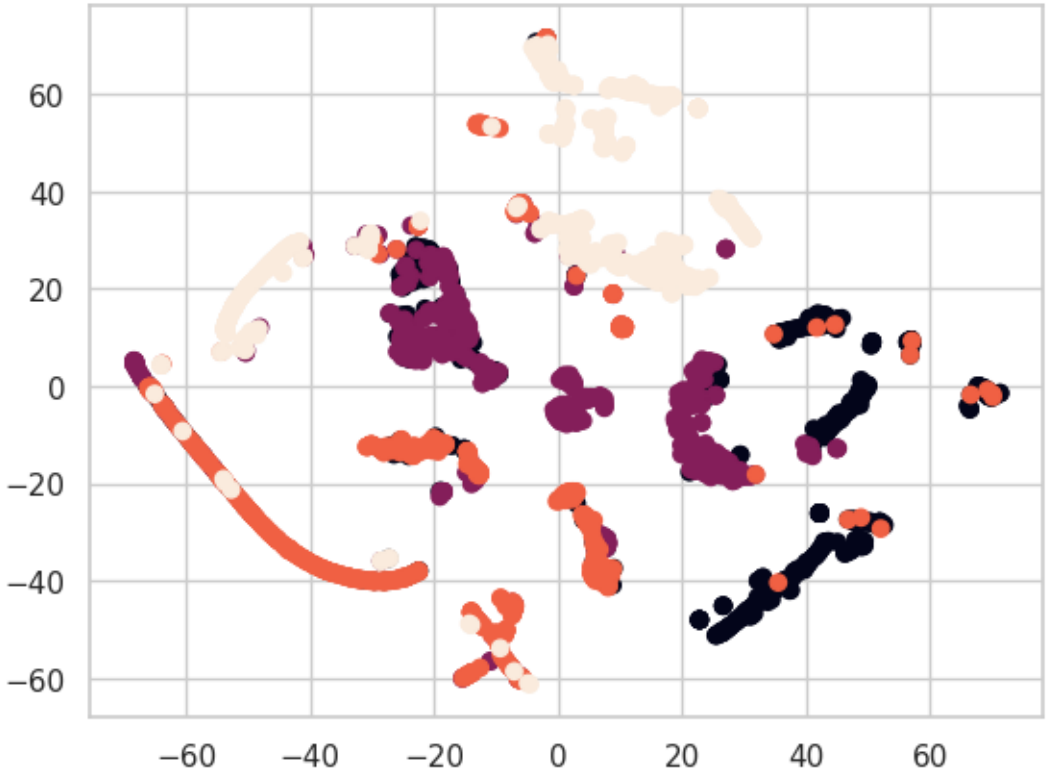
Şekil 6.2. KEY2023 veri seti modellerin başarı oranları grafiği

Bu tez çalışması SCADA sistemlerine düzenlenen DDoS saldırılarından elde edilen veri seti ile çalışmalar gerçekleştirilmiştir. Bu çalışmaların sonucunda Şekil 6.2'de verilen modellerin performansları karşılaştırıldığında ikili sınıflandırma sonuçlardı çoklu sınıflandırmaya göre daha iyi olduğu sonucuna ulaşılmıştır. Bu çalışmada DÖ modellerinin başarıları üzerine odaklanılmıştır fakat ikili sınıflandırmada ESA modeli %92,43 başarı oranı ile KEYK modelinin başarısı %96,30'un gerisinde kalmıştır fakat

sonuç olarak sınıflandırma başarısı yüksektir. Çoklu sınıflandırmada da TSA modeli ile %89,32 oranında başarı elde edilirken, RO modeli %94,75 ile daha iyi sonuç vermiştir. Çizelge 6.3'te modellerin başarı oranları sonuçları verilmiştir.

