



T.C.
KONYA TEKNİK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ



CICIOT2023 VERİ SETİ İLE IOT
ORTAMLARINDA SİBER SALDIRILARIN
TESPİTİ VE ANALİZİ
Ekrem TÜRKAY

YÜKSEK LİSANS TEZİ

Bilgisayar Mühendisliği Anabilim Dalı

Haziran-2025
KONYA
Her Hakkı Saklıdır

TEZ KABUL VE ONAYI

Ekrem TRKAY tarafından hazırlanan “CICIOT2023 VERİ SETİ İLE IOT ORTAMLARINDA SİBER SALDIRILARIN TESPİTİ VE ANALİZİ” adlı tez çalışması 18/06/2025 tarihinde aşağıdaki jüri tarafından oy birliği / oy çokluğu ile Konya Teknik Üniversitesi Lisansüstü Eğitim Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı’nda YKSEK LİSANS TEZİ olarak kabul edilmiştir.

Jri yeleri

İmza

Başkan

Dr. Öğr. yesi Ali ÇETİNKAYA

.....

Danışman

Prof. Dr. Halife KODAZ

.....

ye

Dr. Öğr. yesi Hazim İŞCAN

.....

Yukarıdaki sonucu onaylarım.

Prof. Dr. Mevlt UYAN
Enstit Mdr

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.

Ekrem TÜRKAY

Tarih: 18/06/2025

ÖZET**YÜKSEK LİSANS TEZİ****CICIOT2023 VERİ SETİ İLE IOT ORTAMLARINDA SİBER SALDIRILARIN
TESPİTİ VE ANALİZİ****Ekrem TÜRKEY****Konya Teknik Üniversitesi
Lisansüstü Eğitim Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı****Danışman: Prof. Dr. Halife KODAZ****2025, 201 Sayfa****Jüri****Prof. Dr. Halife KODAZ
Dr. Öğr. Üyesi Hazim İŞCAN
Dr. Öğr. Üyesi Ali ÇETİNKAYA**

Nesnelerin İnterneti (IoT) teknolojilerinin hızla yaygınlaşması, bu sistemlere yönelik siber saldırı risklerini de beraberinde getirmektedir. Özellikle sınırlı işlem gücüne ve güvenlik önlemlerine sahip IoT cihazları, DDoS saldırıları ve diğer siber tehditler karşısında savunmasız hale gelmekte, bu da hizmet kesintilerine ve kritik altyapıların zarar görmesine neden olabilmektedir. Bu çalışmada, IoT ortamlarında meydana gelen siber saldırıların tespit edilmesi ve analiz edilmesi amacıyla CICIOT2023 veri seti kullanılarak çeşitli makine öğrenmesi ve derin öğrenme algoritmalarının performansları değerlendirilmiştir. Lojistik Regresyon (LR), Karar Ağaçları (KA), Naive Bayes (NB), K-En Yakın Komşular (KEYK), Rasgele Orman (RO), Gradyan Artırma (GA), Aşırı Gradyan Artırma (AGA), Yapay Sinir Ağları (YSA), Uzun Kısa Süreli Bellek (UKSB), Tekrarlı Sinir Ağları (TSA) ve Evrişimli Sinir Ağları (ESA) gibi modeller kullanılarak, saldırı tespitindeki etkinlikleri karşılaştırılmıştır. Elde edilen sonuçlar, yapay zekâ ve makine öğrenmesi tabanlı yaklaşımların IoT sistemlerinde siber tehditleri tespit etmede etkili olduğunu göstermektedir. Çalışma, IoT güvenliğini artırmaya yönelik daha güçlü savunma mekanizmalarının geliştirilmesine katkı sağlamayı ve gelecekteki araştırmalar için yol gösterici olmayı amaçlamaktadır.

Anahtar Kelimeler: CICIOT2023, DDoS, derin öğrenme, makine öğrenmesi, siber güvenlik, siber saldırı, veri seti.

ABSTRACT**MS THESIS****DETECTION AND ANALYSIS OF CYBER ATTACKS IN IOT
ENVIRONMENTS USING THE CICIOT2023 DATASET****Ekrem TÜRKAY****Konya Technical University
Institute of Graduate Studies
Department of Computer Engineering****Advisor: Prof. Dr. Halife KODAZ****2025, 201 Pages****Jury
Prof. Dr. Halife KODAZ
Assist. Prof. Dr. Hazim İŞCAN
Assist. Prof. Dr. Ali ÇETİNKAYA**

The rapid proliferation of Internet of Things (IoT) technologies has also increased the risk of cyber attacks targeting these systems. IoT devices, which often have limited processing power and security measures, are vulnerable to DDoS attacks and other cyber threats, leading to service disruptions and damage to critical infrastructures. In this study, various machine learning and deep learning algorithms were evaluated using the CICIOT2023 dataset to detect and analyze cyber attacks in IoT environments. Models such as Logistic Regression (LR), Decision Trees (DT), Naive Bayes (NB), K-Nearest Neighbors (KNN), Random Forest (RF), Gradient Boosting (GB), Extreme Gradient Boosting (XGBoost), Artificial Neural Networks (ANN), Long Short-Term Memory (LSTM), Recurrent Neural Networks (RNN) and Convolutional Neural Networks (CNN) were compared in terms of their effectiveness in attack detection. The results indicate that AI and machine learning-based approaches are effective in identifying cyber threats in IoT systems. This study aims to contribute to the development of more robust security mechanisms for IoT environments and serve as a guide for future research.

Keywords: CICIOT2023, DDoS, deep learning, machine learning, cybersecurity, cyber attack, dataset.

ÖNSÖZ

Bu tez çalışmam süresince bilgi ve deneyimleriyle bana yol gösteren, değerli görüşleri ve destekleriyle çalışmama büyük katkı sağlayan danışman hocam Prof. Dr. Halife KODAZ'a;

Tez sürecinde desteklerini esirgemeyen Bilgisayar Mühendisliği Bölümü'ndeki saygı değer hocalarıma;

Yüksek Lisans eğitimine başlamama vesile olan ve bu süreç boyunca sonsuz desteği ile bana güç veren değerli eşim Hatice TÜRKAY'a, çalışmalarım boyunca sabırla beni destekleyen kızım Zeynep Berra TÜRKAY'a, oğlum Yusuf Talha TÜRKAY'a ve çalışma arkadaşlarıma sonsuz teşekkürlerimi sunarım.

Ekrem TÜRKAY
KONYA-2025

İÇİNDEKİLER

ÖZET	iv
ABSTRACT.....	v
ÖNSÖZ	vi
İÇİNDEKİLER	vii
SİMGELER VE KISALTMALAR	xi
1. GİRİŞ.....	1
1.1. Problemin Tanımı.....	2
1.2. Amaç ve Hedef	2
1.3. Tezin Organizasyonu	3
2. KAYNAK ARAŞTIRMASI	5
2.1. IoT Teknolojisi ve Güvenlik Riskleri	5
2.1.1. Nesnelerin İnterneti (IoT) Kavramı	6
2.1.2. IoT ve Siber Güvenlik Arasındaki İlişki	7
2.1.3. IoT’de Karşılaşılan Siber Tehditler	8
2.1.3.1. Dağıtık Hizmet Reddi (DDoS) Saldırıları	9
2.1.3.2. Man-in-the-Middle (MitM) Saldırıları.....	9
2.1.3.3. Kimlik Avı (Phishing) ve Yetkisiz Erişim.....	10
2.1.3.4. Kötü Amaçlı Yazılımlar (Malware).....	10
2.1.3.5. Yan Kanal Saldırıları (Side Channel Attacks)	10
2.1.3.6. Veri Sızıntısı ve Gizlilik İhlalleri.....	10
2.1.4. IOT Sistemlerine Yapılan Siber Saldırı Örnekleri.....	10
2.1.5. Mevcut IoT Güvenlik Çözümleri ve Sınırlamaları	15
2.2. Literatürde Öne Çıkan Çalışmalar	16
3. MATERYAL VE YÖNTEM.....	29
3.1. Kullanılan Veri Seti: CICIoT2023	29
3.1.1. CICIoT2023 Veri Setinin Önemi ve Kullanım Alanları.....	32
3.1.2. CICIoT2023 Veri Setinin Özellikleri	33
3.1.3. Normal ve Saldırı Trafiğinin Karakterizasyonu	35
3.2. CICIoT2023 Veri Setindeki IoT Saldırı Türleri	37
3.2.1. DDoS (Distributed Denial of Service) Saldırıları	40
3.2.1.1. ACK Fragmentation.....	42
3.2.1.2. UDP Flood	43
3.2.1.3. Slowloris	44
3.2.1.4. ICMP flood	45
3.2.1.5. RSTFIN Flood	46
3.2.1.6. PSH-ACK Flood	46
3.2.1.7. HTTP Flood	47
3.2.1.8. UDP Fragmentation	48
3.2.1.9. TCP Flood.....	48

3.2.1.10.	SYN Flood	49
3.2.1.11.	SynonymousIP Flood.....	50
3.2.2.	Brute Force (Kaba Kuvvet) Saldırıları.....	51
3.2.3.	Spoofing (Sahtecilik) Saldırıları	53
3.2.3.1.	ARP Spoofing	53
3.2.3.2.	DNS Spoofing	55
3.2.4.	DoS (Denial of Service) Saldırıları.....	56
3.2.5.	Reconnaissance (Keşif) Saldırıları.....	57
3.2.5.1.	Ping Tarama (Ping Sweep)	57
3.2.5.2.	İşletim Sistemi Tarama (OS Scan).....	58
3.2.5.3.	Zafiyet Tarama (Vulnerability Scan).....	58
3.2.5.4.	Port Tarama (Port Scan)	58
3.2.5.5.	Cihaz Keşfi (Host Discovery).....	58
3.2.6.	Web-Based (Web Tabanlı) Saldırıları	58
3.2.6.1.	SQL Injection.....	58
3.2.6.2.	Command Injection.....	60
3.2.6.3.	Backdoor Malware.....	61
3.2.6.4.	Uploading Attack.....	62
3.2.6.5.	XSS (Cross-Site Scripting)	63
3.2.6.6.	Browser Hijacking	65
3.2.7.	Mirai Botnet Saldırıları.....	65
3.2.7.1.	GREIP Flood Saldırısı	66
3.2.7.2.	Greeth Flood Saldırısı.....	67
3.2.7.3.	UDPPlain Saldırısı.....	67
3.3.	Saldırı Tespit Sistemleri	67
3.3.1.	Ağ tabanlı saldırı tespit sistemi.....	67
3.3.2.	İmza tabanlı saldırı tespiti.....	68
3.3.3.	Anomali tabanlı saldırı tespiti.....	68
3.3.4.	Ana bilgisayar tabanlı saldırı tespit sistemi	69
3.3.5.	Derin öğrenme tabanlı saldırı tespit sistemi	69
3.4.	Makine Öğrenmesi.....	70
3.4.1.	Lojistik Regresyon (LR)	70
3.4.2.	Navie Bayes (NB).....	71
3.4.3.	K En Yakın Komşu (KEYK)	73
3.4.4.	Karar Ağaçları (KA)	74
3.4.5.	Rastgele Orman (RO)	75
3.4.6.	Gradyan Artırma (GA).....	75
3.4.7.	Aşırı Gradyan Artırma (AGA).....	76
3.5.	Derin Öğrenme (DÖ)	77
3.5.1.	Yapay sinir ağları (YSA)	77
3.5.2.	Evrişimsel Sinir Ağları (ESA)	78
3.5.3.	Tekrarlayan Sinir Ağları (TSA).....	79
3.5.4.	Uzun Kısa Süreli Bellek (UKSB)	80
3.6.	Değerlendirme Metrikleri	80
3.6.1.	Karmaşıklık matrisi.....	81
3.6.2.	Performans metrikleri	82
3.7.	CICIoT2023 Veri Ön İşleme.....	83
3.7.1.	CICIoT2023 Veri Seti: Kategorik Verilerin Kodlanması.....	84
3.7.2.	Sınıf Dengesizliğinin Giderilmesi	84

3.7.2.1.	SMOTE, ADASYN, Borderline-SMOTE ve SMOTEENN Yöntemleri	85
3.7.2.2.	Farklı Dengeleme Stratejilerinin Seçim Gerekçeleri	86
3.7.3.	CICIoT2023 Veri Seti: İkili Sınıflandırma İçin Hazırlık	86
3.7.4.	CICIoT2023 Veri: Sekizli Sınıflandırma İçin Hazırlık	87
3.7.5.	CICIoT2023 Veri: Otuz Dört Sınıflı Sınıflandırma İçin Hazırlık	91
3.7.6.	CICIoT2023 Veri: Özellik seçimi	92
3.7.7.	Rastgele Orman (RO) Tabanlı Özellik Seçimi	93
4.	ARAŞTIRMA SONUÇLARI VE TARTIŞMA	94
4.1.	Çalışma Ortamı	95
4.2.	CICIoT2023 Veri Seti Sonuçları	96
4.2.1.	İkili sınıflandırma sonuçları	96
4.2.1.1.	Lojistik Regresyon (LR) algoritması sonuçları	97
4.2.1.2.	Naive Bayes (NB) algoritması sonuçları	100
4.2.1.3.	K En Yakın Komşu (KEYK) algoritması sonuçları	103
4.2.1.4.	Karar Ağacı (KA) algoritması sonuçları	107
4.2.1.5.	Rastgele Orman (RO) algoritması sonuçları	109
4.2.1.6.	Gradyan Artırma (GA) algoritması sonuçları	113
4.2.1.7.	Aşırı Gradyan Artırma (AGA) algoritması sonuçları	115
4.2.1.8.	Yapay sinir ağları (YSA) algoritması sonuçları	118
4.2.1.9.	Evrişimsel Sinir Ağları (ESA) algoritması sonuçları	121
4.2.1.10.	Tekrarlayan sinir ağları (TSA) algoritması sonuçları	123
4.2.1.11.	Uzun Kısa Süreli Bellek (UKSB) algoritması sonuçları	126
4.2.2.	Sekizli sınıflandırma sonuçları	129
4.2.2.1.	Lojistik Regresyon (LR) algoritması sonuçları	130
4.2.2.2.	Naive Bayes (NB) algoritması sonuçları	134
4.2.2.3.	K En Yakın Komşu (KEYK) algoritması sonuçları	135
4.2.2.4.	Karar Ağacı (KA) algoritması sonuçları	136
4.2.2.5.	Rastgele Orman (RO) algoritması sonuçları	139
4.2.2.6.	Gradyan Artırma (GA) algoritması sonuçları	142
4.2.2.7.	Aşırı Gradyan Artırma (AGA) algoritması sonuçları	145
4.2.2.8.	Yapay sinir ağları (YSA) algoritması sonuçları	148
4.2.2.9.	Evrişimsel Sinir Ağları (ESA) algoritması sonuçları	150
4.2.2.10.	Tekrarlayan sinir ağları (TSA) algoritması sonuçları	153
4.2.2.11.	Uzun Kısa Süreli Bellek (UKSB) algoritması sonuçları	156
4.2.3.	Otuz dördü sınıflandırma sonuçları	160
4.2.3.1.	Lojistik Regresyon (LR) algoritması sonuçları	160
4.2.3.2.	Naive Bayes (NB) algoritması sonuçları	164
4.2.3.3.	K En Yakın Komşu (KEYK) algoritması sonuçları	166
4.2.3.4.	Karar Ağacı (KA) algoritması sonuçları	169
4.2.3.5.	Rastgele Orman (RO) algoritması sonuçları	173
4.2.3.6.	Gradyan Artırma (GA) algoritması sonuçları	177
4.2.3.7.	Aşırı Gradyan Artırma (AGA) algoritması sonuçları	180
4.2.3.8.	Yapay sinir ağları (YSA) algoritması sonuçları	182
4.2.3.9.	Evrişimsel Sinir Ağları (ESA) algoritması sonuçları	184
4.2.3.10.	Tekrarlayan sinir ağları (TSA) algoritması sonuçları	186
4.2.3.11.	Uzun Kısa Süreli Bellek (UKSB) algoritması sonuçları	188
4.3.	Tartışma	190

5. SONUÇLAR VE ÖNERİLER	192
5.1 Sonuçlar	192
5.2 Öneriler	193
KAYNAKLAR	195



SİMGELER VE KISALTMALAR

Simgeler

b : Eğilim
 F : Evrişimsel katman nöronlarının boyutu
 N : Nöron sayısı
 P : Sıfır dolgulama miktarı
 γ : Küme normalleştirilmesi
 β : Hiper-parametre
 α, η : Öğrenme oranı
 μ_B : Düzeltilen kümenin ortalaması
 σ_B^2 : Düzeltilen küme varyansı
 w : Ağırlık
 W : Girdi boyutu
 z : Ürün

Kısaltmalar

ACC : Doğruluk Oranı
 ACK : Onay
 ADAM : Uyarlanabilir Moment Tahmini
 ADAMAX : Uyarlanabilir Maksimum Havuzlama
 AUC : Eğri Altında Kalan Alan
 BotNet : Robot Ağı
 CICIoT2023 : Canadian Institute for Cybersecurity IoT 2023 Veri Seti
 ÇKA : Çok Katmanlı Algılayıcı
 DAE : Derin Oto-Kodlayıcı Ağları
 DBN : Derin İnanç Ağı
 DCS : Dağıtık Kontrol Sistemi
 DDoS : Dağıtılmış Hizmet Engelleme Saldırısı
 DNS : Alan Adı Sistemi
 DoS : Hizmet Dışı Bırakma
 DÖ : Derin Öğrenme
 DSA : Derin Sinir Ağı
 DVM : Destek Vektör Makinesi
 ESA : Evrişimli Sinir Ağı
 F1-Score : Doğruluk ve Hassasiyetin Harmonik Ortalaması
 FN : Yanlış Negatif
 FNN : İleri Beslemeli Sinir Ağı
 FP : Yanlış Pozitif
 GB : Gradyan Artırma
 GRU : Geçitli Tekrarlayan Birim
 HMI : İnsan-Makine Arayüzü
 HTTP : Üst Metin Transfer Protokolü
 HTTPS : Güvenli Üst Metin Transfer Protokolü
 IAT : Paketler Arası Varış Süresi
 ICMP : İnternet Kontrol Mesajı Protokolü

IIoT	: Endüstriyel Nesnelerin İnterneti
IoT	: Nesnelerin İnterneti
IP	: İnternet Protokolü
ISO	: Uluslararası Standardizasyon Örgütü
KA	: Karar Ağacı
KEYK	: K-En Yakın Komşu
LDA	: Doğrusal Diskriminant Analizi
LDAP	: Basit Dizin Erişim Protokolü
LR	: Lojistik Regresyon
MÖ	: Makine Öğrenmesi
MSSQL	: Microsoft SQL Server
NB	: Naive Bayes
NDAE	: Simetrik Olmayan Derin Otomatik Kodlayıcı
NETBIOS	: Ağ Temel Giriş/Çıkış Sistemi
NIDS	: Ağ Tabanlı Saldırı Tespit Sistemi
NTP	: Ağ Zaman Protokolü
OSI	: Açık Sistem Ara Bağlantısı
PLC	: Programlanabilir Mantık Denetleyicisi
ReLU	: Doğrultulmuş Doğrusal Birim
Rmsprop	: Kök Ortalama Kare Yayılımı
RNN	: Tekrarlayan Sinir Ağı
RO	: Rastgele Orman Algoritması
ROC	: Alıcı İşletim Karakteristiği
ROC-AUC	: ROC Eğrisi Altındaki Alan
RPS	: Saniye Başına İstek
SDN	: Yazılım Tanımlı Ağ
SGD	: Stokastik Gradyan İnişi
SHAP	: Özellik Önem Açıklama Tekniği
SMOTE	: Sentetik Azınlık Aşırı Örnekleme
SMTP	: Basit Posta Aktarım Protokolü
SNMP	: Basit Ağ Yönetimi Protokolü
SSDP	: Basit Hizmet Keşif Protokolü
SÖS	: Saldırı Önleme Sistemi
STS	: Saldırı Tespit Sistemi
SYN	: Senkronize
TCP	: İletim Kontrol Protokolü
TFTP	: Önemsiz Dosya Aktarım Protokolü
TN	: Gerçek Negatif
Tot_size	: Paket Boyutu (Toplam)
TP	: Gerçek Pozitif
TSA	: Tekrarlayan Sinir Ağı
UDP	: Kullanıcı Datagram Protokolü
UKSB	: Uzun Kısa Süreli Bellek
YSA	: Yapay Sinir Ağı

1. GİRİŞ

Son yıllarda, Nesnelerin İnterneti (IoT - Internet of Things) teknolojisi hızla gelişmiş ve günlük yaşantıdan endüstriyel sistemlere kadar birçok alanda yaygın olarak kullanılmaya başlanmıştır. IoT, fiziksel cihazların internet aracılığıyla birbirleriyle bağlantılı hale gelmesini sağlayarak, akıllı şehirler, sağlık hizmetleri, endüstriyel otomasyon, ulaşım ve tarım gibi sektörlerde büyük bir dönüşüm sağlamaktadır (Kolias ve ark., 2017). Bu dönüşüm, operasyonel verimliliği artırmakta, insan müdahalesini azaltmakta ve süreçlerin otomatikleştirilmesini sağlamaktadır (Sicari ve ark., 2015).

Ancak, IoT cihazlarının hızlı yayılması ve geniş çapta benimsenmesi, beraberinde ciddi güvenlik risklerini de getirmiştir (Weber, 2010). 2030 yılına kadar dünya genelinde yaklaşık 29 milyar IoT cihazının aktif olacağı tahmin edilmektedir (Vailshery, 2023). Bu büyüme, IoT ekosistemine büyük avantajlar sağlarken, aynı zamanda siber saldırılar için geniş bir yüzey alanı oluşturmakta ve güvenlik açıklarını artırmaktadır (Hassija ve ark., 2019).

IoT cihazlarının çoğu, düşük maliyetli üretim nedeniyle güçlü güvenlik önlemleri ile donatılmamaktadır. Bu da onları, Dağıtılmış Hizmet Engelleme (DDoS) saldırıları, kimlik sahtekarlığı (spoofing), kötü amaçlı yazılımlar (malware), kaba kuvvet saldırıları (brute-force) ve Mirai botnet gibi tehditler karşısında savunmasız hale getirmektedir (Mirkovic ve Reiher, 2004; Antonakakis ve ark., 2017). IoT cihazlarının zayıf güvenlik önlemlerinden yararlanarak sistemlere sızılabilmekte, büyük ölçekli veri ihlalleri, hizmet kesintileri ve kritik altyapılara yönelik saldırılar gerçekleştirilebilmektedir (Sadeghi ve ark., 2015). Özellikle kritik altyapılara yönelik saldırılar, büyük ekonomik kayıplara ve operasyonel kesintilere neden olabilmektedir (Fernández-Caramés ve Fraga-Lamas, 2018).

Bu tez çalışması, IoT sistemlerine yönelik siber saldırıları tespit etmek ve analiz etmek amacıyla CICIOT2023 veri setini kullanmayı amaçlamaktadır. CICIOT2023 veri seti, 105 farklı IoT cihazını içeren geniş kapsamlı bir veri kümesi olup, 33 farklı saldırı türünü barındırmaktadır (Sharafaldin ve ark., 2018a). IoT güvenliği üzerine çalışan araştırmacılar için kritik bir kaynak olan bu veri seti, makine öğrenmesi ve derin öğrenme tabanlı saldırı tespit sistemlerinin geliştirilmesi ve test edilmesi açısından büyük bir potansiyele sahiptir.

Bu çalışma kapsamında, makine öğrenimi (MÖ) ve derin öğrenme (DÖ) teknikleri kullanılarak IoT sistemlerine yönelik saldırıların tespit edilmesi ve önlenmesine yönelik

çözümler geliştirilecektir. Çalışmada, farklı saldırı tespit yöntemlerinin performansları karşılaştırılacak ve IoT güvenliğini artırmaya yönelik öneriler sunulacaktır.

1.1. Problemin Tanımı

IoT teknolojisinin hızlı yayılması, cihazların güvenliğini sağlamada önemli zorlukları da beraberinde getirmiştir. IoT cihazları genellikle sınırlı işlem gücü ve düşük enerji tüketimi gibi kısıtlamalara sahiptir, bu da geleneksel güvenlik önlemlerinin uygulanmasını zorlaştırmaktadır (Sadeghi ve ark., 2015). Bunun yanı sıra, çoğu IoT cihazı varsayılan şifrelerle çalışmakta ve düzenli güncellenmemektedir, bu da saldırganlar için kolay bir erişim noktası oluşturmaktadır (Kolias ve ark., 2017). Özellikle akıllı şehirler, endüstriyel sistemler ve sağlık sektöründe kullanılan IoT cihazlarının saldırılara açık olması, büyük ölçekli güvenlik risklerine yol açmaktadır.

IoT ekosisteminde meydana gelen siber saldırılar, bireysel kullanıcılar, kurumsal ağlar ve kritik altyapılar üzerinde ciddi güvenlik tehditleri oluşturmaktadır. Özellikle Dağıtılmış Hizmet Reddi (DDoS) saldırıları, IoT cihazlarının ele geçirilmesiyle oluşturulan botnet ağları aracılığıyla gerçekleştirilmektedir. Bu saldırılar, hedef sistemlerin hizmetlerini devre dışı bırakarak finansal kayıplara, veri ihlallerine ve itibar kayıplarına neden olabilmektedir (Mirkovic ve Reiher, 2004; Antonakakis ve ark., 2017).

Mevcut güvenlik çözümleri, IoT cihazlarının özelliklerine uygun olmadığı için yetersiz kalmaktadır. Geleneksel siber güvenlik sistemleri statik kurallar ve imza tabanlı yöntemler kullanırken, IoT ortamındaki saldırılar dinamik ve sürekli değişen bir yapıya sahip olduğu için bu sistemler etkisiz kalmaktadır (Yang et al., 2022). Bu nedenle, anomali tabanlı ve yapay zekâ destekli saldırı tespit mekanizmalarına ihtiyaç duyulmaktadır (Hassija ve ark., 2019).

1.2. Amaç ve Hedef

Bu çalışmanın temel amacı, CICIOT2023 veri seti kullanılarak IoT sistemlerinde gerçekleşen siber saldırıları analiz etmek, saldırı tespit süreçlerini iyileştirmek ve güvenlik açıklarını belirlemek için makine öğrenimi ve derin öğrenme tekniklerinden faydalanarak etkin çözümler geliştirmektir.

IoT cihazlarının hızlı yayılması, geleneksel güvenlik mekanizmalarının yetersiz kalmasına neden olmakta ve saldırganlara yeni fırsatlar sunmaktadır. Özellikle DDoS,

brute-force, kimlik sahtekarlığı(spoofing) ve Mirai botnet gibi tehditler, IoT ekosisteminde yaygın olarak görülmektedir. Bu çalışmada, IoT sistemlerindeki saldırıları tespit edebilmek için makine öğrenimi ve derin öğrenme modelleri kullanılacak ve bu modellerin performansları karşılaştırılacaktır.

Bu kapsamda, CICIOT2023 veri setinde yer alan DDoS, brute-force, kimlik sahtekarlığı (spoofing) ve Mirai botnet gibi tehdit türleri analiz edilerek saldırı türleri sınıflandırılacaktır. Bununla birlikte, IoT cihazlarının en çok hedef alınan zayıf noktaları ve saldırı vektörleri belirlenecek, böylece saldırganların IoT sistemlerine yönelik en sık kullandığı yöntemler tespit edilecektir.

Makine öğrenimi ve derin öğrenme yöntemleri kullanılarak, CICIOT2023 veri setinden elde edilen özellikler ile saldırıları yüksek doğruluk oranıyla tespit edebilen güvenlik modelleri geliştirilecektir. Bu modellerin etkinliğini değerlendirmek amacıyla Rastgele Orman (Random Forest), Evrimsel Sinir Ağları (CNN) ve Uzun Kısa Süreli Bellek (LSTM) gibi farklı algoritmalar test edilerek performans karşılaştırmaları yapılacaktır.

Son olarak, geliştirilen tespit mekanizmalarının IoT ekosistemlerinde pratik olarak uygulanabilir olup olmadığı değerlendirilecek ve IoT güvenlik sistemlerine entegre edilmesi için öneriler sunulacaktır. Böylece, gerçek dünya kullanımına uygun, güvenilir ve ölçeklenebilir bir saldırı tespit sistemi oluşturulması hedeflenmektedir.

1.3. Tezin Organizasyonu

Tez çalışması beş ana bölümden oluşmaktadır.

Birinci bölümde, IoT sistemlerinde siber saldırıların artan öneminden bahsedilerek, çalışmanın amacı, problemi, hedefleri ve tezin organizasyonu açıklanmıştır.

İkinci bölümde, IoT teknolojisinin temel kavramları, IoT cihazlarının karşılaştığı güvenlik riskleri ve tehditleri ele alınmıştır. Ayrıca CICIOT2023 veri seti tanıtılmış ve mevcut IoT güvenlik çözümleri ve literatürdeki önemli çalışmalar incelenmiştir.

Üçüncü bölümde, kullanılan CICIOT2023 veri setinin içeriği, saldırı türleri, veri setine uygulanan veri ön işleme teknikleri (veri kodlama, sınıf dengesizliğini giderme, normalizasyon ve özellik seçimi) ayrıntılı olarak açıklanmıştır. Makine öğrenmesi algoritmaları (Lojistik Regresyon, Naive Bayes, K En Yakın Komşu, Karar Ağaçları, Rastgele Orman, Gradyan Artırma, Aşırı Gradyan Artırma) ve derin öğrenme yöntemleri (Yapay Sinir Ağları, Evrimsel Sinir Ağları, Tekrarlayan Sinir Ağları ve Uzun Kısa

Sürekli Bellek) hakkında bilgiler verilmiş, modellerin değerlendirilmesinde kullanılan performans ölçütleri anlatılmıştır.

Dördüncü bölümde, çalışmada kullanılan yöntemler ve algoritmalar kullanılarak gerçekleştirilen deneysel analizlerin sonuçları sunulmuş ve elde edilen sonuçlar kapsamlı bir şekilde tartışılarak modellerin etkinliği karşılaştırılmıştır.

Beşinci bölümde ise yapılan çalışmanın genel sonuçları özetlenmiş ve IoT güvenliğinin artırılmasına yönelik öneriler sunularak gelecekte yapılabilecek çalışmalarla ilgili tavsiyelerde bulunulmuştur.



2. KAYNAK ARAŞTIRMASI

Kaynak araştırması iki ana bölümden oluşmaktadır. Bölümler, literatürde yer alan çalışmaların içeriklerine ve kullanılan yöntemlerine göre sınıflandırılmıştır. Birinci bölümde, IoT teknolojisinin temel kavramları ve IoT ile ilgili güvenlik riskleri ele alınmıştır. Bu kapsamda, IoT sistemlerinde karşılaşılan önemli siber tehditler açıklanmış, gerçek dünya örnekleri incelenmiş ve mevcut güvenlik çözümleri ile bunların eksik yönleri değerlendirilmiştir. İkinci bölümde ise literatürde ön plana çıkan araştırmalar detaylı biçimde incelenmiş ve IoT güvenliği konusunda yapılan güncel çalışmaların bulguları özetlenmiştir.

2.1. IoT Teknolojisi ve Güvenlik Riskleri

IoT, fiziksel nesnelerin internet ağı üzerinden birbirleriyle ve merkezi sistemlerle iletişim kurmasını sağlayan bir teknolojidir. Bu teknoloji, cihazların veri toplamasına, paylaşmasına ve analiz edilmesine olanak tanıyarak endüstriden sağlığa, akıllı şehirlerden ev otomasyonuna kadar geniş bir kullanım alanına sahiptir (Weber, 2010). Ancak IoT cihazlarının yaygınlaşmasıyla birlikte siber güvenlik açısından yeni tehditler ve riskler ortaya çıkmıştır (Zhao ve Ge, 2013).

IoT cihazları, genellikle düşük donanım kapasitelerine sahip olup sürekli internete bağlı olduklarından, siber saldırılar açısından savunmasız hale gelebilmektedirler. Bu cihazların büyük bir kısmında güçlü kimlik doğrulama mekanizmalarının bulunmaması, yazılım güncellemelerinin düzenli olarak yapılmaması ve şifreleme yöntemlerinin yetersiz olması, veri güvenliği ihlallerine yol açabilmektedir. Örneğin, Li ve arkadaşlarının (Li ve ark., 2023) çalışmasında, popüler IoT cihazlarının çeşitli siber saldırılara karşı savunmasız olduğu ve bu durumun kullanıcıların günlük yaşamlarını etkileyebileceği belirtilmiştir.

IoT teknolojisi ve güvenlik arasındaki ilişki, güvenilir bir mimari tasarımını zorunlu kılmaktadır. IoT ekosisteminde güvenliği sağlamak için uçtan uca veri şifreleme, güçlü kimlik doğrulama protokolleri, güvenlik yamalarının düzenli olarak uygulanması ve ağ segmentasyonu gibi önlemler alınmalıdır (Zhao ve Ge, 2013). Ayrıca, cihaz üreticilerinin güvenlik standartlarına uyum sağlaması ve kullanıcıların bilinçlendirilmesi, IoT sistemlerinin korunmasında kritik bir rol oynamaktadır.

Sonuç olarak, IoT teknolojisi büyük fırsatlar sunarken, güvenlik riskleri de göz ardı edilmemesi gereken önemli bir konu olarak karşımıza çıkmaktadır. Geliştiricilerin ve kullanıcıların güvenlik önlemlerini dikkate alarak hareket etmeleri, IoT ekosisteminin sürdürülebilirliği açısından hayati önem taşımaktadır (Weber, 2010).

2.1.1. Nesnelerin İnterneti (IoT) Kavramı

IoT, fiziksel cihazların internet bağlantısı aracılığıyla veri toplama, paylaşma ve işleme yeteneği kazanmasını sağlayan bir ekosistemdir. IoT'nin temel amacı, nesneler arasındaki iletişimi artırarak veri odaklı karar alma süreçlerini optimize etmek ve günlük yaşamı kolaylaştırmaktır. Akıllı ev sistemlerinden sanayi otomasyonuna, sağlık hizmetlerinden akıllı şehir projelerine kadar geniş bir kullanım alanına sahip olan IoT, büyük veri analitiği, yapay zeka ve kablosuz iletişim teknolojileri ile entegre edilerek gelişimini sürdürmektedir (Atzori ve ark., 2010; Gubbi ve ark., 2013).



Şekil 2.1. IoT cihazları arasındaki bağlantıyı gösteren temsili görsel

Şekil 2.1’de, Nesnelerin İnterneti (IoT) kapsamında farklı akıllı cihazların internet aracılığıyla birbirine bağlanması temsil edilmektedir. Merkezdeki IoT bulutu, cihazlar arası veri iletişimini simgelerken; çevresindeki simgeler, bu teknolojiye entegre edilebilecek çeşitli cihaz türlerini göstermektedir.

IoT kavramı, ilk olarak 1999 yılında Kevin Ashton tarafından ortaya atılmış olup, fiziksel nesnelerin internet aracılığıyla veri paylaşımında bulunmasını ifade eder. IoT

sistemleri, veri toplama, paylaşma ve işleme işlevlerini yerine getiren dört temel bileşenden oluşur (Atzori ve ark., 2010):

- **Nesneler:** Çevresel verileri toplamak ve iletmek için kullanılan sensörler, akıllı cihazlar ve diğer internet bağlantılı objeler.
- **Ağ Bağlantı Noktaları:** IoT cihazlarının birbirleriyle iletişim kurmasını sağlayan kablosuz veya kablolu ağ altyapıları (örneğin, Wi-Fi, Bluetooth, ZigBee, RFID).
- **Veri İşleme Üniteleri:** Toplanan verileri analiz eden ve anlamlandıran, merkezi sistemler veya uç bilişim (edge computing) altyapıları.
- **İletişim Protokolleri:** IoT cihazlarının veri iletmelerini sağlayan MQTT, CoAP, HTTP gibi protokoller.

Bu yapısal bileşenler, IoT teknolojisinin akıllı ev uygulamaları, endüstriyel otomasyon, sağlık hizmetleri ve akıllı şehir projeleri gibi farklı alanlarda veri odaklı çözümler üretmesine olanak tanımaktadır (Gubbi ve ark., 2013).

IoT'nin sunduğu avantajlar arasında yüksek verimlilik, maliyet tasarrufu ve otomatik karar mekanizmalarının etkinleştirilmesi yer almaktadır. Örneğin, sağlık alanında giyilebilir cihazlar hastaların uzaktan izlenmesini sağlarken; sanayi sektöründe IoT cihazları üretim süreçlerini optimize etmektedir (Güler, 2024).

Bununla birlikte, IoT teknolojisinin hızlı gelişimi beraberinde çeşitli güvenlik tehditlerini de getirmektedir. Düşük işlem gücü ve sınırlı güvenlik özellikleri nedeniyle, IoT cihazları kötü amaçlı yazılımlar, veri ihlalleri ve hizmet reddi (DDoS) saldırıları gibi siber tehditlere karşı savunmasız kalabilmektedir. Bu nedenle, IoT sistemlerinin güvenliğinin sağlanması amacıyla kriptografik yaklaşımlar, makine öğrenimi tabanlı güvenlik çözümleri ve gelişmiş ağ güvenliği mekanizmaları devreye alınmaktadır (Roman ve ark., 2011).

Gelişen yapay zeka, büyük veri ve 5G teknolojileriyle birlikte IoT'nin daha da ileri seviyelere taşınması beklenmektedir. Ancak, bu teknolojinin uzun vadeli başarısını sağlamak için güvenlik önlemlerinin artırılması ve veri mahremiyetinin korunması büyük önem taşımaktadır.

2.1.2. IoT ve Siber Güvenlik Arasındaki İlişki

IoT teknolojisinin yaygınlaşması, yeni siber güvenlik tehditlerini de beraberinde getirmiştir. IoT cihazları, genellikle güçlü güvenlik önlemlerine sahip olmadıkları ve merkezi olmayan bir yapıya sahip oldukları için siber saldırılara açık hale gelmektedir

(Alqahtani ve ark., 2024). Bu nedenle, IoT sistemlerinde veri gizliliği, kimlik doğrulama ve yetkilendirme gibi konular kritik önem taşımaktadır.

IoT cihazlarının güvenliği, şifreleme, kimlik doğrulama ve ağ izleme gibi siber güvenlik önlemleriyle sağlanmaya çalışılmaktadır (Erdal ve Ergüzen, 2020). Ancak, bu cihazların birçoğu düşük işlem kapasitesine sahip olduğundan, geleneksel güvenlik çözümlerinin uygulanmasında zorluklar yaşanmaktadır (El-Sofany ve ark., 2024). Bunun sonucunda, IoT ekosisteminde güvenlik ihlalleri yaygın hale gelmekte ve IoT cihazları standart güvenlik önlemlerine sahip olmadıkları için siber saldırıların hedefi haline gelmektedir (Abomhara ve Køien, 2014)

IoT güvenliği, şu temel konulara odaklanmaktadır:

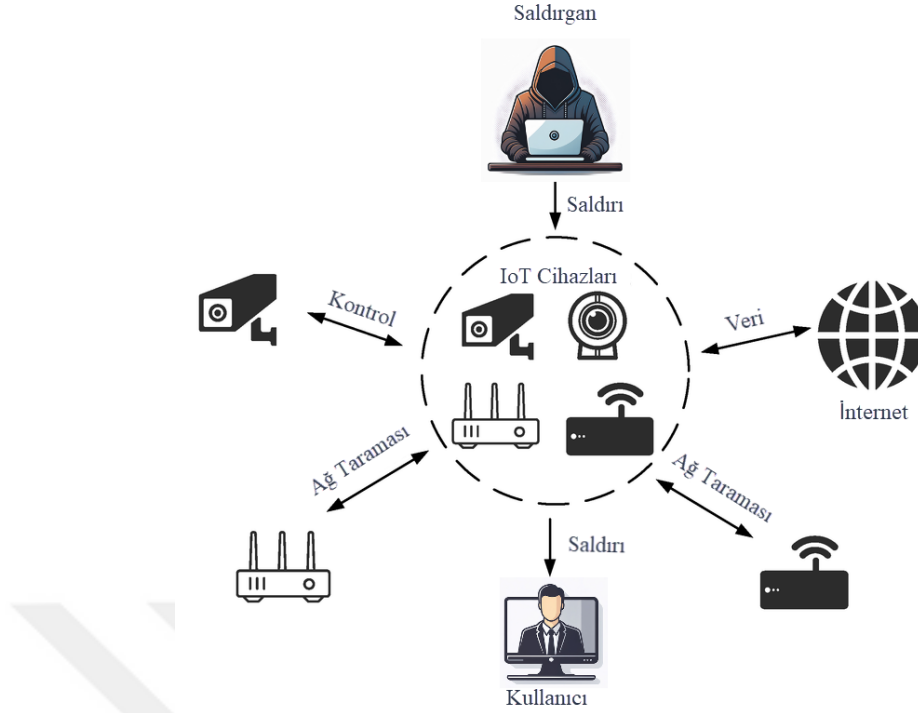
- **Kimlik doğrulama ve yetkilendirme:** IoT cihazlarının yalnızca yetkili kullanıcılar tarafından erişilebilmesini sağlar.
- **Veri şifreleme:** IoT cihazlarından gelen verilerin üçüncü taraflar tarafından ele geçirilmesini önler.
- **Güvenlik güncellemeleri:** IoT cihazları düzenli olarak güncellenmeli ve güvenlik açıkları kapatılmalıdır (Erdal ve Ergüzen, 2020).

Ayrıca, IoT cihazlarının merkezi olmayan yapısı ve farklı üreticiler tarafından geliştirilen çeşitli sistemleri barındırması, güvenlik yönetimini zorlaştırmaktadır. Bu nedenle, IoT güvenliği için özel olarak geliştirilmiş saldırı tespit ve önleme sistemlerine olan ihtiyaç giderek artmaktadır (Ullah ve ark., 2024). Yapay zeka destekli saldırı tespit sistemleri, IoT güvenliğini sağlamak için etkili bir çözüm olarak öne çıkmaktadır (Villegas-Ch ve ark., 2024).

Sonuç olarak, IoT güvenliği, geleneksel bilişim sistemlerinden farklı olarak özel güvenlik önlemleri gerektiren bir alandır. Bu nedenle, IoT cihazlarının güvenliği için hem yazılım hem de donanım bazlı güvenlik mekanizmalarının entegrasyonu önemlidir.

2.1.3. IoT’de Karşılaşılan Siber Tehditler

Günümüzde IoT ekosistemi, hızla gelişen ve genişleyen bir yapı olmakla birlikte, birçok siber güvenlik tehdidine de açık hale gelmiştir. IoT cihazlarının düşük güvenlik önlemleri, geniş ölçekli bağlantıları ve sınırlı kaynakları nedeniyle saldırganlar için cazip bir hedef haline geldiği görülmektedir. Bu bağlamda, en yaygın IoT siber tehditleri aşağıda ele alınmaktadır.



Şekil 2.2. IoT cihazlarına yönelik saldırı yolları ve veri akışı

Şekil 2.2’de, saldırganların IoT cihazlarına nasıl saldırı düzenlediği, ağ taraması yaptığı ve cihazları kontrol altına aldığı gösterilmektedir. Aynı zamanda IoT cihazlarının internet üzerinden veri ilettiği ve kullanıcıların bu sistemlerle etkileşimde bulunduğu bir yapı temsili olarak sunulmuştur.

2.1.3.1. Dağıtık Hizmet Reddi (DDoS) Saldırıları

DDoS (Distributed Denial of Service) saldırıları, IoT cihazlarının kötü amaçlı yazılımlar (botnet’ler) aracılığıyla ele geçirilerek büyük ölçekli hizmet kesintilerine neden olduğu saldırı türlerindendir. Özellikle Mirai Botnet gibi zararlı yazılımlar, IoT cihazlarını hedef alarak geniş çaplı internet kesintilerine yol açabilmektedir (Calp ve Bütünler; Antonakakis ve ark., 2017).

2.1.3.2. Man-in-the-Middle (MitM) Saldırıları

MitM saldırıları, IoT cihazları arasındaki veri iletimini ele geçirerek veya değiştirerek hassas bilgilerin çalınmasına yol açabilir. IoT cihazlarının genellikle güvenli olmayan iletişim protokolleri kullanması, saldırganların cihazlar arası iletişimi manipüle etmesini kolaylaştırmaktadır (Helbig ve ark., 2023; Jony ve Arnob, 2024).

2.1.3.3. Kimlik Avı (Phishing) ve Yetkisiz Erişim

IoT cihazları, genellikle zayıf kimlik doğrulama yöntemleri kullandığından saldırganlar tarafından kimlik bilgileri kolaylıkla ele geçirilebilmektedir. Sahte IoT uygulamaları veya oltalama saldırıları aracılığıyla kullanıcılar kandırılarak erişim bilgileri çalınabilir ve bu durum cihazların kötü niyetli kişiler tarafından kontrol edilmesine sebep olabilir (Abbas ve ark., 2021).

2.1.3.4. Kötü Amaçlı Yazılımlar (Malware)

IoT cihazlarına yönelik kötü amaçlı yazılımlar, veri hırsızlığı, sabotaj veya cihazların botnet ağlarına dahil edilmesi amacıyla kullanılmaktadır. IoT ortamlarında güvenlik açıklarının yaygın olması, kötü amaçlı yazılımların bulaşmasını hızlandırmaktadır (Erdal ve Ergüzen, 2020)

2.1.3.5. Yan Kanal Saldırıları (Side Channel Attacks)

Yan kanal saldırıları, IoT cihazlarının elektromanyetik dalgalar, enerji tüketimi veya işlem süreleri gibi fiziksel özelliklerini analiz ederek şifrelenmiş verilerin ele geçirilmesini amaçlayan saldırılardır. Bu tür saldırılar, özellikle donanım seviyesinde veri güvenliği sağlanmadığında ciddi riskler oluşturabilmektedir (Mithran ve Gopi, 2022).

2.1.3.6. Veri Sızıntısı ve Gizlilik İhlalleri

IoT cihazlarından toplanan büyük miktarda veri, kötü niyetli aktörler tarafından hedef alınabilir ve kimlik hırsızlığı gibi ciddi güvenlik ihlallerine neden olabilir. Bu tür saldırılar, veri şifreleme eksiklikleri ve yetkisiz erişimler sebebiyle yaygın olarak görülmektedir (Abomhara ve Køien, 2014).

2.1.4. IOT Sistemlerine Yapılan Siber Saldırı Örnekleri

IoT sistemleri, geniş dağıtık yapıları, düşük işlem gücüne sahip cihazları ve sürekli internet bağlantıları nedeniyle siber saldırılara karşı savunmasızdır (Khanday ve ark., 2024). IoT, akıllı ev cihazlarından endüstriyel otomasyon sistemlerine, sağlık hizmetlerinden akıllı şehir uygulamalarına kadar geniş bir kullanım alanına sahiptir.

Ancak, cihazların internet üzerinden sürekli bağlantılı olması, siber saldırganlar için yeni güvenlik açıkları yaratmaktadır.

IoT sistemlerine yönelik siber saldırılar; hizmet dışı bırakma saldırıları (DDoS - Distributed Denial of Service), kötü amaçlı yazılım (malware), veri sızıntısı, cihaz ele geçirme (hijacking) ve kimlik sahtekarlığı gibi farklı kategorilere ayrılmaktadır. Bu tür saldırılar, cihazların yetkisiz kişiler tarafından kontrol edilmesine, kişisel ve kurumsal verilerin ele geçirilmesine veya cihazların kötü amaçlarla kullanılarak büyük ölçekli saldırılar düzenlenmesine yol açabilir. Özellikle Mirai botnet saldırısı, IoT güvenliğinin zayıflığını ortaya koyan en önemli örneklerden biridir.

IoT güvenliğinin sağlanamaması yalnızca bireysel kullanıcıları değil, kritik altyapılar, akıllı şehir sistemleri, sağlık hizmetleri ve endüstriyel kontrol sistemleri (ICS) gibi hayati öneme sahip alanları da doğrudan tehdit etmektedir (Narayan ve ark., 2023). Örneğin, sağlık sektöründe kullanılan IoT cihazlarına yapılan saldırılar, hastaların sağlık verilerinin ele geçirilmesine ve hatta tıbbi cihazların işlevsiz hale getirilmesine neden olabilir. Aynı şekilde, akıllı ulaşım sistemlerine yönelik bir siber saldırı, trafik yönetiminde ciddi aksamalara yol açarak büyük ölçekli kazalara sebep olabilir. IoT sistemlerine yönelik gerçekleşmiş bazı önemli siber saldırılar şunlardır:

Stuxnet, 2010 yılında İran'ın Natanz nükleer tesislerini hedef alarak fiziksel altyapıya zarar veren ve siber saldırılar tarihinde ilk dijital silah olarak kabul edilen dikkat çekici bir örnektir. Siemens PLC cihazlarını manipüle ederek santrifüjlerin bozulmasına ve uranyum zenginleştirme sürecinin durmasına neden olan bu saldırı, USB bellekler ve sıfır gün açıklarından yararlanarak yayılmış ve algılanması zorlaştırılmıştır. Endüstriyel kontrol sistemlerindeki (ICS) güvenlik zayıflıklarını hedef alan Stuxnet, aynı zamanda IoT cihazlarında da görülen kod bütünlüğü eksikliği, zayıf kimlik doğrulama ve fiziksel erişim açıkları gibi tehditleri vurgulamaktadır. Bu saldırı, dijital imza doğrulama, düzenli yazılım güncellemeleri ve yapılandırma izleme gibi güvenlik önlemlerinin önemini göstererek endüstriyel IoT sistemlerinin savunmasızlığını açıkça ortaya koymuştur. Stuxnet, IoT sistemlerine yönelik siber saldırıların ne kadar yıkıcı olabileceğini gözler önüne sererek, bu tür tehditlere karşı alınması gereken önlemlerin bir uyarı niteliği taşımaktadır (Langner, 2011).

Mirai botnet, 2016 yılında gerçekleşen ve geniş çaplı DDoS saldırılarıyla dikkat çeken, IoT cihazlarını hedef alan kötü amaçlı bir yazılım olarak öne çıkmıştır. Zayıf güvenlik önlemlerine sahip DVR, IP kamera ve yönlendirici gibi cihazları enfekte eden Mirai, toplamda 600.000'den fazla cihazı ele geçirmiş ve Krebs on Security, Dyn DNS ve

OVH gibi büyük platformlara saldırarak internetin işleyişinde ciddi kesintilere yol açmıştır. Kaynak kodunun yayımlanmasıyla farklı varyantlara dönüşen Mirai, daha etkili tarama yapabilen ve daha karmaşık saldırılar düzenleyebilen bir botnet haline gelmiştir. Varsayılan şifreler ve açık portlar gibi güvenlik zafiyetlerini hedef alan Mirai, IoT ekosisteminin savunmasızlığını gözler önüne sermiştir. Bu olay, IoT cihazlarının güvenliğini artırmaya yönelik yeni standartların ve savunma mekanizmalarının geliştirilmesine öncülük ederek, IoT güvenliğinin kritik önemini bir kez daha vurgulamıştır (Antonakakis ve ark., 2017).

2015 yılında güvenlik araştırmacıları Charlie Miller ve Chris Valasek, Jeep Cherokee'nin Uconnect adlı internet bağlantılı multimedya sistemindeki bir güvenlik açığını kullanarak aracın uzaktan hacklenebileceğini kanıtlamışlardır. Yalnızca aracın IP adresi üzerinden gerçekleştirilen bu saldırı, araştırmacıların radyo, klima, silecekler, hız kontrolü, fren ve motor gibi kritik sistemleri kontrol etmelerine olanak sağlamıştır. Wired dergisi muhabiri Andy Greenberg ile yapılan canlı test sırasında, klimayı ve radyoyu uzaktan çalıştırmışlar, silecekleri devreye sokmuşlar, aracı hızlandırırken frenleri devre dışı bırakmışlar ve motoru durdurarak tehlikeli bir durum yaratmışlardır. Bu olay, modern otomobillerin internet bağlantılı sistemlerinin ciddi güvenlik açıklarına sahip olduğunu gözler önüne sermiştir. Chrysler, bu olayın ardından 1.4 milyon aracı geri çağırması güvenlik yamaları yayımlamıştır. Bu saldırı, otomotiv sektöründe siber güvenlik standartlarının geliştirilmesine yönelik farkındalık yaratarak IoT tabanlı sistemlerde güvenlik önlemlerinin önemini bir kez daha ortaya koymuştur (Jeep, 2015).

2021 yılının Mart ayında, güvenlik kamerası üreticisi Verkada, ciddi bir veri ihlaliyle karşılaşmıştır. Saldırganlar, yanlış yapılandırılmış ve internete açık bir müşteri destek sunucusu üzerindeki yönetici kimlik bilgilerini ele geçirerek şirketin platformuna sızmışlardır. Bu güvenlik açığı, saldırıya uğrayanlara 97 müşteriye ait güvenlik kameralarına uzaktan erişim sağlamıştır ve bu müşterilere ait video, görüntü verileri, sekiz müşterinin erişim kontrol bilgileri (örneğin kart verileri) ve sekiz müşterinin Wi-Fi kimlik bilgileri gibi hassas bilgilerin sızdırılmasına yol açmıştır. Bu ihlal, Verkada'nın yaklaşık 6.000 müşterisinin %2'sinden daha azını etkilemesine rağmen, IoT cihazlarının güvenlik açıklarını bir kez daha gündeme taşımıştır. Saldırıyı hızlı bir şekilde tespit eden Verkada, erişimi engelleyerek etkilenen müşterilere bilgi ve destek sağlamıştır. Şirket, bu olayın ardından güvenlik önlemlerini artırmak için kapsamlı adımlar atmıştır. Bu olay, güvenlik kameraları gibi kritik IoT cihazlarının güvenliğinin sürekli izlenmesi ve güncellenmesi gerektiğini bir kez daha hatırlatmıştır (Verkada, 2021).

2017 yılında, siber saldırganlar bir casinonun internete bağlı akıllı balık tankı termostatındaki güvenlik açıklarını kullanarak kurumun ağına sızmayı başarmışlardır. Termostat, saldırganlar için ağın diğer bölümlerine geçiş sağlayan bir giriş kapısı olarak kullanılmıştır. Bu süreçte saldırganlar, lateral movement (yan hareket) yöntemiyle ödeme sistemleri, müşteri veri tabanları ve çalışan bilgileri gibi kritik sistemlere erişim sağlamışlardır. Çalınan veriler arasında isimler, adresler, bankacılık bilgileri ve kumar alışkanlıkları gibi hassas bilgiler yer almıştır. Saldırganlar, elde ettikleri bu verileri bulut sunucularına transfer etmişlerdir. Bu olay, IoT cihazlarının zayıf güvenlik önlemleriyle donatılmasının ne kadar büyük riskler doğurabileceğini açıkça ortaya koyarak şirketlerin bu cihazların güvenliğini sağlama gerekliliğini bir kez daha hatırlatmıştır (Fish, 2024).

IoT sistemlerine yapılan siber saldırılardan biri olarak Amazon'un Ring güvenlik kameralarına yönelik 2019 yılındaki saldırılar, mahremiyet ve güvenlik sorunlarını açıkça ortaya koymuştur. Saldırganlar, halka açık veri ihlalleri sonucunda ele geçirdikleri e-posta ve şifre kombinasyonlarını kullanarak credential stuffing yöntemiyle kullanıcı hesaplarına giriş yapmışlardır. Zayıf ve yeniden kullanılan şifreler bu saldırıları kolaylaştırmış, hackerlar cihazların kameralarına izinsiz erişim sağlayarak kullanıcıların özel alanlarını ihlal etmişler ve bazı durumlarda mikrofonlar üzerinden tehditlerde bulunmuşlardır. Örneğin, bir kullanıcıdan Bitcoin fidyesi talep edilirken, başka bir olayda bir çocuk taciz edilmiştir. Bu olaylar, IoT cihazlarının güvenlik açıklarını gözler önüne sererken, Ring kullanıcılarının bir kısmında endişe yaratmış ancak cihazların sağladığı kolaylık nedeniyle birçok kullanıcı bu sistemleri kullanmaya devam etmiştir. Şirket, iki faktörlü kimlik doğrulama ve güvenlik panelleri gibi iyileştirmeler sunarak bu tür tehditlere karşı önlemler geliştirmiştir. Bu durum, IoT cihazlarında güçlü ve benzersiz şifrelerin yanı sıra ek güvenlik önlemlerinin uygulanmasının önemini bir kez daha ortaya koymuştur (Ring, 2020).

Satori botnet, 2017 yılında Mirai botnet'in geliştirilmiş bir versiyonu olarak ortaya çıkan ve IoT cihazlarını hedef alan tehlikeli bir siber saldırı aracı olarak dikkat çekmiştir. Huawei yönlendiricilerdeki Universal Plug-and-Play (UPnP) protokolü ve Realtek yazılım geliştirme kitindeki güvenlik açıklarını hedef alarak yayılan Satori, varsayılan kullanıcı adı ve şifre denemek yerine cihazların spesifik güvenlik açıklarını kullanarak etkili ve sofistike saldırılar gerçekleştirmiştir. Saniyede 280.000'den fazla IP adresini tarayabilen Satori, IoT cihazlarını enfekte ederek büyük ölçekli DDoS saldırıları düzenlemiş ve Komut ve Kontrol (C&C) sunucuları aracılığıyla cihazları yönetmiştir. 2018 yılında ortaya çıkan Satori Coin Robber varyantı ise Ethereum madenciliği yapan

yazılımları hedef alarak madencilik havuzlarına erişim sağlamış ve kullanıcıların Ether paralarını çalmıştır. Satori botnet, IoT cihazlarının güvenlik açıklarının ne kadar ciddi tehditler oluşturabileceğini ortaya koyarken, üreticilere güvenlik açıklarını hızla kapatma ve kullanıcıların güçlü parolalar ile cihazlarını koruma gerekliliğini vurgulamıştır. Bu saldırı, IoT cihazlarında düzenli güvenlik güncellemelerinin ve güvenlik standartlarının geliştirilmesinin önemine dair önemli bir uyarı niteliği taşımaktadır (Jin ve ark., 2024).

BrickerBot, 2017 yılında IoT cihazlarını hedef alan ve cihazları kalıcı olarak kullanılamaz hale getiren bir botnet saldırısıdır. Permanent Denial-of-Service (PDOS) adı verilen bu saldırılar, cihazların temel donanım ve yazılımlarını bozarak onarılamaz zararlar vermeyi amaçlamıştır. BrickerBot, Telnet brute force yöntemiyle varsayılan şifreleri kullanarak IoT cihazlarına erişim sağlamış, Linux komutlarıyla cihazların dosya sistemlerini silmiş ve ağ bağlantılarını kesmiştir. Özellikle Linux/BusyBox tabanlı eski yazılımlara ve Telnet portu açık olan cihazlara odaklanarak, Ubiquiti ağ cihazları gibi hedeflerde büyük etkiler yaratmıştır. BrickerBot'un farklı varyantları (örneğin, BrickerBot.1 ve BrickerBot.2) daha hızlı ve kapsamlı saldırılar gerçekleştirmiş, bazen TOR ağı üzerinden gizlilik sağlamıştır. Bu saldırılar, IoT cihazlarının güvenlik açıklarını vurgulayarak güçlü şifrelerin kullanılması, Telnet erişiminin devre dışı bırakılması ve düzenli güvenlik güncellemelerinin yapılması gerektiğini bir kez daha göstermiştir. BrickerBot, IoT sistemlerinin zayıf güvenlik önlemleriyle nasıl büyük zararlar görebileceğini ortaya koyarak, kalıcı zarar veren botnet saldırılarının ciddiyetine dikkat çekmiştir (BrickerBot, 2017).

2020 yılında yapılan bir güvenlik araştırması, Philips Hue akıllı ampullerdeki bir güvenlik açığının sadece bu cihazları değil, aynı zamanda bağlı oldukları ağları da tehdit edebileceğini ortaya koymuştur. Saldırganlar, ZigBee protokolünü kullanan bu ampulleri hedef alarak sahte bir ZigBee ampulü gibi davranmış, cihazın yazılımını değiştirmiş ve köprü (bridge) cihazındaki güvenlik açıklarını istismar etmiştir. Bu saldırılar, yalnızca ampulün kontrolünü ele geçirmekle kalmamış, aynı zamanda ağ üzerinde tam kontrol sağlayarak hassas verilere erişim sağlamıştır. ZigBee protokolündeki bu açıklar, saldırının cihazdan ağa yayılmasını mümkün kılmış ve IoT cihazlarının fiziksel güvenlik risklerinin ötesinde, ağ güvenliği açısından da ciddi tehditler oluşturabileceğini göstermiştir. Bu olay, IoT cihazlarının düzenli yazılım güncellemeleri ve güvenlik yamalarıyla korunmasının, ağ segmentasyonu ile izole edilmesinin ve güvenlik önlemlerinin hızlı bir şekilde uygulanmasının ne kadar önemli olduğunu vurgulamaktadır. Araştırma, akıllı ev sistemlerinin yalnızca kullanım kolaylığı değil,

güvenlik açısından da dikkatli yönetilmesi gerektiğini bir kez daha ortaya koymuştur (Hue, 2020).

IoT sistemlerine yönelik gerçekleşen siber saldırılar, bu teknolojilerin sağladığı kolaylık ve yeniliklerin yanı sıra önemli güvenlik zafiyetlerini de beraberinde getirdiğini açıkça ortaya koymaktadır. Stuxnet'ten BrickerBot'a, Mirai'den Philips Hue saldırılarına kadar birçok örnek, IoT cihazlarının hem bireylerin mahremiyetini hem de kritik altyapıları tehlikeye atabilecek ölçüde kötüye kullanılabileceğini göstermektedir. Bu durum, IoT ekosisteminde yer alan tüm paydaşların – cihaz üreticilerinden son kullanıcılara kadar – güvenlik farkındalığını artırmasını ve daha ciddi önlemler almasını zorunlu hale getirmektedir. Varsayılan şifrelerin değiştirilmesi, düzenli yazılım güncellemelerinin yapılması, ağ segmentasyonu ile cihazların izole edilmesi ve gelişmiş siber güvenlik standartlarının uygulanması, bu tür saldırılara karşı temel savunma hattını oluşturmaktadır. IoT teknolojilerinin hızla yaygınlaştığı günümüzde, güvenlik öncelikli bir yaklaşım benimsenmediği takdirde, daha karmaşık ve yıkıcı saldırıların yaşanması kaçınılmaz olacaktır. Bu bağlamda, IoT sistemlerinin güvenliğinin sağlanması, yalnızca bireylerin mahremiyetini değil, aynı zamanda kritik altyapıların ve toplumsal düzenin korunmasını sağlamak adına stratejik bir gereklilik haline gelmiştir.

2.1.5. Mevcut IoT Güvenlik Çözümleri ve Sınırlamaları

IoT teknolojileri, büyük veri toplama, cihazlar arası iletişim ve otomasyon gibi avantajlar sunsa da, ciddi siber güvenlik riskleri de barındırmaktadır. Bu riskleri azaltmak için çeşitli güvenlik çözümleri geliştirilmiştir. Ancak, IoT cihazlarının donanım ve yazılım kısıtlamaları nedeniyle bu çözümler bazı sınırlamalara sahiptir. IoT güvenliği sağlamak için kullanılan yöntemler arasında şifreleme ve veri koruma, makine öğrenmesi destekli tehdit tespiti, blockchain tabanlı kimlik doğrulama ve güvenlik, güvenli kimlik doğrulama ve çok faktörlü kimlik doğrulama (MFA), bulut tabanlı güvenlik çözümleri gibi yaklaşımlar bulunmaktadır. Hafif şifreleme algoritmaları, IoT cihazlarının işlem kapasitesine uygun olarak veri güvenliğini sağlarken (Carlos A. Rivera A., 2024), makine öğrenmesi tabanlı sistemler, anormal trafik desenlerini analiz ederek siber saldırıları tespit etmektedir (Neto ve ark., 2023). Blockchain teknolojisi, merkeziyetsiz bir güvenlik modeli sunarak veri bütünlüğünü korumakta, kimlik doğrulama süreçlerini güçlendirmektedir (Jena ve ark., 2024). Çok faktörlü kimlik doğrulama (MFA), IoT sistemlerinde yetkisiz erişimi engellemek için etkili bir yöntemdir. Ometov ve

arkadaşlarının belirttiği gibi, MFA'nın IoT uygulamalarında uygulanması bazı zorluklar içerse de, güvenliği artırmada önemli bir rol oynamaktadır (Ometov ve ark., 2019). Bulut tabanlı güvenlik çözümleri ise IoT cihazlarından gelen verileri analiz ederek tehdit tespiti yapmaktadır (Alqahtani ve ark., 2024).

Bu güvenlik çözümleri, bazı sınırlamalara da sahiptir. IoT cihazlarının düşük donanım kapasiteleri, güçlü güvenlik mekanizmalarının uygulanmasını zorlaştırmaktadır (Ji ve ark., 2024). Birçok IoT cihazı, güvenlik güncellemeleri alacak şekilde tasarlanmamış olup, zamanla savunmasız hale gelmektedir (Erdal ve Ergüzen, 2020). IoT sistemlerinin heterojen yapısı, tüm cihazları kapsayan tek tip bir güvenlik standardı belirlemeyi zorlaştırmaktadır (Fei, 2024). Büyük ölçekli IoT sistemlerinde merkezi güvenlik modelleri performans darboğazları oluşturabilmekte (Abiodun ve ark., 2021) ve IoT cihazları tarafından toplanan verilerin üçüncü taraflarca işlenmesi, gizlilik ihlallerine yol açabilmektedir (Alqahtani ve ark., 2024).

IoT ortamlarında güvenlik çözümlerini geliştirmek ve yeni tehditleri analiz edebilmek için büyük veri setlerine ihtiyaç duyulmaktadır. CICIOT2023 Veri Seti, IoT sistemlerinde gerçekleşen siber saldırıları tespit etmek ve analiz etmek için kullanılan en kapsamlı veri kümelerinden biridir. Bu veri seti, farklı IoT bileşenlerinden toplanan çeşitli saldırı türlerini içermekte ve makine öğrenmesi destekli tehdit algılama sistemlerinin etkinliğini test etmek için önemli bir kaynak sunmaktadır (Tseng ve ark., 2024). IoT teknolojileri hayatımıza büyük kolaylıklar getirse de, siber güvenlik tehditleri kritik riskler oluşturmaktadır. IoT cihazlarının güvenliğini sağlamak için şifreleme, kimlik doğrulama, izleme ve güncellemeler gibi birçok teknik kullanılmakta, ancak bu çözümler donanım kısıtlamaları, merkeziyet sorunları ve standart eksiklikleri gibi engellerle karşı karşıya kalmaktadır. CICIOT2023 Veri Seti, IoT ortamlarındaki siber saldırıların analizinde kritik bir rol oynamakta ve gelecekte daha etkili güvenlik mekanizmaları geliştirilmesine olanak tanımaktadır.

2.2. Literatürde Öne Çıkan Çalışmalar

IoT sistemleri, geniş ölçekli bağlantı yapısı nedeniyle güvenlik tehditlerine açık hale gelmektedir. Günümüzde IoT güvenliğini sağlamak amacıyla makine öğrenmesi (MÖ), derin öğrenme (DÖ) ve hibrit yaklaşımlar üzerine yapılan çalışmalar giderek artmaktadır (Wang ve ark., 2024a). Bu bağlamda, CICIOT2023 veri seti, IoT ortamlarında

siber saldırı tespitine yönelik yapılan akademik çalışmalarda yaygın olarak kullanılan en kapsamlı ve güncel veri setlerinden biri haline gelmiştir (Narayan ve ark., 2023).

Bu bölümde, IoT güvenliği üzerine yapılan literatürde öne çıkan çalışmalar, CICIOT2023 veri seti kullanılarak gerçekleştirilen araştırmalar ve farklı saldırı tespit yaklaşımları detaylandırılmaktadır.

Shubh Gupta ve arkadaşları (Gupta ve ark., 2024), IoT cihazlarının güvenlik risklerini ele almak için dinamik oylama mekanizmasına dayalı bir hibrit sınıflandırıcı modeli önermiştir. Çalışmada, Logistic Regression, AdaBoost, Gradient Boosting ve Multi-Layer Perceptron (MLP) gibi modeller birleştirilmiş ve dinamik ağırlıklandırma ile sınıflandırma performansı optimize edilmiştir. Deney sonuçlarına göre, ikili sınıflandırmada (normal vs. saldırı) hibrit model %99.58 doğruluk ve %95.45 F1 skoru elde ederek tek başına kullanılan modellerin performansını aşmış, 8'li sınıflandırmada %99.39 doğruluk, %90.89 geri çağırma ve %83.01 F1 skoru, 34'lü sınıflandırmada ise %98.95 doğruluk, %76.72 geri çağırma ve %72.01 F1 skoru ile en yüksek performansı sağlamıştır. Ayrıca, özellik seçimi için Pearson korelasyonu kullanılarak işlem maliyeti azaltılmış ve modelin ölçeklenebilirliği artırılmıştır. Bu yöntem, IoT güvenliği için büyük ölçekli ortamlarda uygulanabilir esnek bir sistem sunmakta olup, derin öğrenme ile optimize edildiğinde daha karmaşık senaryolara uygun hale getirilebileceği belirtilmektedir.

Ali Alqahtani ve arkadaşları (Alqahtani ve ark., 2024), asimetrik IoT ağlarında ağ trafiğini izlemek ve siber saldırıları sınıflandırmak için bir güvenlik çerçevesi önermiştir. Çalışma, PCA ile veri boyutunu %50 oranında azaltarak işlem maliyetini düşürmüş ve çeşitli makine öğrenimi modellerini kullanarak etkili bir saldırı tespiti sağlamıştır. Veri kümesinde, her sınıftan maksimum 40.000 kayıt alınmıştır. Deney sonuçlarına göre, 34'lü sınıflandırmada LSTM modeli %98.13 doğruluk oranıyla en iyi performansı göstermiştir. PCA yöntemi, boyutları azaltılmış verilerin orijinal verilerle %94.43 oranında benzerlik taşımasını sağlamıştır. Çerçeve, saldırı türlerini etkili bir şekilde sınıflandırırken işlem maliyetlerini optimize etmiş ve ağ trafiğini görselleştirmiştir. Bu yöntem, gerçek zamanlı uygulamalar ve sıfır gün saldırılarını kapsayacak şekilde genişletilmeye uygun bir temel sağlamaktadır.

Vajratiya Vajrobol ve arkadaşları (Vajrobol ve ark., 2024) tarafından geliştirilen bu çalışma, IoT cihazlarını hedef alan Mirai botnet saldırılarının tespiti için yenilikçi bir çözüm sunmaktadır. Araştırmacılar, DNN, CNN, LSTM, LSTM+RandomForest ve LSTM+XGBoost olmak üzere beş farklı makine öğrenmesi ve derin öğrenme

algoritmasını karşılaştırmış ve LSTM ile XGBoost'un hibrit model olarak birleştirilmesinin en yüksek başarıyı sağladığını göstermiştir. CICIOT2023 veri seti kullanılarak eğitilen model, BenignTraffic, Mirai-greeth_flood, Mirai-greip_flood ve Mirai-udpplain olmak üzere dört farklı trafik sınıfını ayırt edebilmiştir. LSTM+XGBoost modeli, normal eğitim sürecinde %97.7 doğruluk oranına ulaşmıştır. Ancak çalışmayı özgün kılan, adversarial training (ters öğrenme) tekniğinin kullanılmasıdır. Adversarial eğitim, modeli Fast Gradient Method (FGM) ile oluşturulan yanıltıcı saldırı örnekleriyle test ederek saldırılara karşı dayanıklılığını artırmaktadır ve modelin gerçek dünya koşullarındaki değişimlere adaptasyonunu geliştirmektedir. Elde edilen sonuçlar, ters öğrenme yaklaşımının normal trafiği %100 doğrulukla tespit ettiğini ve saldırı tespitinde yüksek hassasiyet, geri çağırma ve F1 skorları sağladığını göstermektedir. Çalışma, LSTM'nin zamansal bağımlılıkları yakalama yeteneği ile XGBoost'un güçlü sınıflandırma performansını birleştirerek IoT güvenliğine önemli bir katkı sunmaktadır. Araştırmacılar, gelecekte modelin yeni gelişen Mirai varyantlarına karşı adaptif hale gelebilmesi için online öğrenme algoritmalarının entegrasyonunu önermektedir.

Xiao Wang ve arkadaşları (Wang ve ark., 2024b) bu çalışmada, IoT ağlarında siber saldırıları tespit etmek için derin öğrenme tabanlı bir ağ saldırı tespit sistemi geliştirmiştir. Model, ağ trafiğinin zamansal ve mekânsal özelliklerini çıkarmayı hedeflerken, veri dengesizliği sorununu çözmek için Koşullu Tablo Oluşturma Karşıt Ağ (CTGAN) kullanılmıştır. UNSW-NB15, CIC-IDS2018 ve CIC-IOT2023 veri setleri üzerinde test edilen model, sırasıyla %91.08, %94.55 ve %97.47 doğruluk oranlarına ulaşmıştır. Araştırma, önerilen derin öğrenme tabanlı sistemin IoT ortamlarında çok sınıflı ağ saldırılarını tespit etmede etkili bir çözüm sunduğunu göstermektedir. Bu yöntem, siber güvenlik tehditlerine karşı IoT ağlarının korunmasında güçlü bir araç olarak değerlendirilmektedir.

Raghavendra Narayan ve arkadaşları (Narayan ve ark., 2023), IoT ortamlarında siber saldırıların tespiti için makine öğrenimi tabanlı zekâ temelli bir izinsiz giriş tespit sistemi (IIDS) geliştirmiştir. CICIOT2023 veri seti kullanılarak oluşturulan bu çerçevede, dengesiz veri seti sorunlarını gidermek amacıyla özellik seçimi ve sınıf dengeleme teknikleri bir arada uygulanmıştır. Araştırmacılar, özellik seçimi için CFS (Correlation-based Feature Selection) ve RF-MRMR yöntemlerini kullanmıştır. CFS yöntemi, Weka aracı kullanılarak uygulanmış ve 46 orijinal özellik arasından sınıf etiketleriyle en yüksek korelasyona ve kendi aralarında düşük korelasyona sahip 6 özellik seçilmiştir. RF-MRMR ise Recursive Feature Elimination (RFE) yöntemiyle seçilen en iyi 25 özellik ile

Minimum Redundancy Maximum Relevance (mRMR) yöntemiyle seçilen en iyi 25 özelliğin kesişimi alınarak belirlenen 11 özellikten oluşan bir yöntemdir. Sınıf dengeleme için ise Random Oversampling (ROS) ve Balanced Random Forest Classifier (BRFC) teknikleri yalnızca eğitim verilerine uygulanmıştır. Random Forest algoritması temel sınıflandırıcı olarak kullanılmıştır. Araştırma sonuçlarına göre, önerilen CFS+BRFC modeli, temel modele kıyasla %3.72 precision, %3.75 recall ve %4.69 F1 skoru artışı sağlamış, genel doğruluk oranı %99.23 olarak elde edilmiştir. Özellikle, F1 skoru %99'dan düşük olan "doygunluğa ulaşmamış sınıflarda" %7.9'luk bir iyileşme sağlanmıştır. Bu çalışma, dengesiz veri setlerindeki azınlık sınıflarının tespitini iyileştirerek IoT ağlarında sıfır gün saldırıları da dahil olmak üzere siber tehditlerin erken tespiti için güçlü ve etkili bir yaklaşım sunmaktadır. Özellikle sözlük saldırıları (Dictionary Brute Force), tarayıcı ele geçirme (Browser Hijacking) ve SQL enjeksiyonu gibi az rastlanan ancak kritik saldırıların tespitinde önemli iyileştirmeler sağlanmıştır.

Shahbaz Ahmad Khanday ve arkadaşları (Khanday ve ark., 2024) tarafından yapılan çalışmada, IoT cihazları için hafif ve etkili bir saldırı tespit modeli önerilmiştir. CIC-IoT2023 veri seti kullanılarak yapılan çalışmada, veri sınıfları SMOTE ile dengelenmiş ve Extra Tree Classifier ile önemli özellikler seçilmiştir. Model, 1D-CNN ve LSTM algoritmalarını içermektedir. Araştırma sonuçlarına göre, 1D-CNN %99.87 doğruluk, %100 kesinlik (precision) ve %99 geri çağırma (recall) oranıyla en iyi performansı sergilerken, LSTM %92 doğrulukla daha düşük bir başarı göstermiştir. Önerilen model, IoT saldırı tespiti için yüksek doğruluk ve düşük işlem yüküyle etkili bir çözüm sunmaktadır.

Nimisha Pandey ve Pramod Kumar Mishra (Pandey ve Mishra, 2025), IoT ağlarındaki DDoS saldırılarını tespit etmek için koşullu entropi tabanlı hibrit bir makine öğrenimi modeli geliştirmiştir. Model, entropi analizi ve hibrit sınıflandırıcı yaklaşımını birleştirerek, CatBoost, Random Forest, Extra Trees ve LightGBM algoritmalarının sonuçlarını ikinci aşamada Logistic Regression ile birleştirmiştir (Stacking Generalization). CIC-IoT2023 veri seti üzerinde yapılan deneylerde, model %99.86 doğruluk oranına ulaşmış ve önceki çalışmalardan daha yüksek performans göstermiştir. Çalışma ayrıca, saldırı ve normal trafik arasındaki farkı ölçmek için beş farklı mesafe metriğini karşılaştırmış ve bilgi mesafesi (Information Distance) metriğinin en etkili sonucu verdiğini göstermiştir. Bu araştırmada 11 farklı DDoS saldırı türü, sınıflandırma modelinde tek bir "saldırı" kategorisi olarak ele alınmış ve normal trafik ile

karşılaştırılmıştır. Bu çalışma, ağ trafiği analizinde entropi tabanlı metriklerin önemini vurgulamakta ve IoT ortamında saldırı tespiti için etkili bir çözüm sunmaktadır.

Neto ve arkadaşları (Neto ve ark., 2023), IoT güvenlik analitiği uygulamalarını desteklemek amacıyla, 105 gerçek IoT cihazından oluşan geniş bir topoloji kullanarak 7 farklı kategoride 33 saldırı türünü içeren kapsamlı bir veri seti olan CICIoT2023'ü sunmuştur. Bu veri seti, saldırıların gerçek IoT cihazları tarafından gerçekleştirilmesi özelliğiyle literatürdeki diğer çalışmalardan ayrılmakta olup, toplam 548 GB ağ trafiği verisinden DPKT paketi kullanılarak 47 özellik çıkarılmıştır. Akış süresi, başlık uzunluğu, protokol türü, TTL, aktarım hızı, bayrak değerleri ve çeşitli istatistiksel ölçümleri içeren bu özellikler, veri setinin hem pcap formatında ham veri hem de CSV formatında işlenmiş olarak sunulmasını sağlamıştır. Çalışmada, IoT güvenliği açısından kritik olan kötü amaçlı trafik tespitine yönelik olarak Lojistik Regresyon, Perceptron, Adaboost, Rastgele Orman ve Derin Sinir Ağı olmak üzere beş farklı makine öğrenmesi algoritması üç farklı sınıflandırma senaryosunda değerlendirilmiştir: ikili sınıflandırma (kötücül/iyi huylu), 8 sınıflı gruplandırma (7 saldırı kategorisi + normal trafik) ve 34 sınıflı detaylı sınıflandırma (33 saldırı türü + normal trafik). Deneysel sonuçlar, Rastgele Orman ve Derin Sinir Ağı modellerinin tüm senaryolarda en yüksek performansı gösterdiğini ortaya koyarken, ikili sınıflandırmada tüm modeller %98'in üzerinde doğruluk oranına ulaşmıştır. 8 sınıflı kategorik sınıflandırmada Rastgele Orman %99.44 doğruluk ve %71.93 F1 skoru, Derin Sinir Ağı ise %99.11 doğruluk ve %69.73 F1 skoru elde ederken, 34 sınıflı detaylı sınıflandırmada Rastgele Orman %99.16 doğruluk ve %71.40 F1 skoru, Derin Sinir Ağı ise %98.61 doğruluk ve %67.23 F1 skoru ile başarılı sonuçlar vermiştir. Sınıf sayısının artmasıyla Lojistik Regresyon, Perceptron ve Adaboost modellerinin performansında belirgin bir düşüş gözlemlenirken, Rastgele Orman ve Derin Sinir Ağı modelleri yüksek başarı oranlarını korumuştur. DDoS, DoS ve Mirai saldırıları yüksek doğrulukla tespit edilirken, Web tabanlı saldırılar ve Brute Force saldırılarının sınıflandırılması daha zorlu olmuştur. Bu çalışma, sunduğu kapsamlı veri seti ve detaylı performans analizi ile IoT güvenlik çözümlerinin geliştirilmesine önemli bir katkı sağlamanın yanı sıra, model optimizasyonu, özellik analizi ve farklı veri setleri ile karşılaştırmalı çalışmalar için temel oluşturmaya uygun bir kaynak niteliği taşımaktadır.

Akinul Islam Jony ve Arjun Kumar Bose Arnob (Jony ve Arnob, 2024) bu çalışmada, IoT ortamlarında siber saldırıları tespit etmek için LSTM tabanlı bir model geliştirmiştir. Model, ağ trafiğinin zamansal ve mekânsal özelliklerini etkili bir şekilde

analiz ederek, IoT cihazlarının güvenliğini artırmayı hedeflemektedir. CIC-IoT2023 veri seti üzerinde gerçekleştirilen deneylerde, model %98.75 doğruluk , %98.59 F1 skoru ve hassasiyeti %98.66 olarak elde etmiştir. Çalışma, özellikle IoT ağlarında yeni tehditleri tespit etmek için LSTM'nin güçlü bir araç olduğunu vurgulamakta ve IoT güvenliğini sağlamak için yenilikçi bir çözüm sunmaktadır.

Chandan Kumar ve Md. Sarfaraj Alam Ansari (Kumar ve Ansari, 2024), Software-Defined IoT (SD-IoT) uygulamalarında güvenlik tehditlerini tespit etmek için açıklanabilir ve hafif bir saldırı tespit sistemi geliştirmiştir. Önerilen sistemde, gereksiz özellikleri eleyerek modelin etkinliğini artırmak amacıyla Sheep Flock Optimization Algorithm (SFOA) ve Least Absolute Shrinkage and Selection Operator (LASSO) yöntemleri birleştirilmiştir. Ayrıca, model tahminleri Shapley Değerleri (SHAP) kullanılarak açıklanabilir hale getirilmiş ve güvenlik uzmanlarının saldırı modellerini daha iyi anlaması sağlanmıştır. Sistem, SD-IoT veri setinin yanı sıra CIC-IoT2023 veri seti üzerinde de test edilmiş olup, CIC-IoT2023 veri setinde 8 özellik kullanılarak yapılan ikili sınıflandırma testlerinde yüksek performans elde edilmiştir. SFOA-LASSO yaklaşımıyla oluşturulan Karar Ağacı (DT), Rastgele Orman (RF) ve XGBoost modelleri yaklaşık %99.5 doğruluk oranına ulaşırken, Çok Katmanlı Algılayıcı (MLP) modeli yaklaşık %99 doğruluk sağlamıştır. Bu sonuçlar, geliştirilen hafif ve açıklanabilir saldırı tespit sisteminin farklı veri setleri üzerinde de etkin çalıştığını göstermektedir. Genel olarak, önerilen sistem minimal özelliklerle güçlü bir performans sergileyen, açıklanabilir ve düşük maliyetli bir güvenlik çözümü sunarak IoT ortamlarında siber tehditlere karşı etkili bir koruma sağlamaktadır.

Farhan Ullah ve arkadaşları (Ullah ve ark., 2024), IoT güvenliği için multimodal büyük veri temsili, transfer öğrenimi ve oyun teorisini birleştiren bir Ağ Saldırı Tespit Sistemi (IDS) önermiştir. Çalışmada, ağ baytlarını gri tonlamalı görsellere dönüştürerek metin ve görsel özellikleri entegre eden bir yaklaşım sunulmuş ve CNN-LSTM modeli kullanılmıştır. Deney sonuçları, CNN-LSTM modelinin %96,4'lük doğruluk oranıyla IoT tabanlı saldırıları tespit etmede en iyi performansı sağladığını göstermiştir. Oyun teorisi çerçevesinde Nash Dengesi kullanılarak IDS'nin güvenilirliği artırılmış, metin ve görsel özelliklerin entegrasyonu ile saldırı tespit oranları yükseltilmiştir. Önerilen yaklaşım, farklı veri setlerinde test edilmiş ve multimodal yöntemlerin IoT güvenliği için etkili sonuçlar sağladığı kanıtlanmıştır.

T. Niu ve arkadaşları (Niu ve ark., 2024) bu çalışmada, IoT ortamlarında kötü amaçlı trafik tespit etmek için Docker tabanlı, ölçeklenebilir ve gizliliği koruyan bir

mimari geliřtirmiřtir. alıřmada, veri paketlerinin ilk 128 baytlık veri yk kısmı kullanılmıř ve bu veriler modelin zellik ıkarma kabiliyetini artırmak iin ikili kodlama ile kodlanmıřtır. Model, farklı IoT cihazlarından gelen verileri yerel olarak eęitmek iin federe ęrenme/kenar hesaplama yaklařımını kullanmaktadır. Bu yntemle, veriler cihazda tutulur ve yalnızca model parametreleri merkezi bir sunucuya gnderilir. Nihai model parametreleri, IPFS dosya depolama sisteminde saklanırken, ilgili hash deęeri blockchain'de tutularak geniřleme sırasında model parametrelerinin doęruluęu saęlanmıřtır. Deneyler, Docker ortamında CIC-IoT2022 ve CIC-IoT2023 veri setleri kullanarak gerekleřtirilmiř ve nerilen mimarinin bilinen anormal trafięi %98.6 n-eęitim doęruluęuyla, bilinmeyen kt amalı trafięi ise %79 doęruluk oranıyla tespit ettięi grlmřtr. Birka eęitim turu sonrasında, bu doęruluk oranları sırasıyla %99.5 ve %89.4'e ykselmiřtir. Ayrıca, model geniřleme sırasında da gl performans sergilemiřtir. Docker tabanlı yapı sayesinde model, IoT cihazlarına kolayca daęıtılabilir ve byyen IoT aęlarına uyum saęlayabilir. alıřma, IoT gvenlięi iin yksek doęruluklu, gizlilięi koruyan ve leklenebilir bir czm sunmaktadır.

Gehad Ismail Sayed ve Aboul Ella Hassanien (Sayed ve Hassanien, 2024), IoT ve Metaverse aęlarında siber saldırıları tespit etmek iin Rough Set tabanlı Electric Eel Foraging Optimization (RSEFO) algoritması ve AdaBoost sınıflandırıcısıyla optimize edilmiř bir akıllı saldırı tespit sistemi (IIDS) geliřtirmiřtir. CIC-IoT-2023 veri setinde benign traffic iin %99.7, DDoS iin %100, brute force iin %100, spoofing iin %99.8, DoS iin %100, Mirai iin %100, recon iin %99.8 ve web-based saldırılar iin %100 doęruluk oranları elde edilmiřtir. Model, one-vs-all yaklařımıyla ok sınıflı sınıflandırmayı gerekleřtirmiř ve Random Over-Sampling (ROS) yntemiyle sınıf dengesizlięi sorununu ele almıřtır. zellikle, RSEFO algoritması her saldırı tr iin optimal zellik alt kmesini belirleyerek (benign traffic iin 28, DDoS iin 22, brute force iin 17, spoofing iin 18, DoS iin sadece 1, recon iin 11, web-based iin 17 ve Mirai iin 20 zellik) sınıflandırma performansını nemli lde artırmıřtır.

Viet Anh Phan ve arkadařları (Phan ve ark., 2024) tarafından yapılan bu alıřmada, IoT aęlarında saldırı tespiti iin birden fazla zellik seimi ynteminin etkinlięi karřılařtırılmıřtır. Arařtırmada CIC-IoT2023 veri seti kullanılmıř ve Random Forest (RF), Recursive Feature Elimination (RFE), Logistic Regression (LR), XGBoost ve Information Gain (IG) yntemleriyle eřitli zellik seimi teknikleri incelenmiřtir. CIC-IoT2023 veri setindeki 33 farklı IoT saldırı tr, sınıflandırmayı daha etkili hale getirmek iin 7 ana kategoriye (DDoS, DoS, Brute Force, Spoofing, Recon, Web-based

ve Mirai) ayrılmıştır. Özellik seçimi yöntemleri, Decision Tree (DT), Random Forest (RF), k-Nearest Neighbors (k-NN), Gradient Boosting (GB) ve Multi-layer Perceptron (MLP) gibi makine öğrenimi algoritmalarıyla entegre edilmiş ve 5, 15 ve 30 özellikli senaryolar karşılaştırılmıştır. Sonuçlara göre, RFE yöntemi özellikle RF modeliyle birlikte en yüksek doğruluk oranına (%99.57) ulaşmıştır ve RF, %83'ten %99.56'ya varan doğruluk oranlarıyla en kararlı performansı gösteren özellik seçimi yöntemi olmuştur. Ayrıca, sınırlı kaynaklara sahip IoT cihazları için 5 özellik içeren minimal bir model önerilmiş ve bu durumda RFE ile RF modelinin (%99.45 doğruluk) en etkili kombinasyon olduğu gösterilmiştir. Özellik sayısını azaltmak, veri seti boyutunu %12.77'ye kadar düşürerek (12.8 GB yerine 1.64 GB) IoT cihazlarında etkili saldırı tespit sistemlerinin uygulanmasını mümkün kılmaktadır. Çalışma, IoT ortamlarında siber saldırıların tespiti için düşük maliyetli ve yüksek doğruluk sağlayan optimize edilmiş çözümler sunmaktadır.