Çizelge 6.3. KEY2023 veri seti modellerin başarı oranları

Model	*Çoklu Sınıflandırma*	*İkili Sınıflandırma*
YSA	%87	%92,26
UKSB	%84,67	%92,40
TSA	%89,32	%92,35
ESA	%87,07	%92,43
LR	%89,42	%91,96
RO	%94,75	%96,28
KA	%94,42	%96,08
NB	%71,65	%88,95
KEYK	%94,52	%96,30



Şekil 6.3. KEY2023 veri seti t-SNE grafiği ile sınıf dağılımları

Yapılan çalışmalarda model performanslarının ikili sınıflandırmada daha iyi olmalarının sebebi ise Şekil 6.3.'de gösterilen KEY2023 veri setinden elde edilen t-SNE grafiği incelendiğinde görülmektedir. Burada sınıf dağılımlarının genel olarak üst üste

geldiği gözlemlenmektedir. Yani bu bir DDoS saldırısı ve türü ne olursa olsun saldırı olarak görüleceği anlamına da gelmektedir. Buradan elde edilen sonuç, DDoS saldırılarının tespitinde ikili sınıflandırma yapılmasının daha etkili sonuçlar vereceğidir.

6.2 Öneriler

Bu tez çalışmasında KEY2023 veri seti ile yapılan çalışmalar ile başarılı sonuçlar elde edilmesine rağmen özellikle çoklu sınıflandırmada bazı sınıfların tahmin performansı düşük kalmıştır. Saldırı sınıflarında benzerliklerin yoğun olması saldırı türlerinin tespitini bu anlamda zorlaştırmıştır. Çalışmada sınıfların eşitlenmesinde aşağı örnekleme yapılmıştır. KEY2023 veri seti kamuya açık bir platformda yayınlanarak literatürdeki çalışmalarda kullanım için desteklenebilir. Böylece literatüre SCADA sistemleri üzerinde DDoS saldırılarından oluşan bir veri seti kazandırılmış olacaktır. Buna göre ilerideki çalışmalarda veri arttırım teknikleri kullanılarak modellere farklı parametreler denenerek performansları arttırılabilir ve karşılaştırmalar yapılabilir.

KAYNAKLAR

Abadi, M., Agarwal, A., Barham, P., Brevdo, E., Chen, Z., Citro, C., Corrado, G. S., Davis, A., Dean, J. ve Devin, M., 2016, Tensorflow: Large-scale machine learning on heterogeneous distributed systems, *arXiv preprint arXiv:1603.04467*.

Academy, B., 2022, What are distributed denial of service (ddos) attacks?, https://bunny.net/academy/network/what-are-distributed-denial-of-service-ddos-attacks/:

Ahmed, I., Obermeier, S., Sudhakaran, S. ve Roussev, V., 2017, Programmable logic controller forensics, *IEEE Security & Privacy*, 15 (6), 18-24.

Ahmed, M., Mahmood, A. N. ve Hu, J., 2016, A survey of network anomaly detection techniques, *Journal of Network and Computer Applications*, 60, 19-31.

Ahmetoğlu, H. ve Daş, R., 2019, Derin öğrenme ile büyük veri kumelerinden saldırı türlerinin sınıflandırılması, *2019 International Artificial Intelligence and Data Processing Symposium (IDAP)*, 1-9.

Akamai, 2023, What is an ICMP flood DDoS attack?, https://www.akamai.com/glossary/what-is-icmp-flood-ddos-attack: [16.02.2023].

Akgun, D., Hizal, S. ve Cavusoglu, U., 2022, A new DDoS attacks intrusion detection model based on deep learning for cybersecurity, *Computers & Security*, 118, 102748.

Alanazi, M., Mahmood, A. ve Chowdhury, M. J. M., 2022, SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues, *Computers & Security*, 103028.

Albawi, S., Mohammed, T. A. ve Al-Zawi, S., 2017, Understanding of a convolutional neural network, *2017 international conference on engineering and technology (ICET)*, 1-6.

Alert, U.-C., 2020, NTP amplification attacks using CVE-2013-5211.

Alhaidari, F. A. ve AL-Dahasi, E. M., 2019, New approach to determine DDoS attack patterns on SCADA system using machine learning, *2019 International Conference on Computer and Information Sciences (ICCIS)*, 1-6.

Alkan, M., 2012, Siber Güvenlik ve Siber Savaşlar: Bilgi Güvenliği Derneği TBMM İnternet Komisyonu Sunumu, *Tİ Komisyonu*.

Almalawi, A., Yu, X., Tari, Z., Fahad, A. ve Khalil, I., 2014, An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems, *Computers & Security*, 46, 94-110.

Alphonsus, E. R. ve Abdullah, M. O., 2016, A review on the applications of programmable logic controllers (PLCs), *Renewable and Sustainable Energy Reviews*, 60, 1185-1205.

Alzahrani, S. ve Hong, L., 2018, Detection of distributed denial of service (ddos) attacks using artificial intelligence on cloud, *2018 IEEE World Congress on Services (SERVICES)*, 35-36.

Amidi, A. ve Amidi, S., Evrişimli Sinir Ağları el kitabı, https://stanford.edu/~shervine/l/tr/teaching/cs-230/cheatsheet-convolutional-neural-networks: [25.12.2021].

Assis, M. V., Carvalho, L. F., Lloret, J. ve Proença Jr, M. L., 2021, A GRU deep learning system against attacks in software defined networks, *Journal of Network and Computer Applications*, 177, 102942.

Atasever, S., Özçelik, İ. ve Sağıroğlu, Ş., 2019, Siber terör ve DDoS, *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 23 (1), 238-244.

Ateş, Ç., Özdel, S., Yıldırım, M. ve Anarım, E., 2019, Network anomaly detection using header information with greedy algorithm, *2019 27th Signal Processing and Communications Applications Conference (SIU)*, 1-4.

Ayaburi, E. ve Sobrevinas, L., 2015, Securing supervisory control and data acquisition systems: Factors and research direction.

Aydın, H., Orman, Z. ve Aydın, M. A., 2022, A long short-term memory (LSTM)-based distributed denial of service (DDoS) detection and defense system design in public cloud network environment, *Computers & Security*, 118, 102725.

Aytaç, T., Aydın, M. A. ve Zaim, A. H., 2020, Detection DDOS attacks using machine learning methods.

Baldini, G. ve Amerini, I., 2022, Online Distributed Denial of Service (DDoS) intrusion detection based on adaptive sliding window and morphological fractal dimension, *Computer Networks*, 210, 108923.

Baykara, M. ve Resul, D., 2019, Saldırı tespit ve engelleme araçlarının incelenmesi, *Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi*, 10 (1), 57-75.

Bhatia, S., Kush, N. S., Djamaludin, C., Akande, A. J. ve Foo, E., 2014, Practical modbus flooding attack and detection, *Proceedings of the Twelfth Australasian Information Security Conference (AISC 2014)[Conferences in Research and Practice in Information Technology, Volume 149]*, 57-65.

Biau, G. ve Scornet, E., 2016, A random forest guided tour, *Test*, 25, 197-227.

Bitchkei, S., 2017, Dragonfly 2.0 Targets Energy Sector Gaining Access To SCADA Systems, https://hitachi-systems-security.com/dragonfly-2-0-targets-energy-sector-gaining-access-to-scada-systems/: [20.02.2023].

Brahanyaa, S. ve Anbarasi, L. J., 2018, Classification of SNMP Network Dataset for DDoS attack prevention, *2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, 1-5.

Case, J. D., Fedor, M., Schoffstall, M. L. ve Davin, J., 1989, Simple network management protocol (SNMP).

Catak, F. O. ve Mustacoglu, A. F., 2019, Distributed denial of service attack detection using autoencoder and deep neural networks, *Journal of Intelligent & Fuzzy Systems*, 37 (3), 3969-3979.

Chen, B., Butler-Purry, K. L., Nuthalapati, S. ve Kundur, D., 2014, Network delay caused by cyber attacks on SVC and its impact on transient stability of smart grids, *2014 IEEE PES General Meeting| Conference & Exposition*, 1-5.