Ram Ji ve arkadaşları (Ji ve ark., 2024), siber-fiziksel sistemlerde (CPS) karşılaşılan karmaşık siber tehditlerin tespiti için iki yenilikçi topluluk öğrenme tabanlı saldırı tespit modeli geliştirmiştir. İlk model olan CNN-GWO-Voting, çok sınıflı sınıflandırma yaklaşımı olup, Convolutional Neural Network (CNN) ile özellik çıkarımı yaparak Gray Wolf Optimization (GWO) algoritmasıyla en uygun 15 özelliği seçmiş ve Soft Voting Ensemble yaklaşımıyla dört temel sınıflandırıcının (Random Forest, SVM, Decision Tree ve XGBoost) tahminlerini birleştirmiştir. Bu model, CIC-IoT-2023 veri setinde %99.15 doğruluk, 0.99 hassasiyet, 0.99 duyarlılık, 0.99 F1-skoru ve 0.008 yanlış pozitiflik oranıyla dikkat çekici bir başarı elde etmiştir. İkinci model ise ikili sınıflandırma yapan Hibrit Ensemble Modelidir. Bu model, Logistic Regression, SVM, Naïve Bayes, K-NN ve MLP gibi farklı baz sınıflandırıcıları bir araya getirerek çeşitli topluluk teknikleri (Voting, Stacking, Bagging, Boosting) kullanmaktadır. Hibrit modelde en iyi sonuçlar Boosting tekniğiyle elde edilmiş, %98.16 doğruluk, 0.99 hassasiyet, 0.98 duyarlılık ve 0.98 F1-skoru değerlerine ulaşılmıştır. Her iki model de yüksek doğruluk ve düşük yanlış pozitiflik oranıyla CPS ortamları için etkili ve ölçeklenebilir çözümler sunarken, özellikle CNN-GWO-Voting modeli, optimize edilmiş özellik kümesi sayesinde hesaplama karmaşıklığını azaltarak hızlı ve etkili bir yaklaşım sağlamaktadır.

Sidra Abbas ve arkadaşları (Abbas ve ark., 2023), IoT altyapılarında siber saldırıları tespit etmek için federated learning (FL) tabanlı yenilikçi bir yaklaşım geliştirmiştir. Önerilen model, iki istemci ve bir sunucudan oluşan bir mimaride

çalışmakta olup, her istemci kendi verisiyle modeli ayrı ayrı eğitmekte ve sunucu güncellemeleri birleştirerek global modeli oluşturmaktadır. CIC-IoT2023 veri setinde yapılan çalışmada, veri hazırlama aşamasında SMOTE tekniği ile veri dengelemesi ve MinMaxScaler ile özellik normalizasyonu uygulanmıştır. 46 giriş özelliği ile tasarlanan federated deep neural network (DNN) modeli, ReLU aktivasyon fonksiyonlu gizli katmanlar ve sigmoid aktivasyonlu çıkış katmanı içermektedir. Önerilen yaklaşım, %99 doğruluk, kesinlik, geri çağırma ve F1 skoru elde ederek etkinliğini kanıtlamıştır. Bu yöntem, istemciler arasında doğrudan veri paylaşımı gerektirmeden, veri gizliliğini koruyarak ve sunucunun işlem yükünü azaltarak IoT cihazları için etkili bir saldırı tespit sistemi sağlamaktadır.

Kai Yang ve arkadaşları (Yang ve ark., 2024), Endüstriyel Nesnelerin İnterneti (IIoT) alanında saldırı trafiğini tespit etmedeki düşük doğruluk, yüksek boyutlu ve karmaşık saldırı trafiğindeki özellik fazlalığı ve dengesiz veri setlerinde yaygın kategorileri öğrenme eğilimi gibi üç temel sorunu ele alan NIDS-BAI adlı gelişmiş bir saldırı tespit modeli önermiştir. Model, dikkat mekanizmaları, Çift Yönlü Geçitli Tekrarlayan Birim (BiGRU) ve Başlangıç-Evrişimli Sinir Ağını (Inception-CNN) birleştirerek saldırı tespit oranını artırırken, ADASYN ve RENN algoritmalarını içeren ARL karma örnekleme stratejisi ile veri dengesizliği sorununu çözmekte ve LOF algoritması ile olası gürültüleri gidermektedir. Özellik seçimi için Pearson korelasyon katsayısı ve Rastgele Orman algoritmasını birleştiren RF-P yöntemi ile gereksiz özellikleri eleyerek kritik özelliklere odaklanan model, tespit doğruluğunu önemli ölçüde artırmaktadır. Edge-IIoTset, CIC-IDS2017 ve CIC IoT 2023 olmak üzere üç uluslararası veri seti üzerinde yapılan testlerde, NIDS-BAI modeli özellikle CIC IoT 2023 veri setinde %99.5 doğruluk oranı elde ederek üstün performans sergilemiş ve mevcut yaklaşımların çoğunu geride bırakmıştır. Bu sonuçlar, önerilen modelin IIoT ağlarında güvenlik tehditlerini tespit etmede etkili bir çözüm sunduğunu göstermektedir.

Al-Na'amneh ve arkadaşlarının (Al-Na'amneh ve ark., 2024) çalışmasında, IoT ağlarında hizmet reddi (DoS) ve dağıtılmış hizmet reddi (DDoS) saldırılarını gerçek zamanlı olarak tespit etmek amacıyla Convolutional Neural Network (CNN) ve Support Vector Machine (SVM) algoritmalarını birleştiren hibrit bir model geliştirmiştir. Üç farklı sınıfı ayırt etmeye odaklanan model, DDoS, DoS ve Benign (zararsız/normal trafik) kategorilerini başarılı bir şekilde sınıflandırmaktadır. Üç evrişimsel, üç maksimum havuzlama ve iki tam bağlı katmandan oluşan sekiz katmanlı CNN mimarisi, ağ trafiğinden önemli özellikleri çıkarırken, SVM bu özellikleri analiz ederek trafiğin hangi

kategoriye ait olduğunu yüksek doğrulukla belirlemektedir. Kanada Siber Güvenlik Enstitüsü'nün (CIC) IoT 2023 veri seti üzerinde test edilen model, %99.8 doğruluk, %100 kesinlik, %99 duyarlılık ve %99 F1-skoru elde ederek, SVM, KNN, Naïve Bayes ve Lojistik Regresyon gibi geleneksel makine öğrenimi yöntemlerine kıyasla üstün bir performans göstermiştir. Modelin sağlamlığını değerlendirmek amacıyla ToN-IoT veri seti üzerinde yapılan ek testlerde de %99.85 doğruluk oranına ulaşılmış ve farklı veri kümelerinde tutarlı bir başarı sergilediği kanıtlanmıştır. Ölçeklenebilirlik sorunlarını ele almak adına model sıkıştırma, budama ve dağıtılmış hesaplama tekniklerinden faydalanılarak IoT cihazları için daha verimli bir güvenlik çözümü sunulmuştur. Hibrit derin öğrenme yöntemlerinin IoT güvenliğini güçlendirme potansiyelini vurgulayan çalışma, 0.999 AUC değeriyle mükemmel bir sınıflandırma performansı sunduğunu da ortaya koymuştur.

Wang ve arkadaşlarının (Wang ve ark., 2024a) çalışmasında, Endüstriyel Nesnelerin İnterneti (IIoT) ağlarının güvenliğini artırmak için Federated Learning (FL) tabanlı bir ağ saldırı tespit sistemi olan NIDS-FGPA modeli geliştirilmiştir. Model, eksik veri özellikleri, eksik etiketler, parametre sızıntısı ve yüksek iletişim yükü gibi mevcut saldırı tespit sistemlerinin karşılaştığı zorlukları ele alırken, gradyan benzerliğine dayalı model birleştirme algoritması (Gradient Similarity Model Aggregation - GSA) kullanarak yerel modellerin dinamik ağırlıklandırılmasını ve yüksek kaliteli güncellemelerin seçilmesini sağlamış, böylece iletişim yükünü %22-%51 oranında azaltarak daha hızlı model yakınsaması sunmuştur. Non-IID (bağımsız ve özdeş olmayan dağılımlı) verilerin olumsuz etkilerini azaltarak federe öğrenme sisteminin performansını artıran model, ağ trafiği verilerini gri tonlamalı görüntülere dönüştürerek iki boyutlu konvolüsyonel sinir ağları (2D-CNN) ve çift yönlü kapılı tekrarlayan üniteler (BIGRU) kombinasyonu ile ağ trafiğindeki mekânsal ve zamansal özelliklerin etkin bir şekilde çıkarılmasını sağlamış ve geleneksel derin öğrenme modellerinin eksik veri özelliklerini işleme konusundaki sınırlamalarını aşmıştır. Modelin etkinliği Edge-IIoTset ve CIC IoT 2023 veri setlerinde test edilmiş ve sırasıyla %94.5 ve %99.2 doğruluk oranlarına ulaşarak FedNova, FedAvg, SVM, KNN, DNN, BiLSTM ve DL-BiLSTM gibi mevcut modellerden daha üstün performans göstermiştir. FL mimarisine entegre edilen Paillier homomorfik şifreleme teknolojisi sayesinde model parametreleri güvenli bir şekilde paylaşılmış ve veri gizliliği korunarak saldırganların kaynak verileri çıkarsama risklerine karşı koruma sağlanmıştır. Elde edilen sonuçlar, NIDS-FGPA'nın karmaşık ağ saldırılarını tanımlama ve yakalama kabiliyetine sahip olduğunu, böylece ağın genel güvenliğini önemli ölçüde artırdığını

ortaya koymaktadır. Bu çalışma, ağ saldırı tespiti etkinliğini artırma ve veri güvenliğini koruma açısından yenilikçi bir çözüm sunmaktadır.

Emanuel Krzysztoń ve arkadaşlarının (Krzysztoń ve ark., 2024) çalışmasında, IoT ağlarında anomali tespitini optimize etmek amacıyla çeşitli makine öğrenmesi (MÖ) teknikleri karşılaştırılmış ve IoT-23 ile CIC-IoT 2023 veri setleri üzerinde test edilerek farklı yöntemlerin performansları analiz edilmiştir. Çalışmada kullanılan temel modeller arasında Random Forest (RF), Autoencoder (AE) ve Isolation Forest (IF) yer almakta olup, ikili sınıflandırma (normal/anomali) bağlamında yapılan deneylerde RF, IoT-23 veri setinde %99.99 doğruluk ve %100 F1-Skoru, CIC-IoT 2023 veri setinde ise %99.45 doğruluk ve %99.45 F1-Skoru ile en yüksek başarıyı göstermiştir. AE modeli, IoT-23 veri setinde %99.26 doğruluk ve %98 F1-Skoru, CIC-IoT 2023'te ise %98.76 doğruluk ve %99 F1-Skoru elde ederken, IF modeli IoT-23'te %100 F1-Skoru yakalamasına rağmen CIC-IoT 2023'te %64 F1-Skoru ile daha düşük performans sergilemiştir. Çalışmada ayrıca, DDoS, Mirai, SQL Injection, MITM gibi farklı saldırı türlerinin tespitine yönelik çok sınıflı analizler gerçekleştirilmiştir. Özellik mühendisliği sürecinde, IoT-23 veri setindeki 83 özellikten 12'sine indirgeme yapılırken, CIC-IoT 2023'te başlangıçta 47 özellik bulunmakta olup, çeşitli seçim yöntemleri (RFE, IGR, CFS, GSK) ile azaltılmış ancak kesin sayı belirtilmemiştir. Deneyler, 10-15 özellik kullanımının en iyi sonuçları verdiğini göstermektedir. Bulgular, RF ve AE modellerinin IoT ağlarında anomali tespiti için yüksek doğruluk oranlarına sahip olduğunu ortaya koyarken, IF modelinin performansının veri setine bağlı olarak değişkenlik gösterdiğini işaret etmektedir. Çalışma, merkezi makine öğrenmesi yerine federated learning gibi dağıtılmış yöntemlerin IoT güvenliği açısından avantajlarını vurgularken, veri ön işleme, özellik seçimi ve hiperparametre optimizasyonunun model başarısı üzerindeki kritik rolünü ortaya koymaktadır.

CICIoT2023 veri seti ile yapılan çalışmalar, IoT güvenliği için önemli ilerlemeler sağlamış olup, gelecekte daha gelişmiş, ölçeklenebilir ve gerçek zamanlı çözümler üzerine araştırmaların devam etmesi beklenmektedir (Taşcı, 2024). Makine öğrenmesi ve derin öğrenme tabanlı saldırı tespit modellerinin gelişimi, IoT cihazlarının güvenliğini artırarak siber tehditlere karşı daha dayanıklı hale gelmesini sağlayacaktır.

Bu çalışmaların genel bulguları, DÖ ve MÖ gibi yöntemlerin kullanılmasıyla IoT ortamına yönelik saldırılara karşı etkili sonuçlar elde edildiğini göstermektedir. Literatürde yapılan çalışmaların karşılaştırması Çizelge 2.1'de sunulmaktadır.

Çizelge 2.1. IOT sistemlerine yapılan siber saldırılarının literatür karşılaştırması

	Makale	Algoritma	Özellik Sayısı	Sınıflandırma Sayısı	Doğruluk
1	Gupta ve ark.,	Hibrit	42	2	%99,58
				8	%99,39
				34	%98,95
2	Alqahtani ve ark.	LSTM	20	34	%98,13
3	Vajrobol ve ark.	LSTM-XGBoost	46	4	%97,7
4	Wang ve ark.	Önerilen Model	46	13	%97,47
5	Narayan ve ark.	FW4: CFS+BRFC	6	2	%99,62
				8	%99,43
				34	%99,23
		RF_MRMR+BRFC	11	2	%99,55
				8	%99,40
				34	%99,23
6	Khanday ve ark.	1D-CNN			%99,87
7	Pandey ve Mishra	Hibrit(DDOS)		2	%99,86
8	Neto ve ark.	RF	-	2	%99,68
				8	%99,43
				34	%99,16
9	Jony ve Arnob	LSTM	46	34	%98,66
10	Kumar ve Ansari	SFOA-LASSO_XGBoost	8	2	%99,5
11	Ullah ve ark.	CNN-LSTM		10	%99,64
12	Niu ve ark.	Önerilen Model		2	%99,5
				8	%98,25
13	Sayed ve Hassanien	IIDS-RSEFO	Benign Traffic: 28	2	%99,7
			DDoS: 22		%100

			Brute Force: 17		%100
			Spoofing: 18		%99,8
			DoS: 1		%100
			Recon: 11		%100
			Web-Based: 17		%99,8
			Mirai: 20		%100
14	Phan ve ark.	RF+RFE	5	8	%99,45
		RF+RFE	15	8	%99,52
		RF+RFE	30	8	%99,57
15	Ji ve ark.	CNN-GWO-Voting	15	34	%99,15
		Hibrit Ensemble	15	2	%98,16
16	Abbas ve ark.	FDNN	46	2	%99,83
17	Yang ve ark.	NIDS-BAI	35	8	%99,5
18	Al-Na'amneh ve ark.	CNN-SVM	46	3	%99,8
19	Wang ve ark.	NIDS-FGPA	46	8	%99,2
20	Krzysztoń ve ark.	RF	10-15	2	%99,45

3. MATERYAL VE YÖNTEM

Bu bölümde, CICIoT2023 veri seti, uygulanan veri işleme yöntemleri ve saldırı tespiti amacıyla geliştirilen yaklaşımlar ayrıntılı olarak ele alınmaktadır. Çalışma kapsamında, makine öğrenmesi ve derin öğrenme algoritmalarını kullanarak IoT saldırılarını tespit etmek amacıyla CICIoT2023 veri seti kullanılmıştır. Veri setinin genel yapısı, saldırı türleri ve kullanım alanları kapsamlı biçimde analiz edilmiştir.

3.1. Kullanılan Veri Seti: CICIoT2023

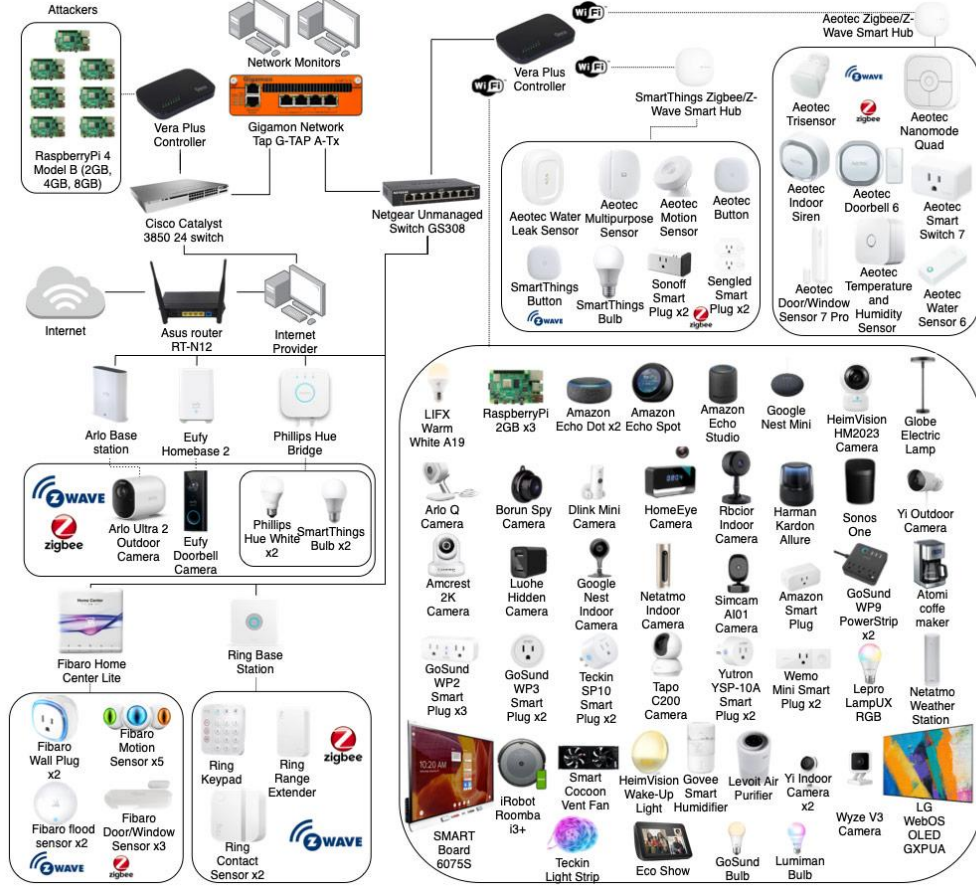
CICIoT2023 veri seti, IoT cihazlarının güvenlik tehditlerine karşı analiz edilmesi ve yeni güvenlik çözümleri geliştirilmesi amacıyla oluşturulmuş kapsamlı bir benchmark veri setidir. Günümüzde IoT cihazlarının artan kullanımıyla birlikte, siber saldırılar da daha yaygın hale gelmiştir. Bu veri seti, çeşitli saldırı türlerini ve normal trafiği içeren geniş çaplı veriler sunarak araştırmacılara güvenlik çözümleri geliştirmeleri için olanak tanımaktadır (CICIoT2023, 2023).

CICIoT2023 veri seti, IoT ortamlarında büyük ölçekli saldırıları analiz etmek ve güvenlik çözümleri geliştirmek için gerçek zamanlı veriler sunar. Farklı saldırı türlerini ve normal trafik verilerini içeren bu veri seti, IoT cihazlarının siber tehditlere karşı dayanıklılığını test etmek ve yeni tehdit algılama sistemleri geliştirmek için kritik bir kaynak olarak değerlendirilir.

Veri setinin oluşturulmasında ağ yönetimi için yönlendiriciler, ağ anahtarları ve ağ izleme cihazları kullanılmıştır. Saldırıları, kötü niyetli IoT cihazlarını taklit eden Raspberry Pi cihazları aracılığıyla gerçekleştirilmiştir. Farklı saldırı türleri uygulanarak gerçekçi bir tehdit ortamı oluşturulmuş ve saldırılar; Dağıtık Hizmet Engelleme (DDoS), Hizmet Engelleme (DoS), keşif (reconnaissance), web tabanlı saldırılar, brute force, kimlik sahtekarlığı (spoofing) ve Mirai botnet saldırıları şeklinde kategorize edilmiştir.

Tüm ağ trafiği, Wireshark ve benzeri analiz araçlarıyla kaydedilmiş; Cisco anahtarlar ve ağ izleme cihazları aracılığıyla saldırı ve normal trafik verileri ayrıştırılmıştır. Elde edilen veriler, saldırı türlerine göre etiketlenerek pcap formatında depolanmış ve makine öğrenimi uygulamaları için uygun hale getirilmiştir. Ağ trafiğinden çıkarılan 47 farklı özellik, saldırı tespiti amacıyla işlenmiş ve çeşitli makine öğrenimi modelleri ile test edilmiştir.

Bu yapı, IoT güvenliği için gerçek dünya senaryolarını içeren kapsamlı bir veri seti oluşturmak amacıyla tasarlanmıştır. Farklı saldırı türlerini ve geniş cihaz yelpazesini içermesi sayesinde, saldırı tespit sistemlerinin geliştirilmesi ve performanslarının değerlendirilmesi açısından önemli bir kaynak sunmaktadır.



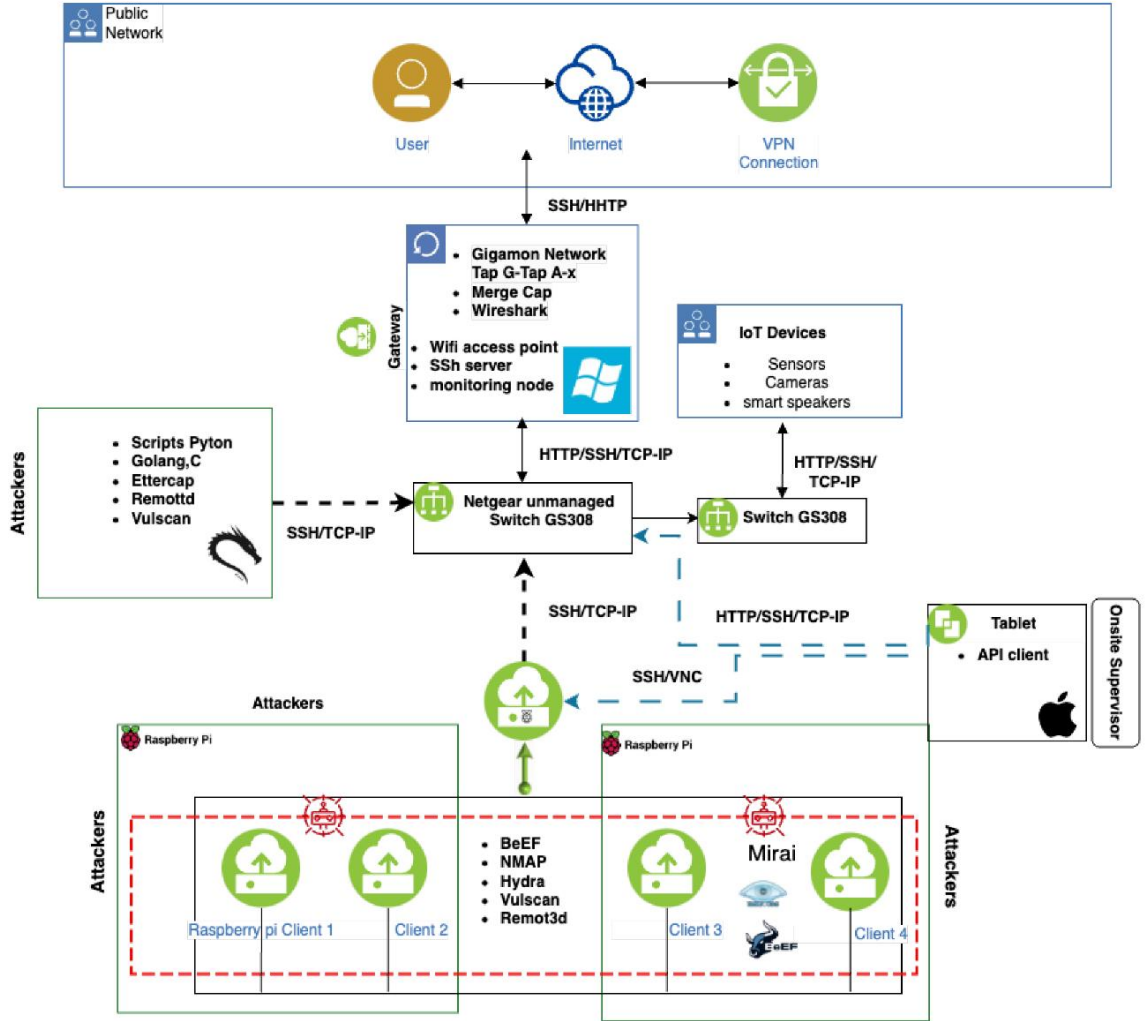
Şekil 3.1. Deneylerde kullanılan IoT ağ topolojisi (Neto ve ark., 2023)

Şekil 3.1, IoT ortamında gerçekleştirilen saldırıları ve veri setinin oluşturulma sürecini göstermektedir. Çeşitli akıllı ev cihazları, kameralar, sensörler ve mikro denetleyicilerden oluşan geniş bir ağ yapısı kurulmuştur. Bu cihazlar, Zigbee, Z-Wave, Wi-Fi ve kablolu bağlantılar üzerinden birbirine bağlanmış ve gerçek bir ev otomasyonu ortamı simüle edilmiştir.

Saldırı senaryoları, Raspberry Pi cihazları kullanılarak gerçekleştirilmiş ve farklı saldırı teknikleri uygulanmıştır. Yapıda iki ana saldırgan bölgesi bulunmaktadır. İlk saldırı grubu, ağ manipülasyonu ve bilgi toplama için Python betikleri, Golang, Ettercap, Remot3d ve Vulscan gibi araçları kullanmaktadır. İkinci saldırı grubu ise, daha karmaşık saldırılar için Mirai botnet, BeEF, NMAP, Hydra gibi yazılımları kullanarak IoT

cihazlarını hedef almaktadır. Saldırılar SSH, TCP/IP, HTTP protokolleri üzerinden yürütülerek ağ güvenlik mekanizmalarının etkinliği test edilmiştir.

Bu yapı, IoT ortamlarında gerçek tehditleri modellemek ve saldırı tespit sistemlerinin etkinliğini ölçmek için kapsamlı bir test ortamı sunmaktadır. Ağ üzerindeki kötü niyetli trafiğin normal trafiğe kıyasla nasıl davrandığını analiz etmek için saldırılar sırasında toplanan veriler, makine öğrenimi algoritmaları kullanılarak değerlendirilmiştir. CICIOT2023 veri seti, IoT güvenliği alanında tehdit tespiti ve saldırı sınıflandırması üzerine geliştirilecek yeni yöntemler için geniş ölçekli bir kaynak sağlamaktadır.



Şekil 3.2. Veri kümesi için temel saldırı çerçevesi (Neto ve ark., 2023)

Şekil 3.2, CICIOT2023 veri setinin oluşturulma sürecini temsil eden bu yapı, gerçek zamanlı IoT saldırılarını simüle etmek ve ağ güvenliğini test etmek amacıyla tasarlanmıştır. Şekilde, kullanıcıların internet üzerinden bir VPN bağlantısı aracılığıyla IoT ağına erişimi gösterilmektedir. IoT cihazları, sensörler, kameralar ve akıllı

hoparlörler gibi farklı bileşenlerden oluşmakta olup, bu cihazlar Netgear GS308 yönetilmeyen ağ anahtarı üzerinden haberleşmektedir. Ağ üzerindeki trafik, Gigamon Network Tap ve Wireshark gibi izleme araçlarıyla kaydedilerek analiz edilmiştir.

3.1.1. CICIOT2023 Veri Setinin Önemi ve Kullanım Alanları

CICIOT2023 veri seti, IoT sistemlerinde siber güvenliği artırmak, saldırı tespit sistemlerinin geliştirilmesi ve test edilmesini sağlamak amacıyla oluşturulmuş kapsamlı bir araştırma kaynağıdır. IoT teknolojilerinin yaygınlaşması, bu sistemlere yönelik siber tehditlerin de artmasına yol açmış ve güvenlik açıklarının tespiti ile etkili savunma mekanizmalarının geliştirilmesini zorunlu hale getirmiştir (CICIOT2023, 2023).

Bu veri seti, IoT ağlarında siber tehditleri tespit etmek için anomali ve imza tabanlı saldırı tespit sistemlerinin geliştirilmesine olanak tanımaktadır. Özellikle makine öğrenimi ve derin öğrenme tabanlı çözümlerin eğitilmesi ve değerlendirilmesi için önemli bir veri kaynağı sunmaktadır (Neto ve ark., 2023). CICIOT2023 veri seti, DDoS, DoS, brute force, kimlik sahtekarlığı (spoofing) ve web tabanlı saldırılar gibi IoT sistemlerine yönelik çeşitli tehditleri içermektedir. Gerçek saldırı örneklerinden oluşan bu veri seti, güvenlik çözümlerinin etkinliğini test etmek ve saldırı tespit sistemlerini optimize etmek için kullanılmaktadır (CICIOT2023, 2023).

Anomali tespiti algoritmalarının geliştirilmesi açısından da önemli bir kaynak sağlayan bu veri seti, IoT ağ trafiğinde normal ve anormal verileri ayırt etmek için kullanılmaktadır. Böylece, bilinmeyen veya daha önce karşılaşılmamış saldırı türlerinin tespit edilmesine katkı sağlamaktadır (Neto ve ark., 2023). Bunun yanı sıra, akademik ve endüstriyel araştırmalar kapsamında, IoT güvenliği alanında çalışan araştırmacılar ve sektör uzmanları tarafından yeni güvenlik protokollerinin test edilmesi, saldırı simülasyonlarının gerçekleştirilmesi ve IDS (Intrusion Detection Systems) sistemlerinin geliştirilmesi amacıyla kullanılmaktadır. Özellikle eğitim ve simülasyon ortamlarında, gerçek saldırı verileriyle çalışarak pratik yapma imkanı sunması, veri setinin siber güvenlik alanında önemli bir referans kaynağı olmasını sağlamaktadır (CICIOT2023, 2023).

Sonuç olarak, CICIOT2023 veri seti, IoT sistemlerinin güvenliğini artırmak ve tehditleri daha etkin bir şekilde analiz etmek için kritik bir araç olup, akademik araştırmalardan endüstriyel uygulamalara kadar geniş bir kullanım alanına sahiptir.

3.1.2. CICIOT2023 Veri Setinin Özellikleri

CICIOT2023 veri seti, IoT güvenliği alanında gerçekleştirilen akademik ve endüstriyel araştırmalarda kullanılan kapsamlı bir veri kaynağıdır. IoT ortamlarında meydana gelen çeşitli siber saldırıları içeren bu veri seti, saldırı tespit sistemlerinin geliştirilmesi ve test edilmesi amacıyla oluşturulmuştur. İçeriğinde hem normal ağ trafiği hem de farklı saldırı türleri yer almakta olup, geniş kapsamlı analizler için uygun bir yapı sunmaktadır (CICIOT2023, 2023).

Bu veri seti, IoT sistemlerinde gözlemlenen hem zararsız hem de kötü niyetli ağ trafiği örneklerini içermektedir. Normal trafik, IoT cihazlarının olağan iletişim süreçlerini kapsarken, saldırı trafiği DDoS, kimlik sahtekarlığı (spoofing), brute force, port tarama ve kötü amaçlı yazılım bulaşma girişimleri gibi tehditlerden oluşmaktadır (CICIOT2023, 2023). Toplamda 105 farklı IoT cihazından toplanan ve 46.686.579 adet ağ trafiği örneğini içeren bu veri kümesi, 33 farklı saldırı kategorisini ve bir benign trafik sınıfını kapsamaktadır (Neto ve ark., 2023).

Ağ protokolleri ve paket seviyesi analizler açısından detaylı bilgiler sunan veri seti, HTTP, TCP ve UDP gibi farklı protokollere dayalı trafik verilerini içermektedir. Ayrıca, paket uzunlukları, bayrak bilgileri (SYN, ACK, FIN vb.) ve bağlantı süreleri gibi parametreleri içeren detaylı ağ trafiği verileri barındırmaktadır (CICIOT2023, 2023). Veri setindeki geniş özellik kümesi, saldırı tespit süreçlerinde boyut indirgeme tekniklerinin uygulanmasını gerektirebilir (Ullah ve ark., 2024).

Gerçek dünya senaryolarını yansıtan bu veri seti, IoT ekosisteminde sık karşılaşılan saldırıları içermektedir. DDoS, DoS, brute force, spoofing, kimlik avı (phishing), zafiyet taraması, web tabanlı saldırılar (SQL Injection, XSS vb.) ve Mirai botnet saldırıları gibi tehditler, veri setinin sunduğu önemli içerikler arasındadır (Neto ve ark., 2023). Farklı IoT cihaz türlerinden elde edilen trafik verileri sayesinde, IoT ağlarında güvenlik tehditlerine karşı geliştirilen çözümlerin etkinliği artırılabilir (CICIOT2023, 2023).

Bu veri setinin özgün yönlerinden biri, gerçek IoT cihazları üzerinde uygulanarak oluşturulan gerçekçi saldırı senaryolarıdır. Böylece, gerçek dünya koşullarını yansıtan güvenilir bir kaynak sunmaktadır.

Çizelge 3.1, CICIOT2023 veri setinde yer alan ağ trafiği özelliklerinin isimlerini ve açıklamalarını içermektedir. Bu özellikler, saldırı tespiti ve veri analizi süreçlerinde temel parametreler olarak kullanılmaktadır.

Çizelge 3.1. CICIoT2023 veri setinin verilerinin özellik ve açıklamaları

Özellik Adı	Açıklaması	Özellik Adı	Açıklaması
1 flow_duration	Akışın toplam süresi (mikrosaniye cinsinden).	25 SSH	Akışın SSH protokolünü kullanıp kullanmadığını belirtir (binary değer).
2 Header_Length	Veri paketlerinin başlık (header) uzunluğu (byte cinsinden).	26 IRC	Akışın IRC protokolünü kullanıp kullanmadığını belirtir (binary değer).
3 Protocol_Type	Akışta kullanılan protokol türü (örneğin, TCP, UDP gibi).	27 TCP	Akışın TCP protokolünü kullanıp kullanmadığını belirtir (binary değer).
4 Duration	Akışın başlangıç ve bitiş zamanları arasındaki süre.	28 UDP	Akışın UDP protokolünü kullanıp kullanmadığını belirtir (binary değer).
5 Rate	Akışın veri aktarım hızı (bit/saniye cinsinden).	29 DHCP	Akışın DHCP protokolünü kullanıp kullanmadığını belirtir (binary değer).
6 Srate	Gönderici yönündeki veri aktarım hızı.	30 ARP	Akışın ARP protokolünü kullanıp kullanmadığını belirtir (binary değer).
7 Drate	Alıcı yönündeki veri aktarım hızı.	31 ICMP	Akışın ICMP protokolünü kullanıp kullanmadığını belirtir (binary değer).
8 fin_flag_number	Akıştaki "FIN" bayrağı sayısı.	32 IPv	Akışın IP versiyonunu belirtir (örneğin, IPv4, IPv6).
9 syn_flag_number	Akıştaki "SYN" bayrağı sayısı.	33 LLC	Akışın LLC protokolünü kullanıp kullanmadığını belirtir (binary değer).
10 rst_flag_number	Akıştaki "RST" bayrağı sayısı.	34 Tot sum	Akıştaki tüm veri paketlerinin toplam uzunluğu.
11 psh_flag_number	Akıştaki "PSH" bayrağı sayısı.	35 Min	Akıştaki veri paketlerinin minimum uzunluğu.
12 ack_flag_number	Akıştaki "ACK" bayrağı sayısı.	36 Max	Akıştaki veri paketlerinin maksimum uzunluğu.
13 ece_flag_number	Akıştaki "ECE" bayrağı sayısı.	37 AVG	Akıştaki veri paketlerinin ortalama uzunluğu.

14	cwr_flag_number	Akıştaki "CWR" bayrağı sayısı.	38	Std	Akıştaki veri paketlerinin standart sapması.
15	ack_count	Akıştaki gönderilen "ACK" mesajlarının toplam sayısı.	39	Tot size	Akışın toplam boyutu (byte cinsinden).
16	syn_count	Akıştaki gönderilen "SYN" mesajlarının toplam sayısı.	40	IAT	Akıştaki iki veri paketi arasındaki ortalama süre.
17	fin_count	Akıştaki gönderilen "FIN" mesajlarının toplam sayısı.	41	Number	Akıştaki toplam paket sayısı.
18	urg_count	Akıştaki gönderilen "URG" bayrağı sayısı.	42	Magnitude	Akışın büyüklüğünü ifade eden bir metrik.
19	rst_count	Akıştaki gönderilen "RST" bayrağı sayısı.	43	Radius	Akıştaki veri paketlerinin özelliklerine bağlı olarak hesaplanan bir metrik.
20	HTTP	Akışın HTTP protokolünü kullanıp kullanmadığını belirtir (binary değer).	44	Covariance	Akıştaki paketlerin değişkenlik kovaryansı.
21	HTTPS	Akışın HTTPS protokolünü kullanıp kullanmadığını belirtir (binary değer).	45	Variance	Akıştaki paketlerin boyutlarının varyansı.
22	DNS	Akışın DNS protokolünü kullanıp kullanmadığını belirtir (binary değer).	46	Weight	Akıştaki paketlerin ağırlık metriği (belirli bir bağlama bağlı olarak hesaplanabilir).
23	Telnet	Akışın Telnet protokolünü kullanıp kullanmadığını belirtir (binary değer).	47	label	Akışın sınıfı veya etiketi (örneğin, normal, anormal, saldırı türü).
24	SMTP	Akışın SMTP protokolünü kullanıp kullanmadığını belirtir (binary değer).			

3.1.3. Normal ve Saldırı Trafikinin Karakterizasyonu

CICIoT2023 veri setinde yer alan normal ve saldırı trafiği, çeşitli ağ parametreleri ve saldırı teknikleri açısından farklılık göstermektedir. Normal trafik, IoT cihazlarının olağan çalışma süreçlerinde ürettiği düzenli veri akışlarını içerirken, saldırı trafiği genellikle belirli hedeflere odaklanan anormal davranışlar sergilemektedir. Özellikle kaynak ve hedef IP dağılımı açısından bakıldığında, normal trafik daha geniş bir IP aralığına yayılmışken, saldırı trafiği belirli noktalarda yoğunlaşarak olağandışı paternler

oluşturmaktadır. Ayrıca, saldırı trafiğinde paket boyutları standart dışı olup, belirli bir büyüklükte veya sürekli değişkenlik gösteren yapılar içermektedir. Zaman serisi analizi açısından ise, normal trafik belirli bir düzen içinde ilerlerken, saldırılar genellikle belirli zaman aralıklarında yoğunlaşarak istatistiksel dalgalanmalara neden olmaktadır. IoT cihazlarının hem saldırgan hem de hedef olarak kullanıldığı bu yapı, araştırmacıların savunma sistemlerini daha etkili şekilde test etmesini sağlamaktadır.

Dağıtık Hizmet Engelleme (DDoS) saldırıları, ICMP Flood, HTTP Flood ve UDP Flood gibi yöntemler kullanılarak hedef sistemlerin işlevsiz hale getirilmesini amaçlamaktadır. Hizmet Engelleme (DoS) saldırıları ise, HTTP ve TCP SYN Flood gibi teknikler ile sistemin yanıt verme süresini artırarak performansını düşürmeye yöneliktir. Zafiyet taraması saldırıları, sistemin açık portlarını ve güvenlik zafiyetlerini tespit etmeye yönelik keşif saldırıları olup, Host Discovery ve Ping Sweep gibi yöntemler ile gerçekleştirilir (Wang ve ark., 2024b).

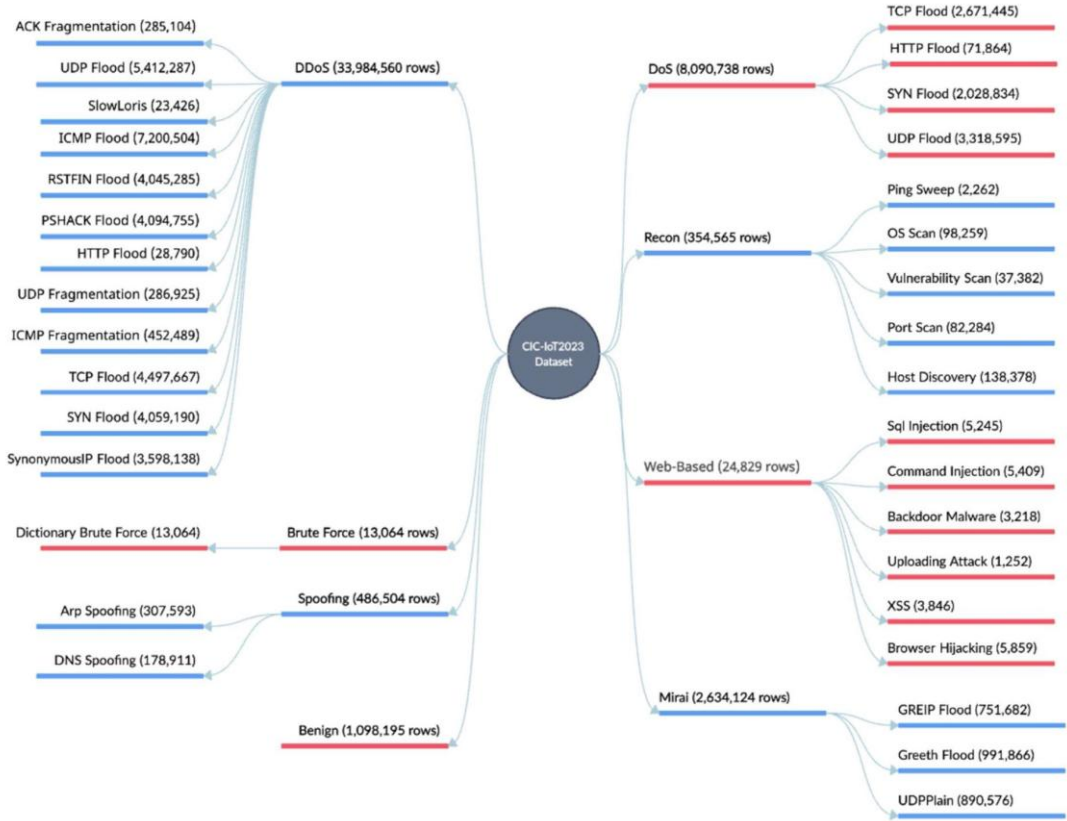
IoT ağlarında yaygın olarak görülen bir diğer tehdit, kimlik sahtekarlığı saldırılarıdır. Bu tür saldırılarda, kötü niyetli aktörler ağ trafiğini manipüle ederek yetkisiz erişim sağlamaya çalışmaktadır. Web tabanlı saldırılar ise genellikle SQL Injection ve XSS gibi teknikler kullanılarak gerçekleştirilmektedir ve bu saldırılar, web uygulamalarındaki güvenlik açıklarından yararlanmayı hedeflemektedir. Brute force saldırıları, zayıf şifreleri kırarak yetkisiz erişim sağlamaya çalışırken, Mirai botnet saldırıları, IoT cihazlarını ele geçirerek büyük ölçekli botnet ağları oluşturmayı amaçlamaktadır. Mirai saldırıları, ele geçirilen IoT cihazlarını kötüye kullanarak dağıtık hizmet engelleme saldırıları gerçekleştirme potansiyeline sahiptir (Taş, 2022).

Veri setinde bulunan her bir saldırı türü, trafik hacmi, paket boyutu dağılımı, bağlantı süresi ve paketler arası zaman farkı gibi belirli ölçütler kullanılarak analiz edilmektedir. Bu ölçütler, saldırı tespit sistemlerinin etkinliğini artırmak ve IoT güvenlik çözümlerinin geliştirilmesine katkı sağlamak açısından kritik bir öneme sahiptir. Özellikle, saldırı trafiği normal trafikten ayrıştırılarak, makine öğrenimi tabanlı tespit sistemlerinin eğitilmesi ve performanslarının optimize edilmesi için önemli bir veri kaynağı sunmaktadır. CICIoT2023 veri seti, IoT güvenliği alanında çalışan araştırmacılar için kapsamlı bir analiz imkanı sağlayarak, siber tehditlere karşı geliştirilen savunma mekanizmalarının iyileştirilmesine katkıda bulunmaktadır (Jony ve Arnob, 2024).

Bu farklılıkların analizi, IoT güvenlik sistemlerinin geliştirilmesi ve saldırı tespit süreçlerinin iyileştirilmesi açısından büyük önem taşımaktadır.

3.2. CICIOT2023 Veri Setindeki IoT Saldırı Türleri

DDoS ve DoS saldırıları, veri setinde en büyük saldırı kümelerini oluşturmaktadır. Bu kategorilerin alt başlıklarında yaygın olarak UDP flood, TCP flood, SYN flood, HTTP flood ve ICMP flood gibi saldırı türleri yer almaktadır. Brute force saldırıları ise tek bir kategori altında toplanmıştır. Web tabanlı saldırılar, SQL injection, XSS ve browser hijacking gibi çeşitli tehditleri içermektedir. Öte yandan, Mirai botnet saldırıları, GREIP flood, Greeth flood ve UDPPlain gibi alt türlerle detaylandırılmıştır.



Şekil 3.3. CICIOT2023 veri seti-IoT ağ trafiği saldırı sınıflandırması (Jony ve Arnob, 2024)

Şekil 3.3'de gösterilen CICIOT2023 veri seti, IoT ağ trafiğini analiz etmek için oluşturulmuş kapsamlı bir saldırı sınıflandırma yapısına sahiptir. Veri seti, DDoS, DoS, brute force, spoofing, reconnaissance, web tabanlı saldırılar, Mirai ve benign (zararsız) trafik olmak üzere sekiz ana kategoriye ayrılmıştır.

Çizelge 3.2, CICIOT2023 veri setinde bulunan farklı saldırı türlerinin satır sayılarına göre dağılımını göstermektedir. Grafikte en fazla örnek içeren saldırı türü DDoS-ICMP Flood olup, 7.200.504 satır ile veri setinin büyük bir bölümünü oluşturmaktadır. Bu saldırıyı sırasıyla DDoS-UDP Flood (5.412.287 satır), DDoS-TCP

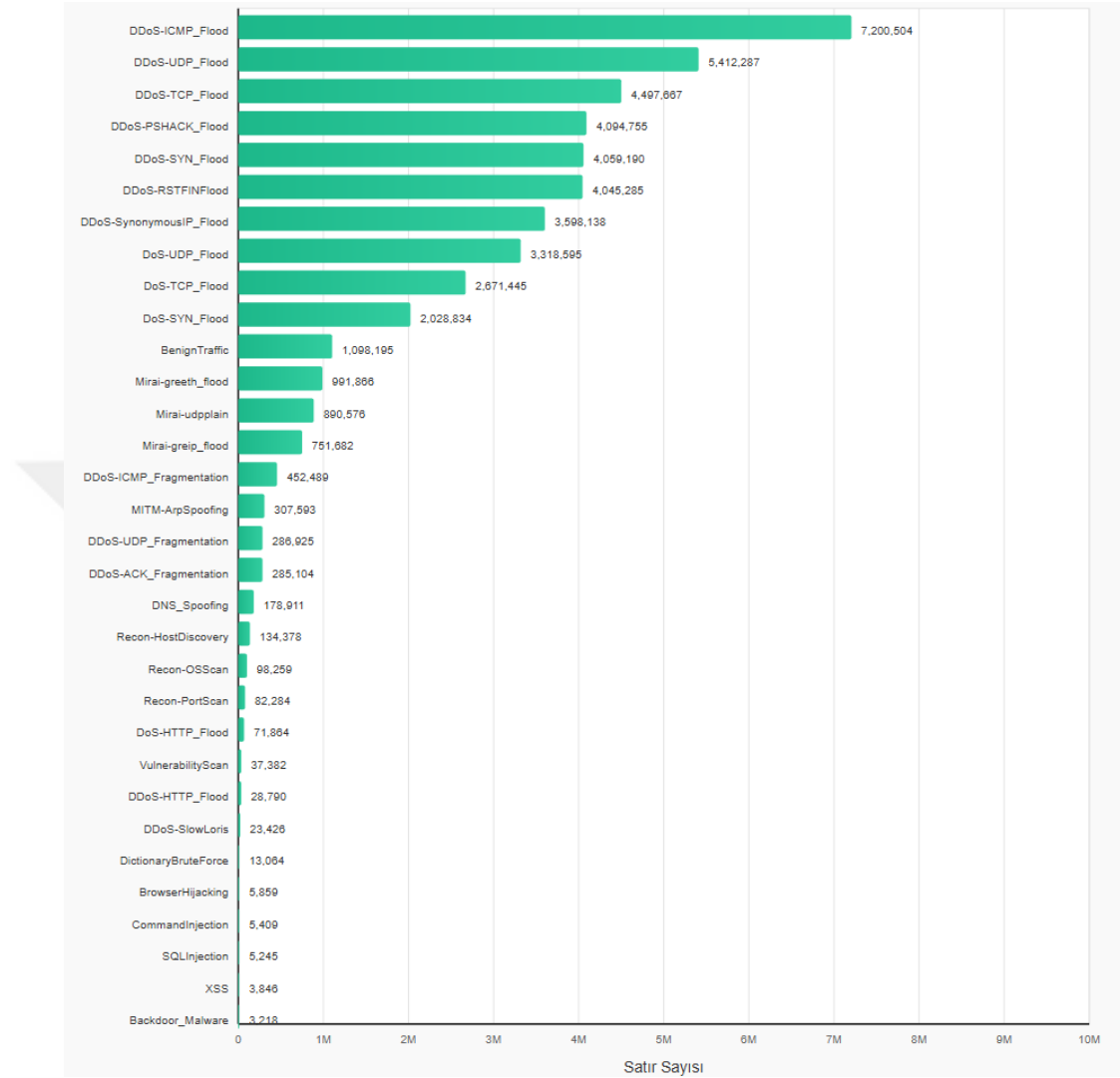
Flood (4.497.867 satır) ve DDoS-PSHACK Flood (4.094.755 satır) takip etmektedir. Genel olarak, DDoS ve DoS saldırıları veri setinde en baskın kategoriler olarak öne çıkmaktadır.

Çizelge 3.2. Her bir saldırı ve kategori için satır sayıları

Saldırı	Satır Sayısı	Saldırı	Satır Sayısı	Kategori	Satır Sayısı
DDoS-ICMP_Flood	7,200,504	DoS-TCP_Flood	2,671,445	DDoS	33,984,560
DDoS-UDP_Flood	5,412,287	DoS-SYN_Flood	2,028,834	DoS	8,090,738
DDoS-TCP_Flood	4,497,667	BenignTraffic	1,098,195	Mirai	2,634,124
DDoS-PSHACK_Flood	4,094,755	Mirai-greeth_flood	991,866	Benign	1,098,195
DDoS-SYN_Flood	4,059,190	Mirai-udpplain	890,576	Spoofing	486,504
DDoS-RSTFINFlood	4,045,285	Mirai-greip_flood	751,682	Recon	354,565
DDoS-SynonymousIP_Flood	3,598,138	DDoS-ICMP_Fragmentation	452,489	Web	24,829
DoS-UDP_Flood	3,318,595	MITM-ArpSpoofing	307,593	BruteForce	13,064
Recon-PingSweep	2262	Uploading_Attack	1252		
DDoS-UDP_Fragmentation	286,925	DDoS-HTTP_Flood	28,790		
DDoS-ACK_Fragmentation	285,104	DDoS-SlowLoris	23,426		
DNS_Spoofing	178,911	DictionaryBruteForce	13,064		
Recon-HostDiscovery	134,378	BrowserHijacking	5859		
Recon-OSScan	98,250	CommandInjection	5409		
Recon-PortScan	82,284	SqlInjection	5245		
DoS-HTTP_Flood	71,864	XSS	3846		
VulnerabilityScan	37,382	Backdoor_Malware	3218		

Benign (zararsız) trafik, 1.098.105 satır ile saldırı türlerine kıyasla daha az örnek içermektedir. Mirai, Spoofing, Recon, Web ve Brute Force saldırıları nispeten daha düşük örnek sayısına sahipken, özellikle SQL Injection, XSS ve Backdoor Malware gibi saldırı türleri çok sınırlı sayıda örnek barındırmaktadır. Veri setinde gözlemlenen bu dengesizlik, makine öğrenimi modellerinin eğitimi sırasında sınıf dengesizliği (class imbalance)

sorunlarına yol açabileceğinden, veri ön işleme aşamasında dikkate alınması gereken önemli bir faktördür.

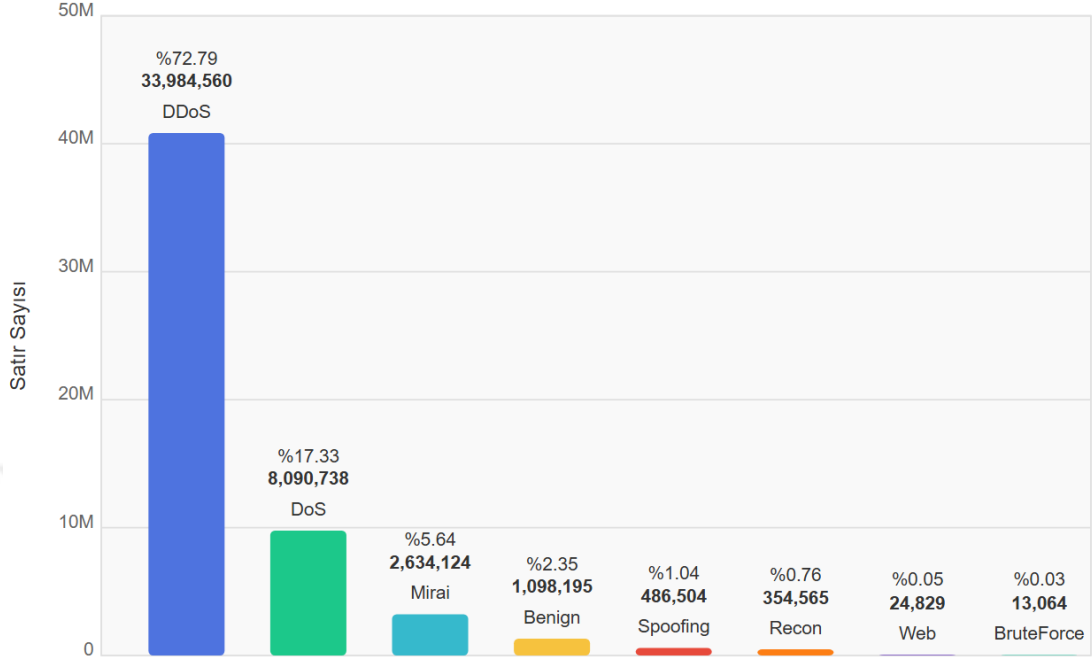


Şekil 3.4. CICIoT 2023 veri setindeki sınıf dağılımı

Şekil 3.4, CICIoT2023 veri setinde yer alan saldırı türlerini satır sayılarına göre azalan sırada göstermektedir.

Şekil 3.5, CICIoT2023 veri setindeki saldırı türlerinin kategorilere göre dağılımı gösterilmektedir. Veri setinde en fazla örnek içeren kategori, %72.79'luk oran ve 33,984,560 satır ile DDoS saldırılarıdır. Bunu %17.33 oranında (8,090,738 satır) DoS saldırıları takip etmektedir. Mirai saldırıları, toplam verinin %5.64'ünü (2,634,124 satır) oluştururken, Benign (zararsız) trafik %2.35 oranında (1,098,195 satır) yer almaktadır. Spoofing, Recon, Web ve BruteForce saldırıları ise toplam verinin yalnızca %1.88'ini kapsamaktadır. Veri setindeki bu dengesiz dağılım, makine öğrenimi modellerinin

eđitimi sırasında sınıf dengesizliđi (class imbalance) sorununa yol aabileceđinden veri n iřleme ařamasında dikkate alınması gereken nemli bir faktrdr.



řekil 3.5. CICIoT2023 veri setindeki saldırı türlerinin kategorilere göre dağılımı

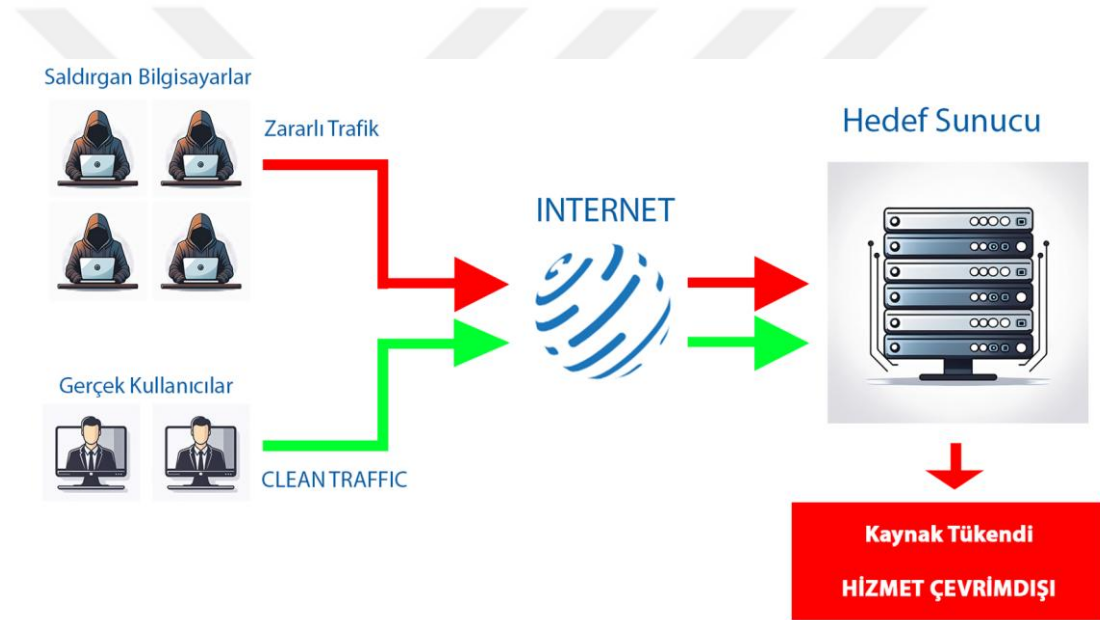
3.2.1. DDoS (Distributed Denial of Service) Saldırıları

Dağıtılmış Hizmet Reddi (DDoS) saldırıları, siber güvenlik dünyasında en yaygın ve yıkıcı saldırı türlerinden biridir. Bu saldırılar, hedef sistemin kaynaklarını aşırı yükleyerek hizmetlerin geçici veya kalıcı olarak kullanılamaz hale gelmesini amaçlar. Genellikle, kötü amaçlı yazılımlar tarafından ele geçirilmiş cihazlardan oluşan botnetler aracılığıyla gerçekleştirilir. Bu cihazlar saldırganlar tarafından uzaktan kontrol edilerek yüksek hacimli zararlı trafik oluşturur ve hedef sisteme yönlendirilir (Mirkovic ve Reiher, 2004).

DDoS saldırılarının temel amacı, hedef sistemin bant genişliğini, işlem gücünü ve bellek kapasitesini aşırı yükleyerek hizmetleri engellemektir. Özellikle IoT cihazlarının yaygınlaşmasıyla birlikte, bu cihazların güvenlik açıkları saldırganlar tarafından suistimal edilerek geniş çaplı botnet ağları oluşturulabilmektedir. 2016 yılında ortaya çıkan Mirai botneti, yüz binlerce IoT cihazını ele geçirerek büyük çaplı DDoS saldırıları gerçekleştirmiş ve küresel ölçekte hizmet kesintilerine yol açmıştır (Antonakakis ve ark., 2017). IoT cihazlarının sınırlı kaynaklara sahip olması, onları bu tür saldırılar karşısında daha savunmasız hale getirmektedir.

DDoS saldırıları genellikle üç ana kategoriye ayrılmaktadır: Bant genişliği tüketimi, hedef sisteme aşırı trafik yönlendirerek ağ bağlantısını tıkayıp hizmetlere erişimi engeller. Kaynak tüketimi, sunucuların işlem gücünü ve bellek kapasitesini aşırı yükleyerek çökmesine neden olur. Uygulama katmanı saldırıları ise belirli servisleri hedef alarak web uygulamalarının işleyişini bozmayı amaçlar (Zargar ve ark., 2013).

Bu tür saldırılar, bireysel ve kurumsal sistemler üzerinde ciddi etkiler yaratarak hizmet kesintilerine, veri kayıplarına ve finansal zararlara yol açabilir. DDoS saldırılarına karşı korunmak için trafik filtreleme, yük dengeleme ve güvenlik duvarı gibi önlemler alınarak sistemlerin dayanıklılığı artırılmalıdır (Mirkovic ve Reiher, 2004). Bunun yanı sıra, IoT cihazlarının güvenliği artırılarak, bu cihazların saldırganlar tarafından ele geçirilmesi önlenmeli ve güçlü kimlik doğrulama mekanizmaları uygulanmalıdır.



Şekil 3.6. DDoS (dağıtılmış hizmet engelleme) saldırısı ve kaynak tüketimi mekanizması

Şekil 3.6’da DDoS (Distributed Denial of Service) saldırısının temel işleyişi görselleştirilmiştir. Saldırgan tarafından ele geçirilmiş bilgisayarlardan (botnet) oluşan sistem, hedef sunucuya büyük miktarda zararlı trafik göndererek kaynaklarını tüketmekte ve hizmetin durmasına neden olmaktadır. Bu durum, gerçek kullanıcıların hedef sisteme erişimini zorlaştırmakta veya tamamen engellemektedir. Hedef sistemin aşırı yüklenmesi sonucunda, sunucu kaynaklarının tükenmesi nedeniyle hizmet dışı kalmaktadır.

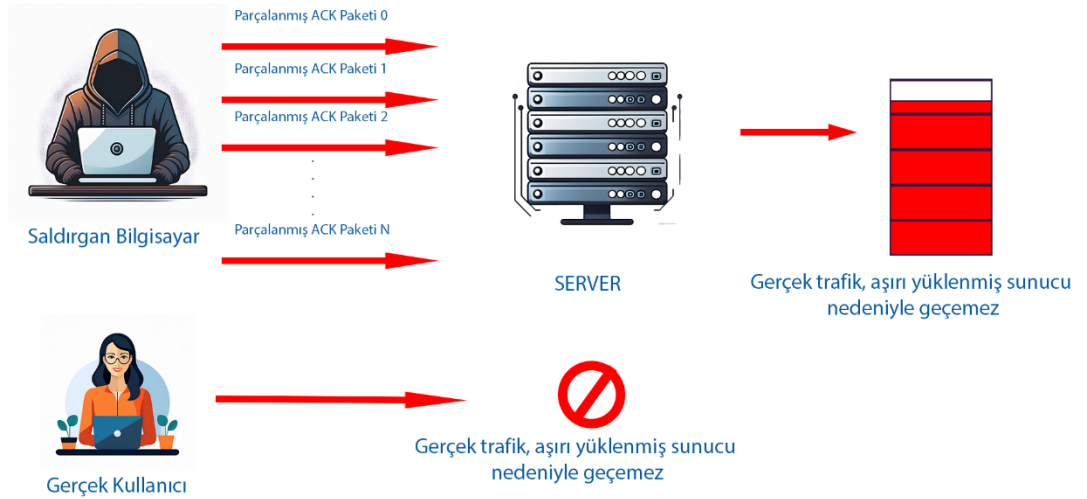
IoT ortamlarında, DDoS saldırılarının etkisini analiz etmek ve tespit etmek için CICIoT2023 veri seti önemli bir kaynak sunmaktadır. Bu veri seti, farklı DDoS saldırı türlerini içeren çeşitli senaryoları kapsamakta ve saldırıların tespiti için makine öğrenmesi

tabanlı yöntemlerin geliştirilmesine olanak tanımaktadır. Bu bağlamda, IoT cihazlarının güvenliğini artırmak ve DDoS saldırılarını önlemek için yapılacak analizler büyük önem taşımaktadır. CICIOT2023 veri seti üzerinde gerçekleştirilecek çalışmalar, saldırı tespit sistemlerinin geliştirilmesine katkı sağlayarak gelecekteki tehditlere karşı daha etkili savunma mekanizmalarının oluşturulmasına yardımcı olacaktır (CICIOT2023, 2023).

CICIOT2023 veri setinde yer alan en yaygın DDoS saldırı türleri aşağıda detaylı olarak açıklanmıştır:

3.2.1.1. ACK Fragmentation

ACK Fragmentation (ACK Parçalanması) saldırısı, saldırganların büyük boyutlu ACK (Acknowledge) paketlerini küçük parçalara bölerek hedef sisteme göndermesiyle gerçekleşen bir tür DDoS (Distributed Denial of Service) saldırısıdır. Bu yöntemle, hedef sistemin kaynakları tüketilir ve ağ performansı ciddi şekilde düşer. Saldırganlar, özellikle güvenlik duvarları ve saldırı tespit sistemlerinin bu tür parçalanmış paketleri yeniden birleştirmekte zorlanmasından faydalananarak, tespit edilmeden saldırılarını sürdürebilirler.



Şekil 3.7. ACK parçalanması (fragmentation) DDoS saldırısı ve sunucu kaynak tüketimi mekanizması

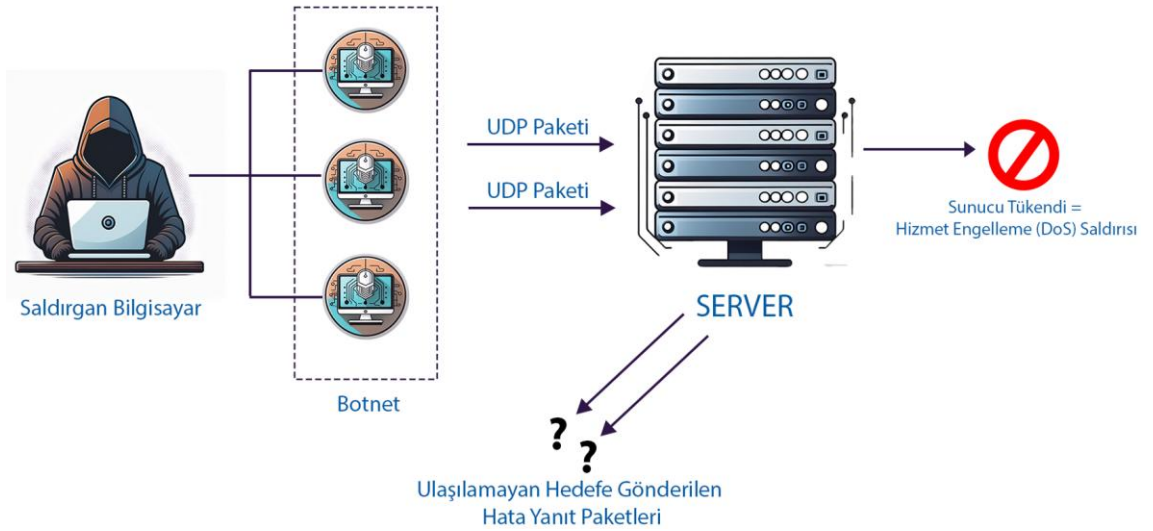
Şekil 3.7, ACK parçalanması saldırısını temsil etmektedir. Saldırgan, sunucuya art arda parçalanmış ACK paketleri göndererek sistemi aşırı yüklemekte ve kaynak tüketimine neden olmaktadır. Bu durum, aynı sunucuya erişmeye çalışan gerçek kullanıcıların bağlantısını engeller. Sonuç olarak, sunucu meşru trafiği işleyemez hale

gelir ve hizmet kesintisi yaşanır. Bu tür saldırılar, DDoS (Dağıtık Hizmet Engelleme) kapsamında değerlendirilen ve hizmet aksamasına yol açan siber tehditlerdir.

Bu tür saldırılardan korunmak için, ağ yöneticilerinin parçalanmış paketleri izleyip analiz edebilen gelişmiş güvenlik çözümleri kullanmaları önemlidir. Ayrıca, ağ cihazlarının ve sunucuların en son güvenlik yamalarıyla güncel tutulması, bilinen zafiyetlerin kapatılmasına yardımcı olur. Ağ trafiğinin sürekli izlenmesi ve anormalliklerin hızlı bir şekilde tespit edilip müdahale edilmesi, ACK Fragmentation saldırılarının etkisini minimize etmek için kritik öneme sahiptir (Indusface Fragmented ACK, 2025).

3.2.1.2. UDP Flood

UDP Flood Saldırısı, hedef sistemin bant genişliğini veya kaynaklarını tüketmek amacıyla büyük miktarda UDP (User Datagram Protocol) paketinin gönderilmesiyle gerçekleştirilen bir tür Hizmet Engelleme (DoS) saldırısıdır. UDP, bağlantısız bir protokol olduğundan, saldırganlar bu özelliği kullanarak hedef sisteme rastgele portlara sahip çok sayıda UDP paketi yollar. Hedef sistem, her bir paketin ulaştığı portta bir uygulama olup olmadığını kontrol eder ve eğer yoksa, genellikle "Hedefe Ulaşılamıyor" mesajı içeren ICMP paketleriyle yanıt verir. Bu süreç, sistemin kaynaklarını hızla tüketerek performansın düşmesine veya tamamen hizmet dışı kalmasına neden olabilir.



Şekil 3.8. Botnet destekli UDP flood DDoS saldırısı ve sunucu kaynak tüketimi

Şekil 3.8, botnet kullanılarak gerçekleştirilen bir DDoS saldırısını göstermektedir. Saldırgan, kontrol ettiği çok sayıda zombi bilgisayardan hedef sunucuya yoğun UDP

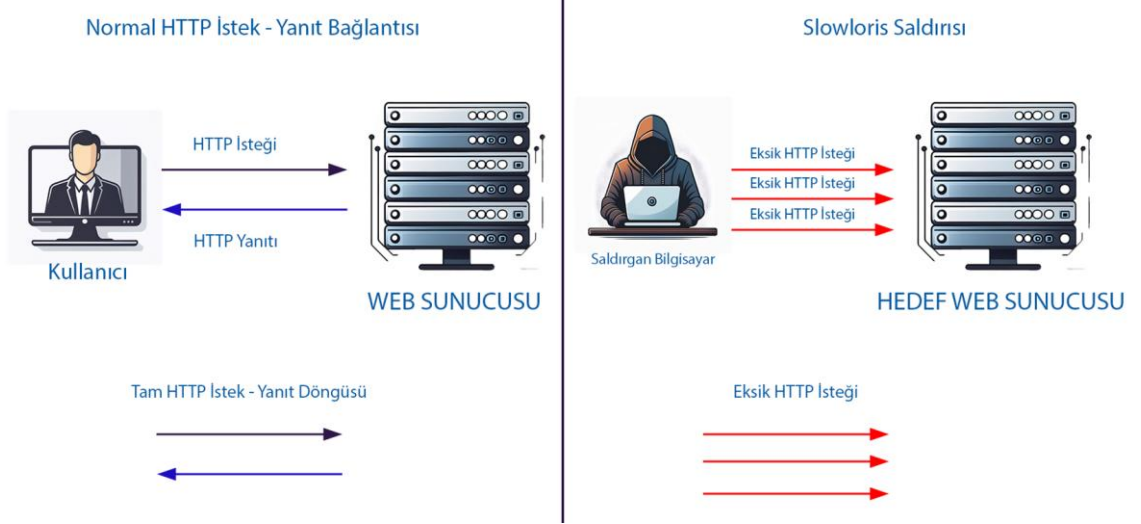
paketleri göndererek sistemi aşırı yüklemektedir. Sonuç olarak sunucu kaynakları tükenir ve hizmet veremez hale gelir. Sunucunun gönderdiği hata yanıtları ise saldırının etkisini azaltmakta yetersiz kalır. Bu yöntem, çoklu kaynaklardan gelen trafikle sistemin işlevsiz bırakılmasını amaçlayan etkili bir dağıtılmış hizmet engelleme saldırısıdır.

Bu tür saldırılardan korunmak için çeşitli önlemler alınabilir. Öncelikle, gereksiz UDP hizmetlerinin devre dışı bırakılması saldırı yüzeyini daraltır. Ayrıca, ağ trafiğini izleyerek anormallikleri tespit eden Giriş Tespit ve Önleme Sistemleri (IDPS), şüpheli aktiviteleri erken aşamada belirleyip müdahale edilmesini sağlar. Trafik sınırlama (rate limiting) uygulamaları, belirli bir zaman diliminde kabul edilen istek sayısını kontrol ederek sunucunun aşırı yüklenmesini önler. Son olarak, kapsamlı DDoS koruma çözümleri, gelen trafiği analiz ederek meşru ve zararlı istekleri ayırt edebilir; böylece UDP flood saldırılarını etkili bir şekilde engelleyebilir (Indusface UDP Flood, 2025).

3.2.1.3. Slowloris

Slowloris saldırısı, düşük bant genişliği kullanarak bir web sunucusunun tüm bağlantı yuvalarını meşgul eden ve böylece meşru kullanıcıların erişimini engelleyen bir hizmet reddi (DoS) saldırısıdır. Bu saldırıda, saldırgan sunucuya birçok HTTP isteği başlatır ancak her isteği eksik bırakır ve belirli aralıklarla küçük veri paketleri göndererek bağlantıları açık tutar. Sunucu, bu eksik istekleri tamamlanmış bir yanıt bekleyerek uzun süre boyunca tutar ve zamanla yeni bağlantıları kabul edemez hale gelir. Bu yöntem özellikle Apache gibi belirli web sunucularını hedef alarak büyük kesintilere yol açabilir ve geleneksel güvenlik duvarları tarafından tespit edilmesi zor olabilir.

Slowloris saldırılarından korunmak için çeşitli yöntemler uygulanabilir. Öncelikle, sunucu konfigürasyonları optimize edilerek her bağlantı için belirli bir zaman aşımı süresi belirlenmeli ve aynı IP adresinden gelen maksimum eşzamanlı bağlantı sayısı sınırlandırılmalıdır. Yük dengeleyiciler veya ters proxy sunucular kullanılarak gelen trafik daha etkin bir şekilde yönetilebilir. Ayrıca, saldırıları tespit edebilen güvenlik duvarları ve saldırı tespit sistemleri (IDS) kullanmak, anormal bağlantı taleplerini belirleyerek sunucunun korunmasına yardımcı olabilir. Web sunucularının güncel tutulması ve savunma mekanizmalarının güçlendirilmesi, Slowloris gibi sinsi saldırılara karşı en etkili önlemler arasında yer alır (Markova, 2024).



Şekil 3.9. Normal HTTP trafiği ve Slowloris saldırısı karşılaştırması

Şekil 3.9, normal HTTP bağlantısı ile Slowloris saldırısı arasındaki farkı göstermektedir. Normal bağlantıda kullanıcı, sunucuya tam bir HTTP isteği gönderir ve sunucudan yanıt alarak işlem tamamlanır. Slowloris saldırısında ise saldırgan, sunucuya ardışık ve eksik HTTP istekleri gönderir; bu istekler tamamlanmadığı için sunucu her biri için bağlantıyı açık tutar ve kaynaklarını tüketir. Böylece bağlantı havuzu dolarak sunucu, gerçek kullanıcılara hizmet veremez hale gelir. Düşük bant genişliğiyle gerçekleştirilebilen bu yöntem, etkili bir DoS saldırı tekniğidir.

3.2.1.4. ICMP flood

ICMP Flood saldırısı, hedef sistemin ağ kapasitesini ve işlem gücünü tüketerek hizmet dışı kalmasına neden olan bir DoS (Denial of Service) saldırı türüdür. Bu saldırıda, saldırgan hedef sisteme aşırı miktarda ICMP Echo Request (ping) paketleri gönderir ve sistemin her pakete yanıt vermeye çalışması, kaynaklarını hızla tüketerek ağın yavaşlamasına veya tamamen devre dışı kalmasına yol açar. Bağlantısız bir protokol olan ICMP, saldırganlar için avantaj sağlar çünkü oturum yönetimi gerektirmez, bu da büyük ölçekli trafiğin daha az çaba ile yönlendirilmesini mümkün kılar. Eğer saldırı birden fazla kaynaktan organize edilirse, Dağıtılmış Hizmet Engelleme (DDoS) saldırısı haline gelir ve hedef sistemin korunmasını daha da zorlaştırır.

Bu tür saldırılardan korunmak için ağ yöneticileri çeşitli güvenlik önlemleri almalıdır. Öncelikle, güvenlik duvarları veya ağ yönlendiricileri üzerinden ICMP trafiğine hız sınırlandırması (rate limiting) uygulanarak aşırı yüklenmenin önüne

geçilebilir. Ayrıca, Intrusion Detection Systems (IDS) ve Intrusion Prevention Systems (IPS) kullanılarak, anormal ICMP trafiği tespit edilebilir ve gerektiğinde filtrelenebilir. Kritik sistemlerde gereksiz ICMP isteklerine tamamen yanıt verilmesini engellemek de etkili bir savunma yöntemi olabilir. Özellikle büyük ölçekli ağlar için DDoS koruma hizmetleri kullanılarak bu tür saldırılar erken aşamada durdurulabilir ve sistemlerin kesintisiz çalışması sağlanabilir (Indusface ICMP Flood, 2025).

3.2.1.5. RSTFIN Flood

RST-FIN Flood saldırısı, ağ trafiğini kesintiye uğratmak amacıyla hedef sisteme sürekli olarak TCP protokolünün RST (Reset) ve FIN (Finish) bayraklarını içeren paketlerin gönderildiği bir tür Dağıtılmış Hizmet Engelleme (DDoS) saldırısıdır. Bu saldırı, özellikle durum bilgisi tutan (stateful) güvenlik cihazlarının bant genişliğini ve kaynaklarını tüketerek, ağ performansının düşmesine veya tamamen hizmet dışı kalmasına neden olabilir. Saldırganlar, geçerli bir TCP el sıkışması olmadan yüksek hızda RST-FIN paketleri göndererek, hedef sistemin bağlantılarını sonlandırmaya zorlar ve bu da meşru kullanıcıların hizmetlere erişimini engeller.

Bu tür saldırılardan korunmak için, ağ yöneticilerinin anormal trafik desenlerini tespit edebilen ve RST-FIN paketlerinin etkisini minimize edebilen gelişmiş güvenlik çözümleri uygulamaları önemlidir. Ayrıca, ağ cihazlarının en son güvenlik yamalarıyla güncel tutulması ve gereksiz veya şüpheli trafiği filtrelemek için uygun güvenlik duvarı kurallarının yapılandırılması, RST-FIN Flood saldırılarının etkisini azaltmada etkili olacaktır (DDoS-Guard, 2025).

3.2.1.6. PSH-ACK Flood

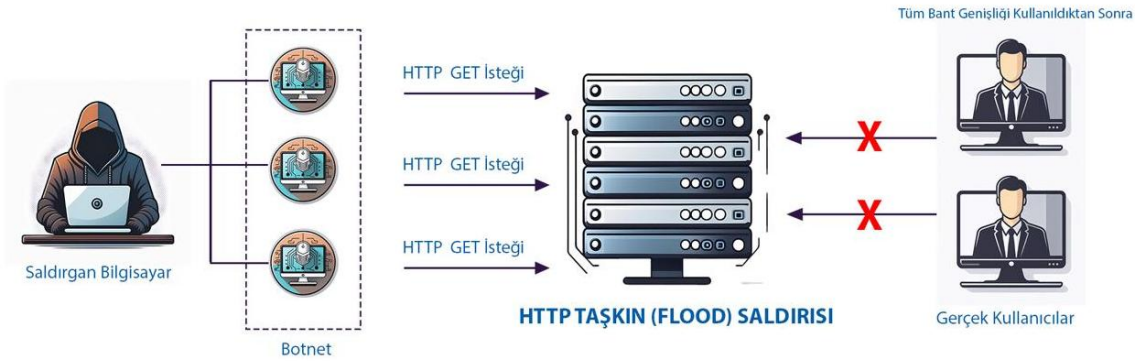
PSH-ACK Flood saldırısı, hedef sisteme aşırı miktarda sahte PSH (Push) ve ACK (Onay) bayrakları içeren TCP paketleri göndererek ağ trafiğini kontrol edilemez hale getiren bir DDoS (Distributed Denial-of-Service) saldırı türüdür. Bu saldırının temel amacı, sistem kaynaklarını tüketerek TCP tabanlı hizmetleri aksatmak ve meşru kullanıcıların hizmetlere erişimini engellemektir. Sürekli gelen yoğun trafik, sunucunun bağlantı kuyruğunu doldurarak işlem gücü ve bellek kullanımını artırır, bu da sistem performansının düşmesine ve hizmetlerin yanıt süresinin uzamasına yol açabilir. Geleneksel güvenlik duvarları (firewall) ve izinsiz giriş tespit sistemleri (IDS), sahte

PSH-ACK trafiğini meşru veri trafiğinden ayırt etmekte zorlanabilir, bu da saldırının etkisini artırarak ağ kesintilerine ve hizmet kayıplarına neden olabilir.

Al-Naeem (2021) tarafından yapılan deneysel çalışmalara göre, özellikle kablosuz sensör ağları (WSN) bu tür saldırılara karşı daha savunmasız olabilir. Çalışmada, PSH-ACK Flood saldırılarının etkilerinin 23 milisaniyelik (ms) gecikme süresi ile tespit edilebileceği ve aşırı trafik yükü nedeniyle sensör düğümlerinin hizmet dışı kalabileceği gösterilmiştir. Ayrıca, makine öğrenmesi tabanlı güvenlik çözümlerinin, geleneksel yöntemlere kıyasla daha yüksek doğruluk oranı sağlayarak bu tür saldırıları daha erken tespit edebileceği belirtilmiştir. Bu nedenle, sistemlerin anormal veri akışlarını izleyerek ve güvenlik duvarlarını uygun şekilde yapılandırarak korunması büyük önem taşımaktadır (Al-Naeem, 2021).

3.2.1.7. HTTP Flood

HTTP Flood saldırısı, hedef web sunucusunu aşırı miktarda HTTP istekleriyle bunaltarak hizmet dışı bırakmayı amaçlayan bir Dağıtılmış Hizmet Engelleme (DDoS) saldırı türüdür. Bu saldırıda, saldırganlar genellikle botnet adı verilen kötü amaçlı yazılımlarla enfekte olmuş birçok cihazı kullanarak, hedef sunucuya meşru görünümlü ancak yoğun bir trafik yönlendirirler. Bu yoğun istek trafiği, sunucunun kaynaklarını tüketerek performansın düşmesine veya tamamen erişilemez hale gelmesine neden olabilir.



Şekil 3.10. HTTP taşkın (flood) saldırısı

Şekil 3.10'da görüldüğü gibi, saldırgan bilgisayar botnet ağını yönlendirerek sunuculara HTTP GET istekleri göndermekte, bu da sunucuların tüm bant genişliğini tüketmektedir. Gerçek kullanıcılar ise artık sunuculara erişemez hale gelmekte, bu durum görselde kırmızı X işaretleriyle sembolize edilmektedir.

HTTP flood saldırıları, özellikle uygulama katmanında gerçekleştiği için tespit edilmesi ve engellenmesi zor olabilir. Saldırganlar, normal kullanıcı davranışlarını taklit eden istekler göndererek güvenlik önlemlerini aşmaya çalışırlar. Bu tür saldırılardan korunmak için, web uygulama güvenlik duvarları (WAF) kullanmak, trafiği izlemek ve anormal istekleri filtrelemek önemlidir. Ayrıca, IP kara listeleri oluşturmak, hız sınırlamaları uygulamak ve CAPTCHA gibi insan doğrulama yöntemleri kullanmak da etkili savunma stratejileri arasında yer alır (Indusface HTTP Flood, 2025).

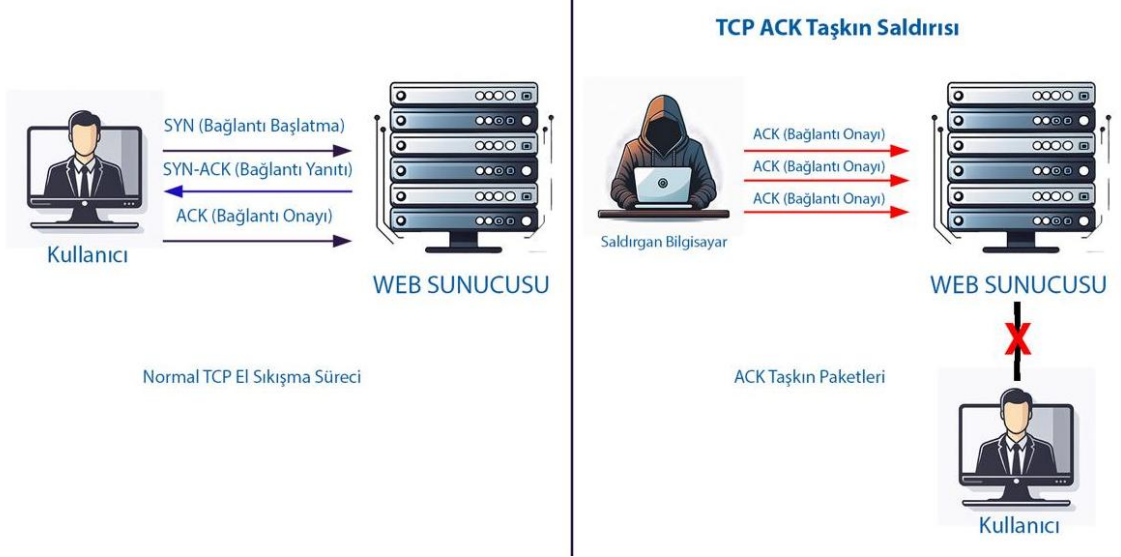
3.2.1.8. UDP Fragmentation

UDP flood saldırısının bir varyasyonu olan bu yöntemde, saldırgan büyük boyutlu (1500 bayt) UDP paketleri kullanarak daha az paketle daha fazla bant genişliği tüketmeyi hedefler. Gönderilen bu parçalanmış paketler sahte olup, gerçek birleştirme işlemi için gerekli ilişkiye sahip değildir. Hedef sunucu, bu paketleri bir araya getirmeye çalışırken gereksiz CPU kaynakları harcar. Sonuç olarak, işlemciler aşırı yüklenebilir ve hatta sunucu yeniden başlatılabilir. Bu saldırı, meşru trafiğe benzediği için tespit edilmesi zor olan bir DDoS saldırı türüdür (RioRey, 2025).

3.2.1.9. TCP Flood

TCP ACK flood saldırısı, bir hedef sunucunun ağ kaynaklarını tüketerek hizmet dışı kalmasına neden olan bir Hizmet Engelleme (DoS) saldırı türüdür. Bu saldırıda, saldırganlar hedef sunucuya büyük miktarda sahte ACK (Acknowledge) paketi gönderirler. ACK paketleri, TCP bağlantılarında veri iletiminin başarılı olduğunu onaylamak için kullanılır; ancak bu saldırıda, sunucuya aşırı sayıda sahte ACK paketi gönderilerek sunucunun kaynakları tüketilir ve performansı düşürülür.

Bu tür saldırılardan korunmak için çeşitli önlemler alınabilir. Güvenlik duvarları ve saldırı tespit sistemleri, anormal trafik desenlerini izleyerek şüpheli ACK paketlerini engelleyebilir. Ayrıca, sunucu yapılandırmalarının optimize edilmesi ve ağ kaynaklarının izlenmesi, bu tür saldırıların etkisini azaltmada önemli rol oynar. Proaktif savunma stratejileri uygulayarak, ağ yöneticileri ACK Flood saldırılarına karşı sistemlerini daha güvenli hale getirebilirler (Indusface ACK Flood, 2025).



Şekil 3.11. TCP ACK taşkın (flood) saldırısı

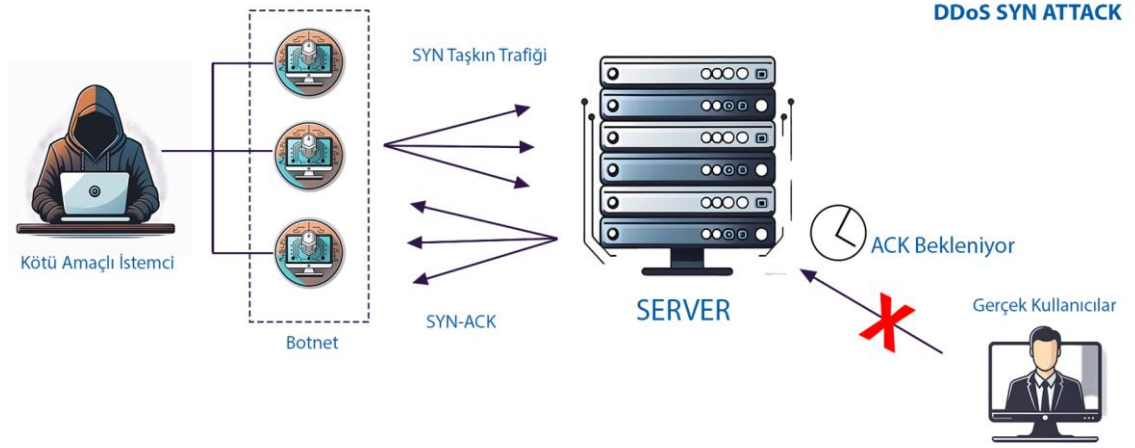
Şekil 3.11, TCP ACK Taşkın Saldırısı'nın nasıl işlediği iki aşamalı olarak göstermektedir. Sol kısımda, TCP protokolünün normal üçlü el sıkışma süreci (SYN, SYN-ACK, ACK) anlatılırken; sağ kısımda saldırganın, gerçek bağlantılarla ilgisi olmayan çok sayıda sahte ACK paketi göndererek hedef sunucuyu meşgul ettiği bir saldırı senaryosu yer almaktadır. Bu sahte ACK paketleri, sunucu kaynaklarını gereksiz yere tüketir ve meşru kullanıcıların erişimini engeller. Normal trafik gibi görüldüğü için bu saldırı güvenlik sistemlerini aşabilir ve tespiti oldukça zordur. Bu yönüyle, TCP ACK taşkın saldırısı, DDoS saldırılarının sinsi ve etkili türlerinden biridir.