Chen, G., 2016, A gentle tutorial of recurrent neural network with error backpropagation, *arXiv preprint arXiv:1610.02583*.

Chollet, F., 2021, Deep learning with Python, Simon and Schuster, p.

Cil, A. E., Yildiz, K. ve Buldu, A., 2021, Detection of DDoS attacks with feed forward based deep neural network model, *Expert Systems with Applications*, 169, 114520.

Cisar, P. ve Pinter, R., 2019, Some ethical hacking possibilities in Kali Linux environment, *Journal of Applied Technical and Educational Sciences*, 9 (4), 129-149.

Cisco, 2022, Cisco Annual Internet Report (2018–2023), https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html: [27.12.2022].

Cloudflare, Technical Details Behind a 400Gbps NTP Amplification DDoS Attack, https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/: [10.01.2023].

Combe, T., Martin, A. ve Di Pietro, R., 2016, To docker or not to docker: A security perspective, *IEEE Cloud Computing*, 3 (5), 54-62.

Crane, C., 2020, Re-Hash: The Largest DDoS Attacks in History, *Hashed Out by The SSL Store™. Available online: https://www. thesslstore. com/blog/largest-ddos-attack-in-history/(accessed on 27 January 2021)*.

Cyberedge, 2022, Cyberthreat Defense Report, https://cyber-edge.com/wp-content/uploads/2022/04/CyberEdge-2022-CDR-Report.pdf: [22.12.2022].

Cybersecurity, C. I. f., 2017, CICFlowMeter (formerly ISCXFlowMeter), https://www.unb.ca/cic/research/applications.html:

Çatak, F. Ö. ve Mustaçoglu, A. F., 2017, Derin öğrenme teknolojileri kullanarak dağıtık hizmet dışı bırakma saldırılarının tespit edilmesi, *The 5th High Performance Computing Conference*, 1-8.

Daneels, A. ve Salter, W., 1999, What is SCADA?

do Nascimento, P. P., Pereira, P., Mialaret, J. M., Ferreira, I. ve Maciel, P., 2021, A methodology for selecting hardware performance counters for supporting non-intrusive diagnostic of flood DDoS attacks on web servers, *Computers & Security*, 110, 102434.

Efe, A., 2021, Yapay zeka odaklı siber risk ve güvenlik yönetimi, *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi*, 5 (2), 144-165.

Elsayed, M. S., Le-Khac, N.-A., Dev, S. ve Jurcut, A. D., 2020, Ddosnet: A deep-learning model for detecting network attacks, *2020 IEEE 21st International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*, 391-396.

Gandhi, N. ve Kansal, E. R., 2019, Comparative Analysis of DDoS Attack Tools and Techniques, *JETIR*, 6 (6), 7.

Gupta, N., 2013, Artificial neural network, *Network and Complex Systems*, 3 (1), 24-28.

Hasan, M. Z., Hasan, K. Z. ve Sattar, A., 2018, Burst header packet flood detection in optical burst switching network using deep learning model, *Procedia computer science*, 143, 970-977.

Hoyos Ll, M. S., Isaza E, G. A., Vélez, J. I. ve Castillo O, L., 2016, Distributed denial of service (ddos) attacks detection using machine learning prototype, *Distributed Computing and Artificial Intelligence, 13th International Conference*, 33-41.

Imperva, 2023a, TCP SYN flood, https://www.imperva.com/learn/ddos/syn-flood/: [16.02.2023].

Imperva, 2023b, UDP Flood, https://www.imperva.com/learn/ddos/udp-flood/: [16.02.2023].

İtübidb, 2013, Saldırı Tespit Sistemleri, https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/sald%C4%B1r%C4%B1-tespit-sistemleri:

Jasiul, B., Szpyrka, M. ve Śliwa, J., 2014, Detection and modeling of cyber attacks with petri nets, *Entropy*, 16 (12), 6602-6623.

Kakanakov, N. ve Spasov, G., 2011, Securing against Denial of Service attacks in remote energy management systems, *Annual Jornal of Electronics*.

Kantardzic, M., 2011, Data mining: concepts, models, methods, and algorithms, John Wiley & Sons, p.

Karaman, M. S., Turan, M. ve AYDIN, M. A., 2020, Yapay sinir ağı kullanılarak anomali tabanlı saldırı tespit modeli uygulaması, *Avrupa Bilim ve Teknoloji Dergisi* (Ejosat Ek Özel Sayı (HORA)), 10-17.

Karataş, G., 2020, Derin öğrenme tabanlı saldırı tespit sistemi.

Kaspersky, 2018, Gelmiş geçmiş en ünlü 5 siber saldırı, https://www.kaspersky.com.tr/blog/five-most-notorious-cyberattacks/5394/:

Kaynar, O., Arslan, H., Görmez, Y. ve Işık, Y. E., 2018, Makine Öğrenmesi ve Öznitelik Seçim Yöntemleriyle Saldırı Tespiti, *Bilişim Teknolojileri Dergisi*, 11 (2), 175-185.

Kotey, S. D., Tchao, E. T. ve Gadze, J. D., 2019, On distributed denial of service current defense schemes, *Technologies*, 7 (1), 19.

Krishnan, P., Duttagupta, S. ve Achuthan, K., 2019, VARMAN: Multi-plane security framework for software defined networks, *Computer Communications*, 148, 215-239.

Kumar, D., Pateriya, R., Gupta, R. K., Dehalwar, V. ve Sharma, A., 2023, DDoS Detection using Deep Learning, *Procedia computer science*, 218, 2420-2429.

Kyspersky, 2021, DDoS attacks hit a record high in Q4 2021, Kyspersky, https://www.kaspersky.com/about/press-releases/2022_ddos-attacks-hit-a-record-high-in-q4-2021: [22.09.2022].

Lau, F., Rubin, S. H., Smith, M. H. ve Trajkovic, L., 2000, Distributed denial of service attacks, *Smc 2000 conference proceedings. 2000 ieee international conference on systems, man and cybernetics.'cybernetics evolving to systems, humans, organizations, and their complex interactions'(cat. no. 0*, 2275-2280.

Linux, K., 2020, Kali Linux, Obtenido de Official Kali Linux Documentation: http://docs. kali. org ….

Liu, Y., Zhi, T., Shen, M., Wang, L., Li, Y. ve Wan, M., 2022, Software-defined DDoS detection with information entropy analysis and optimized deep learning, *Future Generation Computer Systems*, 129, 99-114.

MacFarland, D. C., Shue, C. A. ve Kalafut, A. J., 2017, The best bang for the byte: Characterizing the potential of DNS amplification attacks, *Computer Networks*, 116, 12-21.

Mall, R., Abhishek, K., Manimurugan, S., Shankar, A. ve Kumar, A., 2023, Stacking ensemble approach for DDoS attack detection in software-defined cyber–physical systems, *Computers and Electrical Engineering*, 107, 108635.

Marino, A. ve Zio, E., 2021, A framework for the resilience analysis of complex natural gas pipeline networks from a cyber-physical system perspective, *Computers & Industrial Engineering*, 162, 107727.

Markovic-Petrovic, J. D. ve Stojanovic, M. D., 2013, Analysis of SCADA system vulnerabilities to DDoS attacks, *2013 11th international conference on telecommunications in modern satellite, cable and broadcasting services (telsiks)*, 591-594.

Mehta, B. R. ve Reddy, Y. J., 2014, Industrial process automation systems: design and implementation, Butterworth-Heinemann, p. 237-300.

Mohamed Najeh, L., 2017, Review on SCADA Cybersecurity for Critical Infrastructures, *Journal of Computer Science & Control Systems*, 10 (1).