3.2.1.10. SYN Flood

SYN Flood saldırısı, TCP bağlantı kurma sürecindeki güvenlik açıklarını kullanarak hedef sistemin bağlantı kuyruğunu dolduran ve yeni bağlantıları engelleyen bir saldırı türüdür. Genellikle botnetler aracılığıyla geniş çapta gerçekleştirilen bu saldırılar, meşru kullanıcıların hizmetlere erişimini zorlaştırarak sistemleri işlevsiz hale getirebilir.

Saldırı sırasında, hedef sunucuya aşırı miktarda sahte SYN paketleri gönderilir. Sunucu, her isteğe karşılık olarak SYN-ACK yanıtı verir ve bağlantının tamamlanmasını bekler. Ancak saldırgan, süreci tamamlamadığı için sunucu bekleme durumunda kalır ve bağlantı kuyruğu hızla dolar. Bu durum, yeni gelen bağlantı isteklerinin reddedilmesine ve sistemin erişilemez hale gelmesine yol açar.

Bu saldırılar, sunucunun kaynaklarını gereksiz bağlantılara tahsis ederek hizmet veremez hale gelmesine neden olur. Gerçek TCP trafiğine benzerliği nedeniyle firewall ve izinsiz giriş tespit sistemleri saldırıyı belirlemekte zorlanabilir. Özellikle büyük ölçekli botnet saldırılarında, sunucular saatlerce hizmet dışı kalabilir ve ciddi kesintilere neden olabilir. Korunma yöntemleri arasında SYN cookie kullanımı, trafik filtreleme ve bağlantı sınırlandırma gibi önlemler bulunur (Goldschmidt, 2019).



Şekil 3.12. DDoS SYN taşkın (flood) saldırısı

Şekil 3.12, DDoS (Dağıtılmış Hizmet Engelleme) saldırılarının bir alt türü olan SYN Flood saldırısının temel işleyişini şematik olarak göstermektedir. Saldırganın kontrolündeki botnet ağı, hedef sunucuya yoğun şekilde sahte SYN paketleri göndererek TCP bağlantı sürecini başlatmakta, ancak bağlantıyı tamamlayacak ACK paketlerini kasıtlı olarak göndermemektedir. Bu durum, sunucunun her gelen isteğe kaynak ayırmasına neden olmakta ve "yarım açık" bağlantılar birikerek sistem kaynaklarını tüketmektedir. Sonuç olarak, gerçek kullanıcılar sunucuya erişemez hale gelir. Görselde bu mekanizma; saldırgan, botnet, hedef sunucu ve etkilenmiş meşru kullanıcılar üzerinden sade bir şekilde gösterilmiş olup, SYN Flood saldırılarının hizmet kesintisine yol açan etkili bir DDoS yöntemi olduğunu açıkça ortaya koymaktadır.

3.2.1.11. SynonymousIP Flood

Synonymous IP Flood saldırısı, saldırganın aynı fiziksel kaynaktan veya botnetlerden farklı ancak benzer IP adresleriyle hedef sisteme yoğun trafik yönlendirdiği bir DDoS saldırı türüdür. Bu saldırının temel amacı, gelen trafiği sürekli değişen IP

adresleriyle meşru trafik gibi göstererek tespit edilmesini zorlaştırmak ve hedef sistemin hizmet dışı kalmasını sağlamaktır.

Saldırı sırasında, saldırgan veya botnet ağı, hedef sunucuya yüksek hacimli sahte trafik gönderir. Sürekli değişen IP adresleri nedeniyle saldırının kaynağını belirlemek güçleşir. Sunucu, gelen trafiği işlemede zorlanarak sistem kaynaklarını tüketir ve zamanla hizmet veremez hale gelir.

Bu saldırılar, meşru kullanıcı trafiğiyle benzerlik gösterdiği için klasik güvenlik duvarları ve filtreleme yöntemleriyle tespit edilmesi oldukça zordur. Geleneksel güvenlik önlemleri yetersiz kalabildiğinden, saldırıyı belirlemek için makine öğrenimi tabanlı analiz teknikleri kullanılmaktadır. Özellikle IP değişimini dinamik olarak yöneten bu tür saldırılar, sistemlerin güvenliğini tehdit eden en sofistike DDoS saldırıları arasında yer alır (Batra ve Dash, 2024).

3.2.2. Brute Force (Kaba Kuvvet) Saldırıları

Brute force saldırıları, siber güvenlik alanında sıkça karşılaşılan tehditlerden biridir ve kimlik doğrulama bilgilerini sistematik olarak tahmin ederek yetkisiz erişim sağlamaya çalışan bir saldırı yöntemidir (Saputra ve Noranita, 2019). IoT cihazları, genellikle düşük işlem gücüne sahip olmaları ve varsayılan fabrika ayarlarında gelen zayıf şifrelerle piyasaya sürülmeleri sebebiyle bu tür saldırılara karşı büyük bir risk altındadır (Subhan ve ark., 2023).

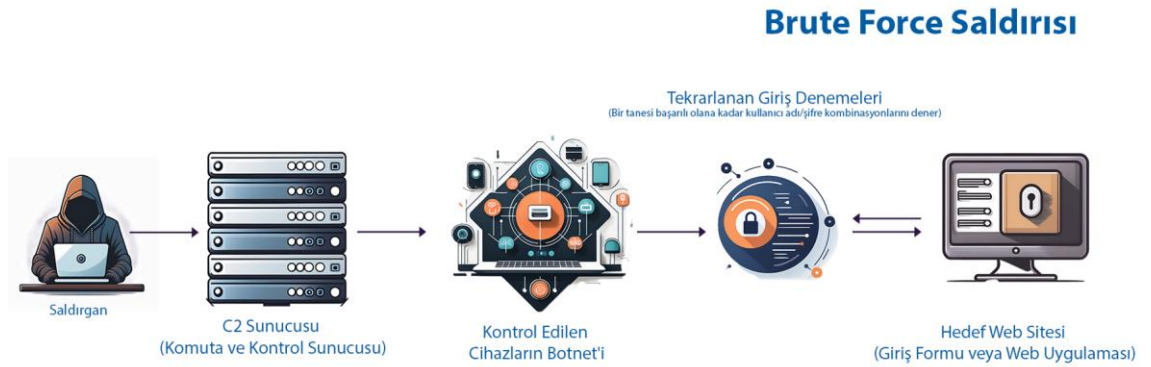
Özellikle SSH, Telnet ve HTTP kimlik doğrulama sistemleri, brute force saldırılarının en yaygın hedefleri arasında yer almaktadır. Bu sistemlerde saldırganlar, yaygın kullanılan şifreleri ve tahmin edilebilir parola kombinasyonlarını kullanarak yetkisiz erişim sağlamaya çalışmaktadır. Ele geçirilen IoT cihazları, çoğunlukla Mirai botneti gibi kötü amaçlı yazılımlar tarafından kontrol altına alınarak geniş ölçekli siber saldırılarda kullanılmaktadır (Subhan ve ark., 2023).

Brute force saldırıları arasında, özellikle dictionary brute force saldırısı öne çıkmaktadır. Bu saldırı türü, önceden hazırlanmış kelime listeleri kullanılarak yaygın parola kombinasyonlarının tahmin edilmesini esas almaktadır. Dictionary brute force saldırılarının en yaygın hedefleri, "admin", "password", "123456", "root" gibi basit ve tahmin edilebilir şifrelerdir (Saputra ve Noranita, 2019). Bu saldırı yöntemi, klasik brute force saldırılarına kıyasla daha az işlem gücü gerektirmesi ve daha hızlı çalışması nedeniyle saldırganlar tarafından sıkça tercih edilmektedir.

Brute force saldırılarına karşı IoT cihazlarının korunması için güçlü kimlik doğrulama mekanizmaları, giriş deneme sınırlamaları ve güvenli ağ yönetimi önlemlerinin uygulanması gerekmektedir. Öncelikle, IoT cihazlarının varsayılan fabrika şifreleri değiştirilmelidir ve şifrelerin en az 12 karakter uzunluğunda, büyük/küçük harf, rakam ve özel karakter içermesi sağlanmalıdır (Saputra ve Noranita, 2019). SSH gibi uzak erişim protokollerinde iki faktörlü kimlik doğrulama (2FA) zorunlu hale getirilmeli ve SSH bağlantılarında kullanılan port numaraları değiştirilerek saldırı yüzeyi daraltılmalıdır (Subhan ve ark., 2023).

Bunun yanı sıra, belirli sayıda başarısız giriş denemesinden sonra IP engelleme mekanizmaları uygulanmalı ve makine öğrenmesi tabanlı tehdit algılama sistemleriyle anormal trafik hareketleri izlenmelidir (Saputra ve Noranita, 2019). IoT cihazları, ağ segmentasyonu yapılarak ana ağdan izole edilmeli ve yalnızca belirlenen IP adreslerinden erişime izin verilmelidir. Ayrıca, güvenlik duvarları (firewall) ve saldırı tespit sistemleri (IPS/IDS) kullanılarak yetkisiz erişim girişimleri engellenmelidir.

Son olarak, IoT üreticileri tarafından cihazlara düzenli güvenlik güncellemeleri ve firmware yamaları sağlanmalıdır. Kullanıcılar, bu güncellemeleri takip etmeli ve güvenlik açıklarını kapatan yamaları zamanında yüklemelidir (Saputra ve Noranita, 2019).



Şekil 3.13. Brute force (kaba kuvvet) saldırısı

Şekil 3.13, Brute Force (Kaba Kuvvet) saldırısının temel işleyişini ve bileşenlerini şematik olarak sunmaktadır. Saldırgan, C2 (Komuta ve Kontrol) sunucusu aracılığıyla kontrol ettiği botnet'e komutlar göndererek hedef web sistemine yönelik sistematik şifre denemeleri başlatır. Botnet, farklı kullanıcı adı ve şifre kombinasyonlarını otomatik biçimde deneyerek doğru eşleşmeyi bulmaya çalışır. Bu süreç, hedef sistemde bir zayıflık bulunana kadar veya tüm olasılıklar tükenene dek devam eder.

Sonuç olarak, brute force saldırıları, özellikle IoT sistemlerinde kimlik doğrulama açıklarından kaynaklanan ciddi güvenlik zafiyetlerine neden olmaktadır. Bu tür saldırılara karşı, güçlü kimlik doğrulama mekanizmalarının benimsenmesi, giriş deneme sınırlamalarının uygulanması, ağ segmentasyonu ve güncel yazılım kullanımı gibi proaktif güvenlik önlemleri hayata geçirilmelidir. Dictionary brute force saldırıları gibi yaygın kullanılan tekniklere karşı, zayıf parolalardan kaçınılmalı ve modern güvenlik stratejileri benimsenmelidir. Bu doğrultuda, IoT cihazlarının kötü amaçlı yazılımlar tarafından ele geçirilme riski minimize edilerek, daha güvenli ve sürdürülebilir bir internet altyapısı oluşturulabilir.

3.2.3. Spoofing (Sahtecilik) Saldırıları

IoT, fiziksel cihazların internet üzerinden birbirine bağlanmasını sağlayan bir sistemdir. Ancak, bu sistemin güvenlik açıkları, kötü niyetli saldırganların çeşitli siber saldırılar gerçekleştirmesine olanak tanımaktadır. IoT ağlarına yönelik en yaygın tehditlerden biri spoofing saldırılarıdır. Bu tür saldırılar, saldırganların meşru bir ağ kaynağının kimliğini taklit ederek yetkisiz erişim elde etmesine veya hedef sistemleri sahte verilerle manipüle etmesine dayanır. ARP (Address Resolution Protocol) Spoofing ve DNS (Domain Name System) Spoofing, IoT cihazlarını etkileyen en kritik spoofing türleri olup, ağ güvenliğini zayıflatarak veri gizliliğinin ihlaline, oturum ele geçirme girişimlerine ve hizmet kesintilerine neden olabilir (Hamza ve ark., 2018; Satılmış ve Akleyek, 2021).

3.2.3.1. ARP Spoofing

ARP (Address Resolution Protocol) spoofing, ağ üzerindeki cihazlara sahte ARP yanıtları göndererek trafiği manipüle etmeye yönelik bir saldırı tekniğidir. Bu saldırılar, özellikle yönlendirilmiş hizmet reddi (DoS) saldırıları, Man-in-the-Middle (MitM) saldırıları ve veri manipülasyonu gibi güvenlik ihlallerinde sıkça kullanılmaktadır (Mvah ve ark., 2024).

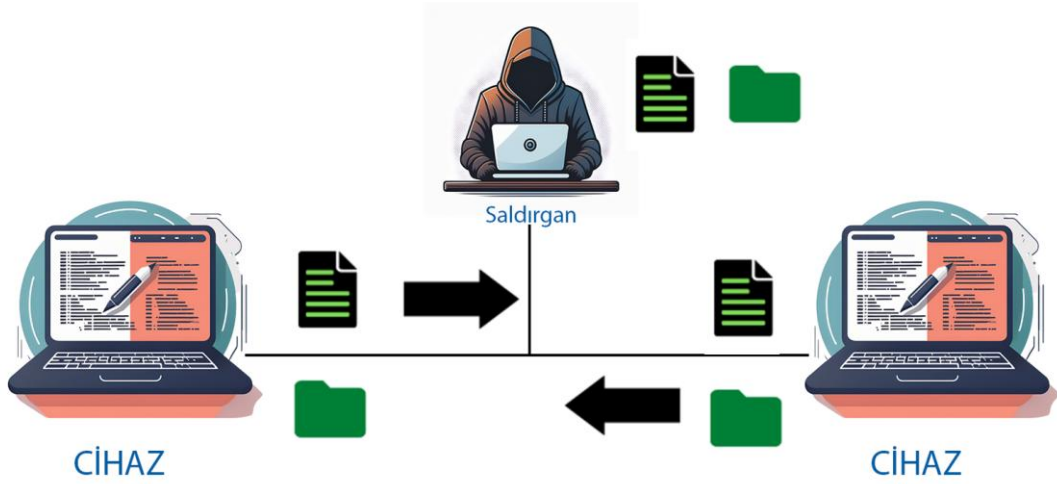
Bu saldırı, ağdaki cihazların ARP tablolarını manipüle ederek saldırganın kendisini güvenilir bir ağ kaynağı gibi göstermesine dayanır. Saldırının işleyişi şu şekilde özetlenebilir:

1. Saldırgan, meşru cihazların ARP tablolarını değiştirmek için sahte ARP yanıtları gönderir.
2. Hedef cihazlar, bu sahte yanıtları doğru kabul ederek trafiği saldırganın yönlendirdiği noktaya iletir.
3. Saldırgan, yönlendirdiği ağ trafiğini izleyebilir, değiştirebilir veya farklı bir hedefe yönlendirebilir. Bu durum, gizli veri sızıntısı ve kimlik avı saldırıları gibi ciddi güvenlik açıklarına yol açabilir.

ARP spoofing saldırıları, ağ güvenliğini zayıflatarak birçok tehdide neden olabilir.

Man-in-the-Middle (MitM) saldırıları gerçekleştirme imkânı sunarak, saldırganın kullanıcıların iletişimini izlemesine veya manipüle etmesine neden olabilir. Yetkisiz veri erişimi sağlayarak, gizli bilgilerin çalınmasına veya sahte yönlendirmeler aracılığıyla kullanıcıların yanıltılmasına sebep olabilir. Hizmet aksaklıklarına yol açarak, ağ trafiğini kesintiye uğratabilir ve hedef sistemlerin işlevselliğini bozabilir.

ARP Sahtekarlığı(Spoofing)



Şekil 3.14. ARP sahtekarlığı (spoofing) saldırısı

Şekil 3.14, ARP sahtekarlığı (ARP spoofing) saldırısının temel işleyişini şematik olarak göstermektedir. Bu senaryoda, saldırgan yerel ağ üzerindeki ARP trafiğini manipüle ederek cihazlar arası veri akışını kendi üzerinden yönlendirmekte ve böylece bir ortadaki adam (Man-in-the-Middle, MitM) saldırısı gerçekleştirmektedir. Saldırgan, sahte ARP mesajları ile iki meşru cihazın birbirine ait MAC adresi bilgisini değiştirerek, verilerin önce kendisine, ardından hedef cihaza ulaşmasını sağlar. Bu sayede ağ trafiğini pasif olarak izleyebilir veya aktif şekilde müdahale edebilir.

ARP spoofing saldırılarının önlenmesi için geliştirilen stratejiler özellikle yazılım tanımlı ağlar (SDN) tabanlı çözümlerle saldırıların tespit edilmesi ve engellenmesine odaklanmaktadır (Mvah ve ark., 2024). Bu kapsamda önerilen başlıca korunma yöntemleri şunlardır:

Dinamik ARP Denetimi (DAI), SDN tabanlı ağlarda sahte ARP yanıtlarının filtrelenmesini sağlayarak saldırı girişimlerini engeller. Makine öğrenimi destekli tespit mekanizmaları, ağ trafiğindeki anomalileri analiz eden algoritmalar aracılığıyla ARP spoofing saldırılarını erken tespit etmeye yardımcı olabilir. SDN tabanlı oyun teorisi yaklaşımı, ağ trafiğini modelleyerek saldırı olasılıklarını minimize eden güvenlik politikaları geliştirilmesini sağlar (Mvah ve ark., 2024). Statik ARP tabloları kullanımı, belirli cihazların ARP adreslerini sabitleyerek saldırganların sahte ARP mesajları ile ağı manipüle etmesini zorlaştırır.

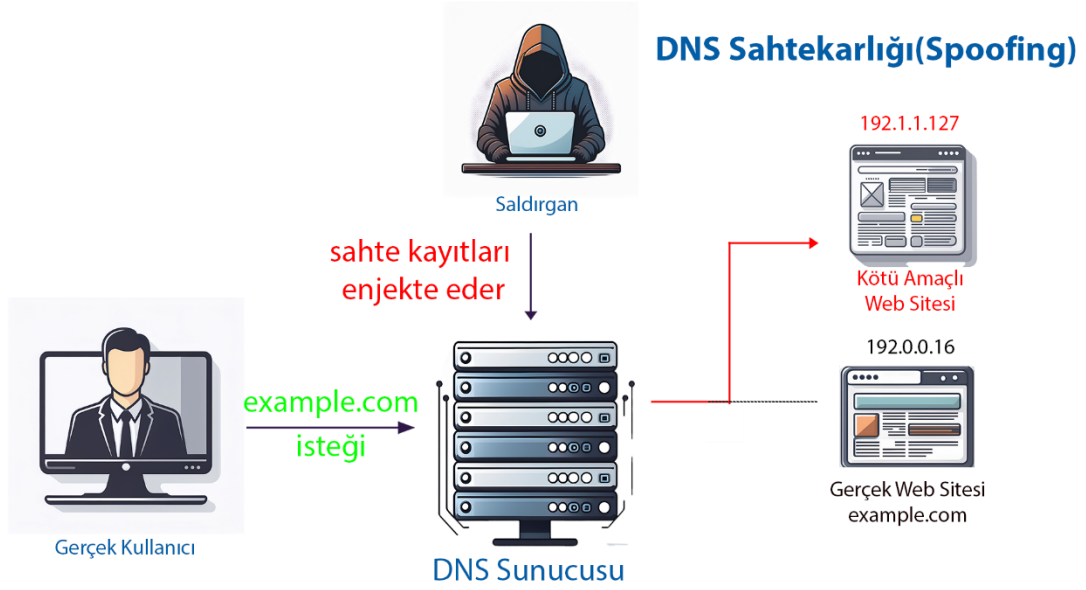
Bu yöntemlerin uygulanması, ağ güvenliğini artırarak ARP spoofing kaynaklı tehditlerin minimize edilmesini sağlayabilir. Özellikle SDN tabanlı çözümler, saldırıların daha etkin bir şekilde tespit edilmesine ve ağ güvenliğinin güçlendirilmesine katkı sunmaktadır.

3.2.3.2. DNS Spoofing

DNS Spoofing, kullanıcıları sahte web sitelerine yönlendiren bir siber saldırı türüdür. Saldırganlar, DNS (Domain Name System) yanıtlarını manipüle ederek kullanıcıları yanlış IP adreslerine yönlendirir. Bu saldırı genellikle DNS önbellek zehirlenme (DNS Cache Poisoning) yöntemiyle gerçekleştirilir ve kullanıcıların farkında olmadan kimlik avı, veri hırsızlığı ve kötü amaçlı yazılım bulaşan sitelere bağlanmasına neden olur. Sahte DNS yanıtları, meşru DNS sorgularına müdahale edilerek oluşturulur ve DNS sunucularının önbelleğine eklenerek geniş çapta kullanıcıları etkileyebilir. Sonuç olarak, kullanıcılar güvenilir sandıkları platformlara giriş yaparken kimlik bilgilerini kaybedebilir veya cihazlarına zararlı yazılımlar yükleyebilir.

Bu tür saldırılara karşı DNSSEC (Domain Name System Security Extensions), güvenilir DNS sunucuları ve şifreli DNS protokolleri (DoH, DoT) gibi güvenlik önlemleri alınmalıdır. Intrusion Detection System (IDS) ile DNS trafiği izlenerek şüpheli aktiviteler tespit edilebilir. Bu güvenlik önlemleri, saldırganların sahte yanıtlar oluşturmalarını zorlaştırarak DNS trafiğini daha güvenli hale getirir. DNS Spoofing saldırıları, bireyler ve kuruluşlar için ciddi güvenlik tehditleri oluşturduğundan, siber güvenlik farkındalığını

artırmak ve proaktif savunma stratejileri geliştirmek büyük önem taşır (Adiwal ve ark., 2023).



Şekil 3.15. DNS sahtekarlığı (DNS spoofing) saldırısı

Şekil 3.15, DNS sahtekarlığı (DNS spoofing) saldırısının temel bileşenlerini ve işleyiş sürecini şematik olarak sunmakta olup, saldırganın DNS sistemine sahte kayıtlar enjekte ederek kullanıcıları sahte bir web sitesine yönlendirdiği bir durumu temsil etmektedir. Kullanıcı "example.com" adresine erişmek istediğinde, DNS sunucusu saldırgan tarafından manipüle edilmiş kayıtlar nedeniyle gerçek IP adresi yerine kötü amaçlı sitenin IP'sini döndürmekte, böylece kullanıcı sahte bir siteye yönlendirilmektedir.

3.2.4. DoS (Denial of Service) Saldırıları

DoS saldırısı, bir sistemin, ağın veya servisin normal işleyişini aksatmayı amaçlayan kötü niyetli bir saldırdır. Bu saldırılar genellikle hedef sistemin kaynaklarını aşırı yükleyerek meşru kullanıcıların hizmetlere erişimini engeller. Saldırganlar, bir hizmete aşırı sayıda istek göndererek sunucunun işlem gücünü ve bant genişliğini tüketir. IoT cihazları, sınırlı işlem gücü ve bellek kapasitesine sahip oldukları için DoS saldırılarına karşı daha savunmasızdır. Saldırganlar, IoT cihazlarının ağ protokollerindeki güvenlik açıklarını hedef alarak cihazların işlevselliğini devre dışı bırakabilirler.

DoS saldırıları farklı tekniklerle gerçekleştirilebilir. Flooding saldırılarında, hedef sistemin bant genişliği veya işlem gücü büyük miktarda veri gönderilerek tüketilir. Protokol istismarı saldırılarında, TCP SYN Flood ve UDP Flood gibi yöntemler kullanılarak ağ protokollerindeki zayıflıklar istismar edilir. Uygulama katmanı saldırılarında ise, HTTP GET veya POST flood gibi yöntemlerle belirli bir hizmete yoğun talep oluşturularak sunucu kaynakları tükenir. Bu tür saldırılar, özellikle IoT cihazlarında büyük ölçekli hizmet kesintilerine yol açabilir ve sistem güvenliğini ciddi şekilde tehdit edebilir (Şimşek ve Atılğan, 2024).

3.2.5. Reconnaissance (Keşif) Saldırıları

Keşif (Reconnaissance) saldırıları, saldırganların hedef sistem hakkında bilgi toplamak amacıyla gerçekleştirdiği siber saldırı türlerinden biridir. Bu saldırılar doğrudan zarar vermekten ziyade, daha büyük ve yıkıcı saldırılar için ön hazırlık niteliği taşır. Hedef ağın açık portlarını, işletim sistemini ve güvenlik açıklarını belirlemek için çeşitli teknikler kullanılır. IoT sistemlerinde, açık portları ve çalışan servisleri analiz ederek ilerleyen aşamalarda gerçekleştirilecek saldırılar için zemin hazırlanır. CIC-IoT 2023 veri setinde de yer alan bu saldırılar, genellikle büyük ölçekli tehditlerin ilk aşamasını oluşturur ve saldırganların hedef sistemin ağ yapısını anlamasına yardımcı olur (Neto ve ark., 2023; Sayed ve Hassanien, 2024).

Keşif saldırıları, genellikle doğrudan zarar vermek yerine daha büyük saldırılar için bilgi toplama amacıyla gerçekleştirilir. Bu saldırılardan korunmak için ağ izleme sistemleri, güçlü şifreleme yöntemleri, güvenlik duvarları ve düzenli sızma testleri uygulanmalıdır. Özellikle IoT sistemleri gibi geniş ağ yapılarında, saldırganların bilgi toplamasını engellemek için sıkı güvenlik önlemleri alınması gereklidir.

3.2.5.1. Ping Tarama (Ping Sweep)

Ping Sweep, saldırganların bir ağ üzerindeki aktif cihazları belirlemek için ICMP (Internet Control Message Protocol) Echo Request paketleri göndermesiyle gerçekleşir. Yanıt veren cihazlar tespit edilerek potansiyel hedefler belirlenir ve saldırganlar hangi cihazların açık olduğunu anlamış olur (Haque ve ark., 2023; Neto ve ark., 2023).

3.2.5.2. İşletim Sistemi Tarama (OS Scan)

Bir sistemin işletim sistemi türünü ve sürümünü belirlemek için özel ağ paketleri gönderilir. Gelen yanıtlar, işletim sisteminin imzalarını içerir ve saldırganlar bu bilgiyi kullanarak güvenlik açıklarını tespit edebilir (Haque ve ark., 2023; Neto ve ark., 2023).

3.2.5.3. Zafiyet Tarama (Vulnerability Scan)

Otomatik araçlar kullanılarak sistemdeki güvenlik açıkları, eksik yamalar, yanlış yapılandırmalar ve eski yazılımlar taranır. Bu bilgiler, saldırganın hedef sistemde en zayıf noktaları bulmasına olanak tanır (Neto ve ark., 2023).

3.2.5.4. Port Tarama (Port Scan)

Saldırgan, hedef sistemde hangi portların açık olduğunu belirlemek için çeşitli tarama teknikleri uygular. Açık portlar, saldırganın hangi servislerin çalıştığını anlamasına yardımcı olur ve bu servislere yönelik özel saldırılar düzenlenebilir (Neto ve ark., 2023).

3.2.5.5. Cihaz Keşfi (Host Discovery)

Bir ağda hangi cihazların aktif olduğunu ve hangi IP adreslerini kullandığını belirlemek için gerçekleştirilir. Bu saldırı, ağda bulunan cihazların tespit edilmesini ve saldırganın hedeflerini daraltmasını sağlar (Neto ve ark., 2023).

Bu keşif saldırıları, saldırganların ağ yapısını ve güvenlik açıklarını belirleyerek daha karmaşık saldırılar gerçekleştirmesine yardımcı olur. Özellikle IoT cihazları gibi savunmasız ağlarda sıkça uygulanmaktadır.

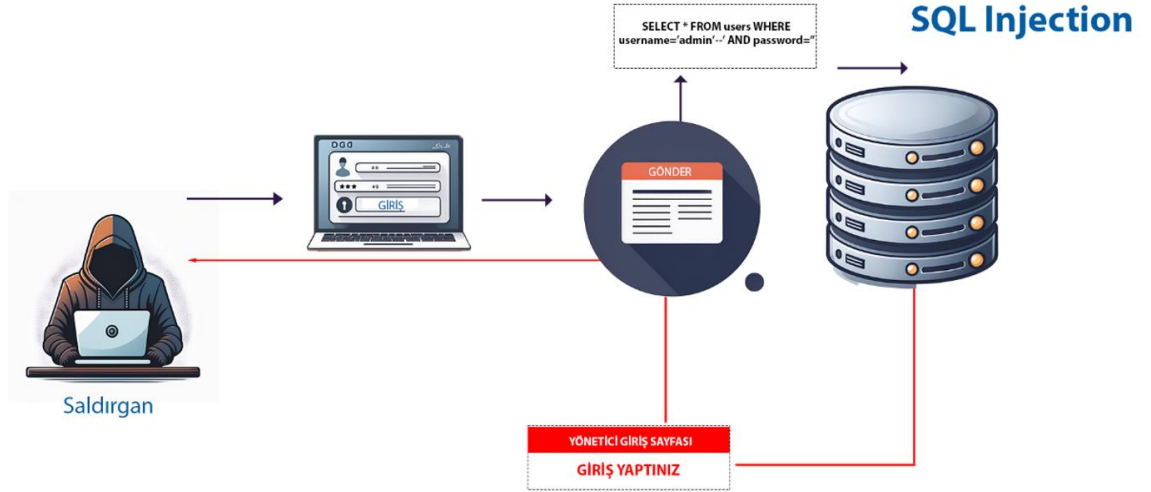
3.2.6. Web-Based (Web Tabanlı) Saldırıları

3.2.6.1. SQL Injection

SQL enjeksiyonu, bir web uygulamasının kullanıcı girdilerini yeterince filtrelemediği durumlarda, saldırganların kötü niyetli SQL sorguları enjekte etmesine olanak tanıyan bir güvenlik açığıdır. Bu tür saldırılar, veri tabanındaki bilgilerin yetkisiz

şekilde erişilmesine, değiştirilmesine veya silinmesine neden olabilir. Özellikle, kullanıcı giriş formları, arama kutuları ve URL parametreleri gibi dinamik veri giriş noktaları hedef alınarak veri tabanı manipüle edilebilir. Saldırganlar, SQL komutlarını kullanarak sistemdeki oturum açmış kullanıcıların kimlik bilgilerini çalabilir, veri tabanına zararlı kodlar ekleyerek sistemin bütünlüğünü bozabilir veya tüm veri tabanını silebilirler. Veri tabanı sunucusunun yapısına bağlı olarak, SQL enjeksiyonu saldırıları yalnızca belirli tabloları etkilemekle kalmayıp tüm sistemin kontrolünü ele geçirmeye kadar ilerleyebilir.

Bu tür saldırıları önlemek için, geliştiricilerin güvenli kodlama tekniklerini benimsemesi gerekmektedir. Öncelikli olarak, parametrelili sorgular (prepared statements) ve saklı prosedürler kullanılarak kullanıcı girdilerinin doğrudan SQL sorgularına dahil edilmesi engellenmelidir. Ayrıca, giriş doğrulama ve temizleme yöntemleri uygulanarak yalnızca beklenen formatta verilerin kabul edilmesi sağlanmalıdır. Web uygulamalarında, veri tabanı kullanıcılarına en düşük yetkilerin atanması da olası bir saldırının etkisini sınırlandıracaktır. Güvenlik duvarları, saldırı tespit sistemleri ve düzenli güvenlik testleri ile sistem sürekli izlenmeli ve olası zafiyetler giderilmelidir. SQL enjeksiyonu, yaygın ancak önlenabilir bir güvenlik açığıdır ve modern yazılım geliştirme süreçlerinde bu tür tehditlere karşı proaktif önlemler alınmalıdır (OWASP SQL Injection, 2025).



Şekil 3.16. SQL enjeksiyonu (SQL Injection) saldırısı

Şekil 3.16, SQL Injection (SQL Enjeksiyonu) saldırısının temel bileşenlerini ve işleyişini şematik olarak göstermekte olup, saldırıanın web uygulamasındaki kullanıcı giriş alanlarına kötü amaçlı SQL komutları enjekte ederek veritabanına yetkisiz erişim sağlamasını konu almaktadır. Yetersiz giriş doğrulamasına sahip formlar aracılığıyla iletilen bu sorgular, veritabanı tarafından doğrudan çalıştırılmakta ve saldırıanın veri

okuma, değiştirme veya silme gibi işlemler gerçekleştirmesine olanak tanımaktadır. Görselde, bu süreç saldırgan, web arayüzü, SQL sorgusu ve hedef veritabanı arasındaki etkileşimlerle birlikte sunulmakta ve başarılı bir enjeksiyon sonucunda yönetici paneline yetkisiz erişimin sağlanabileceği vurgulanmaktadır. Bu saldırı türü, güvenlik kontrolleri yetersiz olan sistemler için ciddi bir tehdit oluşturmaktadır.

3.2.6.2. Command Injection

Komut Enjeksiyonu (Command Injection), bir uygulamanın kullanıcıdan aldığı verileri yeterince doğrulamadığı durumlarda ortaya çıkan kritik bir güvenlik açığıdır. Bu zafiyet, saldırganların uygulama üzerinden işletim sistemine ait komutları çalıştırmasına olanak tanır. Örneğin, bir web uygulaması kullanıcıdan dosya adını alıp bu adı bir sistem komutunda kullanıyorsa ve bu girdi uygun şekilde filtrelenmiyorsa, saldırganlar bu mekanizmayı kötüye kullanarak sunucuda yetkisiz komutlar çalıştırabilirler. Bu tür saldırılar, hassas verilerin ifşasına, sistem bütünlüğünün bozulmasına ve sunucunun tamamen ele geçirilmesine kadar varan ciddi sonuçlara yol açabilir.



Şekil 3.17. Komut enjeksiyonu (Command Injection) saldırısı

Şekil 3.17, Komut Enjeksiyonu saldırısının temel bileşenlerini ve işleyişini şematik olarak sunmakta olup, saldırganın zafiyet içeren bir yazılım aracılığıyla sistem komutlarını yetkisiz şekilde çalıştırmasını konu almaktadır. Saldırgan tarafından hazırlanan zararlı komutlar, yeterli giriş doğrulaması yapılmadan doğrudan işletim sistemi düzeyinde yürütülmekte ve bu durum, özellikle güvenlik önlemleri zayıf olan IoT cihazları için ciddi tehdit oluşturmaktadır. Komut enjeksiyonu sonucunda saldırgan, sistemde yetki yükseltebilir, veri çalabilir veya kalıcı arka kapılar oluşturabilir. Bu saldırı

türü, yazılım bileşenlerinin kullanıcı girdilerini doğrudan komut satırına aktarması durumunda ortaya çıkan kritik bir güvenlik açığıdır.

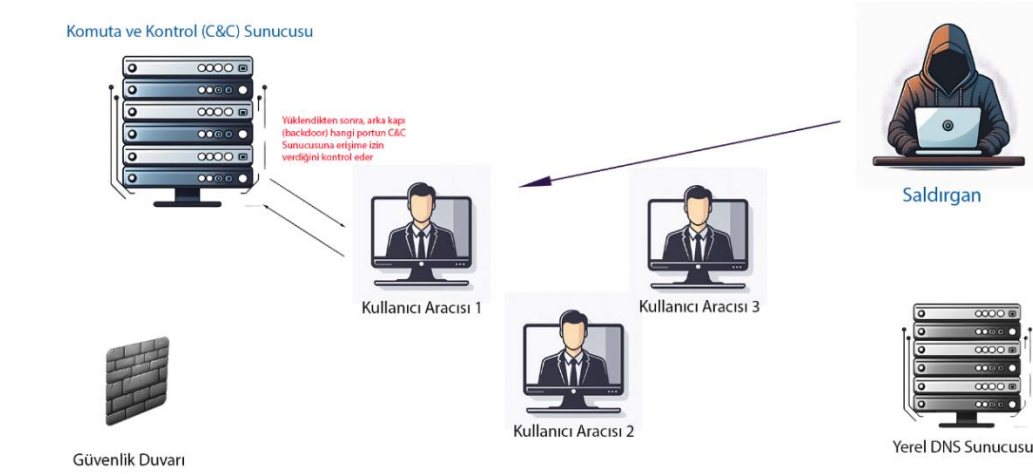
Komut enjeksiyonu saldırılarını önlemek için, geliştiricilerin kullanıcı girdilerini titizlikle doğrulamaları ve temizlemeleri esastır. Parametrelili sorgular veya güvenli API'ler kullanarak kullanıcı girdilerinin doğrudan sistem komutlarına dahil edilmesini engellemek, bu tür saldırılara karşı etkili bir koruma sağlar. Ayrıca, uygulamanın çalıştığı ortamda en az ayrıcalık ilkesini benimsemek, olası bir saldırının etkisini minimize eder. Düzenli güvenlik testleri ve kod incelemeleriyle potansiyel zafiyetlerin erken tespiti ve giderilmesi, uygulamaların güvenliğini artırmada kritik bir rol oynar (Zhong, 2025).

3.2.6.3. Backdoor Malware

Backdoor (Arka Kapı), bir bilgisayar sistemine, ağa veya yazılım uygulamasına normal güvenlik önlemlerini atlayarak yetkili veya yetkisiz kullanıcıların yüksek düzeyde erişim (örneğin, yönetici erişimi) elde etmelerini sağlayan gizli yöntemleri ifade eder. Bu tür arka kapılar, kötü niyetli aktörler tarafından sisteme sızmak, kişisel ve finansal verileri çalmak, ek kötü amaçlı yazılımlar yüklemek veya cihazları ele geçirmek için kullanılabilir. Örneğin, bir saldırgan, bir arka kapı aracılığıyla sisteme erişim sağlayarak, kullanıcıların fark etmeden verilerini çalabilir veya sistemde zararlı işlemler gerçekleştirebilir.

Arka kapılar her zaman kötü niyetli amaçlarla oluşturulmaz; bazı durumlarda, yazılım veya donanım üreticileri, ürünlerine daha sonra erişim sağlamak amacıyla kasıtlı olarak arka kapılar yerleştirebilirler. Ancak, bu tür arka kapılar, keşfedildiklerinde kötü niyetli kişiler tarafından da istismar edilebilir, bu da ciddi güvenlik açıklarına yol açabilir. Bu nedenle, sistemlerin ve yazılımların düzenli olarak güncellenmesi, güçlü parolalar kullanılması ve güvenilir güvenlik yazılımlarıyla korunması, arka kapıların oluşturabileceği potansiyel tehditlere karşı alınabilecek önemli önlemler arasındadır (Malwarebytes Backdoor, 2025).

Siber Güvenlikte Arka Kapı (Backdoor) Saldırısı



Şekil 3.18. Siber güvenlikte arka kapı (backdoor) saldırısı

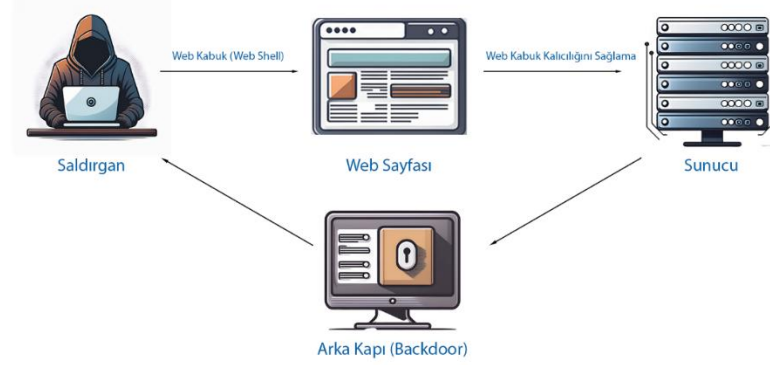
Şekil 3.18, Arka Kapı (backdoor) saldırısının temel bileşenlerini ve işleyiş mekanizmasını şematik olarak sunmakta olup, saldırganın hedef sisteme gizli erişim noktaları oluşturarak Komuta ve Kontrol (C&C) sunucusu aracılığıyla uzaktan yetkisiz erişim sağladığı bir senaryoyu temsil etmektedir. Arka kapı yazılımı genellikle zafiyet istismarı, kötü amaçlı yazılımlar veya sahte güncellemeler yoluyla sisteme yerleştirilir ve çalışmaya başladığında güvenlik duvarlarını bypass ederek C&C sunucusuna bağlanır. Bu bağlantı üzerinden saldırgan, sistemi kontrol etme, veri sızdırma ve kalıcı erişim sağlama gibi zararlı faaliyetlerde bulunabilir. Görselde çoklu kullanıcı arayüzleri, DNS sunucusu ve güvenlik duvarı gibi bileşenlerle saldırının ağ üzerindeki etkisi bütünsel biçimde gösterilmekte olup, arka kapıların siber güvenlik açısından ciddi bir tehdit oluşturduğuna işaret edilmektedir.

3.2.6.4. Uploading Attack

Yükleme saldırısı (uploading attack), web uygulamalarında saldırganların kötü niyetli dosyaları sunucuya yüklemelerine olanak tanıyan kritik bir güvenlik açığıdır. Bu açık, saldırganların sunucuda zararlı kod çalıştırmasına, dosya sistemini aşırı yüklemesine veya istemci tarafında saldırılar gerçekleştirmesine imkan tanır. Örneğin, saldırganlar zararlı bir dosyayı yükleyerek sunucuda komut çalıştırabilir veya diğer sistemlere saldırılar düzenleyebilirler. Ayrıca, yüklenen dosyalar aracılığıyla web

sitesinin içeriği değiştirilebilir veya kullanıcıların tarayıcılarında zararlı kodlar çalıştırılabilir.

Uploading Attack



Şekil 3.19. Yükleme saldırısı (uploading attack) ve web kabuk (web shell) enjeksiyon mekanizması

Şekil 3.19, Yükleme Saldırısı olarak bilinen siber saldırı türünün temel işleyişini ve bileşenlerini şematik olarak sunmakta olup, saldırganın hedef web uygulamasındaki güvenlik açıklarını kullanarak kötü amaçlı bir web kabuğunu (web shell) sunucuya yüklemesiyle gerçekleştirilen bir süreci temsil etmektedir. Yüklenen zararlı betik, sunucuda çalıştırılarak saldırgana uzaktan komut yürütme ve sistem üzerinde kontrol sağlama imkânı tanır. Saldırgan, bu kabuğu kullanarak sistemde kalıcı arka kapılar oluşturabilir ve sunucu yeniden başlatılsa dahi erişimini sürdürebilir. Bu saldırı türü, sunucu taraflı dosya yükleme mekanizmalarının yeterli doğrulama ve filtreleme yapılmadan tasarlanması durumunda ciddi güvenlik riskleri doğurmaktadır.

Bu tür saldırıları önlemek için, dosya yükleme işlemlerinde dosya türü, boyutu ve içeriği gibi özelliklerin sıkı bir şekilde doğrulanması gerekmektedir. Ayrıca, yüklenen dosyaların sunucuda çalıştırılabilir alanlara kaydedilmemesi ve dosya isimlerinin güvenli bir şekilde işlenmesi önemlidir. Güvenlik duvarları ve antivirüs yazılımları gibi ek güvenlik önlemleri de alınarak, potansiyel tehditlerin etkisi minimize edilebilir (OWASP File Upload, 2025).

3.2.6.5. XSS (Cross-Site Scripting)

Siteler Arası Betik Çalıştırma (XSS), saldırganların güvenilir web sitelerine kötü amaçlı kod enjekte etmelerine olanak tanıyan bir güvenlik açığıdır. Bu açık, genellikle

web uygulamalarının kullanıcı girdilerini yeterince doğrulamadığı veya uygun şekilde filtrelemediği durumlarda ortaya çıkar. Saldırganlar, bu zafiyetten yararlanarak, kullanıcıların tarayıcılarında zararlı komut dosyaları çalıştırabilir ve böylece çerezler, oturum jetonları veya diğer hassas bilgilere erişim sağlayabilirler. Ayrıca, bu tür saldırılar kullanıcıları sahte web sitelerine yönlendirebilir veya mevcut sayfanın içeriğini değiştirebilir (KirstenS, 2025).

XSS açıkları üç ana kategoriye ayrılır: Yansıtılmış (Reflected), Saklı (Stored) ve DOM Tabanlı (DOM-based) XSS. Yansıtılmış XSS, saldırıncının zararlı kodunun bir HTTP isteğiyle gönderildiği ve sunucunun bu kodu hemen yanıt olarak geri döndürdüğü durumlardır. Saklı XSS ise, zararlı kodun sunucuda depolandığı ve daha sonra diğer kullanıcılar tarafından erişildiği durumlardır; örneğin, bir blog yorumunda veya forum mesajında. DOM Tabanlı XSS ise istemci tarafında çalışan JavaScript kodlarının, kullanıcı girdilerini güvensiz bir şekilde işlemesi sonucu ortaya çıkar. Her üç tür de, kullanıcıların tarayıcılarında zararlı kodların çalıştırılmasına ve ciddi güvenlik ihlallerine yol açabilir (PortSwigger, 2025)

Depolanmış siteler arası komut çalıştırma (Stored XSS)



Şekil 3.20. Depolanmış XSS (stored cross-site scripting) saldırısı

Şekil 3.20, depolanmış XSS (Cross-Site Scripting) saldırısının temel bileşenlerini ve işleyiş sürecini şematik olarak sunmakta olup, saldırıncının bir web sitesindeki yetersiz giriş filtrelemesinden yararlanarak zararlı JavaScript kodlarını kalıcı olarak siteye enjekte etmesiyle başlayan bir süreci temsil etmektedir. Söz konusu zararlı kod, siteyi ziyaret eden kullanıcıların tarayıcılarında otomatik olarak çalışmakta ve oturum çerezleri gibi hassas bilgileri saldırıncının kontrolündeki sunucuya iletmektedir.

3.2.6.6. Browser Hijacking

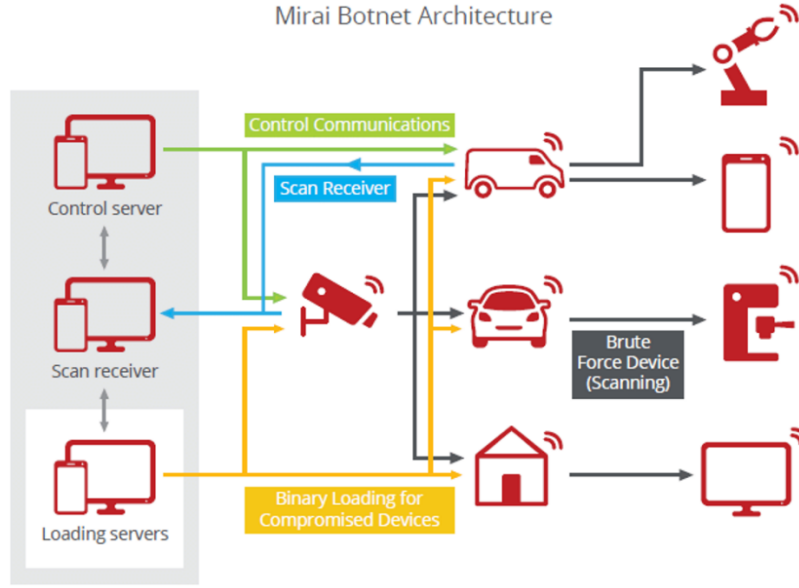
Tarayıcı Ele Geçirme (Browser Hijacking), kullanıcıların bilgisi veya izni olmadan internet tarayıcılarının ayarlarını değiştiren bir tür kötü amaçlı yazılımdır. Genellikle, ana sayfa ve varsayılan arama motoru ayarlarını değiştirirler. Bazıları, kullanıcıları belirli sitelere yönlendirerek reklam gelirini artırmayı hedefler. Daha tehlikeli olanları, kullanıcıların tuş vuruşlarını kaydederek banka hesap bilgileri gibi hassas verileri çalabilir.

Bu tür yazılımlar genellikle ücretsiz yazılımlarla birlikte gelen araç çubukları veya üçüncü taraf sitelerden indirilen programlar aracılığıyla sisteme bulaşır. Bazıları, ziyaret edilen sitelere gömülü kodlar veya açılır pencereler yoluyla da bulaşabilir. Tarayıcı ele geçirme yazılımları, sistem kararlılığını bozabilir ve kullanıcı deneyimini olumsuz etkileyebilir. Kendilerini kalıcı kılmak için sistem kayıt defterinde değişiklikler yapabilirler, bu da kaldırılmalarını zorlaştırır (Malwarebytes Browser Hijacker, 2025).

3.2.7. Mirai Botnet Saldırıları

Mirai botnet, gömülü sistemler ve IoT cihazlarını hedef alarak büyük ölçekli dağıtılmış hizmet reddi (DDoS) saldırıları gerçekleştiren kötü amaçlı bir yazılım türüdür. İlk olarak 2016 yılında tespit edilen bu zararlı yazılım, zayıf güvenlik önlemlerine sahip IoT cihazlarını ele geçirerek geniş çaplı bir botnet ağı oluşturmuş ve kritik internet altyapılarını hedef almıştır. Özellikle, varsayılan kimlik bilgileriyle erişilebilen cihazlar Mirai tarafından otomatik olarak taranarak kötü amaçlı yazılım bulaştırılmakta ve ardından saldırı için uzaktan kontrol edilebilmektedir.

Mirai'nin temel çalışma prensibi, kaba kuvvet (brute-force) saldırıları kullanarak hedef cihazlara yetkisiz erişim sağlaması ve ele geçirilen cihazları merkezi bir komuta ve kontrol sunucusuna bağlamasıdır. Bu botnet, cihazları DDoS saldırılarında kullanarak hedef sistemleri aşırı yükleyebilir ve hizmet kesintilerine yol açabilir. Mirai'nin en bilinen saldırıları arasında 2016 yılında Dyn DNS sağlayıcısına düzenlenen saldırı yer almakta olup, bu saldırı sonucu birçok popüler web sitesi erişilemez hale gelmiştir. Mirai botnetinin yayılması, IoT güvenlik açıklarının siber tehditlerde nasıl istismar edilebileceğini gözler önüne sermekte ve bu tür tehditlere karşı güvenlik önlemlerinin artırılmasının önemini vurgulamaktadır (Antonakakis ve ark., 2017).



Şekil 3.21. Mirai botnet mimarisi ve zararlı yazılım yayılma mekanizması (Liévin ve ark., 2021)

Şekil 3.21, 2016 yılında ortaya çıkan ve büyük ölçekli DDoS saldırılarıyla tanınan Mirai botnet'inin temel mimarisini ve çalışma prensibini göstermektedir.

3.2.7.1. GREIP Flood Saldırısı

GRE-IP flood, Mirai botnet tarafından kullanılan daha az yaygın ancak etkili bir DDoS saldırı türüdür. Bu saldırı, Generic Routing Encapsulation (GRE) protokolünü hedef alarak ağ altyapısını istismar etmeye yöneliktir. Saldırganlar, sahte GRE paketleri oluşturarak hedef sistemlerin ağ kaynaklarını tüketmekte ve hizmetlerin aksamasına yol açmaktadır. Özellikle, Mirai tarafından gerçekleştirilen saldırılar arasında 994 kez uygulandığı tespit edilmiştir.

GRE-IP flood saldırıları, özellikle büyük ölçekli DDoS saldırılarında destekleyici bir saldırı mekanizması olarak kullanılmıştır. Bu saldırı, Mirai'nin hedef sistemlere aşırı yük bindirme stratejisinin bir parçası olup, ağ performansına ciddi zararlar verebilmektedir. GRE tünelleme mekanizmasının manipüle edilmesiyle gerçekleştirilen bu saldırılar, internet servis sağlayıcıları (ISP) ve büyük ağ altyapılarını etkileyerek hizmet kesintilerine neden olabilmektedir (Antonakakis ve ark., 2017).

3.2.7.2. Greeth Flood Saldırısı

Greeth Flood (GRE Ethernet Flood) saldırısı, Mirai botnet ve türevleri tarafından gerçekleştirilen bir DDoS saldırı türüdür. Bu saldırıda, GRE protokolü kullanılarak rastgele kaynak ve hedef MAC adresleri içeren Ethernet çerçeveleri gönderilir, böylece ağ altyapısı aşırı yüklenerek hizmet kesintileri meydana gelir. Özellikle yönlendiriciler, IoT cihazları ve güvenlik duvarları bu saldırıdan etkilenebilir, çünkü gelen yoğun trafiği işlemeye çalışırken performans kaybı yaşarlar.

Bu tür saldırılara karşı GRE paketlerinin filtrelenmesi, Layer 2 trafik izleme sistemlerinin kullanılması ve deep packet inspection (DPI) ile analiz yapılması önerilir. Ayrıca, rate limiting (hız sınırlandırma) teknikleri ve gelişmiş DDoS koruma çözümleri uygulanarak ağ üzerindeki zararlı trafik minimize edilebilir (Systems, 2019).

3.2.7.3. UDPPlain Saldırısı

UDP-PLAIN flood, Mirai botnet tarafından kullanılan en yaygın DDoS saldırı türlerinden biridir. Bu saldırıda, botnet'e bağlı cihazlar hedef sunucuya büyük miktarda UDP (User Datagram Protocol) paketi göndererek bant genişliğini tüketmeye çalışır. Hedef sistem, bu büyük hacimli trafiği işlerken aşırı yüklenir ve meşru kullanıcı isteklerine yanıt veremez hale gelir. Mirai'nin gerçekleştirdiği 15.194 saldırı arasında 2.542'si UDP-PLAIN flood yöntemiyle gerçekleştirilmiştir (Antonakakis ve ark., 2017).

3.3. Saldırı Tespit Sistemleri

Saldırı Tespit Sistemleri (IDS), bilgisayar ağlarına veya sistemlere yönelik izinsiz erişim girişimlerini ve güvenlik ihlallerini tanımlamak için tasarlanan güvenlik çözümleridir. IoT ortamlarında saldırı tespit, cihazların kısıtlı kaynakları ve farklı protokoller nedeniyle özel zorluklar içerir (Zarpelão ve ark., 2017). CICIOT2023 gibi veri setleri, bu sistemlerin geliştirilmesi ve test edilmesi için değerli kaynaklar sunmaktadır.

3.3.1. Ağ tabanlı saldırı tespit sistemi

Ağ tabanlı saldırı tespit sistemleri, stratejik noktalara yerleştirilen sensörler aracılığıyla ağ segmentlerindeki tüm trafiği izleyerek zararlı aktiviteleri tespit etmeye

yönelik güvenlik çözümleridir. Bu sistemler, paket içeriklerini ve trafik desenlerini analiz ederek, bilinen saldırı imzalarını veya anormal ağ davranışlarını belirler ve potansiyel tehditlere karşı alarmlar üretir. NIDS'ler özellikle DDoS saldırıları, port taramaları ve diğer ağ düzeyindeki tehditler konusunda etkilidir ve kurumsal ağlarda derinlemesine savunma stratejisinin kritik bir bileşenidir. Bu sistemlerin en önemli avantajları, birden fazla sistemi eş zamanlı koruyabilmeleri ve uç noktaların performansını etkilememeleri; dezavantajları ise şifreli trafiği analiz etmekte zorlanmaları ve yüksek hızlı ağlarda performans sorunları yaşayabilmeleridir (Zarpelão ve ark., 2017).

3.3.2. İmza tabanlı saldırı tespiti

İmza tabanlı saldırı tespit sistemleri, önceden tanımlanmış saldırı kalıplarını veya imzalarını kullanarak bilinen tehditleri tespit eden bir güvenlik yaklaşımıdır. Bu sistemler, ağ trafiğindeki veya sistem olaylarındaki paketleri bir tehdit veritabanındaki bilinen kötü amaçlı davranış kalıplarıyla karşılaştırarak çalışır ve eşleşme durumunda alarm üretir. CICIOT2023 veri setindeki Dictionary Brute Force, XSS, SQL Injection, Command Injection ve Backdoor Malware gibi saldırılar, belirli kalıplar içerdiklerinden imza tabanlı sistemlerle etkili şekilde tespit edilebilmektedir.

İmza tabanlı yaklaşımın en büyük avantajı, bilinen saldırıları yüksek doğrulukla ve düşük yanlış pozitif oranlarıyla tespit edebilmesi ve IoT gibi kaynak kısıtlı ortamlarda bile verimli çalışabilmesidir; ancak sıfır-gün saldırıları gibi daha önce görülmemiş tehditleri tespit etmede yetersiz kalması ve imza veritabanının sürekli güncellenmesi gerekliliği önemli dezavantajlarıdır (Liao ve ark., 2013; Raza ve ark., 2013).

3.3.3. Anomali tabanlı saldırı tespiti

Anomali tabanlı saldırı tespit sistemleri, normal ağ trafiği veya sistem davranışının profilini oluşturarak bu profilden sapan her türlü aktiviteyi potansiyel tehdit olarak değerlendiren gelişmiş bir siber güvenlik yaklaşımıdır (Chandola ve ark., 2009). CICIOT2023 veri setindeki DDoS-ICMP Flood, DoS-TCP Flood, Recon-PortScan ve MITM-ArpSpoofing gibi saldırılar, normal trafik davranışından belirgin sapmalar gösterdiği için anomali tabanlı tespit yöntemleriyle başarıyla tanımlanabilmektedir. Bu sistemler, istatistiksel modeller, makine öğrenmesi algoritmaları veya derin öğrenme teknikleri kullanarak sistemin veya cihazın normal davranış desenlerini öğrenir ve

normalden sapmalar tespit edildiğinde alarm verir. Modern IDS sistemleri çoğunlukla her iki yaklaşımın avantajlarını birleştiren hibrit modeller kullanmaktadır; örneğin bazı DDoS saldırıları hem imza tabanlı hem de anomali tabanlı yöntemlerle tespit edilebilmekte, bu da daha kapsamlı bir koruma sağlamaktadır (Meidan ve ark., 2018). CICIOT2023 veri setindeki çalışmaların çoğunda kullanılan makine öğrenmesi modelleri de aslında hem imza hem de anomali tabanlı tespitleri kapsayan birleşik bir yaklaşım sunmaktadır, bu da IoT ortamlarındaki karmaşık saldırı senaryolarına karşı daha etkili koruma sağlamaktadır.

3.3.4. Ana bilgisayar tabanlı saldırı tespit sistemi

Ana bilgisayar tabanlı saldırı tespit sistemleri, belirli bir bilgisayar veya sunucu üzerinde çalışarak bu sistemdeki olayları, aktiviteleri ve dosya bütünlüğünü sürekli izleyen güvenlik çözümleridir. HIDS, işletim sistemi seviyesinde çalışarak sistem kayıtlarını, uygulama loglarını, dosya değişikliklerini ve sistem çağrılarını analiz eder. Bu sistemler, yetkisiz erişim girişimlerini, kötü amaçlı yazılım aktivitelerini ve içeriden gelen tehditleri tespit etmek için özellikle etkilidir. Dosya bütünlüğü izleme, davranış analizleri ve sistem günlüklerinin denetlenmesi gibi temel fonksiyonları içerir. Ana bilgisayar tabanlı sistemlerin en önemli avantajları, şifreli trafiği izleyebilmeleri, yerel sistemdeki anormallikleri tespit edebilmeleri ve yetkili kullanıcıların kötüye kullanımını belirleyebilmeleridir; buna karşın her korunacak sistemde ayrı ayrı yapılandırılmaları gerektiğinden yönetim zorlukları, sistem kaynaklarının tüketimi ve sadece kuruldukları sistemi koruyabilmeleri dezavantajları arasındadır (Mitchell ve Chen, 2014).

3.3.5. Derin öğrenme tabanlı saldırı tespit sistemi

Derin öğrenme tabanlı saldırı tespit sistemleri, geleneksel makine öğrenmesi yaklaşımlarının ötesine geçerek, karmaşık ve çok katmanlı yapay sinir ağları aracılığıyla siber saldırıları tespit eden gelişmiş güvenlik çözümleridir. Bu sistemler, ağ trafiğindeki veya sistem davranışlarındaki karmaşık kalıpları otomatik olarak öğrenebilme ve tespit edebilme yetenekleriyle öne çıkar. Derin sinir ağları, konvolüsyonel sinir ağları (CNN), tekrarlayan sinir ağları (RNN), uzun-kısa vadeli bellek ağları (LSTM) ve otokodlayıcılar gibi çeşitli mimari yapılar üzerine kurulabilen bu sistemler, özellikle yüksek boyutlu veri kümelerinde gizli ilişkileri keşfetmede etkilidir. Derin öğrenme tabanlı yaklaşımların en

önemli avantajları, manuel özellik mühendisliğine daha az ihtiyaç duyması, ham verilerden karmaşık özellikleri otomatik olarak çıkarabilmesi, yüksek doğrulukla anomali tespiti yapabilmesi ve zamanla kendini geliştirebilmesidir. Bununla birlikte, eğitim için büyük miktarda veri gerektirmesi, hesaplama maliyetinin yüksek olması, modelin kararlarının yorumlanabilirliğinin düşük olması ve aşırı öğrenme riski taşıması bu yaklaşımın başlıca dezavantajları olarak sayılabilir (Diro ve Chilamkurti, 2018).

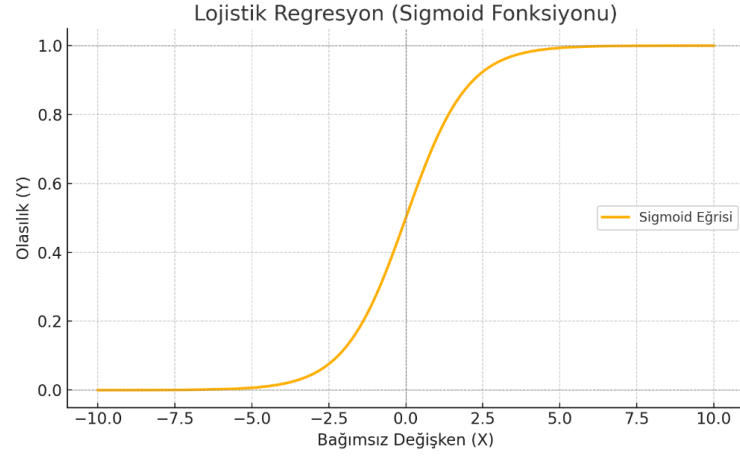
3.4. Makine Öğrenmesi

Makine öğrenmesi, bilgisayar sistemlerinin açıkça programlanmadan veri desenlerinden öğrenme ve karar verme yetenekleri geliştirmelerini sağlayan yapay zeka alt disiplini. IoT ortamlarındaki siber saldırıların tespiti bağlamında makine öğrenmesi, normal ve anormal trafik kalıpları arasındaki karmaşık ilişkileri otomatik olarak tanımlayabilen modeller oluşturmak için CICIOT2023 gibi veri setlerinden yararlanır. Bu teknoloji, denetimli öğrenme (etiketli veri kullanarak belirli saldırı türlerini sınıflandırma), denetimsiz öğrenme (etiketlenmemiş verilerden anormallikleri tespit etme) ve pekiştirmeli öğrenme (dinamik savunma stratejileri geliştirme) yaklaşımları aracılığıyla, IoT ekosistemindeki geleneksel yöntemlerle tespit edilmesi zor olan karmaşık ve gelişen saldırı vektörlerini belirlemede kritik bir rol oynamaktadır (Jordan ve Mitchell, 2015). Makine öğrenmesi tabanlı saldırı tespit sistemleri, statik kuralların ötesine geçerek, sürekli evrimleşen tehdit ortamına adaptasyon sağlama ve sıfır-gün saldırılarını tespit etme yetenekleriyle IoT güvenliğinde önemli bir avantaj sağlamaktadır (Hodo ve ark., 2016).

3.4.1. Lojistik Regresyon (LR)

Lojistik Regression (LR) veya doğrusal olmayan regresyon, özellikle ikili sınıflandırma problemlerinde kullanılan, bağımsız değişkenlerin doğrusal kombinasyonunu sigmoid fonksiyon aracılığıyla 0 ile 1 arasında olasılığa dönüştüren temel bir istatistiksel modeldir. Bu yöntem, sosyal bilimler, tıp ve finans gibi alanlarda yaygın olarak tercih edilmektedir (Hastie, 2009).

Algoritma, girdilerin ağırlıklı toplamını hesaplayarak, bu değeri $1/(1+\exp(-z))$ formülü ile sigmoid fonksiyona sokar. Elde edilen olasılık, genellikle 0.5 eşik değeri ile karşılaştırılarak sınıflandırma kararı verilir (Hastie, 2009).



Şekil 3.22. Lojistik regresyon modelinde sigmoid fonksiyonu

Şekil 3.22’de, lojistik regresyonda kullanılan sigmoid fonksiyonunun eğrisi gösterilmektedir. Fonksiyon, X eksenindeki bağımsız değişkenlere karşılık, Y ekseninde 0 ile 1 arasında bir olasılık değeri üretmektedir. Bu yapı, ikili sınıflandırma problemlerinde sınıf olasılıklarını tahmin etmek için kullanılır.

LR, yapısının sadeliği, hızlı hesaplanabilirliği ve sonuçların kolay yorumlanabilir olmasıyla öne çıkar. Ancak, modelin doğrusal varsayımına bağlı olması, karmaşık ve doğrusal olmayan ilişkileri yakalamada yetersiz kalmasına neden olabilir (Peng ve ark., 2002).

Bu algoritma, kredi risk analizi, hasta teşhisi, e-posta spam filtreleme ve pazarlama kampanyalarının başarısını tahmin etme gibi pek çok alanda kullanılmaktadır. LR, özellikle yorumlanabilirlik ve hız gerektiren uygulamalarda tercih edilen bir yöntemdir (Mitchell ve Mitchell, 1997).

Özetle, LR algoritması, basit yapısı ve yüksek yorumlanabilirliği sayesinde, ikili sınıflandırma problemlerinde etkili ve pratik çözümler sunan önemli bir yöntemdir.

3.4.2. Navie Bayes (NB)

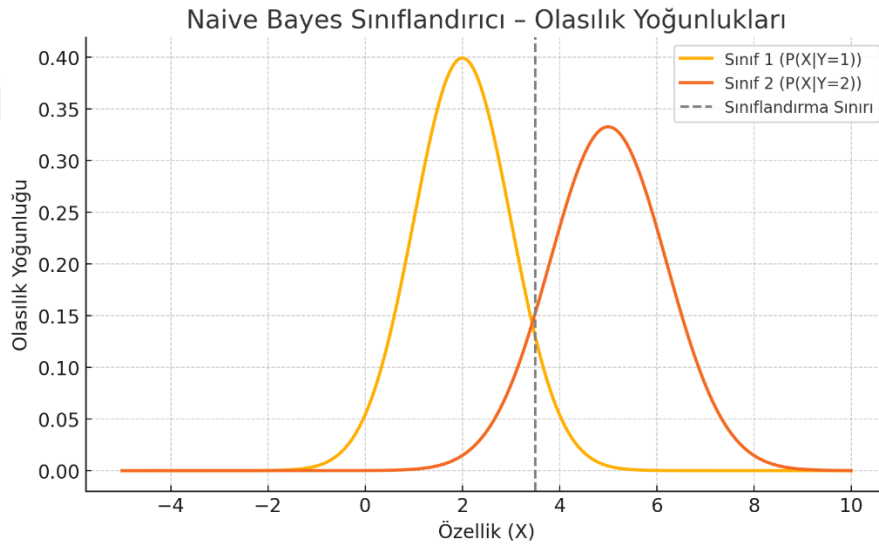
Naive Bayes (NB) algoritması, Bayes teoremi temelli olup, her özelliğin diğerlerinden bağımsız olduğu varsayımına dayanan basit ama etkili bir sınıflandırma yöntemidir. Bu yöntem, özellikle metin sınıflandırması ve spam tespiti gibi uygulamalarda yaygın olarak kullanılmaktadır (Mitchell ve Mitchell, 1997).

NB, her özelliğin birbirinden bağımsız olduğunu varsayarak, bir gözlemin hangi sınıfa ait olduğunu olasılıklara göre belirleyen bir sınıflandırma yöntemidir. Model, her sınıfa ait olasılık dağılımını kullanarak en yüksek olasılığa sahip sınıfı tahmin eder.

Algoritma, bir gözlemin belirli bir sınıfa ait olma olasılığını hesaplamak için, her özelliğin koşullu olasılıklarını çarparak Bayes teoremini uygular. Böylece, tüm özelliklerin etkisi birleştirilir ve en yüksek olasılığa sahip sınıf seçilerek karar verilir (Rish, 2001).

NB algoritması, hesaplama açısından hızlı olması ve uygulanmasının kolay olması gibi önemli avantajlara sahiptir. Ancak, özellikler arasındaki bağımsızlık varsayımının gerçek dünya verilerinde her zaman sağlanamaması, modelin doğruluğunu sınırlayabilmektedir (Mitchell ve Mitchell, 1997).

NB algoritması, metin sınıflandırması, spam filtreleme, duygu analizi ve haber kategorilendirme gibi çeşitli uygulamalarda kullanılarak, hızlı ve pratik çözümler sunmaktadır. Bu geniş kullanım alanı, algoritmanın esnekliği ve düşük hesaplama maliyeti sayesinde mümkün olmaktadır (Rish, 2001).



Şekil 3.23. NB sınıflandırıcısı için olasılık dağılımları

Şekil 3.23'te, NB sınıflandırıcısının iki farklı sınıf için hesapladığı koşullu olasılık yoğunlukları gösterilmektedir. Eğrilerin kesişim noktası, sınıflar arasındaki karar (sınıflandırma) sınırını temsil eder. Model, gözlemin hangi sınıfa ait olduğunu bu olasılıklara göre belirlemektedir.

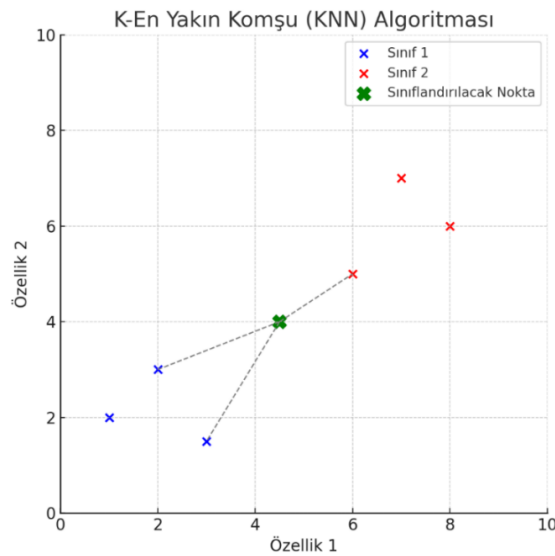
3.4.3. K En Yakın Komşu (KEYK)

K-En Yakın Komşu algoritması (KEYK), denetimli öğrenme kapsamında kullanılan basit ve etkili bir sınıflandırma yöntemidir. Bu algoritma, yeni bir veri noktasının sınıfını belirlemek için eğitim setindeki en yakın komşuların etiketlerine bakar; bu sayede, özellikle örüntü tanıma ve sınıflandırma problemlerinde başarılı sonuçlar elde edilir (Cover ve Hart, 1967).

KEYK algoritması, genellikle Öklidyen mesafe gibi bir mesafe ölçütü kullanarak, test verisi ile eğitim verisindeki her örnek arasındaki benzerliği hesaplar. Belirlenen “K” değeri kadar en yakın komşunun sınıf etiketlerine bakılarak, çoğunluk oyu prensibiyle sınıflandırma gerçekleştirilir ya da regresyon problemlerinde ortalama değer tahmini yapılır (Duda ve Hart, 2006).

KEYK algoritmasının en büyük avantajlarından biri, model oluşturma aşamasında herhangi bir parametre tahmini yapmadan doğrudan eğitim verisini kullanmasıdır. Bu basit yapı, uygulama kolaylığı ve esneklik sağlar. KEYK, küçük veri setleri ve düşük boyutlu problemlerde ideal bir seçimdir. Ancak, özellikle yüksek boyutlu veri setlerinde hesaplama maliyetinin artması, bellek kullanımının yoğunlaşması ve gürültülü verilerin sınıflandırma başarısını olumsuz etkilemesi gibi dezavantajlar da bulunmaktadır.

KEYK algoritması, tıbbi teşhis, kredi risk analizi, görüntü sınıflandırma ve öneri sistemleri gibi pek çok farklı alanda başarıyla uygulanmaktadır. Bu geniş kullanım alanı, algoritmanın çeşitli veri tiplerine ve problemlere adapte olabilme yeteneğini göstermektedir.



Şekil 3.24. KEYK algoritması ile sınıflandırma örneği

Şekil 3.24, mavi ve kırmızı noktalar iki farklı sınıfı temsil eder. Yeşil X noktası sınıflandırılmak istenen veridir. KEYK algoritması, bu noktaya en yakın 3 komşuya ($K=3$) bakar ve çoğunluğa göre yeşil noktanın hangi sınıfa ait olduğunu belirler.

KEYK algoritması, basit yapısı ve uygulanabilirliği sayesinde pek çok sınıflandırma probleminde tercih edilen yöntemlerden biridir. Doğru “K” değerinin belirlenmesi ve uygun mesafe ölçütlerinin kullanılmasıyla, KEYK algoritması çeşitli uygulama alanlarında güvenilir ve etkili sonuçlar sunmaktadır (Cover ve Hart, 1967).

3.4.4. Karar Ağaçları (KA)

Karar Ağaçları (KA), makine öğrenimi kapsamında hem sınıflandırma hem de regresyon problemlerini çözmek amacıyla kullanılan etkili ve açıklanabilir bir algoritmadır. Model, veriyi hiyerarşik bir yapıya göre bölerek, kök düğümden başlayıp dallar ve yaprak düğümlere kadar ilerleyen bir yapı oluşturur. Bu yapı, verilerin "evet" veya "hayır" gibi basit kararlar aracılığıyla nihai bir sınıfa veya tahmine ulaşmasını sağlar; böylece analitik karar süreçlerinin görselleştirilmesine olanak tanır (Mitchell ve Mitchell, 1997).

KA algoritması, veri setindeki örnekleri özelliklerine göre en iyi şekilde ayıran düğümler oluşturur. Her düğümden, örneklerin homojenliğini artırmak için bilgi kazancı, Gini indeksi veya benzeri ölçütler kullanılarak en uygun ayırım gerçekleştirilir. Bu süreç, veriler tamamen sınıflandırılana kadar veya belirlenen durdurma kriterlerine ulaşılan kadar devam eder (Quinlan, 1986).

KA, modelin görsel olarak sunulabilmesi ve sonuçların yorumlanabilir olması gibi önemli avantajlara sahiptir. Ayrıca, veri ön işleme gereksinimi azdır. Özellikle küçük ve orta büyüklükteki veri setlerinde yüksek doğruluk oranı sağlar. Ancak, çok derin ağaçlar oluştuğunda aşırı uyum (overfitting) riski ve küçük veri değişikliklerine karşı kararsızlık gibi dezavantajlar gözlemlenebilir (Quinlan, 1986).

KA, tıbbi teşhis, kredi risk analizleri, müşteri segmentasyonu ve pazarlama stratejileri gibi çok çeşitli alanlarda kullanılarak, karmaşık veri setlerinden anlamlı sonuçlar elde edilmesine olanak tanır.

3.4.5. Rastgele Orman (RO)

Rastgele Orman (RO) algoritması, çok sayıda karar ağacının oluşturulması ve bunların sonuçlarının topluluk (ensemble) yöntemiyle birleştirilmesi prensibine dayanan güçlü bir makine öğrenmesi yöntemidir. Bu yapı, tek bir karar ağacının öngörü gücünü artırarak, sınıflandırma ve regresyon problemlerinde daha doğru sonuçlar elde edilmesine olanak tanır (Breiman, 2001).

RO, eğitim verisinden bootstrap yöntemiyle rastgele örnekler seçip, her örnek üzerinde ayrı karar ağaçları oluşturur. Ayrıca, her ağacın her düğümünde, rastgele seçilen bir özellik alt kümesi üzerinden en iyi bölme yapılır. Bu yöntem, ağaçlar arasındaki korelasyonu azaltarak, modelin genel doğruluğunu artırır (Hastie, 2009).

RO algoritmasının en büyük avantajı, yüksek doğruluk oranı ve aşırı uyum (overfitting) riskinin nispeten düşük olmasıdır. Aynı zamanda, eksik veriler ve gürültülü veri setlerinde de sağlam performans gösterir. Ancak, çok sayıda ağaç oluşturulması nedeniyle hesaplama maliyeti artabilir ve modelin yorumlanabilirliği, tek ağaç modellerine kıyasla daha zor olabilir (Breiman, 2001).

RO, tıbbi teşhis, finansal risk analizi, müşteri segmentasyonu ve görüntü işleme gibi geniş bir yelpazede kullanılmaktadır. Bu çeşitlilik, algoritmanın esnek yapısı ve farklı veri tiplerine uyum sağlayabilme kapasitesi ile açıklanabilir.

Sonuç olarak, RO algoritması, topluluk öğrenme yöntemlerinin gücünü kullanarak, karar ağaçlarının zayıflıklarını gideren ve güvenilir sonuçlar sunan etkili bir yaklaşımdır. Uygun parametre ayarlamaları ve yeterli veri ile RO, birçok gerçek dünya probleminde yüksek başarı sağlamaktadır.

3.4.6. Gradyan Artırma (GA)

Gradyan Artırma (GA), makine öğrenmesinde kullanılan güçlü bir topluluk (ensemble) yöntemidir. Temel prensibi, birden fazla zayıf tahmin modelini (genellikle karar ağaçları) ardışık olarak eğiterek, daha güçlü ve doğru bir model oluşturmaktır. Her adımda, önceki modelin yapmış olduğu hatalar analiz edilir ve yeni model, bu hataları minimize etmek için eğitilir. Bu süreç, hata fonksiyonunun negatif gradyanı yönünde optimizasyon yaparak ilerler ve gradyan iniş tekniğini temel alır (Friedman, 2001). GA algoritması, hem regresyon hem de sınıflandırma problemlerinde yüksek performans gösteren bir yöntem olarak öne çıkmaktadır.

GA'nın başarısı, ardışık öğrenme mekanizmasında yatmaktadır. Her yeni model, önceki modellerin yapamadığı tahmin hatalarını hedefleyerek eğitildiği için, genel model doğruluğu kademeli olarak artar. Ancak bu güçlü yapı, aynı zamanda aşırı öğrenme (overfitting) riskini de beraberinde getirebilir. Bu nedenle, öğrenme oranı (learning rate), ağaç derinliği ve iterasyon sayısı gibi hiper parametrelerin dikkatlice ayarlanması gerekmektedir (Natekin ve Knoll, 2013). Günümüzde XGBoost, LightGBM ve CatBoost gibi popüler kütüphaneler, GA'nın hız ve doğruluk açısından optimize edilmiş versiyonlarını sunarak veri bilimi uygulamalarında önemli bir yer edinmiştir.

Bu algoritmanın yaygın kullanım alanları arasında finans, tıp, pazarlama analitiği ve doğal dil işleme gibi çeşitli endüstriyel ve akademik uygulamalar bulunmaktadır. GA, hem yapılandırılmış veriler üzerinde üstün performans gösteren bir yöntem olması hem de tahmin doğruluğunun yüksek olması nedeniyle, veri bilimi yarışmalarında sıkça kullanılan bir tekniktir (Nielsen, 2016). Ancak, hesaplama maliyetinin yüksek olması ve model karmaşıklığının artması, bu yöntemin dikkatli hiper parametre optimizasyonu gerektirdiğini gösterir. Sonuç olarak, GA, modern makine öğrenmesi problemlerine güçlü ve esnek çözümler sunarak, büyük veri setleriyle etkili bir şekilde çalışabilen önemli bir algoritma haline gelmiştir (Bentéjac ve ark., 2021).

3.4.7. Aşırı Gradyan Artırma (AGA)

AGA (XGBoost-eXtreme Gradient Boosting), yüksek doğruluk ve hesaplama verimliliği sağlayan optimize edilmiş bir GA algoritmasıdır. Tianqi Chen ve Carlos Guestrin (2016) tarafından geliştirilmiş olup, büyük veri setlerinde ölçeklenebilir ve hızlı çalışması için tasarlanmıştır. Algoritmanın temel avantajları arasında ikinci dereceden gradyan bilgisi kullanarak kayıp fonksiyonunu optimize etmesi, aşırı öğrenmeyi önleyen düzensizleştirme mekanizması ve paralel hesaplama desteği ile işlem süresini önemli ölçüde azaltması bulunmaktadır (Chen ve Guestrin, 2016). Ayrıca, veri saklama için sıkıştırılmış sütun formatı kullanarak bellek yönetimini optimize etmesi ve eksik verileri otomatik işleyebilmesi, büyük ölçekli projelerde kullanımını yaygınlaştırmıştır (Bentéjac ve ark., 2021).

AGA, GPU hızlandırması sayesinde model eğitim sürecini hızlandırabilir ve çapraz doğrulama, özellik önem analizi gibi kullanıcı dostu işlevler sunarak performansı artırır. Özellikle Kaggle yarışmalarında sıkça tercih edilmesi, geleneksel Gradient Boosting yöntemlerine kıyasla daha hızlı ve genelleme yeteneği yüksek tahminler

yapabilmesinden kaynaklanmaktadır (Nielsen, 2016). Finans, sağlık, e-ticaret ve doğal dil işleme gibi birçok alanda kullanılan algoritma, sahtekarlık tespiti, kredi skorlama ve tıbbi teşhis gibi kritik uygulamalarda başarıyla uygulanmaktadır. En büyük avantajları yüksek doğruluk, hesaplama verimliliği ve büyük veri setlerinde etkili olmasıdır, ancak hiper parametre ayarlarının karmaşıklığı ve modelin yorumlanabilirliğinin düşük olması bazı zorluklar olarak değerlendirilmektedir. Sonuç olarak, AGA, modern makine öğrenmesi ekosisteminde güçlü ve esnek bir algoritma olarak kabul edilmektedir.

3.5. Derin Öğrenme (DÖ)

Derin öğrenme (DÖ), çok katmanlı yapay sinir ağları kullanarak veriden otomatik olarak özellik çıkarımı yapan ve karmaşık ilişkileri modelleyebilen güçlü bir makine öğrenmesi yöntemidir. Bu yöntem, özellikle büyük veri setleri ve yüksek boyutlu verilerle çalışırken önemli avantajlar sunmaktadır (LeCun ve ark., 2015).

DÖ algoritmaları, veriyi katmanlar halinde işleyerek, her katmanda daha soyut ve anlamlı özellikler elde eder. Bu hiyerarşik yapı sayesinde, model karmaşık desenleri ve ilişkileri öğrenir; giriş verileri, ardışık katmanlar vasıtasıyla nihai çıktıya dönüştürülür (LeCun ve ark., 2015).

DÖ, büyük ve karmaşık veri setlerinde üstün performans gösterirken, otomatik özellik çıkarımı yapabilme yeteneğiyle dikkat çeker. Ancak, eğitim sürecinde yüksek hesaplama gücü ve geniş veri gereksinimi, modelin uygulanmasında bazı zorluklara yol açabilir (Schmidhuber, 2015).

DÖ, görüntü işleme, ses tanıma, doğal dil işleme, otonom araçlar ve sağlık teşhisi gibi pek çok alanda kullanılmaktadır. Bu geniş uygulama yelpazesi, algoritmanın esnek yapısı ve yüksek doğruluk oranı sayesinde mümkün olmaktadır (Schmidhuber, 2015).

Özetle, DÖ algoritmaları, veriden otomatik özellik çıkarımı yapabilme ve karmaşık ilişkileri modelleyebilme kabiliyetleriyle modern yapay zekâ uygulamalarının temel taşlarından biri haline gelmiştir. Doğru yapılandırma ve yeterli veri desteğiyle, bu yöntem pek çok gerçek dünya probleminde etkili sonuçlar sunmaktadır.

3.5.1. Yapay sinir ağları (YSA)

Yapay Sinir Ağları (YSA), insan beyninin çalışma prensiplerinden esinlenerek geliştirilmiş, veriden öğrenme ve karmaşık ilişkileri modelleme yeteneğine sahip

denetimli ya da denetimsiz öğrenme algoritmalarıdır. Bu yöntem, özellikle büyük veri setleriyle çalışırken öne çıkarak sınıflandırma, regresyon ve örüntü tanıma gibi alanlarda kullanılmaktadır (Goodfellow, 2016).

YSA, birbirine bağlı çok katmanlı nöronlardan oluşur; her nöron, aldığı girdiyi belirli ağırlıklarla çarpar, bir toplama işlemi gerçekleştirir ve sonrasında doğrusal olmayan aktivasyon fonksiyonlarıyla işleyerek çıktıyı üretir. Bu yapıda, eğitim sürecinde hata geriye yayılım (backpropagation) yöntemi kullanılarak ağırlıklar güncellenir ve model, istenen çıktılara yaklaşıpacak şekilde optimize edilir (Rumelhart ve ark., 1986).

YSA, karmaşık ve doğrusal olmayan ilişkileri modelleyebilme yetenekleri sayesinde geniş bir uygulama alanında etkili sonuçlar sunmaktadır. Ancak, bu modellerin yüksek hesaplama gücü gerektirmesi, büyük miktarda veri ile eğitilme zorunluluğu ve aşırı uyum (overfitting) riski gibi dezavantajları bulunmaktadır. Modelin genelleştirme kapasitesini artırmak için düzenleme (regularization) teknikleri ve büyük veri setleri ile eğitim gibi yöntemler yaygın olarak kullanılmaktadır (Goodfellow, 2016).

YSA, görüntü ve ses tanıma, doğal dil işleme, tıbbi teşhis, finansal tahmin ve otonom sistemler gibi pek çok alanda yaygın olarak kullanılmaktadır. Bu geniş uygulama yelpazesi, algoritmanın esnekliğini ve farklı veri tiplerine uyum sağlama kabiliyetini göstermektedir (LeCun ve ark., 2015).

Sonuç olarak, YSA, karmaşık veri yapılarındaki örüntüleri başarıyla öğrenebilen ve geniş bir uygulama alanında etkili çözümler sunan güçlü bir yöntemdir. Doğru yapılandırma, yeterli veri ve uygun optimizasyon teknikleriyle eğitildiğinde, YSA farklı veri türlerine uyum sağlayarak yüksek doğruluk oranlarıyla çalışabilir. Gelişen hesaplama gücü ve DÖ teknikleri sayesinde, bu yöntem günümüzde birçok alanda yapay zekanın temel bileşenlerinden biri olmaya devam etmektedir.

3.5.2. Evrimsel Sinir Ağları (ESA)

Evrimsel Sinir Ağları (ESA), özellikle görüntü işleme, video analizi ve benzeri alanlarda kullanılan, görsel verilerdeki yerel özellikleri otomatik olarak öğrenebilen güçlü bir DÖ mimarisidir. ESA'lar, çekirdek (kernel) adı verilen filtreler aracılığıyla görüntülerdeki desenleri algılar ve özellik haritaları (feature maps) oluşturur. Bu yapı, DÖ modellerinin büyük veri kümelerinde başarılı sonuçlar elde etmesini sağlamaktadır. DÖ alanında önemli bir kaynak olan Goodfellow, Bengio ve Courville (Goodfellow,

2016), ESA'nın görüntü sınıflandırma, nesne algılama ve doğal dil işleme gibi birçok alanda etkin bir şekilde kullanıldığını vurgulamaktadır.

ESA, temel olarak konvolüsyonel katmanlar, havuzlama (pooling) katmanları ve tam bağlantılı katmanlardan oluşur. Konvolüsyonel katmanlar, giriş görüntüsündeki küçük bölgeler üzerinde kayan filtreler (kernel) uygulayarak öznitelik haritaları üretir; havuzlama katmanları ise bu öznitelik haritalarının boyutunu küçülterek hesaplama maliyetini düşürür ve özet bilgi sağlar (Goodfellow, 2016).

ESA, görüntülerdeki uzamsal ilişkileri etkili biçimde yakalayabilme ve otomatik özellik çıkarımı yapabilme yeteneği ile öne çıkar. Bu avantajlar, nesne tanıma ve sınıflandırma gibi görevlerde yüksek başarı sağlar. Ancak, modelin eğitimi için geniş veri setleri ve yüksek hesaplama gücü gerekliliği, uygulama alanlarında bazı sınırlamalara yol açabilir (Krizhevsky ve ark., 2012).

ESA algoritması, otomatik yüz tanıma, tıbbi görüntü analizi, nesne algılama, otonom sürüş ve video gözetim sistemleri gibi pek çok alanda kullanılmaktadır. Özellikle görsel verilerden karmaşık özniteliklerin çıkarılması, bu alanlarda başarılı uygulamaların temelini oluşturur. Krizhevsky, Sutskever ve Hinton (Krizhevsky ve ark., 2012), derin ESA modellerinin büyük ölçekli veri kümelerinde son derece başarılı sonuçlar verdiğini göstermiş ve ImageNet yarışmasında kazandıkları başarıyla DÖ alanında devrim yaratmışlardır. Günümüzde CNN tabanlı modeller, çeşitli görüntü işleme ve bilgisayarlı görü (computer vision) uygulamalarında en yaygın kullanılan mimarilerden biri haline gelmiştir.

3.5.3. Tekrarlayan Sinir Ağları (TSA)

Tekrarlayan Sinir Ağları (TSA), özellikle ardışık verilerdeki zaman bağımlılıklarını modelleyebilmek amacıyla geliştirilmiş bir DÖ mimarisidir. Bu yapı, geçmiş bilgileri de hesaba katarak, dil modellemesi, konuşma tanıma ve zaman serisi tahmini gibi uygulamalarda etkili sonuçlar elde edilmesini sağlar (Elman, 1990).

TSA'lar, her zaman adımında hem mevcut girdiyi hem de önceki adımın gizli durum bilgisini kullanarak çıktıyı hesaplar. Bu tekrarlayan yapı sayesinde model, ardışık verideki örüntüleri öğrenir ve zamana bağlı ilişkileri yakalar. Böylece, geçmiş bilgilerin gelecekteki tahminlerde etkili rol oynaması sağlanır (Schmidhuber, 2015).

TSA'ların en önemli avantajı, ardışık verilerdeki uzun süreli bağımlılıkları modelleyebilmesidir. Ancak, uzun dizilerde eğitim sırasında gradyanların sönmesi veya

patlaması gibi sorunlarla karşılaşılabilir. Bu nedenle, uzun vadeli ilişkileri daha iyi öğrenebilmek için LSTM ve GRU gibi geliştirilmiş modeller de önerilmiştir (Pascanu, 2013).

TSA'lar, dil işleme, makine çevirisi, ses tanıma ve finansal zaman serisi analizi gibi pek çok alanda kullanılmaktadır. Bu geniş uygulama yelpazesi, modelin ardışık verileri analiz etmedeki başarısını ve esnekliğini ortaya koymaktadır (Schmidhuber, 2015).