Munz, G. ve Carle, G., 2008, Distributed network analysis using TOPAS and wireshark, *NOMS Workshops 2008-IEEE Network Operations and Management Symposium Workshops*, 161-164.

Myneni, S., Chowdhary, A., Huang, D. ve Alshamrani, A., 2022, SmartDefense: A distributed deep defense against DDoS attacks with edge computing, *Computer Networks*, 209, 108874.

Nazir, S., Patel, S. ve Patel, D., 2017, Assessing and augmenting SCADA cyber security: A survey of techniques, *Computers & Security*, 70, 436-454.

Netscout, What is a DNS Reflection/Amplification DDoS Attack?, https://www.netscout.com/what-is-ddos/what-are-reflection-amplification-attacks: [14.02.2023].

Netscout, 2022, Netscout Ddos Threat Intelligence Report, https://www.netscout.com/threatreport/emea/: [29.12.2022].

Nexusguard, 2022, DDoS Statistical Report for 1HY 2022, https://blog.nexusguard.com/threat-report/ddos-statistical-report-for-1hy-2022: [3.12.2022].

Nwoba, E. G., Chuka-Ogwude, D., Vadiveloo, A. ve Ogbonna, J. C., 2022, Process control strategies applied to microalgae-based biofuel production, In: 3rd Generation Biofuels, Eds: Elsevier, p. 105-134.

O'Shea, K. ve Nash, R., 2015, An introduction to convolutional neural networks, *arXiv preprint arXiv:1511.08458*.

Onyeji, I., Bazilian, M. ve Bronk, C., 2014, Cyber security and critical energy infrastructure, *The Electricity Journal*, 27 (2), 52-60.

Öztürk, E., 2018, Enerji sektörü için büyük tehlike: Triton malware, https://blog.cyberage.com.tr/2018/01/17/enerji-sektoru-icin-buyuk-tehlike-triton-malware/: [20.02.2023].

Paganini, P., 2017, DragonFly 2.0: The Alleged Nation-State Actor Hits the Energy Sector Again, https://resources.infosecinstitute.com/topic/dragonfly-2-0-alleged-nation-state-actor-hit-energy-sector/: [20.02.2023].

Patel, D., 2018, Introduction Practical PLC (Programmable Logic Controller) Programming, GRIN Verlag, p.

Polat, H., Türkoğlu, M., Polat, O. ve Şengür, A., 2022, A novel approach for accurate detection of the DDoS attacks in SDN-based SCADA systems based on deep recurrent neural networks, *Expert Systems with Applications*, 197, 116748.

Prakash, A. ve Priyadarshini, R., 2018, An intelligent software defined network controller for preventing distributed denial of service attack, *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, 585-589.

Pushpa Singh, N. S., Krishna Kant Singh, Akansha Singh, 2021, Diagnosing of disease using machine learning, In: Machine Learning and the Internet of Medical Things in Healthcare, Eds: Krishna Kant Singh, M. E., Akansha Singh, Ahmed A. Elngar: Academic Press, p. 89-111.

Rad, B. B., Bhatti, H. J. ve Ahmadi, M., 2017, An introduction to docker and analysis of its performance, *International Journal of Computer Science and Network Security (IJCSNS)*, 17 (3), 228.

Radware, 2022, LAND Attack, https://www.radware.com/security/ddos-knowledge-center/ddospedia/land-attack/: [13.12.2022].

Raza, A., 2021, Russian Internet Giant Suffers Largest DDoS Attack in History, https://blog.koddos.net/russian-internet-giant-suffers-largest-ddos-attack-in-history/: [13.08.2022].

Sağıroğlu, Ş., 2021, SİBER GÜVENLİK ONTOLOJİSİ-I, *Siber Güvenlik ve Savunma Kitap Serisi 6: SİBER GÜVENLİK ONTOLOJİSİ, TEHDİTLER VE ÇÖZÜMLER*, 6, 1.

Samtani, S., Yu, S., Zhu, H., Patton, M. ve Chen, H., 2016, Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques, *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, 25-30.