3.5.4. Uzun Kısa Süreli Bellek (UKSB)

Uzun Kısa Süreli Bellek (UKSB), geleneksel TSA'nın uzun dönemli bağımlılıkları öğrenmede yaşadığı zorlukları aşmak amacıyla geliştirilmiş bir mimaridir. Bu algoritma, özellikle dil modelleme, konuşma tanıma ve zaman serisi analizi gibi ardışık veri gerektiren uygulamalarda etkili sonuçlar üretmektedir (Hochreiter, 1997).

UKSB, bilgi akışını kontrol eden giriş, unutma ve çıkış kapıları aracılığıyla çalışır. Bu kapılar, her zaman adımında gelen verinin ne kadarının hatırlanacağını ne kadarının unutulacağını ve hangi bilginin sonraki adımlara aktarılacağını belirler. Böylece, model uzun vadeli ilişkileri daha etkili bir şekilde öğrenir (Goodfellow, 2016).

UKSB, uzun dizilerdeki bilgiyi koruyarak geleneksel TSA'ların yaşadığı gradyan sönmesi problemini önemli ölçüde azaltır. Bu özellik sayesinde, dil işleme, müzik analizi ve video işleme gibi sıralı verilerde başarılı sonuçlar elde edilmektedir. Ancak, UKSB'nin hücre yapısındaki ek kapılar ve parametreler, modelin hesaplama maliyetini artırarak eğitim süresini uzatabilir (Hochreiter, 1997).

UKSB, doğal dil işleme, makine çevirisi, ses tanıma ve finansal zaman serileri tahmini gibi birçok alanda yaygın olarak kullanılmaktadır. Bu geniş uygulama yelpazesi, algoritmanın ardışık verilerdeki örüntüleri yakalama ve uzun vadeli bağımlılıkları öğrenme yeteneğini ortaya koymaktadır (Goodfellow, 2016).

3.6. Değerlendirme Metrikleri

Bu çalışmada, CICIOT2023 veri kümesindeki saldırıların sınıflandırılması amacıyla DÖ ve MÖ temelli farklı algoritmalar karşılaştırmalı olarak incelenmiştir. DÖ modellerinden YSA, UKSB Ağları, TSA ve ESA ile MÖ algoritmalarından ise LR, RO, KEYK, KA, GA, AGA ve NB yöntemleri kullanılarak kapsamlı bir analiz

gerçekleştirilmiştir. Kullanılan modellerin performans değerlendirmesi için karmaşıklık matrisi, doğruluk, kesinlik, duyarlılık ve F1-skoru gibi metriklerden yararlanılmış, yöntemlerin sınıflandırma başarısı karşılaştırmalı olarak ortaya konulmuştur.

3.6.1. Karmaşıklık matrisi

Sınıflandırma algoritmalarının performansının değerlendirilmesi için farklı metriklerden faydalanılmıştır. Bu değerlendirme sürecinde karmaşıklık matrisi (confusion matrix) temel bir ölçüt olarak kullanılmıştır. Karmaşıklık matrisi, sınıflandırma modellerinin başarısını ölçerken temel alınan, farklı performans kriterlerinin hesaplanmasına olanak sağlayan bir araçtır. Siber güvenlik alanında, özellikle DDoS saldırılarının tespit edilmesinde, bu matris sayesinde modelin normal ağ trafiği ile zararlı trafik arasındaki ayırım gücü etkili bir şekilde değerlendirilebilir.

Çizelge 3.3. Karmaşıklık matrisi

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

Çizelge 3.3'te gösterilen karmaşıklık matrisi parametreleri aşağıdaki şekilde açıklanabilir:

- **Doğru Pozitif (TP):** Model tarafından pozitif olarak tahmin edilen ve gerçekte de pozitif olan örneklerin sayısını ifade eder.
- **Yanlış Pozitif (FP):** Model tarafından pozitif olarak tahmin edilen ancak gerçekte negatif olan örneklerin sayısını gösterir. Bu, Tip I hata olarak da bilinir.
- **Doğru Negatif (TN):** Model tarafından negatif olarak tahmin edilen ve gerçekte de negatif olan örneklerin sayısını ifade eder.
- **Yanlış Negatif (FN):** Model tarafından negatif olarak tahmin edilen ancak gerçekte pozitif olan örneklerin sayısını gösterir. Bu, Tip II hata olarak da adlandırılır.

Karmaşıklık matrisindeki TP ve TN değerleri, modelin doğru tahmin ettiği örneklerin toplam sayısını vermektedir. Bu değerler, modelin performansının olumlu

yönünü temsil eder. Öte yandan, FN ve FP değerleri ise modelin yanlış sınıflandırdığı örneklerin sayısını göstermektedir ve bu değerler model performansının iyileştirilmesi gereken yönlerini işaret eder (Pushpa Singh, 2021). IoT güvenliği bağlamında, yanlış negatifler özellikle tehlikelidir çünkü tespit edilmeyen saldırıları temsil ederken, yanlış pozitifler gereksiz uyarılara ve kaynak tüketimine yol açabilir (Hodo ve ark., 2016).

3.6.2. Performans metrikleri

Modellerin performansını doğru bir biçimde değerlendirebilmek ve sonuçların daha net anlaşılmasını sağlamak amacıyla karmaşıklık matrisi ve buradan elde edilen metriklerden faydalanılmaktadır. Karmaşıklık matrisinden türetilen performans parametreleri aşağıda detaylandırılmıştır.

- Doğruluk (Accuracy): Model performansının değerlendirilmesinde sıklıkla kullanılan temel bir ölçüttür. Doğruluk, doğru tahmin edilen örneklerin sayısının toplam örnek sayısına bölünmesi ile hesaplanmaktadır. Denklem 3.5 ile ifade edilmektedir:

$$Accuracy(Dogruluk) = \frac{TP+TN}{TP+TN+FP+FN} \quad (3.5)$$

Yaygın olarak kullanılmasına rağmen, doğruluk tek başına, bir sınıfın diğerini önemli ölçüde aştığı dengesiz veri setlerinde yanıltıcı olabilir, bu da genellikle ağ trafiği verilerinde karşılaşılan bir durumdur (Sharafaldin ve ark., 2018b).

- Kesinlik (Precision): Bu metrik, model tarafından belirli bir sınıfa ait olduğu tahmin edilen örneklerin kaç tanesinin gerçekte o sınıfa ait olduğunu göstermektedir (Denklem 3.6). Başka bir ifadeyle, modelin pozitif olarak işaretlediği tahminlerin doğruluğunu ölçer. Kesinlik değerinin yüksek olması, yanlış pozitiflerin (yanlış alarmların) az olduğu ve tahminlerin güvenilirliği açısından oldukça olumlu bir gösterge olarak kabul edilir (Sokolova ve Lapalme, 2009). Özellikle saldırı tespit sistemlerinde, modelin saldırı olarak belirlediği durumların gerçekte ne kadarının saldırı olduğunun anlaşılması ve yanlış alarm oranlarının düşük tutulması açısından önemli bir değerlendirme ölçütüdür.

$$Precision(Kesinlik) = \frac{TP}{TP+FP} \quad (3.6)$$

- Duyarlılık (Recall): Bu performans ölçütü, modelin gerçekte pozitif olan tüm örnekleri doğru bir şekilde belirleyebilme yeteneğini ifade etmektedir. Doğru pozitif (TP) olarak sınıflandırılan örneklerin sayısının, toplam gerçek pozitif örnek sayısına (doğru pozitif ve yanlış negatiflerin toplamına) oranı olarak hesaplanmaktadır. Denklem 3.7 ile gösterilmektedir:

$$Recall(Duyarlılık) = \frac{TP}{TP + FN} \quad (3.7)$$

Duyarlılık metriği, özellikle yanlış negatiflerin maliyetinin yüksek olduğu durumlarda, örneğin tıbbi teşhislerde veya siber güvenlik saldırı tespitinde kritik öneme sahiptir (Saito ve Rehmsmeier, 2015)

- F1-Score: F1-Skoru, kesinlik (precision) ve duyarlılık (recall) metriklerinin harmonik ortalaması olarak hesaplanan, sınıflandırma modelinin performansını genel olarak değerlendirmeye yarayan bir metriktir (Chicco ve Jurman, 2020). Denklem 3.8 ile ifade edilmektedir:

$$F1 - Skor = \frac{2 * Kesinlik * Hassasiyet}{Kesinlik + Hassasiyet} \quad (3.8)$$

F1-Skoru, özellikle sınıf dağılımının dengesiz olduğu veri kümelerinde, doğruluk (accuracy) metriğine göre daha güvenilir sonuçlar verir. Bu metrik 0 ile 1 arasında değer almakta olup, değer 1'e yaklaşması modelin sınıflandırma başarısının yüksek olduğunu göstermektedir. Yanlış pozitif ve yanlış negatif örnekleri eş zamanlı olarak dikkate aldığı için, model performansının daha dengeli ve kapsamlı değerlendirilmesini sağlamaktadır (Forman, 2003). Siber güvenlik ve benzeri alanlarda, modelin genel performansını değerlendirmede kritik rol oynar.

3.7. CICIOT2023 Veri Ön İşleme

Bu tez çalışmasında, IoT ekosistemlerine yönelik saldırıları içeren CICIOT2023 veri seti temel alınmıştır. Modelleme aşamasına geçmeden önce, veri setinin Makine Öğrenmesi ve DÖ algoritmalarıyla işlenebilir hale getirilmesi amacıyla, Python dili kullanılarak kapsamlı bir veri ön işleme süreci tasarlanmış ve uygulanmıştır. Bu süreç,

veri setinin analitik modellere uygun hale getirilmesini sağlayarak, eğitim aşamasında daha verimli ve doğru sonuçlar elde edilmesine katkıda bulunmuştur.

3.7.1. CICIOT2023 Veri Seti: Kategorik Verilerin Kodlanması

Kategorik verilerin kodlanması, veri işleme sürecinin kritik aşamalarından biri olup, özellikle makine öğrenmesi algoritmaları tarafından analiz edilebilir veri setleri oluşturulması açısından önemlidir. Kategorik veriler, metinsel veya sembolik değerlerden oluştuğundan dolayı doğrudan sayısal analiz yöntemlerine uygun değildir ve bu nedenle belirli yöntemlerle sayısal formata dönüştürülmelidir.

Bu tez çalışmasında kategorik değişkenlerin kodlanmasında Label Encoding yöntemi tercih edilmiştir. Label Encoding yöntemi, kategorik sütunlardaki her benzersiz kategoriye ayrı bir tamsayı değeri atar. Bu sayısal dönüşüm sayesinde kategorik veriler, sayısal yöntemlerle işlenebilir hale gelir. Çalışmada, veriler üzerinde dengeleme işlemleri (SMOTE, ADASYN, Borderline SMOTE, SMOTEENN vb.) uygulanmadan önce, Label Encoder kullanılarak kategorik sütunlar geçici olarak sayısal değerlere çevrilmiştir.

Dengeleme işlemleri tamamlandıktan sonra, verilerin anlaşılabilirliğini ve analiz edilebilirliğini korumak amacıyla sayısal formattaki veriler tekrar orijinal kategorik değerlere dönüştürülmüştür. Böylece veri setinin özgünlüğü korunarak, yapılan örnekleme işlemleri sonucunda verilerin kalitesi ve model doğruluğu artırılmıştır. Sonuç olarak, tez çalışmasında uygulanan bu yöntem, sınıflandırma algoritmalarının performansını artırmak açısından kritik önem taşıyan bir ön işleme adımıdır.

3.7.2. Sınıf Dengesizliğinin Giderilmesi

Makine öğrenmesi uygulamalarında, sınıflar arasındaki dengesizlik sıklıkla karşılaşılan ve model performansını düşüren önemli bir sorundur. Bu tez çalışmasında, CICIOT2023 veri setindeki sınıf dengesizliğini gidermek amacıyla farklı örnekleme stratejileri kullanılmıştır. Bu yöntemler; SMOTE, ADASYN, Borderline-SMOTE ve SMOTEENN gibi etkin tekniklerden oluşmaktadır. Bu işlemler sonucunda ikili, sekizli ve otuz dört sınıflı dengeli veri kümeleri oluşturulmuştur. Dengelenmiş veri setlerine aşağıdaki bağlantı üzerinden erişim sağlanabilir:

<https://www.kaggle.com/datasets/ekremturkay/ciciot2023-balanced>

3.7.2.1. SMOTE, ADASYN, Borderline-SMOTE ve SMOTEENN Yöntemleri

Veri setindeki sınıfların dağılımlarındaki karmaşıklık ve sınıf sınırlarının belirsizliği nedeniyle farklı aşırı örnekleme yöntemleri tercih edilmiştir. Kullanılan yöntemler, sınıfların büyüklüğüne, sınır yapısına ve karmaşıklık düzeyine göre belirlenmiştir.

SMOTE (Synthetic Minority Over-sampling Technique) yöntemi, özellikle orta ve büyük boyutlu sınıflar için temel dengeleme stratejisi olarak kullanılmıştır. Bu yöntem, mevcut azınlık sınıfına ait örneklerin özellik uzayındaki yakın komşularını kullanarak yeni sentetik örnekler üretir. DDoS-ICMPFlood, DDoS-UDP_Flood ve Recon-PingSweep gibi sınıflarda SMOTE uygulanarak sınıfların örnek sayıları artırılmıştır. Böylece, sınıflandırma modellerinin azınlık sınıflarını daha iyi öğrenmesi ve genel performanslarının artması sağlanmıştır (Chawla ve ark., 2002).

Borderline-SMOTE yöntemi, özellikle karar sınırlarına yakın, yani belirsiz sınıf sınırlarına sahip sınıflar için tercih edilmiştir. Bu yöntem, sınıf sınırındaki örneklerden sentetik veri üreterek sınıf ayrımının daha belirgin hale gelmesini sağlar. Bu çalışmada DDoS-RSTFINFlood ve DDoS-SynonymousIP_Flood gibi sınıflarda kullanılarak, sınıf sınırlarının netleşmesi hedeflenmiştir (Han ve ark., 2005).

ADASYN (Adaptive Synthetic Sampling) yöntemi, öğrenilmesi daha karmaşık olan sınıflarda tercih edilmiştir. Bu yöntem, veri uzayında öğrenilmesi zor alanlara odaklanarak daha fazla sentetik veri üretir. Mirai saldırıları ve Web saldırıları gibi karmaşık dağılımlara sahip sınıflarda ADASYN yöntemi kullanılarak, sınıflar arası dengesizlik azaltılmış ve modelin hassasiyeti artırılmıştır (He ve ark., 2008).

SMOTEENN yöntemi ise, ilk aşamada SMOTE tekniği ile sentetik veri üretimi gerçekleştirilir ve ardından Edited Nearest Neighbors (ENN) yöntemi kullanılarak üretilen sentetik veriler arasındaki gürültü ve hatalı örnekler temizlenir. Bu yöntem özellikle MITM (Man-In-The-Middle), DNS_Spoofing ve Reconnaissance gibi sınıflar için tercih edilmiştir. SMOTEENN, gürültülü örneklerin yoğun olduğu sınıflarda sınıf sınırlarını daha net ve temiz hale getirerek, sınıflandırıcıların performansını iyileştirmiştir (Batista ve ark., 2004).

Son olarak, BenignTraffic sınıfı veri setindeki en büyük örnek sayısına sahip sınıf olduğundan, aşırı uyumu önlemek amacıyla alt örnekleme (undersampling) yöntemi kullanılarak örnek sayısı azaltılmıştır.

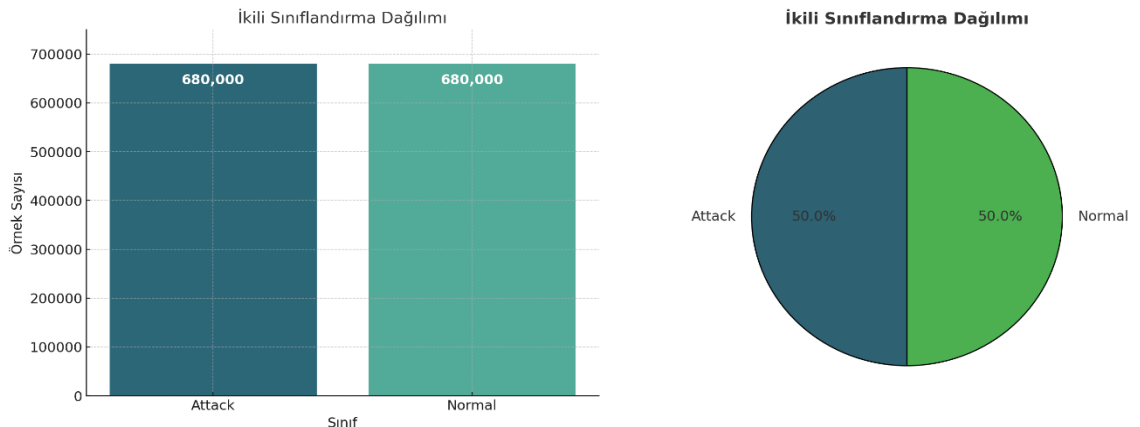
Bu farklılaştırılmış ve stratejik örnekleme yaklaşımları sayesinde sınıfların yapısına uygun sentetik veriler üretilmiş ve sınıflandırma modellerinin genel doğruluk, hassasiyet ve genelleme performansları önemli ölçüde artırılmıştır.

3.7.2.2. Farklı Dengeleme Stratejilerinin Seçim Gerekçeleri

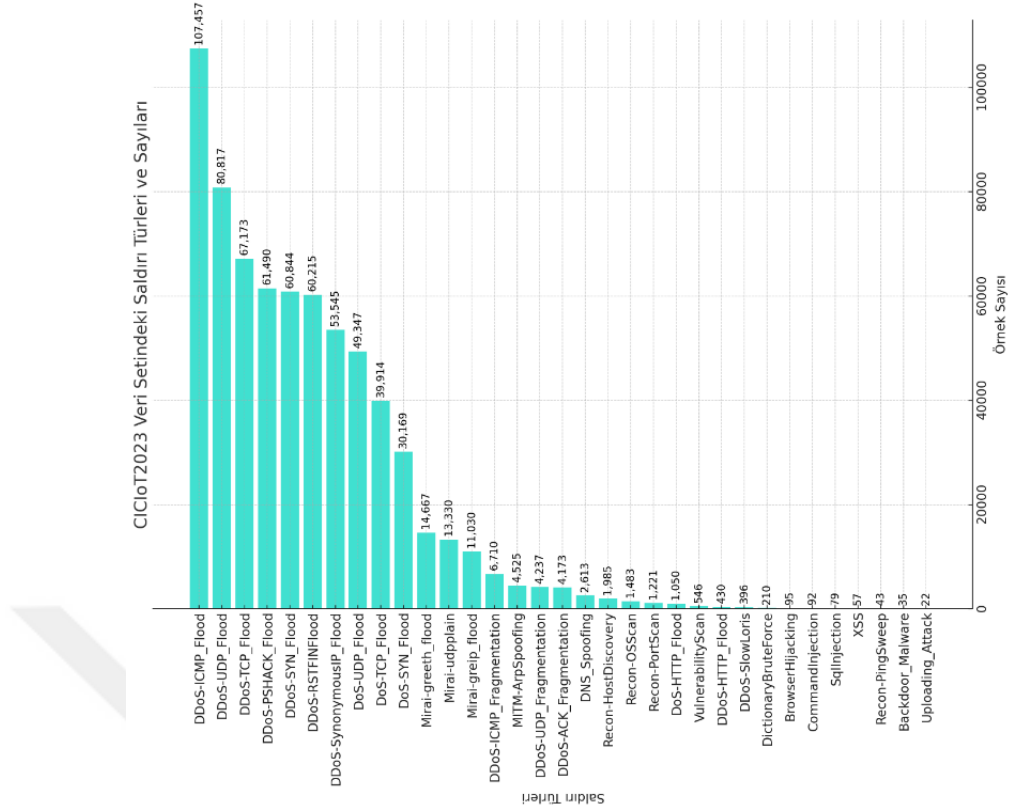
Çalışmada farklı dengeleme yöntemlerinin seçimi yapılırken sınıf büyüklüğü, saldırı türünün karmaşıklığı ve pozitif-negatif örnek sayısı arasındaki fark temel kriterler olarak dikkate alınmıştır. Küçük boyutlu ve karmaşık sınıflarda (örn. Mirai, Web Attacks) ADASYN yöntemi; sınıf sınırları belirsiz orta büyüklükteki sınıflarda (örn. DDoS-RSTFINFlood, DDoS-SynonymousIP_Flood) Borderline-SMOTE; orta boyutlu ancak gürültülü sınıflarda ise SMOTEENN yöntemi tercih edilmiştir. Çok büyük sınıflarda ise temel SMOTE uygulaması yeterli görülmüştür. Ayrıca, en fazla örneğe sahip BenignTraffic sınıfında aşırı uyumun önüne geçmek için alt örnekleme yöntemi kullanılmıştır. Bu farklılaştırılmış strateji yaklaşımı, sentetik örneklerin gerçek veri dağılımına daha yakın oluşturulmasını sağlayarak sınıflandırma modellerinin doğruluk ve genelleme yeteneklerini iyileştirmiştir.

3.7.3. CICIOT2023 Veri Seti: İkili Sınıflandırma İçin Hazırlık

Şekil 3.3'te görüldüğü gibi, veri setinde ciddi bir dengesizlik bulunmaktadır. Attack sınıfına ait 45,588,384 örnek bulunurken, Normal sınıfı yalnızca 1,098,195 örnek içermektedir. Bu çalışmada ikili sınıflandırma yapılabilmesi için veri dengesinin sağlanması gerekmektedir. Bu amaçla, her iki sınıftan rastgele örnekleme yöntemi kullanılarak 680,000'er örnek seçilmiş ve veri seti dengelenmiştir (Şekil 3.25).



Şekil 3.25. Veri dengeleme işlemi sonrası ikili sınıflandırmaya göre sınıf dağılımı grafikleri



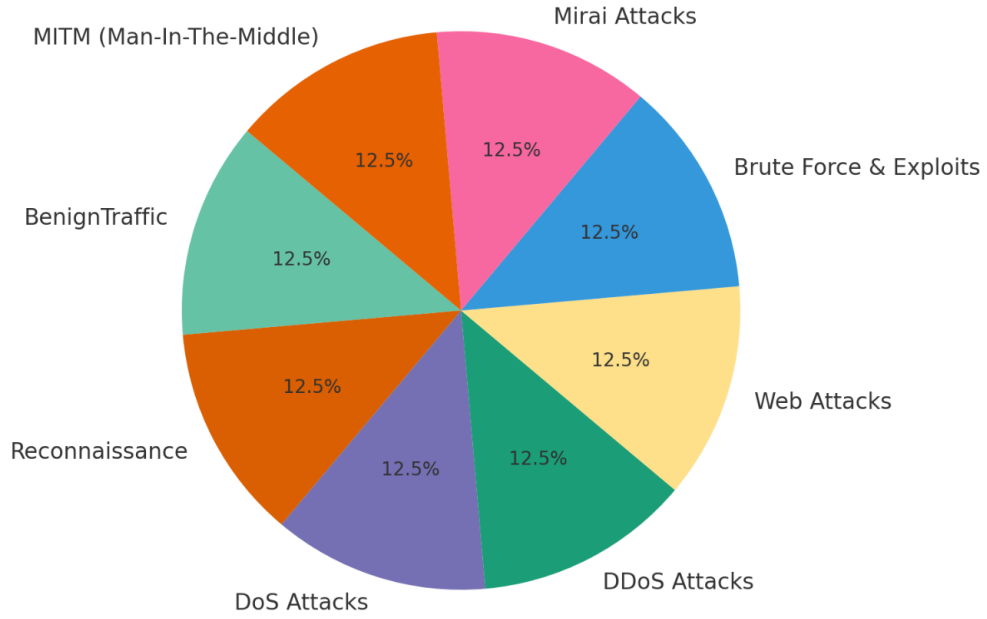
Şekil 3.26. Veri setindeki ikili sınıflandırmaya göre orijinal attack sınıf dağılımı

Şekil 3.26, CICIoT2023 veri setinde yer alan saldırı türlerinin örnek sayılarına göre dağılımını göstermektedir. Grafikte en fazla örnek içeren saldırı türünün DDoS-ICMP Flood olduğu görülmekte olup, bunu DDoS-UDP Flood ve DDoS-TCP Flood saldırıları izlemektedir.

3.7.4. CICIoT2023 Veri: Sekizli Sınıflandırma İçin Hazırlık

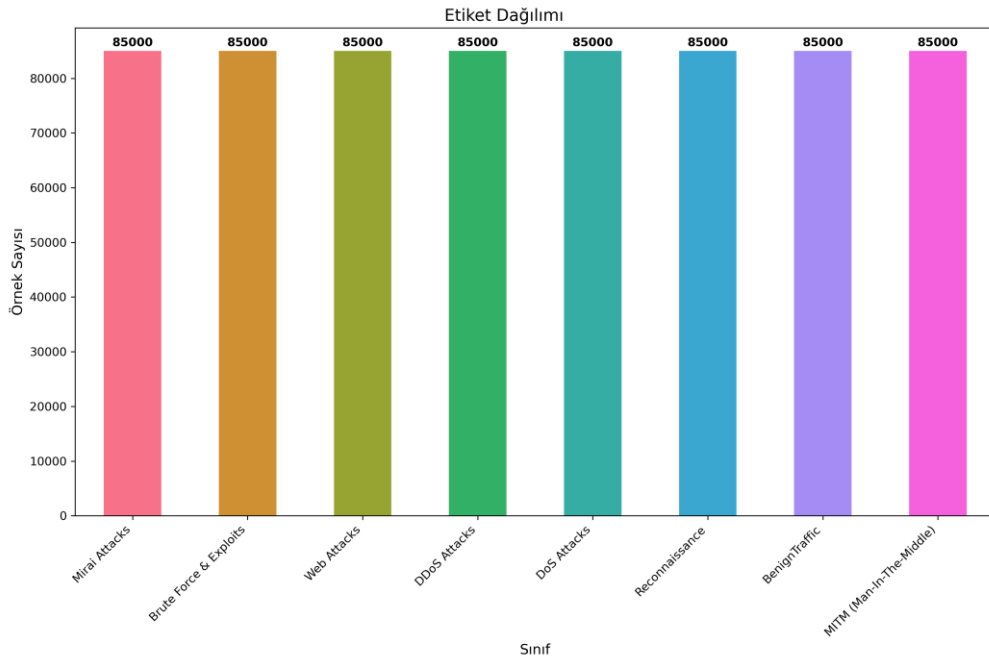
Veri seti içerisindeki sınıflar arasında ciddi bir dengesizlik bulunmaktaydı. Örneğin, DDoS Attacks sınıfı 33,984,560 örnek içerirken, Web Attacks sınıfı yalnızca 14,500 örnekten oluşmaktaydı. Bu tür büyük dengesizlikler, makine öğrenimi modellerinin ağırlıklı olarak büyük sınıflara odaklanmasına ve küçük sınıfları ihmal etmesine neden olabilir. Bu durum, özellikle saldırı türlerinin doğru sınıflandırılması açısından önemli bir risk oluşturmaktadır.

Bu çalışmada, sınıflandırma modelinin tüm sınıfları eşit derecede dikkate almasını sağlamak amacıyla veri dengeleme işlemi gerçekleştirilmiştir. Büyük veri grupları için rastgele alt örnekleme (random undersampling) uygulanırken, küçük veri gruplarına yönelik SMOTE, Borderline-SMOTE ve Adaptive Sampling gibi hibrit yöntemler kullanılmıştır. Özellikle, Brute Force & Exploits ve Web Attacks gibi küçük sınıflar, sentetik veri üretme teknikleriyle 85,000 örneğe çıkarılmıştır.

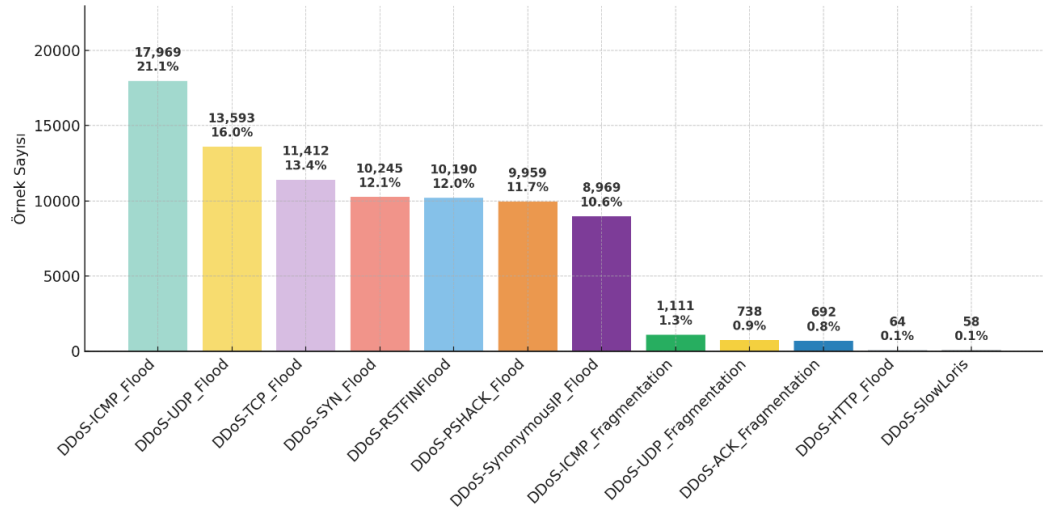


Şekil 3.27. Veri dengeleme işlemi sonrası sınıfların yüzdesel dağılımı

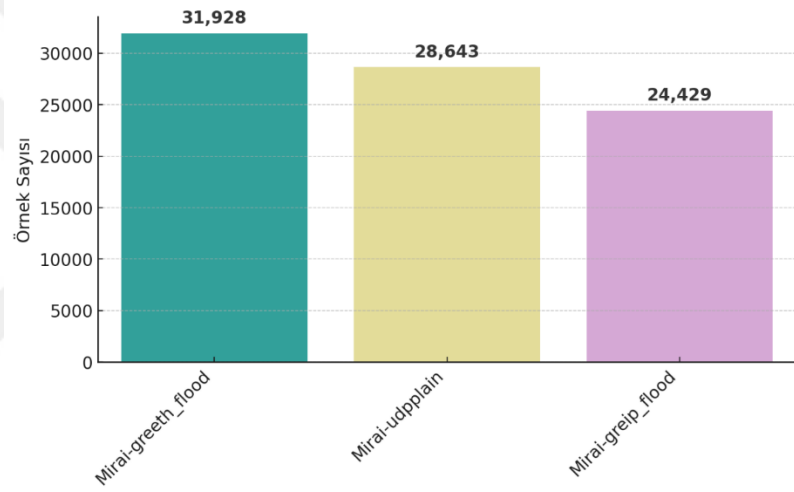
Bu işlemler sonucunda, DDoS Attacks, DoS Attacks, Mirai Attacks, Benign Traffic, MITM (Man-In-The-Middle), Reconnaissance, Brute Force & Exploits ve Web Attacks olmak üzere toplam 8 sınıfın her biri 85,000 örneğe eşitlenmiştir. Böylece, toplam 680,000 örnek içeren dengeli bir veri seti oluşturulmuştur. Bu sayede, sınıflandırma modelinin her bir saldırı türüne eşit ağırlık vermesi sağlanmış ve modelin küçük saldırı türlerini de başarılı bir şekilde öğrenmesi için uygun bir ortam hazırlanmıştır.



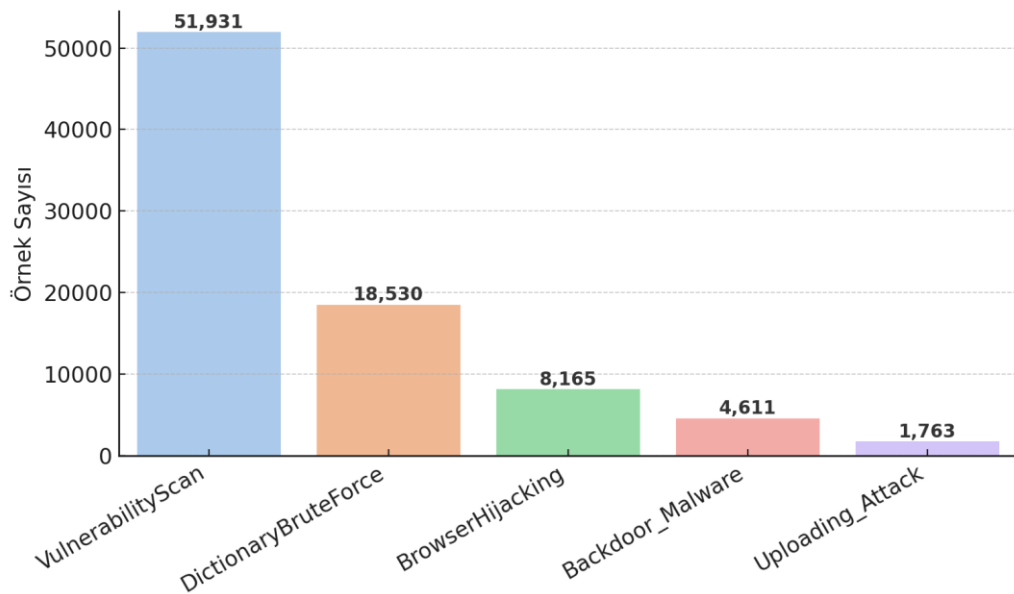
Şekil 3.28. Sekizli sınıflandırmaya göre veri dengeleme işlemi sonrası sınıf dağılımı



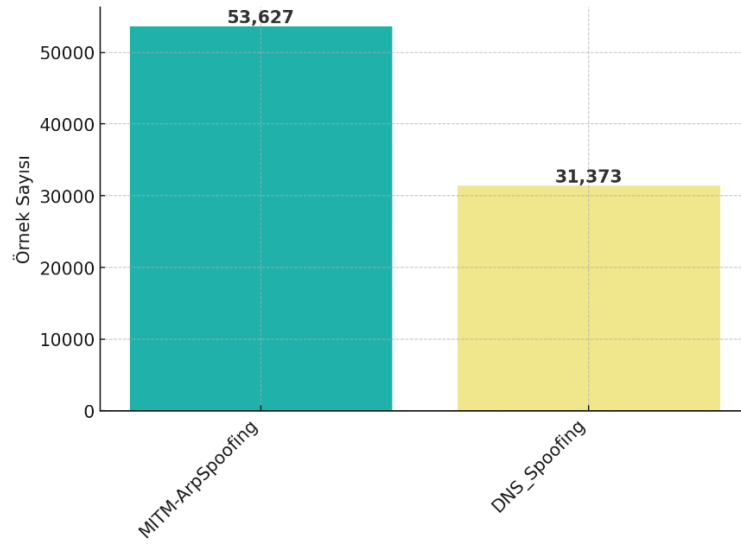
Şekil 3.29. DDoS attacks sınıfındaki orijinal etiket dağılımı



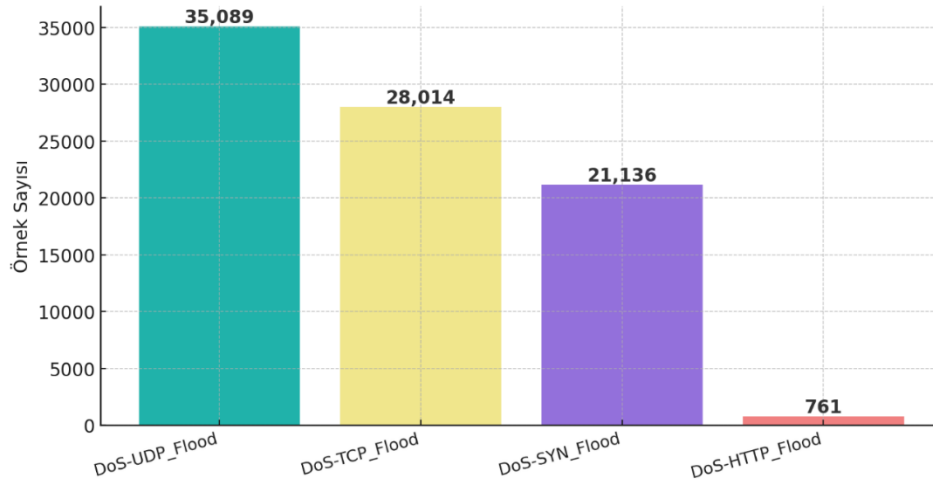
Şekil 3.30. Mirai attacks sınıfındaki orijinal etiket dağılımı



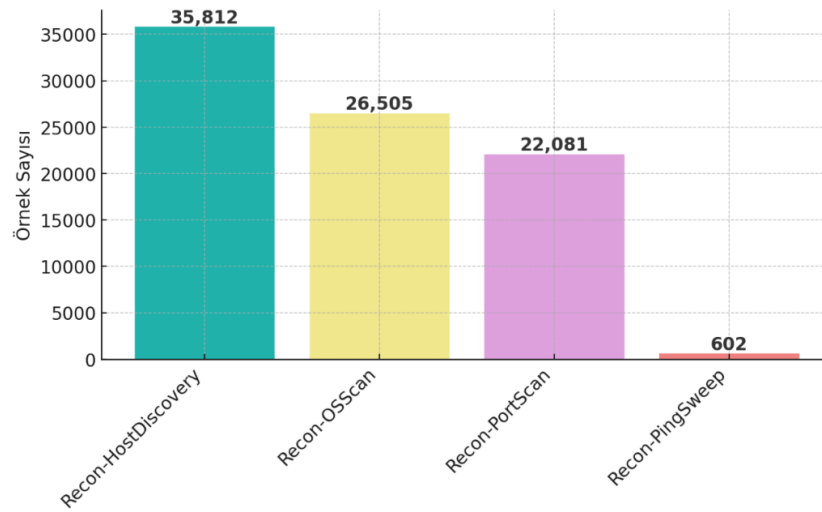
Şekil 3.31. Brute force & exploits sınıfındaki orijinal etiket dağılımı



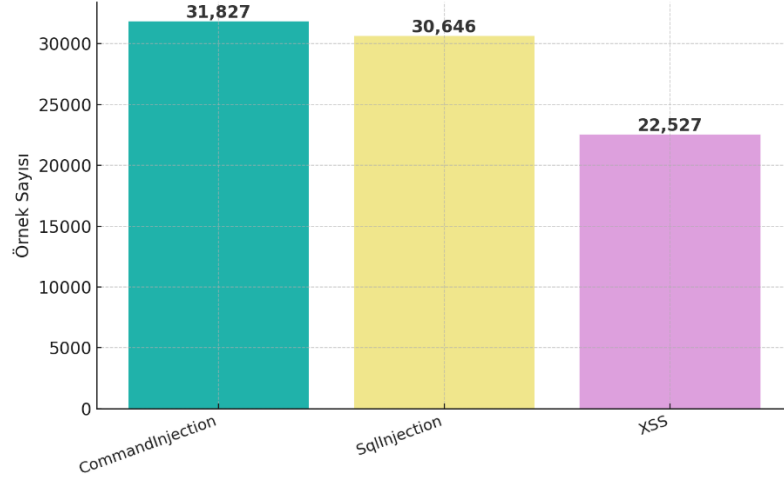
Şekil 3.32. MITM (man-in-the-middle) sınıfındaki orijinal etiket dağılımı



Şekil 3.33. DoS attacks sınıfındaki orijinal etiket dağılımı



Şekil 3.34. Reconnaissance sınıfındaki orijinal etiket dağılımı



Şekil 3.35. Web attacks sınıfındaki orijinal etiket dağılımı

Şekil 3.27–3.35, CICIOT2023 veri setinde yer alan farklı saldırı türlerine ilişkin sınıf dağılımlarını göstermektedir. Bu şekillerde, veri dengesizliği sorununun analiz edilmesine yardımcı olmak amacıyla dengelenmiş veri yapıları görselleştirilmiştir. Dengelenmiş sınıf dağılımları, sekizli sınıflandırma için her bir saldırı türünden eşit sayıda örnek seçilerek oluşturulmuş; DDoS, DoS, brute force, Mirai, MITM, reconnaissance, web tabanlı saldırılar ve diğer alt türler grafiklerle ayrı ayrı sunulmuştur. Bu görselleştirmeler, model eğitimi öncesinde sınıf temsiliyetini dengelemek, örnek yoğunluklarını değerlendirmek ve sınıflar arası dağılım farklılıklarını ortaya koymak amacıyla kullanılmıştır.

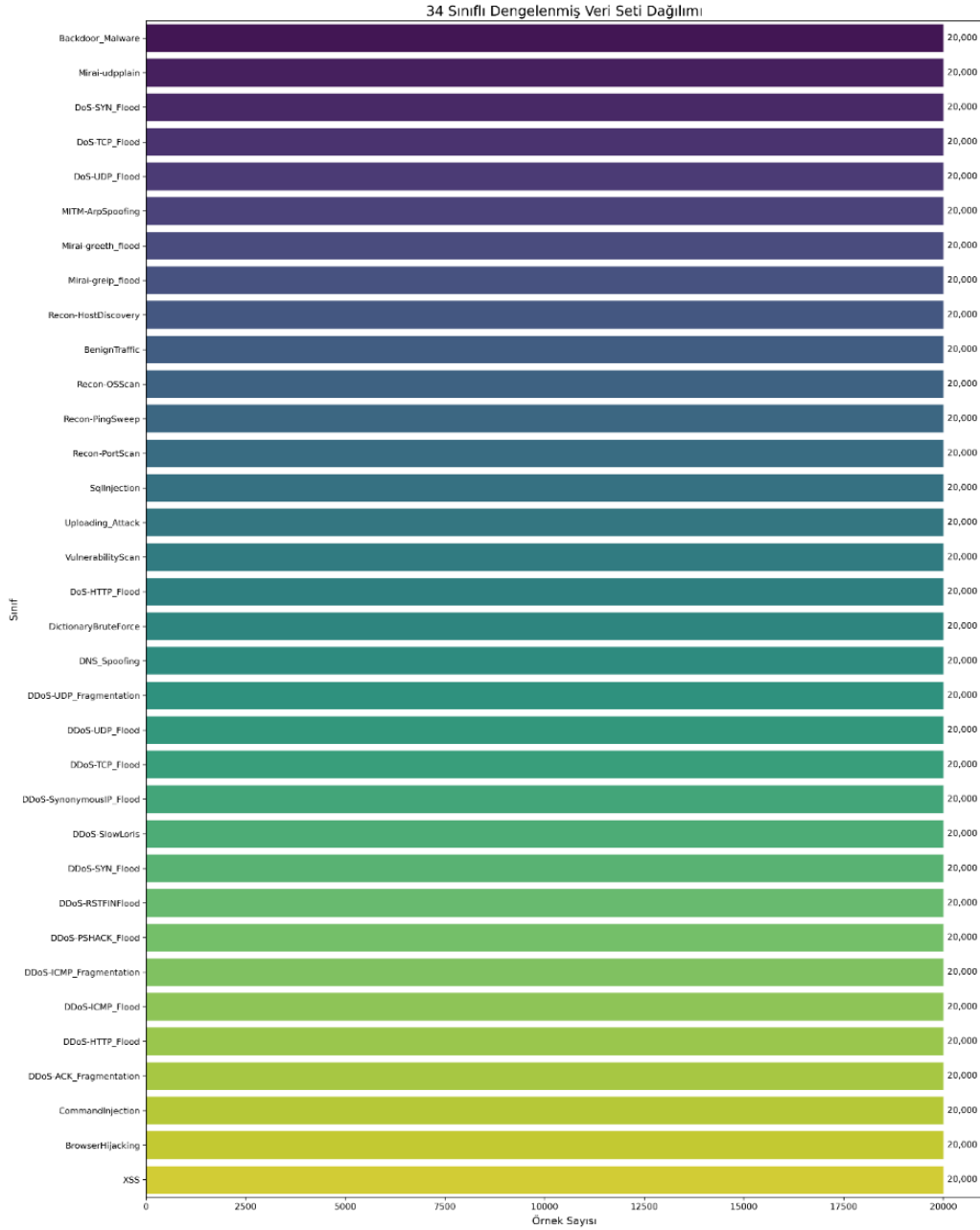
3.7.5. CICIOT2023 Veri: Otuz Dört Sınıflı Sınıflandırma İçin Hazırlık

Veri setinde 33 farklı saldırı türü ve 1 normal trafik sınıfı bulunmaktadır. Ancak, bu sınıflar arasındaki veri dağılımı oldukça dengesizdir. Örneğin, DDoS-ICMP Flood saldırı türü 7,200,504 örnek içerirken, Uploading Attack yalnızca 1,252 örnekten oluşmaktadır. Bu dengesizlik, makine öğrenimi modelinin büyük sınıflara öncelik vererek küçük sınıfları göz ardı etmesine neden olabileceğinden, veri dengeleme işlemi uygulanmıştır.

Bu süreçte, rastgele alt örnekleme (random undersampling) ve sentetik veri üretme (SMOTE, Borderline-SMOTE, Adaptive Sampling) gibi hibrit yöntemler kullanılmıştır. Büyük örnekleme sahip sınıfların veri miktarı rastgele alt örnekleme ile azaltılırken, küçük örneklemlili sınıflar için SMOTE ve Adaptive Sampling yöntemleri ile sentetik veriler üretilmiştir. Bu sayede, tüm sınıfların 20,000 örneğe eşitlenmesi sağlanarak veri seti dengeli hale getirilmiştir.

Şekil 3.36'da CICIOT2023 veri setinde çoklu sınıflandırma amacıyla dengelenmiş 34 farklı saldırı ve normal trafik sınıfının dağılımı gösterilmektedir. Her bir sınıf için

20.000 örnek olacak şekilde veri seti eşitlenmiş ve bu dengeleme sayesinde modelin sınıflar arasında önyargısız öğrenmesi hedeflenmiştir. Bu grafik, sınıf sayılarının eşit olduğunu ve dengeli bir eğitim ortamı sağlandığını görsel olarak ortaya koymaktadır.



Şekil 3.36. CICIoT2023 veri setinde çoklu sınıflandırma için dengelenmiş sınıf dağılımı

3.7.6. CICIoT2023 Veri: Özellik seçimi

CICIoT2023 veri seti, IoT cihazlarının ağ trafiğine ait saldırı ve normal davranışları içeren kapsamlı bir veri kümesidir. Veri seti, farklı saldırı türlerine (örneğin, DoS, DDoS, Port Scan vb.) karşılık gelen çok sayıda gözlem ve geniş bir özellik yelpazesi

içermektedir. Bu zengin yapısı, siber güvenlik alanında etkin sınıflandırma modelleri geliştirmek için güçlü bir temel sunmaktadır. Ancak, yüksek boyutlu bu veri setinde tüm özelliklerin modele dahil edilmesi, hesaplama maliyetini artırmakta ve bazı durumlarda modelin genelleme kapasitesini olumsuz etkileyebilmektedir.

Bu nedenle, özellikle makine öğrenmesi modelleri uygulanmadan önce özellik seçimi (feature selection) süreci kritik bir adımdır. Özellik seçimi sayesinde, veri setinde yer alan gereksiz, tekrarlayan ya da düşük bilgilendirici nitelikler elenerek, modelin yalnızca anlamlı ve etkili özelliklerle çalışması sağlanır. Bu durum, hem modelin öğrenme sürecini hızlandırmakta hem de doğruluk oranlarını artırarak aşırı öğrenme (overfitting) riskini azaltmaktadır (Guyon ve Elisseeff, 2003). CICIOT2023 veri setine uygulanan uygun özellik seçimi teknikleri, saldırı tespitinde en belirleyici değişkenlerin ortaya konulmasına ve daha güvenilir bir model geliştirilmesine olanak tanımaktadır.

3.7.7. Rastgele Orman (RO) Tabanlı Özellik Seçimi

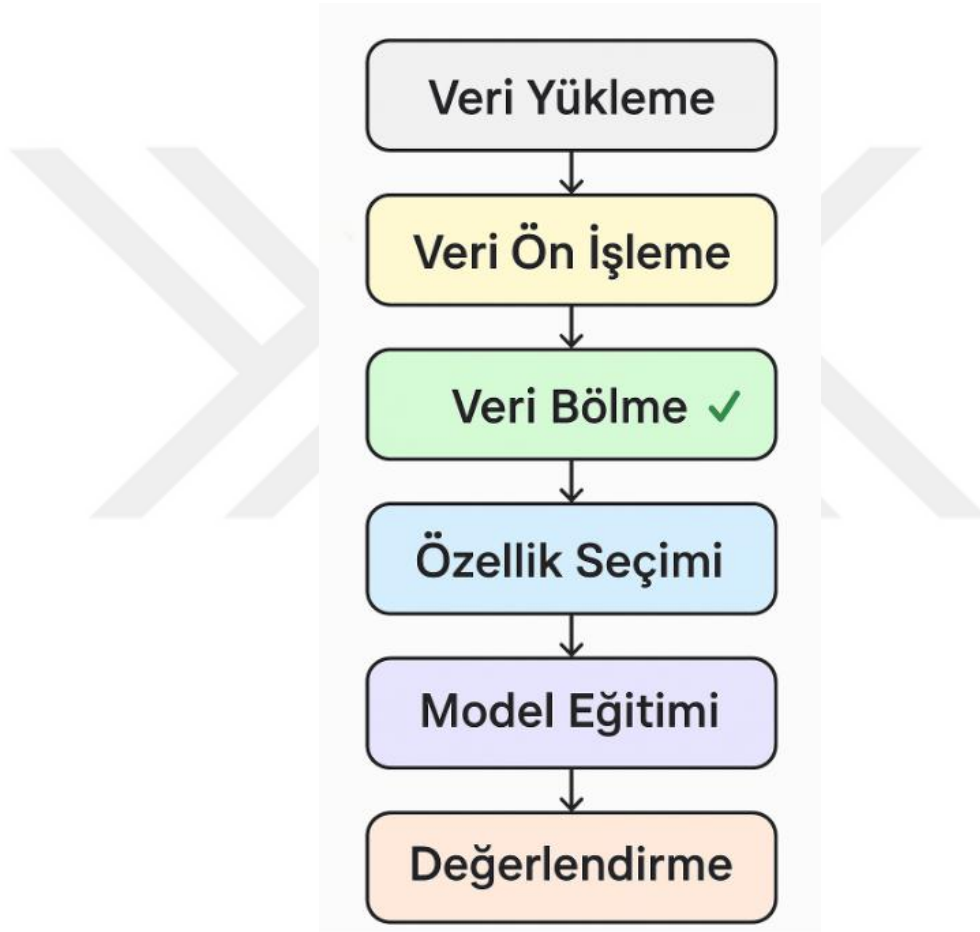
Makine öğrenmesi modellerinde yüksek boyutlu veri setleriyle çalışmak, modelin karmaşıklığını artırarak hem eğitim süresini uzatmakta hem de aşırı öğrenme (overfitting) riskini yükseltmektedir. Bu nedenle, veri setindeki en anlamlı ve etkili değişkenlerin belirlenmesi hem model performansını artırmak hem de hesaplama maliyetini azaltmak açısından kritik bir adımdır. Bu bağlamda, özellik seçimi (feature selection) yöntemleri ön plana çıkmaktadır. Özellikle denetimli öğrenmede sıkça kullanılan RO algoritması, yerleşik (embedded) bir yöntem olarak model eğitimi sırasında her bir özelliğin sınıflandırmaya katkısını ölçerek önem derecelerini belirleme avantajına sahiptir (Breiman, 2001).

RO, birden fazla karar ağacından oluşan topluluk (ensemble) tabanlı bir öğrenme algoritmasıdır ve her bir ağacın oylamasına dayalı olarak karar verir. Özellik önem skoru ise her bir özelliğin modelin tahmin gücüne yaptığı katkının, genellikle Gini indeksine veya bilgi kazancına (information gain) göre ölçülmesiyle elde edilir (Guyon ve Elisseeff, 2003). Özellikler, bu skorlara göre sıralanarak en etkili olanlardan başlayarak seçilir. Bu yöntem, özellikle dengesiz veri setlerinde ve yüksek boyutlu verilerde güvenilir sonuçlar vermesi nedeniyle yaygın şekilde tercih edilmektedir (Breiman, 2001).

RO tabanlı özellik seçimi, ağ trafiği gibi çok sayıda değişkene sahip verilerde, modelin hangi değişkenleri daha fazla dikkate aldığını analiz etmeyi kolaylaştırmakta ve saldırı tespitinde etkili özelliklerin önceliklendirilmesine olanak tanımaktadır.

4. ARAŞTIRMA SONUÇLARI VE TARTIŞMA

Bu çalışmada, IoT ağlarına yönelik saldırıların tespitine yönelik olarak CIIoT2023 veri seti kullanılmış ve hem Makine Öğrenmesi (MÖ) hem de Derin Öğrenme (DÖ) tabanlı modeller ile saldırıların sınıflandırılması gerçekleştirilmiştir. Çalışmanın temel amacı, çeşitli algoritmaların sınıflandırma başarımlarını karşılaştırmalı olarak inceleyerek, IoT tabanlı ağlarda en yüksek performansı sağlayan yöntemi belirlemektir.



Şekil 4.1. Çalışma adımları

Analiz süreci; veri ön işleme, özellik seçimi, dengesizlik giderme, model eğitimi ve performans değerlendirmesi adımlarından oluşmaktadır. Bu süreç Şekil 4.1’de genel hatlarıyla özetlenmiştir. Veri ön işleme aşamasında eksik veriler temizlenmiş, kategorik veriler sayısallaştırılmış ve SMOTE tabanlı örnekleme teknikleriyle sınıf dengesizliği

giderilmiştir. Özellik seçimi için RO tabanlı önem derecelendirmesi uygulanmış ve en belirleyici değişkenler sınıflandırma modellerinde kullanılmıştır.

Modelleme aşamasında DÖ yöntemlerinden YSA, UKSB, TSA ve ESA; MÖ algoritmalarından ise LR, NB, KA, RO, KEYK, GA ve AGA kullanılmıştır.

Eğitim sürecinde DÖ modelleri için optimizasyon algoritması olarak Adam kullanılmış, ikili sınıflandırmada binary_crossentropy, çoklu sınıflandırmada ise categorical_crossentropy kayıp fonksiyonları tercih edilmiştir. Çıkış katmanlarında ikili sınıflandırma için sigmoid, çoklu sınıflandırma için softmax aktivasyon fonksiyonları kullanılmıştır. Eğitim sırasında early stopping tekniği uygulanarak aşırı öğrenme (overfitting) engellenmiştir. Model eğitimi için 50 epoch ve 64 batch size kullanılmıştır.

Veri setleri %75 eğitim, %25 test olarak bölünmüş ve her bir model ayrı ayrı ikili, sekizli ve 34 sınıflı sınıflandırma senaryolarında test edilmiştir. Elde edilen sonuçlar doğruluk, kesinlik, duyarlılık, F1 skoru ve AUC metrikleri ile detaylı biçimde değerlendirilmiş; karmaşıklık matrisleri ve ROC eğrileri ile desteklenmiştir.

Sonuç olarak, özellikle DÖ modelleri küçük saldırı gruplarında daha yüksek duyarlılık gösterirken, makine öğrenmesi modelleri daha hızlı eğitim süresi ve sade yapılarıyla öne çıkmıştır. RO ve AGA modelleri yüksek doğruluk ve düşük yanlış pozitif oranları ile dikkat çekerken, YSA ve UKSB modelleri de özellikle çoklu sınıflandırmada yüksek F1 skorları ile başarılı sonuçlar vermiştir. Farklı senaryolara göre hangi modelin en uygun olduğu çalışmanın ilerleyen alt bölümlerinde detaylı biçimde tartışılmıştır.

4.1. Çalışma Ortamı

Deneysel sonuçlar, Python programlama dili kullanılarak Scikit-learn (sklearn) kütüphanesi ile gerçekleştirilmiştir. Performans ölçümleri için çeşitli metrikler hesaplanmış ve uygulamalar Anaconda ortamında test edilmiştir. Deneyler, donanım ve yazılım özellikleri Çizelge 4.1’de belirtilen bilgisayar ortamında gerçekleştirilmiştir.

Çizelge 4.1. Çalışma alanı

<i>Donanım</i>	<i>Özellikler</i>
CPU	Intel(R) Core(TM) i7-13650HX
İşletim Sistemi	Windows 11 Pro 64-bit
Grafik Kartı	NVIDIA GeForce RTX 4060
Ram	64 GB

Bu tez çalışmasında DÖ modellerinden YSA, UKSB, TSA ve ESA; MÖ modellerinden LR, RO, KA, GA, AGA, 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 50 epoch'da gerçekleştirilmiştir.

4.2. CICIOT2023 Veri Seti Sonuçları

Bu çalışmada, CICIOT2023 veri seti kullanılarak ikili sınıflandırma ile çoklu sınıflandırma (8 sınıf ve 34 sınıf) senaryolarında farklı modellerin performansları değerlendirilmiştir. Veri ön işleme adımları uygulandıktan sonra, elde edilen sonuçlar iki temel başlık altında detaylı olarak incelenmiştir.

4.2.1. İkili sınıflandırma sonuçları

Makine öğrenmesi tabanlı ağ trafiği analizi, günümüzde siber güvenlikte büyük bir öneme sahiptir. Özellikle, saldırı tespiti için kullanılan ikili sınıflandırma algoritmaları, ağ trafiğini zararlı (AttackTraffic) ve zararsız (BenignTraffic) olarak ayırarak saldırılara karşı daha hızlı ve güvenilir tespit mekanizmaları sunmaktadır.

Çizelge 4.2. Algoritmaların ikili sınıflandırma performans karşılaştırması ve özellik seçimi sonuçları

ALGORITMA	ÖZELLİK SAYISI	EN YÜKSEK DOĞRULUK	F1 SKORU
LR	29	0.9867	0.9868
NB	15	0.9864	0.9866
KEYK	31	0.9941	0.9941
KA	27	0.9971	0.9971
RO	36	0.9974	0.9974
GA	38	0.9973	0.9973
AGA	29	0.9971	0.9971
YSA	31	0.9944	0.9944
ESA	34	0.9945	0.9945
TSA	34	0.9948	0.9949
UKSB	39	0.9947	0.9948

Çizelge 4.2'de, farklı algoritmaların ikili sınıflandırma problemi üzerindeki performansları ile bu algoritmalarda kullanılan en uygun özellik sayıları karşılaştırılmıştır. Her bir algoritma için en yüksek doğruluk ve F1 skoru değerleri verilmiştir. Sonuçlara göre, özellikle KA, RO ve AGA modelleri, 0.9971 ve üzeri doğruluk oranlarıyla en başarılı sonuçları elde etmiştir. Bununla birlikte, bazı algoritmalar daha az sayıda özellik ile yüksek başarı sağlamış (örneğin NB), bu da özellik seçiminin model başarısı üzerindeki etkisini ortaya koymuştur.

4.2.1.1. Lojistik Regresyon (LR) algoritması sonuçları

Bu çalışmada, LR algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

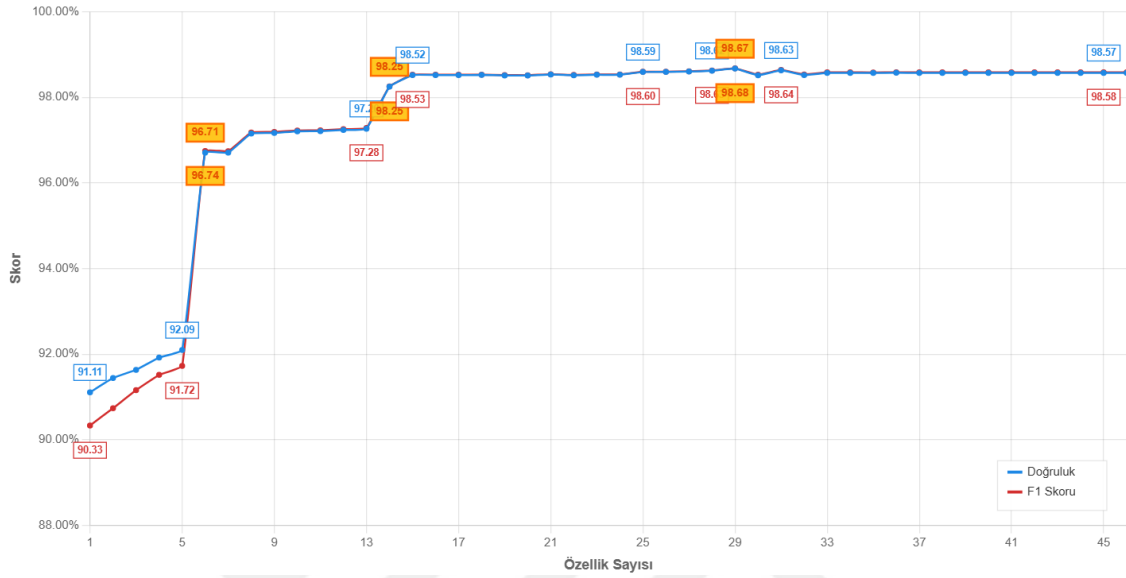
Çizelge 4.3, IoT trafiğinin sınıflandırılmasında kullanılan LR modeline ait doğruluk, kesinlik, duyarlılık, F1 skoru ve C parametresi değerlerini farklı özellik sayıları için göstermektedir.

Çizelge 4.3. LR için performans metrikleri

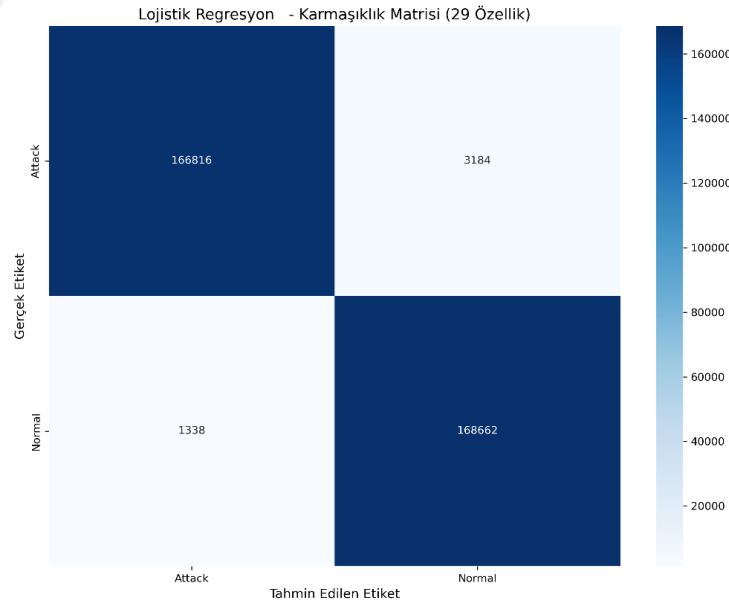
Özellik Sayısı	Doğruluk	Kesinlik	Duyarlılık	F1 Skoru	C Değeri
1	0.911059	0.989267	0.831135	0.903333	10.0
2	0.914418	0.989019	0.838141	0.907351	100.0
3	0.916332	0.966522	0.862541	0.911576	10.0
4	0.919179	0.963353	0.871512	0.915134	10.0
5	0.920941	0.962178	0.876329	0.917250	1.0
10	0.972065	0.965806	0.978782	0.972251	10.0
15	0.985200	0.980925	0.990612	0.98528	100.0
18	0.985215	0.980067	0.990576	0.985294	100.00
28	0.986188	0.981195	0.991376	0.98626	1.0
29	0.9867	0.981472	0.992129	0.986772	1.0
38	0.985715	0.977604	0.994206	0.985835	0.1
40	0.985706	0.977576	0.994218	0.985827	0.1
41	0.985703	0.977575	0.994212	0.985824	0.1

Şekil 4.2, LR modelinin RO tabanlı özellik seçimine göre doğruluk ve F1 skoru açısından gösterdiği performans değişimini ortaya koymaktadır. İlk 5 özellik kullanıldığında doğruluk %91.11–92.09, F1 skoru ise %90.33–91.73 aralığında kalmıştır. 6. özellik ile her iki metrikte de dikkate değer bir artış yaşanmış; doğruluk %96.71, F1 skoru ise %96.74 olarak gerçekleşmiştir. Özellik sayısı arttıkça performans da yükselmiş, 15. özellik ile birlikte doğruluk %98.52, F1 skoru %98.53 seviyelerine ulaşmıştır. En

yüksek değerler 29. özelliğe görülmüş (%98.67 doğruluk, %98.68 F1 skoru), ancak bu noktadan sonra artışın oldukça sınırlı olduğu gözlemlenmiştir. Bu nedenle, hesaplama maliyeti ve modelin sadeliği göz önünde bulundurulduğunda, 15 özelliğin optimal bir tercih olduğu değerlendirilmektedir.

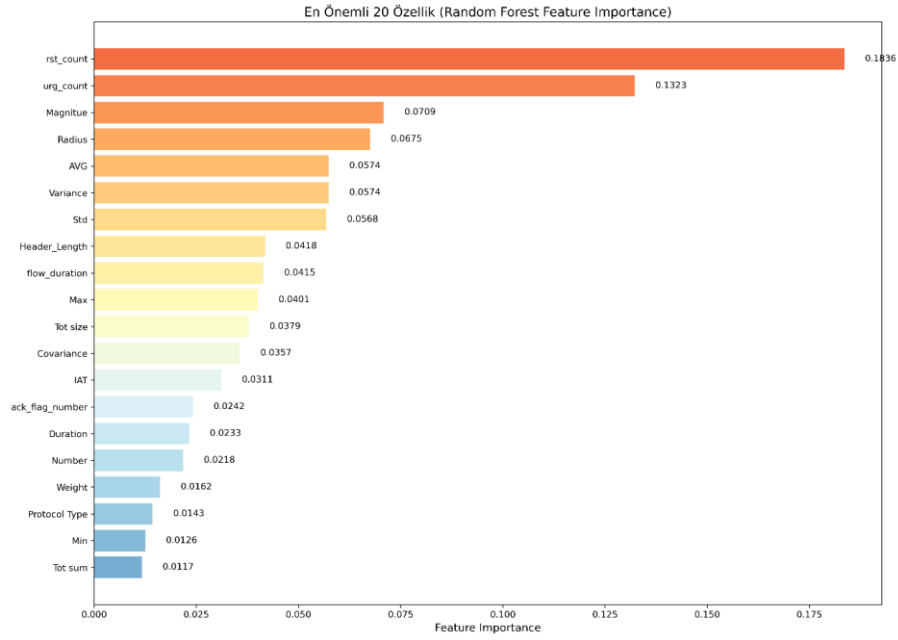


Şekil 4.2. LR modelinin özellik sayısına göre performans değişimi



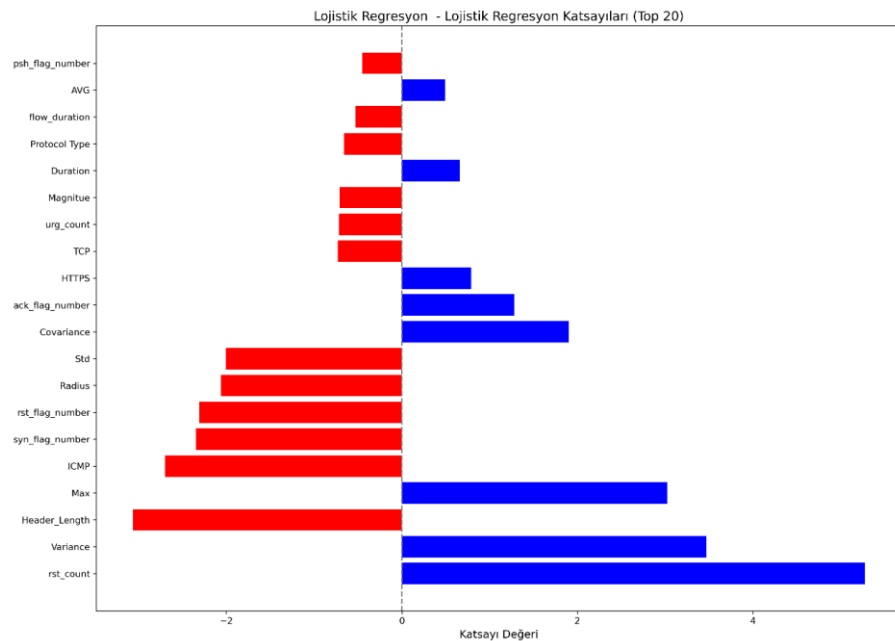
Şekil 4.3. LR modelinin iki sınıflı karmaşıklık matrisi (29 Özellik)

Şekil 4.3'te yer alan karmaşıklık matrisi, 29 özellikli LR modelinin %98.7 genel doğrulukla IoT ağ trafiğini sınıflandırdığını göstermektedir. Model, saldırıları %99.2 duyarlılık ve normal trafiği %98.1 özgüllükle tespit ederek, 340.000 veri noktası üzerinde yüksek performans sergilemiştir.



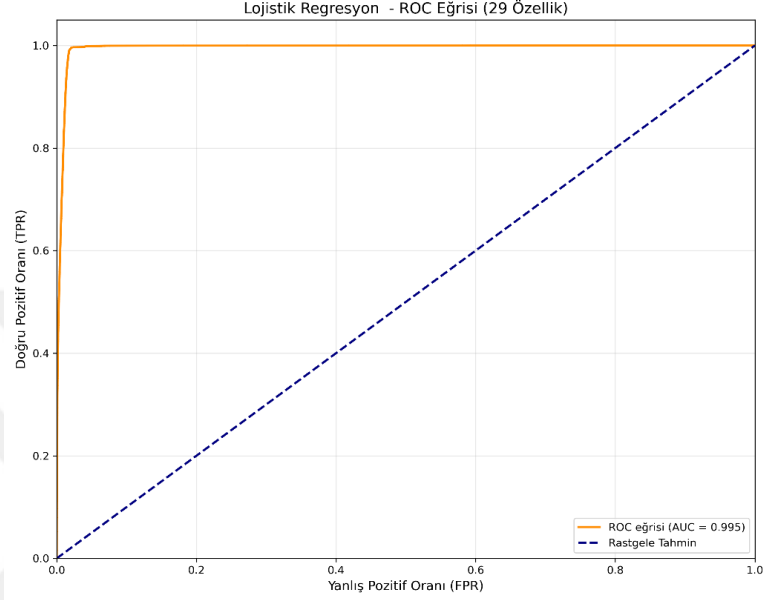
Şekil 4.4. En etkili 20 özelliğin RO ile belirlenen önem dereceleri

Şekli 4.4, IoT ağ trafiğini "Normal" ve "Attack" olarak sınıflandırmada kullanılan özelliklerin önem derecelerini, RO algoritmasıyla hesaplayarak göstermektedir. Özellikle rst_count (0.1836) en belirgin öneme sahip olup ağ trafiği sınıflandırmasında en güçlü belirleyici olarak öne çıkmaktadır. Bu özelliği sırasıyla urg_count ve Magnitude takip etmektedir. Grafik, özelliklerin saldırı veya normal trafik tespitinde ne kadar etkili olduğunu açıkça ortaya koymakta ve bu sayede IoT güvenlik sistemlerinde hangi özelliklerin öncelikli olarak değerlendirilmesi gerektiğini vurgulamaktadır.



Şekil 4.5. LR modelinde IOT ağ trafiğini etkileyen en güçlü 20 özelliğin katsayıları

Şekil 4.5, LR modelinde IoT ağ trafiğini sınıflandırmada en etkili 20 özelliğin katsayılarını göstermektedir. Pozitif katsayılar (mavi) saldırı trafiğini, negatif katsayılar (kırmızı) ise normal trafiği temsil etmektedir. Özellikle rst_count ve Variance gibi özellikler saldırı tespiti açısından öne çıkarken, ICMP ve syn_flag_number gibi özellikler normal trafiği ayırt etmede etkilidir.



Şekil 4.6. LR sınıflandırma algoritmasına ait ROC eğrisi

Şekil 4.6, 29 özellikli Lojistik Regresyon modeline ait ROC eğrisini göstermektedir. Eğrinin sol üst köşeye yakın konumlanması ve AUC değerinin 0.995 gibi yüksek bir seviyede olması, modelin düşük yanlış pozitif oranlarında bile yüksek doğru pozitiflik sağladığını ve saldırıları başarılı şekilde ayırt ettiğini göstermektedir. Rastgele tahmin eğrisinden net biçimde ayrılan bu yapı, modelin güçlü sınıflandırma performansını doğrulamaktadır.

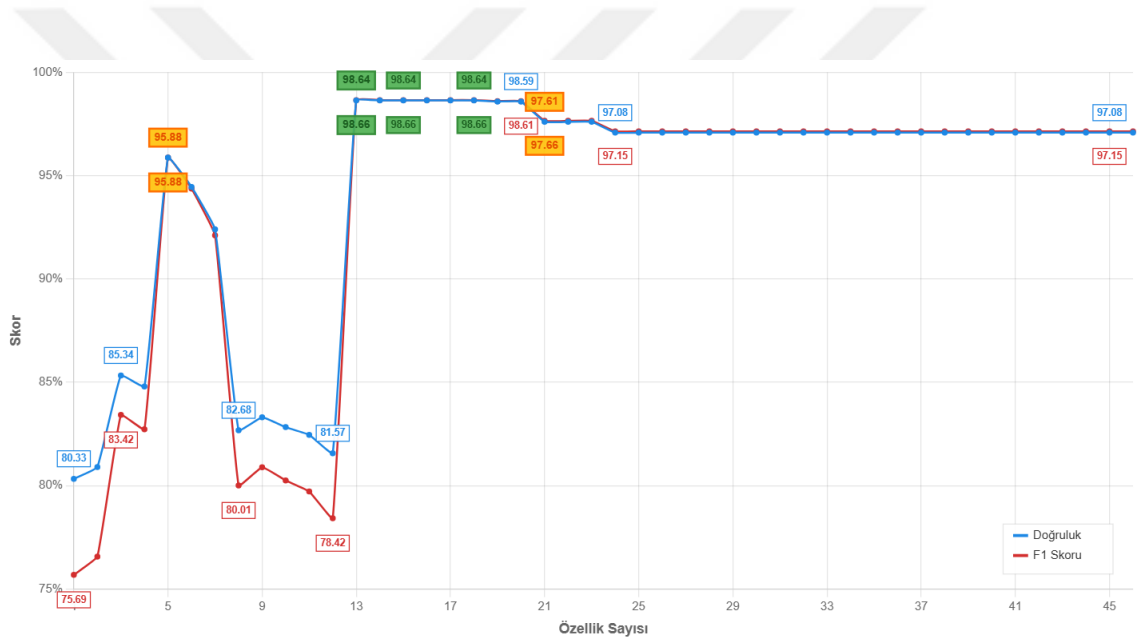
4.2.1.2. Naive Bayes (NB) algoritması sonuçları

Bu çalışmada, NB algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.4'te NB modelinin farklı sayıda özellikte elde ettiği doğruluk ve F1 skoru değerleri yer almaktadır.

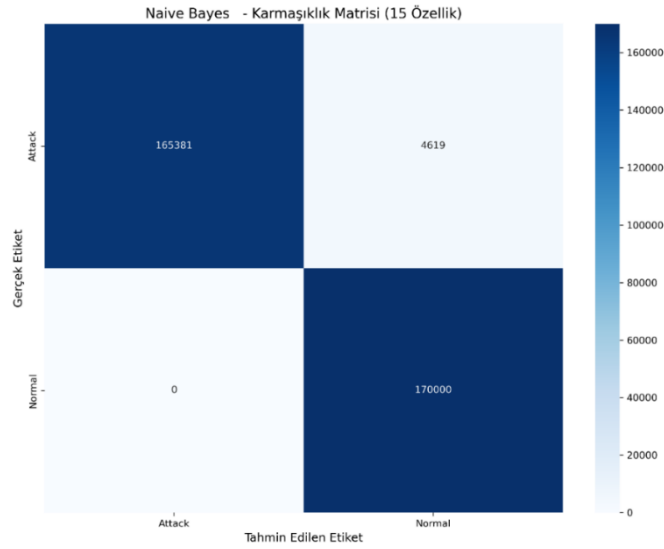
Çizelge 4.4. NB için performans metrikleri

Özellik Sayısı	Doğruluk	Kesinlik	Duyarlılık	F1 Skoru
1	0.803344	0.991115	0.612176	0.756864
3	0.853356	0.959406	0.737935	0.834222
5	0.958759	0.957247	0.960412	0.958827
7	0.924076	0.958379	0.886659	0.921125
9	0.833082	0.945950	0.706535	0.808899
11	0.824626	0.944798	0.689541	0.797236
13	0.986412	0.973543	1.000000	0.986594
15	0.986415	0.973548	1.000000	0.986597
17	0.986415	0.973548	1.000000	0.986597
19	0.985879	0.972534	1.000000	0.986076
21	0.976085	0.957384	0.996529	0.976564
23	0.976085	0.957384	0.996529	0.976564
25	0.970838	0.951165	0.992641	0.971460
27	0.970838	0.951165	0.992641	0.971460
45	0.970838	0.951165	0.992641	0.971460
46	0.970838	0.951165	0.992641	0.971460



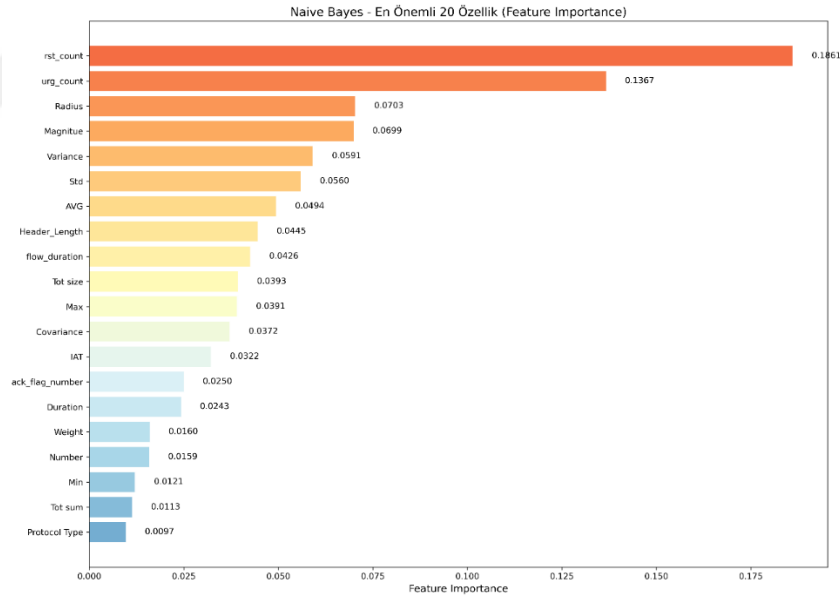
Şekil 4.7. NB modelinin özellik sayısına göre performans değişimi

Şekil 4.7, NB modelinin RO tabanlı özellik seçimine göre doğruluk ve F1 skoru performansını göstermektedir. Başlangıçta düşük kalan performans, 5. özelliikle birlikte %95.88'e yükselmiş; ancak 12. özelliğe kadar tekrar düşüş göstermiştir. 13. özelliikten sonra artan başarı, 13–20 aralığında en yüksek seviyelere ulaşmış; 21. özelliikten sonra ise azalarak 24. özelliikten itibaren yaklaşık %97 düzeyinde sabitlenmiştir. Bu nedenle, en iyi sonuçlar için 13–20 aralığı yeterli görülürken, düşük maliyetli uygulamalar için 5 özellikli yapı da yeterli olabilir.



Şekil 4.8. NB modelinin iki sınıflı karmaşıklık matrisi (15 Özellik)

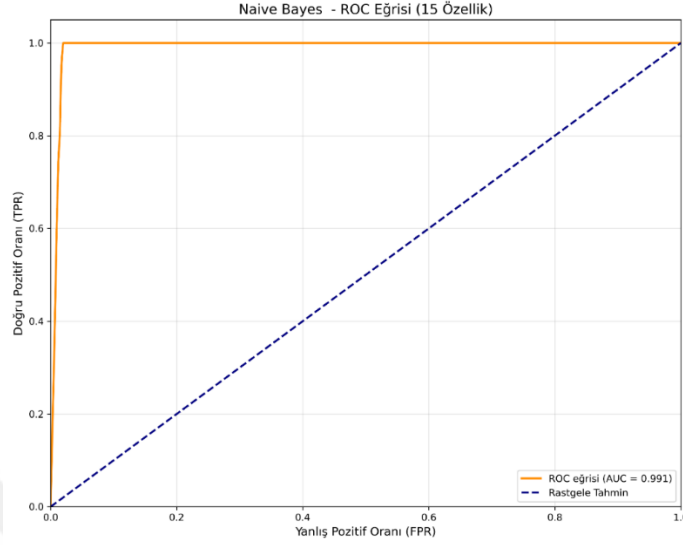
Şekil 4.8, IoT ağ trafiği verilerinin "Attack" ve "Normal" olarak sınıflandırılmasında kullanılan 15 özellikli bir NB modelinin karmaşıklık matrisini göstermektedir.



Şekil 4.9. En etkili 20 özelliğin RO ile belirlenen önem dereceleri

Şekil 4.9’da IoT ağ trafiğini “Normal” ve “Attack” olarak ayırt etmede kullanılan özelliklerin önem düzeyleri RO algoritmasıyla belirlenmiştir. En yüksek öneme sahip rst_count (0.1861) özelliğini sırasıyla urg_count (0.1367) ve Radius (0.0703) takip etmektedir. Ayrıca Magnitude, Variance ve Std gibi özellikler de sınıflandırmada anlamlı katkı sağlamaktadır. Bu bulgular, saldırı tespitinde hangi özniteliklerin daha belirleyici

olduğunu ortaya koymakta ve güvenlik sistemlerinde öncelikli değerlendirilmesi gereken kriterleri göstermektedir.



Şekil 4.10. NB sınıflandırma algoritmasına ait ROC eğrisi

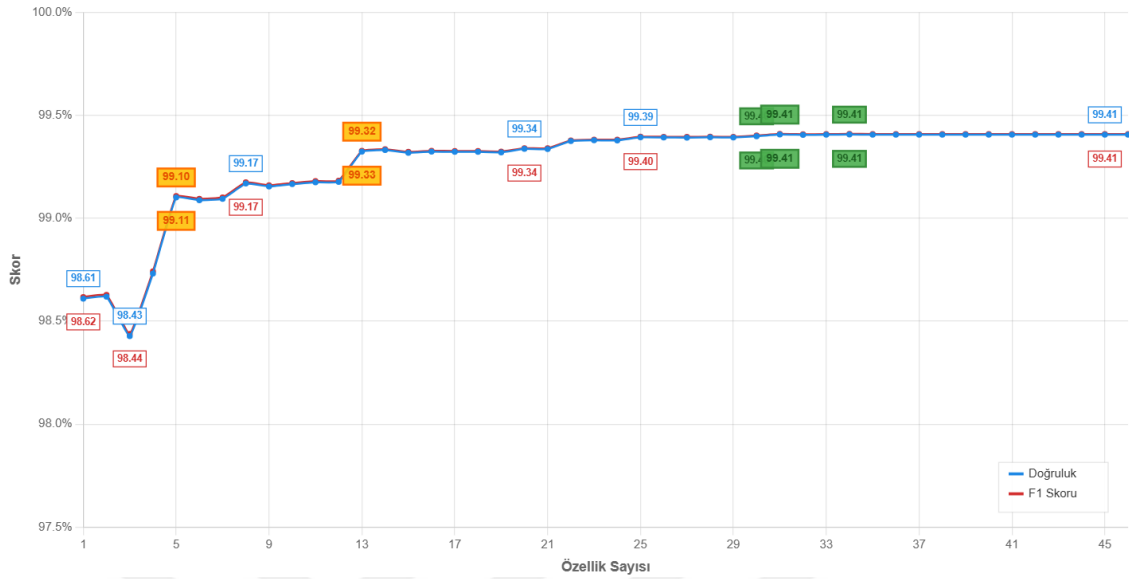
Şekil 4.10, 15 özellik kullanılarak oluşturulan NB modeline ait ROC eğrisi, modelin yüksek doğrulukta sınıflandırma yaptığını göstermektedir. AUC değerinin 0.991 olması, modelin hem saldırı tespiti başarısının yüksek olduğunu hem de düşük yanlış alarm oranına sahip olduğunu ortaya koymaktadır. Eğrinin sol üst köşeye yakın seyretmesi ve rastgele tahmin eğrisinden belirgin şekilde ayrılması, modelin IoT ağlarındaki saldırıları farklı eşik değerlerinde dahi etkili biçimde ayırt edebildiğini kanıtlamaktadır.

4.2.1.3. K En Yakın Komşu (KEYK) algoritması sonuçları

Bu çalışmada, KEYK algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Şekil 4.11, KEYK modelinin RO tabanlı özellik seçimine göre doğruluk ve F1 skoru performansını göstermektedir. Model, başlangıçta %98.61 doğrulukla çalışırken, 3. özellikte %98.43'e gerilemiş; ardından kademeli bir artış göstermiştir. 5. özellikle birlikte doğruluk %99.10 seviyesine ulaşmış, 13. özellikte %99.32'ye yükselmiştir. En yüksek değer olan %99.41 doğruluk ve F1 skoru, 31. özellikte elde edilmiş ve bu değer 32. özellikten itibaren sabit kalmıştır. Bu nedenle, maliyet-performans dengesi

gözetildiğinde, 13–15 aralığındaki özellik sayısı model için optimal olarak değerlendirilebilir.

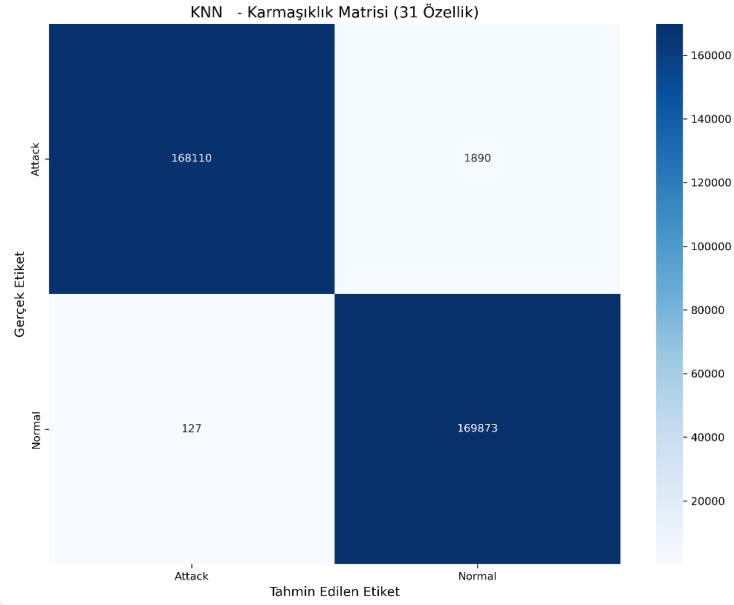


Şekil 4.11. KEYK modelinin özellik sayısına göre performans değişimi

Çizelge 4.5'te KEYK modelinin farklı özellik sayılarındaki performans metrikleri gösterilmektedir. En yüksek değer 31. özelliğe (%99.41 doğruluk, %99.41 F1 skoru) elde edilmiştir. Model çoğunlukla $k=5$ değeriyle optimal performans göstermiş, sadece 3. ve 17. özelliklerde sırasıyla $k=17$ ve $k=7$ değerleri daha etkili olmuştur. Genel olarak performans özellik sayısı arttıkça yükselmiş ve 31. özellikten sonra sabitlenmiştir.

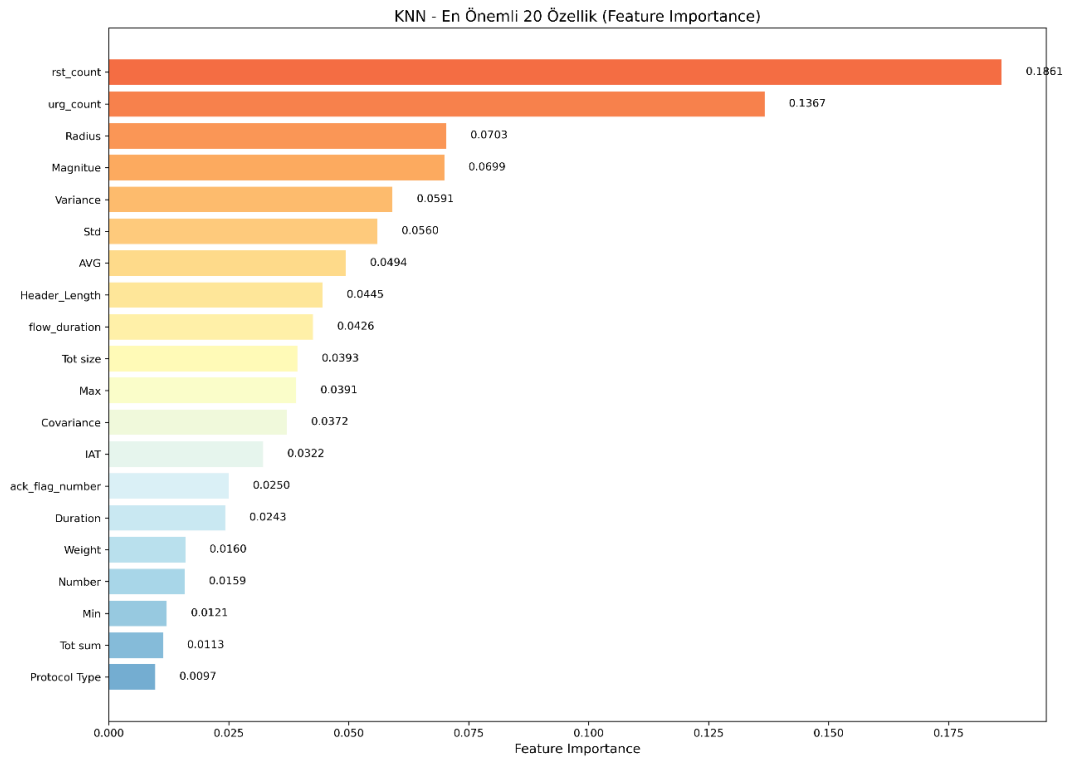
Çizelge 4.5. KEYK için performans metrikleri

Özellik Sayısı	En İyi k	Doğruluk	Kesinlik	Duyarlılık	F1 Skoru
1	5	0.986100	0.980722	0.991694	0.986177
2	5	0.986194	0.980167	0.992471	0.986280
3	17	0.984282	0.978195	0.990647	0.984382
4	11	0.987321	0.979516	0.995459	0.987423
5	5	0.991015	0.983543	0.998741	0.991084
6	5	0.990874	0.983353	0.998653	0.990944
10	5	0.991656	0.985107	0.998406	0.991712
15	7	0.993182	0.987397	0.999118	0.993223
16	5	0.993241	0.987676	0.998947	0.993280
17	7	0.993226	0.987454	0.999147	0.993266
18	5	0.993224	0.987653	0.998935	0.993262
19	5	0.993203	0.987658	0.998888	0.993241
20	5	0.993368	0.987991	0.998876	0.993404
25	5	0.99392	0.98879	0.99918	0.99396
31	5	0.99406	0.98899	0.99925	0.99409
40	5	0.99405	0.98902	0.99920	0.99408
46	5	0.99405	0.98902	0.99920	0.99408



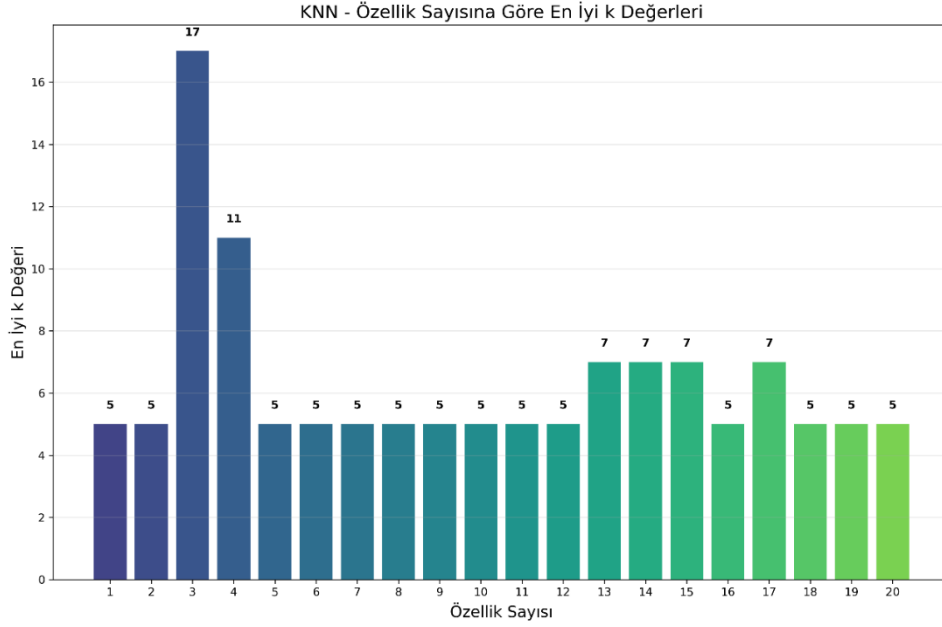
Şekil 4.12. KEYK modelinin iki sınıflı karmaşıklık matrisi (31 Özellik)

Şekil 4.12, 31 özellekle eğitilen KEYK modeline ait karmaşıklık matrisini göstermektedir. Model, saldırı verilerini %98,9, normal trafiği ise %99,9 doğrulukla ayırt edebilmiştir. Toplam 340.000 örnek üzerinden elde edilen bu sonuçlar, KNN modelinin ikili sınıflandırma görevinde yüksek doğruluk ve güvenilirlik sunduğunu ortaya koymaktadır.



Şekil 4.13. En etkili 20 özelliğin RO ile belirlenen önem dereceleri

Şekil 4.13, IoT ağ trafiğini "Normal" ve "Attack" olarak sınıflandırmada kullanılan KEYK modelindeki özelliklerin önem derecelerini, RO algoritmasıyla hesaplayarak göstermektedir. Özellikle rst_count (0.1861) en belirgin öneme sahip olup, ağ trafiği sınıflandırmasında en güçlü belirleyici olarak öne çıkmaktadır. Bu özelliği sırasıyla urg_count (0.1367), Radius (0.0703) ve Magnitue (0.0699) takip etmektedir. Grafik, diğer özelliklerin göreceli önemini de açıkça ortaya koymakta ve böylece IoT güvenlik sistemlerinde hangi özelliklerin öncelikli olarak değerlendirilmesi gerektiğini vurgulamaktadır.

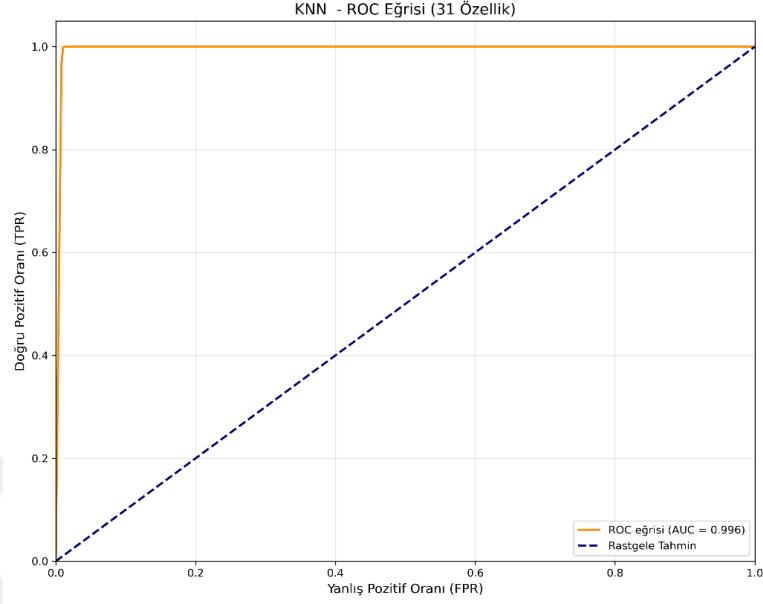


Şekil 4.14. KEYK modelinde özellik sayısına göre en iyi K değerleri

Şekil 4.14, KEYK algoritmasında kullanılan özellik sayısına göre en uygun k değerlerini göstermektedir. Genel olarak k=5 değeri en iyi sonuçları verirken, az sayıda özellikle (3 ve 4) daha yüksek k değerleri (k=17, k=11) tercih edilmiştir. Ayrıca, 13–15 özellik aralığında k=7 optimum sonuç sağlamıştır. Bu durum, KEYK modelinde k değerinin, özellik sayısına bağlı olarak değiştiğini ve düşük boyutlu modellerde daha yüksek k değerlerinin avantaj sağladığını göstermektedir.

Şekil 4.15'te yer alan ROC eğrisi, 31 özellikli KEYK modelinin ikili sınıflandırma görevinde oldukça başarılı bir performans sergilediğini göstermektedir. ROC eğrisinin sol üst köşeye çok yakın seyretmesi ve AUC değerinin 0.996 gibi yüksek bir seviyede olması, modelin düşük yanlış pozitif oranlarında bile yüksek doğru pozitif oranlarına ulaştığını ve saldırıları yüksek doğrulukla tespit edebildiğini göstermektedir. Rastgele

tahmin eğrisinden belirgin şekilde ayrılan bu eğri, KEYK modelinin ağ trafiğindeki saldırıları etkili bir şekilde ayırt etme yeteneğini ortaya koymaktadır.



Şekil 4.15. KEYK sınıflandırma algoritmasına ait ROC eğrisi (31 Özellik)

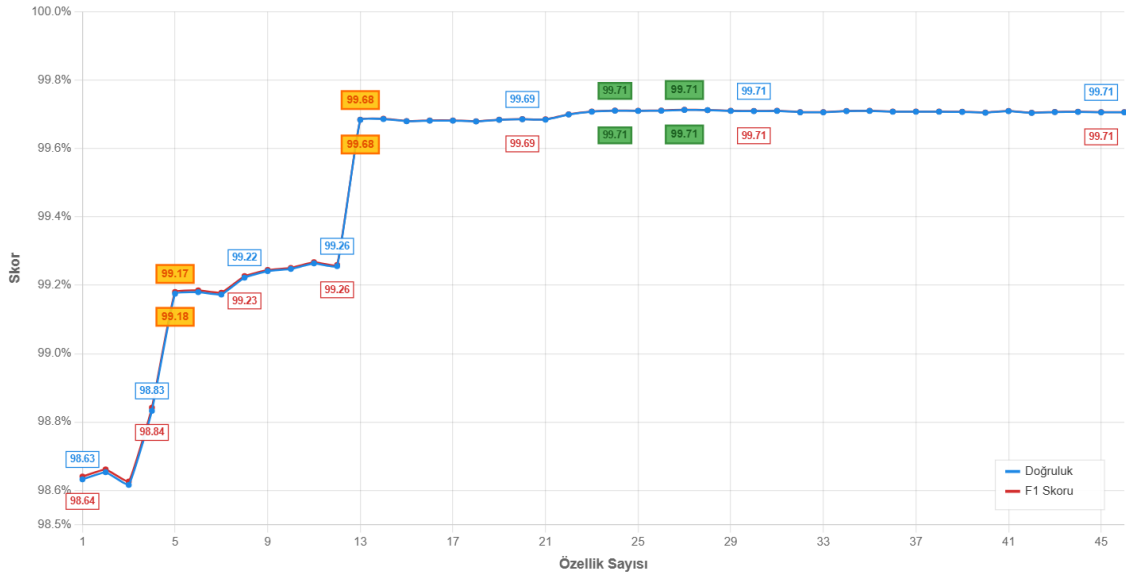
4.2.1.4. Karar Ağacı (KA) algoritması sonuçları

Bu çalışmada, KA algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.6, KA modelinin özellik sayısına göre performans ve karmaşıklık değişimini göstermektedir.

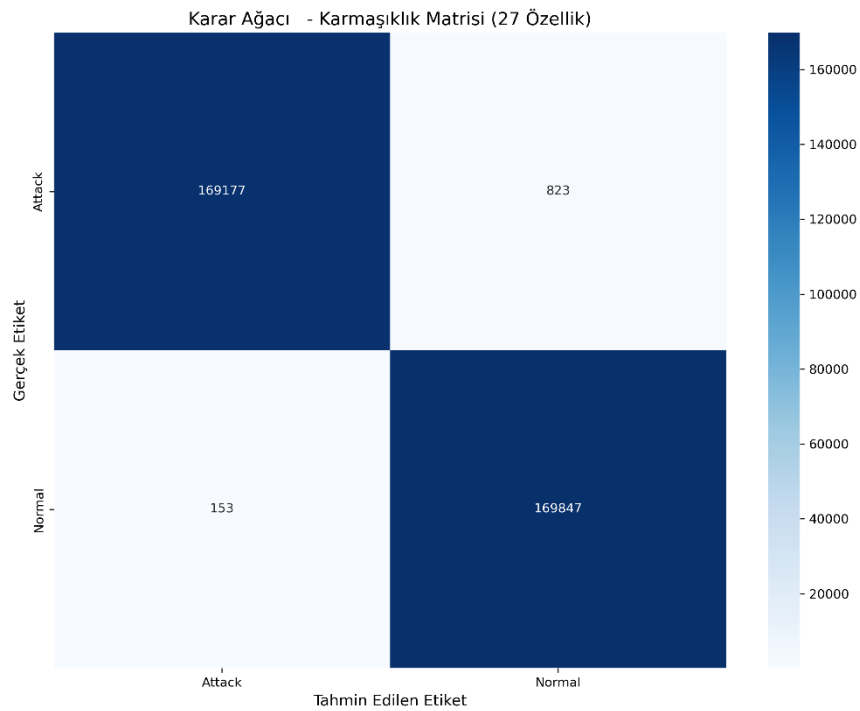
Çizelge 4.6. KA için performans metrikleri

Özellik Sayısı	Ağaç Derinliği	Düğüm Sayısı	Doğruluk	Kesinlik	Duyarlılık	F1 Skoru	Criterion
1	112	16687	0.9863	0.9807	0.9923	0.9864	entropy
2	15	3447	0.9865	0.9897	0.9923	0.9866	gini
5	15	2991	0.9918	0.9557	0.9981	0.9918	gini
10	15	3426	0.9909	0.988	0.9973	0.9911	entropy
14	15	1033	0.9969	0.9947	0.9991	0.9969	entropy
15	15	963	0.9964	0.9948	0.9989	0.9968	entropy
20	15	1097	0.9969	0.9948	0.999	0.9969	entropy
25	15	1097	0.9971	0.9951	0.9991	0.9971	entropy
27	15	1109	0.9971	0.9952	0.9991	0.9971	entropy
30	15	1087	0.9971	0.9952	0.9992	0.9971	entropy
35	15	1021	0.9972	0.9951	0.999	0.9972	entropy
40	15	1017	0.997	0.9951	0.999	0.9971	entropy
46	15	955	0.9971	0.9951	0.999	0.9971	entropy



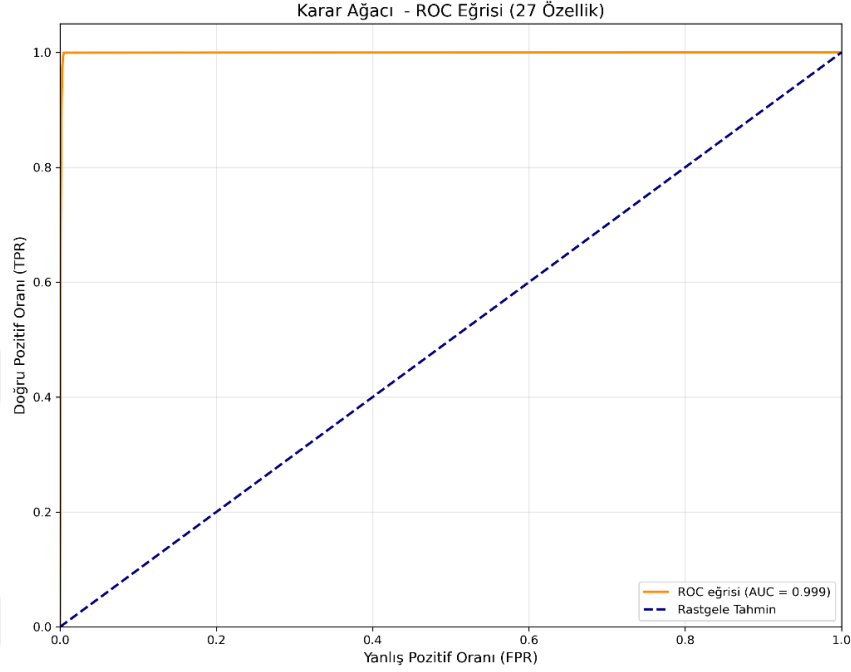
Şekil 4.16. KA modelinin özellik sayısına göre performans değişimi

Şekil 4.16, KA modelinin RO tabanlı özellik seçimine göre doğruluk ve F1 skoru performansını göstermektedir. Model, başlangıçta %98.63 doğruluk ve %98.64 F1 skoru ile başlamış; 5. özelliğe bu değerler %99.12 ve %99.18'e yükselmiştir. 13. özelliğe doğruluk %99.26, F1 skoru ise %99.26 olarak hesaplanmıştır. En yüksek performans ise %99.71 doğruluk ve F1 skoru ile 27. özelliğe elde edilmiş; bu seviye 28. özelliğe itibaren korunmuştur. Maliyet-fayda dengesi dikkate alındığında, 13–15 aralığındaki özellik sayısı model için optimal bir seçim olarak değerlendirilebilir.



Şekil 4.17. KA modelinin iki sınıflı karmaşıklık matrisi (27 Özellik)

Şekil 4.17, 27 özellekle eğitilen Karar Ağacı (KA) modeline ait karmaşıklık matrisini göstermektedir. Model, saldırı verilerini %99,5; normal trafiği ise %99,9 doğrulukla sınıflandırmıştır. Toplam 340.000 veri üzerinden elde edilen sonuçlarla modelin genel doğruluk oranı %99,7'ye ulaşmış, bu da KA modelinin IoT ağlarında etkili ve güvenilir bir sınıflandırma performansı sunduğunu göstermektedir.



Şekil 4.18. KA sınıflandırma algoritmasına ait ROC eğrisi (27 Özellik)

Şekil 4.18'de gösterilen ROC eğrisi, 27 özellekle eğitilen KA modelinin ikili sınıflandırma görevinde neredeyse mükemmel bir performans sergilediğini ortaya koymaktadır. Eğrinin sol üst köşeye çok yakın ilerlemesi ve eğri altındaki alanın (AUC) 0.999 gibi yüksek bir değere ulaşması, modelin düşük yanlış pozitif oranlarında bile yüksek doğru pozitif oranı sağladığını ve saldırıları büyük bir isabetle tespit edebildiğini göstermektedir. ROC eğrisinin rastgele tahmin çizgisinden belirgin biçimde ayrılması ise modelin güçlü ayırt etme yeteneğine sahip olduğunu açıkça ortaya koymaktadır.

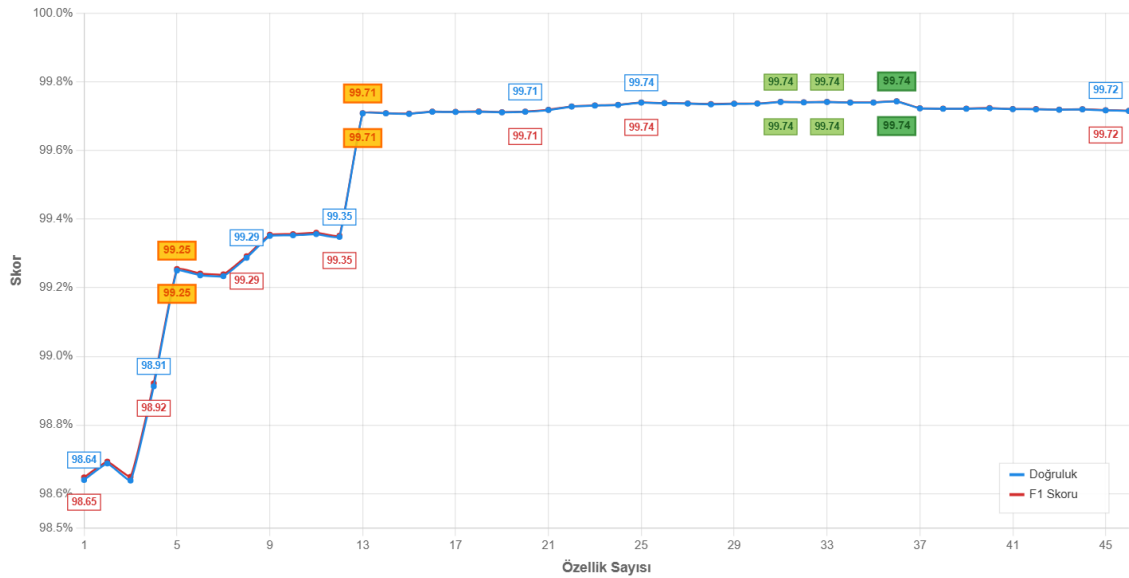
4.2.1.5. Rastgele Orman (RO) algoritması sonuçları

Bu çalışmada, RO algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.7, RO modelinin özellik sayısına göre performans değişimini göstermektedir.

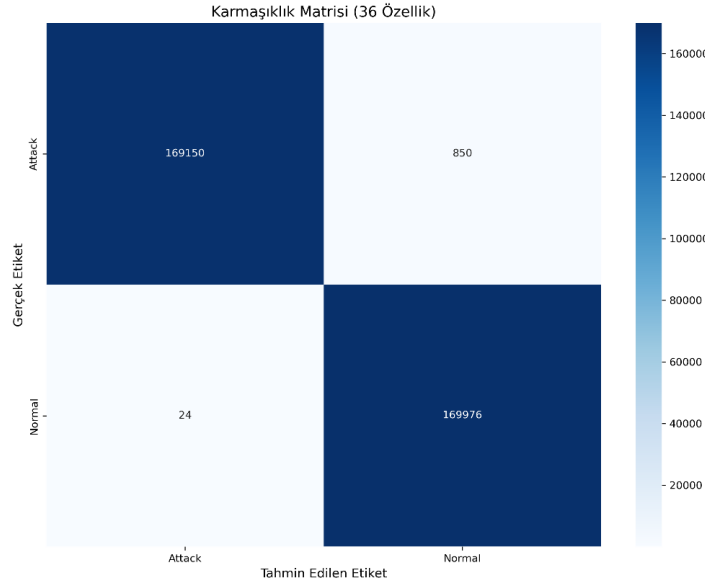
Çizelge 4.7. RO için performans metrikleri

Özellik Sayısı	Doğruluk	Kesinlik	Duyarlılık	F1 Skoru
1	0.986400	0.980912	0.992106	0.986477
3	0.986379	0.978335	0.994788	0.986493
5	0.992500	0.986191	0.998988	0.992548
10	0.993526	0.987881	0.999312	0.993564
15	0.997065	0.994430	0.999729	0.997073
18	0.997129	0.994465	0.999824	0.997137
20	0.997124	0.994471	0.999806	0.997131
25	0.997391	0.994931	0.999876	0.997398
30	0.997362	0.994867	0.999882	0.997368
35	0.997394	0.994960	0.999853	0.997401
36	0.997429	0.995024	0.999859	0.997436
40	0.997226	0.994570	0.999912	0.997234
45	0.997168	0.994448	0.999918	0.997175
46	0.997150	0.994407	0.999924	0.997158



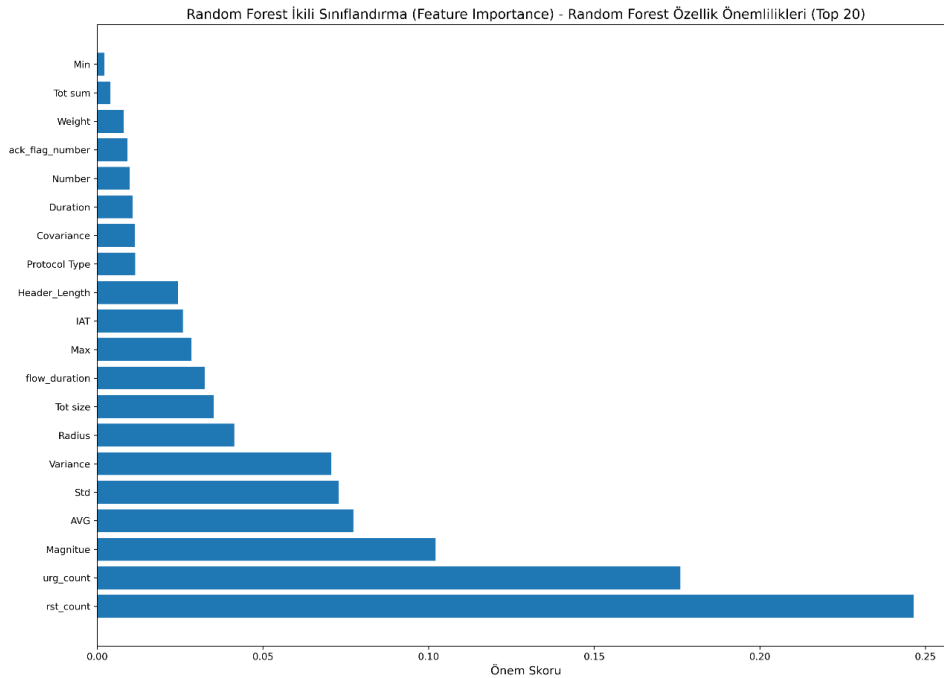
Şekil 4.19. RO modelinin özellik sayısına göre performans değişimi

Şekil 4.19, RO modelinin RO tabanlı özellik seçimine göre doğruluk ve F1 skoru performansını göstermektedir. Model, başlangıçta %98.64 doğruluk ve %98.65 F1 skoru ile başlamış; 5. özellikte bu değerler %99.25'e yükselmiştir. 13. özellikte doğruluk %99.71, F1 skoru ise %99.71 olarak gerçekleşmiştir. En yüksek performans ise %99.74 doğruluk ve %99.74 F1 skoru ile 36. özellikte elde edilmiştir. Ancak 13. özellikten sonra artışın sınırlı olduğu dikkate alındığında, maliyet-fayda açısından 13–15 arası özellik kullanımı model için en uygun aralık olarak değerlendirilebilir.



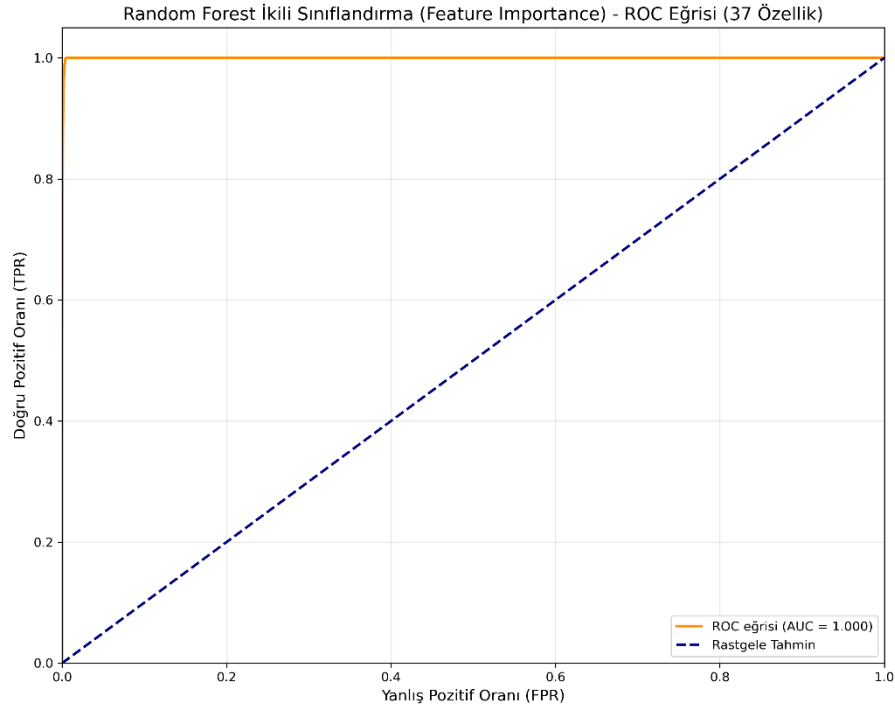
Şekil 4.20. RO modelinin iki sınıflı karmaşıklık matrisi (36 Özellik)

Şekil 4.20’de sunulan karmaşıklık matrisi, 36 özellik kullanılarak eğitilen bir modelin IoT ağ trafiğini "Attack" ve "Normal" olarak yüksek doğrulukla sınıflandırdığını göstermektedir. Modelin saldırı tespit oranı yaklaşık %99.5, normal trafik tespit oranı ise %99.99 seviyesindedir. 340.000 veri üzerinden elde edilen bu sonuçlarla birlikte genel doğruluk oranı %99.7 olarak hesaplanmıştır. Özellikle düşük yanlış alarm sayısı (24 yanlış pozitif) ve sınırlı sayıdaki kaçırılan saldırı (850 yanlış negatif), modelin siber güvenlik alanında güvenilir ve etkili bir sınıflandırma aracı olduğunu göstermektedir.



Şekil 4.21. RO ikili sınıflandırma modelinde özellik önem sıralaması (İlk 20 özellik)

Şekil 4.21, IoT ağ trafiğinin normal ve saldırı olarak sınıflandırılmasında etkin olan özelliklerin önem derecelerini göstermektedir. RO algoritmasıyla belirlenen sıralamada, rst_count parametresi 0.25 değeriyle en kritik belirleyici konumundadır. Bunu 0.17 civarında önem skoruyla urg_count ve 0.10 civarında değerlerle Magnitude, AVG ve Std takip etmektedir. Grafikte açıkça görüldüğü üzere, ilk iki özelliğin toplam katkısı diğer özelliklerin toplamına yakındır, bu da saldırı tespitinde az sayıda belirleyici parametreyle etkili bir sınıflandırma yapılabileceğini göstermektedir.



Şekil 4.22. RO sınıflandırma algoritmasına ait ROC eğrisi

Şekil 4.22’de gösterilen ROC eğrisi, 37 özellik kullanılarak eğitilen RO modelinin ikili sınıflandırma görevinde neredeyse mükemmel bir performans sergilediğini ortaya koymaktadır. ROC eğrisinin sol üst köşeye çok yakın ilerlemesi ve AUC değerinin 1.000 olması, modelin saldırı tespitinde maksimum doğruluk ve sıfıra yakın yanlış alarm oranı sağladığını göstermektedir. Eğrinin rastgele tahmin çizgisinden net şekilde ayrılması, modelin ayırt etme gücünün son derece yüksek olduğunu kanıtlamaktadır. Bu sonuçlar, RO algoritmasının ve kullanılan özellik seçiminin IoT güvenliği açısından oldukça etkili olduğunu göstermektedir.

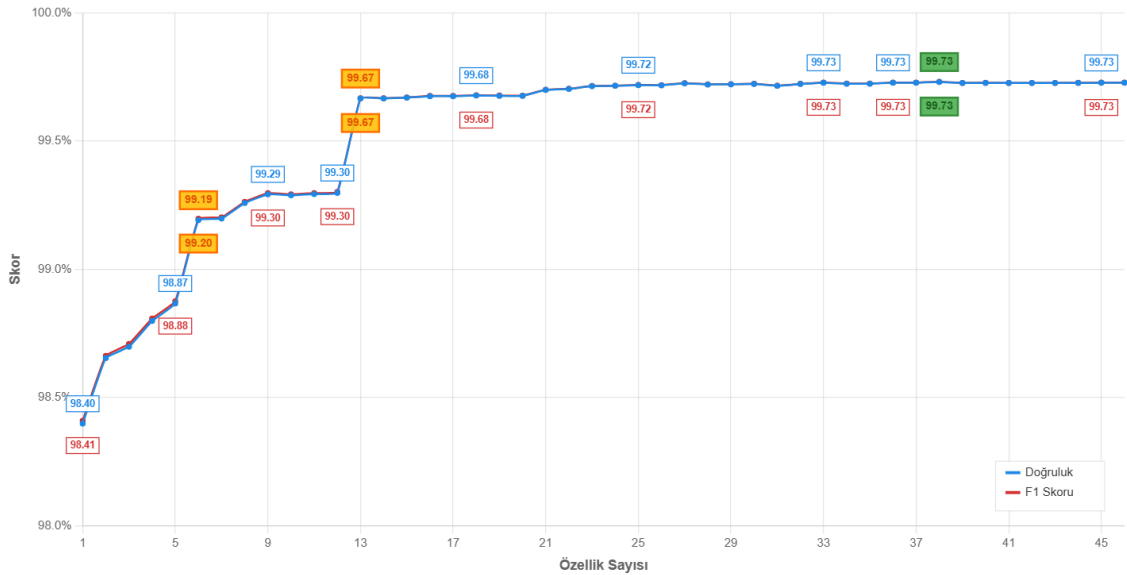
4.2.1.6. Gradyan Artırma (GA) algoritması sonuçları

Bu çalışmada, GA algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.8'de GA modelinin farklı özellik sayılarındaki performans metrikleri gösterilmektedir. En yüksek değerler 38. özellikte (%99.73 doğruluk, %99.73 F1 skoru) elde edilmiştir.

Çizelge 4.8. GA için performans metrikleri

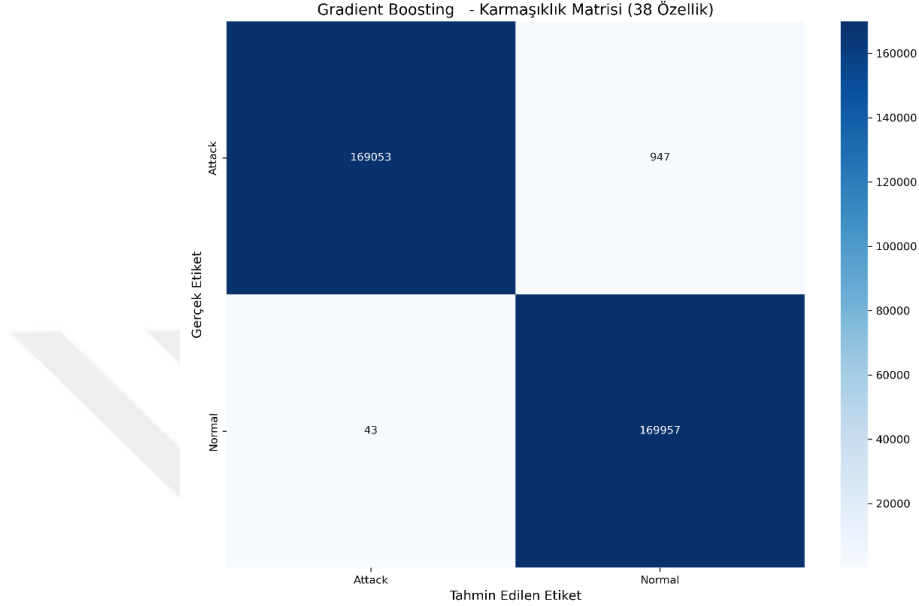
Özellik Sayısı	Doğruluk	F1 Skoru	Ağaç Sayısı	max_depth
1	0.98398	0.98409	200	5
5	0.98867	0.98875	200	5
10	0.99288	0.99292	200	5
15	0.99669	0.99670	200	5
18	0.99677	0.99678	200	5
20	0.99676	0.99677	200	5
25	0.99719	0.99719	200	5
30	0.99723	0.99723	200	5
38	0.99730	0.99731	200	5
40	0.99728	0.99727	200	5
46	0.99727	0.99728	200	5



Şekil 4.23. GA modelinin özellik sayısına göre performans değişimi

Şekil 4.23, GA modelinin RO tabanlı özellik seçimine göre doğruluk ve F1 skoru performansını göstermektedir. Model, başlangıçta %98.40 doğruluk ve %98.41 F1 skoru ile nispeten düşük bir performans sergilemiş; 6. özellikte bu değerler %99.19 ve

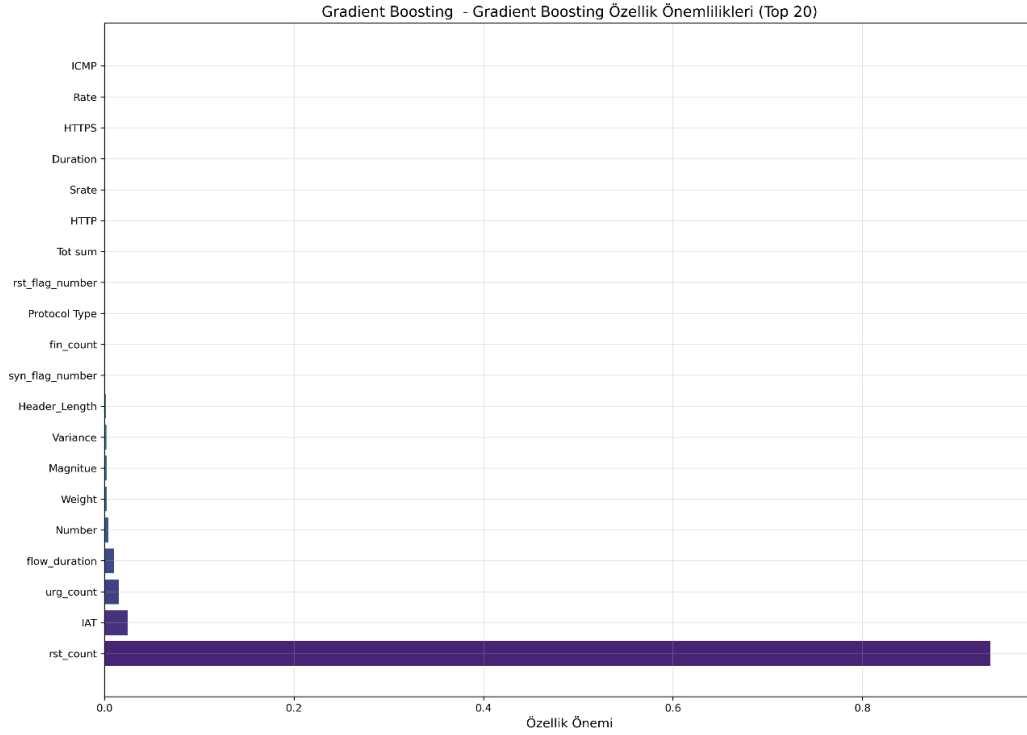
%99.20'ye yükselmiştir. 13. özellikten itibaren belirgin bir sıçrama gözlemlenmiş, doğruluk ve F1 skoru 38. özellikte %99.73'e ulaşarak en yüksek seviyeye erişmiştir. Ancak 13. özellikten sonra artış oldukça sınırlı kaldığından, maliyet-fayda dengesi açısından 13–15 arası özellik sayısı model için en uygun aralık olarak değerlendirilebilir.



Şekil 4.24. GA modelinin iki sınıflı karmaşıklık matrisi (38 Özellik)

Şekil 4.24'te sunulan karmaşıklık matrisi, 38 özellik kullanılarak eğitilen GA modelinin hem normal trafiği hem de saldırı verilerini yüksek doğrulukla sınıflandırabildiğini göstermektedir. Modelin saldırı tespit oranı yaklaşık %99.4, normal trafik tespit oranı ise %99.97 düzeyindedir. Genel doğruluk oranı %99.7 seviyesinde olup, düşük yanlış negatif sayısı sayesinde modelin özellikle saldırı tespitinde güvenilir ve etkili bir performans sergilediği görülmektedir. Bu sonuçlar, GA algoritmasının IoT güvenliği açısından güçlü bir sınıflandırma yöntemi olduğunu ortaya koymaktadır.

Şekil 4.25, GA modeline göre en etkili 20 özelliği göstermektedir. Grafikte, rst_count özelliği açık ara en yüksek öneme sahiptir ve modelin kararlarında belirleyici rol oynamaktadır. Diğer özellikler, özellikle IAT ve flow_duration, daha düşük önemlilik düzeyine sahiptir. Bu durum, RST bayraklı paketlerin IoT ağlarında saldırı tespiti açısından kritik bir gösterge olduğunu ve modelin büyük ölçüde bu özelliğe dayandığını ortaya koymaktadır.



Şekil 4.25. GA modelinde en önemli 20 özelliğin katkı oranları

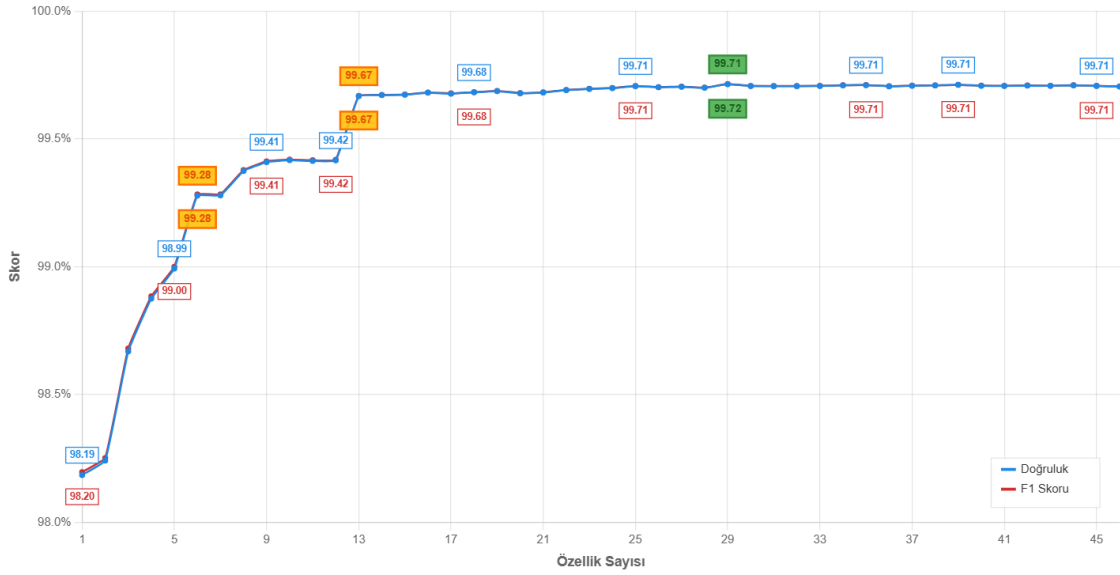
4.2.1.7. Aşırı Gradyan Artırma (AGA) algoritması sonuçları

Bu çalışmada, AGA algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.9, AGA modelinin farklı sayıda özellikle elde ettiği performans metriklerini karşılaştırmaktadır.

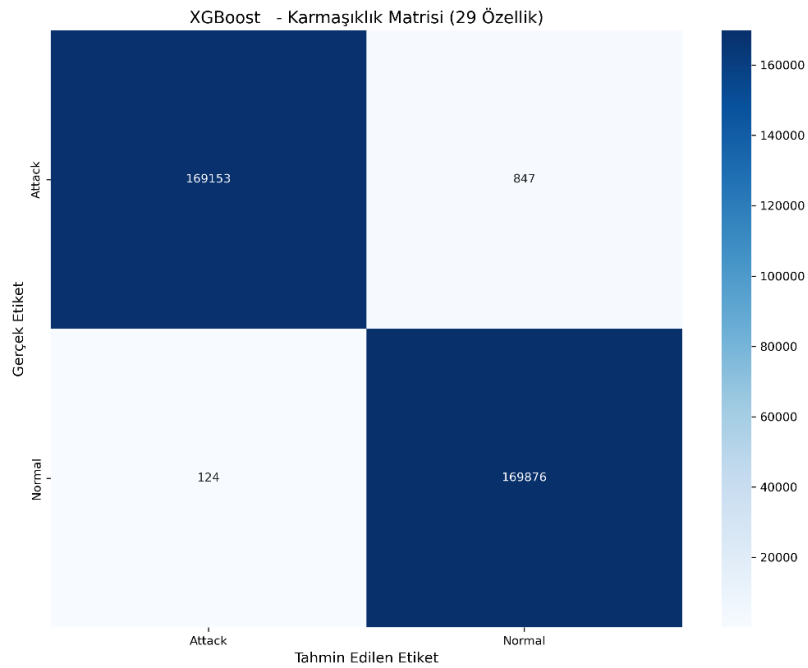
Çizelge 4.9. AGA modeli için performans metrikleri

Özellik Sayısı	Doğruluk	Kesinlik	Duyarlılık	F1 Skoru	Ağaç Sayısı
1	0.98185	0.97573	0.98828	0.98196	50
5	0.98992	0.98289	0.99721	0.99000	200
10	0.99416	0.98921	0.99922	0.99419	200
15	0.99673	0.99425	0.99924	0.99674	200
19	0.99687	0.99443	0.99934	0.99688	200
25	0.99706	0.99491	0.99924	0.99707	200
29	0.99714	0.99503	0.99927	0.99715	200
30	0.99707	0.99485	0.99931	0.99707	200
35	0.99710	0.99500	0.99923	0.99711	200
39	0.99711	0.99497	0.99928	0.99712	200
46	0.99705	0.99479	0.99932	0.99705	200



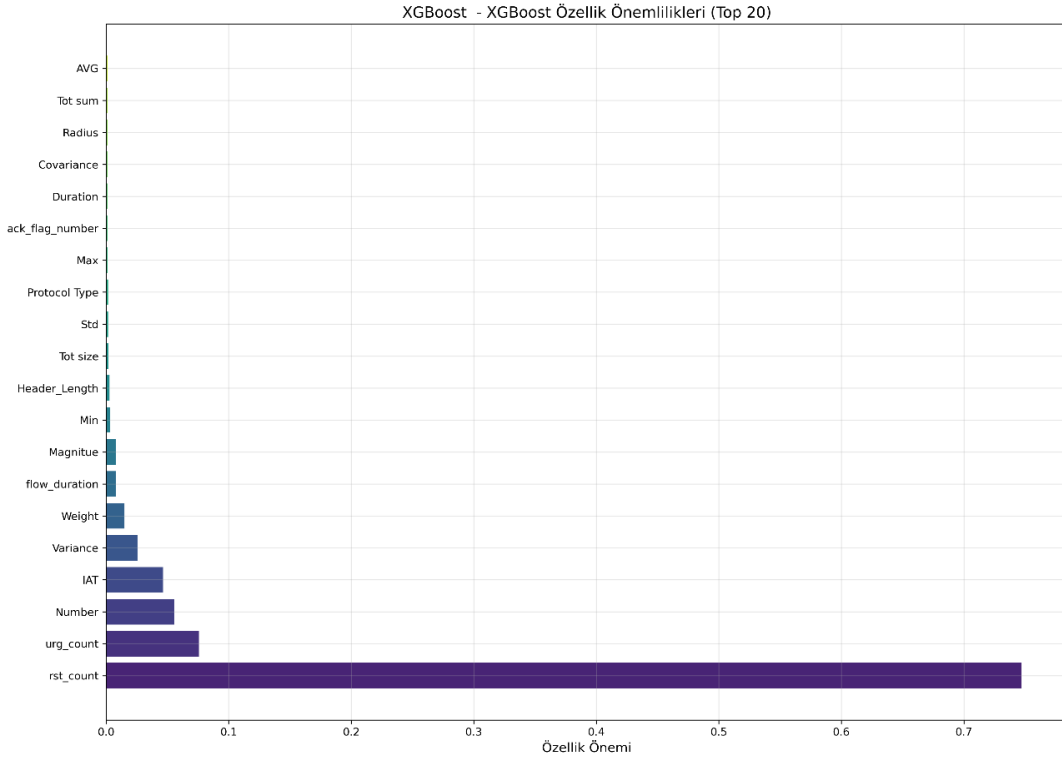
Şekil 4.26. AGA modelinin özellik sayısına göre performans değişimi

Şekil 4.26, AGA modelinin RO tabanlı özellik seçimine göre doğruluk ve F1 skoru performansını göstermektedir. Model, başlangıçta %98.19 doğruluk ve %98.20 F1 skoru ile düşük bir performans sergilemiş; 6. özellikte bu değerler %99.28 ve %99.28 seviyesine yükselmiştir. 13. özellik itibarıyla belirgin bir sıçrama görülmüş; doğruluk %99.67, F1 skoru ise %99.67'ye ulaşmıştır. En yüksek performans, %99.71 doğruluk ve %99.72 F1 skoru ile 29. özellikte elde edilmiştir. Ancak 13. özellikten sonraki artışlar oldukça sınırlı kaldığından, maliyet-fayda açısından 13–15 özellik aralığı model için en uygun seçim olarak değerlendirilebilir.



Şekil 4.27. AGA modelinin iki sınıflı karmaşıklık matrisi (29 Özellik)

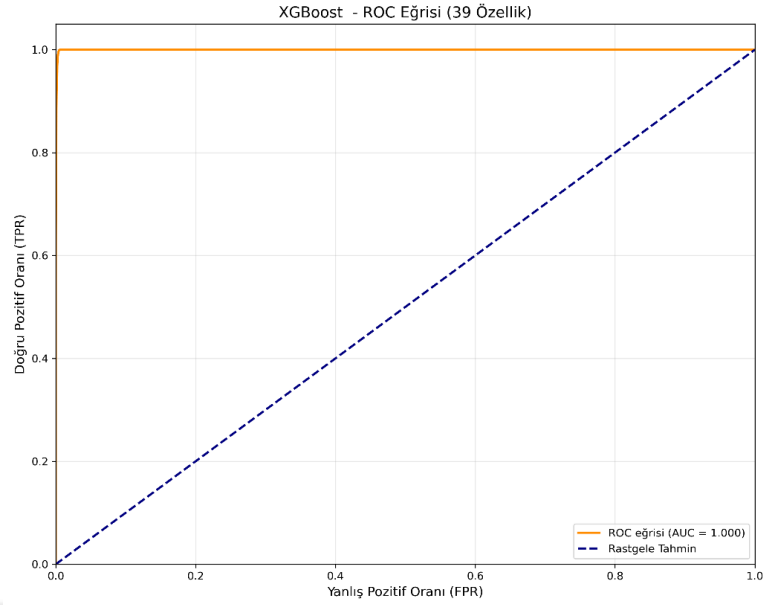
Şekil 4.27, 29 özelliikle eğitilen AGA modeline ait karmaşıklık matrisini göstermektedir. Model, saldırı trafiğini %99,5; normal trafiği ise %99,93 doğrulukla sınıflandırmış ve genel doğruluk oranı %99,7'ye ulaşmıştır. Düşük yanlış pozitif (124) ve yanlış negatif (847) değerleri, AGA algoritmasının özellikle saldırı tespitinde güvenilir ve etkili bir performans sunduğunu ortaya koymaktadır.



Şekil 4.28. AGA modelinde en önemli 20 özelliğin katkı oranları

Şekil 4.28, AGA modelinde kullanılan en önemli 20 özelliğin katkı düzeyini göstermektedir. Özellikle `rst_count`, modelin tahminlerinde belirleyici rol oynarken; `urg_count`, `number` ve `IAT` gibi ağ trafiğiyle ilişkili özellikler onu takip etmektedir. Diğer özelliklerin katkısı ise oldukça sınırlıdır. Bu durum, az sayıda etkili özellikle yüksek doğruluk elde edilebileceğini ve kaynak verimliliğinin artırılabilirliğini göstermektedir.

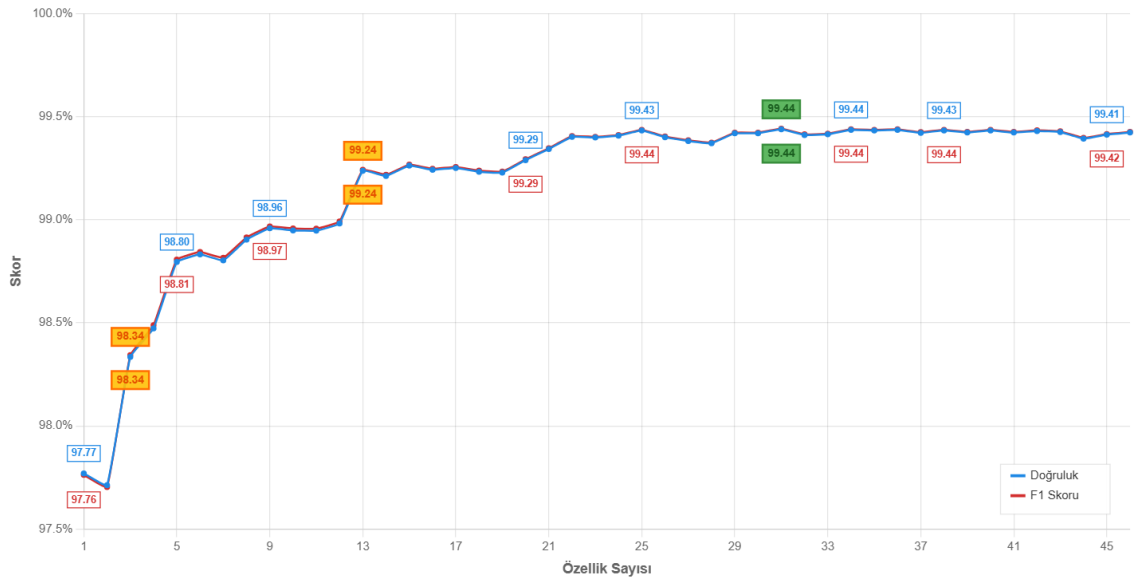
Şekil 4.29, 39 özelliikle eğitilen AGA modeline ait ROC eğrisini göstermektedir. AUC değerinin 1.000 olarak hesaplanması, modelin pozitif ve negatif sınıfları neredeyse kusursuz şekilde ayırt ettiğini göstermektedir. Eğrinin sol üst köşeye yakın seyretmesi ve rastgele tahmin çizgisinden tamamen ayrılması, modelin üstün ayırt etme yeteneğini ortaya koymaktadır.



Şekil 4.29. AGA sınıflandırma algoritmasına ait ROC eğrisi

4.2.1.8. Yapay sinir ağları (YSA) algoritması sonuçları

Bu çalışmada, YSA algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.



Şekil 4.30. YSA modelinin özellik sayısına göre performans değişimi

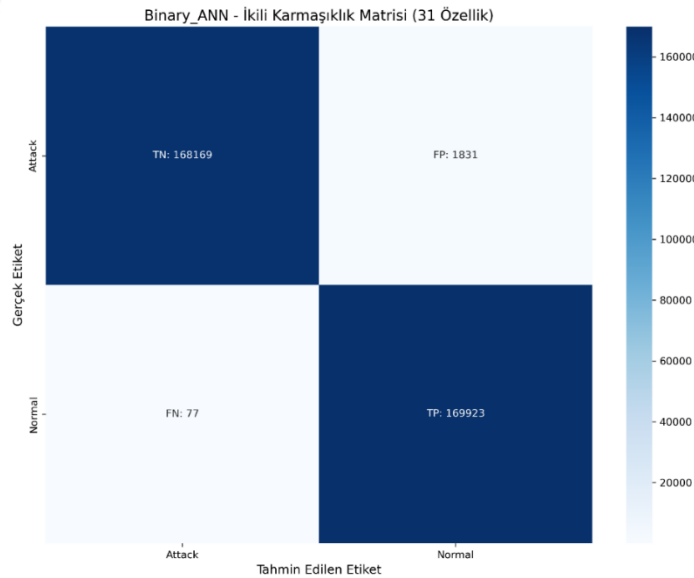
Şekil 4.30, YSA modelinin RO tabanlı özellik seçimine göre doğruluk ve F1 skoru performansını göstermektedir. Model, başlangıçta %97.77 doğruluk ve %97.76 F1 skoru

ile düşük bir başlangıç sergilemiş; 12. özelliğe kadar kademeli bir artışla %98.98 doğruluk ve %98.99 F1 skoruna ulaşmıştır. 13. özellikte birlikte %99.24 seviyesine sıçrama gözlemlenmiş ve bu artış devam ederek, 31. özellikte %99.44 doğruluk ve F1 skoru ile en yüksek değerlere ulaşılmıştır. Bu noktadan sonra ise performans küçük dalgalanmalar göstermektedir. Maliyet-fayda açısından değerlendirildiğinde, 15–20 arası özellik sayısı model için optimal aralık olarak öne çıkmaktadır.

Çizelge 4.10, YSA modelinin farklı sayıda özellikte elde ettiği performans metriklerini karşılaştırmaktadır.

Çizelge 4.10. YSA için performans metrikleri

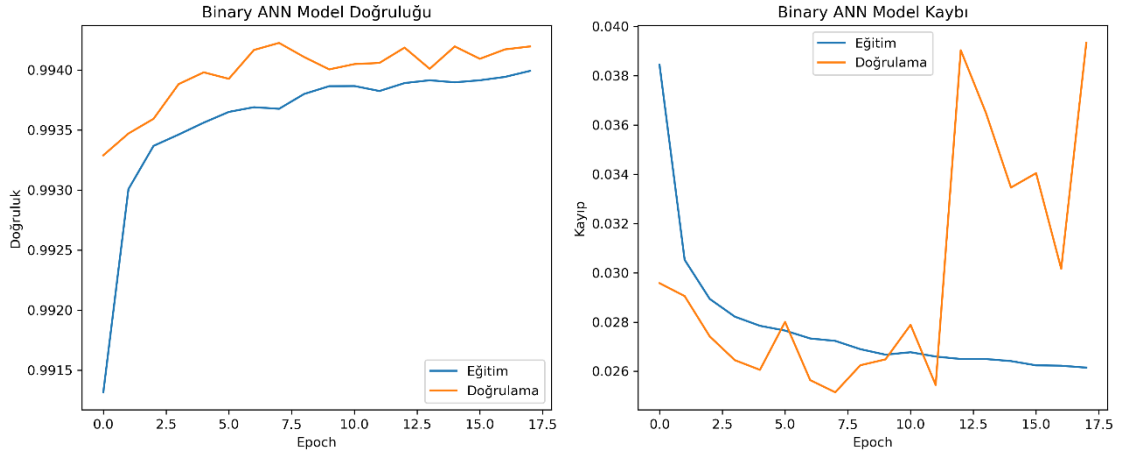
Özellik Sayısı	Doğruluk	Kesinlik	Duyarlılık	F1 Skoru
1	0.977700	0.980800	0.974476	0.977628
4	0.984732	0.975104	0.994865	0.984885
10	0.989485	0.980955	0.998353	0.989578
15	0.992626	0.986545	0.998876	0.992672
20	0.992891	0.987021	0.998918	0.992934
31	0.994388	0.989339	0.999547	0.994417
40	0.994326	0.988968	0.999806	0.994357
46	0.994232	0.988966	0.999618	0.994263



Şekil 4.31. YSA modelinin iki sınıflı karmaşıklık matrisi (31 Özellik)

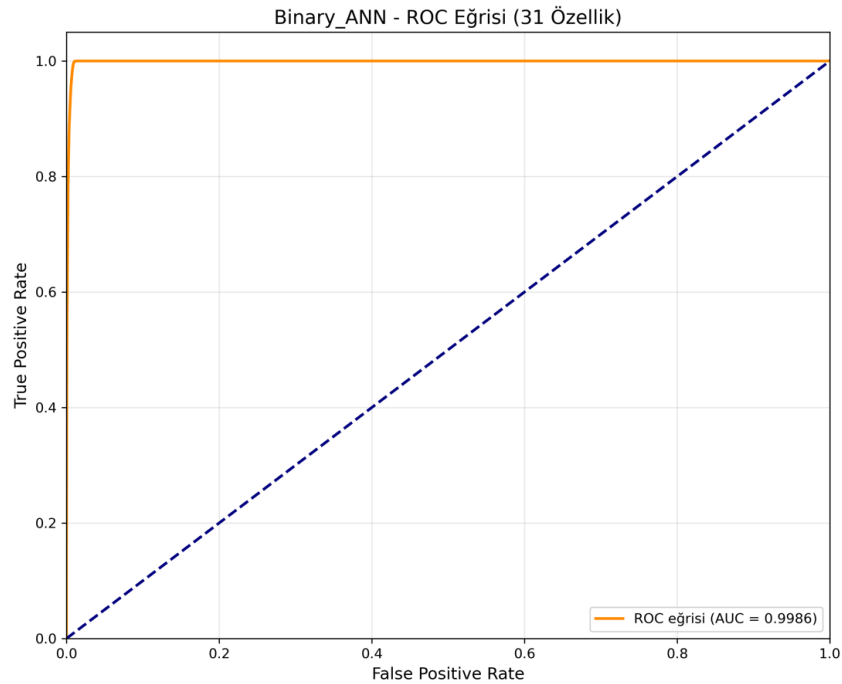
Şekil 4.31, YSA modeli ile oluşturulan karmaşıklık matrisi, ağ trafiğini "Attack" (saldırı) ve "Normal" olarak sınıflandırmakta ve toplamda yaklaşık 340,000 veri örneğini değerlendirmektedir. Model, saldırıların 168,169'unu ve normal trafiğin 169,923'ünü doğru tespit etmiştir. Sadece 1,831 saldırıyı normal, 77 normal trafiği ise saldırı olarak

yanlış sınıflandırmıştır. Bu sonuçlar, modelin yüksek doğruluk oranıyla çalıştığını ve ağ güvenliği açısından saldırı tespitinde oldukça başarılı olduğunu göstermektedir.



Şekil 4.32. YSA modelinin eğitim süreci: doğruluk ve kayıp grafikleri (31 özellik)

Şekil 4.32’de YSA modelinin eğitim süreci iki grafikte gösterilmiştir: eğitim ve doğrulama doğruluğu epoch sayısı arttıkça genel olarak yükselmekte ve yaklaşık 2.5 epoch sonrası artış yavaşlamaktadır; doğrulama doğruluğu eğitim doğruluğundan daha yüksek fakat daha dalgalıdır. Eğitim kaybı epoch sayısı ile sürekli azalırken, doğrulama kaybı 10-12 epoch arasında en düşük seviyeye ulaşmakta ve sonrasında ani dalgalanmalar göstermektedir; bu durum, 12. epochtan sonra aşırı öğrenmenin (overfitting) başladığını işaret etmekte ve eğitimin bu noktada durdurulmasının ideal olduğunu göstermektedir.



Şekil 4.33. YSA sınıflandırma algoritmasına ait ROC eğrisi

Şekil 4.33, 31 özellik kullanılarak eğitilen YSA modelinin ROC eğrisini göstermektedir. ROC eğrisi, modelin farklı eşiklerdeki doğruluk ve hata oranlarını karşılaştırarak genel sınıflandırma başarısını ortaya koyar. AUC değerinin 0.9986 gibi 1'e oldukça yakın olması, modelin neredeyse kusursuz bir ayırım gücüne sahip olduğunu göstermektedir. ROC eğrisinin formu, modelin çok düşük yanlış pozitif oranıyla yüksek doğrulukta pozitif sınıfları ayırt edebildiğini göstermekte olup, bu da modelin "Normal" ve "Attack" sınıflarını son derece etkili şekilde ayırt ettiğini ortaya koymaktadır.

4.2.1.9. Evrişimsel Sinir Ağları (ESA) algoritması sonuçları

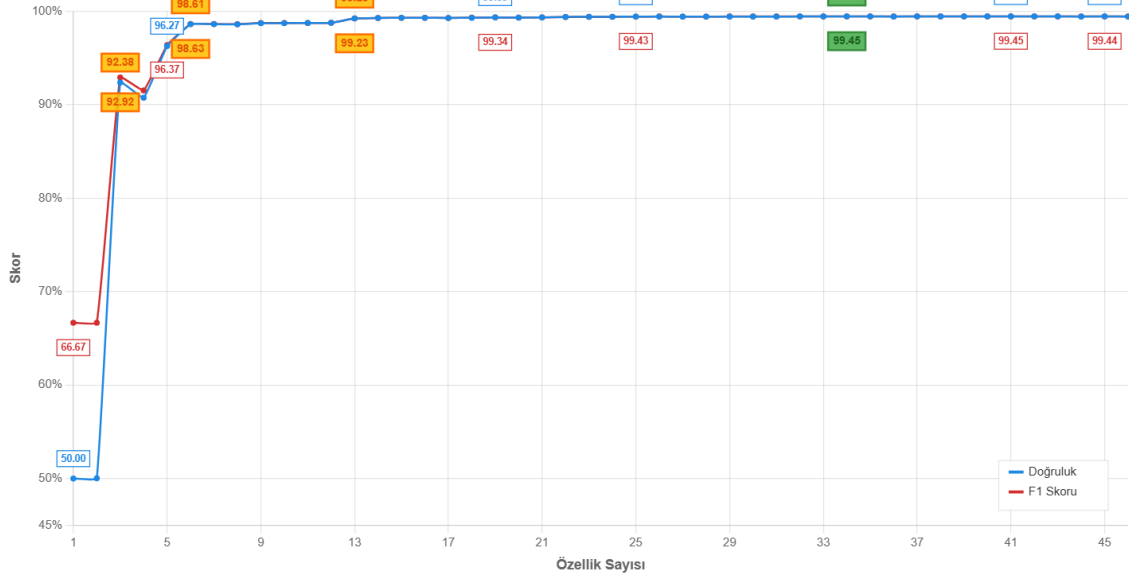
Bu çalışmada, ESA algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.11'de ESA modelinin farklı özellik sayılarındaki performans metrikleri gösterilmektedir. En yüksek değerler 34. özellikte (%99.45 doğruluk, %99.45 F1 skoru) elde edilmiştir.

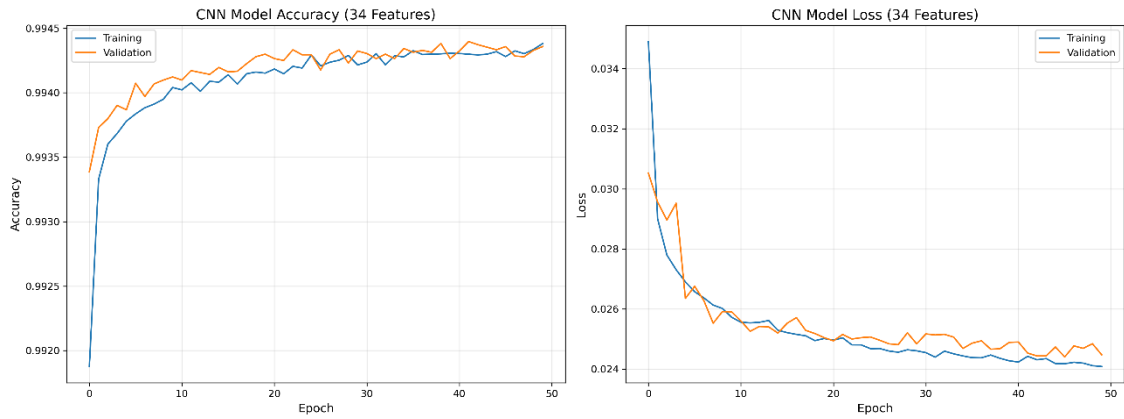
Çizelge 4.11. ESA için performans metrikleri

Özellik Sayısı	Doğruluk	Kesinlik	Duyarlılık	F1 Skoru
1	0.500000	0.500000	1.000000	0.666667
3	0.923826	0.868181	0.999394	0.929178
6	0.986126	0.974839	0.998018	0.986292
10	0.987329	0.977207	0.997935	0.987462
13	0.992253	0.985355	0.999359	0.992308
19	0.993309	0.987100	0.999682	0.993351
24	0.994056	0.988422	0.999824	0.994090
30	0.994329	0.988934	0.999847	0.994361
34	0.994509	0.989370	0.999759	0.994538
42	0.994397	0.989163	0.999747	0.994427
46	0.994338	0.989111	0.999682	0.994368

Şekil 4.34, ESA modelinin RO tabanlı özellik seçimine göre doğruluk ve F1 skoru performansını göstermektedir. Model, başlangıçta %50.00 doğruluk ve %66.67 F1 skoru ile oldukça düşük bir performans sergilemiş; 3. özellikte %92.38 doğruluk ve %92.92 F1 skoru ile belirgin bir artış göstermiştir. 4. özellikte geçici bir düşüş gözlenmiş; ancak 6. özellikten itibaren kademeli bir yükseliş başlamıştır. 13. özellikte birlikte performans %99.23 seviyesine ulaşmış; en yüksek değerler ise %99.45 doğruluk ve %99.45 F1 skoru ile 34. özellikte elde edilmiştir.



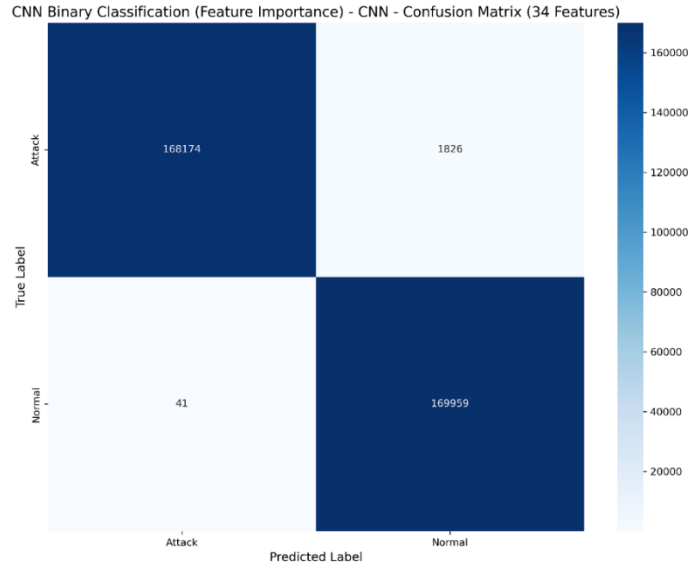
Şekil 4.34. ESA modelinin özellik sayısına göre performans değişimi



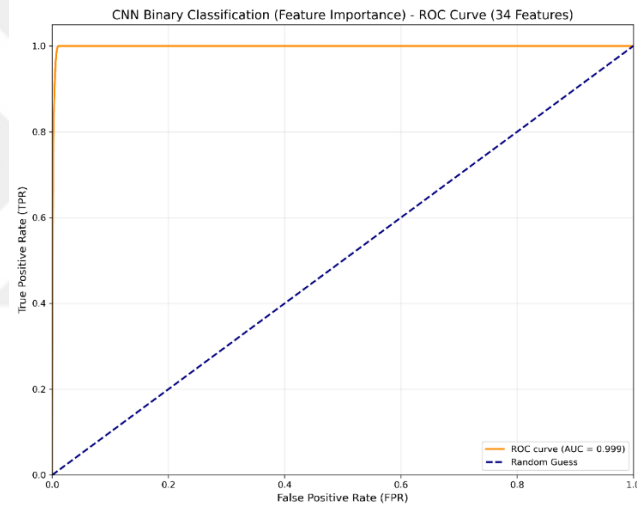
Şekil 4.35. ESA modelinin eğitim süreci: doğruluk ve kayıp grafikleri (34 özellik)

Şekil 4.35'te 34 özellik kullanılarak eğitilen CNN modelinin eğitim sürecine ait doğruluk ve kayıp grafiklerine yer verilmiştir. Grafikler, modelin hem eğitim hem de doğrulama verilerinde istikrarlı bir performans sergilediğini göstermektedir. Doğruluk değerleri zamanla artarak %99.44 seviyesine ulaşmış, kayıp değerleri ise yaklaşık 0.024 civarına kadar düşmüştür. Eğitim ve doğrulama eğrilerinin birbirine oldukça yakın seyretmesi, modelin aşırı öğrenme yapmadığını ve güçlü bir genelleme yeteneğine sahip olduğunu ortaya koymaktadır.

Şekil 4.36'da sunulan karmaşıklık matrisi, 34 özellik ile eğitilen CNN modelinin saldırı ve normal IoT trafiğini yüksek doğrulukla ayırt edebildiğini göstermektedir. Yaklaşık %98.9 saldırı tespiti ve %99.98 normal trafik doğruluğu ile model, ikili sınıflandırmada başarılı ve güvenilir bir performans sergilemiştir.



Şekil 4.36. ESA modelinin iki sınıflı karmaşıklık matrisi (34 Özellik)



Şekil 4.37. ESA sınıflandırma algoritmasına ait ROC eğrisi

Şekil 4.37, 34 özellik kullanan ESA modeline ait ROC eğrisini göstermektedir. Eğrinin sol üst köşeye çok yakın konumlanması ve AUC değerinin 0.999 gibi oldukça yüksek bir seviyede olması, modelin hem yüksek duyarlılığa hem de yüksek özgüllüğe sahip olduğunu göstermektedir. Bu durum, ESA modelinin ikili sınıflandırma görevinde saldırı ve normal trafiği büyük bir doğrulukla ayırt edebildiğini ortaya koymaktadır.

4.2.1.10. Tekrarlayan sinir ağları (TSA) algoritması sonuçları

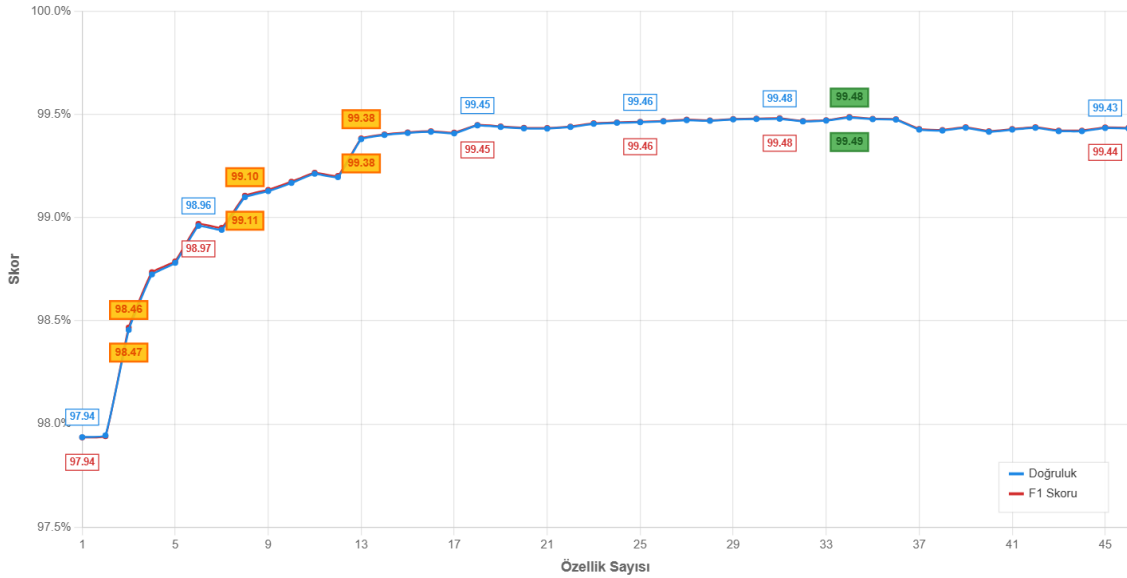
Bu çalışmada, TSA algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki

başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.12'de TSA modelinin farklı özellik sayılarındaki performans metrikleri gösterilmektedir. En yüksek değerler 34. özelliğe (%99.48 doğruluk, %99.49 F1 skoru) elde edilmiştir.

Çizelge 4.12. TSA için performans metrikleri

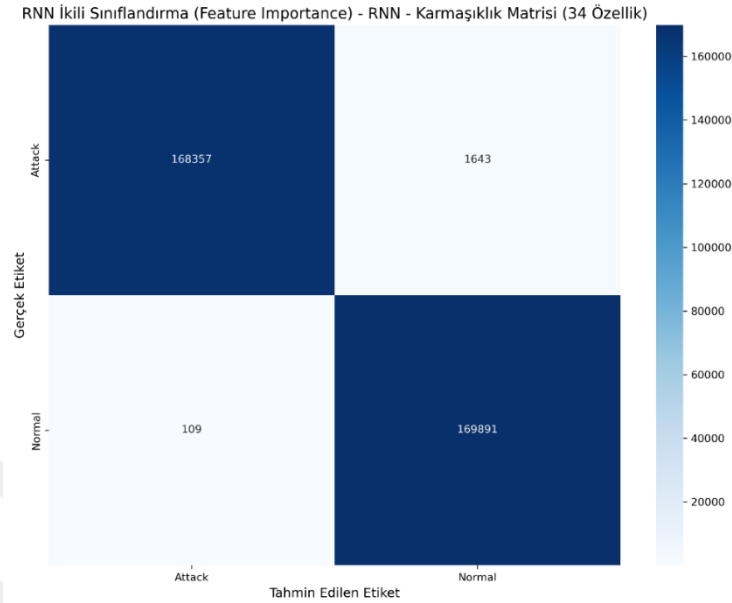
Özellik Sayısı	Doğruluk	Kesinlik	Duyarlılık	F1 Skoru
1	0.979368	0.979975	0.978735	0.979355
3	0.984556	0.977342	0.992112	0.984672
5	0.987806	0.981848	0.993988	0.987881
10	0.991676	0.984708	0.998865	0.991736
15	0.994100	0.989054	0.999259	0.994130
20	0.994318	0.989378	0.999365	0.994346
25	0.994618	0.989846	0.999488	0.994644
30	0.994771	0.990203	0.999429	0.994795
34	0.994847	0.990422	0.999359	0.994870
40	0.994156	0.988822	0.999612	0.994188
46	0.994318	0.989047	0.999706	0.994348



Şekil 4.38. TSA modelinin özellik sayısına göre performans değişimi

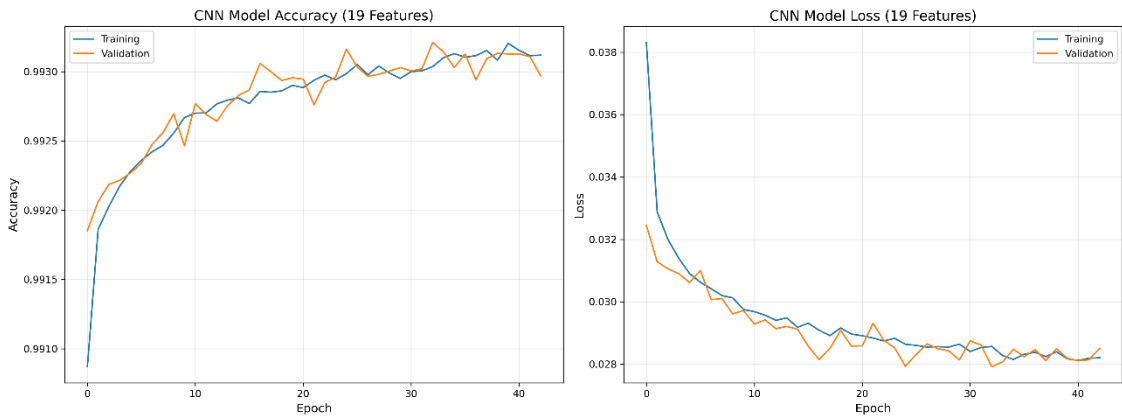
Şekil 4.38, TSA modelinin RO tabanlı özellik seçimine göre doğruluk ve F1 skoru performansını göstermektedir. Model, başlangıçta %97.94 doğruluk ve %97.94 F1 skoru ile başlamış; 3. özelliğe %98.46 doğruluk ve %98.47 F1 skoru ile ilk büyük sıçramayı gerçekleştirmiştir. 13. özellikte birlikte doğruluk %99.38'e, F1 skoru ise %99.38'e ulaşmış; en yüksek performans %99.48 doğruluk ve %99.49 F1 skoru ile 34. özellikte elde edilmiştir. Ancak 13. özellikten sonra artış oranı oldukça sınırlı kaldığı için, maliyet-

fayda dengesi açısından 13–16 özellik aralığı model için en uygun seçenek olarak değerlendirilebilir.



Şekil 4.39. TSA modelinin iki sınıflı karmaşıklık matrisi (15 Özellik)

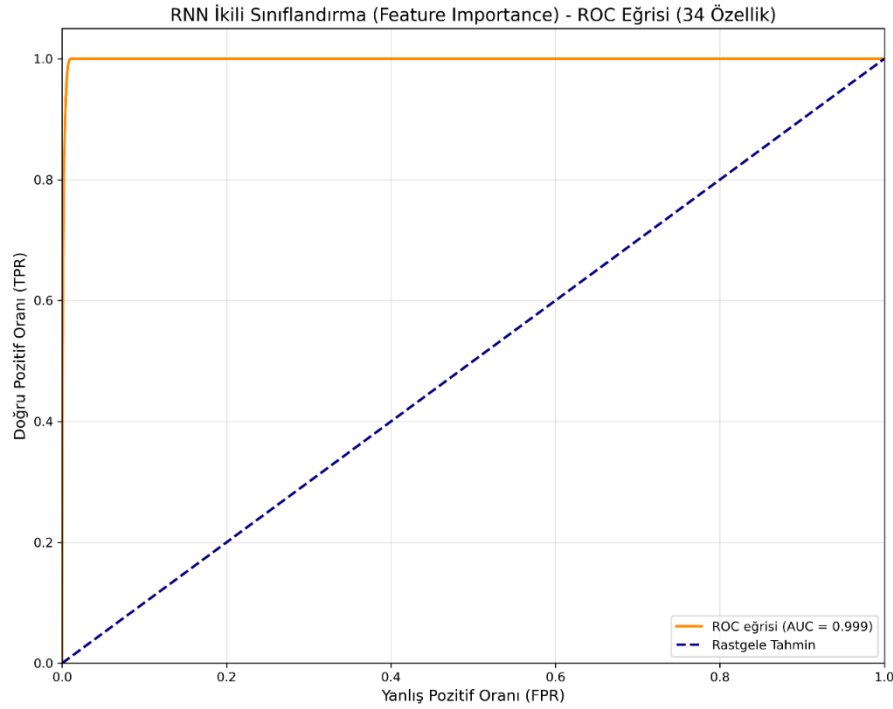
Şekil 4.39’da sunulan karmaşıklık matrisi, 34 özellik kullanılarak eğitilen TSA modelinin ikili sınıflandırma görevinde oldukça başarılı olduğunu göstermektedir. Model, saldırı trafiğinde yaklaşık %98.7, normal trafiğinde ise %99.9 doğruluk oranına ulaşarak düşük yanlış sınıflandırma sayısı ile yüksek güvenilirlik sergilemiştir. Bu sonuç, TSA’nın saldırı tespiti gibi kritik görevlerde etkin bir yöntem olduğunu ortaya koymaktadır.



Şekil 4.40. TSA modelinin eğitim süreci: doğruluk ve kayıp grafikleri (34 özellik)

Şekil 4.40’ta gösterilen grafikler, TSA modelinin 34 özellikle eğitildiği süreçte doğruluk ve kayıp değerlerinin istikrarlı seyrettiğini göstermektedir. Eğitim ve doğrulama

doğruluğu %99.4'ün üzerinde sabitlenirken, kayıp değerleri yaklaşık 0.023 seviyelerine gerileyerek düşük hata ile yüksek performans sergilendiğini ortaya koymuştur. Eğitim ve doğrulama eğrilerinin yakınlığı, modelin aşırı öğrenme yapmadığını ve güçlü bir genelleme yeteneğine sahip olduğunu göstermektedir.



Şekil 4.41. TSA sınıflandırma algoritmasına ait ROC eğrisi (34 özellik)

Şekil 4.41'de gösterilen ROC eğrisi, 34 özellikli TSA modelinin ikili sınıflandırma görevinde üstün performans sergilediğini ortaya koymaktadır. Eğrinin sol üst köşeye yakın ilerlemesi ve AUC değerinin 0.999 gibi çok yüksek bir seviyede olması, modelin hem saldırı hem de normal trafiği yüksek doğrulukla ayırt edebildiğini, dolayısıyla yüksek duyarlılık ve özgüllüğe sahip olduğunu göstermektedir.

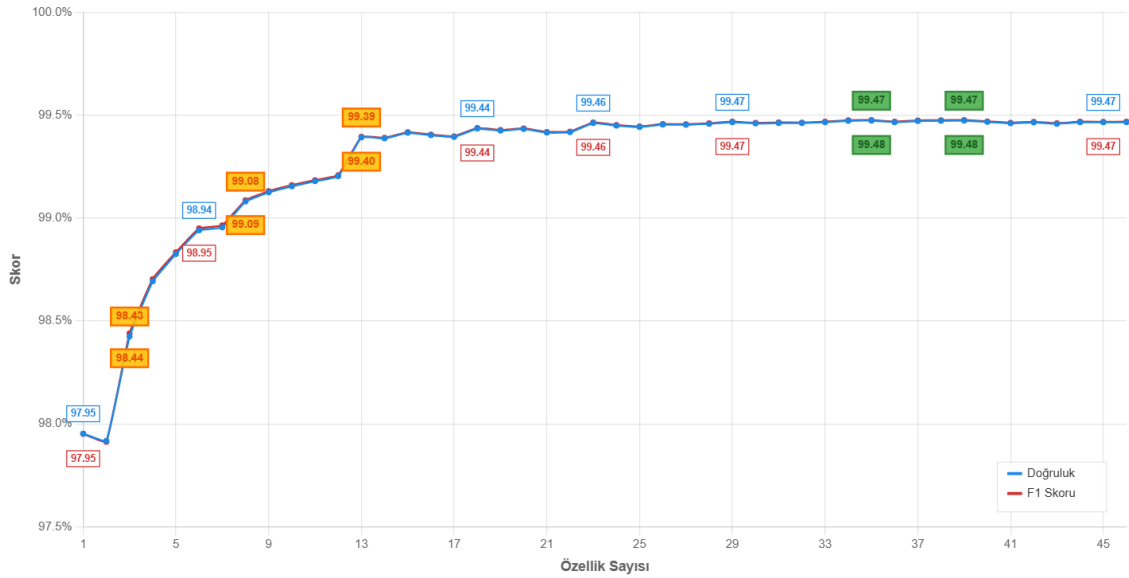
4.2.1.11. Uzun Kısa Süreli Bellek (UKSB) algoritması sonuçları

Bu çalışmada, Uzun Kısa Süreli Bellek (UKSB) algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.13'te UKSB modelinin farklı özellik sayılarındaki performans metrikleri gösterilmektedir. En yüksek değerler 35. ve 39. özelliklerde (%99.47 doğruluk, %99.48 F1 skoru) elde edilmiştir.

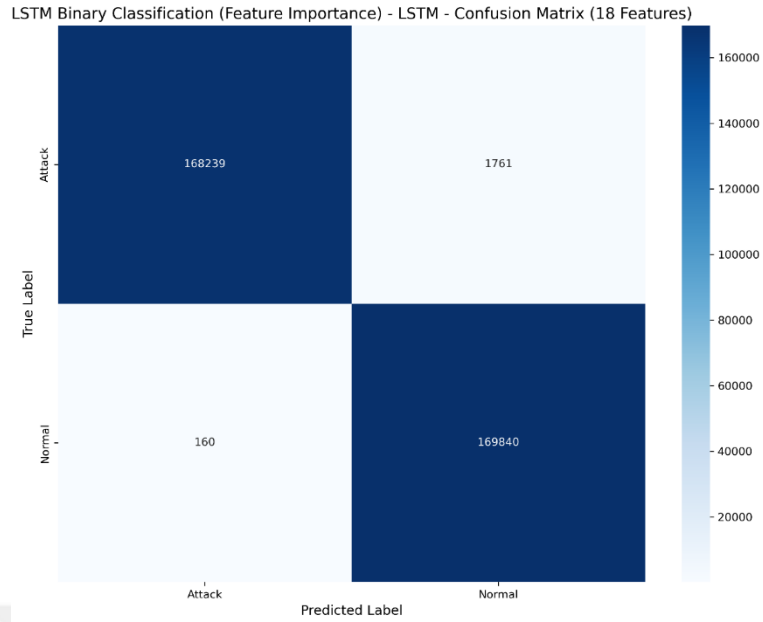
Çizelge 4.13. UKSB için performans metrikleri

Özellik Sayısı	Doğruluk	Kesinlik	Duyarlılık	F1 Skoru
1	0.979526	0.979885	0.979153	0.979519
3	0.984253	0.975191	0.993788	0.984402
5	0.988756	0.981082	0.996712	0.988343
8	0.990806	0.983912	0.997929	0.990871
10	0.991544	0.984743	0.998123	0.991603
13	0.993921	0.988851	0.999106	0.993952
15	0.994144	0.989118	0.999282	0.994174
18	0.994350	0.989738	0.999659	0.994376
20	0.994326	0.989367	0.999394	0.994355
25	0.994426	0.989694	0.999259	0.994453
30	0.994600	0.989692	0.999612	0.994627
35	0.994738	0.990065	0.999506	0.994763
39	0.994738	0.990060	0.999512	0.994763
40	0.994676	0.989899	0.999553	0.994702
45	0.994656	0.989795	0.999618	0.994682
46	0.994659	0.989978	0.999435	0.994684



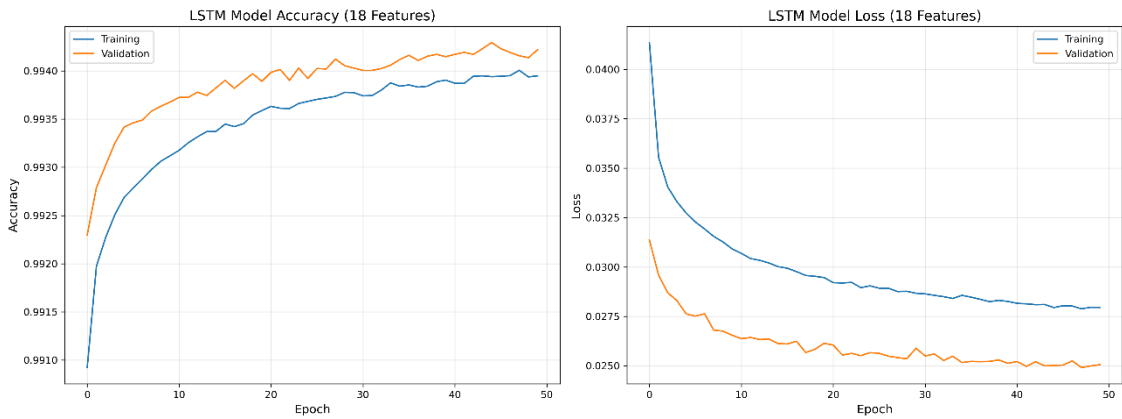
Şekil 4.42. UKSB modelinin özellik sayısına göre performans değişimi

Şekil 4.42, UKSB modelinin RO tabanlı özellik seçimine göre doğruluk ve F1 skoru performansını göstermektedir. Model, başlangıçta %97.95 doğruluk ve %97.95 F1 skoru ile başlamış; 3. özellikte %98.43 doğruluk ve %98.44 F1 skoru ile kayda değer bir artış göstermiştir. Performans, 13. özellikte %99.39 doğruluk ve %99.39 F1 skoru ile önemli bir sıçrama yapmış, en yüksek değerler ise 35–39 özellik aralığında %99.47 doğruluk ve %99.48 F1 skoru ile elde edilmiştir. Ancak 13. özellikten sonra artış %0.08 seviyesinde kaldığından, maliyet-fayda dengesi açısından 13–15 özellik aralığı yeterli görülmektedir.



Şekil 4.43. UKSB modelinin iki sınıflı karmaşıklık matrisi (18 Özellik)

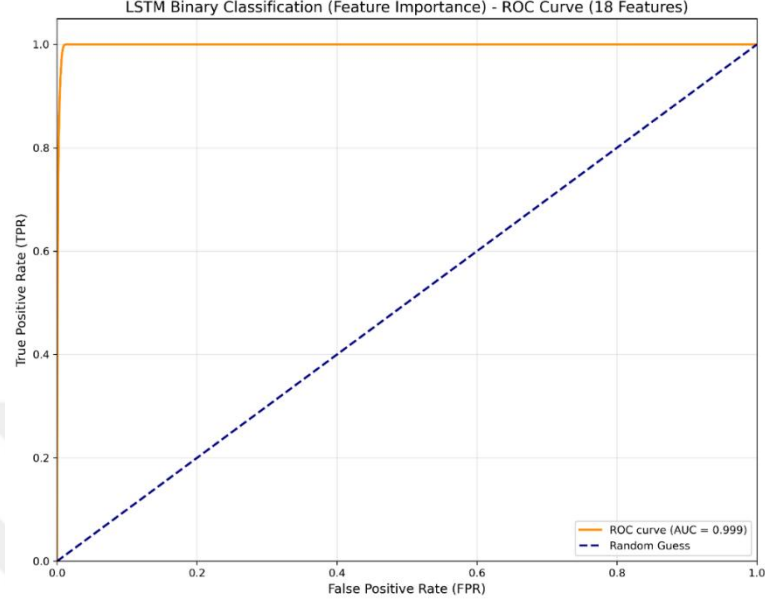
Şekil 4.43, 18 özellik kullanılan UKSB modeline ait karmaşıklık matrisi, modelin ikili sınıflandırma görevinde yüksek doğrulukla çalıştığını göstermektedir. Model, saldırı verilerinin %98,4'ünü ve normal verilerin %99,9'unu doğru şekilde sınıflandırmıştır. Yanlış pozitif ve yanlış negatif sayılarının oldukça düşük olması, modelin hem saldırı hem de normal trafiği etkili şekilde ayırt edebildiğini ve genelleme yeteneğinin güçlü olduğunu ortaya koymaktadır.