Savaş, S. ve Karataş, S., 2022, Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance, *International Cybersecurity Law Review*, 3 (1), 7-34.

Sharafaldin, I., Lashkari, A. H., Hakak, S. ve Ghorbani, A. A., 2019, Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy, *2019 International Carnahan Conference on Security Technology (ICCST)*, 1-8.

Sharma, S., Kumar, V., Sharma, P., Gupta, S. ve Shukla, A., 2022, SCADA Communication Protocols: Modbus & IEC 60870–5, *2022 1st International Conference on Sustainable Technology for Power and Energy Systems (STPES)*, 1-6.

Shirazi, S. N., Gouglidis, A., Syeda, K. N., Simpson, S., Mauthe, A., Stephanakis, I. M. ve Hutchison, D., 2016, Evaluation of anomaly detection techniques for scada communication resilience, *2016 Resilience Week (RWS)*, 140-145.

Shitharth, S. ve Winston, D. P., 2015, A comparative analysis between two countermeasure techniques to detect DDoS with sniffers in a SCADA network, *Procedia Technology*, 21, 179-186.

Sokolova, M. ve Lapalme, G., 2009, A systematic analysis of performance measures for classification tasks, *Information processing & management*, 45 (4), 427-437.

Söğüt, E. ve Erdem, O. A., 2020, Endüstriyel kontrol sistemlerine (scada) yönelik siber terör saldırı analizi, *Politeknik Dergisi*, 23 (2), 557-566.

Şeker, E., 2020, Yapay Zekâ Tekniklerinin/Uygulamalarının Siber Savunmada Kullanımı, *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 6 (2), 108-115.

Takaoğlu, M. ve Özer, Ç., 2019, Saldırı Tespit Sistemlerine Makine Öğrenme Etkisi, *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi*, 3 (1), 11-22.

Taşdelen, İ., 2022, SCADA Sistemleri Tam Olarak Nedir ?, Medium, https://medium.com/databulls/scada-sistemleri-tam-olarak-nedir-77434b59e542: [27.03.2023].

Thinktech, S., 2022, Yapay Zekânın Geleceği, https://thinktech.stm.com.tr/tr/yapay-zekanin-gelecegi: [12.10.2022].

Van Houdt, G., Mosquera, C. ve Nápoles, G., 2020, A review on the long short-term memory model, *Artificial Intelligence Review*, 53, 5929-5955.

Wang, S., Xu, D. ve Yan, S., 2010, Analysis and application of Wireshark in TCP/IP protocol teaching, *2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT)*, 269-272.

Webb, G. I., Keogh, E. ve Miikkulainen, R., 2010, Naïve Bayes, *Encyclopedia of machine learning*, 15, 713-714.

Wikipedia, 2016, DDoS Attacks on Dyn, https://en.wikipedia.org/wiki/DDoS_attacks_on_Dyn#Affected_services: [17.11.2022].

Wingpath, 2014-2023, Modbus Protocol, https://wingpath.co.uk/modbus/modbus_protocol.php: [22.12.2022].

Wired, 2016, Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/: [13.01.2023].

Yang, H., Cheng, L. ve Chuah, M. C., 2019, Deep-learning-based network intrusion detection for SCADA systems, *2019 IEEE Conference on Communications and Network Security (CNS)*, 1-7.

Yousuf, O. ve Mir, R. N., 2022, DDoS attack detection in Internet of Things using recurrent neural network, *Computers and Electrical Engineering*, 101, 108034.

Zhong, Y., 2016, The analysis of cases based on decision tree, *2016 7th IEEE international conference on software engineering and service science (ICSESS)*, 142-147.

Zhu, M., Ye, K. ve Xu, C.-Z., 2018, Network anomaly detection and identification based on deep learning methods, *International Conference on Cloud Computing*, 219-234.

Zimmerman, G. P., 2008, Programmable logic controllers and ladder logic, *Rapid City: Dr. Alfred R. Boysen, Department of Humanities, South Dakota School of Mines and Technology*.