Şekil 4.44. UKSB modelinin eğitim süreci: doğruluk ve kayıp grafikleri (18 özellik)

Şekil 4.44, 18 özellikli LSTM modeline ait eğitim süreci grafikleri, modelin doğrulukta istikrarlı bir artış ve kayıpta düzenli bir azalma gösterdiğini ortaya koymaktadır. Doğrulama doğruluğu, eğitim doğruluğundan hafifçe yüksek; doğrulama kaybı ise sürekli olarak daha düşüktür. Bu durum, genellikle eğitimde uygulanan

düzenleştirme tekniklerinden veya eğitim verisinin daha zorlu örnekler içermesinden kaynaklanabilir. Sonuçlar, modelin genelleme yeteneğinin güçlü olduğunu ve doğrulama setinde oldukça başarılı performans sergilediğini göstermektedir.



Şekil 4.45. UKSB sınıflandırma algoritmasına ait ROC eğrisi

Şekil 4.45, 18 özellik kullanan UKSB modeline ait ROC eğrisi, modelin ikili sınıflandırma görevinde neredeyse mükemmel bir performans sergilediğini göstermektedir. Eğrinin sol üst köşeye yakın olması ve AUC değerinin 0.999 gibi çok yüksek bir seviyede bulunması, modelin hem yüksek duyarlılık hem de yüksek özgüllükle çalıştığını ortaya koymaktadır. Bu sonuç, modelin gerçek pozitifleri başarıyla tespit ederken, yanlış pozitif oranını minimumda tuttuğunu ve genel olarak güçlü bir ayırım yeteneğine sahip olduğunu göstermektedir.

4.2.2. Sekizli sınıflandırma sonuçları

Makine öğrenmesi tabanlı ağ trafiği analizi, günümüzde siber güvenlikte büyük bir öneme sahiptir. Özellikle, saldırı tespiti için kullanılan çok sınıflı sınıflandırma algoritmaları, ağ trafiğini BenignTraffic, Mirai Attacks, Brute Force & Exploits, Web Attacks, DDoS Attacks, DoS Attacks, Reconnaissance ve MITM (Man-In-The-Middle) olmak üzere sekiz farklı kategoriye ayırarak daha detaylı ve hassas tespit mekanizmaları sunmaktadır. Bu sayede, her saldırı türü için özelleştirilmiş güvenlik önlemleri alınarak siber tehditlere karşı daha etkin bir savunma sağlanabilir.

Çizelge 4.14'te, sekizli sınıflandırma için kullanılan algoritmaların performansları ve bu algoritmalarla elde edilen özellik seçim sonuçları karşılaştırılmıştır. Elde edilen sonuçlara göre, RO, KA ve GA algoritmaları yüksek doğruluk ve F1 skoru ile öne çıkmaktadır. Özellikle KEYK algoritması yalnızca 2 özellik kullanarak oldukça başarılı bir sonuç vermiştir. Buna karşılık, NB ve LR gibi bazı algoritmaların düşük performans sergilediği görülmektedir. Bu durum hem algoritma seçiminin hem de uygun özellik sayısının model başarısı üzerinde önemli etkileri olduğunu göstermektedir.

Çizelge 4.14. Algoritmaların sekizli sınıflandırma performans karşılaştırması ve özellik seçimi sonuçları

ALGORITMA	ÖZELLİK SAYISI	EN YÜKSEK DOĞRULUK	F1 SKORU
LR	40	0.669106	0.666020
NB	34	0.556682	0.525788
KEYK	2	0.867888	0.866145
KA	37	0.920641	0.920908
RO	26	0.952918	0.952701
GA	36	0.922565	0.922896
AGA	33	0.914994	0.915575
YSA	37	0.783835	0.786597
ESA	8	0.793118	0.793115
TSA	30	0.837594	0.838131
UKSB	42	0.848500	0.848700

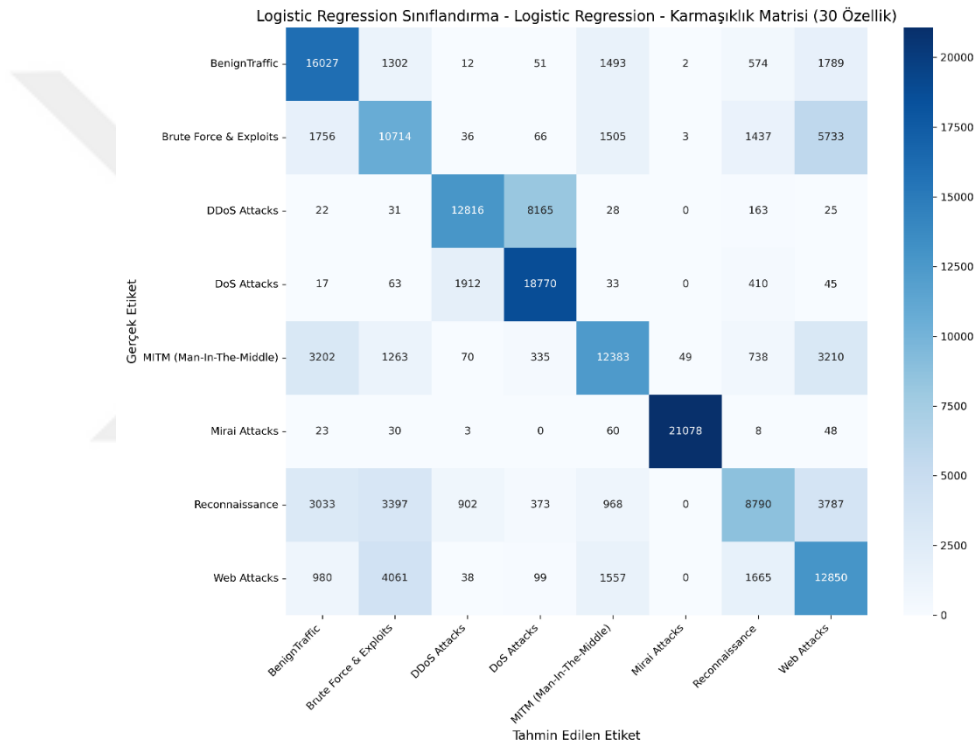
4.2.2.1. Lojistik Regresyon (LR) algoritması sonuçları

Bu çalışmada, LR algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.15'te LR modelinin farklı sayıda özellikle elde ettiği doğruluk ve F1 skoru değerleri gösterilmektedir. Özellik sayısı arttıkça performans da yükselmiş ve en iyi sonuç 46 özellikle elde edilmiştir.

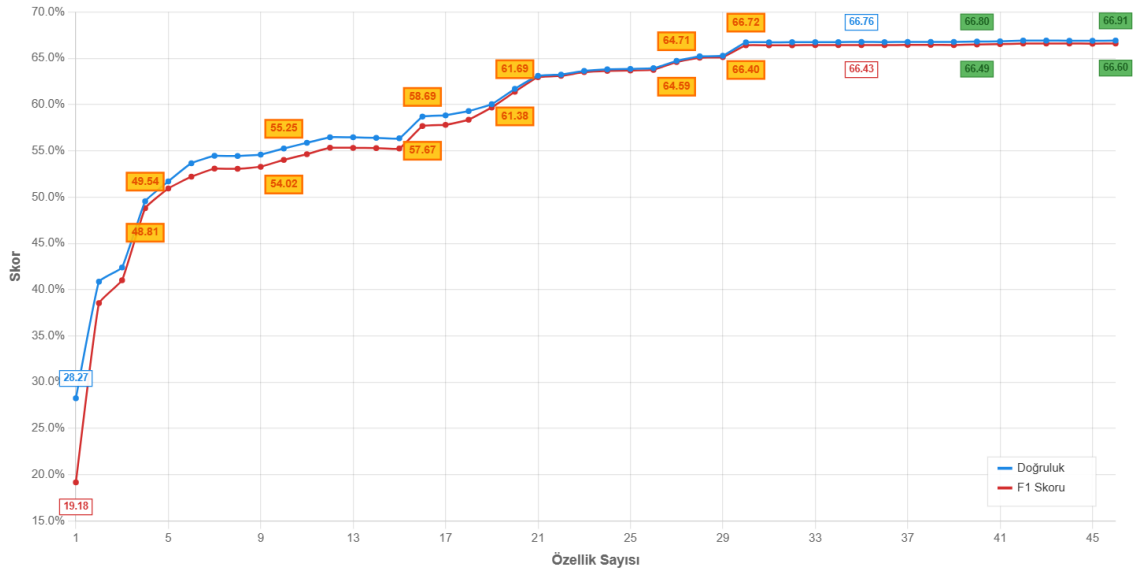
Çizelge 4.15. LR için önemli performans metrikleri

Özellik Sayısı	Doğruluk	F1 Skoru
1	0.282706	0.191779
2	0.408682	0.385419
4	0.495435	0.488092
6	0.536565	0.522084
10	0.552512	0.540180
16	0.586935	0.576673
20	0.616912	0.613825
25	0.638529	0.636834
30	0.667224	0.663972
35	0.667582	0.664308
40	0.667971	0.664869
46	0.669106	0.666020



Şekil 4.46. LR modeli sekiz sınıflı karmaşıklık matrisi (30 özellik)

Şekil 4.46, 30 özellikli LR modelinin karmaşıklık matrisini göstermektedir. En iyi model teknik olarak 46 özellikli model olsa da model karmaşıklığı ve hesaplama maliyeti göz önüne alındığında 30 özellikli model daha dengeli bir seçim olacaktır. Özellik sayısını 30'dan 46'ya çıkarmanın getirdiği çok küçük performans artışı, ek hesaplama maliyetini ve model karmaşıklığını genellikle haklı çıkarmaz. Bu nedenle, pratik uygulamada 30 özellikli model daha verimli bir seçim olarak değerlendirilebilir. Veri bilimi uygulamalarında, model performansında minimal bir artış için karmaşıklığı önemli ölçüde artırmak genellikle tercih edilmez.



Şekil 4.47 Özellik sayısına göre LR modelinin doğruluk ve F1 skoru değişimi.

Şekil 4.47, LR modelinin doğruluk ve F1 skoru değerlerinin özellik sayısı arttıkça yükseldiğini, 30. özellikten sonra ise performansın sabit kaldığını göstermektedir.

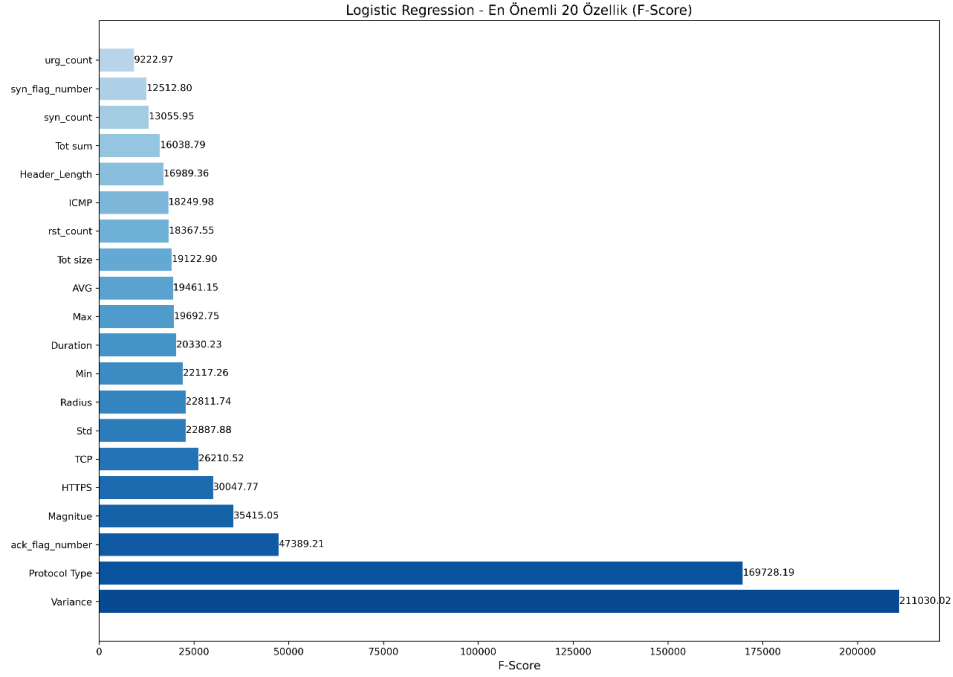
Çizelge 4.16’da LR modelinin 12 ve 30 özellik kullanarak farklı saldırı türleri üzerindeki performansı karşılaştırılmıştır.

Çizelge 4.16. LR için performans metrikleri (12 ve 30 özellik)

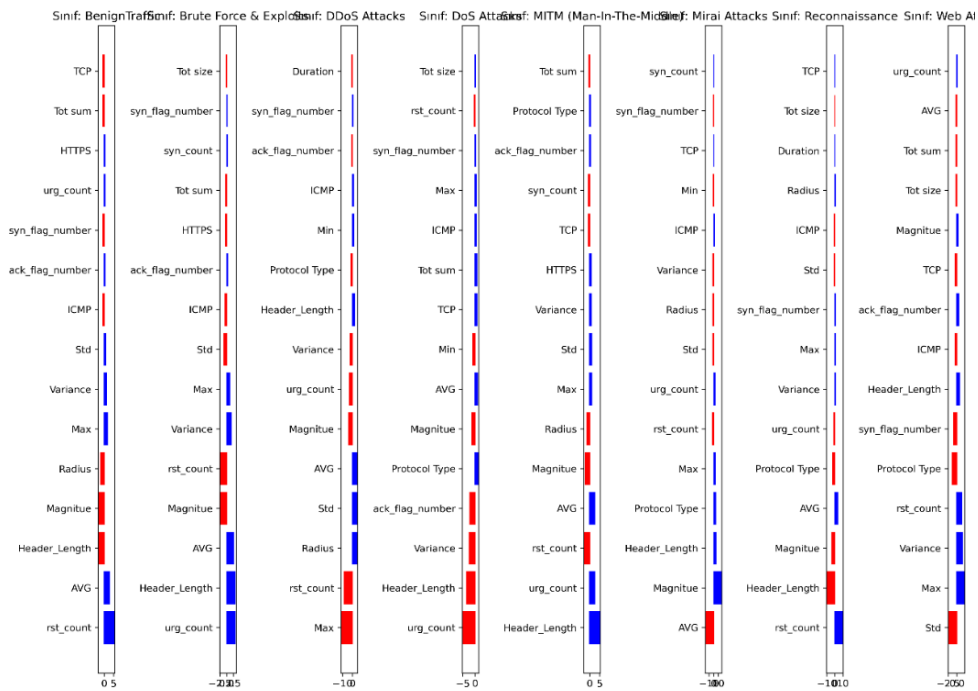
Özellik Sayısı	Sınıf	Doğruluk (%)	Keskinlik (%)	Duyarlılık (%)	F1 Skoru (%)
12	BenignTraffic	84.53	40.98	53.91	46.56
	Brute Force & Exploits	85.51	42.57	45.56	44.01
	DDoS Attacks	90.36	76.23	33.29	46.35
	DoS Attacks	91.40	59.59	97.08	73.85
	MITM	87.60	50.41	49.19	49.79
	Mirai Attacks	99.84	99.58	99.11	99.35
	Reconnaissance	88.45	55.94	35.87	43.71
	Web Attacks	85.24	40.33	37.74	38.99
	Doğruluk (%)	56.47			
30	BenignTraffic	91.61	63.95	75.42	69.22
	Brute Force & Exploits	87.83	51.36	50.42	50.88
	DDoS Attacks	93.29	81.17	60.31	69.20
	DoS Attacks	93.19	67.37	88.33	76.44
	MITM	91.46	68.69	58.27	63.05
	Mirai Attacks	99.87	99.74	99.19	99.47
	Reconnaissance	89.73	63.76	41.36	50.18
	Web Attacks	86.45	46.75	60.47	52.73
	Doğruluk (%)	66.72			

Şekil 4.48, Lojistik Regresyon modelinde kullanılan en önemli 20 özelliği F-Score değerlerine göre sıralı şekilde göstermektedir. IoT ağ trafiğinin sınıflandırılmasında en belirleyici özellikler arasında Variance (211030.02), Protocol Type (169728.19) ve

ack_flag_number (47389.21) öne çıkmaktadır. Bu özellikleri Magnitude, HTTPS, TCP ve Std gibi orta düzey öneme sahip değişkenler takip etmektedir. Öte yandan, urg_count, syn_flag_number ve syn_count gibi bazı özelliklerin model üzerindeki etkisi daha düşük seviyededir. Bu analiz, modelin performansını artırmak amacıyla yapılacak özellik seçimi süreci için önemli bir yol haritası sunmaktadır.



Şekil 4.48. LR modeli için en etkili 20 özelliğin önem skorları



Şekil 4.49. SHAP analizi ile saldırı ve normal trafik için özellik etkileri (20 özellik)

Şekil 4.49, farklı saldırı türleri ve normal ağ trafiği için geniş bir özellik kümesi üzerinden SHAP değerlerini göstermektedir. Grafik sütunları; Benign Traffic, Brute Force & Exploits, DDoS Attacks, DoS Attacks, MITM, Mirai Attacks, Reconnaissance ve Web Attacks gibi sınıfları temsil etmektedir. Özelliklerin pozitif (kırmızı) veya negatif (mavi) etkileri saldırı türüne göre değişmekte olup, örneğin DDoS saldırılarında Duration ve syn_flag_number pozitif, Benign Traffic için rst_count negatif yönde belirleyicidir. Bu analiz, saldırı türlerinin hangi özelliklerle daha iyi tanınabileceğini göstererek saldırı tespit sistemlerinin etkinliğini artırmada yol göstericidir.

4.2.2.2. Navie Bayes (NB) algoritması sonuçları

Bu çalışmada, NB algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.17, NB modelinin farklı sayıda özellikle elde ettiği doğruluk ve F1 skoru değerlerini göstermektedir.

Çizelge 4.17. NB için önemli performans metrikleri

Özellik Sayısı	Doğruluk	F1 Skoru
1	0.253641	0.151861
4	0.429100	0.347976
7	0.450100	0.365522
10	0.457724	0.391072
17	0.462576	0.406816
20	0.507212	0.455623
23	0.519682	0.482175
25	0.543171	0.514718
27	0.551829	0.531771
34	0.556682	0.525788
38	0.508588	0.471968
46	0.504271	0.468392

NB algoritmasının farklı özellik sayılarıyla elde ettiği sonuçlar değerlendirildiğinde, en düşük performansın 1 özellikle, en yüksek doğruluk (%55.67) ve F1 skorunun (%52.58) ise 34 özellikle elde edildiği görülmüştür. Özellik sayısı arttıkça model performansı genelde iyileşmiş, ancak 34'ten sonra düşüş eğilimi gözlenmiş; bu durum aşırı özellik kullanımının genelleme kapasitesini olumsuz etkileyerek boyutluluk laneti sorununa yol açabileceğini göstermektedir.

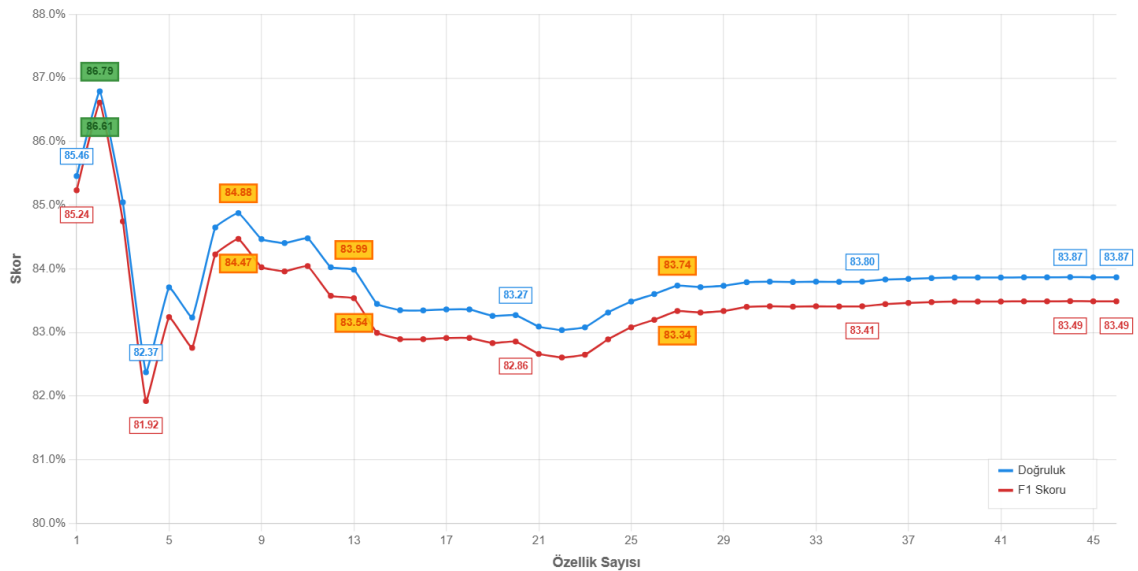
4.2.2.3.K En Yakın Komşu (KEYK) algoritması sonuçları

Bu çalışmada, KEYK algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.18, KEYK modelinin farklı sayıda özellikle elde ettiği doğruluk ve F1 skoru değerlerini göstermektedir.

Çizelge 4.18. KEYK için önemli performans metrikleri

Özellik Sayısı	Doğruluk	F1 Skoru
1	0.854594	0.852356
2	0.867888	0.866145
3	0.850453	0.847471
5	0.837100	0.832405
8	0.848776	0.844708
13	0.839876	0.835374
20	0.832735	0.828583
27	0.837371	0.833368
30	0.837882	0.834012
35	0.837976	0.834111
40	0.838635	0.834860
46	0.838682	0.834905



Şekil 4.50. Özellik sayısına göre KEYK modelinin doğruluk ve F1 skoru değişimi.

Şekil 4.50, KEYK modelinin RO tabanlı özellik seçimine göre doğruluk ve F1 skoru performansını göstermektedir. Model, başlangıçta %85.46 doğruluk ile düşük bir seviyede başlamış, 2. özellikle %86.79 doğruluk ve %86.61 F1 skoruna ulaşarak en

yüksek performansı göstermiştir. Sonrasında düşüş eğilimi sergileyerek %83.8 seviyelerinde sabitlenmiştir. Bu nedenle, KEYK modeli için 2–3 özellikli yapı, optimum performans ve maliyet-fayda dengesi açısından yeterlidir.

4.2.2.4. Karar Ağacı (KA) algoritması sonuçları

Bu çalışmada, KA algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.19, KA modelinin farklı özellik sayılarıyla elde ettiği doğruluk ve F1 skoru değerlerini göstermektedir. Özellik sayısı arttıkça modelin performansında genel bir iyileşme gözlemlenmiştir.

Çizelge 4.19. KA için önemli performans metrikleri

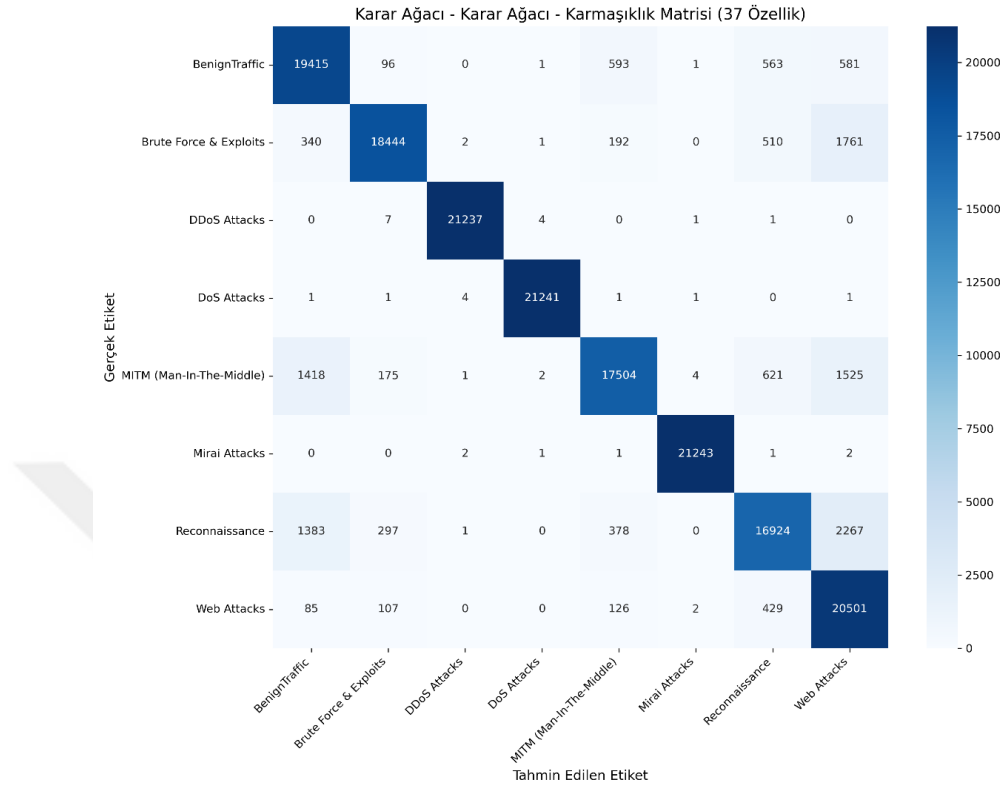
Özellik Sayısı	Doğruluk	F1 Skoru
1	0.828824	0.830609
2	0.854782	0.856743
3	0.856200	0.857659
7	0.859747	0.860992
8	0.860459	0.861565
9	0.860482	0.861586
20	0.859424	0.859847
21	0.908306	0.909027
25	0.910982	0.912096
37	0.920641	0.920908
40	0.920618	0.920887
46	0.920571	0.920838

Çizelge 4.20. KA için performans metrikleri (37 özellik)

Özellik Sayısı	Sınıf	Doğruluk (%)	Kesinlik (%)	Duyarlılık (%)	F1 Skoru (%)
37	BenignTraffic	97.02	85.75	91.36	88.47
	Brute Force & Exploits	97.95	96.43	86.80	91.36
	DDoS Attacks	99.99	99.95	99.94	99.95
	DoS Attacks	99.99	99.96	99.96	99.96
	MITM	97.04	93.13	82.37	87.42
	Mirai Attacks	99.99	99.96	99.97	99.96
	Reconnaissance	96.21	88.84	79.64	83.99
	Web Attacks	95.95	76.96	96.48	85.62
	Doğruluk (%)	92.06			

Çizelge 4.20, 37 özellik kullanılarak KA modelinin her bir sınıf için elde ettiği doğruluk, kesinlik, duyarlılık ve F1 skoru sonuçlarını göstermektedir. DDoS, DoS ve

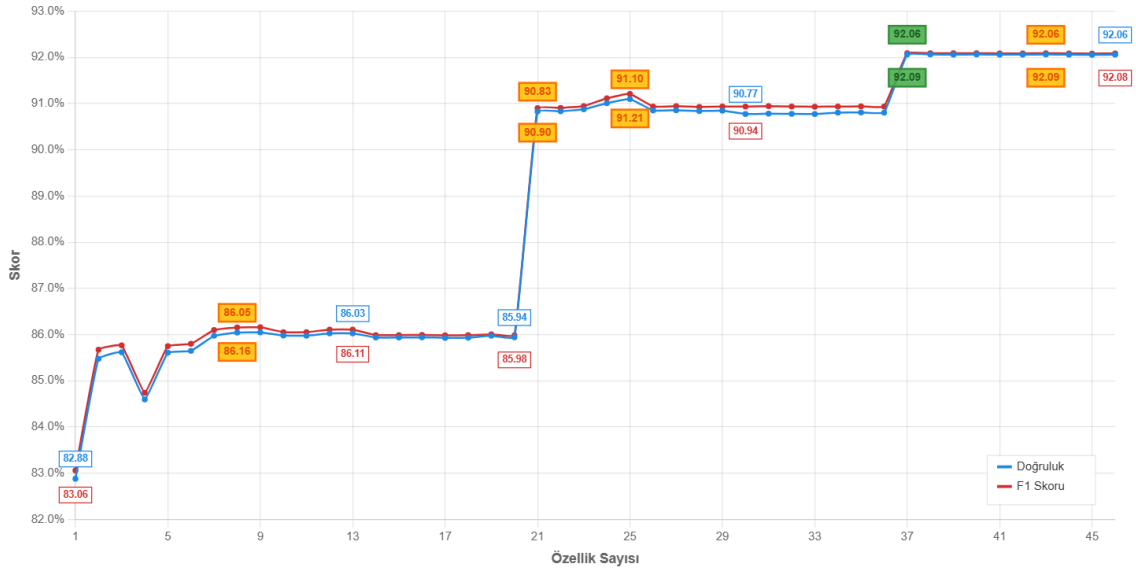
Mirai saldırıları %99'un üzerinde doğruluk ve F1 skoru ile yüksek başarıyla sınıflandırılmıştır. Genel model doğruluğu %92.06 olarak hesaplanmıştır.



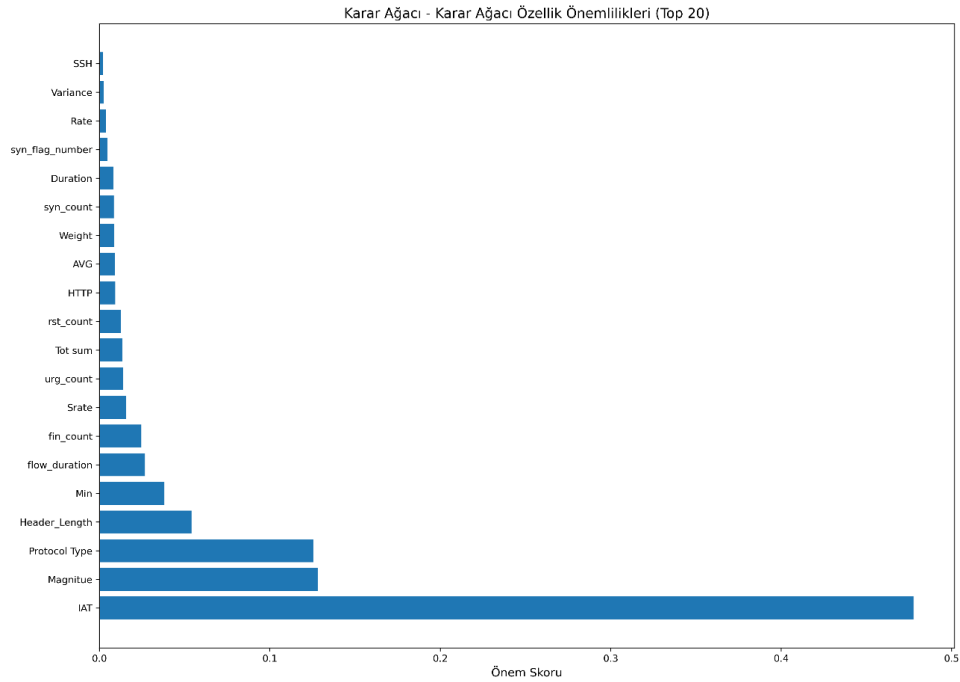
Şekil 4.51. KA modeli sekiz sınıflı karmaşıklık matrisi (37 özellik)

Şekil 4.51’de sunulan 37 özellikli KA modeline ait karmaşıklık matrisi, modelin sekiz saldırı türünü yüksek doğrulukla sınıflandırabildiğini göstermektedir. Özellikle DDoS, DoS, Mirai ve Web saldırılarında oldukça başarılı sonuçlar elde edilmiş, diğer sınıflarda da tatmin edici performans gözlemlenmiştir. Daha fazla özellikte teknik olarak daha iyi sonuçlar alınsa da, hesaplama maliyeti ve model karmaşıklığı dikkate alındığında 37 özellikli yapı, performans ve verimlilik açısından dengeli bir tercih olarak öne çıkmaktadır. Bu durum, özellikle kaynak kısıtlı IoT ortamlarında modelin uygulanabilirliğini artırmaktadır.

Şekil 4.52, KA modelinin RO tabanlı özellik seçimine göre doğruluk ve F1 skoru performansını göstermektedir. İlk 20 özelliğe kadar doğruluk ve F1 skoru %85–86 seviyelerinde kalmıştır. 21. özellikten itibaren performansta belirgin bir artış gözlenmiş, 37. özellikte en yüksek değerlere ulaşılmıştır (%92.06 doğruluk, %92.09 F1 skoru). Bu seviyeden sonra skorlar sabit kaldığından, optimum verimlilik açısından 37–43 arası özellik sayısı yeterli görülmektedir.



Şekil 4.52. Özellik sayısına göre KA modelinin doğruluk ve F1 skoru değişimi.



Şekil 4.53. KA modeli için en etkili 20 özelliğin önem skorları

Şekil 4.53'te KA modelinde kullanılan özelliklerin sınıflandırmadaki etkisi görülmektedir. Yaklaşık 0.48'lik önem skoru ile IAT en belirleyici özellik olarak öne çıkarken, Magnitude ve Protocol Type onu takip etmektedir. Orta düzey etkili değişkenler arasında Header_Length, Min ve flow_duration yer alırken, SSH, Variance ve syn_flag_number gibi özelliklerin katkısı oldukça düşüktür. Bu durum, modelin sadeleştirilmesi ve önemli parametrelerin belirlenmesi açısından değerli bir sonuç sunmaktadır.

4.2.2.5. Rastgele Orman (RO) algoritması sonuçları

Bu çalışmada, RO algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.21, RO modelinin farklı özellik sayılarıyla elde ettiği doğruluk ve F1 skoru değerlerini göstermektedir. Performans, özellikle 26 özelliğe kadar istikrarlı şekilde artmış; en yüksek doğruluk (%95.29) ve F1 skoru (%95.27) bu noktada elde edilmiştir.

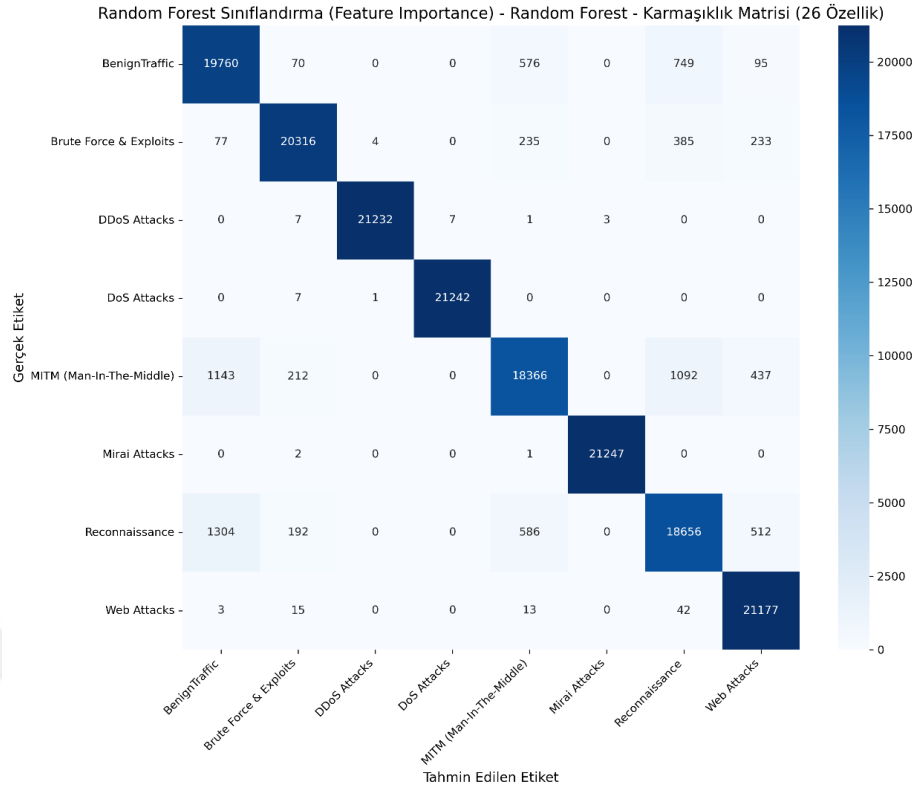
Çizelge 4.21. RO için önemli performans metrikleri

Özellik Sayısı	Doğruluk	F1 Skoru
1	0.852276	0.850772
2	0.894794	0.893923
3	0.922459	0.921924
5	0.939618	0.939157
9	0.945494	0.945156
14	0.947547	0.947264
20	0.950400	0.950172
26	0.952918	0.952701
36	0.951700	0.951488
37	0.929624	0.929686
40	0.928982	0.929015
46	0.926082	0.926067

Çizelge 4.22, 26 özellik kullanılarak RO modelinin sınıf bazında ulaştığı performans metriklerini sunmaktadır. Tüm sınıflarda %95.29 doğruluk oranı yakalanmış; özellikle DDoS, DoS ve Web saldırılarında yüksek kesinlik ve F1 skoru değerleri elde edilmiştir. Modelin genel doğruluğu %95.29 olarak hesaplanmıştır.

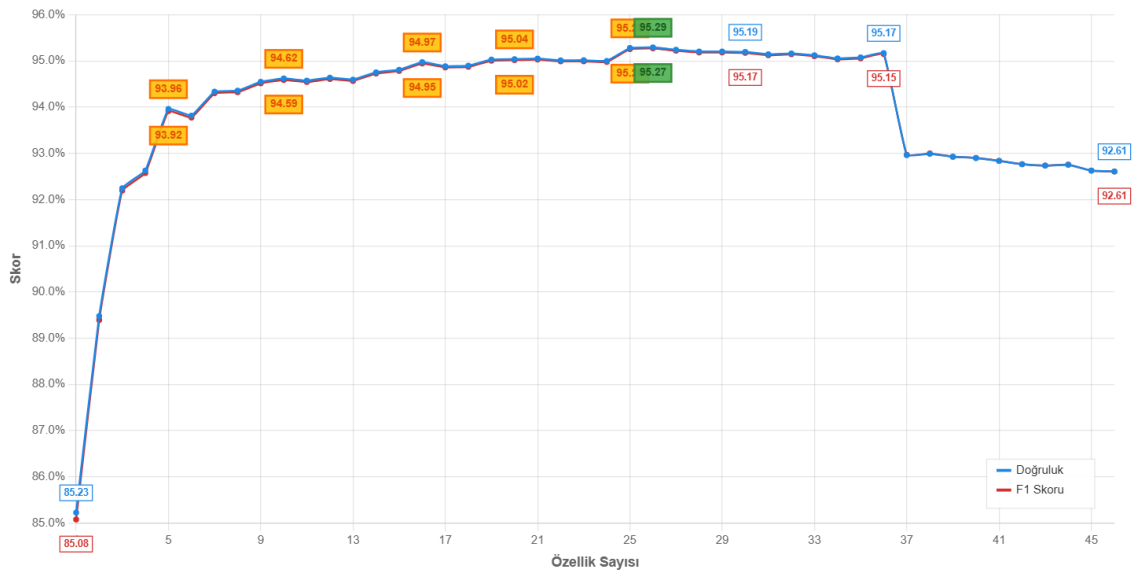
Çizelge 4.22. RO için performans metrikleri (26 özellik)

Özellik Sayısı	Sınıf	Doğruluk (%)	Kesinlik (%)	Duyarlılık (%)	F1 Skoru (%)
26	BenignTraffic	95.29	88.66	92.99	90.77
	Brute Force & Exploits	95.29	97.57	95.60	96.58
	DDoS Attacks	95.29	99.98	99.92	99.95
	DoS Attacks	95.29	99.97	99.96	99.96
	MITM	95.29	92.86	86.43	89.53
	Mirai Attacks	95.29	99.99	99.99	99.99
	Reconnaissance	95.29	89.16	87.79	88.47
	Web Attacks	95.29	94.31	99.66	96.91
	Doğruluk (%)	95.29			



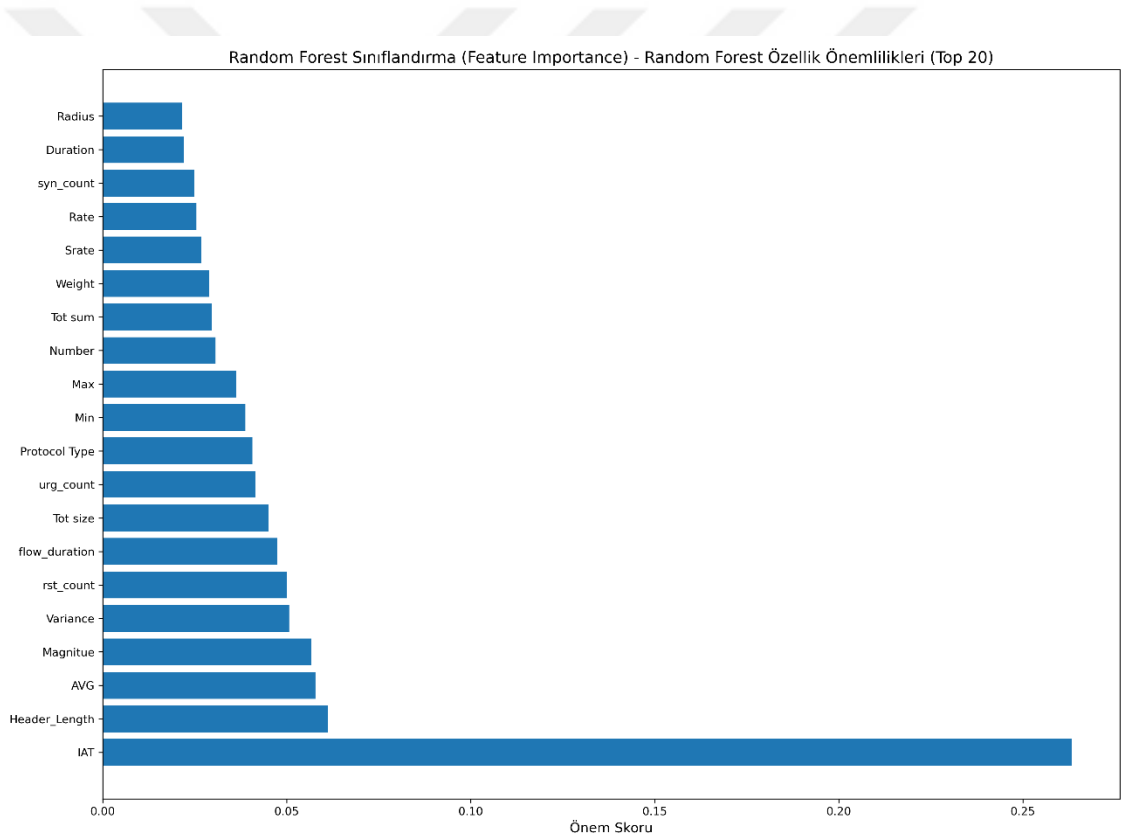
Şekil 4.54. RO modeli sekiz sınıflı karmaşıklık matrisi (26 özellik)

Şekil 4.54, 26 özellikli RO modeline ait karmaşıklık matrisini göstermektedir. Model, özellikle DDoS, DoS, Mirai ve Web saldırılarında yüksek doğruluk sergilemiştir. Diğer sınıflarda da genel olarak başarılı sonuçlar elde edilmiş, sınıflar arası karışıklık ise sınırlı düzeyde kalmıştır. Bu yapı, performans ve kaynak kullanımı açısından dengeli bir çözüm sunarak IoT ortamları için uygun bir seçenek olarak öne çıkmaktadır.



Şekil 4.55. Özellik sayısına göre RO modelinin doğruluk ve F1 skoru değişimi.

Şekil 4.55, RO modelinin RO tabanlı özellik seçimine göre doğruluk ve F1 skoru performansını göstermektedir. Model, başlangıçta %85,23 doğruluk ve %85,08 F1 skoru ile düşük bir performans sergilemiştir. 19. özellikle birlikte %95,03 doğruluk ve %95,01 F1 skoru seviyelerine ulaşılmış; en yüksek değerler ise %95,29 doğruluk ve %95,27 F1 skoru ile 26. özellikte elde edilmiştir. Özellikle 20–36 özellik aralığında modelin yüksek ve istikrarlı bir performans sergilediği, bu aralığın dışına çıkıldığında ise doğruluk ve F1 skorlarında belirgin düşüşler yaşandığı gözlemlenmiştir. Nitekim, 45 özellik kullanıldığında doğruluk %92,63 ve F1 skoru %92,62 seviyelerine gerilemiştir. Bu durum, 26–36 arası özellik sayısının model için optimal olduğunu; daha fazla özelliğin aşırı öğrenmeye neden olarak genel performansı olumsuz etkileyebileceğini göstermektedir.



Şekil 4.56. RO modeli için en etkili 20 özelliğin önem skorları

Şekil 4.56, RO modelinde kullanılan özelliklerin önem düzeylerini ortaya koymaktadır. Özellikle IAT (Inter-Arrival Time), yaklaşık 0.25’lik skoruyla açık ara en etkili özellik olarak öne çıkmaktadır. Bunu Header_Length, AVG ve Magnitude gibi özellikler takip ederken, Variance, rst_count ve flow_duration orta düzeyde katkı sağlamaktadır. Radius, Duration ve syn_count gibi değişkenlerin ise daha düşük etkiye olduğu görülmektedir. Bu analiz, IoT ağlarında saldırı tespiti için en belirleyici

parametreleri ortaya koyarak, model tasarımı ve özellik seçimi süreçlerinde yol gösterici bir rol üstlenmektedir.

4.2.2.6. Gradyan Artırma (GA) algoritması sonuçları

Bu çalışmada, GA algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.23, GA modelinin farklı özellik sayılarıyla elde ettiği doğruluk ve F1 skoru değerlerini göstermektedir.

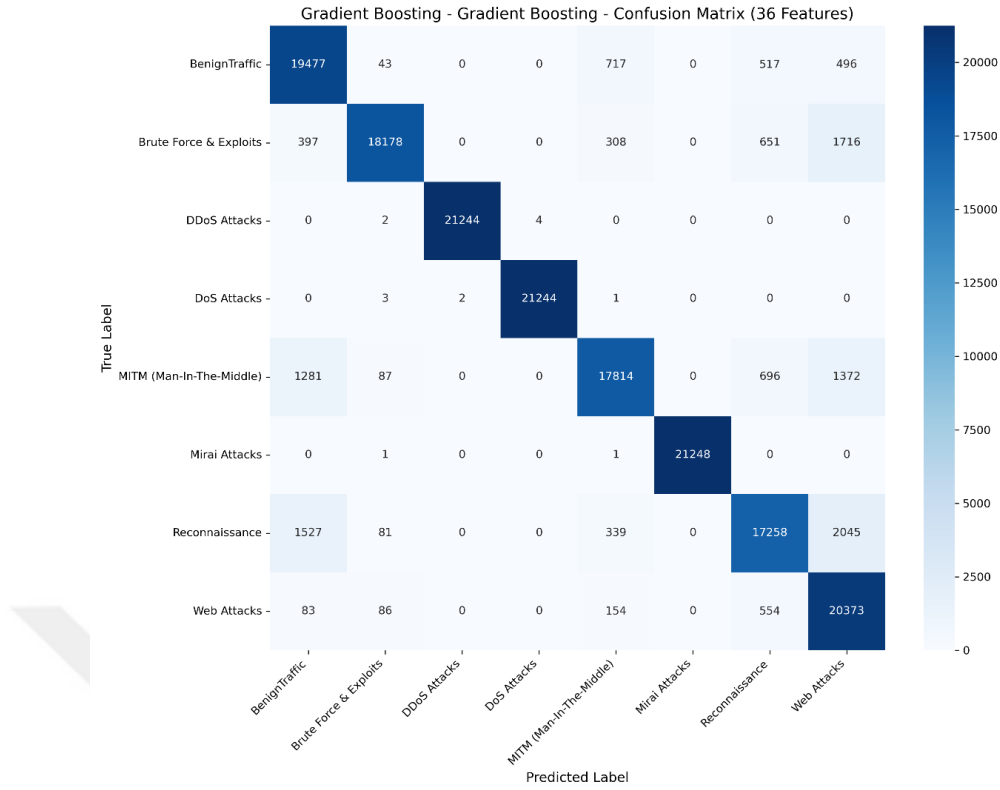
Çizelge 4.23. GA için önemli performans metrikleri

Özellik Sayısı	Doğruluk	F1 Skoru
1	0.829882	0.831494
2	0.867429	0.869442
3	0.886153	0.888176
5	0.904841	0.905560
10	0.913100	0.913631
15	0.917529	0.917842
20	0.920782	0.920996
25	0.920853	0.921125
30	0.922429	0.922748
36	0.922565	0.922896
40	0.919335	0.919661
45	0.919318	0.919664
46	0.919341	0.919673

Çizelge 4.24, 36 özellik kullanılarak GA modelinin sınıf bazında ulaştığı doğruluk, kesinlik, duyarlılık ve F1 skoru değerlerini sunmaktadır. Model özellikle DDoS, DoS ve Mirai saldırılarında %99'un üzerinde başarı sağlamış; genel doğruluk oranı %92.26 olarak hesaplanmıştır.

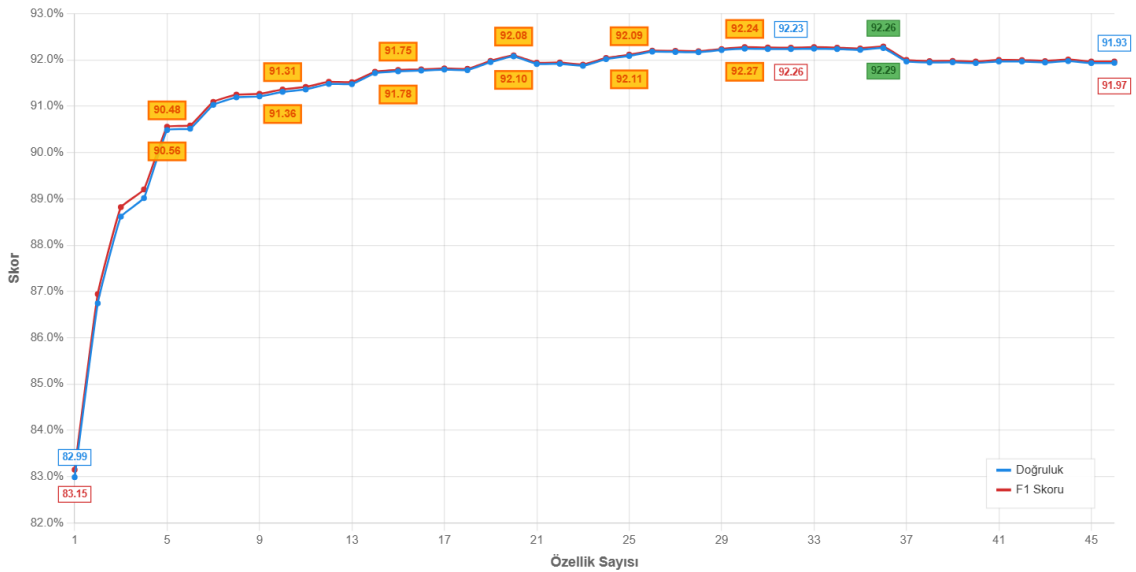
Çizelge 4.24. GA için performans metrikleri (36 özellik)

Özellik Sayısı	Sınıf	Doğruluk (%)	Kesinlik (%)	Duyarlılık (%)	F1 Skoru (%)
36	BenignTraffic	91.67	85.58	91.67	88.53
	Brute Force & Exploits	85.52	97.77	85.52	91.24
	DDoS Attacks	99.97	99.97	99.97	99.97
	DoS Attacks	99.97	99.97	99.97	99.97
	MITM	83.71	93.48	83.71	88.34
	Mirai Attacks	99.99	99.99	99.99	99.99
	Reconnaissance	81.20	90.52	81.20	85.62
	Web Attacks	96.01	95.68	96.01	95.84
	Doğruluk (%)	92.26			



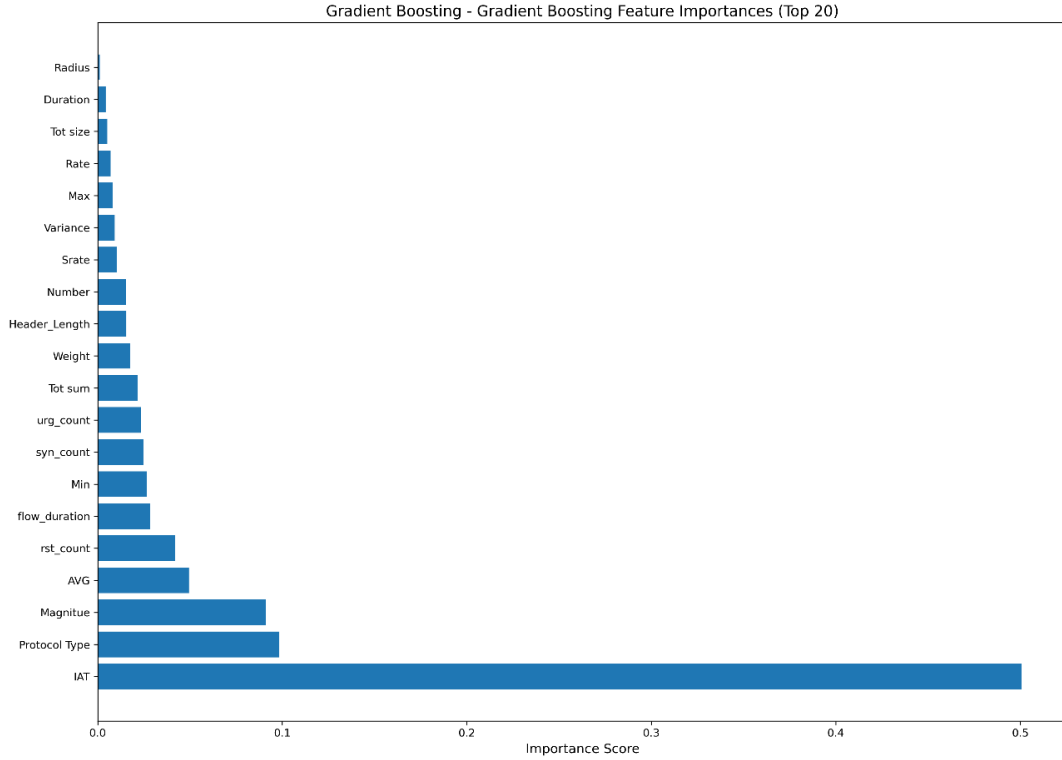
Şekil 4.57. GA modeli sekiz sınıflı karmaşıklık matrisi (36 özellik)

Şekil 4.57’de verilen karmaşıklık matrisi, 36 özellik kullanılan GA modelinin çok sınıflı saldırı tespitindeki performansını göstermektedir. Model özellikle DDoS, DoS ve Mirai saldırılarını yüksek doğrulukla tahmin etmiştir. BenignTraffic ve Web Attacks sınıfları da iyi sonuçlar göstermiştir. Ancak Reconnaissance, MITM ve Brute Force & Exploits sınıflarında bazı yanlış sınıflandırmalar meydana gelmiştir. Bu durumun temel sebebi, ilgili saldırı türlerinin benzer özelliklere sahip olmasıdır.



Şekil 4.58. Özellik sayısına göre GA modelinin doğruluk ve F1 skoru değişimi.

Şekil 4.58, GA modelinin RO tabanlı özellik seçimine göre doğruluk ve F1 skoru performansını göstermektedir. Model, başlangıçta %82.99 doğruluk ve %83.15 F1 skoru ile düşük bir performans sergilemiş; 5. özellikle %90.48 doğruluk ve %90.56 F1 skoru seviyelerine ulaşmıştır. Performans artışı kademeli olarak devam ederek, 20. özellikte %92.08 doğruluk ve %92.10 F1 skoruna ulaşmıştır. En yüksek başarı, %92.26 doğruluk ve %92.29 F1 skoru ile 36. özellikte elde edilmiştir. 30. özellik civarında performansın zirveye yaklaştığı, 37. özellikten sonra ise %91.97 doğruluk ve %92.00 F1 skoru ile hafif bir düşüş yaşandığı görülmektedir. GA modeli, diğer algoritmalara kıyasla daha dengeli ve kademeli bir performans artışı sergilemektedir. Bu nedenle, optimum verimlilik ve başarı açısından 25–36 arası özellik sayısı ideal görülmekte; daha sade uygulamalar için ise 14–17 özellik yeterli olabilmektedir.



Şekil 4.59. GA modeli için en etkili 20 özelliğin önem skorları

Şekil 4.59'da GA modelindeki en önemli 20 özellik, önem skorlarına göre sıralanarak gösterilmiştir. "Inter-Arrival Time (IAT)" özelliği, yaklaşık 0.5 önem skoruyla açık ara en etkili özellik olarak öne çıkmıştır. Bunu, çok daha düşük önem skorlarıyla "Protocol Type", "Magnitude", "AVG", "rst_count", "flow_duration" ve "Min" özellikleri takip etmektedir. En düşük önem değerlerine sahip olan özellikler ise "Radius" ve "Duration" olarak belirlenmiştir. Sonuç olarak, saldırı tespitinde paketler

arası varış süresinin (IAT) kritik öneme sahip olduğu ve sınırlı sayıda en etkili özelliklerle bile yüksek performans sağlanabileceği anlaşılmaktadır.

4.2.2.7. Aşırı Gradyan Artırma (AGA) algoritması sonuçları

Bu çalışmada, AGA algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.25, AGA modelinin farklı özellik sayılarıyla elde ettiği doğruluk ve F1 skoru değerlerini göstermektedir.

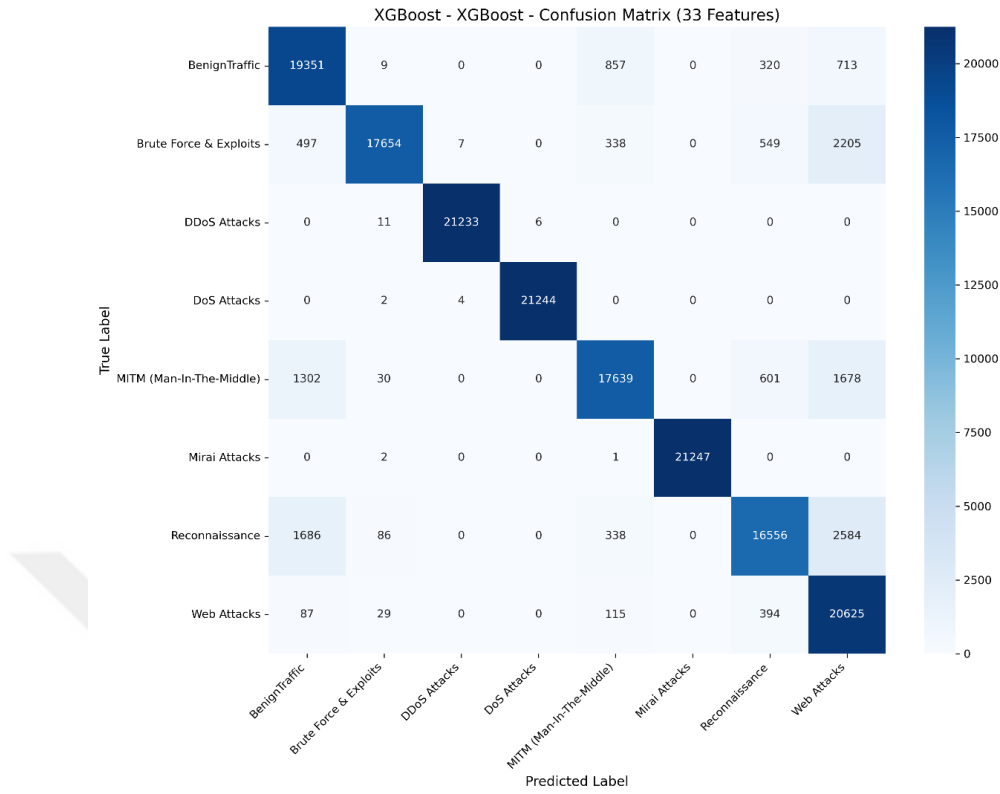
Çizelge 4.25. AGA için önemli performans metrikleri

Özellik Sayısı	Doğruluk	F1 Skoru
1	0.814400	0.815778
3	0.876524	0.878987
5	0.898559	0.899431
7	0.903241	0.904047
10	0.906082	0.906822
15	0.910876	0.911348
20	0.914794	0.915155
25	0.914006	0.914519
33	0.914994	0.915575
37	0.913841	0.914360
40	0.913347	0.913832
46	0.913476	0.913968

Çizelge 4.26, AGA modelinin 33 özellik kullanılarak elde ettiği sınıf bazlı performansını göstermektedir. Model, özellikle DDoS, DoS ve Mirai saldırılarında %99'un üzerinde doğruluk ve F1 skoru ile yüksek başarı sağlamıştır. Genel doğruluk oranı %91.50 olarak hesaplanmış, bu yapı güçlü sınıflandırma performansı ile öne çıkmıştır.

Çizelge 4.26. AGA için performans metrikleri (33 özellik)

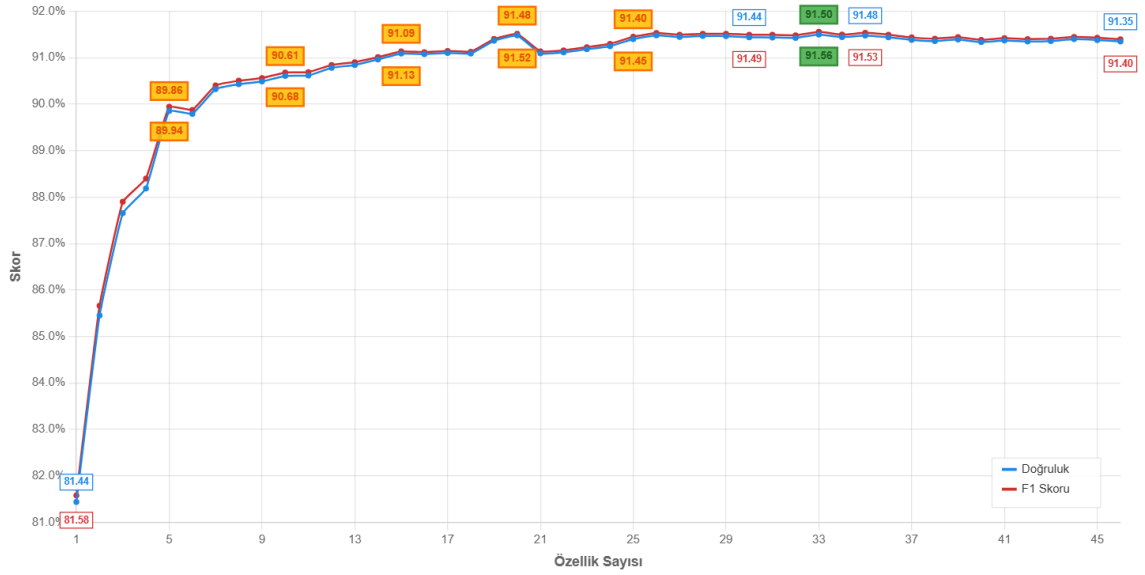
Özellik Sayısı	Sınıf	Doğruluk (%)	Kesinlik (%)	Duyarlılık (%)	F1 Skoru (%)
33	BenignTraffic	96.78	84.42	91.06	87.61
	Brute Force & Exploits	97.79	99.05	83.08	90.36
	DDoS Attacks	99.98	99.95	99.92	99.93
	DoS Attacks	99.99	99.97	99.97	99.97
	MITM	96.91	91.45	83.01	87.02
	Mirai Attacks	100.00	100.00	99.99	99.99
	Reconnaissance	96.14	89.88	77.91	83.47
	Web Attacks	95.41	74.18	97.06	84.09
	Doğruluk (%)	91.50			



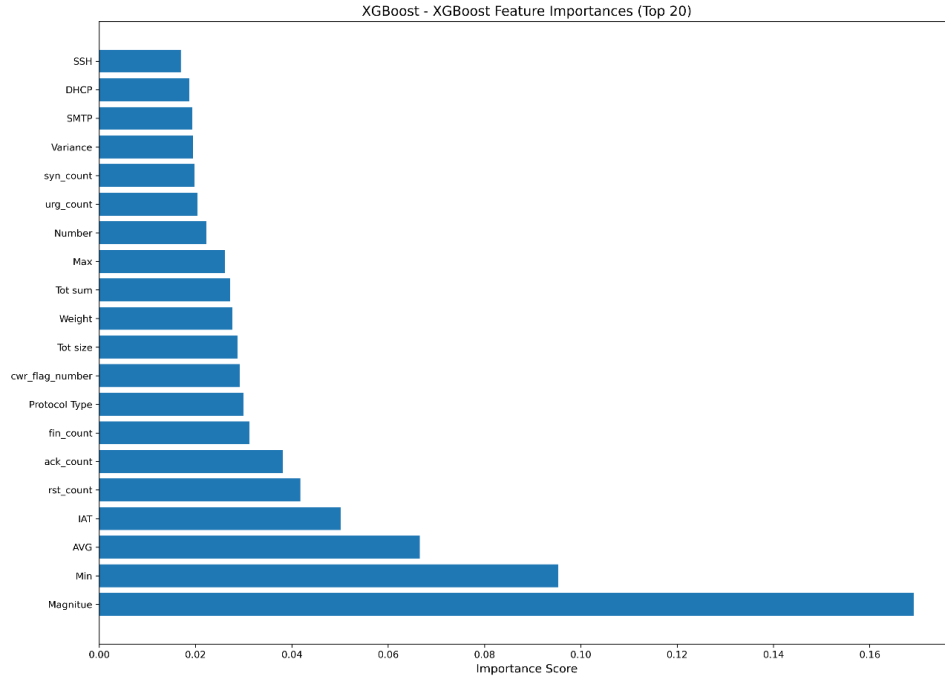
Şekil 4.60.AGA modeli sekiz sınıflı karmaşıklık matrisi (33 özellik)

Şekil 4.60’de sunulan karmaşıklık matrisi, 33 özellikli AGA modelinin birçok saldırı türünü yüksek doğrulukla sınıflandırabildiğini göstermektedir. Özellikle DDoS, DoS, Mirai ve Web saldırılarında güçlü performans sergileyen model, MITM ve Reconnaissance gibi sınıflarda da kabul edilebilir doğruluklar sunmuştur. Ancak, 33 özellikli modelin 20 özellikli modele kıyasla yalnızca %0.02’lik performans artışı sağlaması, artan hesaplama maliyetini haklı çıkarmamaktadır. Bu nedenle, kaynak kısıtlı IoT uygulamaları için 20 özellikli AGA modeli daha verimli ve dengeli bir tercih olarak öne çıkmaktadır.

Şekil 4.61, AGA modelinin RO tabanlı özellik seçimine göre doğruluk ve F1 skoru performansını göstermektedir. Model, başlangıçta %81.44 seviyesinde düşük bir performans sergilemiş; 5. özellikte %89.86’ya, 20. özellikte ise %91.48 düzeyine ulaşmıştır. En yüksek değerler %91.50 doğruluk ve %91.56 F1 skoru ile 33. özellikte elde edilmiştir. Bu noktadan sonra performans hafif bir düşüşle %91.30–%91.40 aralığında sabitlenmiştir. AGA modeli, kademeli ve dengeli bir performans artışı göstermektedir. Optimum başarı ve verimlilik açısından 26–35 arası özellik sayısı ideal görülürken, daha sade modeller için 15–20 aralığı da yeterli sonuç verebilmektedir.



Şekil 4.61. Özellik sayısına göre AGA modelinin doğruluk ve F1 skoru değişimi.



Şekil 4.62. AGA modeli için en etkili 20 özelliğin önem skorları

Şekil 4.62’de AGA modelinde kullanılan özelliklerin sınıflandırma üzerindeki etkisi gösterilmektedir. Magnitude yaklaşık 0.16’lık önem skoru ile en belirleyici özellik olarak öne çıkarken, Min ve AVG gibi özellikler de önemli katkı sağlamaktadır. IAT, rst_count ve ack_count orta düzeyde etki gösterirken; SSH, DHCP ve Variance gibi özelliklerin katkısı düşüktür. Bu analiz, modelin performansını koruyarak daha az sayıda özellikli çalışılabileceğini göstermekte ve 20 özellikli modelin, doğruluk-verimlilik dengesi açısından ideal bir tercih olduğunu desteklemektedir.

4.2.2.8. Yapay sinir ağı (YSA) algoritması sonuçları

Bu çalışmada, YSA algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.27, YSA modelinin farklı özellik sayılarıyla elde ettiği doğruluk ve F1 skoru değerlerini göstermektedir.

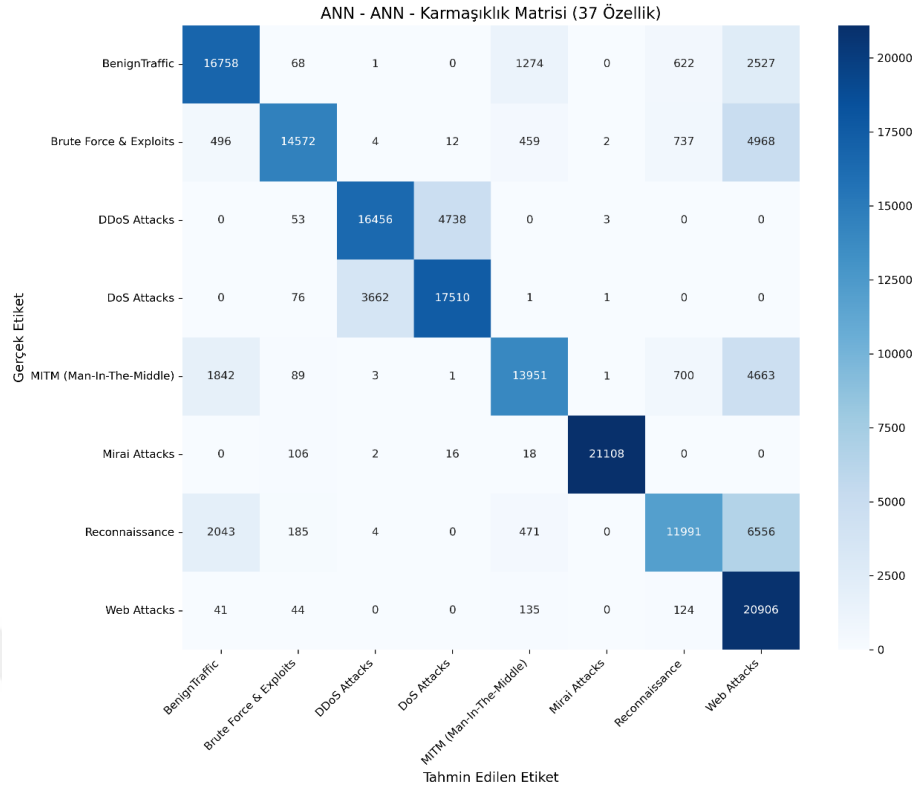
Çizelge 4.27. YSA için önemli performans metrikleri

Özellik Sayısı	Doğruluk	F1 Skoru
1	0.484712	0.409363
2	0.674535	0.671922
5	0.756412	0.755631
10	0.737341	0.738646
15	0.749418	0.749480
20	0.755553	0.754884
23	0.761118	0.762144
27	0.774135	0.775998
30	0.780376	0.782029
32	0.782976	0.785239
37	0.783835	0.786597
42	0.776000	0.778090
46	0.780182	0.782260

Çizelge 4.28, YSA modelinin 5 ve 37 özellik kullanılarak sınıf bazında gösterdiği performansı sunmaktadır.

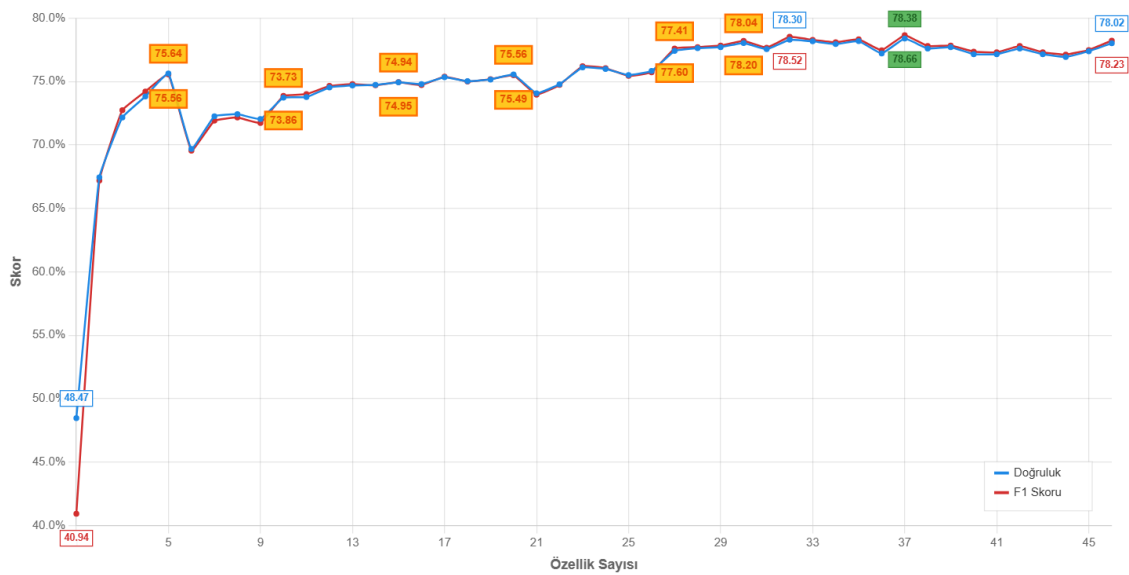
Çizelge 4.28. YSA için performans metrikleri (5 ve 37 özellik)

Özellik Sayısı	Sınıf	Doğruluk (%)	Kesinlik (%)	Duyarlılık (%)	F1 Skoru (%)
5	BenignTraffic	79.12	59.39	81.09	68.56
	Brute Force & Exploits	57.89	97.63	57.29	72.21
	DDoS Attacks	93.13	96.59	93.32	94.93
	DoS Attacks	98.91	94.20	99.20	96.64
	MITM	31.16	74.82	46.80	57.58
	Mirai Attacks	99.19	98.37	99.19	98.78
	Reconnaissance	46.84	67.59	47.62	55.87
	Web Attacks	78.58	47.70	80.64	59.94
	Doğruluk (%)	75.64			
37	BenignTraffic	79.01	79.12	78.86	78.99
	Brute Force & Exploits	69.24	95.91	68.57	79.97
	DDoS Attacks	77.38	81.74	77.44	79.53
	DoS Attacks	82.15	78.60	82.40	80.46
	MITM	65.60	85.54	65.65	74.29
	Mirai Attacks	99.33	99.97	99.33	99.65
	Reconnaissance	55.56	84.60	56.43	67.70
	Web Attacks	98.35	52.77	98.38	68.69
	Doğruluk (%)	78.38			



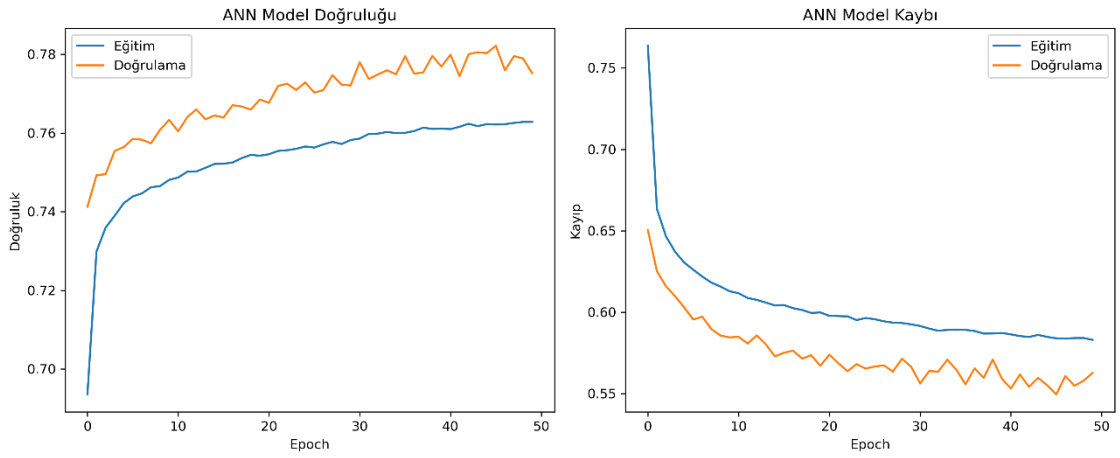
Şekil 4.63. YSA modeli sekiz sınıflı karmaşıklık matrisi (37 özellik)

Şekil 4.63, 37 özellikli YSA modelinin sınıflandırma başarısını göstermektedir. Web, Mirai ve BenignTraffic sınıflarında yüksek doğruluk sağlanırken, DDoS ve DoS arasında karışıklık yaşanmıştır. 37 özellik en iyi sonucu verse de 5 özellikli model %75.64 doğrulukla daha sade ve verimli bir seçenek sunmaktadır. Bu fark, IoT gibi kaynak kısıtlı ortamlarda düşük özellikli modellerin tercih edilebileceğini göstermektedir.



Şekil 4.64. Özellik sayısına göre YSA modelinin doğruluk ve F1 skoru değişimi.

Şekil 4.64, YSA modelinin RO tabanlı özellik seçimine göre doğruluk ve F1 skoru performansını göstermektedir. Model, başlangıçta %48.47 doğruluk ve %40.94 F1 skoru ile oldukça düşük bir performans sergilemiş; 3. özellikte %72.17 doğruluk ve %72.74 F1 skoruna ulaşmıştır. Kademeli artışla 20. özellikte %75.56 doğruluk ve %75.49 F1 skoru elde edilmiştir. En yüksek performans %78.38 doğruluk ve %78.66 F1 skoru ile 37. özellikte görülmüştür. Bu noktadan sonra performans dalgalanarak %77–78 aralığında seyretmiştir. Optimum başarı ve verimlilik açısından 27–37 arası özellik sayısı ideal olarak değerlendirilmekte; daha basit modeller için 13 civarı özellik yeterli olabilmektedir.



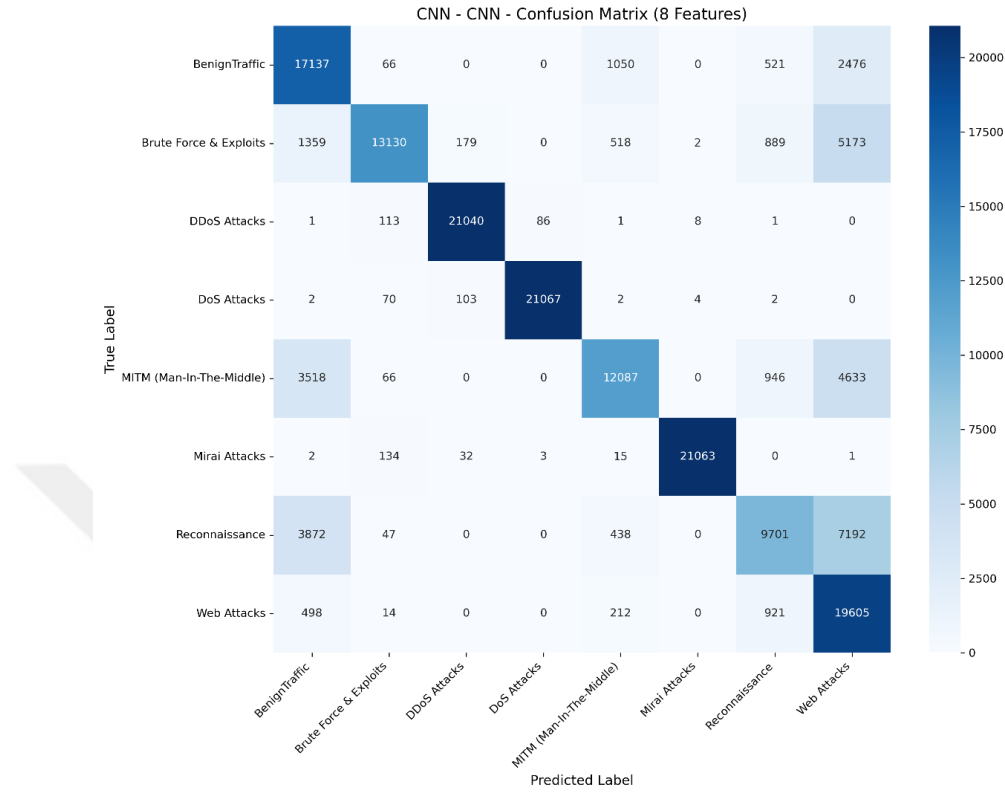
Şekil 4.65. YSA modelinin 37 özellik ile eğitim sürecine ait doğruluk ve kayıp eğrileri

Şekil 4.65, Yapay Sinir Ağı (YSA) modelinin eğitim sürecine ait doğruluk ve kayıp grafiklerini göstermektedir. Eğitim başlangıcında doğruluk değeri %69 seviyesindeyken, ilk 10 epoch'ta hızlı bir artış, sonraki dönemlerde ise istikrarlı bir yükseliş gözlemlenmiştir. Eğitim sonunda doğruluk eğitim verisi için %76, doğrulama verisi için ise %78 seviyesine ulaşmıştır. Kayıp fonksiyonu ise her iki veri setinde de düzenli şekilde azalarak sırasıyla 0.58 ve 0.55 değerlerine gerilemiştir. Doğrulama doğruluğunun eğitim doğruluğundan yüksek olması, modelin aşırı öğrenmeden kaçındığını ve genelleme kabiliyetinin güçlü olduğunu göstermektedir.

4.2.2.9. Evrimsel Sinir Ağları (ESA) algoritması sonuçları

Bu çalışmada, ESA algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki

başarımını değerlendirmek amacıyla, veri集中的 tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.



Şekil 4.66. ESA modeli sekiz sınıflı karmaşıklık matrisi (8 özellik)

Şekil 4.66, 8 özellik kullanılarak eğitilen ESA modeline ait karmaşıklık matrisini göstermektedir. Model, DDoS, DoS ve Mirai saldırılarını yüksek doğrulukla sınıflandırırken; MITM ve Reconnaissance gibi sınıflarda daha fazla karışıklık yaşanmıştır. Özellikle Reconnaissance sınıfı sıklıkla Web Attacks ile, MITM ise BenignTraffic ve Web Attacks ile karıştırılmıştır. Bu durum, modelin bazı saldırı türlerini ayırt etmede başarılı olduğunu ancak belirli sınıflar arasında ayırım yapmada zorlandığını ortaya koymaktadır.

Çizelge 4.29. ESA için performans metrikleri (8 ve 36 özellik)

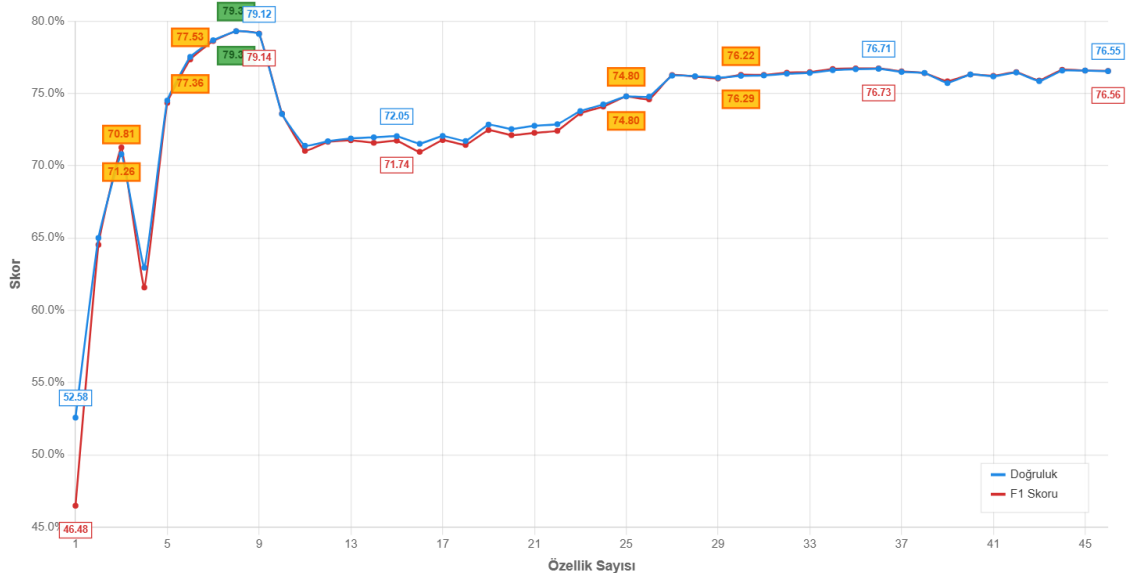
Özellik Sayısı	Sınıf	Doğruluk (%)	Kesinlik (%)	Duyarlılık (%)	F1 Skoru (%)
8	BenignTraffic	79.31	81.10	80.67	80.88
	Brute Force & Exploits	61.83	96.51	61.83	75.35
	DDoS Attacks	99.01	98.53	99.01	98.77
	DoS Attacks	99.14	99.59	99.14	99.37
	MITM	56.93	86.30	56.93	68.57
	Mirai Attacks	99.12	99.50	99.12	99.31
	Reconnaissance	45.72	73.80	45.72	56.50
	Web Attacks	92.27	83.33	92.27	87.58
	Doğruluk (%)	79.31			

Çizelge 4.29, ESA modelinin 8 özellik kullanılarak sınıf bazında gösterdiği performansı sunmaktadır. Model, DDoS, DoS ve Mirai saldırılarını yüksek doğrulukla sınıflandırırken; MITM ve Reconnaissance sınıflarında daha düşük performans sergilemiştir. Genel doğruluk %79.31 olarak hesaplanmıştır.

Çizelge 4.30, ESA modelinin farklı özellik sayılarıyla elde ettiği doğruluk ve F1 skoru değerlerini göstermektedir. En yüksek başarı 8 özellik ile elde edilmiş olup, bu yapı %79.31 doğruluk ve %79.31 F1 skoru ile öne çıkmıştır.

Çizelge 4.30. ESA için önemli performans metrikleri

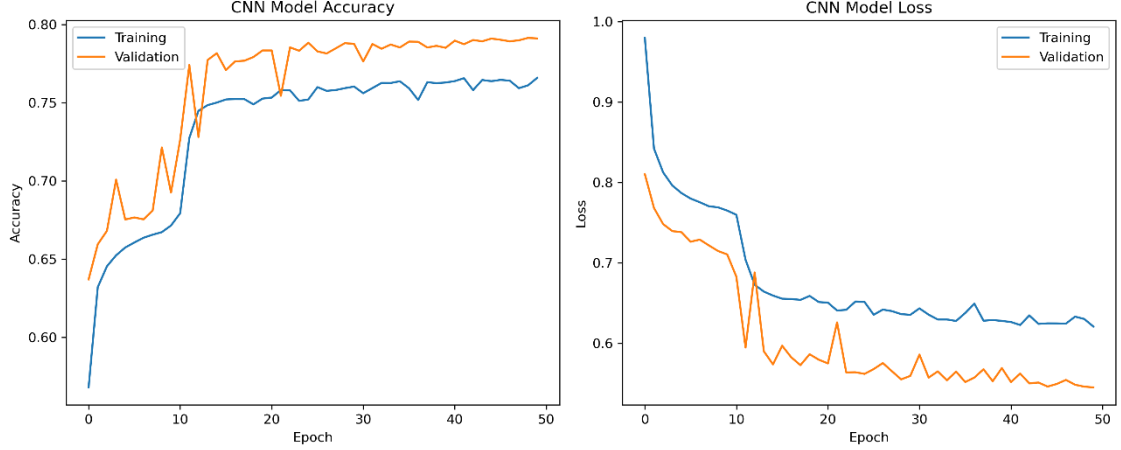
Özellik Sayısı	Doğruluk	F1 Skoru
1	0.525776	0.464767
2	0.650012	0.645325
3	0.700059	0.712581
5	0.745147	0.743520
7	0.786882	0.786375
8	0.793118	0.793115
9	0.791194	0.791411
15	0.720524	0.717381
19	0.728494	0.724633
25	0.747959	0.747962
27	0.762324	0.762757
35	0.766891	0.767321
36	0.767100	0.767298
40	0.763218	0.763178
46	0.765465	0.765565



Şekil 4.67. Özellik sayısına göre ESA modelinin doğruluk ve F1 skoru değişimi.

Şekil 4.67, ESA modelinin RO tabanlı özellik seçimine göre doğruluk ve F1 skoru performansını göstermektedir. Model, başlangıçta düşük performans sergilemiş; 8.

özellikle en yüksek değerlere ulaşmıştır (%79.31 doğruluk, %79.41 F1 skoru). Sonraki özelliklerde performans düşmüş, 25. özellikten itibaren ise kademeli artış gözlenmiştir. ESA modeli erken zirveye ulaşp ardından düşüş eğilimi gösterdiği için, optimum performans açısından 7–10 arası özellik yeterli görülmektedir.ve F1 skorunda dalgalı ancak durağan bir seyir izlediği görülmektedir.



Şekil 4.68. ESA modelinin eğitim süreci: Doğruluk ve kayıp grafikleri (8 özellik)

Şekil 4.68, ESA modelinin eğitim sürecine ait doğruluk ve kayıp grafiklerini göstermektedir. Sol grafikte, modelin doğruluğu ilk 10 epoch'ta hızla artmış, eğitim sonunda %76 eğitim ve %79 doğrulama seviyelerine ulaşmıştır. Sağ grafikte ise eğitim ve doğrulama kayıplarının düzenli olarak azaldığı, sırasıyla 0.62 ve 0.55 seviyelerine kadar düştüğü görülmektedir. Doğrulama doğruluğunun daha yüksek olması, modelin genelleme yeteneğinin güçlü olduğunu göstermektedir. Küçük dalgalanmalar mini-batch yapısından kaynaklanmakta olup genel öğrenme başarısını etkilememektedir.

4.2.2.10. Tekrarlayan sinir ağları (TSA) algoritması sonuçları

Bu çalışmada, TSA algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.31, TSA modelinin farklı özellik sayılarıyla elde ettiği doğruluk ve F1 skoru değerlerini göstermektedir. En yüksek performans, 30 özellikle elde edilmiş olup doğruluk %83.76, F1 skoru ise %83.81 olarak hesaplanmıştır.

Çizelge 4.31. TSA için önemli performans metrikleri

Özellik Sayısı	Doğruluk	F1 Skoru
1	0.559682	0.488364
3	0.723471	0.727254
5	0.784841	0.782501
8	0.739024	0.738691
11	0.816624	0.817173
16	0.817165	0.817484
19	0.823465	0.824542
20	0.804282	0.804200
21	0.828206	0.828324
25	0.831235	0.831668
30	0.837594	0.838131
37	0.830835	0.831600
42	0.833629	0.834069
46	0.833206	0.833821

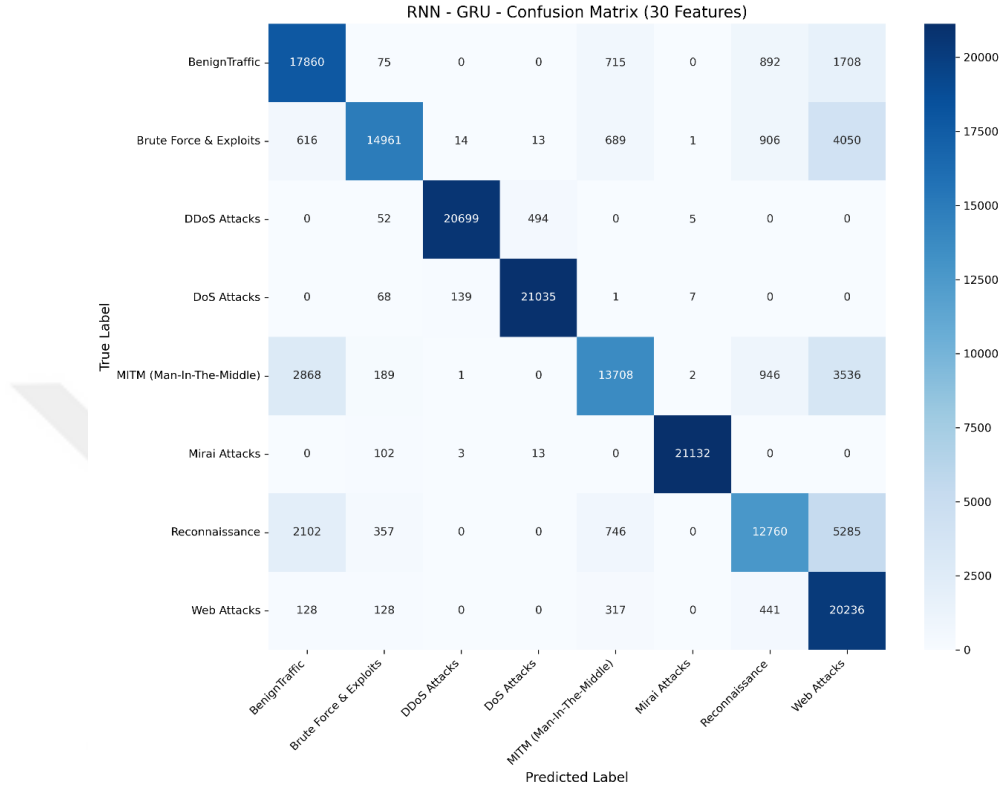
Çizelge 4.32. TSA modelinin 19 ve 30 özellik kullanılarak sınıf bazlı ulaştığı performans metriklerini sunmaktadır. Her iki yapı da yüksek doğruluk sağlamış, özellikle DDoS, DoS ve Mirai saldırılarında %99'un üzerinde başarı elde edilmiştir. Genel doğruluk, 19 özellikte %82.35, 30 özellikte ise %83.76 olarak gerçekleşmiştir.

Çizelge 4.32. TSA için performans metrikleri (19 ve 30 özellik)

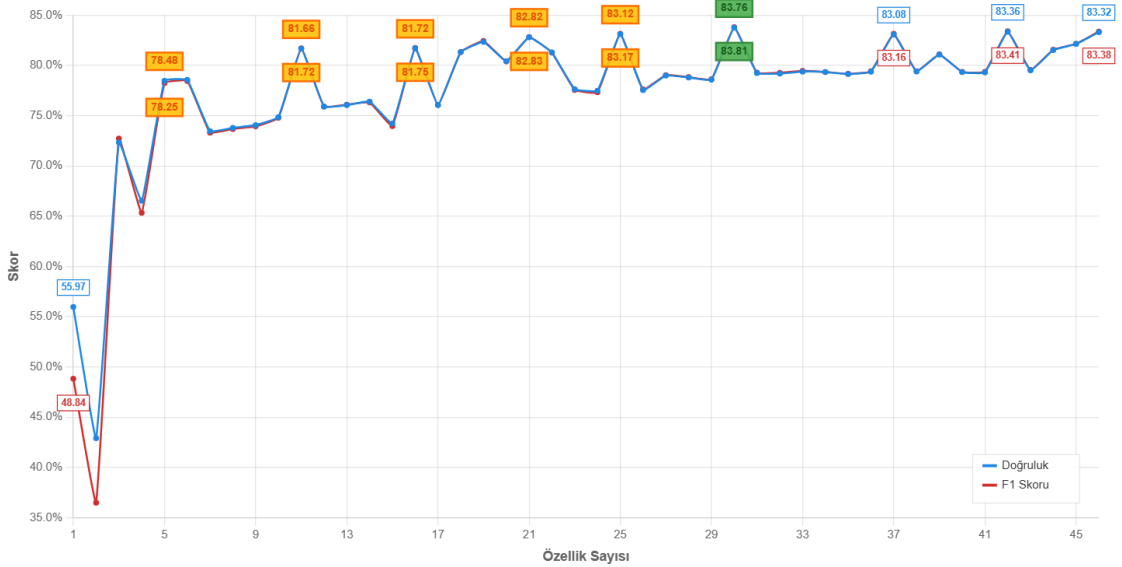
Özellik Sayısı	Sınıf	Doğruluk (%)	Kesinlik (%)	Duyarlılık (%)	F1 Skoru (%)
19	BenignTraffic	81.86	82.64	81.86	82.25
	Brute Force & Exploits	65.10	94.60	65.10	77.13
	DDoS Attacks	99.30	99.47	99.30	99.38
	DoS Attacks	99.33	99.53	99.33	99.43
	MITM	65.04	84.16	65.04	73.37
	Mirai Attacks	99.32	99.99	99.32	99.65
	Reconnaissance	52.78	86.29	52.78	65.47
	Web Attacks	96.10	85.28	96.10	90.36
	Doğruluk	82.35			
30	BenignTraffic	84.16	80.51	84.16	82.30
	Brute Force & Exploits	70.56	95.67	70.56	81.22
	DDoS Attacks	97.39	99.69	97.39	98.52
	DoS Attacks	99.01	98.01	99.01	98.51
	MITM	64.67	89.06	64.67	74.88
	Mirai Attacks	99.44	99.97	99.44	99.70
	Reconnaissance	60.12	84.95	60.12	70.41
	Web Attacks	95.21	86.36	95.21	90.57
	Doğruluk	83.76			

Şekil 4.69, 30 özellik kullanılarak eğitilen TSA modeline ait karmaşıklık matrisi sunulmaktadır. Model, DoS, DDoS ve Mirai saldırılarını yüksek doğrulukla sınıflandırırken; MITM ve özellikle Reconnaissance sınıflarında daha fazla hata yapmaktadır. Reconnaissance örneklerinin önemli bir kısmının Web Attacks olarak yanlış

sınıflandırılması, bu iki saldırı türü arasında benzerlikler olabileceğini göstermektedir. Genel olarak model, çoğu sınıfta başarılı sonuçlar vermiş, ancak bazı sınıflar arasında ayırım yapmakta zorlanmıştır.

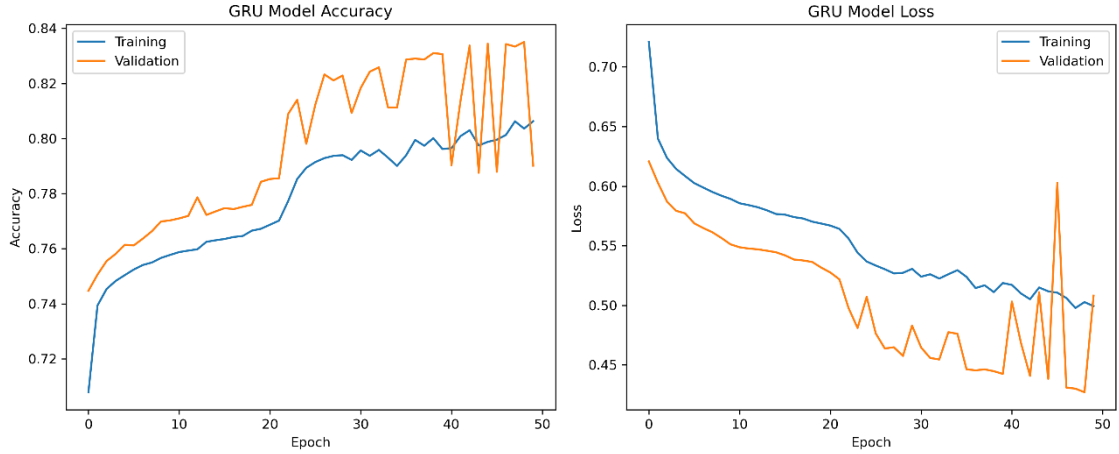


Şekil 4.69. TSA modeli sekiz sınıflı karmaşıklık matrisi (30 özellik)



Şekil 4.70. Özellik sayısına göre TSA modelinin doğruluk ve F1 skoru değişimi.

Şekil 4.70, TSA modelinin RO tabanlı özellik seçimine göre doğruluk ve F1 skoru performansını göstermektedir. Model, düşük başlangıç performansından sonra 11. özellikle birlikte %81.66 doğruluk ve %81.72 F1 skoru seviyesine ulaşmış, ardından dalgalı bir seyir izlemiştir. En yüksek performans 30. özellikle elde edilmiş olup doğruluk %83.76, F1 skoru ise %83.81 olarak kaydedilmiştir. Özellikle 25–42 özellik aralığında modelin istikrarlı bir şekilde yüksek performans sergilediği gözlemlenmiştir.



Şekil 4.71. TSA modelinin eğitim süreci: Doğruluk ve kayıp grafikleri (30 özellik)

Şekil 4.71, TSA modelinin eğitim sürecine ait doğruluk ve kayıp grafiklerini göstermektedir. Sol grafikte, eğitim doğruluğu zamanla istikrarlı bir şekilde artarak %81'e ulaşırken, doğrulama doğruluğu %80-84 aralığında dalgalanmakta ancak genel olarak daha yüksek seyretmektedir. Bu durum, modelin aşırı öğrenmeden kaçındığını ve genelleme yeteneğinin güçlü olduğunu göstermektedir. Sağ grafikte ise hem eğitim hem doğrulama kaybı azalma eğilimi göstermekte; eğitim kaybı yaklaşık 0.50'ye, doğrulama kaybı ise 0.43'e kadar düşmektedir. Dalgalanmalar, mini-batch optimizasyonuna bağlı olup genel eğilim, modelin etkili bir öğrenme süreci geçirdiğini ortaya koymaktadır.

4.2.2.11. Uzun Kısa Süreli Bellek (UKSB) algoritması sonuçları

Bu çalışmada, Uzun Kısa Süreli Bellek (UKSB) algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.33, UKSB modelinin farklı özellik sayılarıyla elde ettiği doğruluk ve F1 skoru değerlerini göstermektedir. En yüksek performans 42 özellik ile elde edilmiş olup, doğruluk %84.85, F1 skoru ise %84.87 olarak hesaplanmıştır.

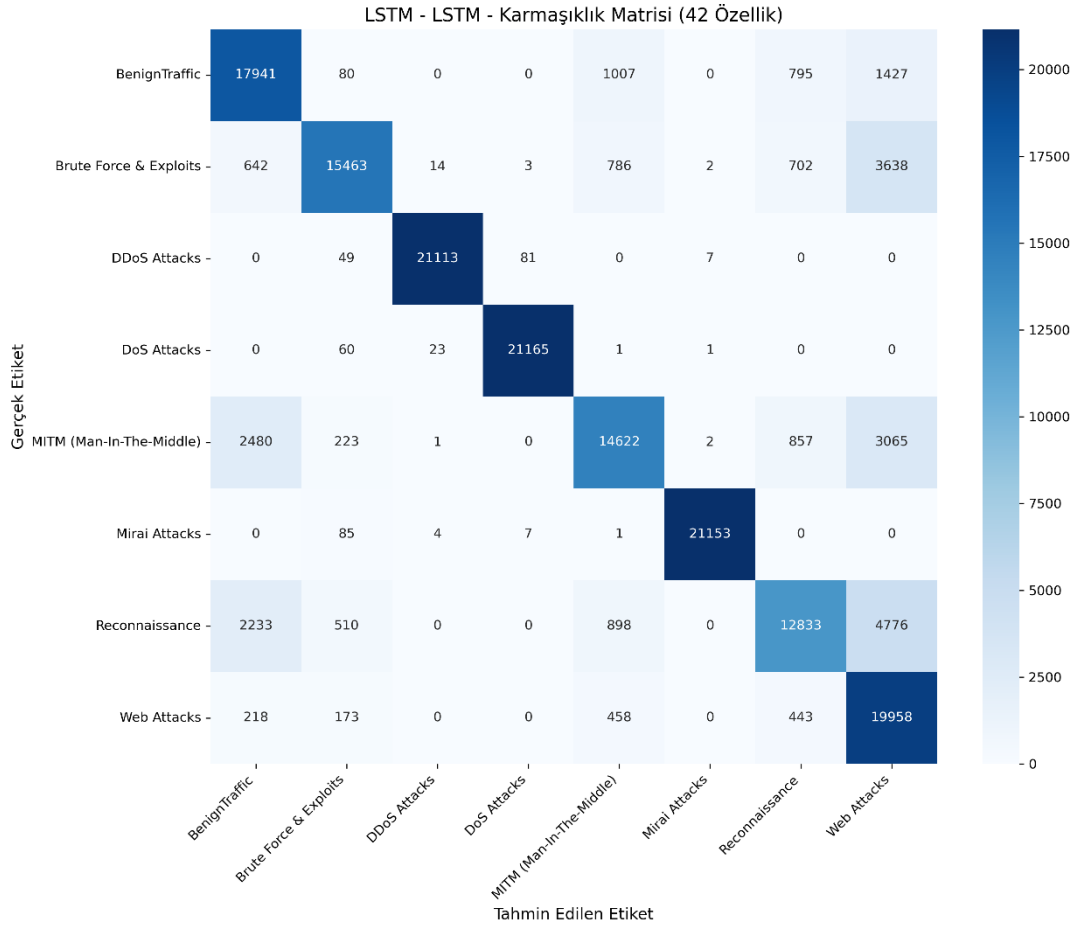
Çizelge 4.33. UKSB için önemli performans metrikleri

Özellik Sayısı	Doğruluk	F1 Skoru
1	0.5087	0.4557
2	0.6556	0.6497
4	0.7504	0.7545
6	0.7967	0.7957
8	0.8112	0.8112
10	0.8154	0.8150
12	0.8247	0.8248
14	0.8247	0.8252
18	0.8249	0.8251
20	0.8225	0.8228
27	0.8431	0.8437
33	0.8474	0.8477
38	0.8478	0.8479
42	0.8485	0.8487
46	0.8421	0.8427

Çizelge 4.34, UKSB modelinin 12 ve 42 özellik kullanılarak sınıf bazında gösterdiği performansı sunmaktadır. Her iki yapı da özellikle DDoS, DoS ve Mirai saldırılarında yüksek doğruluk sağlamıştır. Genel doğruluk 12 özellikte %82.47, 42 özellikte ise %84.55 olarak gerçekleşmiştir.

Çizelge 4.34. UKSB için performans metrikleri (12 ve 42 özellik)

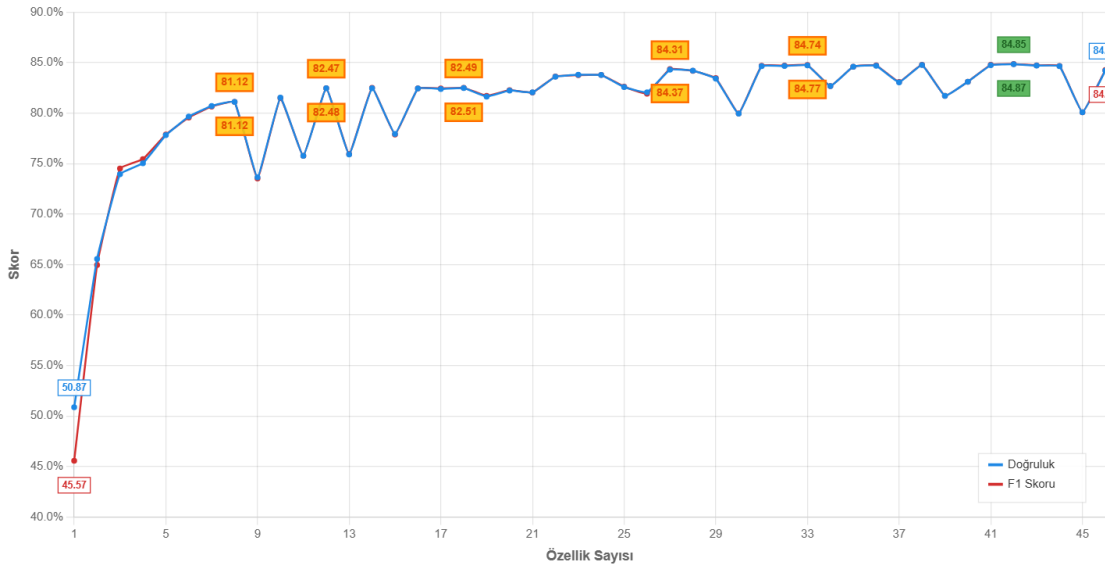
Özellik Sayısı	Sınıf	Doğruluk (%)	Kesinlik (%)	Duyarlılık (%)	F1 Skoru (%)
12	BenignTraffic	82.63	83.05	82.63	82.84
	Brute Force & Exploits	65.71	93.81	65.71	77.33
	DDoS Attacks	99.42	99.63	99.42	99.53
	DoS Attacks	99.52	99.59	99.52	99.56
	MITM	65.85	86.22	65.85	74.67
	Mirai Attacks	99.37	99.97	99.37	99.67
	Reconnaissance	54.12	84.83	54.12	66.04
	Web Attacks	93.18	86.18	93.18	89.54
	Doğruluk	82.47			
42	BenignTraffic	84.41	83.59	84.41	84.00
	Brute Force & Exploits	72.73	93.29	72.73	81.77
	DDoS Attacks	99.33	99.80	99.33	99.57
	DoS Attacks	99.60	99.58	99.60	99.59
	MITM	68.76	86.51	68.76	76.64
	Mirai Attacks	99.54	99.95	99.54	99.75
	Reconnaissance	60.46	86.44	60.46	71.14
	Web Attacks	93.84	85.82	93.84	89.66
	Doğruluk	84.85			



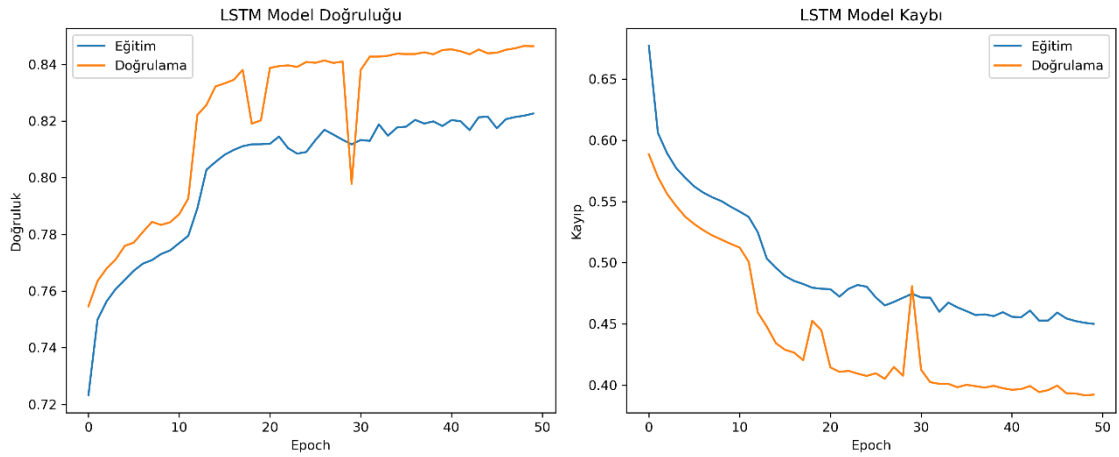
Şekil 4.72. UKSB modeli sekiz sınıflı karmaşıklık matrisi (42 özellik)

Şekil 4.72, 42 özellik kullanılarak eğitilen UKSB modeline ait karmaşıklık matrisini göstermektedir. Model, DoS, DDoS ve Mirai saldırılarını yüksek doğrulukla sınıflandırırken; MITM ve Reconnaissance gibi sınıflarda daha fazla hata yapmıştır. Özellikle MITM örneklerinin BenignTraffic ve Web Attacks, Reconnaissance örneklerinin ise yine BenignTraffic ve Web Attacks ile karıştırıldığı görülmektedir. Ayrıca Brute Force & Exploits sınıfı da Web Attacks ile sıkça karıştırılmıştır. Bu karışıklıklar, bazı saldırı türleri arasında benzer veri desenleri bulunduğuna işaret etmektedir. Genel olarak model, belirli saldırı türlerinde güçlü performans sergilerken, bazı sınıflar arasında ayırım yapmakta zorlanmaktadır.

Şekil 4.73, UKSB modelinin RO tabanlı özellik seçimine göre doğruluk ve F1 skoru performansını göstermektedir. Model, başlangıçta %50.87 seviyesindeyken, 8. özellikte %81.12, 12. özellikte %82.47 doğruluğa ulaşmıştır. En yüksek başarı, %84.85 doğruluk ve %84.87 F1 skoru ile 42. özellikte elde edilmiştir.



Şekil 4.73. Özellik sayısına göre UKSB modelinin doğruluk ve F1 skoru değişimi.



Şekil 4.74. UKSB modelinin eğitim süreci: Doğruluk ve kayıp grafikleri (42 özellik)

Şekil 4.74, UKSB modelinin eğitim sürecine ait doğruluk ve kayıp grafiklerini göstermektedir. Eğitim doğruluğu %72'den başlayarak %82'ye kadar yükselmiş; doğrulama doğruluğu ise ilk 15 epoch'ta hızlı bir artışla %85 seviyelerine ulaşmış ve bu düzeyde dengelenmiştir. Eğitim kaybı 0.67'den 0.45'e, doğrulama kaybı ise 0.59'dan 0.39'a kadar azalmıştır. 20. ve 30. epoch'lardaki ani değişimler, mini-batch ve örneklemeye bağlı geçici dalgalanmalardır. Genel olarak model, istikrarlı öğrenme ve iyi genelleme performansı göstermektedir.

4.2.3. Otuz dördlü sınıflandırma sonuçları

Makine öğrenmesi tabanlı ağ trafiği analizi, günümüzde siber güvenlikte büyük bir öneme sahiptir. Özellikle, saldırı tespiti için kullanılan ikili sınıflandırma algoritmaları, ağ trafiğini zararlı (AttackTraffic) ve zararsız (BenignTraffic) olarak ayırarak saldırılara karşı daha hızlı ve güvenilir tespit mekanizmaları sunmaktadır.

Çizelge 4.35, 34 sınıflı veri setiyle elde edilen sınıflandırma sonuçlarını göstermektedir. RO, GA ve AGA algoritmaları yüksek doğruluk ve F1 skoru ile öne çıkarken, NB ve LR'nin performansı daha düşüktür. En iyi sonuç, %95'in üzerindeki başarıyla RO algoritmasında elde edilmiştir.

Çizelge 4.35. Algoritmaların 34 sınıflı performans ve özellik seçimi karşılaştırması.

ALGORITMA	ÖZELLİK SAYISI	EN YÜKSEK DOĞRULUK	F1 SKORU
LR	32	0.550171	0.533159
NB	34	0.483982	0.444524
KEYK	1	0.882659	0.879556
KA	37	0.889418	0.894542
RO	26	0.954394	0.953743
GA	20	0.924559	0.924241
AGA	34	0.936147	0.935615
YSA	45	0.725194	0.722985
ESA	16	0.698488	0.681859
TSA	37	0.796171	0.797565
UKSB	46	0.7994	0.8004

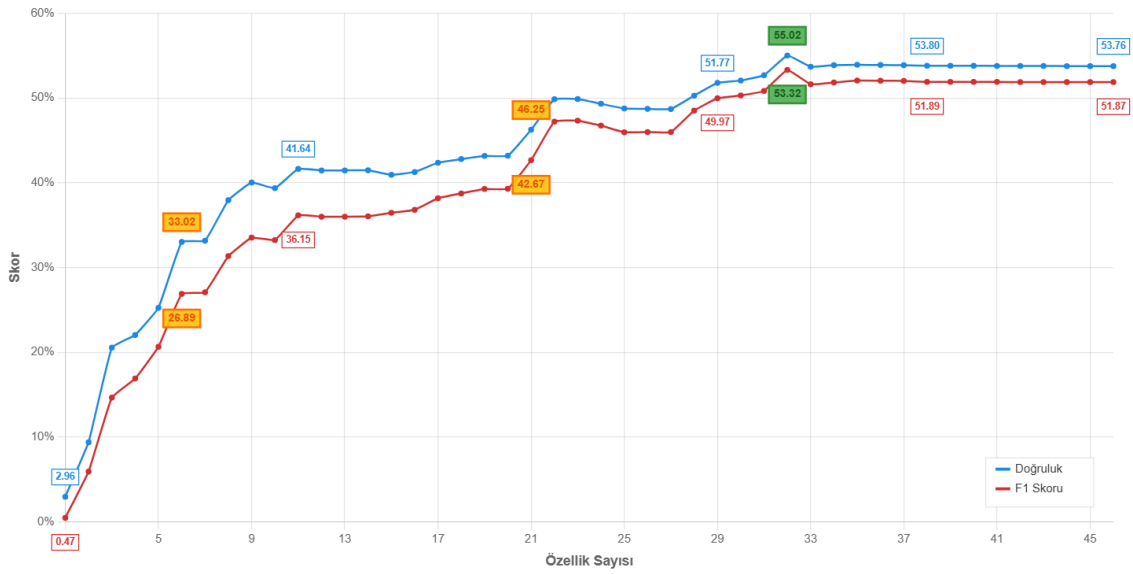
4.2.3.1. Lojistik Regresyon (LR) algoritması sonuçları

Bu çalışmada, Lojistik Regresyon algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.36, LR modelinin özellik sayısına göre performansını göstermektedir. En iyi sonuç 32 özellikle elde edilmiş (%55.01 doğruluk, %53.32 F1 skoru) olup, modelin genel performansı sınırlı kalmıştır.

Çizelge 4.36. LR için önemli performans metrikleri

Özellik Sayısı	Doğruluk	F1 Skoru
1	0.029600	0.004742
5	0.252447	0.206490
10	0.393518	0.332390
15	0.409300	0.364526
20	0.431835	0.392854
25	0.487618	0.459570
30	0.520482	0.502969
32	0.550171	0.533159
35	0.539106	0.520560
40	0.537965	0.518950
46	0.537594	0.518683

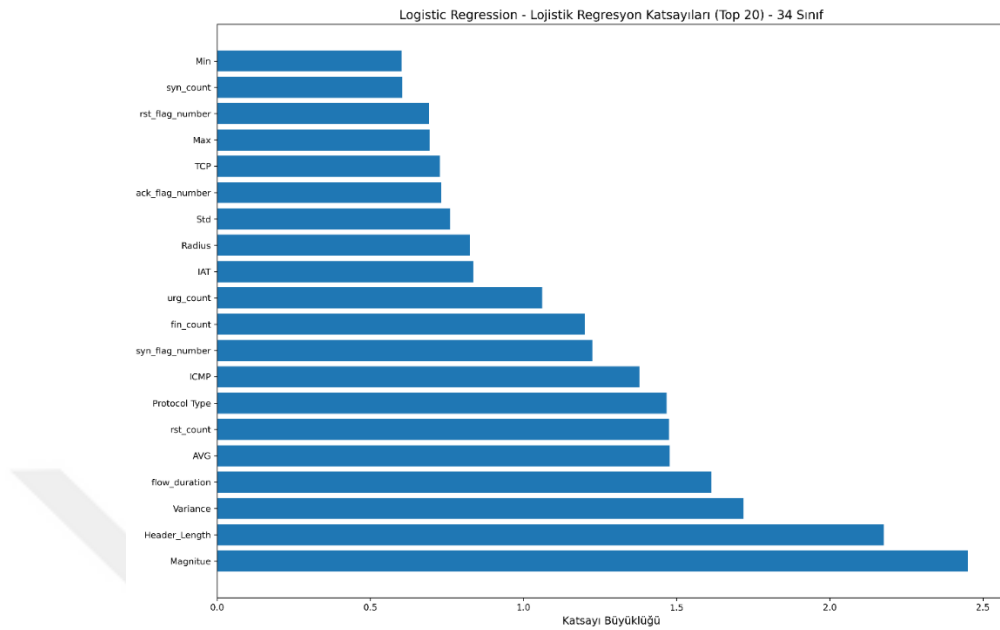


Şekil 4.75. Özellik sayısına göre LR modelinin doğruluk ve F1 skoru değişimi.

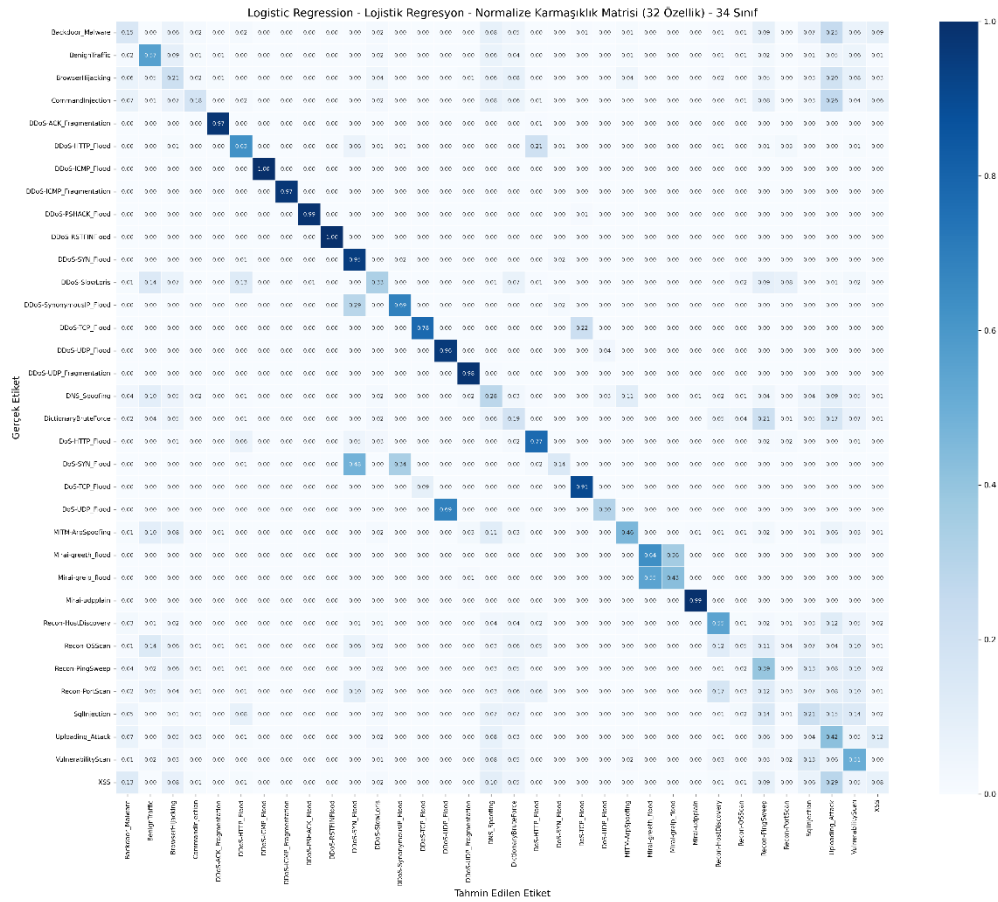
Şekil 4.75, LR modelinin kademeli özellik eklenmesiyle elde ettiği doğruluk ve F1 skoru performansını göstermektedir. Model, başlangıçta %2,96 gibi çok düşük bir doğrulukla başlamış; 13. özelliğe %41,64'e, 32. özelliğe ise en yüksek değerlere ulaşmıştır (%55,02 doğruluk, %53,32 F1 skoru). Bu noktadan sonra performans sabitlenmiş ve hafif bir düşüş göstermiştir. LR modeli, genel olarak %50–55 bandında seyreden sınırlı bir başarı sunmuş, diğer algoritmalarla kıyasla düşük performans sergilemiştir.

Şekil 4.76'da Lojistik Regresyon modeli için en etkili 20 özellik katsayı büyüklüğüne göre sıralanmıştır. Grafik incelendiğinde, Magnitude, Header_Length ve Variance özelliklerinin modelde en fazla etkiye sahip olduğu görülmektedir. Flow_duration, AVG ve Protocol Type orta düzeyde katkı sağlarken, Min ve syn_count gibi bazı özelliklerin etkisi daha düşüktür. Bu dağılım, 34 sınıf üzerinden yapılan

sınıflandırmada hangi özelliklerin daha belirleyici olduğunu net şekilde ortaya koymaktadır.

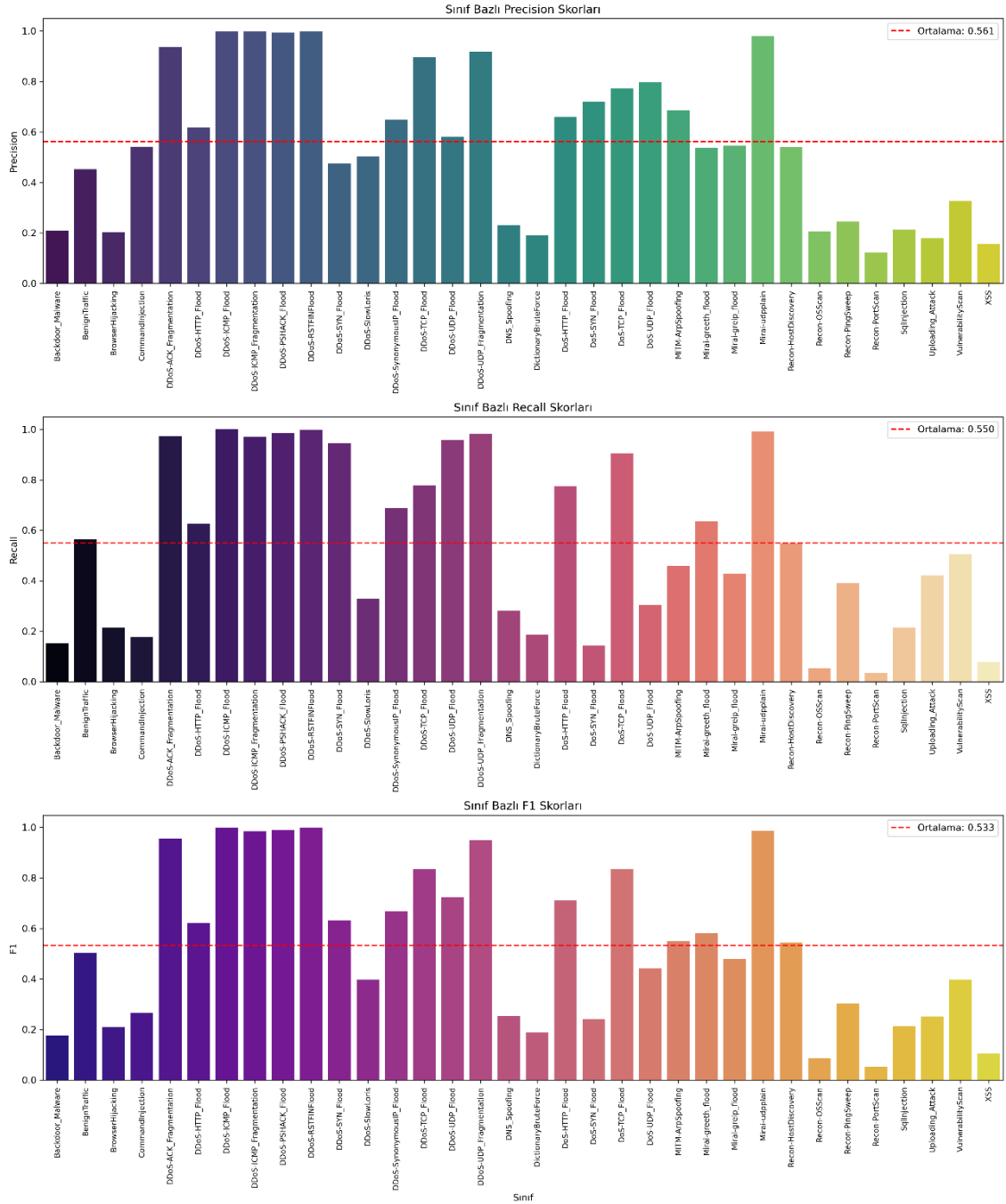


Şekil 4.76. LR modeli için en etkili 20 özelliğin önem skorları



Şekil 4.77. LR modeline ait karmaşıklık matrisi (32 Özellik, 34 Sınıf)

Şekil 4.77, 32 özellikli LR modelinin karmaşıklık matrisini göstermekte olup, %55.02 doğruluk ve %53.32 F1 skoru ile en iyi performansın bu modelde elde edildiğini ortaya koymaktadır. Karmaşıklık matrisine göre, model 34 sınıfın bazılarında yüksek doğruluk sağlarken, bazı sınıflarda daha düşük başarı göstermiştir.



Şekil 4.78. LR modelinin 32 özellikle sınıf bazlı Kesinlik, Duyarlılık ve F1 skorları.

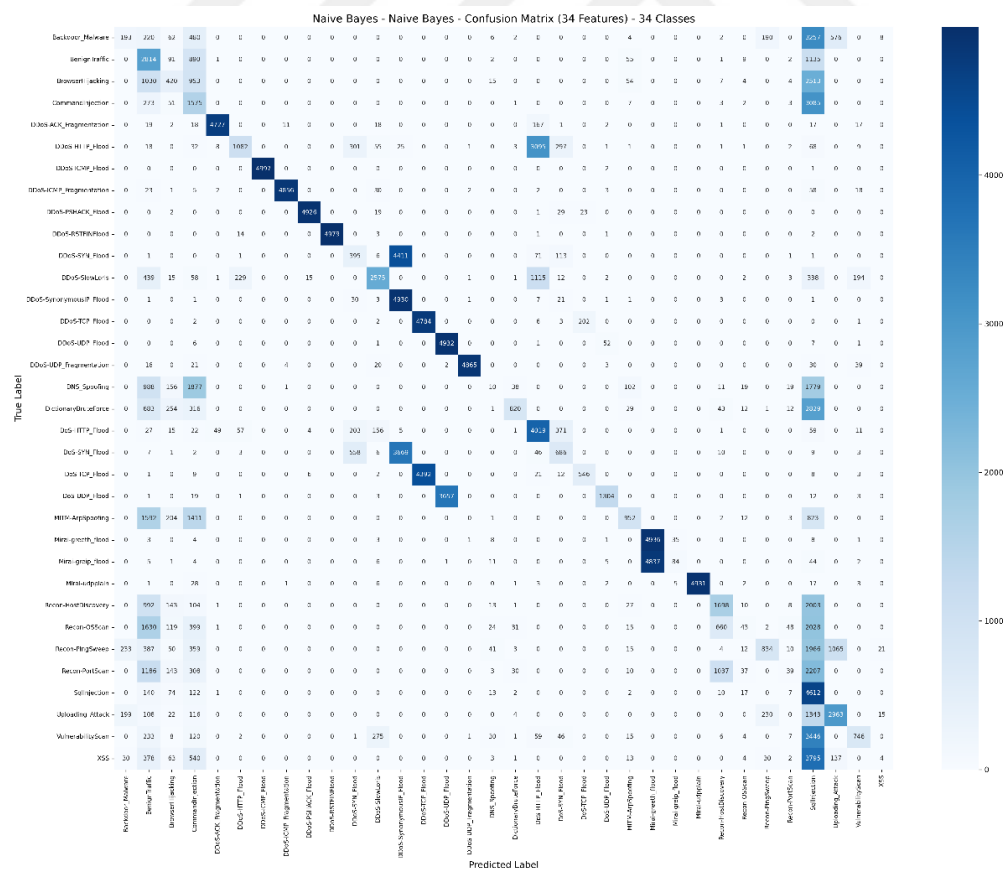
Şekil 4.78, 32 özellikli LR modelinin 34 sınıfa ait ortalama kesinlik, duyarlılık ve F1 skorlarını sırasıyla 0.561, 0.550 ve 0.533 olarak göstermektedir. Model, DDoS türlerinde yüksek başarı sergilerken, XSS, Backdoor_Malware ve BruteForceHacking

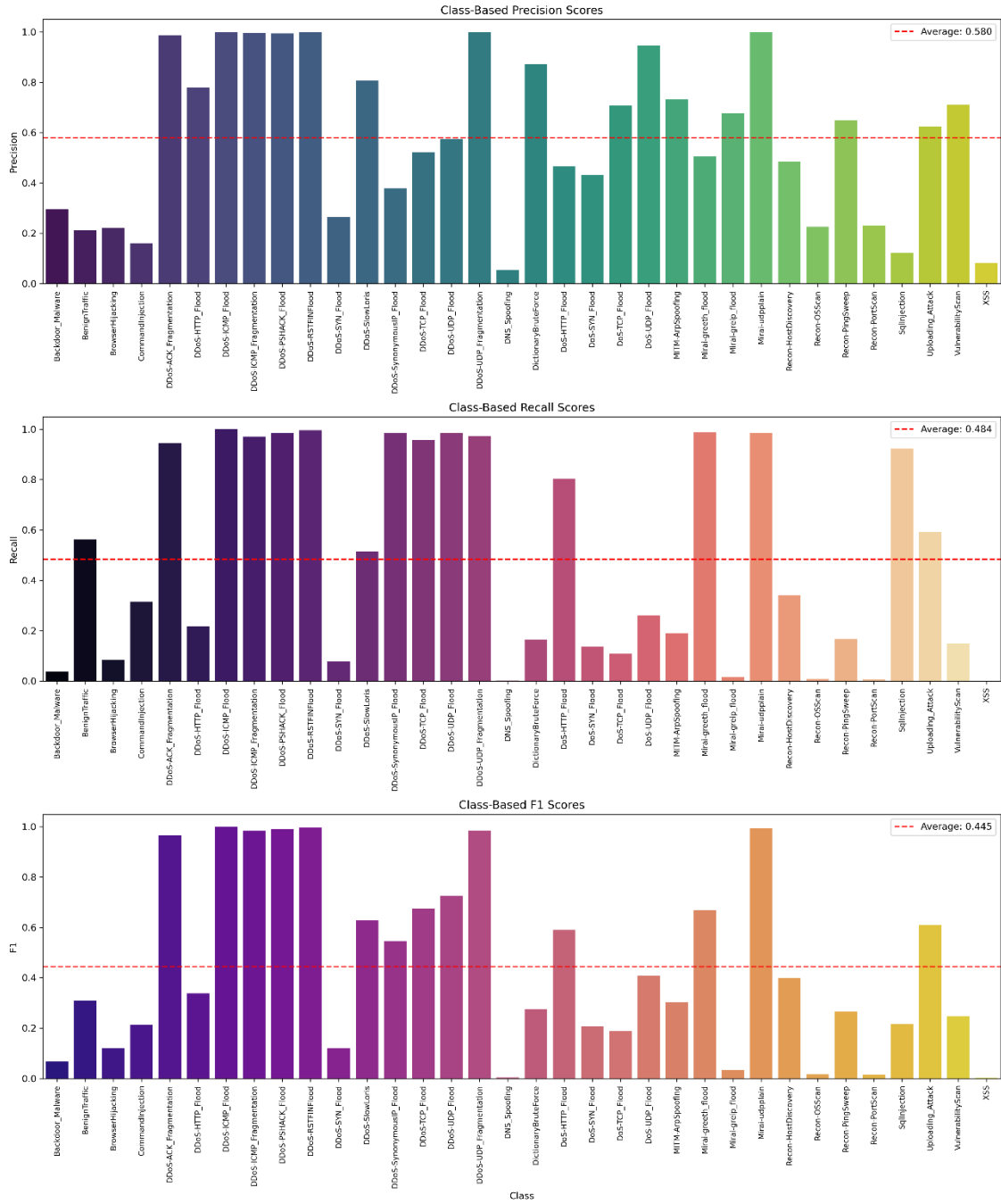
gibi sınıflarda düşük performans göstermiştir. Performans farkları, sınıf dengesizliği veya ayırt edici özellik eksikliğinden kaynaklanabilir. Genel olarak model, çok sınıflı ayırmda makul bir başarı düzeyi sunmaktadır.

4.2.3.2. Naive Bayes (NB) algoritması sonuçları

Bu çalışmada, NB algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Şekil 4.79, 34 özellikli NB modelinin 34 sınıf için tahmin performansını gösteren karmaşıklık matrisini sunmakta ve modelin %48.39 doğruluk, %44.45 F1 skoru ile en iyi sonucunu bu özellik sayısında verdiğini ortaya koymaktadır. Köşegendeki koyu mavi hücreler doğru tahminleri, köşegen dışındakiler ise yanlış sınıflandırmaları yansıtmaktadır. Bazı sınıflarda yüksek doğruluk sağlanırken, bazı sınıflarda karışıklık gözlenmiştir.





Şekil 4.80. NB modelinin 34 özelliikle sınıf bazlı Kesinlik, Duyarlılık ve F1 skorları.

Şekil 4.80, 34 özellikli NB modelinin 34 sınıf için kesinlik, duyarlılık ve F1 skorlarını göstermekte olup, ortalama değerler sırasıyla 0.580, 0.484 ve 0.445'tir. Model, "DDoS-ICMP_Flood", "DDoS-UDP_Flood" gibi DDoS sınıflarında yüksek performans sergilerken, "XSS", "Backdoor_Malware" gibi sınıflarda düşük başarı göstermektedir. Bazı sınıflarda kesinlik ve duyarlılık arasında belirgin farklar bulunmakta, bu da yanlış pozitif veya negatif oranlarının yüksekliğini göstermektedir. Genel olarak model, 0.445 F1 skoru ile 34 özellikli yapısının etkili olduğunu ortaya koymaktadır.

Çizelge 4.37, NB modelinin farklı özellik sayılarıyla elde ettiği performansı göstermektedir. En yüksek doğruluk (%48.39) ve F1 skoru (%44.45) 34 özellikle elde edilmiş, genel olarak modelin başarı düzeyi düşük kalmıştır.

Çizelge 4.37. NB için önemli performans metrikleri

Özellik Sayısı	Doğruluk	F1 Skoru
1	0.059653	0.013912
5	0.249324	0.200967
10	0.396388	0.345172
11	0.395571	0.355872
15	0.373453	0.337378
20	0.383694	0.343719
25	0.449653	0.404693
30	0.468082	0.425483
34	0.483982	0.444524
40	0.478912	0.420262
45	0.479424	0.420543

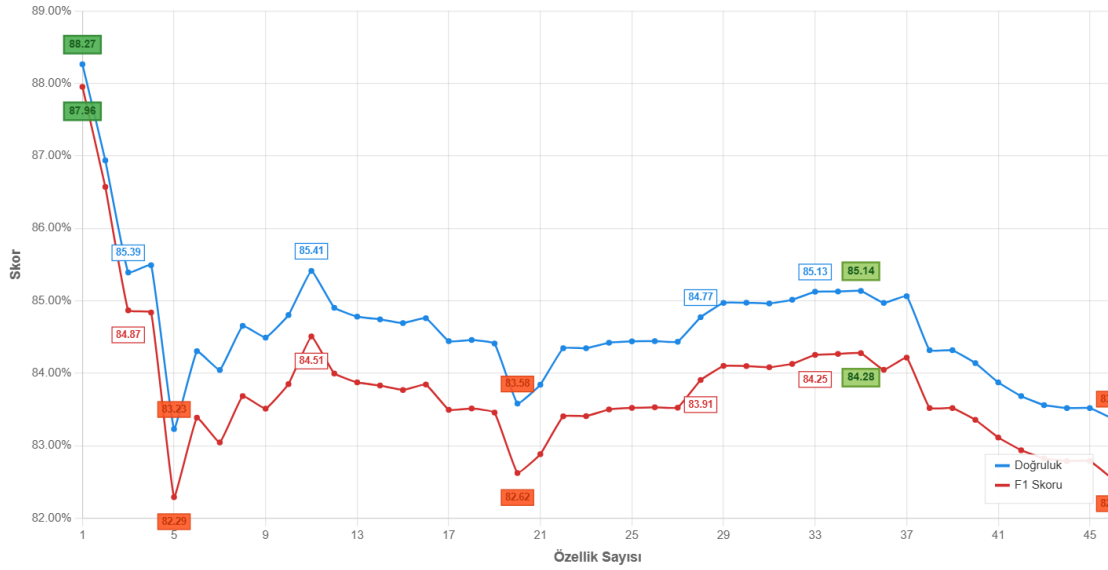
4.2.3.3. K En Yakın Komşu (KEYK) algoritması sonuçları

Bu çalışmada, K-En Yakın Komşu (KEYK) algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.38, LR modelinin farklı özellik ve komşu sayılarıyla elde ettiği performansı göstermektedir. En iyi sonuç %88.27 doğruluk ve %87.96 F1 skoru ile 1 özellikle elde edilmiştir

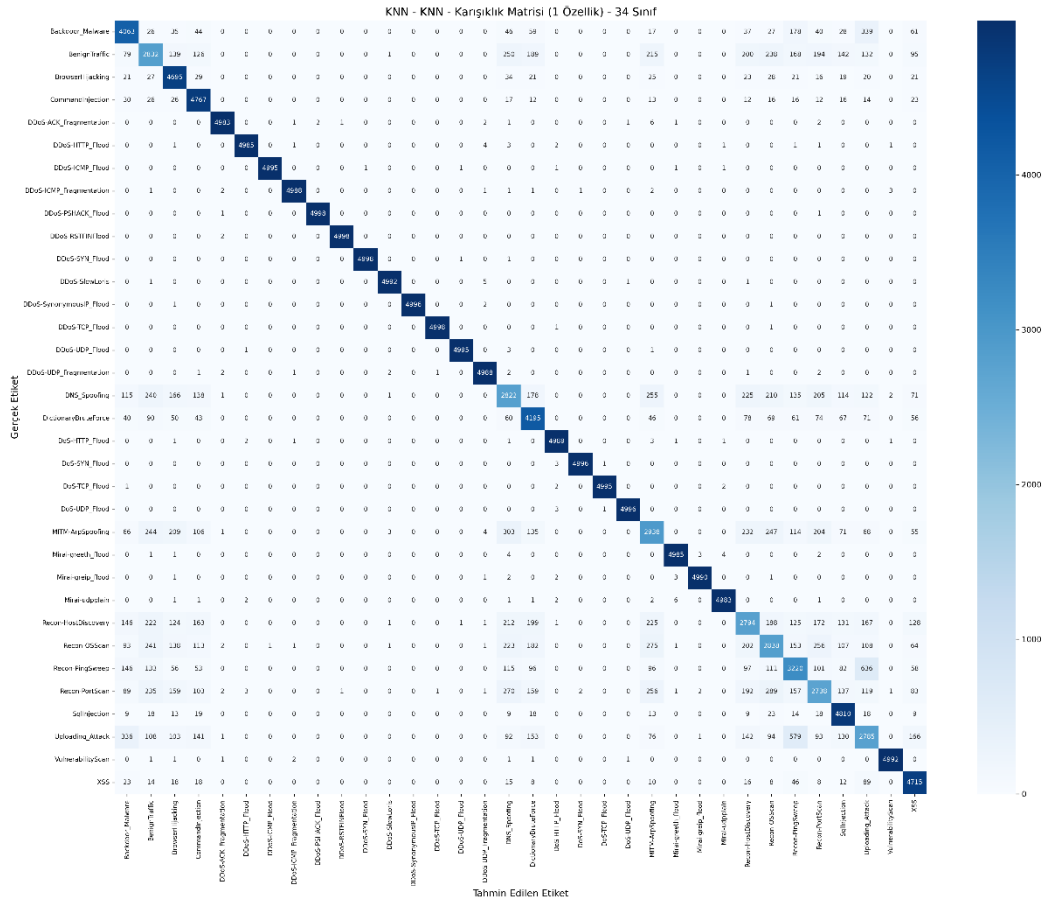
Çizelge 4.38. LR için önemli performans metrikleri

Özellik Sayısı	Komşu Sayısı	Doğruluk	F1 Skoru
1	5	0.882659	0.879556
5	5	0.832294	0.822898
10	5	0.848035	0.838512
15	5	0.846918	0.837693
20	5	0.835812	0.826237
25	5	0.844406	0.835216
30	5	0.849741	0.840999
35	5	0.851376	0.842779
36	7	0.849706	0.840471
40	5	0.841400	0.833570
45	5	0.835200	0.827885
46	9	0.833718	0.825388



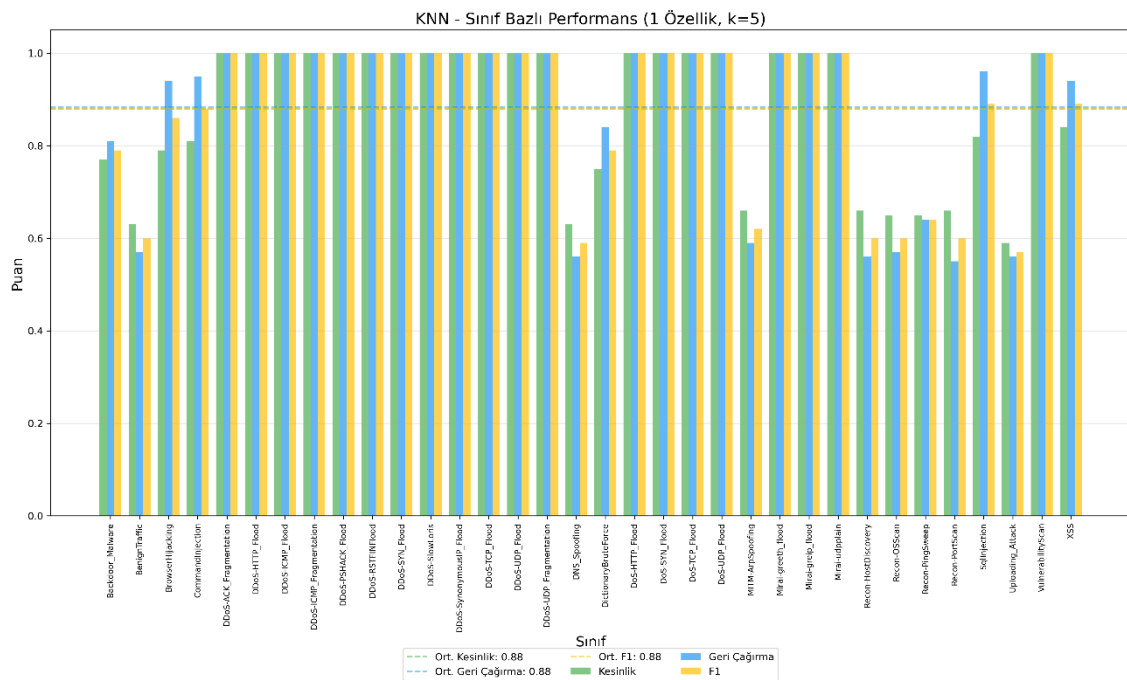
Şekil 4.81. Özellik sayısına göre K-En Yakın Komşu (KEYK) modelinin doğruluk ve F1 skoru değişimi.

Şekil 4.81’de, KEYK modelinin doğruluk ve F1 skorunun ilk birkaç özellikte yüksek olduğu, ancak özellik sayısı arttıkça performansın dalgalanarak az da olsa düştüğü görülmektedir. Bu durum, modelin az sayıda özellikte daha verimli çalıştığını göstermektedir.



Şekil 4.82. K-En Yakın Komşu (KEYK) modeline ait karmaşıklık matrisi (1 Özellik, 34 Sınıf)

Şekil 4.82, KEYK modelinin %88.27 doğrulukla en iyi performansı 1 özellikli modelde gösterdiğini ortaya koymaktadır. Model, DoS ve DDoS gibi sınıflarda yüksek başarı sağlarken, benzer özelliklere sahip saldırı türleri arasında (örneğin MITM-ArpSpoofing ile Recon türleri) karışıklıklar gözlenmiştir. Bu da KEYK modelinin benzer davranışlı saldırılar arasında ayırım yapmada zorlandığını göstermektedir.

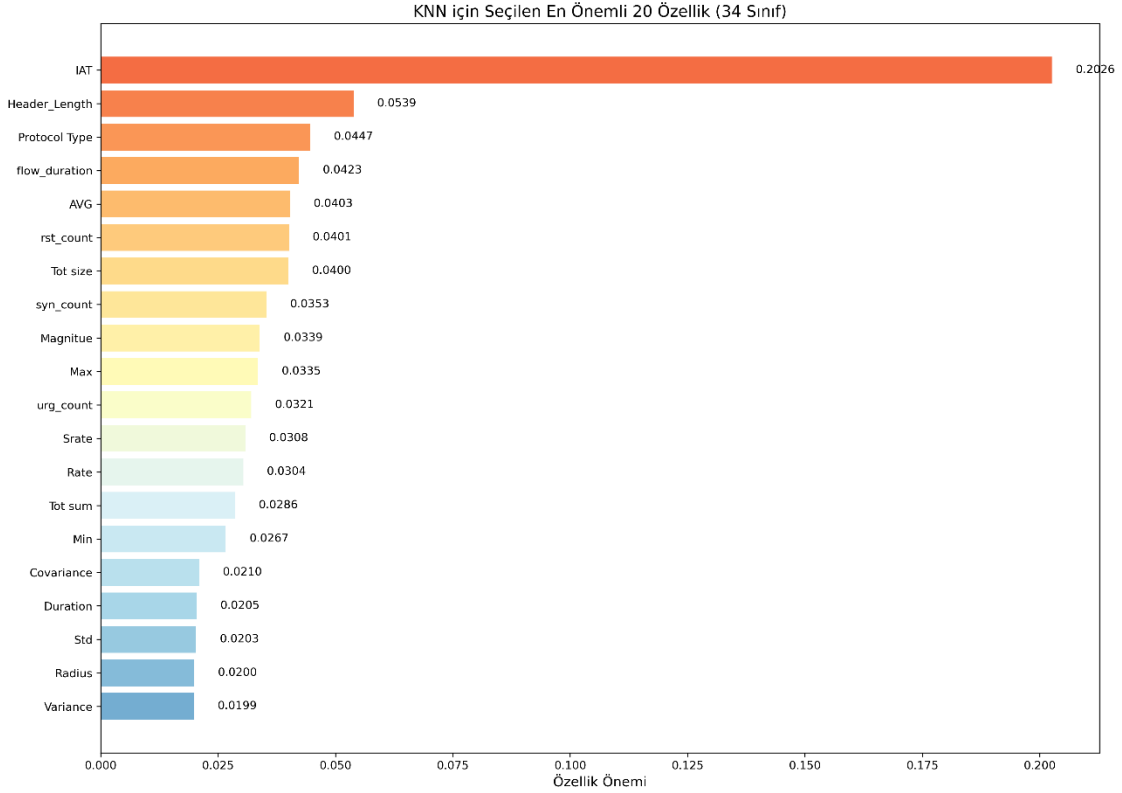


Şekil 4.83. KEYK modelinin sınıf bazlı 1 özellikli Precision, Recall ve F1 skorları.

Şekil 4.83, KEYK modelinin yalnızca IAT özelliği ve $k=5$ komşu sayısı ile 34 sınıf üzerindeki performansını göstermekte olup, DoS ve DDoS saldırılarında neredeyse kusursuz sonuçlar elde edildiğini ortaya koymaktadır. CommandInjection, SQL_Injection ve VulnerabilityScan gibi sınıflarda ortalamanın üzerinde performans görülürken, BenignTraffic, Backdoor_Malware, DNS_Spoofing, MITM-ArpSpoofing ve Recon saldırılarında başarı düşmüştür. Bazı sınıflarda kesinlik ve geri çağırma arasında belirgin farklılıklar bulunmakta, bu da hata türlerinin değişkenlik gösterdiğini göstermektedir. Genel ortalama kesinlik, geri çağırma ve F1 skoru 0.88 olup, IAT özelliğinin DoS/DDoS tespitinde etkili, ancak karmaşık saldırı türlerinde sınırlı olduğunu göstermektedir.

Şekil 4.84, KEYK modelinde en etkili 20 özelliği sıralamakta olup, IAT özelliği açık ara en yüksek öneme (0.2026) sahiptir ve diğer tüm özelliklerden belirgin şekilde ayrılmaktadır. Header_Length, Protocol_Type ve flow_duration gibi özellikler daha düşük önem değerleriyle onu takip etmektedir. Korelasyon analiziyle yüksek ilişki

gösteren AVG, Magnitude ve Tot_size ise önem sıralamasında beklenenden daha alt sıralarda yer almıştır. Özellikle Magnitude ve Max gibi özelliklerin orta düzey öneme sahip olması, model başarısının büyük ölçüde IAT özelliğine bağlı olduğunu göstermektedir. Bu bulgular, KEYK modelinde tek bir güçlü özellik seçiminin performans üzerinde belirleyici etkisi olduğunu ortaya koymaktadır.



Şekil 4.84. KEYK modeli için en etkili 20 özelliğin önem skorları

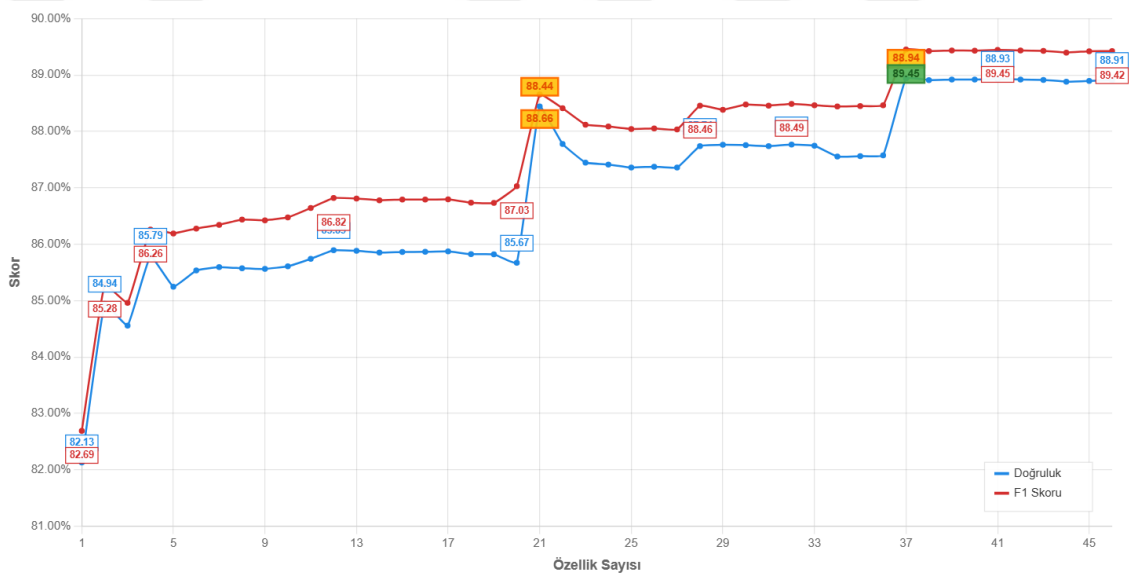
4.2.3.4. Karar Ağacı (KA) algoritması sonuçları

Bu çalışmada, KA algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.39, KA modelinin özellik sayısına göre performansını göstermektedir. En yüksek doğruluk (%89.41) ve F1 skoru (%89.45), 37 özellikle elde edilmiştir. Model genel olarak yüksek ve dengeli bir başarı sergilemiştir.

Çizelge 4.39. KA için önemli performans metrikleri

Özellik Sayısı	Doğruluk	F1 Skoru
1	0.821282	0.826892
2	0.849424	0.852832
3	0.845553	0.849600
4	0.857929	0.862597
5	0.852465	0.861913
10	0.856076	0.864747
15	0.858618	0.867925
20	0.856694	0.870304
25	0.873594	0.880433
30	0.877765	0.884768
35	0.875618	0.884497
37	0.889418	0.894542
40	0.889194	0.894328
45	0.889065	0.894231
46	0.889094	0.894245

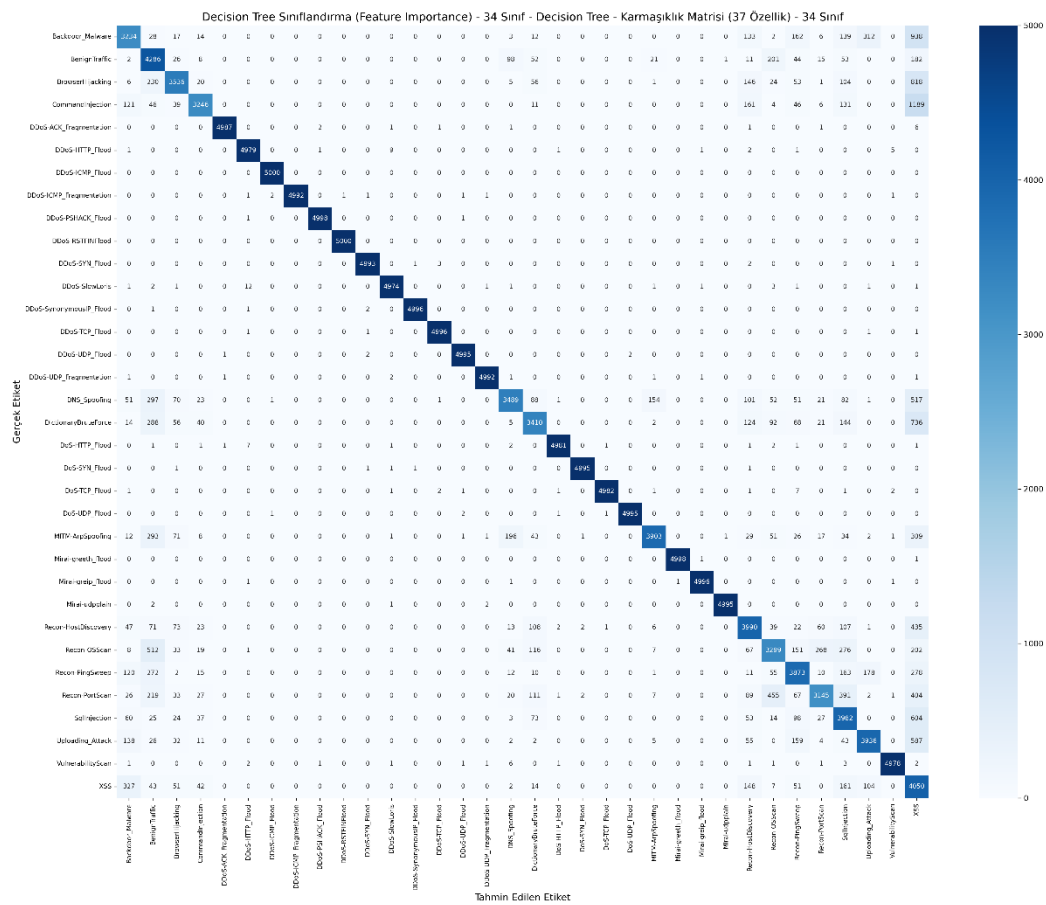


Şekil 4.85. Özellik sayısına göre KA modelinin doğruluk ve F1 skoru değişimi.

Şekil 4.85, KA modelinin en yüksek önem sırasına göre kademeli olarak özellik eklenmesiyle elde ettiği doğruluk ve F1 skoru performansını göstermektedir. Model, başlangıçta %82,13 doğruluk ile düşük bir performans sergilemiş; 12. özelliikle %85,89'a, 21. özelliikle ise %88,44'e ulaşmıştır. 37. özelliikle birlikte doğruluk %88,94'e, F1 skoru ise %89,45'e yükselerek en yüksek değerlere ulaşmıştır. Bu noktadan sonra performansın sabitlenme eğiliminde olduğu gözlemlenmiştir. Dolayısıyla, optimum başarı ve verimlilik için 37–40 arası özellik sayısının yeterli olduğu söylenebilir.

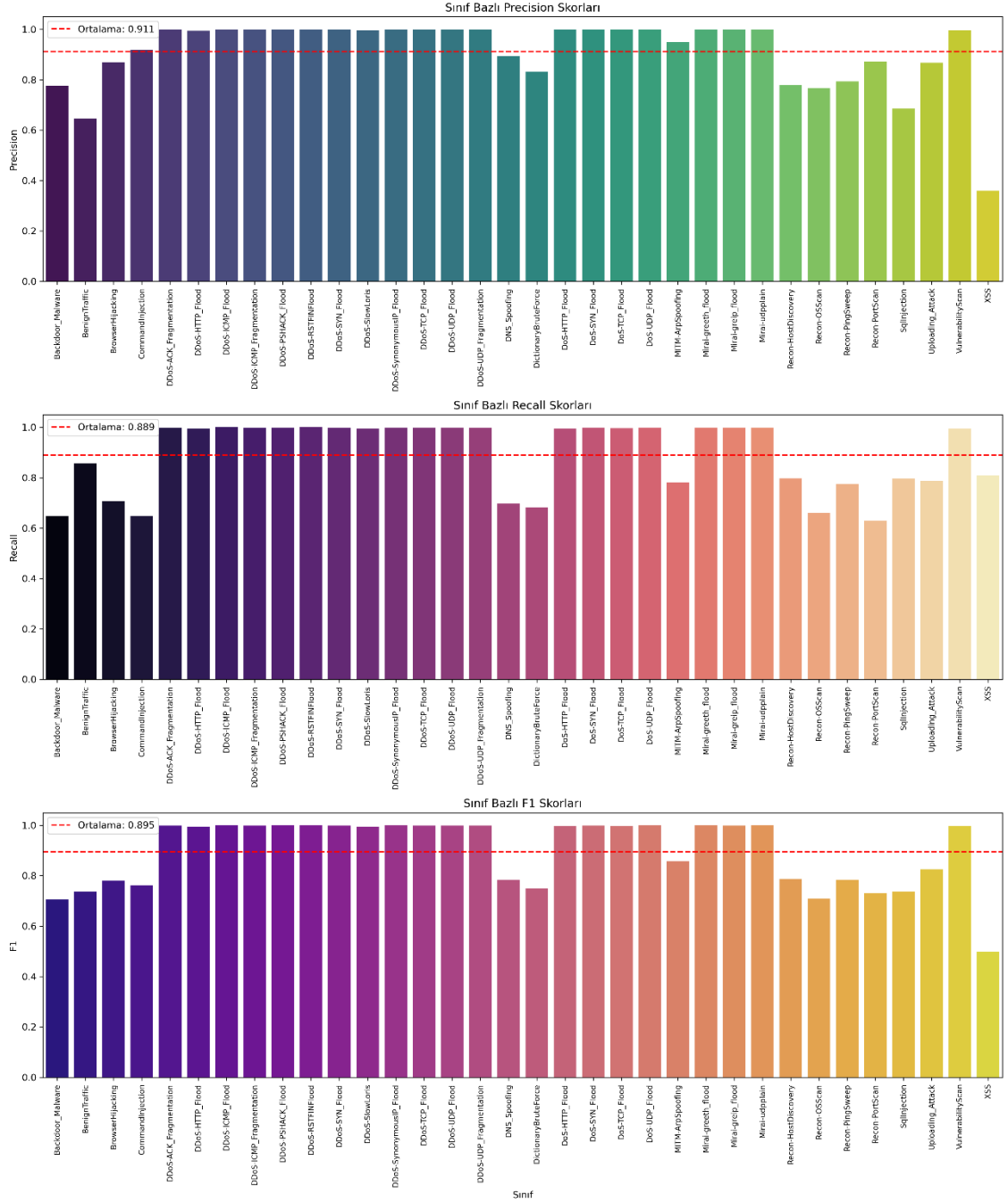
Şekil 4.86, 37 özellikli KA modelinin %88.94 doğruluk ve %89.45 F1 skoru ile siber saldırı sınıflandırmasında başarılı bir performans sergilediğini göstermektedir. Model, özellikle DoS ve DDoS türlerinde yüksek doğrulukla sınıflandırma yaparken,

Recon grubu ve web tabanlı saldırılarda (özellikle SqlInjection, Uploading_Attack ve XSS) belirgin karışmalar gözlemlenmiştir. Recon-PortScan ve MITM-ArpSpoofing gibi benzer davranışlı sınıflar arasında sınıflandırma zorlukları yaşanmış; DNS_Spoofing ve DictionaryBruteForce gibi bazı sınıflar da birbirine karıştırılmıştır. Bu bulgular, KA modelinin özellikle belirgin örüntülere sahip saldırıları ayırt etmede etkili, ancak benzer yapılı ve karmaşık saldırılar arasında ayırım yapmada sınırlı olduğunu ortaya koymaktadır.



Şekil 4.86. KA modeline ait karmaşıklık matrisi (37 Özellik, 34 Sınıf)

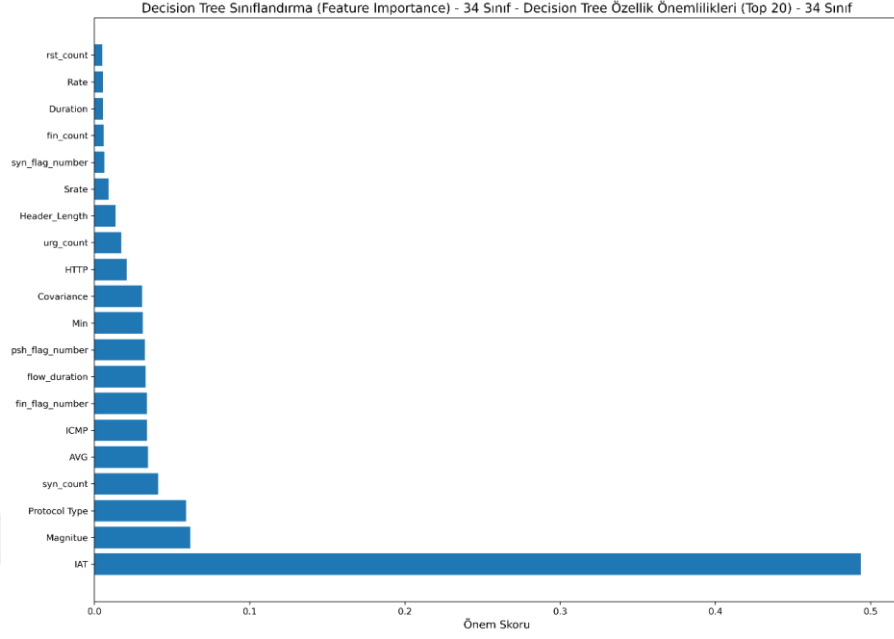
Şekil 4.87, 37 özellikli KA modelinin ortalama %89.5 F1 skoru ile iyi bir sınıflandırma performansı sunduğunu göstermektedir. Model, DDoS saldırılarında yüksek başarı sağlarken, Recon ve bazı web tabanlı saldırılarda (örneğin XSS, Backdoor_Malware) duyarlılık değerleri düşmüş ve yanlış sınıflandırmalar artmıştır. Kesinlik ve duyarlılık arasındaki farklar, bazı sınıflarda hatalı tahminlerin yoğunlaştığını göstermektedir. Bu sonuçlar, modelin genel olarak etkili olmakla birlikte karmaşık saldırı türlerinde sınırlı kaldığını ortaya koymaktadır.



Şekil 4.87. KA modelinin 37 özellikle sınıf bazlı Kesinlik, Duyarlılık ve F1 skorları.

Şekil 4.88, KA modelinde IAT özelliğinin açık ara en yüksek öneme (~ 0.48) sahip olduğunu göstermekte; Magnitude ve Protocol Type gibi diğer öznitelikler ise çok daha düşük katkılar sunmaktadır. syn_count, AVG, ICMP ve flow_duration gibi öznitelikler orta düzeyde önem taşıırken, Header_Length, Rate ve rst_count gibi değişkenler düşük önemde yer almıştır. IAT'nin diğer tüm özelliklerin toplamından daha fazla etki sağlaması, bu değişkenin siber saldırıların tespitinde kritik bir rol oynadığını ortaya koymaktadır. Benzer şekilde diğer algoritalarda da IAT'nin yüksek önem taşıması, bu

özniteliğin siber güvenlik sınıflandırmalarında genel olarak ayırt edici bir unsur olduğunu göstermektedir.



Şekil 4.88. KA modeli için en etkili 20 özelliğin önem skorları

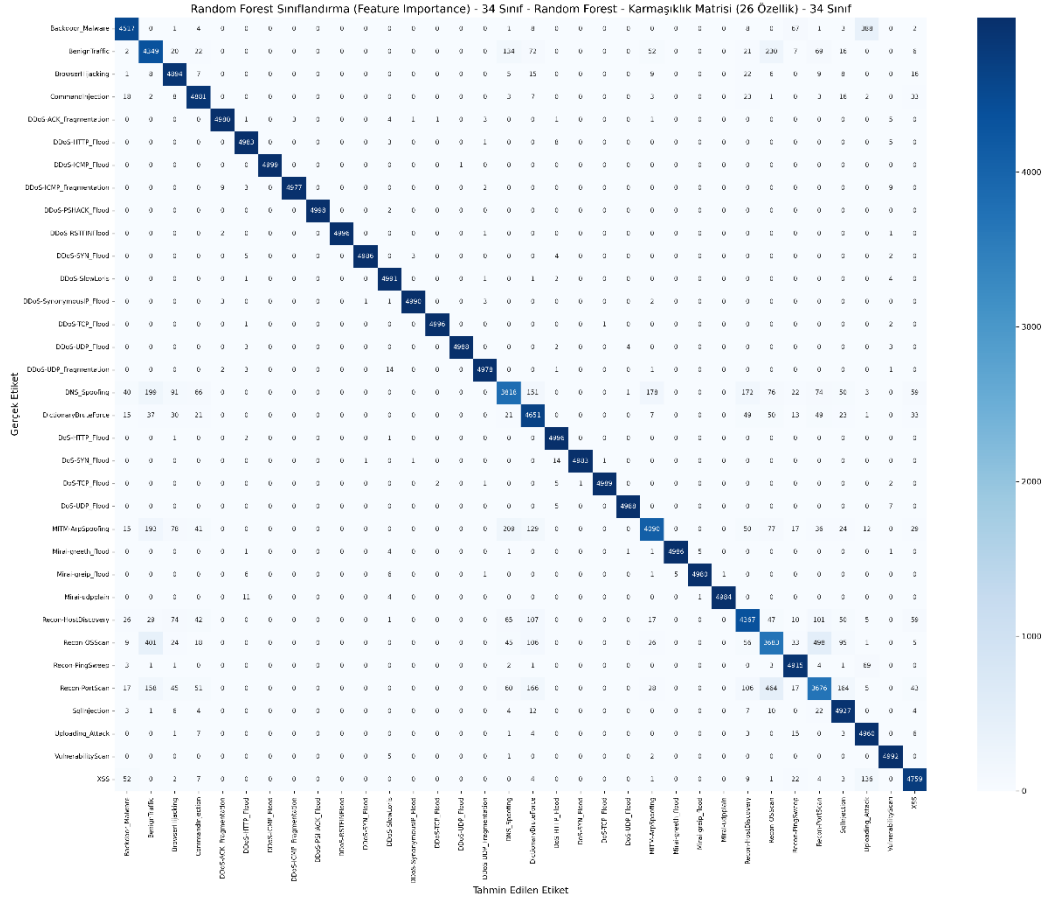
4.2.3.5. Rastgele Orman (RO) algoritması sonuçları

Bu çalışmada, RO algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.40. RO için önemli performans metrikleri

Özellik Sayısı	Ağaç Sayısı	Doğruluk	F1 Skoru
1	150	0.877818	0.875701
2	150	0.910429	0.908707
3	150	0.922347	0.920677
4	150	0.941159	0.939875
5	150	0.945900	0.944791
6	150	0.946782	0.945690
8	150	0.947776	0.946814
9	150	0.948818	0.947821
10	150	0.949176	0.948214
15	150	0.952159	0.951385
20	150	0.954112	0.953377
26	200	0.954394	0.953743
30	200	0.953553	0.952897
35	200	0.952406	0.951759
40	250	0.937229	0.936667
46	250	0.936859	0.936151

Çizelge 4.40'ta RO modelinin farklı özellik sayılarıyla elde ettiği doğruluk ve F1 skoru değerleri karşılaştırılmıştır. Özellikle 20-26 aralığında modelin en yüksek performansa ulaştığı, 26 özellikle en iyi sonuçların alındığı görülmektedir.

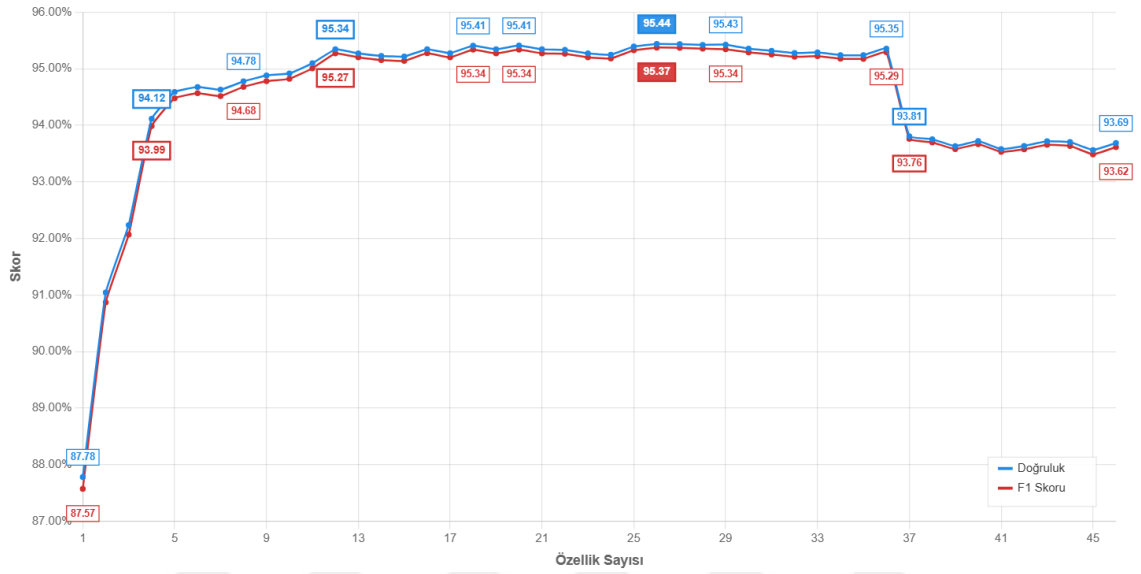


Şekil 4.89. RO modeline ait karmaşıklık matrisi (26 Özellik, 34 Sınıf)

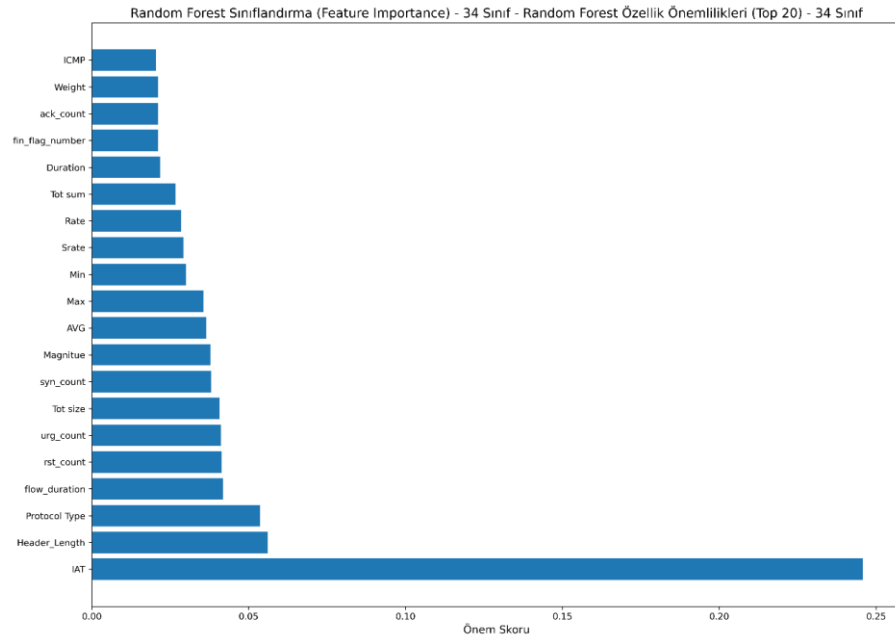
Şekil 4.89, 26 özellikli RO modelinin %95.44 doğrulukla güçlü bir sınıflandırma performansı gösterdiğini ortaya koymaktadır. Model, DoS ve DDoS türlerinde neredeyse kusursuz sonuçlar verirken, Recon ve MITM gibi benzer saldırılar arasında sınırlı karışmalar yaşanmıştır. Diyagonal yoğunluğu yüksek olan matris, genel doğruluğun yüksekliğini yansıtmaktadır.

Şekil 4.90, RO modelinin en yüksek önem derecesine sahip özelliklerin sırayla eklenmesiyle elde ettiği doğruluk ve F1 skoru performansını göstermektedir. Model, yalnızca 1 özellikle %87,78 doğruluk ve %87,57 F1 skoru ile başlamış; 4. özellikle birlikte %94,12 doğruluk ve %93,99 F1 skoruna ulaşarak hızlı bir yükseliş göstermiştir. 12. özellikte model %95,34 doğruluk ve %95,27 F1 skoru ile yüksek bir başarı yakalamıştır. En yüksek doğruluk (%95,44) ve F1 skoru (%95,37), 26. özellikte elde edilmiştir. Bu noktadan sonra 36. özelliğe kadar performans %95,20–%95,40 bandında

stabil seyretmiştir. Ancak 37. özellikten itibaren belirgin bir düşüş yaşanmış; doğruluk %93,81'e, F1 skoru ise %93,76'ya gerilemiştir. Bu durum, fazla sayıda özelliğin modele katkı sağlamadığı gibi aşırı öğrenmeye yol açarak genel performansı olumsuz etkileyebileceğini göstermektedir. Bu nedenle, optimum performans için 26–29 arası özellik sayısı yeterli kabul edilebilir.



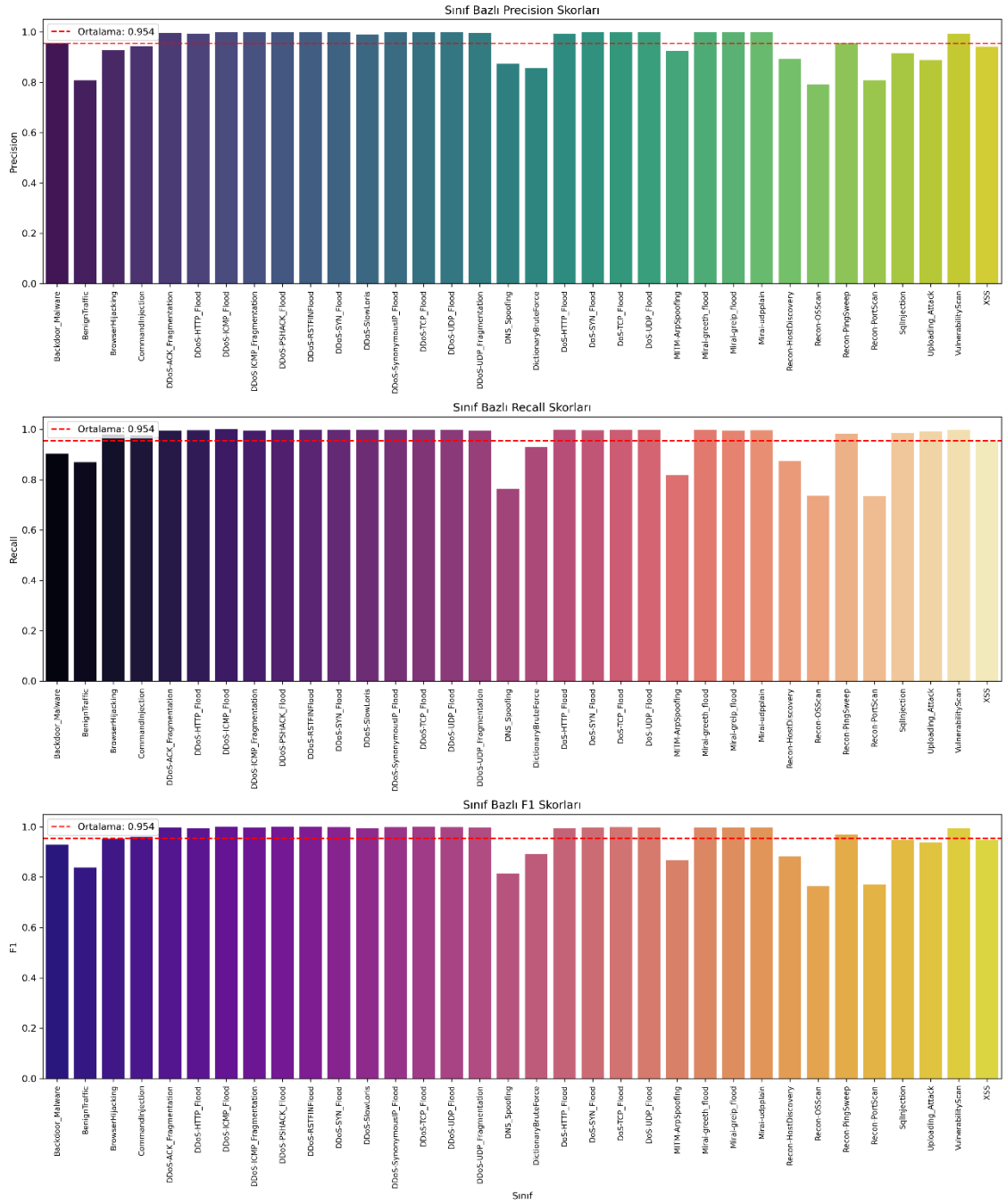
Şekil 4.90. Özellik sayısına göre RO modelinin doğruluk ve F1 skoru değişimi.



Şekil 4.91. RO Modeli İçin En Etkili 20 Özelliğın Önem Skorları

Şekil 4.91, RO modelinde en etkili 20 özelliğın önem derecelerine göre sıralandığını göstermekte olup, IAT özelliğının (~0,25) diğeri tüm özelliklerden açık ara

daha yüksek bir öneme sahip olduğu görülmektedir. Bunu Header_Length ve Protocol_Type (~ 0.05) takip ederken, flow_duration, rst_count, urg_count ve diğer bazı özellikler orta düzeyde katkı sağlamıştır. Min, Srate, Rate ve Duration gibi değişkenler daha düşük önem taşıırken, en alt sıralarda fin_flag_number, ack_count, Weight ve ICMP yer almaktadır. Bu sonuçlar, özellikle IAT'nin siber saldırı tespitinde kritik bir belirleyici olduğunu ve özellik seçimi sürecinde öncelikli değerlendirilmesi gerektiğini ortaya koymaktadır.



Şekil 4.92. RO modelinin 26 özellikle sınıf bazlı Kesinlik, Duyarlılık ve F1 skorları.

Şekil 4.92, 26 özellikli RO modelinin 34 sınıf için kesinlik, duyarlılık ve F1 skorlarını ortaya koymakta olup, her üç metrik için de ortalama değerin 0.954 olduğu görülmektedir. Model, özellikle DDoS ve DoS türlerinde (örneğin DDoS-ICMP_Flood, DDoS-UDP_Flood) mükemmel performans sergilemiş; ancak DNS_Spoofing ve Recon alt türleri gibi bazı sınıflarda görece daha düşük sonuçlar elde edilmiştir. Özellikle BenignTraffic ve Backdoor_Malware gibi sınıflarda yüksek kesinlik değerlerine rağmen düşük duyarlılık, modelin bu sınıflarda daha fazla yanlış negatif ürettiğini göstermektedir. Genel olarak, modelin çoğu sınıfta 0.8'in üzerinde F1 skoruna ulaşması, saldırı türlerini ayırt etmede oldukça başarılı olduğunu ortaya koymakta ve 26 özellikli yapının bu veri seti için optimal seçim olduğunu desteklemektedir.

4.2.3.6. Gradyan Artırma (GA) algoritması sonuçları

Bu çalışmada, GA algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

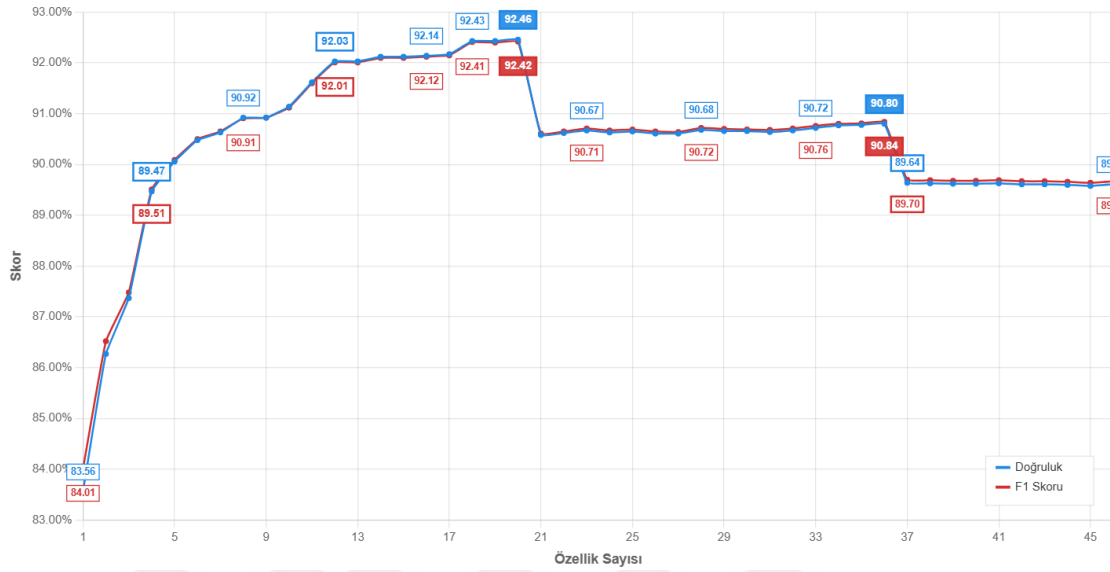
Çizelge 4.41, GA modelinin farklı özellik sayılarıyla elde ettiği sonuçları göstermektedir. En yüksek doğruluk (%92.46) ve F1 skoru (%91.53) 20 özelliikle elde edilmiş, bu yapı modelin en verimli noktası olmuştur.

Çizelge 4.41. GA için önemli performans metrikleri

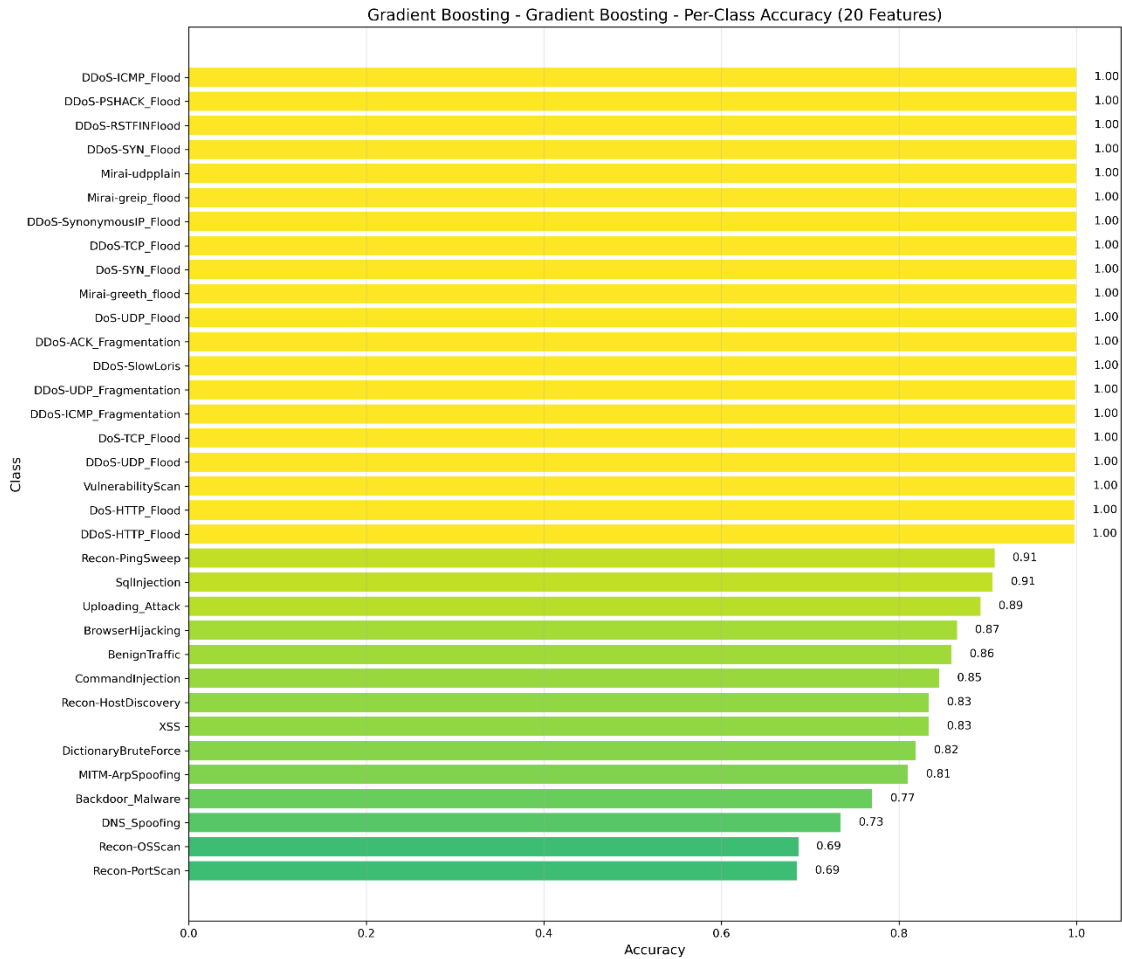
Özellik Sayısı	Doğruluk	F1 Skoru
1	0.8356	0.8401
2	0.8627	0.8652
4	0.8947	0.8951
5	0.9006	0.9009
12	0.9203	0.9201
18	0.9243	0.9241
20	0.9246	0.9242
21	0.9058	0.9061
25	0.9065	0.9069
30	0.9066	0.9069
36	0.9080	0.9084
37	0.8964	0.8970
45	0.8958	0.8964
46	0.8961	0.8967

Şekil 4.93'e göre, GA modeli tek özelliikle %83,56 doğrulukla başlamış, 20. özelliğe kadar artarak %92,46 doğruluk ve %92,42 F1 skoru elde etmiştir. Ancak 20. özellikten sonra performans düşmüş, 45. özellikte doğruluk %89,58 seviyesine

gerilemiştir. Bu durum, GA modeli için optimum özellik sayısının yaklaşık 20 olduğunu ve daha fazla özelliğin aşırı öğrenmeye yol açtığını göstermektedir.

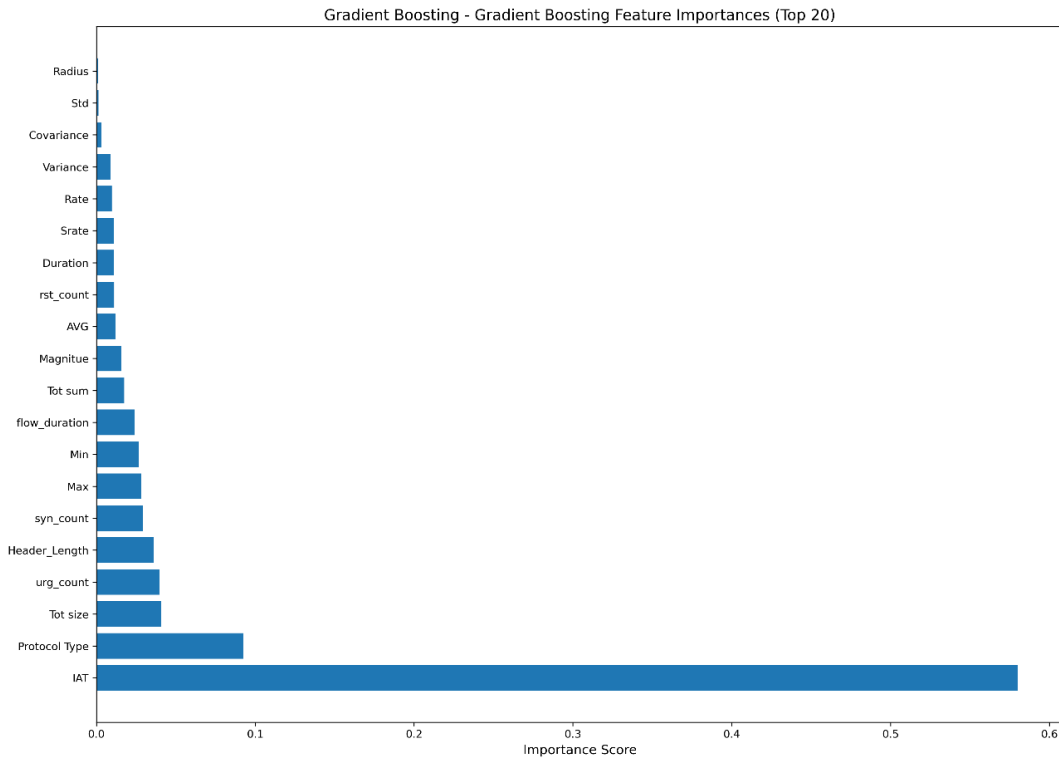


Şekil 4.93. Özellik sayısına göre GA modelinin doğruluk ve F1 skoru değişimi.



Şekil 4.94. Sınıf bazında GA modeli doğruluk oranları (20 özellik)

Şekil 4.94, 20 özellik kullanılarak eğitilen GA modelinin sınıf bazlı doğruluklarını göstermekte olup, modelin özellikle DDoS/DoS ve Mirai botnet saldırılarını %100 doğrulukla başarıyla tespit edebildiğini ortaya koymaktadır. Ayrıca VulnerabilityScan saldırılarında da benzer düzeyde yüksek performans gözlenmiştir. Buna karşın, Recon-OSScan ve Recon-PortScan gibi keşif saldırılarında doğruluk oranı %69'a kadar düşmekte, DNS_Spoofing, Backdoor_Malware ve MITM-ArpSpoofing gibi daha karmaşık sınıflarda ise model %73–%81 aralığında performans sergilemektedir. Bu bulgular, GA modelinin optimize edilmiş 20 öznelikle ortalama %92.46 doğruluk sunarken, bazı ince ayrımlı saldırı türlerinde ayırt edici gücünün sınırlı olduğunu göstermektedir.



Şekil 4.95. GA modeli için en etkili 20 özelliğin önem skorları

Şekil 4.95'teki sıralamaya göre, GA modelinde en önemli özellik yaklaşık 0.57'lik skoruyla IAT oldu. Bu da paketler arası zaman bilgisinin saldırı tespiti için ne kadar önemli olduğunu gösteriyor. Protocol Type, Tot_size, urg_count gibi özellikler orta düzeyde katkı sağlarken, bazı istatistiksel özellikler (örneğin Variance, Covariance) daha düşük skora sahip olsa da tamamen göz ardı edilmemeli. Bu sonuçlar, özellikle zamansal ve protokol düzeyindeki verilerin önemli olduğunu ve DDoS için 20 özellik yeterli olsa da, keşif türü saldırılar için daha güçlü özneliklere ihtiyaç duyulduğunu düşündürüyor.

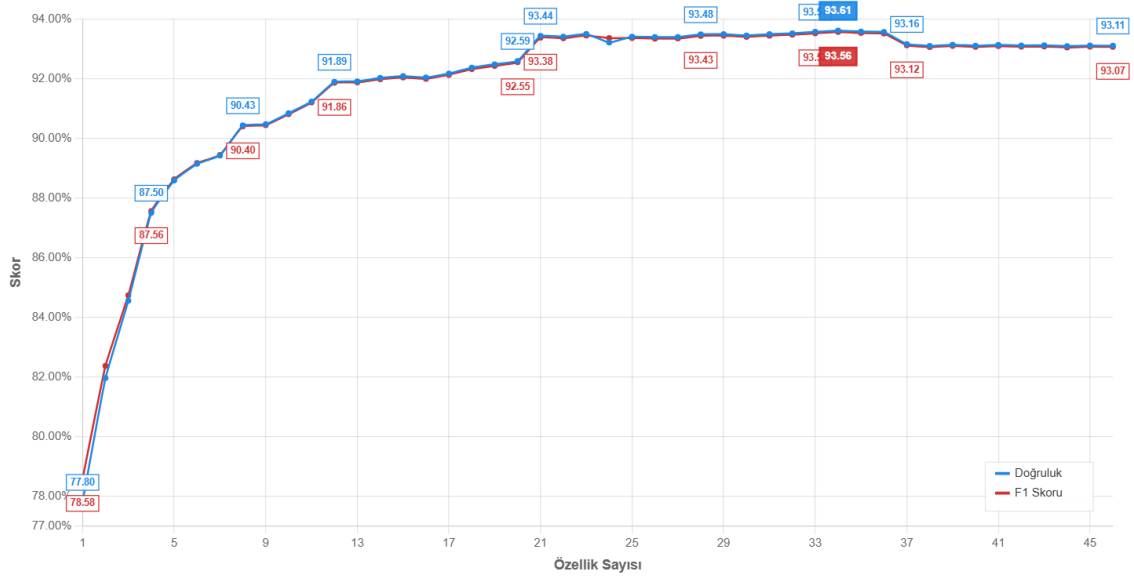
4.2.3.7. Aşırı Gradyan Artırma (AGA) algoritması sonuçları

Bu çalışmada, AGA algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.42, AGA modelinin farklı özellik sayılarıyla elde ettiği doğruluk ve F1 skoru değerlerini göstermektedir.

Çizelge 4.42. AGA için önemli performans metrikleri

Özellik Sayısı	Doğruluk	F1 Skoru
1	0.778029	0.785793
2	0.819606	0.823706
5	0.882647	0.882761
10	0.904412	0.904072
15	0.920829	0.920401
20	0.925906	0.925496
25	0.934094	0.933621
30	0.934494	0.934016
34	0.936147	0.935615
35	0.935812	0.935302
40	0.931059	0.930669
46	0.931059	0.930662

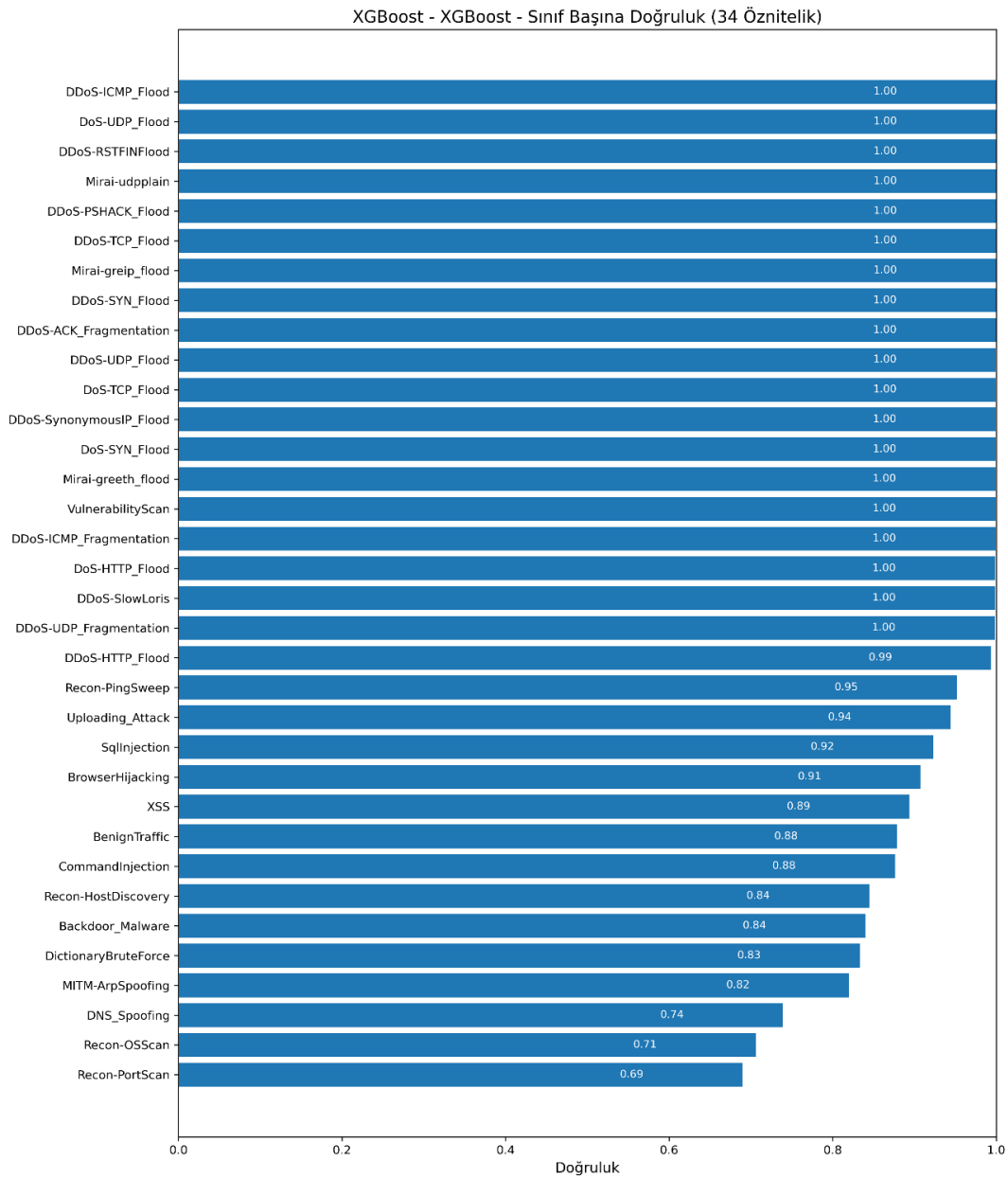


Şekil 4.96. Özellik sayısına göre AGA modelinin doğruluk ve F1 skoru değişimi.

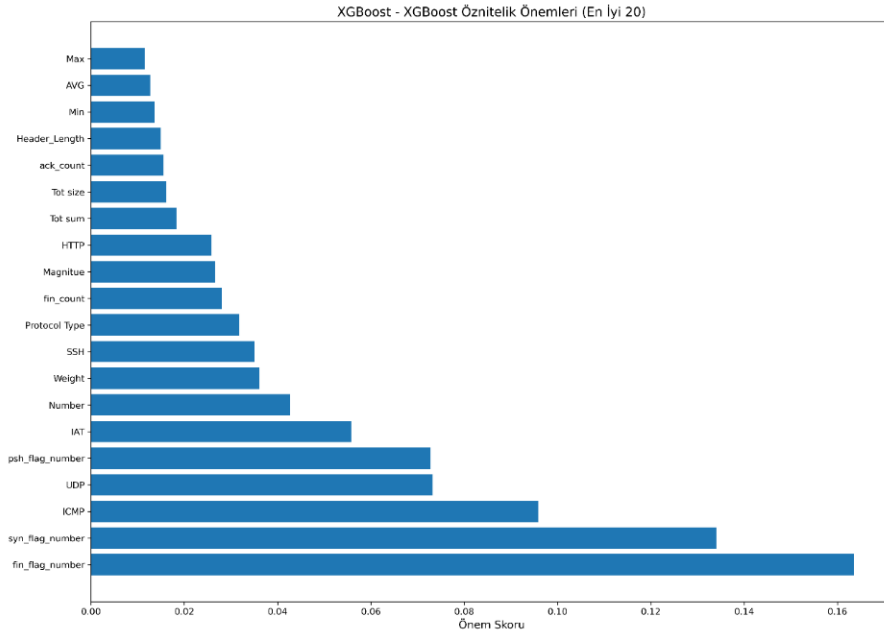
Şekil 4.96, AGA algoritmasında öznelik önemi sırasına göre eklenen özelliklerle doğruluk ve F1 skorundaki değişimi göstermektedir. Model, 1. özellikle %77,80 doğruluk sunarken, ilk 10 özellikle %90,84'e ulaşmıştır. En yüksek doğruluk (%93,61) ve F1 skoru (%93,56) 34. özellikte elde edilmiş, sonrasında skorlar %93,10 seviyesinde

sabitlenmiştir. Sonuçlar, 30–36 özellik aralığının model için en verimli yapı olduğunu göstermektedir.

Şekil 4.97, 34 öznitelikli AGA modelinin 34 farklı siber saldırı türü için doğruluk performansını göstermektedir. DoS ve DDoS gibi çoğu saldırı türünde %100 doğruluk elde edilmiştir. Ancak Recon-PortScan (%69), Recon-OSScan (%71), DNS_Spoofing (%74) ve MITM-ArpSpoofing (%82) gibi keşif ve aldatma temelli saldırılarda başarı düşmüştür. Bu durum, modelin genel olarak yüksek doğruluk sağladığını, ancak bazı karmaşık keşif saldırılarında zorlandığını göstermektedir.



Şekil 4.97. AGA modelinin 34 öznitelikle sınıf bazlı doğruluk performansı



Şekil 4.98. AGA modeli için en etkili 20 özelliğin önem skorları

Şekil 4.98, AGA modelinde en etkili 20 özneliği önem sırasına göre sunmakta olup, fin_flag_number, syn_flag_number ve ICMP özneliklerinin en yüksek katkısı sağladığı görülmektedir. IAT özneliği, RO modelinde en önemli değişken iken bu modelde beşinci sırada yer almakta, bu da algoritmaların öznelik değerlendirme yaklaşımlarındaki farkı ortaya koymaktadır. Bayrak sayıları ve protokol türleri gibi ağ trafiği göstergelerinin öne çıkması, modelin özellikle TCP/UDP düzeyindeki anomalileri etkili biçimde ayırt ettiğini göstermektedir. Bu dağılım, modelin %93.61 doğrulukla elde ettiği yüksek performansın arkasındaki temel etkenleri ortaya koymakta ve öznelik seçimi sürecine yön vermektedir.

4.2.3.8. Yapay sinir ağıları (YSA) algoritması sonuçları

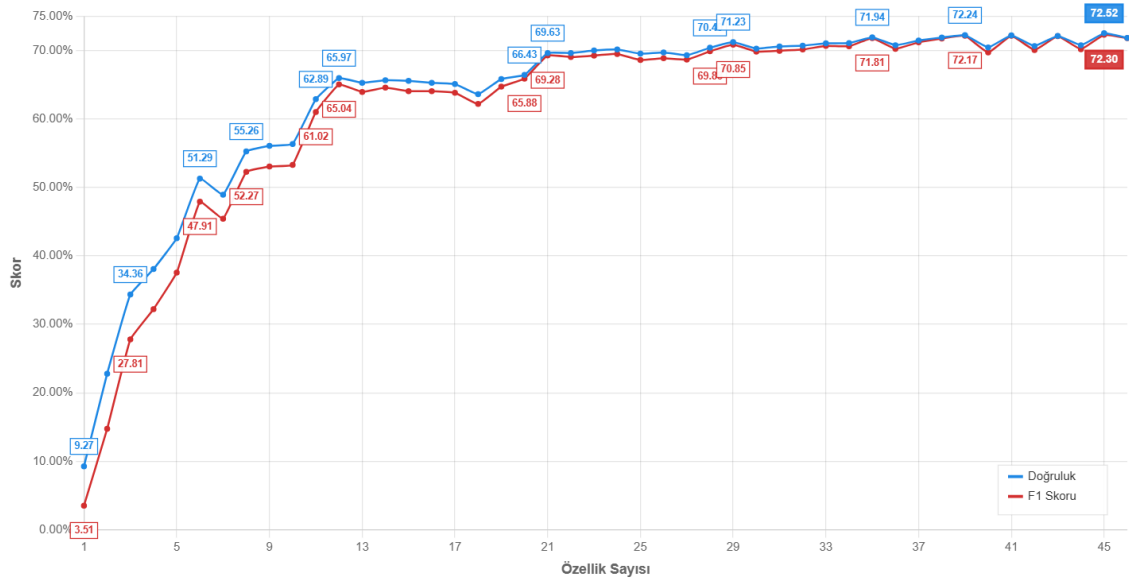
Bu çalışmada, YSA algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.43, YSA modelinin farklı özellik sayılarıyla elde ettiği doğruluk ve F1 skoru sonuçlarını göstermektedir. En yüksek performans %72.52 doğruluk ve %72.30 F1 skoru ile 45 özellikle elde edilmiştir. Modelin başarı seviyesi, özellik sayısı arttıkça istikrarlı biçimde yükselmiştir.

Çizelge 4.43. YSA için önemli performans metrikleri

Özellik Sayısı	Doğruluk	F1 Skoru
1	0.092682	0.035145
2	0.227971	0.147302
3	0.343612	0.278099
4	0.380741	0.322234
5	0.425753	0.375528
10	0.563459	0.533030
15	0.655665	0.640683
20	0.664306	0.658778
25	0.695365	0.686058
30	0.702741	0.698459
35	0.719365	0.718065
39	0.722359	0.721666
40	0.704406	0.697030
45	0.725194	0.722985
46	0.718424	0.718178

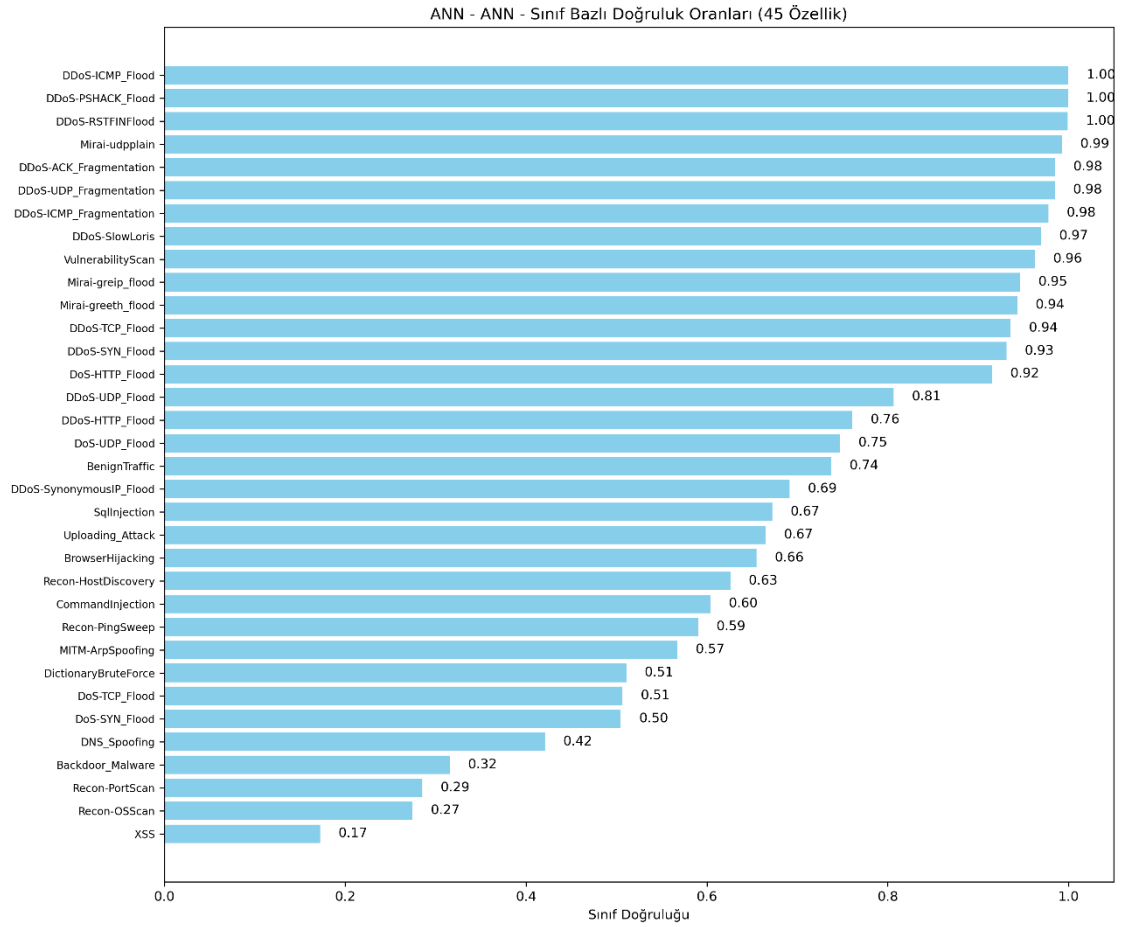
Şekil 4.99, YSA modelinin öznelilik önemi sıralamasına göre artan sayıda özellekle elde ettiği doğruluk ve F1 skoru değişimini göstermektedir. Model, başlangıçta %9,27 doğruluk ile düşük bir performans sergilemiş; ilk 20 özellekte bu oran %66,43'e yükselmiştir. En yüksek doğruluk (%72,52) ve F1 skoru (%72,30) ise 45. özellekte elde edilmiştir. Ancak genel başarı düzeyi diğer modellere kıyasla düşüktür. Bu durum, YSA'nın daha etkili sonuçlar verebilmesi için mimari ve hiper parametre iyileştirmelerine ihtiyaç duyduğunu göstermektedir.



Şekil 4.99. Özellik sayısına göre YSA modelinin doğruluk ve F1 skoru değişimi.

Şekil 4.100, 45 öznelilikli YSA modelinin sınıf bazlı doğruluklarını göstermektedir. Model, DoS ve DDoS saldırılarında yüksek doğruluk sağlamış; ancak

Web tabanlı saldırılar, Recon ve Backdoor_Malware sınıflarında düşük başarı göstermiştir.



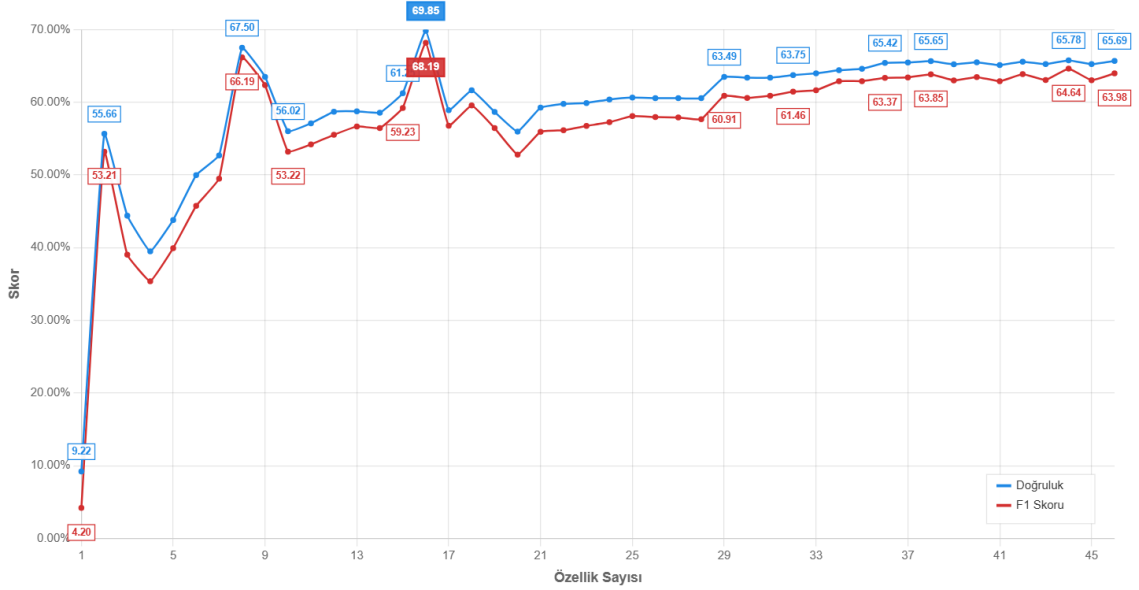
Şekil 4.100. YSA modelinin 45 öznitelikle sınıf bazlı doğruluk performansı

4.2.3.9. Evrimsel Sinir Ağları (ESA) algoritması sonuçları

Bu çalışmada, ESA algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarılarını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Şekil 4.101, ESA modelinin öznitelik önemi sıralamasına göre artan özellik sayısı ile doğruluk ve F1 skoru değişimini göstermektedir. Model, başlangıçta %9,2 gibi düşük bir doğruluk sergilemiş; 16. özellikle birlikte doğruluk %69,85, F1 skoru ise %68,19 ile en yüksek seviyeye ulaşmıştır. Bu noktadan sonra performans dalgalı seyretniş ancak belirgin bir artış sağlanamamıştır. Sonuçlar, ESA modelinin sınırlı sayıda

öznitelikle daha verimli çalıştığını ve optimum başarımlar için 16 özellik kullanımının yeterli olduğunu göstermektedir.



Şekil 4.101. Özellik sayısına göre ESA modelinin doğruluk ve F1 skoru değişimi.

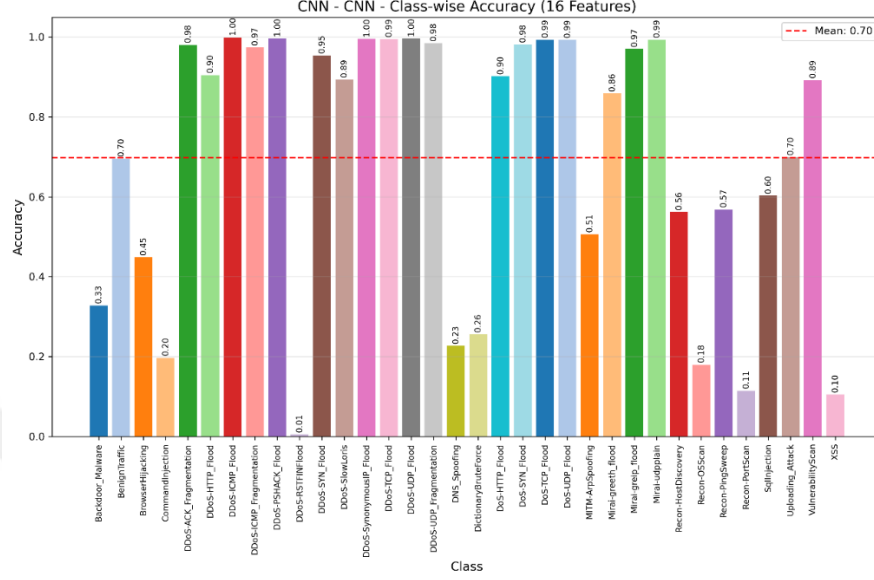
Çizelge 4.44, ESA modelinin farklı özellik sayılarıyla elde ettiği doğruluk ve F1 skoru sonuçlarını göstermektedir. En yüksek performans %69.85 doğruluk ve %68.19 F1 skoru ile 16 özelliikle elde edilmiştir.

Çizelge 4.44. ESA için önemli performans metrikleri

Özellik Sayısı	Doğruluk	F1 Skoru
1	0.092200	0.041963
2	0.556624	0.532142
3	0.444129	0.390239
4	0.395012	0.353828
5	0.438171	0.399404
10	0.560153	0.532156
15	0.612529	0.592286
16	0.698488	0.681859
20	0.559582	0.527990
25	0.606459	0.580991
30	0.633912	0.605872
35	0.645994	0.629146
40	0.655088	0.634841
44	0.657918	0.643653
46	0.656876	0.639808

Şekil 4.102, 16 öznitelik kullanan ESA modelinin sınıf bazlı doğruluklarını göstermekte olup, model ortalama %70 doğrulukla genel olarak makul bir performans sergilemiştir. DDoS-ICMP_Flood, DDoS-RSTFINFlood ve DoS-UDP_Flood gibi bazı saldırı türlerinde %100 doğrulukla başarılı sınıflandırma yapılırken, Recon-PingSweep

(%11), XSS (%10) ve DDoS-SYN_Flood (%1) gibi sınıflarda modelin belirgin şekilde zorlandığı görülmüştür. Bu farklılıklar, modelin belirli saldırı türlerine duyarlılığının yüksek olduğunu, ancak bazı sınıflarda ayırt edici özelliklerin yetersiz kalabildiğini göstermektedir.



Şekil 4.102. ESA modelinin 16 öz nitelik ile sınıf bazlı doğruluk performansı

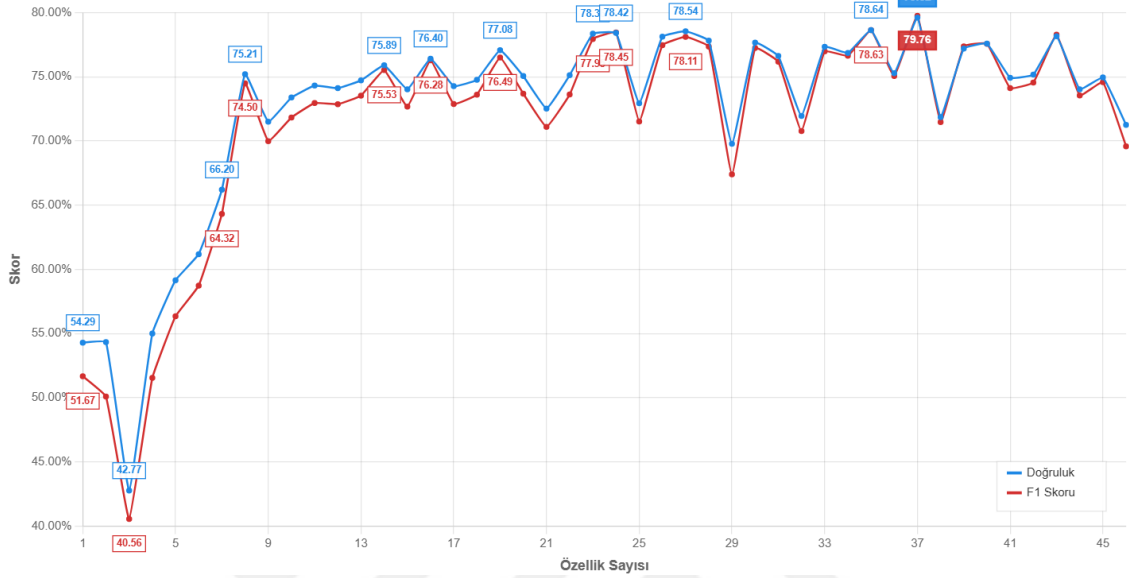
4.2.3.10. Tekrarlayan sinir ağları (TSA) algoritması sonuçları

Bu çalışmada, TSA algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.45. TSA için önemli performans metrikleri

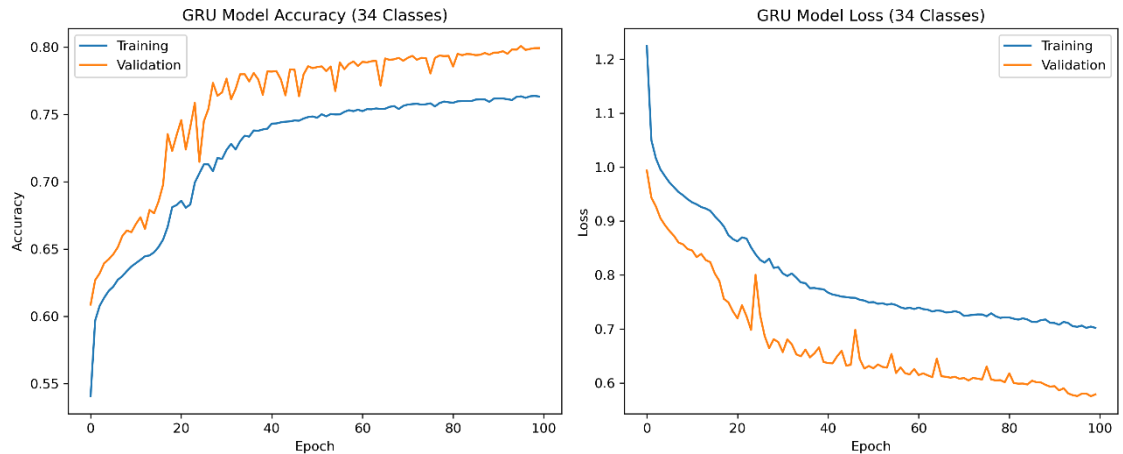
Özellik Sayısı	Doğruluk	F1 Skoru
1	0.542924	0.516705
3	0.447729	0.405635
4	0.550059	0.515416
5	0.591535	0.563433
10	0.733829	0.718266
15	0.740259	0.726769
20	0.750553	0.736869
25	0.729488	0.715229
30	0.776576	0.772493
35	0.786447	0.786305
37	0.796171	0.797565
40	0.775876	0.775763
45	0.749482	0.745806
46	0.712559	0.695864

Çizelge 4.45, TSA modelinin farklı özellik sayılarıyla elde ettiği doğruluk ve F1 skoru değerlerini göstermektedir. En yüksek performans, %79.62 doğruluk ve %79.76 F1 skoru ile 36 özellikle elde edilmiştir. Bu yapı, modelin en verimli konfigürasyonu olarak öne çıkmaktadır.



Şekil 4.103. Özellik sayısına göre TSA modelinin doğruluk ve F1 skoru değişimi.

Şekil 4.103, TSA modelinin artan özellik sayısına göre doğruluk ve F1 skorlarındaki değişimi göstermektedir. Model başlangıçta %54,30 doğruluk ile düşük bir performans sergilemiş, 9. özellikten sonra istikrarlı bir artış yakalayarak 37. özellikte en yüksek değerlere ulaşmıştır (%79,62 doğruluk, %79,76 F1 skoru). Bu noktadan sonra performansta kademeli bir düşüş yaşanmıştır. Sonuçlar, TSA modelinde optimum performans için özellik sayısının dikkatle belirlenmesi gerektiğini ve aşırı özelliğin başarıyı olumsuz etkileyebileceğini ortaya koymaktadır.



Şekil 4.104. TSA modeli eğitim ve doğrulama performans analizi (37 özellik, 34 sınıf)

Şekil 4.104'te sunulan TSA modeline ait doğruluk ve kayıp grafiklerinin analizi, modelin 34 sınıflı sınıflandırma probleminde istikrarlı ve başarılı bir öğrenme süreci geçirdiğini göstermektedir. Eğitim doğruluğu %76, doğrulama doğruluğu ise %80'e ulaşmıştır. Doğrulama eğrisinin eğitim eğrisinden daha yüksek seyretmesi, modelin aşırı öğrenme belirtisi göstermediğini ortaya koymaktadır. Benzer şekilde, eğitim ve doğrulama kayıplarında düzenli bir azalma gözlemlenmiş, doğrulama kaybının eğitim kaybının altında kalması modelin iyi genelleme yeteneğine sahip olduğunu göstermektedir. Bu bulgular, mimari tasarım ve hiper parametrelerin problem yapısına uygun şekilde seçildiğini doğrulamaktadır. Eğrilerin genel eğilimi, daha uzun süreli eğitim ile modelin performansının daha da artırılabilceğine işaret etmektedir.

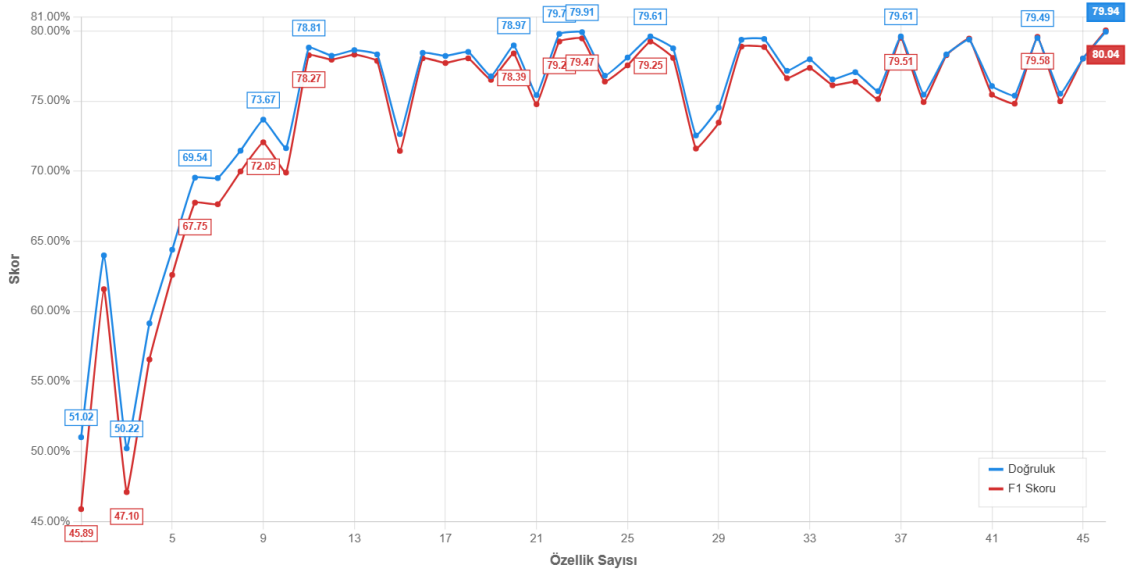
4.2.3.11. Uzun Kısa Süreli Bellek (UKSB) algoritması sonuçları

Bu çalışmada, Uzun Kısa Süreli Bellek (UKSB) algoritması kullanılarak ağ trafiği verisi sınıflandırılmış ve modelin performansı detaylı bir şekilde incelenmiştir. Modelin test verileri üzerindeki başarımını değerlendirmek amacıyla, veri setindeki tüm özellikler kullanılarak eğitim yapılmış ve sonuçlar karşılaştırılmıştır.

Çizelge 4.46, UKSB modelinin farklı özellik sayılarıyla elde ettiği doğruluk ve F1 skoru sonuçlarını göstermektedir. En iyi performans %79.94 doğruluk ve %80.04 F1 skoru ile 46 özelliikle elde edilmiştir.

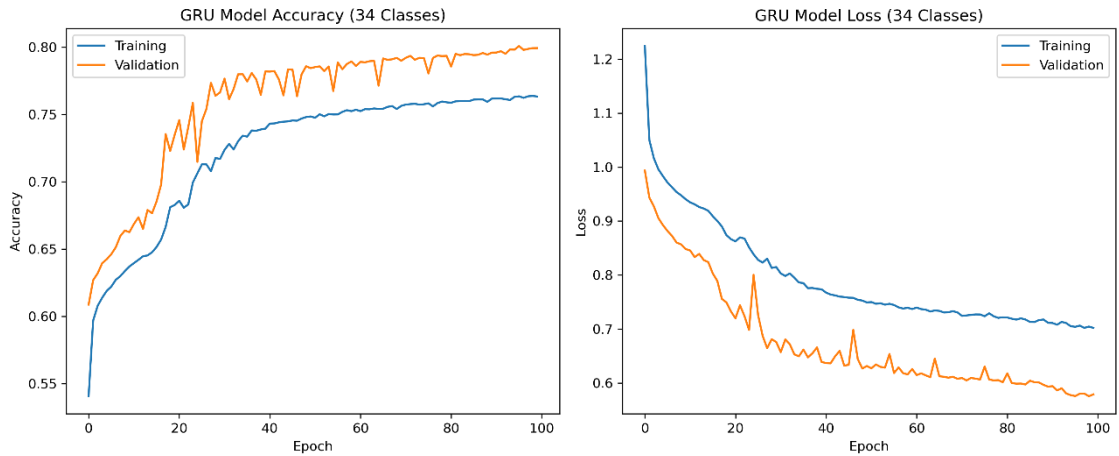
Çizelge 4.46. UKSB için önemli performans metrikleri

Özellik Sayısı	Doğruluk	F1 Skoru
1	0.5102	0.4589
2	0.6399	0.6158
3	0.5022	0.4710
5	0.6439	0.6259
10	0.7164	0.6989
11	0.7881	0.7827
15	0.7264	0.7144
21	0.7543	0.7477
22	0.7979	0.7925
23	0.7991	0.7947
25	0.7810	0.7755
30	0.7937	0.7888
35	0.7706	0.7637
37	0.7961	0.7951
40	0.7939	0.7946
45	0.7803	0.7803
46	0.7994	0.8004



Şekil 4.105. Özellik sayısına göre UKSB modelinin doğruluk ve F1 skoru değişimi.

Şekil 4.105, UKSB modelinin 1-5 özellik arasında düşük (%45-52) performans sergilediğini, 5-9 özellik arasında hızlı artışla %47’den %73’e yükseldiğini, 13. özelliğten itibaren %75-80 aralığında seyrettiğini ve 46. özelliğe en yüksek (%79,94 doğruluk, %80,04 F1) performansa ulaştığını göstermektedir.



Şekil 4.106. UKSB modeli eğitim ve doğrulama performans analizi (23 özellik, 34 sınıf)

Şekil 4.106. UKSB modelinin 23 özellik ve 34 sınıf ile gerçekleştirdiği eğitim sürecine ait doğruluk ve kayıp grafiklerini göstermektedir. Doğrulama doğruluğu eğitimden daha yüksek seyretmiş ve yaklaşık %80 seviyesine ulaşmıştır. Benzer şekilde, doğrulama kaybı da eğitim kaybının altında kalmış, bu durum modelin aşırı öğrenmeden kaçındığını ve iyi bir genelleme yeteneğine sahip olduğunu göstermektedir. Eğitim ilerledikçe öğrenme hızı azalsa da performans artışı devam etmiş, bu da model yapısı ve hiper parametrelerin probleme uygunluğunu desteklemektedir.

4.3. Tartışma

Bu tez çalışmasında, CICIOT2023 veri seti kullanılarak IoT ağlarında gerçekleştirilen siber saldırıların tespiti ve sınıflandırılması amacıyla çeşitli makine öğrenmesi ve DÖ algoritmaları değerlendirilmiştir. İkili, sekizli ve otuz dört sınıflı olmak üzere üç farklı sınıflandırma senaryosunda gerçekleştirilen analizler, model performansları, özneliliklerin etkisi ve sınıflandırma karmaşıklığının sonuçlar üzerindeki yansımaları açısından önemli bulgular sunmaktadır.

İkili sınıflandırma senaryosunda tüm modeller yüksek doğruluk oranlarıyla başarılı sonuçlar vermiştir. RO algoritması, %99.98 doğruluk oranı ve 1.000 AUC değeri ile en yüksek performansı sergilemiştir. Ancak sınıf sayısı sekiz ve otuz dörde çıkarıldığında, özellikle NB ve LR gibi temel modellerin performansında belirgin düşüşler gözlenmiştir. Bu durum, sınıf sayısı arttıkça hem modellerin ayırt edicilik gücünün azaldığını hem de bazı saldırı türlerinin mevcut özneliliklerle yeterince temsil edilemediğini göstermektedir.

Topluluk öğrenmesi temelli algoritmaların, özellikle RO ve GA gibi yöntemlerin, tüm senaryolarda en yüksek başarıyı göstermesi dikkat çekicidir. Bu algoritmaların karar ağaçları ve örnekleme stratejileri sayesinde IoT ağ trafiğindeki karmaşık örüntüleri başarıyla modelleyebildiği görülmüştür. Bu bulgu, literatürde de sıklıkla vurgulanan ensemble yöntemlerinin genelleme kapasitesinin yüksekliğini destekler niteliktedir.

DÖ algoritmaları, ikili sınıflandırma görevlerinde makine öğrenmesi modelleriyle rekabet edebilir düzeyde performans sergilemiş olsa da sekizli ve otuz dört sınıflı senaryolarda başarı oranları belirgin şekilde düşmüştür. Bu durum, DÖ modellerinin başarılı olabilmesi için daha büyük ve dengeli veri kümelerine, iyi optimize edilmiş parametrelere ve yüksek işlem gücüne gereksinim duyduğunu ortaya koymaktadır. Özellikle düşük hacimli saldırı türlerinin tespitinde DÖ modelleri zayıf sonuçlar vermiştir. Bu durum, IoT trafiğinde kullanılan özneliliklerin karmaşık saldırı davranışlarını her zaman yeterince yansıtamadığını düşündürmektedir.

Yapılan öznelilik önem analizlerinde, rst_count, urg_count, IAT, Magnitude, Variance ve Protocol_Type gibi ağ trafiğine özgü parametrelerin, saldırıların doğru şekilde sınıflandırılmasında belirleyici rol oynadığı görülmüştür. Bu bulgular, özellikle IAT gibi zamansal değişkenlerin siber saldırıların tespitinde kritik öneme sahip olduğunu ortaya koymaktadır. Nitekim, bazı algoritmalar sadece birkaç temel öznelilikle yüksek doğruluk oranlarına ulaşabilmiş; bu da kaynak kısıtlı IoT sistemleri için hafif ve verimli

modellerin uygulanabilirliğini göstermektedir. Bununla birlikte, özellik sayısının aşırı artırılması bazı modellerde aşırı öğrenme (overfitting) problemlerine yol açmış ve doğruluk oranlarını olumsuz etkilemiştir.

Saldırı türlerine göre tespit başarısında önemli farklar gözlemlenmiştir. DDoS ve DoS gibi belirgin saldırılar yüksek başarıyla tespit edilebilmişken, Reconnaissance, MITM ve bazı web tabanlı saldırıların tespiti daha zor olmuştur. Bu tür saldırıların, normal trafik davranışlarına daha yakın özellikler taşıması, modellerin bu saldırıları ayırt etme becerisini sınırlamaktadır. Bu bulgu, saldırıya özgü özniteliklerin tasarımı ve daha sofistike analiz yaklaşımlarının geliştirilmesi gerektiğine işaret etmektedir.

Sınıf dengesizliği sorunu da çalışmada öne çıkan konulardan biri olmuştur. Özellikle az örnekli saldırı türlerinde modellerin düşük başarı göstermesi, veri dengesizliğinin etkisini açıkça ortaya koymuştur. Bu probleme karşı uygulanan SMOTE, ADASYN ve benzeri yeniden örnekleme tekniklerinin doğruluk oranlarını artırdığı gözlemlenmiştir. Ancak gelecekte, GAN tabanlı sentetik örnekleme yaklaşımları gibi daha gelişmiş yöntemlerin kullanılmasıyla, sınıf dengesizliğine daha kalıcı çözümler üretilebileceği değerlendirilmektedir.

Model eğitimi sırasında elde edilen doğrulama eğrileri, özellikle DÖ modellerinde overfitting riskinin düşük olduğunu ve genelleme yeteneklerinin güçlü olduğunu göstermiştir. Ancak karmaşık sınıflandırma görevlerinde bu modellerin bazı saldırı türleri arasında ince ayrımları öğrenmekte zorlandığı da gözlemlenmiştir. Bu durum, saldırı türlerine özgü bilgi taşıyan özniteliklerin veya hibrit model yapılarının geliştirilmesini gerekli kılmaktadır.

Sonuç olarak, bu tez çalışması, IoT ortamlarında etkili siber saldırı tespiti için doğru algoritma seçimi, dengeli veri yapısı, optimize edilmiş öznitelik seti ve uygun örnekleme stratejilerinin birlikte ele alınmasının gerekliliğini ortaya koymaktadır. Sınıflandırma başarısının saldırı türüne, veri dağılımına ve öznitelik temsil gücüne bağlı olarak değiştiği bu analizler ışığında, gelecekte zaman serisi analizi, saldırıya özgü özellik çıkarımı ve açıklanabilir yapay zekâ tabanlı sistemlerin entegrasyonuna yönelik çalışmalar yapılması önerilmektedir.

5. SONUÇLAR VE ÖNERİLER

5.1 Sonuçlar

Bu çalışmada, CICIoT2023 veri seti kullanılarak IoT ağ ortamlarında gerçekleşen siber saldırıların tespiti ve sınıflandırılmasına yönelik olarak, farklı makine öğrenmesi ve DÖ algoritmalarının performansları üç farklı senaryo kapsamında (ikili, sekizli ve otuz dörtlü sınıflandırma) kapsamlı biçimde analiz edilmiştir. Elde edilen bulgular, model başarımı, öznetelik seçimi ve sınıflandırma stratejileri açısından önemli içgörüler sunmaktadır.

1. İkili sınıflandırma görevinde, tüm algoritmalar oldukça yüksek doğruluk ve F1 skorları (%93–%99.74 aralığında) elde etmiş ve zararlı-zararsız trafik ayrımı yüksek doğrulukla gerçekleştirilmiştir. Bu başarı, IoT ağ trafiğinde temel saldırı ayrımının görece kolay yapılabildiğini göstermektedir.
2. Sınıf sayısı arttıkça model performansı düşmektedir. Sekizli sınıflandırma senaryosunda doğruluk oranları %78–%95 aralığında kalırken, otuz dört sınıflı senaryoda bazı modellerin doğruluğu %48’e kadar düşmüştür. Bu durum, sınıflar arası benzerlik, veri dengesizliği ve model karmaşıklığı gibi faktörlerin etkisini göstermektedir.
3. Topluluk öğrenmesi (ensemble learning) algoritmaları, tüm sınıflandırma düzeylerinde üstün performans sergilemiştir. Özellikle RO algoritması, ikili (%99.74), sekizli (%95.29) ve otuz dörtlü (%95.44) sınıflandırmalarda en yüksek doğruluk ve F1 skorlarına ulaşarak en başarılı model olmuştur.
4. DÖ modelleri, ikili sınıflandırmada klasik makine öğrenmesi yöntemleriyle rekabet edebilir sonuçlar üretse de çok sınıflı senaryolarda performansları belirgin biçimde düşmüştür. Bu durum, DÖ algoritmalarının daha fazla veri, hiper parametre optimizasyonu ve hesaplama kaynağına ihtiyaç duyduğunu ortaya koymaktadır.
5. Özellik mühendisliği, model başarısı üzerinde doğrudan etkilidir. Genellikle 30–40 arası nitelikle en yüksek performans elde edilirken, daha fazla özellik kullanımı aşırı öğrenmeye (overfitting) ve doğruluk kayıplarına neden olmuştur. Ayrıca, özellik sayısı ile doğruluk arasında doğrusal olmayan bir ilişki tespit edilmiştir.
6. En belirleyici öznetelikler arasında `rst_count`, `urg_count`, `IAT`, `Magnitude`, `Variance`, `Protocol_Type` gibi ağ trafiğine özgü parametreler yer almakta olup,

özellikle DDoS, DoS ve tarama saldırılarının tespitinde yüksek ayırt edici güce sahiptirler. Özellikle IAT, yüksek sınıflı sınıflandırmalarda kritik bir ayrıştırıcı olarak öne çıkmıştır.

7. Saldırı türüne göre tespit başarısı değişmektedir. DDoS ve DoS gibi yüksek hacimli saldırılar kolayca tespit edilirken, Reconnaissance, MITM ve bazı web saldırılarında daha düşük doğruluk oranları elde edilmiştir. Bu durum, düşük hacimli saldırıların normal trafiğe benzer davranışlar sergilemesinden kaynaklanmaktadır.
8. Sınıf dengesizliği problemi, SMOTE, ADASYN, Borderline-SMOTE ve SMOTEENN gibi yeniden örnekleme teknikleriyle başarıyla yönetilmiş; az örnekli saldırı türlerinin tespit performansında iyileşmeler sağlanmıştır.
9. Model eğitim süreçlerinin analizi, özellikle DÖ modellerinin genelleme yeteneğine sahip olduğunu ve overfitting probleminin genellikle başarıyla önlendiğini ortaya koymuştur. Doğrulama doğruluklarının eğitim doğruluklarından yüksek olması bu durumu desteklemektedir.
10. Karmaşıklık matrisleri, bazı saldırı türlerinin benzer trafik desenleri göstermesi nedeniyle karıştırıldığını ortaya koymuştur. Bu durum, özellikle keşif, MITM ve web tabanlı saldırılar için gelişmiş özellik çıkarımı ve hibrit yaklaşımların gerekliliğine işaret etmektedir.

Bu kapsamlı analiz sonucunda, IoT ağlarında siber saldırıların etkili şekilde tespit edilebilmesi için özellikle topluluk öğrenmesi tabanlı algoritmaların, başta RO olmak üzere, oldukça güçlü çözümler sunduğu görülmüştür. Sınıflandırma zorluğunun sınıf sayısına ve saldırı türüne bağlı olarak arttığı, bu nedenle veri ön işleme, uygun algoritma seçimi, güçlü öznitelik mühendisliği ve örnekleme stratejilerinin başarıda belirleyici olduğu sonucuna ulaşılmıştır. Elde edilen bulgular hem akademik araştırmalar hem de gerçek dünya IoT güvenlik uygulamaları için yol gösterici niteliktedir.

5.2 Öneriler

Bu tez çalışmasında elde edilen bulgular doğrultusunda, IoT ağlarında siber saldırı tespiti alanında yapılabilecek gelecekteki araştırmalara yönelik bazı öneriler aşağıda sunulmuştur:

İlk olarak, bazı saldırı türlerinin (örneğin Reconnaissance, MITM ve web tabanlı saldırılar) mevcut özelliklerle yeterince ayırt edilemediği görülmüştür. Bu nedenle, bu saldırılara özgü yeni ve daha açıklayıcı özelliklerin geliştirilmesi önerilmektedir. Özellikle zaman içindeki trafik desenlerini analiz eden zaman serisi tabanlı yöntemlerin (örneğin LSTM, GRU) kullanımı faydalı olabilir.

Çalışma, farklı algoritmaların güçlü yönlerinden yararlanan hibrit modellerin etkili olabileceğini göstermiştir. Topluluk öğrenmesi yöntemleri ile DÖ mimarilerinin birleştirilmesi, sınıflandırma başarısını artırabilir. Ayrıca, bilinen ve bilinmeyen saldırıların birlikte tespit edilmesi için anomali tespiti ve sınıflandırma yöntemlerinin entegre kullanımı da değerlendirilebilir.

Veri dengesizliği, özellikle az sayıda örnek içeren saldırı türlerinde model başarısını olumsuz etkilemiştir. Bu sorunun azaltılması için SMOTE gibi örnekleme tekniklerine ek olarak, GAN tabanlı sentetik veri üretim yöntemleri önerilmektedir.

IoT cihazlarının sınırlı işlem gücü göz önüne alındığında, daha az özellik kullanan ve hızlı çalışan modellerin geliştirilmesi önemlidir. Bu doğrultuda, hafif modellerin oluşturulması ve kaynak verimliliğine uygun çözümlerin sunulması önerilmektedir. Modellerin yalnızca eğitim veri setleriyle değil, gerçek dünyadaki IoT sistemleri üzerinde de test edilmesi gerekmektedir. Bu, sistemlerin pratikte ne kadar etkili olduğunu görmek açısından önemlidir. Ayrıca, farklı veri setleriyle çapraz doğrulama yapılarak modellerin genellenebilirliği artırılabilir.

Son olarak, saldırı tespiti sistemlerine açıklanabilir yapay zekâ yöntemlerinin (örneğin SHAP, LIME) entegre edilmesi önerilmektedir. Böylece modellerin neden belli trafik türlerini saldırı olarak sınıflandırdığı anlaşılabilir hale gelir ve güvenlik uzmanlarının müdahale süreci kolaylaşır.

Bu öneriler doğrultusunda yapılacak çalışmalar, IoT ortamlarında daha güvenli, hızlı ve etkili saldırı tespit sistemlerinin geliştirilmesine katkı sağlayacaktır.

KAYNAKLAR

- Abbas, S., Al Hejaili, A., Sampedro, G. A., Abisado, M., Almadhor, A. S., Shahzad, T. ve Ouahada, K., 2023, A novel federated edge learning approach for detecting cyberattacks in IoT infrastructures, *IEEE Access*, 11, 112189-112198.
- Abbas, S. G., Vaccari, I., Hussain, F., Zahid, S., Fayyaz, U. U., Shah, G. A., Bakhshi, T. ve Cambiaso, E., 2021, Identifying and mitigating phishing attack threats in IoT use cases using a threat modelling approach, *Sensors*, 21 (14), 4816.
- Abiodun, O. I., Abiodun, E. O., Alawida, M., Alkhawaldeh, R. S. ve Arshad, H., 2021, A review on the security of the internet of things: Challenges and solutions, *Wireless Personal Communications*, 119, 2603-2637.
- Abomhara, M. ve Køien, G. M., 2014, Security and privacy in the Internet of Things: Current status and open issues, *2014 international conference on privacy and security in mobile systems (PRISMS)*, 1-8.
- Adiwal, S., Rajendran, B. ve Sudarsan, S. D., 2023, DNS Intrusion Detection (DID)—A SNORT-based solution to detect DNS amplification and DNS tunneling attacks, *Franklin Open*, 2, 100010.
- Al-Na'amneh, Q., Aljaidi, M., Nasayreh, A., Gharaibeh, H., Al Mamlook, R. E., Jaradat, A. S., Alsarhan, A. ve Samara, G., 2024, Enhancing IoT device security: CNN-SVM hybrid approach for real-time detection of DoS and DDoS attacks, *Journal of Intelligent Systems*, 33 (1), 20230150.
- Al-Naeem, M. A., 2021, Prediction of re-occurrences of spoofed ACK packets sent to deflate a target wireless sensor network node by DDOS, *IEEE Access*, 9, 87070-87078.
- Alqahtani, A., Alsulami, A. A., Alqahtani, N., Alturki, B. ve Alghamdi, B. M., 2024, A Comprehensive Security Framework for Asymmetrical IoT Network Environments to Monitor and Classify Cyberattack via Machine Learning, *Symmetry*, 16 (9), 1121.
- Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L. ve Kallitsis, M., 2017, Understanding the mirai botnet, *26th USENIX security symposium (USENIX Security 17)*, 1093-1110.
- Atzori, L., Iera, A. ve Morabito, G., 2010, The internet of things: A survey, *Computer networks*, 54 (15), 2787-2805.
- Batista, G. E., Prati, R. C. ve Monard, M. C., 2004, A study of the behavior of several methods for balancing machine learning training data, *ACM SIGKDD explorations newsletter*, 6 (1), 20-29.
- Batra, S. ve Dash, C. S., 2024, Machine Learning-Based Detection of Synonymous IP Flood Attacks on Server Infrastructure, *International Journal of Science and Research (IJSR)*.
- Bentéjac, C., Csörgő, A. ve Martínez-Muñoz, G., 2021, A comparative analysis of gradient boosting algorithms, *Artificial Intelligence Review*, 54, 1937-1967.
- Breiman, L., 2001, Random forests, *Machine learning*, 45, 5-32.
- BrickerBot, 2017, "BrickerBot" Results In Permanent Denial-of-Service, <https://www.radware.com/security/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/>: [27.01.2025].
- Calp, M. H. ve Bütüner, R., Detecting the Cyber Attacks on IoT-Based Network Devices Using Machine Learning Algorithms, *Politeknik Dergisi*, 1-1.

- Carlos A. Rivera A., X. C., Arash Shaghaghi, Gustavo Batista, Salil S. Kanhere, 2024, Predicting IoT Device Vulnerability Fix Times with Survival and Failure Time Models, *School of Computer Science and Engineering, The University of New South Wales (UNSW Sydney), Australia*.
- Chandola, V., Banerjee, A. ve Kumar, V., 2009, Anomaly detection: A survey, *ACM computing surveys (CSUR)*, 41 (3), 1-58.
- Chawla, N. V., Bowyer, K. W., Hall, L. O. ve Kegelmeyer, W. P., 2002, SMOTE: synthetic minority over-sampling technique, *Journal of artificial intelligence research*, 16, 321-357.
- Chen, T. ve Guestrin, C., 2016, Xgboost: A scalable tree boosting system, *Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining*, 785-794.
- Chicco, D. ve Jurman, G., 2020, The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation, *BMC genomics*, 21, 1-13.
- CICIoT2023, 2023, CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment, University of New Brunswick, <https://www.unb.ca/cic/datasets/iotdataset-2023.html>: [12.02.2025].
- Cover, T. ve Hart, P., 1967, Nearest neighbor pattern classification, *IEEE transactions on information theory*, 13 (1), 21-27.
- DDoS-Guard, 2025, RST & FIN Flood Attacks, <https://ddos-guard.net/terms/ddos-attack-types/rst-fin-flood>: [15.02.2025].
- Diro, A. A. ve Chilamkurti, N., 2018, Distributed attack detection scheme using deep learning approach for Internet of Things, *Future generation computer systems*, 82, 761-768.
- Duda, R. O. ve Hart, P. E., 2006, Pattern classification, John Wiley & Sons, p.
- El-Sofany, H., El-Seoud, S. A., Karam, O. H. ve Bouallegue, B., 2024, Using machine learning algorithms to enhance IoT system security, *Scientific Reports*, 14 (1), 12077.
- Elman, J. L., 1990, Finding structure in time, *Cognitive science*, 14 (2), 179-211.
- Erdal, E. ve Ergüzen, A., 2020, Nesnelerin İnterneti (IoT), *International Journal of Engineering Research and Development*, 12 (3), 24-34.
- Fei, W., 2024, Research on optimization algorithms for artificial intelligence network security management based on All IP Internet of Things fusion technology, *Computers and Electrical Engineering*, 115, 109105.
- Fernández-Caramés, T. M. ve Fraga-Lamas, P., 2018, A Review on the Use of Blockchain for the Internet of Things, *IEEE Access*, 6, 32979-33001.
- Fish, C., 2024, Odd cyber-attack: Casino fish tank hack, <https://www.oryxalign.com/blog/blog/casino-fish-tank-hack>: [27.01.2025].
- Forman, G., 2003, An extensive empirical study of feature selection metrics for text classification, *Journal of machine learning research*, 3 (Mar), 1289-1305.
- Friedman, J. H., 2001, Greedy function approximation: a gradient boosting machine, *Annals of statistics*, 1189-1232.
- Goldschmidt, P., 2019, TCP Reset Cookies—a heuristic method for TCP SYN Flood mitigation, *Excel@ FIT*, 2019.
- Goodfellow, I., 2016, Deep learning, MIT press, p.
- Gubbi, J., Buyya, R., Marusic, S. ve Palaniswami, M., 2013, Internet of Things (IoT): A vision, architectural elements, and future directions, *Future generation computer systems*, 29 (7), 1645-1660.

- Gupta, S., Kumar, S., Singh, K. ve Saini, D., 2024, Unveiling anomalies: harnessing machine learning for detection and insights, *Engineering Research Express*, 6 (3), 035215.
- Guyon, I. ve Elisseeff, A., 2003, An introduction to variable and feature selection, *Journal of machine learning research*, 3 (Mar), 1157-1182.
- Güler, O., 2024, A Model Design Using Blockchain and Smart Contracts Against Cyberattacks in Smart Home Systems, *Acta Infologica*, 8 (1), 11-22.
- Hamza, A., Gharakheili, H. H. ve Sivaraman, V., 2018, Combining MUD policies with SDN for IoT intrusion detection, *Proceedings of the 2018 Workshop on IoT Security and Privacy*, 1-7.
- Han, H., Wang, W.-Y. ve Mao, B.-H., 2005, Borderline-SMOTE: a new over-sampling method in imbalanced data sets learning, *International conference on intelligent computing*, 878-887.
- Haque, S., El-Moussa, F., Komninos, N. ve Muttukrishnan, R., 2023, A systematic review of data-driven attack detection trends in IoT, *Sensors*, 23 (16), 7191.
- Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P. ve Sikdar, B., 2019, A survey on IoT security: application areas, security threats, and solution architectures, *IEEE Access*, 7, 82721-82743.
- Hastie, T., 2009, The elements of statistical learning: data mining, inference, and prediction, Springer.
- He, H., Bai, Y., Garcia, E. A. ve Li, S., 2008, ADASYN: Adaptive synthetic sampling approach for imbalanced learning, *2008 IEEE international joint conference on neural networks (IEEE world congress on computational intelligence)*, 1322-1328.
- Helbig, C., Otoum, S. ve Jararweh, Y., 2023, Modeling and Evaluation of the Internet of Things Communication Protocols in Security Constrained Systems, *2023 IEEE 20th Consumer Communications & Networking Conference (CCNC)*, 1-6.
- Hochreiter, S., 1997, Long Short-term Memory, *Neural Computation MIT-Press*.
- Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P.-L., Iorkyase, E., Tachtatzis, C. ve Atkinson, R., 2016, Threat analysis of IoT networks using artificial neural network intrusion detection system, *2016 International Symposium on Networks, Computers and Communications (ISNCC)*, 1-6.
- Hue, P., 2020, Don't be silly – it's only a lightbulb, <https://research.checkpoint.com/2020/dont-be-silly-its-only-a-lightbulb/>: [27.01.2025].
- Indusface ACK Flood, 2025, ACK Flood Attack, <https://www.indusface.com/learning/tcp-ack-flood-attack/>: [15.02.2025].
- Indusface Fragmented ACK, 2025, Fragmented ACK Flood Attack, <https://www.indusface.com/learning/fragmented-ack-flood-attack/>: [15.02.2025].
- Indusface HTTP Flood, 2025, HTTP Flood Attack, <https://www.indusface.com/learning/http-flood-attack/>: [15.02.2025].
- Indusface ICMP Flood, 2025, ICMP Flood Attack, <https://www.indusface.com/learning/icmp-flood-attacks/>: [15.02.2025].
- Indusface UDP Flood, 2025, UDP Flood Attack, <https://www.indusface.com/learning/udp-flood-attack/>: [15.02.2025].
- Jeep, H., 2015, Hackers Remotely Kill a Jeep on the Highway—With Me in It, <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>: [27.01.2025].

- Jena, S. K., Barik, R. C. ve Priyadarshini, R., 2024, A systematic state-of-art review on digital identity challenges with solutions using conjugation of IOT and blockchain in healthcare, *Internet of Things*, 101111.
- Ji, R., Kumar, N. ve Padha, D., 2024, CNN-GWO-voting & hybrid: ensemble learning inspired intrusion detection approaches for cyber-physical systems, *Proceedings of the Indian National Science Academy*, 1-15.
- Jin, H., Jeon, G., Choi, H. W. A., Jeon, S. ve Seo, J. T., 2024, A threat modeling framework for IoT-Based botnet attacks, *Heliyon*, 10 (20).
- Jony, A. I. ve Arnob, A. K. B., 2024, A long short-term memory based approach for detecting cyber attacks in IoT using CIC-IoT2023 dataset, *Journal of Edge Computing*, 3 (1), 28-42.
- Jordan, M. I. ve Mitchell, T. M., 2015, Machine learning: Trends, perspectives, and prospects, *Science*, 349 (6245), 255-260.
- Khanday, S. A., Fatima, H. ve Rakesh, N., 2024, A Novel Data Preprocessing Model for Lightweight Sensory IoT Intrusion Detection, *Int. J. Math. Eng. Manag. Sci*, 9, 188-204.
- KirstenS, 2025, Cross Site Scripting (XSS)- OWASP, <https://owasp.org/www-community/attacks/xss/>:
- Kolias, C., Kambourakis, G., Stavrou, A. ve Voas, J., 2017, DDoS in the IoT: Mirai and other botnets, *Computer*, 50 (7), 80-84.
- Krizhevsky, A., Sutskever, I. ve Hinton, G. E., 2012, Imagenet classification with deep convolutional neural networks, *Advances in neural information processing systems*, 25.
- Krzysztoń, E., Rojek, I. ve Mikołajewski, D., 2024, A Comparative Analysis of Anomaly Detection Methods in IoT Networks: An Experimental Study, *Applied Sciences*, 14 (24), 11545.
- Kumar, C. ve Ansari, M. S. A., 2024, An explainable nature-inspired cyber attack detection system in Software-Defined IoT applications, *Expert Systems with Applications*, 250, 123853.
- Langner, R., 2011, Stuxnet: Dissecting a cyberwarfare weapon, *IEEE security & privacy*, 9 (3), 49-51.
- LeCun, Y., Bengio, Y. ve Hinton, G., 2015, Deep learning, *nature*, 521 (7553), 436-444.
- Li, Y., Mandalari, A. M. ve Straw, I., 2023, Who let the smart toaster hack the house? An investigation into the security vulnerabilities of consumer IoT devices, *arXiv preprint arXiv:2306.09017*.
- Liao, H.-J., Lin, C.-H. R., Lin, Y.-C. ve Tung, K.-Y., 2013, Intrusion detection system: A comprehensive review, *Journal of Network and Computer Applications*, 36 (1), 16-24.
- Liévin, R., Jamont, J.-P. ve Hély, D., 2021, CLASA: a Cross-Layer Agent Security Architecture for networked embedded systems, *2021 IEEE International Conference on Omni-Layer Intelligent Systems (COINS)*, 1-8.
- Malwarebytes Backdoor, 2025, Backdoor-Malwarebytes, <https://www.malwarebytes.com/backdoor/>:
- Malwarebytes Browser Hijacker, 2025, Browser Hijacker-Malwarebytes, <https://www.malwarebytes.com/blog/threats/browser-hijacker/>:
- Markova, V., 2024, The Slowloris Attack: How It Works and How to Protect Your Website, <https://www.cloudns.net/blog/the-slowloris-attack-how-it-works-and-how-to-protect-your-website/>: [16.02.2025].

- Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D. ve Elovici, Y., 2018, N-baiot—network-based detection of iot botnet attacks using deep autoencoders, *IEEE Pervasive Computing*, 17 (3), 12-22.
- Mirkovic, J. ve Reiher, P., 2004, A taxonomy of DDoS attack and DDoS defense mechanisms, *ACM SIGCOMM Computer Communication Review*, 34 (2), 39-53.
- Mitchell, R. ve Chen, I.-R., 2014, A survey of intrusion detection techniques for cyber-physical systems, *ACM computing surveys (CSUR)*, 46 (4), 1-29.
- Mitchell, T. M. ve Mitchell, T. M., 1997, Machine learning, 9, McGraw-hill New York, p.
- Mithran, K. ve Gopi, C., 2022, Anomaly Detection in IoT Sensor Networks using Machine Learning, *2022 International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS)*, 1-7.
- Mvah, F., Tchendji, V. K., Djamegni, C. T., Anwar, A. H., Tosh, D. K. ve Kamhoua, C., 2024, Countering ARP spoofing attacks in software-defined networks using a game-theoretic approach, *Computers & Security*, 139, 103696.
- Narayan, K. R., Mookherji, S., Odelu, V., Prasath, R., Turlapaty, A. C. ve Das, A. K., 2023, Iids: Design of intelligent intrusion detection system for internet-of-things applications, *2023 IEEE 7th Conference on Information and Communication Technology (CICT)*, 1-6.
- Natekin, A. ve Knoll, A., 2013, Gradient boosting machines, a tutorial, *Frontiers in neurorobotics*, 7, 21.
- Neto, E. C. P., Dadkhah, S., Ferreira, R., Zohourian, A., Lu, R. ve Ghorbani, A. A., 2023, CICIOT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment, *Sensors*, 23 (13), 5941.
- Nielsen, D., 2016, Tree boosting with xgboost-why does xgboost win" every" machine learning competition?, *NTNU*.
- Niu, T., Liu, Y., Li, Q. ve Bao, Q., 2024, An Easily Scalable Docker-based Privacy-Preserving Malicious Traffic Detection Architecture for IoT Environments, *IEEE Access*.
- Ometov, A., Petrov, V., Bezzateev, S., Andreev, S., Koucheryavy, Y. ve Gerla, M., 2019, Challenges of multi-factor authentication for securing advanced IoT applications, *IEEE Network*, 33 (2), 82-88.
- OWASP File Upload, 2025, Unrestricted File Upload - OWASP, https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload:
- OWASP SQL Injection, 2025, SQL Injection - OWASP, https://owasp.org/www-community/attacks/SQL_Injection:
- Pandey, N. ve Mishra, P. K., 2025, Conditional entropy-based hybrid DDoS detection model for IoT networks, *Computers & Security*, 150, 104199.
- Pascanu, R., 2013, On the difficulty of training recurrent neural networks, *arXiv preprint arXiv:1211.5063*.
- Peng, C.-Y. J., Lee, K. L. ve Ingersoll, G. M., 2002, An introduction to logistic regression analysis and reporting, *The journal of educational research*, 96 (1), 3-14.
- Phan, V. A., Jerabek, J. ve Malina, L., 2024, Comparison of Multiple Feature Selection Techniques for Machine Learning-Based Detection of IoT Attacks, *Proceedings of the 19th International Conference on Availability, Reliability and Security*, 1-10.
- PortSwigger, 2025, Cross-Site Scripting (XSS), <https://portswigger.net/web-security/cross-site-scripting>:
- 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.
- Quinlan, J. R., 1986, Induction of decision trees, *Machine learning*, 1, 81-106.
- Raza, S., Wallgren, L. ve Voigt, T., 2013, SVELTE: Real-time intrusion detection in the Internet of Things, *Ad hoc networks*, 11 (8), 2661-2674.
- Ring, C., 2020, Hacks Lead Some to Wonder How Safe Amazon Ring Really, <https://www.businessinsider.com/hacks-lead-some-to-wonder-how-safe-amazon-ring-really-is-2020>: [27.01.2025].
- RioRey, 2025, Types of DDoS Attacks, <https://www.riorey.com/types-of-ddos-attacks>: [15.02.2025].
- Rish, I., 2001, An empirical study of the naive Bayes classifier, *IJCAI 2001 workshop on empirical methods in artificial intelligence*, 41-46.
- Roman, R., Najera, P. ve Lopez, J., 2011, Securing the internet of things, *Computer*, 44 (9), 51-58.
- Rumelhart, D. E., Hinton, G. E. ve Williams, R. J., 1986, Learning representations by back-propagating errors, *nature*, 323 (6088), 533-536.
- Sadeghi, A.-R., Wachsmann, C. ve Waidner, M., 2015, Security and privacy challenges in industrial internet of things, *Proceedings of the 52nd annual design automation conference*, 1-6.
- Saito, T. ve Rehmsmeier, M., 2015, The precision-recall plot is more informative than the ROC plot when evaluating binary classifiers on imbalanced datasets, *PloS one*, 10 (3), e0118432.
- Saputra, R. ve Noranita, B., 2019, Analysis of GPGPU-Based Brute-Force and Dictionary Attack on SHA-1 Password Hash, *2019 3rd International Conference on Informatics and Computational Sciences (ICICoS)*, 1-4.
- Satılmış, H. ve Akleylek, S., 2021, IoT Güvenliği İçin Kullanılan Makine Öğrenimi ve Derin Öğrenme Modelleri Üzerine bir Derleme, *Bilişim Teknolojileri Dergisi*, 14 (4), 457-481.
- Sayed, G. I. ve Hassanien, A. E., 2024, An optimized and intelligent metaverse intrusion detection system based on rough sets, *Internet of Things*, 28, 101360.
- Schmidhuber, J., 2015, Deep learning in neural networks: An overview, Elsevier.
- Sharafaldin, I., Lashkari, A. H. ve Ghorbani, A. A., 2018a, Toward generating a new intrusion detection dataset and intrusion traffic characterization, *ICISSp*, 1, 108-116.
- Sharafaldin, I., Lashkari, A. H. ve Ghorbani, A. A., 2018b, Toward generating a new intrusion detection dataset and intrusion traffic characterization, *ICISSp*, 1 (2018), 108-116.
- Sicari, S., Rizzardi, A., Grieco, L. A. ve Coen-Porisini, A., 2015, Security, privacy and trust in Internet of Things: The road ahead, *Computer networks*, 76, 146-164.
- Sokolova, M. ve Lapalme, G., 2009, A systematic analysis of performance measures for classification tasks, *Information processing & management*, 45 (4), 427-437.
- Subhan, A., Kunang, Y. N. ve Yadi, I. Z., 2023, Analyzing the Attack Pattern of Brute Force Attack on SSH Port, *2023 International Conference on Information Technology and Computing (ICITCOM)*, 67-72.
- Systems, C., 2019, The DNA of Mirai: Modern IoT Attack Botnets.
- Şimşek, M. M. ve Atılgan, E., 2024, DoS and DDoS Attacks on Internet of Things and Their Detection by Machine Learning Algorithms, *Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi*, 15 (2), 341-353.
- Taş, O., 2022, Nesnelerin İnterneti İçin Akıllı Saldırı Tespit Sistemleri Geliştirilmesi, Doktora Tezi, *İstanbul Üniversitesi*.

- Taşcı, B., 2024, Deep-Learning-Based Approach for IoT Attack and Malware Detection, *Applied Sciences* (2076-3417), 14 (18).
- Tseng, S.-M., Wang, Y.-Q. ve Wang, Y.-C., 2024, Multi-Class Intrusion Detection Based on Transformer for IoT Networks Using CIC-IoT-2023 Dataset, *Future Internet*, 16 (8), 284.
- Ullah, F., Turab, A., Ullah, S., Cacciagrano, D. ve Zhao, Y., 2024, Enhanced network intrusion detection system for internet of things security using multimodal big data representation with transfer learning and game theory, *Sensors*, 24 (13), 4152.
- Vailshery, L. S., 2023, Number of IoT connected devices worldwide 2019-2023, with forecasts to 2030, *Statista*. Accessed: Nov, 10.
- Vajrobol, V., Gupta, B. B., Gaurav, A. ve Chuang, H.-M., 2024, Adversarial learning for Mirai botnet detection based on long short-term memory and XGBoost, *International Journal of Cognitive Computing in Engineering*, 5, 153-160.
- Verkada, 2021, Summary: March 9, 2021 Security Incident Report, <https://www.verkada.com/security-update/report/>: [27.01.2025].
- Villegas-Ch, W., Gutierrez, R., Sánchez-Salazar, I. ve Mera-Navarrete, A., 2024, Adaptive Security Framework for the Internet of Things: Improving Threat Detection and Energy Optimization in Distributed Environments, *IEEE Access*.
- Wang, J., Yang, K. ve Li, M., 2024a, NIDS-FGPA: A federated learning network intrusion detection algorithm based on secure aggregation of gradient similarity models, *PloS one*, 19 (10), e0308639.
- Wang, X., Dai, L. ve Yang, G., 2024b, A network intrusion detection system based on deep learning in the IoT, *The Journal of Supercomputing*, 80 (16), 24520-24558.
- Weber, R. H., 2010, Internet of Things–New security and privacy challenges, *Computer law & security review*, 26 (1), 23-30.
- Yang, K., Wang, J. ve Li, M., 2024, An improved intrusion detection method for IIoT using attention mechanisms, BiGRU, and Inception-CNN, *Scientific Reports*, 14 (1), 19339.
- Zargar, S. T., Joshi, J. ve Tipper, D., 2013, A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks, *IEEE communications surveys & tutorials*, 15 (4), 2046-2069.
- Zarpelão, B. B., Miani, R. S., Kawakani, C. T. ve De Alvarenga, S. C., 2017, A survey of intrusion detection in Internet of Things, *Journal of Network and Computer Applications*, 84, 25-37.
- Zhao, K. ve Ge, L., 2013, A survey on the internet of things security, 2013 *Ninth international conference on computational intelligence and security*, 663-667.
- Zhong, W., 2025, Command Injection, https://owasp.org/www-community/attacks/Command_Injection: