MARMARA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

NESNELERİN İNTERNETİ TABANLI AĞLARDA DERİN ÖĞRENME İLE SALDIRI TESPİTİ

NADİR CAN KAVKAS

YÜKSEK LİSANS TEZİ

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Yüksek Lisans Programı

DANIŞMAN

Doç. Dr. Kazım YILDIZ

İSTANBUL, 2024

MARMARA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

NESNELERİN İNTERNETİ TABANLI AĞLARDA DERİN ÖĞRENME İLE SALDIRI TESPİTİ

NADİR CAN KAVKAS

523622604

YÜKSEK LİSANS TEZİ

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Yüksek Lisans Programı

DANIŞMAN

Doç. Dr. Kazım YILDIZ

İSTANBUL, 2024

ÖNSÖZ

Tez çalışmam sürecinde her konuda sabırla destek olan, her fırsatta yardımını sağlamayı esirgemeyen değerli tez danışman hocam Doç.Dr. Kazım YILDIZ'a,

Tez çalışmam süresince desteğini ve sabrını sürekli yanımda hissettiğim kıymetli eşime ve bugünlere ulaşmamda büyük katkı sahibi olan değerli anne ve babama

Teşekkürlerimi sunarım.

ARALIK, 2024 **Nadir Can KAVKAS**

İÇİNDEKİLER

	SAYFA
ÖNSÖZ	**i**
İÇİNDEKİLER	**ii**
ÖZET	**v**
ABSTRACT	**vi**
SEMBOLLER	**vii**
KISALTMALAR	**viii**
ŞEKİL LİSTESİ	**xiv**
TABLO LİSTESİ	**xvii**
1. GİRİŞ	**1**
1.1. Genel Bakış	**1**
1.1.1. Problemin Tanımı	2
1.1.2. Amaç ve Hedef	3
1.1.3. Ana Katkılar	4
1.1.4. Tez Organizasyonu	5
1.2. IoT Tanımı ve Temel Kavramlar	**6**
1.2.1. IoT Mimarisi ve Protokolleri	7
1.2.2. IoT Uygulama Alanları	10
1.2.3. IoT Güvenlik Sorunları ve Açık Problemler	11
1.3. IoV Tanımı ve Temel Kavramlar	**14**
1.3.1. IoV Mimarisi ve Protokolleri	16
1.3.2. IoV Uygulama Alanları	18
1.3.3. IoV Güvenlik Sorunları ve Açık Problemler	19
1.4. IoMT Tanımı ve Temel Kavramlar	**21**
1.4.1. IoMT Mimarisi ve Protokolleri	22
1.4.2. IoMT Uygulama Alanları	24
1.4.3. IoMT Güvenlik Sorunları ve Açık Problemler	25

1.5. Literatürde Yapılan Çalışmalar **27**
1.5.1. IoV Güvenliği Üzerine Yapılan Çalışmalar 27
1.5.2. IoMT Güvenliği Üzerine Yapılan Çalışmalar 30
1.5.3. CICIoV2024 Veri Seti Kullanılan Çalışmalar 31
1.5.4. CICIoMT2024 Veri Seti Kullanılan Çalışmalar 34
2. MATERYAL VE YÖNTEM **37**
2.1. Kullanılan Veri Setleri **37**
2.1.1. CICIoV2024 Veri Seti 37
2.1.2. CICIoMT2024 Veri Seti 42
2.2. Derin Öğrenme **48**
2.2.1. Yapay Sinir Ağları 49
2.2.2. İleri Besleme 51
2.2.3. Kayıp Fonksiyonu 51
2.2.4. Geriye Yayılım Algoritması 51
2.2.5. Aktivasyon Fonksiyonları 52
2.2.6. Mini-batch Boyutu 52
2.2.7. Optimizasyon Algoritmaları 53
2.2.8. Epoch Zamanı 53
2.3. Derin Öğrenme Modelleri Performans Metrikleri **53**
2.3.1. Karmaşıklık Matrisi 54
2.3.2. Doğruluk Performans Metriği 54
2.3.3. Kesinlik Performans Metriği 55
2.3.4. Duyarlılık Performans Metriği 55
2.3.5. F1-skoru Performans Metriği 56
2.4. Tez Çalışmasında Kullanılan Derin Öğrenme Mimarileri **56**
2.4.1. Evrişimli Sinir Ağları (CNN) Mimarisi 56
2.4.2. Derin Sinir Ağları (DNN) Mimarisi 58
2.4.3. Uzun-Kısa Süreli Bellek (LSTM) Mimarisi 59
2.5. Deney Ortamı **60**

2.6. CICIoV2024 Veri Seti Üzerinde Yapılan Deneyler **61**
2.6.1. Veri Ön İşleme 61
2.6.2. Önerilen CNN Modeli 63
2.6.3. Önerilen DNN Modeli 64
2.6.4. Önerilen LSTM Modeli 65
2.7. CICIoMT2024 Veri Seti Üzerinde Yapılan Deneyler **66**
2.7.1. Veri Ön İşleme 66
2.7.2. Önerilen CNN Modeli 68
2.7.3. Önerilen DNN Modeli 69
2.7.4. Önerilen LSTM Modeli 70
3. BULGULAR VE TARTIŞMA **72**
3.1. CICIoV2024 Deney Sonuçları **72**
3.1.1. CNN Modeli Sonuçları 74
3.1.2. DNN Modeli Sonuçları 80
3.1.3. LSTM Modeli Sonuçları 86
3.2. CICIoMT2024 Deney Sonuçları **92**
3.2.1. CNN Modeli Sonuçları 93
3.2.2. DNN Modeli Sonuçları 97
3.2.3. LSTM Modeli Sonuçları 100
3.3. Literatürdeki Sonuçlarla Karşılaştırma **103**
3.3.1. CICIoV2024 Veri Seti 103
3.3.2. CICIoMT2024 Veri Seti 104
4.SONUÇLAR **106**
KAYNAKLAR **108**
ÖZGEÇMİŞ **124**

ÖZET

NESNELERİN İNTERNETİ TABANLI AĞLARDA DERİN ÖĞRENME İLE SALDIRI TESPİTİ

Araçların İnterneti (IoV) ve Tıbbi Nesnelerin İnterneti (IoMT) sistemlerinin hızla yaygınlaşması, bu sistemlerin güvenliğini kritik bir öncelik haline getirmektedir. Bu tez çalışması, IoV ve IoMT sistemlerinde oluşabilecek siber saldırıların tespiti için derin öğrenme tabanlı yeni bir yaklaşım önermektedir. Tez çalışmasında, Evrişimli Sinir Ağları (CNN), Derin Sinir Ağları (DNN) ve Uzun-Kısa Süreli Bellek (LSTM) mimarilerini içeren üç farklı model geliştirilmiş ve bu modeller kapsamlı deneylerle test edilmiştir.

Bu tez çalışmasında yapılan deneylerde CICIoV2024 ve CICIoMT2024 veri setleri kullanılmıştır. CICIoV2024 veri seti üzerinde yapılan deneylerde, önerilen modeller ikili ve üçlü sınıflandırmada mükemmel başarı gösterirken, altılı sınıflandırmada da yüksek doğruluk oranlarına ulaşmıştır. CICIoMT2024 veri seti deneylerinde ise ikili sınıflandırmada çok yüksek doğruluk elde edilmiş, sınıf sayısı arttıkça modelin performansı kademeli olarak değişkenlik göstermiştir. Özellikle LSTM mimarisi, karmaşık saldırı desenlerini tespit etmede üstün performans sergilemiştir.

Deneysel sonuçlar, önerilen yaklaşımların literatürdeki mevcut çalışmalara kıyasla daha başarılı olduğunu göstermektedir. Bu tez çalışması, IoV ve IoMT sistemlerinin güvenliğini artırmak için etkili ve ölçeklenebilir çözümler sunmakta ve gelecekteki araştırmalar için yeni perspektifler sağlamaktadır.

ARALIK, 2024 **Nadir Can KAVKAS**

ABSTRACT

DEEP LEARNING BASED ATTACK DETECTION IN INTERNET OF THINGS NETWORKS

The rapid proliferation of Internet of Vehicles (IoV) and Internet of Medical Things (IoMT) systems has made security a critical priority for these infrastructures. This thesis proposes a novel deep learning-based approach for detecting cyber attacks in IoV and IoMT systems. The research develops and extensively tests three distinct models incorporating Convolutional Neural Networks (CNN), Deep Neural Networks (DNN), and Long Short-Term Memory (LSTM) architectures.

The experimental phase of this thesis utilizes the CICIoV2024 and CICIoMT2024 datasets. In experiments conducted on the CICIoV2024 dataset, the proposed models achieved excellent performance in binary and triple classification tasks while maintaining high accuracy rates in six-class classification scenarios. For the CICIoMT2024 dataset experiments, while binary classification yielded exceptionally high accuracy, model performance showed gradual variability as the number of classes increased. The LSTM architecture demonstrated superior performance in detecting complex attack patterns.

The experimental results indicate that the proposed approaches outperform existing studies in literature. This thesis presents effective and scalable solutions for enhancing the security of IoV and IoMT systems while providing new perspectives for future research endeavors.

DECEMBER, 2024 **Nadir Can KAVKAS**

SEMBOLLER

w_{ij}	:	Nöronun ağırlık vektörü
Z	:	Nöronun ön yargı değeri
α_j	:	Net girdi değeri
β_j	:	Nöronun çıktı değeri
g_i	:	Aktivasyon fonksiyonu
e	:	Euler sayısı
$\sum$	:	Toplam
L	:	Kayıp fonksiyonu
log	:	Doğal logaritma
t	:	Adım sayısı
λ	:	Adım boyutu
ϵ	:	Çok küçük bir değer
W_t	:	Ağırlık vektörü
f	:	Fonksiyon
i	:	Gizli katman sayısı
j	:	Nöron sayısı
x	:	Girdi vektörü

KISALTMALAR

A2C	**:**	Advantage Actor-Critic (Avantaj Aktör-Kritik)
AB	**:**	AdaBoost (Adaptif Güçlendirme)
ACK	**:**	Acknowledgment (Onay)
Adam	**:**	Adaptive Moment Estimation (Uyarlanabilir Moment Tahmini)
AMQP	**:**	Advanced Message Queuing Protocol (Gelişmiş Mesaj Kuyruklama Protokolü)
ARP	**:**	Address Resolution Protocol (Adres Çözümleme Protokolü)
AUC	**:**	Area Under Curve (Eğri Altındaki Alan)
AVG	**:**	Average (Ortalama)
BLE	**:**	Bluetooth Low Energy (Düşük Enerjili Bluetooth)
CAN	**:**	Controller Area Network (Kontrol Alan Ağı)
CBLOF	**:**	Cluster-Based Local Outlier Factor (Küme Tabanlı Yerel Aykırı Değer Faktörü)
CIC	**:**	Canadian Institute for Cybersecurity (Kanada Siber Güvenlik Enstitüsü)
CICIoMT2024	**:**	Canadian Institute for Cybersecurity Internet of Medical Things 2024 (Kanada Siber Güvenlik Enstitüsü Tıbbi Nesnelerin İnterneti 2024)
CICIoV2024	**:**	Canadian Institute for Cybersecurity Internet of Vehicles 2024 (Kanada Siber Güvenlik Enstitüsü Araçların İnterneti 2024)
CNN	**:**	Convolutional Neural Network (Evrişimli Sinir Ağı)
CoAP	**:**	Constrained Application Protocol (Kısıtlı Uygulama Protokolü)
CSV	**:**	Comma-Separated Values (Virgülle Ayrılmış Değerler)
CWR	**:**	Congestion Window Reduced (Tıkanıklık Penceresi Azaltıldı)
DBN	**:**	Deep Belief Network (Derin İnanç Ağı)
DCNN	**:**	Deep Convolutional Neural Network (Derin Evrişimli Sinir Ağı)

DDoS	:	Distributed Denial of Service (Dağıtık Hizmet Engelleme)
DHCP	:	Dynamic Host Configuration Protocol (Dinamik Ana Bilgisayar Yapılandırma Protokolü)
DNS	:	Domain Name System (Alan Adı Sistemi)
DNN	:	Deep Neural Network (Derin Sinir Ağı)
DoS	:	Denial of Service (Hizmet Engelleme)
DPKT	:	Data Packet (Veri Paketi)
DQN	:	Deep Q-Network (Derin Q-Ağı)
DRL	:	Deep Reinforcement Learning (Derin Pekiştirmeli Öğrenme)
DSRC	:	Dedicated Short-Range Communications (Adanmış Kısa Menzilli Haberleşme)
DT	:	Decision Tree (Karar Ağacı)
DTLS	:	Datagram Transport Layer Security (Datagram Taşıma Katmanı Güvenliği)
ECE	:	ECN-Echo (ECN-Yankı)
ECU	:	Electronic Control Unit (Elektronik Kontrol Ünitesi)
ELM32	:	Embedded Lightweight Module 32 (Gömülü Hafif Modül 32)
ETSI	:	European Telecommunications Standards Institute (Avrupa Telekomünikasyon Standartları Enstitüsü)
FDA	:	Food and Drug Administration (Gıda ve İlaç İdaresi)
FIN	:	Finish (Bitiş)
FL	:	Federated Learning (Fedele Öğrenme)
FN	:	False Negative (Yanlış Negatif)
FP	:	False Positive (Yanlış Pozitif)
GDPR	:	General Data Protection Regulation (Genel Veri Koruma Yönetmeliği)

GPU	:	Graphics Processing Unit (Grafik İşlem Birimi)
GRU	:	Gated Recurrent Unit (Geçitli Tekrarlayan Birim)
HTTP	:	Hypertext Transfer Protocol (Köprü Metni Aktarım Protokolü)
HTTPS	:	Hypertext Transfer Protocol Secure (Güvenli Köprü Metni Aktarım Protokolü)
IAT	:	Inter-Arrival Time (Varışlar Arası Süre)
ICMP	:	Internet Control Message Protocol (İnternet Kontrol Mesaj Protokolü)
IDS	:	Intrusion Detection System (Saldırı Tespit Sistemi)
IForest	:	Isolation Forest (İzolasyon Ormanı)
IGMP	:	Internet Group Management Protocol (İnternet Grup Yönetim Protokolü)
IIoT	:	Industrial Internet of Things (Endüstriyel Nesnelerin İnterneti)
IoMT	:	Internet of Medical Things (Tıbbi Nesnelerin İnterneti)
IoT	:	Internet of Things (Nesnelerin İnterneti)
IoV	:	Internet of Vehicles (Araçların İnterneti)
IPv	:	Internet Protocol version (İnternet Protokolü versiyonu)
IPv6	:	Internet Protocol version 6 (İnternet Protokolü versiyon 6)
IRC	:	Internet Relay Chat (İnternet Aktarmalı Sohbet)
KNN	:	K-Nearest Neighbors (K-En Yakın Komşu)
L1/L2	:	Layer 1/Layer 2 (Katman 1/Katman 2)
LCCDE	:	Local Cascade Composition Differential Evolution (Yerel Kaskad Kompozisyon Diferansiyel Evrimi)
LLC	:	Logical Link Control (Mantıksal Bağlantı Kontrolü)
LOF	:	Local Outlier Factor (Yerel Aykırı Değer Faktörü)
LR	:	Logistic Regression (Lojistik Regresyon)

LSTM	:	Long Short-Term Memory (Uzun-Kısa Süreli Bellek)
MAX	:	Maximum (Maksimum)
MIN	:	Minimum (Minimum)
ML	:	Machine Learning (Makine Öğrenmesi)
MLP	:	Multi-Layer Perceptron (Çok Katmanlı Algılayıcı)
MOST	:	Media Oriented Systems Transport (Medya Odaklı Sistemler Taşıması)
MQTT	:	Message Queuing Telemetry Transport (Mesaj Kuyruklama Telemetri Taşıma)
NB	:	Naive Bayes (Saf Bayes)
NFC	:	Near Field Communication (Yakın Alan İletişimi)
NIST	:	National Institute of Standards and Technology (Ulusal Standartlar ve Teknoloji Enstitüsü)
OBD	:	On-Board Diagnostics (Araç İçi Teşhis)
OS	:	Operating System (İşletim Sistemi)
PCAP	:	Packet Capture (Paket Yakalama)
PPO	:	Proximal Policy Optimization (Proksimal Politika Optimizasyonu)
PSH	:	Push (İtme)
RAM	:	Random Access Memory (Rastgele Erişimli Bellek)
ReLU	:	Rectified Linear Unit (Doğrultulmuş Doğrusal Birim)
REST	:	Representational State Transfer (Temsili Durum Aktarımı)
RF	:	Random Forest (Rastgele Orman)
RFE	:	Recursive Feature Elimination (Özyinelemeli Öznitelik Eleme)
RFID	:	Radio Frequency Identification (Radyo Frekansı ile Tanımlama)
RNN	:	Recurrent Neural Network (Tekrarlayan Sinir Ağı)

ROC	:	Receiver Operating Characteristic (Alıcı İşletim Karakteristiği)
RST	:	Reset (Sıfırlama)
RSU	:	Road Side Unit (Yol Kenarı Birimi)
SDN	:	Software Defined Network (Yazılım Tanımlı Ağ)
SHAP	:	SHapley Additive exPlanations (Shapley Katkısal Açıklamalar)
SMOTE	:	Synthetic Minority Over-sampling Technique (Sentetik Azınlık Aşırı Örnekleme Tekniği)
SMTP	:	Simple Mail Transfer Protocol (Basit Posta Transfer Protokolü)
SSH	:	Secure Shell (Güvenli Kabuk)
STD	:	Standard Deviation (Standart Sapma)
SVM	:	Support Vector Machine (Destek Vektör Makinesi)
SYN	:	Synchronize (Senkronizasyon)
TCP	:	Transmission Control Protocol (İletim Kontrol Protokolü)
TLS	:	Transport Layer Security (Taşıma Katmanı Güvenliği)
TN	:	True Negative (Doğru Negatif)
TOT	:	Total (Toplam)
TP	:	True Positive (Doğru Pozitif)
TRPO	:	Trust Region Policy Optimization (Güven Bölgesi Politika Optimizasyonu)
UDP	:	User Datagram Protocol (Kullanıcı Datagram Protokolü)
UMAP	:	Uniform Manifold Approximation and Projection (Tekdüze Manifolt Yaklaşımı ve Projeksiyon)
USB	:	Universal Serial Bus (Evrensel Seri Veri yolu)

USB2CAN	:	Universal Serial Bus to Controller Area Network (Evrensel Seri Veri Yolu'ndan Kontrol Alan Ağı'na)
UUID	:	Universally Unique Identifier (Evrensel Benzersiz Tanımlayıcı)
V2I	:	Vehicle to Infrastructure (Araçtan Altyapıya)
V2N	:	Vehicle to Network (Araçtan Ağa)
V2P	:	Vehicle to Pedestrian (Araçtan Yayaya)
V2S	:	Vehicle to Service (Araçtan Servise)
V2V	:	Vehicle to Vehicle (Araçtan Araca)
V2X	:	Vehicle to Everything (Araçtan Her şeye)
VANET	:	Vehicular Ad Hoc Network (Araçsal Özel Ağ)
VCAN	:	Virtual Controller Area Network (Sanal Kontrol Alan Ağı)
Wi-Fi	:	Wireless Fidelity (Kablosuz Bağlantı)
XAI	:	Explainable Artificial Intelligence (Açıklanabilir Yapay Zeka)
YSA	:	Yapay Sinir Ağları (Artificial Neural Networks)
6LoWPAN	:	IPv6 over Low-Power Wireless Personal Area Networks (Düşük Güçlü Kablosuz Kişisel Alan Ağları üzerinden IPv6)

ŞEKİL LİSTESİ

SAYFA

Şekil 1.1. IoT Ekosistemindeki Birbiriyle Bağlı Cihazlar.....6

Şekil 1.2. IoT Ekosistemindeki Dört Temel Bileşen.....8

Şekil 1.3. Araçların İnterneti Mimarisi.....15

Şekil 1.4. Küresel IoMT pazarının yıllara göre büyüklüğü 2032 yılına kadar yapılan tahminler…22

Şekil 2.1. Ford model aracın kontrol ünitelerinin laboratuvar ortamına aktarılması.....37

Şekil 2.2. Veri setinin oluşturulması için kullanılan test ortamı.....38

Şekil 2.3. Veri setinin oluşturulması için kullanılan test ortamı.....43

Şekil 2.4. CICIoMT2024 Ağ Topolojisi.....43

Şekil 2.5. Biyolojik Sinir Hücresi ve Yapay Sinir Hücresi.....49

Şekil 2.6. Bir yapay sinir ağının genel yapısı.....49

Şekil 2.7. Bir yapay nöronun yapısı ve matematiksel gösterimi.....50

Şekil 2.8. CNN Mimarisi.....57

Şekil 2.9. DNN Mimarisi.....58

Şekil 2.10. LSTM Hücresi Mimarisi.....59

Şekil 2.11. CICIoV2024 veri setinin ön işleme adımları.....62

Şekil 2.12. CICIoMT2024 veri setinin ön işleme adımları.....67

Şekil.3.1. İkili tabandaki veri setinin ikili sınıflandırma eğitiminin doğruluk ve kayıp grafikleri..74

Şekil.3.2. İkili tabandaki veri setinin ikili sınıflandırma testinin karmaşıklık matrisi.....74

Şekil.3.3. İkili tabandaki veri setinin üçlü sınıflandırma eğitiminin doğruluk ve kayıp grafikleri..75

Şekil.3.4. İkili tabandaki veri setinin üçlü sınıflandırma testinin karmaşıklık matrisi.....75

Şekil.3.5. İkili tabandaki veri setinin altılı sınıflandırma eğitiminin doğruluk ve kayıp grafikleri.76

Şekil.3.6. İkili tabandaki veri setinin altılı sınıflandırma eğitiminin doğruluk ve kayıp grafikleri.76

Şekil.3.7. Onluk tabandaki veri setinin ikili sınıflandırma eğitiminin doğruluk ve kayıp graf.....77

Şekil.3.8. Onluk tabandaki veri setinin ikili sınıflandırma testinin karmaşıklık matrisi.....77

Şekil.3.9. Onluk tabandaki veri setinin üçlü sınıflandırma eğitiminin doğruluk ve kayıp graf....78

Şekil.3.10. Onluk tabandaki veri setinin üçlü sınıflandırma testinin karmaşıklık matrisi.....78

Şekil.3.11. Onluk tabandaki veri setinin altılı sınıflandırma eğitiminin doğruluk ve kayıp graf..79

Şekil.3.12. Onluk tabandaki veri setinin altılı sınıflandırma testinin karmaşıklık matrisi.....79

Şekil.3.13. İkili tabandaki veri setinin ikili sınıflandırma eğitiminin doğruluk ve kayıp graf.....80

Şekil.3.14. İkili tabandaki veri setinin ikili sınıflandırma testinin karmaşıklık matrisi..... 80

Şekil.3.15. İkili tabandaki veri setinin üçlü sınıflandırma eğitiminin doğruluk ve kayıp graf.....81

Şekil.3.16. İkili tabandaki veri setinin üçlü sınıflandırma testinin karmaşıklık matrisi.....81

Şekil.3.17. İkili tabandaki veri setinin altılı sınıflandırma eğitiminin doğruluk ve kayıp graf.....82

Şekil.3.18. İkili tabandaki veri setinin altılı sınıflandırma testinin karmaşıklık matrisi.....82

Şekil.3.19. Onluk tabandaki veri setinin ikili sınıflandırma eğitiminin doğruluk ve kayıp graf....83

Şekil.3.20. Onluk tabandaki veri setinin ikili sınıflandırma testinin karmaşıklık matrisi.....83

Şekil.3.21. Onluk tabandaki veri setinin üçlü sınıflandırma eğitiminin doğruluk ve kayıp graf...84

Şekil.3.22. Onluk tabandaki veri setinin üçlü sınıflandırma testinin karmaşıklık matrisi.....84

Şekil.3.23. Onluk tabandaki veri setinin altılı sınıflandırma eğitiminin doğruluk ve kayıp graf...85

Şekil.3.24. Onluk tabandaki veri setinin altılı sınıflandırma testinin karmaşıklık matrisi.....85

Şekil.3.25. İkili tabandaki veri setinin ikili sınıflandırma eğitiminin doğruluk ve kayıp graf.....86

Şekil.3.26. İkili tabandaki veri setinin ikili sınıflandırma testinin karmaşıklık matrisi.....86

Şekil.3.27. İkili tabandaki veri setinin üçlü sınıflandırma eğitiminin doğruluk ve kayıp graf.....87

Şekil.3.28. İkili tabandaki veri setinin üçlü sınıflandırma testinin karmaşıklık matrisi.....87

Şekil.3.29. İkili tabandaki veri setinin altılı sınıflandırma eğitiminin doğruluk ve kayıp graf.....88

Şekil.3.30. İkili tabandaki veri setinin altılı sınıflandırma testinin karmaşıklık matrisi.....88

Şekil.3.31. Onluk tabandaki veri setinin ikili sınıflandırma eğitiminin doğruluk ve kayıp graf.....89

Şekil.3.32. Onluk tabandaki veri setinin ikili sınıflandırma testinin karmaşıklık matrisi.....89

Şekil.3.33. Onluk tabandaki veri setinin üçlü sınıflandırma eğitiminin doğruluk ve kayıp graf.....90

Şekil.3.34. Onluk tabandaki veri setinin üçlü sınıflandırma testinin karmaşıklık matrisi.....90

Şekil.3.35. Onluk tabandaki veri setinin altılı sınıflandırma eğitiminin doğruluk ve kayıp graf....91

Şekil.3.36. Onluk tabandaki veri setinin altılı sınıflandırma testinin karmaşıklık matrisi.....91

Şekil.3.37. İkili sınıflandırma eğitiminin doğruluk ve kayıp grafikleri.....94

Şekil.3.38. İkili sınıflandırma testinin karmaşıklık matrisi.....94

Şekil.3.39. Altılı sınıflandırma eğitiminin doğruluk ve kayıp grafikleri.....95

Şekil.3.40. Altılı sınıflandırma testinin karmaşıklık matrisi.....95

Şekil.3.41. On dokuzlu sınıflandırma eğitiminin doğruluk ve kayıp grafikleri.....96

Şekil.3.42. On dokuzlu sınıflandırma testinin karmaşıklık matrisi.....96

Şekil.3.43. İkili sınıflandırma eğitiminin doğruluk ve kayıp grafikleri.....97

Şekil.3.44. İkili sınıflandırma testinin karmaşıklık matrisi.....97

Şekil.3.45. Altılı sınıflandırma eğitiminin doğruluk ve kayıp grafikleri.....98

Şekil.3.46. Altılı sınıflandırma testinin karmaşıklık matrisi.....98

Şekil.3.47. On dokuzlu sınıflandırma eğitiminin doğruluk ve kayıp grafikleri.....99

Şekil.3.48. On dokuzlu sınıflandırma testinin karmaşıklık matrisi.....99

Şekil.3.49. İkili sınıflandırma eğitiminin doğruluk ve kayıp grafikleri.....100

Şekil.3.50. İkili sınıflandırma testinin karmaşıklık matrisi.....100

Şekil.3.51. Altılı sınıflandırma eğitiminin doğruluk ve kayıp grafikleri.....101

Şekil.3.52. Altılı sınıflandırma testinin karmaşıklık matrisi.....101

Şekil.3.53. On dokuzlu sınıflandırma eğitiminin doğruluk ve kayıp grafikleri.....102

Şekil.3.54. On dokuzlu sınıflandırma testinin karmaşıklık matrisi.....102

TABLO LİSTESİ

SAYFA

Tablo 1.1. Yaygın IoT protokollerinin karşılaştırması.....9

Tablo 1.2. Yaygın IoV protokollerinin temel özelliklerini ve uygulama alanları.....17

Tablo 1.3. IoMT cihazlarının sağlık hizmetlerindeki uygulama örnekleri.....21

Tablo 2.1. CAN Protokolü Paket Yapısı.....38

Tablo 2.2. CICIoV2024 veri setindeki bulunan sınıflar ve örnek sayıları.....40

Tablo 2.3. CICIoV2024 veri setindeki sunulan özellikler.....41

Tablo 2.4. IoMT protokollerinin temel özellikleri.....42

Tablo 2.5. CICIoMT2024 veri setindeki sunulan özellikler.....45

Tablo 2.6. CICIoMT2024 veri setindeki saldırı türleri ve örnek sayıları.....47

Tablo 2.7. Karmaşıklık Matrisi.....54

Tablo 2.8. Önerilen CNN Modelinin Katmanları.....63

Tablo 2.9. Önerilen CNN Modelinin Hiper Parametreleri.....63

Tablo 2.10. Önerilen DNN Modelinin Katmanları.....64

Tablo 2.11. Önerilen DNN Modelinin Hiper Parametreleri.....65

Tablo 2.12. Önerilen LSTM Modelinin Katmanları.....65

Tablo 2.13. Önerilen LSTM Modelinin Hiper Parametreleri.....66

Tablo 2.14. Önerilen CNN Modelinin Katmanları.....68

Tablo 2.15. Önerilen CNN Modelinin Hiper Parametreleri.....68

Tablo 2.16. Önerilen DNN Modelinin Katmanları.....69

Tablo 2.17. Önerilen DNN Modelinin Hiper Parametreleri.....69

Tablo 2.18. Önerilen LSTM Modelinin Katmanları.....70

Tablo 2.19. Önerilen LSTM Modelinin Hiper Parametreleri.....71

Tablo 3.1. CICIoV2024 veri setinin deney sonuçları.....73

Tablo 3.2. CICIoMT2024 veri setinin deney sonuçları.....93

Tablo 3.3. CICIoV2024 veri seti üzerinde yapılan çalışma ile önerilen modeli karşılaştırma...103

Tablo 3.4. CICIoMT2024 veri seti üzerinde yapılan çalışma ile önerilen modeli karşlaştırma.104

1. GİRİŞ

1.1. Genel Bakış

Nesnelerin İnterneti (IoT(Internet of Things)), fiziksel nesnelerin internet üzerinden birbirleriyle ve diğer cihazlarla bağlantı kurarak veri alışverişi yapmalarını sağlayan devrim niteliğinde bir paradigmadır [1]. IoT teknolojileri, sensörler, işlemciler, haberleşme modülleri ve yazılımlar sayesinde nesnelerin akıllı hale getirilmesine ve internet üzerinden kontrolünün sağlanmasına olanak tanır. Bu sayede evler, arabalar, fabrikalar ve hatta şehirler birer akıllı sisteme dönüşmektedir.

IoT'nin sağladığı bağlantı ve otomasyon yetenekleri, endüstri, sağlık, enerji, ulaşım, tarım gibi birçok çeşitli sektörde verimliliği ve konforu artırma potansiyeline içerir [2]. Örneğin IoT cihazlarıyla donatılmış fabrikalar, üretim süreçlerini gerçek zamanlı olarak izleyerek optimize edebilir ve önleyici bakım sayesinde makine arızalarını önceden tespit edebilir [3]. Benzer şekilde akıllı sağlık sistemleri, hastaların takibinin ve teşhisinin uzaktan yapılmasını mümkün kılarak sağlık hizmetlerinin kalitesini ve erişilebilirliğini artırabilir [4].

Ancak IoT'nin sunduğu tüm bu faydaların yanında, beraberinde getirdiği güvenlik ve gizlilik riskleri de dikkate almak gerekir. IoT cihazlarının kısıtlı kapasiteleri, heterojen yapısı ve geniş yayılımı, onları bilinen siber tehditlere karşı daha zayıf hale getirmektedir [5]. Örneğin güvenlik yönünden zayıf kimlik doğrulama mekanizmaları, yetkisiz erişim ve veri sızıntısı risklerini artırmaktadır. Ayrıca yazılımlarının güncel haliyle korunmayan cihazlar, kötü amaçlı yazılımların hedefi haline gelebilmektedir.

IoT güvenliğinin önemli bir boyutu da kritik altyapılara entegre IoT sistemlerinin oluşturduğu risklerdir. Örneğin şehirlerdeki akıllı enerji şebekelerindeki güvenlik açıkları, enerji arzını kesintiye uğratabilir ve toplumsal düzeni bozabilir [6]. Benzer şekilde otonom sürüşe sahip araçlardaki yazılım hatalarının yol açabileceği trafik kazaları, insan hayatını tehlikeye atabilir [7].

Bahsedilen tüm bu riskler, IoT güvenliğinin kapsamlı ve çok katmanlı bir yaklaşımla ele alınması gerektiğini ortaya koymaktadır. Literatür incelendiğinde görünen pek çok çalışma, IoT'ye özgü güvenlik gereksinimlerinin, mevcut güvenlik yöntemleriyle tam olarak çözülmediğini göstermektedir [8], [9]. Günümüzde özellikle ölçeklenebilir, esnek ve gerçek zamanlı güvenlik

sistemlerine ihtiyaç duyulmaktadır. Bu kapsamda, derin öğrenme gibi yapay zekâ tabanlı yaklaşımlar ve yöntemler umut vadeden sonuçlar ortaya koymaktadır [10].

1.1.1. Problemin Tanımı

Bu tez çalışmasında ele alınan temel problem, IoT'nin iki önemli alt alanı olan Araçların İnterneti (IoV(Internet of Vehicles)) ve Tıbbi Nesnelerin İnternetinde (IoMT(Internet of Medical Things)) güvenlik önlemlerini iyileştirilmesine katkıda bulunmaktır. IoV, araçların birbirleriyle ve altyapı elemanlarıyla bağlantı kurarak akıllı ulaşım sistemlerine temel oluşturur [11]. Trafik sıkışıklığı yönetimi, güvenlik, verimlilik ve sürüş deneyimi gibi pek çok alanda yenilikçi ve verimli çözümler sunan IoV, aynı zamanda tehlikelere açık olabildiğinden dolayı siber güvenlik açısından kritik bir alandır. Örneğin, araç içi ağlara sızılarak yetkisizce fren veya direksiyon sistemlerine müdahale edilmesi, trafik kazalarına ve can kayıplarına yol açabilir [12].

IoMT ise sağlık hizmetlerinde kullanılan cihazların ve sensörlerin internet üzerinden birbirleriyle bağlanarak veri paylaşmasını ifade eder [13]. Hastaların uzaktan takibi, teşhis ve tedavi aşamalarının iyileştirilmesi gibi pek çok fayda sağlayan IoMT, diğer yandan hassas sağlık verilerinin mahremiyeti ve bütünlüğü açısından önemli riskler barındırabilir [14]. Yetkisizce yapılan erişim veya verilerin manipülasyonu, hastaların güvenliğini ve mahremiyetini tehdit edebilir.

Hem IoV hem de IoMT alanında güvenliğin sağlanması, bazı zorlukları beraberinde getirmektedir. Bunların ilki, söz konusu sistemlerin büyük ölçekli olması ve karmaşıklığıdır. Çok sayıda cihazın ve protokolün birlikte çalışması, saldırı etki alanını genişletmekte ve savunma sistemlerinin tasarımını güçleştirmektedir [15]. İkinci önemli zorluk, IoV ve IoMT cihazlarının kapasitelerinin kısıtlı olmalarıdır. Düşük işlemci gücü, bellek ve pil kapasitesi, klasik güvenlik çözümlerinin doğrudan uygulanmasını zorlaştırmaktadır [16]. Diğer bir zorluk ise IoV ve IoMT sistemlerindeki yüksek dinamiklik ve mobilitedir. Gün geçtikçe değişen ağ topolojileri ve cihazların konumları, merkezi güvenlik mekanizmalarının korumalarını yetersiz kılmaktadır [17].

Ayrıca IoV ve IoMT gibi kritik alanlarda test ve doğrulama süreçlerinin sağlanması da oldukça karmaşıktır. Gerçek sistemler üzerinde kapsamlı saldırı senaryolarını gerçekleştirme hem etik hem de yasal kısıtlamalar nedeniyle mümkün olmamaktadır [18]. Bu nedenle, bu testler için simülasyon ortamları ve veri setleri, güvenlik araştırmaları için büyük önem taşımaktadır. Fakat IoV ve

IoMT'ye özgü, gerçekçi ve heterojen veri setlerinin eksikliği, bu alandaki çalışmaları sınırlandırmaktadır [19].

Bahsedilen tüm bu zorluklar, IoV ve IoMT sistemleri için hızlı, esnek, ölçeklenebilir ve akıllı güvenlik sistemlerinin geliştirilmesini gerektirmektedir. Derin öğrenme, büyük ve karmaşık veri setlerinden otomatik özellik çıkarımı yapabilme ve üstün genelleme ve sınıflandırma performansı sayesinde, bu alanda umut vadeden bir yaklaşımdır [20]. Bununla beraber, derin öğrenme algoritmalarının doğru bir şekilde eğitilebilmesi ve test edilebilmesi için kapsamlı ve gerçekçi IoV ve IoMT veri setlerine ihtiyaç vardır.

1.1.2. Amaç ve Hedef

Bu tez çalışmasının temel amacı, derin öğrenme yöntemlerini kullanarak IoV ve IoMT sistemleri için güvenlik çözümleri geliştirmektir. Spesifik olarak, bu tez aşağıdaki araştırma hedeflerini içermektedir:

1. IoV ve IoMT sistemlerine yönelik siber tehditleri ve saldırı çeşitlerini kapsamlı bir şekilde incelemek ve sınıflandırmak. Böylelikle, güvenlik çözümlerinin hangi alanlara odaklanması gerektiği belirlenecektir.
2. IoV ve IoMT sistemleri için mevcut açık kaynaklı Kanada Siber Güvenlik Enstitüsü Araçların İnterneti 2024(CICIoV2024(Canadian Institute for Cybersecurity Internet of Vehicles 2024)) [21] ve Kanada Siber Güvenlik Enstitüsü Tıbbi Nesnelerin İnterneti 2024(CICIoMT2024(Canadian Institute for Cybersecurity Internet of Medical Things 2024)) [22] veri setlerini detaylı bir şekilde analiz etmek ve değerlendirmek. Seçilen veri setlerinin farklı cihaz türlerini, iletişim protokollerini ve saldırı senaryolarını ne ölçüde temsil ettiği incelenecektir.
3. Derin öğrenme algoritmalarını kullanarak bahsedilen veri setlerinde IoV ve IoMT sistemleri için anomali ve saldırı tespit modelleri geliştirmek. Bu modeller, öğrenme yeteneği ve ölçeklenebilirlik açısından klasik yöntemlere göre avantajlı olması beklenmektedir.
4. Geliştirilen modelleri, seçilen veri setleri üzerinde kapsamlı bir şekilde test etmek ve performanslarını değerlendirmek. Farklı derin öğrenme mimarileri ve hiper parametre seçenekleri denenerek en uygun yapılandırma parametreleri sağlanacaktır.

5. Test sonuçlarını nicel ve nitel olarak analiz ederek derin öğrenme yaklaşımının IoV ve IoMT güvenliğine katkılarını ortaya koymak. Önerilen yöntemlerin avantajları, sınırlamaları ve gelecekteki iyileştirme alanları tartışılacaktır.

Yukarıda belirtilen hedefler doğrultusunda, bu tez çalışması IoV ve IoMT sistemlerinin güvenliğini artırmak için yenilikçi ve etkili çözümler sunmayı hedeflemektedir. Geliştirilen yöntemler ve elde edilen bulgular, hem akademik literatüre katkı sağlayacak hem de gerçek dünya uygulamalarına örnek olması beklenmektedir.

1.1.3. Ana Katkılar

Bu tez çalışmasının IoV ve IoMT güvenliği alanına sağlaması beklenen ana katkılar şu şekilde özetlenebilir:

1. Kapsamlı IoV ve IoMT güvenlik tehdidi analizi: Tez çalışması kapsamında yapılmış olan detaylı literatür taraması ve sınıflandırma çalışması, IoV ve IoMT sistemlerine yönelik güncel siber tehditlerin daha iyi anlaşılmasını sağlamayı hedeflemektedir. Yapılan bu analiz çalışması, gelecekteki araştırmalara ve pratik savunma stratejilerine yön gösterebilecek değerli bir kaynak olması amaçlanmaktadır.
2. Açık kaynak veri setlerinin detaylı analizi: Tez süresince incelenen ve kullanılan açık kaynaklı CICIoV2024 ve CICIoMT2024 veri setlerinin kapsamlı analizi, gelecekteki araştırmacılara hangi veri setlerinin hangi güvenlik senaryolarına uygun olduğu konusunda rehberlik etmesi amaçlanmaktadır. Yapılan bu analiz çalışması, incelenen veri setlerinin güçlü ve zayıf yönlerini ortaya çıkararak, araştırmacıların çalışmalarında en uygun veri setini seçmelerine yardımcı olması hedeflenmektedir.
3. Derin öğrenme tabanlı anomali ve saldırı tespit modelleri: Tez çalışması kapsamında geliştirilen derin öğrenme modelleri, IoV ve IoMT sistemlerinde anomali ve saldırıların gerçek zamanlı olarak sınıflandırılmasını ve tespit edilmesini sağlayacaktır. Geliştirilen bu modellerin, yüksek doğruluk oranları oranlarıyla öne çıkması hedeflenmektedir. Ayrıca önerilen yöntemler, farklı IoV ve IoMT senaryolarına uyarlanabilir ve ölçeklenebilir olacaktır.
4. Performans değerlendirme ve analiz: Tez çalışmasında sunulan kapsamlı test sonuçları ve analizler, derin öğrenme yaklaşımının IoV ve IoMT güvenliğindeki etkinliğine dair nicel

ve nitel kanıtlar sunacaktır. Bulunan sonuçlar, yöntemlerin güçlü ve zayıf yönlerini ortaya koyarak gelecekteki araştırmalara ışık tutması beklenmektedir.

5. IoV ve IoMT güvenliği için yol haritası: Tez çalışmasının sonuçları ve önerileri, IoV ve IoMT güvenliği alanında gelecekteki araştırmaların konularını şekillendirecektir. Özellikle derin öğrenme mimarilerinin optimizasyonu ve gerçek zamanlı uygulamaların hayata yeni araştırma fırsatları sunulacaktır.

Tez çalışmasında yapılması hedeflenen bu katkılar, IoV ve IoMT sistemlerinin siber güvenlik düzeyinin yükseltilmesine ve bu alandaki akademik ve endüstriyel çabaların hızlandırılmasına yardımcı olmayı amaçlamaktadır. Tezin sunduğu yenilikçi yaklaşımlar ve kapsamlı deneysel değerlendirmeler, akıllı ulaşım ve sağlık hizmetlerinin daha güvenli ve güvenilir hale gelmesine katkıda bulunmasını hedeflemektedir.

1.1.4. Tez Organizasyonu

Bu tez çalışması, dört ana bölümden oluşmaktadır. İlk bölüm olan "Giriş"te, IoT, IoV ve IoMT kavramlarına genel bir bakış sunulmaktadır. Bu alandaki güvenlik sorunları, mevcut çözümlerin sınırlamaları ve derin öğrenme yaklaşımlarının potansiyeli vurgulanmaktadır. Ek olarak problem tanımı, tezin amaç ve hedefleri, araştırma soruları ve beklenen katkılar detaylandırılmıştır. Giriş bölümünde bununla beraber kapsamlı bir literatür taraması yapılarak, IoV ve IoMT güvenliği alanındaki güncel çalışmalar, kullanılan veri setleri ve deney çıktıları incelenmektedir.

İkinci bölüm olan "Materyal ve Yöntem"de, tez kapsamında kullanılan veri setleri (CICIoV2024 ve CICIoMT2024) detaylı olarak tanıtılmaktadır. Bu veri setlerinin özellikleri, içerdiği saldırı sınıfları ve veri toplama süreçleri açıklanmaktadır. Ardından, derin öğrenmenin temel kavramları, avantajları ve yaygın mimarileri hakkında bilgi verilmektedir. Son olarak, tez kapsamında önerilen derin öğrenme modelleri ve mimari yapıları detaylandırılmaktadır. Eğitimde kullanılan modellerin katman tasarım kararları, hiper parametre seçimleri ve eğitim süreçleri açıklanmaktadır.

Üçüncü bölüm olan "Bulgular ve Tartışma"da, önerilen modellerin kapsamlı deney sonuçları sunulmaktadır. CICIoV2024 ve CICIoMT2024 veri setleri kullanılarak, saldırı senaryoları üzerinde gerçekleştirilen testlerin performans metrikleri (doğruluk, kesinlik, duyarlılık, F1-skoru vb.) raporlanmaktadır. Ayrıca modellerin hesaplama verimliliği ve gerçek zamanlı çıkarım süreleri de incelenmektedir. Deneylerden edilen sonuçlar, literatürdeki aynı veri setlerini kullanan diğer

çalışmalarla karşılaştırılarak analiz edilmekte ve tartışılmaktadır. Önerilen yöntemlerin güçlü ve zayıf yönleri, sınırlamaları ve gelecekteki iyileştirme alanları değerlendirilmektedir.

Dördüncü ve son bölüm olan "Sonuç"ta, tez çalışmasının genel bir özeti sunulmaktadır. Tez çalışmasından elde edilen ana bulgular ve katkılar vurgulanarak, IoV ve IoMT sistemlerinin siber güvenliğinin artırılmasına yönelik çıkarımlar yapılmaktadır. Ayrıca gelecekteki araştırma yönleri ve potansiyel uygulamalar tartışılmaktadır. Tez çalışmasının açtığı yeni araştırma soruları ve fırsatları özetlenerek okuyuculara ve araştırma topluluk için yol gösterici öneriler sunulmaktadır.

Bu organizasyon yapısıyla tez çalışması, IoV ve IoMT güvenliği alanındaki mevcut zorlukları, derin öğrenme temelli çözüm önerilerini ve kapsamlı deneysel değerlendirmeleri bütüncül bir şekilde ele almaktadır. Giriş bölümündeki literatür taraması ile konunun önemi ve güncel durumu ortaya konulmakta olup, takip eden bölümlerde ise özgün katkılar ve deney sonuçları sistemli bir şekilde sunulmaktadır. Sonuç bölümüyle de tez çalışmasının ana mesajları ve etkisi vurgulanarak gelecek çalışmalara zemin hazırlanmaktadır.

1.2. IoT Tanımı ve Temel Kavramlar

IoT, fiziksel nesnelerin çeşitli sensörler, aktüatörler, yazılım sistemleri ve ağ bağlantıları üzerinden birbirleriyle ve internet üzerinden diğer cihazlarla veri alışverişinde bulunarak, akıllı bir ekosistem oluşturduğu bir teknolojidir [1]. IoT, nesneleri birbirine bağlayarak, onların uzaktan izlenmesini, kontrol edilmesini ve otomatize şekilde çalışmasını sağlar. Bu sayede, ev aletleri, arabalar, fabrikalar, şehirler gibi pek çok alanda verimlilik, güvenlik, konfor ve sürdürülebilirlik alanlarına katkısı mümkün olmaktadır. Şekil 1.1'deki gibi IoT ekosistemi, çok sayıda cihazın birbiriyle bağlantılı olduğu karmaşık bir ağ yapısına sahiptir.



Şekil 1.1. IoT Ekosistemindeki Birbiriyle Bağlı Cihazlar [1]

IoT sistemleri, en temel haliyle sensörler, iletişim protokolleri, veri işleme ve analiz araçları ile uygulama katmanlarından oluşur. Sensörler, fiziksel ortamdan verileri toplar ve dijital sinyallere dönüştürür. İletişim protokolleri, cihazlar arasında veri alışverişini sağlar. Veri işleme ve analiz araçları, toplanan verileri anlamlı bilgilere dönüştürür ve karar verme süreçlerini destekler. Uygulama katmanı ise, son kullanıcılara IoT hizmetlerini sunar.[1]

IoT sistemlerinin etkin bir şekilde birlikte çalışabilmesi için, cihazların birlikte çalışabilirliği, güvenlik, mahremiyet, ölçeklenebilirlik ve enerji verimliliği gibi konularda çözümler geliştirilmesi beklenmektedir. IoT sistemlerinin standartların oluşturulması, verilerinin güvenliğinin sağlanması, iletişim ağ altyapılarının iyileştirilmesi ve kullanıcı deneyiminin yükseltilmesi, IoT sistemlerinin geleceği açısından son derece önemlidir. IoT sistemlerinin sunduğu bu imkanlar, pek çok sektörde dijital dönüşümü hızlandırmaktadır ve yeni iş modellerinin oluşmasında önemli rol oynamaktadır.

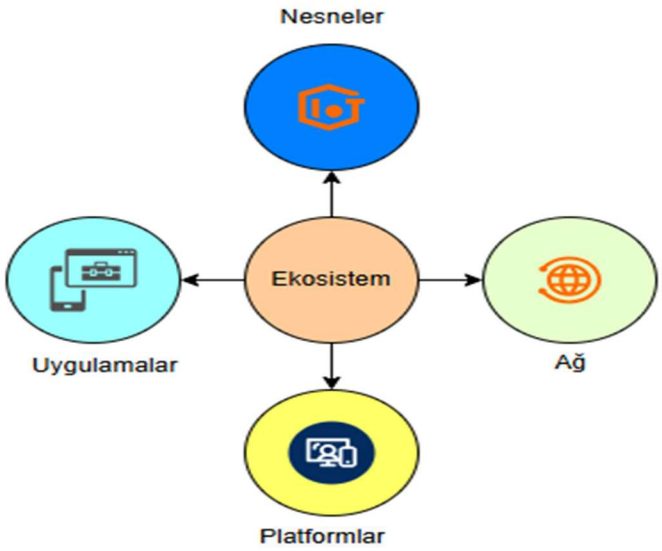
1.2.1 IoT Mimarisi ve Protokolleri

IoT sistemlerinin temel amacı, nesnelerin internet kullanarak birbirleriyle ve insanlarla etkileşime girerek, topladıkları bilgileri anlamlı bilgilere ve hizmetlere dönüştürmesidir. Örneğin, akıllı bir termostat, kullanıcının tercihlerini ve günlük davranışlarını öğrenerek, enerji tasarrufu sağlarken konforlu bir oda sıcaklığı sunabilir [2]. Yine benzer şekilde, akıllı bir sulama sistemi, internet üzerinden aldığı hava durumu tahminlerini ve toprak nem sensörlerinden aldığı verileri kullanarak, bitkilerin ihtiyacı kadar su verilmesini sağlayarak su israfının önlenmesine katkıda bulunabilir.[23].

IoT ekosistemleri, genellikle dört temel bileşenden oluşur [24]:

1. Nesneler: Fiziksel cihazlar, sensörler ve aktüatörler gibi verileri alan, işleyen ve aksiyon alan bileşenlerdir.
2. Ağ: Nesneler arasındaki veri alışverişinin gerçekleşmesini sağlayan kablolu veya kablosuz iletişim altyapısıdır. Kablosuz bağlantı(Wi-Fi(Wireless Fidelity)), Bluetooth, ZigBee, hücresel ağlar (4G/5G) gibi protokoller yaygın olarak kullanılır.
3. Platformlar: IoT verilerini toplayan, saklayan, işleyen ve analiz eden bulut tabanlı veya dağıtık bilişim sistemleridir. Bu platformlar, cihaz yönetimi, verilerin işlenmesi, makine öğrenimi ve güvenlik gibi hizmetleri sağlar.

4. Uygulamalar: IoT cihazlarındaki verileri kullanarak, kullanıcılara fayda sağlayan yazılım çözümleridir. Bu yazılımlar, mobil uygulamalar, web ara yüzleri, kontrol panelleri gibi çeşitli şekillerde olabilir.



Şekil 1.2. IoT Ekosistemindeki Dört Temel Bileşen [24]

IoT cihazları, çeşitli protokoller aracılığıyla iletişim sağlar. Kısıtlı donanım kaynaklarına (işlemci, bellek, pil vb.) sahip olduklarından, özel tasarlanmış hafif iletişim protokolleri kullanırlar. Bu protokoller, uygulama katmanından fiziksel katmana kadar farklı seviyelerde çalışır. Örneğin:

- Mesaj Kuyruklama Telemetri Taşıma(MQTT(Message Queuing Telemetry Transport)): Yayınla/abone ol modelini kullanan hafif bir uygulama katmanı protokolüdür. IoT cihazları arasındaki verimli ve güvenli mesajlaşma için tasarlanmıştır [25].
- Kısıtlı Uygulama Protokolü(CoAP(Constrained Application Protocol)): Kısıtlı donanımsal kaynaklara sahip IoT cihazları için geliştirilmiş, Hiper Metin Transfer Protokolü(HTTP(Hypertext Transfer Protocol)) benzeri bir protokoldür. Kullanıcı Datagram Protokolü(UDP(User Datagram Protocol)) üzerinden çalışır ve Temsili Durum Aktarımı (REST(Representational State Transfer)) mimarisini destekler [26].
- Düşük Güçlü Kablosuz Kişisel Alan Ağları üzerinden IPv6(6LoWPAN(IPv6 over Low-Power Wireless Personal Area Networks)): Düşük güç gerektiren kablosuz kişisel alan ağlarında, İnternet Protokolü Versiyon 6(Ipv6(Internet Protocol version 6)) paketlerinin verimli bir şekilde aktarılmasını sağlayan bir ağ katmanı protokolüdür [27].

IoT protokollerinin seçimi, cihazların kısıtları, ağ topolojisi, güvenlik gereksinimleri ve uygulama ihtiyaçları gibi faktörlere bağlıdır. Tablo 1.1, yaygın IoT protokollerinin bir karşılaştırmasını sunmaktadır.

Tablo 1.1. Yaygın IoT protokollerinin karşılaştırması [28].

Protokol	**Katman**	**Taşıma**	**Mesaj Tipi**	**Güvenlik**	**Avantajlar**
MQTT	Uygulama	İletim Kontrol Protokolü (TCP (Transmission Control Protocol))	Yayınla/Abone Ol	Taşıma Katmanı Güvenliği(TLS (Transport Layer Security))	Hafif, ölçeklenebilir
AMQP (Gelişmiş Mesaj Kuyruklama Protokolü)	Uygulama	TCP	Kuyruk	TLS	Güvenilir, genişletilebilir
HTTP	Uygulama	TCP	İstek/Yanıt	TLS	Yaygın, web uyumlu
CoAP	Uygulama	UDP	İstek/Yanıt	Datagram Taşıma Katmanı Güvenliği (DTLS(Datagram Transport Layer Security))	Hafif, hızlı
6LoWPAN	Ağ	-	-	-	Düşük güç, Ipv6 desteği

Ayrıca, IoT cihazları Evrensel Benzersiz Tanımlayıcılar (UUID(Universally Unique Identifier)) aracılığıyla tanımlanır ve yönetilir. Bu kimlikler, cihazların ağa güvenli bir şekilde katılmasını ve veri paylaşmasını sağlar [29]. Blockchain gibi dağıtık defter teknolojileri de IoT cihazlarının kimlik doğrulaması ve yetkilendirilmesi için umut verici çözümler sunmaktadır [30].

IoT cihazlarının etkin bir şekilde çalışabilmesi için aşağıdaki temel gereksinimlerin sağlanması gerekmektedir [9]:

- Birlikte Çalışabilirlik: Farklı üreticilerin IoT cihazlarının ve platformlarının arasında sorunsuz bir şekilde veri alışverişi yapabilmesi için ortak standartlara ve protokollere ihtiyaç duyulmaktadır.
- Ölçeklenebilirlik: IoT çözümleri, milyarlarca cihazın ve petabaytlarca verinin yönetimi için ölçeklenebilir olması sağlanmalıdır.
- Gerçek Zamanlılık: Kritik IoT uygulamaları (ör. sağlık, güvenlik), verilerin gecikmesiz bir şekilde işlenmesini ve anında cevap verilmesini gerektirir.
- Güvenlik ve Gizlilik: IoT cihazlarının ve verilerinin yetkisiz erişim, sızıntı ve saldırılardan korunması, güvenli ve gizli veri iletişiminin sağlanması için uçtan uca şifreleme sağlanması şarttır.
- Dayanıklılık: IoT cihazları, zorlu çevre koşullarına (ör. sıcaklık, nem, titreşim) uyum sağlamalı ve güvenilir ve kesintisiz çalışabilmelidir.

IoT cihazları, bu temel gereksinimleri karşılayan teknolojiler ve mimarilerle hayata geçirilmektedir. Örneğin, bulut bilişim ve sis bilişim, IoT cihazlarındaki verilerin ölçeklenebilir ve anlık işlenmesine olanak tanır [31]. Blok zinciri ve makine öğrenmesi gibi teknolojiler ise IoT cihazlarının güvenliğini ve otomasyonunu artırmaktadır [32].

1.2.2. IoT Uygulama Alanları

IoT cihazları, endüstri, sağlık, ulaşım, enerji, tarım ve akıllı şehirler gibi birçok sektörde devrim niteliğinde dönüşümlere yol açmaktadır. IoT'nin sağladığı gerçek zamanlı veri toplama, uzaktan izleme ve kontrol yetenekleri, bu sektörlerde verimliliği, güvenliği ve konforu artırmaktadır.

Aşağıda, IoT'nin başlıca uygulama alanları ve örnekleri sunulmaktadır:

1. Akıllı Evler ve Binalar: IoT sistemlerinin ev ve binalarda kullanılmaya başlamasıyla, yapay zeka desteğiyle dağıtık mimariler üzerinden kontrol edilmesi, enerji yönetimi ve otomasyon sistemlerinin akıllı entegrasyonu sağlanmaktadır [33].
2. Endüstriyel Nesnelerin İnterneti (IıoT(Industrial Internet of Things)): Endüstri 4.0 standardını benimseyen işletmelerde, büyük veri kullanılarak makinelerin performansı izlenmekte ve öngörücü bakım uygulamaları yapılmaktadır [34].

3. Akıllı Sağlık: Sağlık kurumlarında kullanılan sağlık teknolojilerinin IoT ile entegrasyonu, hasta takibi ve sağlık hizmetlerinin iyileştirilmesi için yenilikçi çözümler sağlamaktadır [35].
4. Akıllı Ulaşım: Bulut sistemleri üzreinde çalışabilen akıllı otopark sistemleri ile araç sürücüleri anlık park yeri bilgisi gönderilmekte ve park alanlarını yönetimi verimli hale gelmektedir [36].
5. Akıllı Şehirler: Şehirlerin altyapılarının servis odaklı mimariler üzerinden yönetilmesi tüm şehir hizmetlerinin bu servislere entegre olması sağlanmaktadır [37].
6. Akıllı Tarım: Tarımsal üretimde IoT teknolojilerinin kullanımının artmasıyla beraber akıllı çiftlik uygulamaları geliştirilmekte ve tarımsal verimlilik artırılmaktadır [38].

IoT sistemlerinin kullanılmasının sağladığı avantajlar arasında maliyet tasarrufu, verimlilik artışı, hata azaltımı, müşteri memnuniyeti ve sürdürülebilirlik yer almaktadır. Örnek olarak endüstriyel IoT uygulamalarının 2030 yılına kadar küresel ekonomiye 14 trilyon dolar katkı sağlaması beklenmektedir [39]. Akıllı şehir IoT uygulamalarının ise 2025 yılına kadar şehirlerin işletme maliyetlerini %30 azaltabileceği öngörülmektedir [40].

Bunun yanında, IoT uygulamalarının yaygınlaşması, bu teknolojinin riskleri ve zorlukları da ön plana çıkarmaktadır. Siber güvenlik, veri gizliliği, etik ve yasal sorunlar, birlikte çalışabilirlik ve standardizasyon eksikliği bunlardan bazılarıdır. IoT sistemlerinin sürdürülebilir ve güvenli bir şekilde kullanılabilmesi için bu zorlukların kapsamlı ve iş birliği yapan bir yaklaşımla ele alınması gerekmektedir.

1.2.3. IoT Güvenlik Sorunları ve Açık Problemler

IoT cihazları, hayatımızın birçok alanında kolaylık, verimlilik ve inovatif hizmetler sunarken, beraberinde önemli güvenlik ve gizlilik riskleri de getirmektedir. IoT cihazlarının sayısı ve çeşitliliği arttıkça, bu cihazların siber saldırılara karşı savunmasızlığı da artmaktadır. Geleneksel bilgi teknoloji sistemlerinden farklı olarak, IoT cihazları genellikle sınırlı donanım kaynaklarına, özgün protokollere ve zayıf güvenlik önlemlerine sahiptir [41]. Bu durum, saldırganların IoT cihazlarını ele geçirerek, verileri çalmasına, hizmetleri aksatmasına ve hatta fiziksel zararlara yol açabilir.

IoT güvenliğinin başlıca zorlukları şunlardır [42], [43]:

1. Cihaz Güvenliği:
    - Zayıf kimlik doğrulama ve yetkilendirme sistemleri
    - Eski ve güncellenmeyen yazılım/donanım bileşenleri
    - Kötü amaçlı yazılımlara karşı yeterli korunma önlemi alınmaması
2. Ağ Güvenliği:
    - Şifrelenmemiş veya zayıf şifreleme protokollerin varlığı
    - Saldırılara açık kablosuz iletişim kanallarının bulunması
    - Dağıtık hizmet reddi (DDoS(Dağıtık Hizmet Engelleme)) saldırılarına karşı savunmasızlık
3. Veri Güvenliği ve Mahremiyeti:
    - Hassas verilerin yetkisiz erişimi, sızıntısı veya değiştirilmesi
    - Veri toplama, işleme ve paylaşmada şeffaflık olmaması
    - Kullanıcıların veri gizliliği haklarını yönetmede zorluklar bulunması
4. Uçtan Uca Güvenlik:
    - Farklı IoT bileşenleri arasında tutarlı ve bütünleşik güvenlik önlemlerinin sağlanması
    - Güvenli veri iletimi için uçtan uca şifreleme ve kimlik doğrulama mekanizmaları
    - Güvenlik açıklarının yaşam döngüsü boyunca yönetilmesi
5. İnsan Faktörü:
    - Kullanıcıların güvenlik farkındalığı ve eğitimi eksikliği olması
    - Güçlü kimlik bilgilerinin oluşturulması ve güvenli yönetilememesindeki hatalar
    - Kullanıcıların sosyal mühendislik saldırılarına karşı savunmasız olmaları

IoT cihazlarına yönelik gerçek dünya saldırı örnekleri arasında en çok ses getireni Mirai botnet saldırısıdır. Mirai botnet, zayıf kimlik bilgileri olan IoT cihazlarını ele geçirerek, 2016 yılında Twitter, Netflix ve CNN gibi popüler web sitelerine karşı büyük bir DDoS saldırısı gerçekleştirmiştir [44]. Yine buna benzer şekilde, 2017 yılında WannaCry ve NotPetya fidye yazılımları, dünya genelindeki birçok organizasyonun bilgi teknolojileri ve IoT sistemlerini etkilemiş ve milyarlarca dolarlık zarara yol açmışlardır [45].

IoT cihazlarının güvenliğinin sağlanması ve bu tür saldırıların önlenmesi için kapsamlı ve çok katmanlı bir yaklaşım sağlanması gerekmektedir. Bu yaklaşım cihaz, ağ, uygulama ve insan faktörlerini bir arada kapsayan uçtan uca güvenlik önlemlerini barındırmalıdır [46].

Örneğin:

- Cihaz düzeyinde: Güvenli önyükleme, donanımla uyumlu çalışan, güvenli aygıt yazılımı güncellemeleri ve eşsiz kimlik verileri
- Ağ düzeyinde: Güvenli iletişim protokolleri (ör. TLS, DTLS), ağ segmentasyonu, güvenlik duvarları ve saldırı tespit/önleme sistemleri
- Uygulama düzeyinde: Güvenli kod geliştirme, düzenli güvenlik testleri, kimlik doğrulama ve yetkilendirme mekanizmaları
- İnsan faktörü düzeyinde: Güvenlik farkındalığı eğitimleri, güçlü parola politika sistemleri, çok faktörlü kimlik doğrulama aşamaları

Ayrıca, IoT güvenliğinin sağlanmasında, açık standartlar, düzenlemeler ve sertifikasyon programları önemli bir rol oynamaktadır. Buna örnek olarak "Ulusal Standartlar ve Teknoloji Enstitüsü(NIST(National Institute of Standards and Technology))" IoT Cybersecurity Improvement Act of 2020", ABD federal kurumlarının satın aldığı IoT cihazlarının belirli güvenlik gereksinimlerini karşılamasını zorunlu kılmıştır [47]. Benzer şekilde, Avrupa Telekomünikasyon Standartları Enstitüsü(ETSI(European Telecommunications Standards Institute)) EN 303 645, tüketici IoT cihazları için temel siber güvenlik standartlarını belirlemektedir [48].

Sonuç olarak, IoT cihazlarının güvenliği, IoT ekosisteminin geleceği ve topluma sağlayacağı yararlar açısından oldukça önemli bir konudur. IoT ekosisteminin tüm katılımcı (cihaz üreticileri, servis sağlayıcıları, kullanıcılar ve düzenleyiciler), güvenlik ve gizliliği mimarinin merkezine

alarak, birlikte hareket etmelidir. Ancak bu şekilde, IoT sistemlerinin potansiyelinden tam olarak faydalanılabilir ve sürdürülebilir bir dijital gelecek inşa edilebilir.

1.3. IoV Tanımı ve Temel Kavramlar

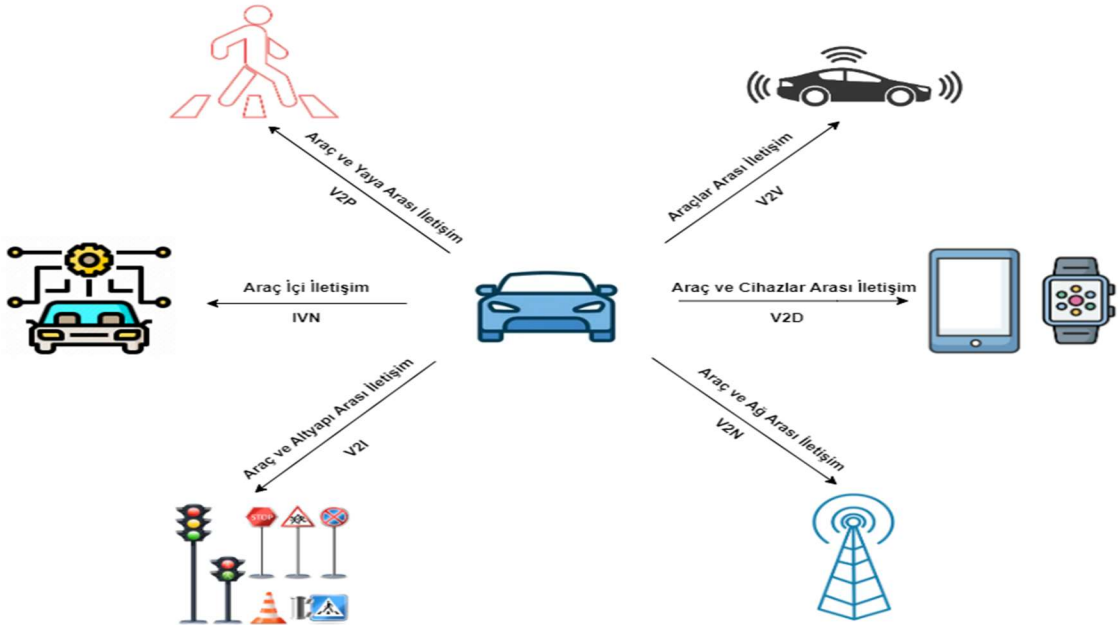
IoV sistemi, IoT paradigmasının ulaşım ve otomotiv sektörüne uyarlanmış özel bir uzantısıdır. IoV, araçları, yol altyapısını, kullanıcıları ve bulut platformlarını kapsayan geniş bir ekosistemi ifade eder [49]. Bu ekosistemde, araçlar hem kendileri arasında araçtan araca (V2V(Vehicle to Vehicle)) hem de araçtan alt yapıya (V2I(Vehicle to Infrastructure)), araçtan yayaya (V2P(Vehicle to Pedestrian)), araçtan ağa (V2N(Vehicle to Network)) ve araçtan servislere (V2S(Vehicle to Service)) ile bağlantı kurup veri alışverişinde bulunmaktadır. Bu bağlanabilirlik, trafik yönetimi, yol güvenliği, sürüş deneyimi ve ekolojik sürdürülebilirlik gibi alanlarda çığır açan ilerlemelere önderlik etmektedir.

IoV sistemlerinin temel amacı, araçların ve yol kullanıcılarının gerçek zamanlı veri paylaşımı ve koordineli çalışması sayesinde ulaşımın daha güvenli, verimli, konforlu ve çevre dostu hale getirilmesidir. Örneğin, trafik sıkışıklığı, yol yapım çalışmaları, kazalar ve hava durumu hakkında gerçek zamanlı veri paylaşımı sayesinde sürücüler farklı güzergah planlayabilir, olası kazalardan kaçabilir ve yolculuk sürelerini kısaltabilirler [50]. Kendi kendine gidebilen otonom araçlar, yapay zeka destekli navigasyon ve kaza önleme sistemleriyle, sürücü hatalarından kaynaklanan kazaları azaltabilir, trafik durumunu iyileştirebilir ve park yeri aramak gibi zaman alıcı ve can sıkıcı durumları ortadan kaldırabilir [51].

IoV sistemlerinin sağladığı bir diğer önemli avantajda ekolojik sürdürülebilirliği sağlamasıdır. Trafik verilerinin anlık analizi sayesinde, çevreye zararlı fosil yakıt tüketimini ve karbon emisyonlarını azaltmak için akıllı sinyalizasyon, değişebilir hız sınırları ve çevre dostu navigasyon gibi yöntemler uygulanabilir [52]. Elektrikli ve hibrit araçların IoV ekosistemine entegrasyonu, şarj istasyonlarının verimli sayıda ve ortak alanlara konumlandırılması ve kullanıcıların şarj/enerji durumuna göre yönlendirilmesi gibi hizmetlerle desteklenebilir [53].

IoV sistemleri, araçların kendi aralarında ve çevrelerindeki diğer bileşenler çeşitli ağlar üzerinden gerçek zamanlı veri iletimi yaparak akıllı bir ulaşım ekosistemine dönüşmesini ifade eder. IoV'un temel bileşenleri şunlardır ve Şekil 1.3'te gösterilmiştir [54]:

1. Akıllı Araçlar: Sensörler, işlemciler, haberleşme modülleri ve yazılımlarla donatılmış, internet üzerinden sürekli veri alışverişi yapabilen araçlardır. Akıllı araçlar, otonom sürüş, çarpışma önleme, acil durum uyarıları gibi gelişmiş sürüş destek özelliklerine sahiptir.
2. Yol Kenarı Birimleri(RSU(Road Side Unit)): Trafik ışıkları, işaret levhaları, kameralar, sensörler ve iletişim sağlayıcıları gibi, yol boyunca yerleştirilmiş altyapı bileşenleridir. Yol kenarı birimleri, araçlara trafik, hava durumu, yol ve park durumları hakkında eş zamanlı bilgiler sağlar.
3. Araçsal Özel Ağlar (VANET(Vehicular Ad Hoc Network)): V2V ve V2I arasında kurulan kablosuz ad hoc ağları ifade eder. Araç üstü ağlar özellikle güvenlik kritik mesajların (örn. çarpışma erken uyarısı) anlık ve güvenilir bir şekilde iletilmesini sağlar.
4. İnternet ve Bulut İletişim Platformları: Araçlar ve yol kenarı birimlerinden gelen verilerin işlendiği, depolandığı ve analiz edildiği merkezi veya dağıtık bilgi işlem platformlarıdır. Bu iletişim platformları, trafik durumu yönetimi, filo yönetimi, akıllı park sistemi, acil durum hizmetleri gibi çeşitli IoV uygulamalarını destekler.
5. Kullanıcılar: Sürücüler, yolcular, yayalar, bisikletliler gibi ulaşım ekosisteminin tüm katılımcılarıdır. IoV sistemi kullanıcıları, akıllı telefonlar, giyilebilir cihazlar ve araç içi eğlence sistemleri gibi arayüzlerle ekosistemin sunduğu hizmetlerden de faydalanır.



Şekil 1.3. Araçların İnterneti Mimarisi [54]

IoV sistemlerinin sağladığı temel faydalar arasında şunlar ön plana çıkmaktadır [55]:

- Gelişmiş trafik durumu yönetimi ve seyahat sürelerinin azalması
- Daha güvenli yollar ve azalan kaza oranları
- Düşen yakıt tüketimi ve düşük emisyonlar
- Sürüş konforunun ve yolcu deneyiminin arttırılması
- Acil durum müdahale sürelerinin kısalması

Ancak IoV sistemlerinin geniş çapta kabullenilmesi ve olgunlaşması için aşılması gereken çeşitli teknik, yasal ve sosyal engellerde bulunmaktadır. Bunlar arasında birlikte çalışabilirlik, ölçeklenebilirlik, güvenlik, mahremiyet, yasal düzenlemeler ve kullanıcı kabulü gibi konular yer almaktadır [56].

1.3.1. IoV Mimarisi ve Protokolleri

IoV sistemleri, farklı teknolojilerin ve protokollerin bir araya geldiği çok katmanlı ve heterojen bir mimari üzerine kurulmuştur. Bu mimari, genellikle algılama, veri iletişimi, veri işleme ve uygulama katmanlarından oluşmaktadır [57]:

1. Algılama Katmanı: Araçlara, yollara ve çevreye yerleştirilmiş çeşitli sensörlerden oluşur. Örneğin, aracın içindeki sensörler (hız, konum, yakıt seviyesi vb.), yol ve trafik sensörleri (yoğunluk, sıcaklık, görüş mesafesi vb.) ve çevresel sensörler (hava kalitesi, meteoroloji vb.) bu katmanda yer alır.
2. Ağ İletişim Katmanı: Araçlar, yol kenarı birimleri, kullanıcıların cihazları ve bulut platformları arasındaki bağlantıyı gerçekleştiren çeşitli kablosuz iletişim teknolojilerini içerir. Bunlar arasında hücresel ağlar (4G/5G), Adanmış Kısa Menzilli Haberleşme (DSRC(Dedicated Short-Range Communications)), Wi-Fi, Bluetooth ve uydu iletişimi sayılabilir.
3. Veri İşleme Katmanı: IoV cihazlardan toplanan işlenmemiş verilerin işlendiği, analiz edildiği ve anlamlı bilgilere dönüştürüldüğü katmandır. Bu katmanda, bulut bilişim, sis bilişim ve büyük veri analitiği gibi teknolojileri kullanarak verileri işlenir ve depolanır.
4. Uygulama Katmanı: İşlenmiş verileri kullanarak sürücülere, yolculara, filo işleticilerine ve diğer katılımcılara değer katan akıllı ulaşım hizmetlerini sunan katmandır. Uygulamalar

arasında gerçek zamanlı navigasyon, trafik acil durum uyarıları, otonom sürüş, akıllı park etme sistemi, yolcu bilgilendirme sistemleri, filo yönetimi yer almaktadır.

IoV ağlarında veri iletişimi, çeşitli protokoller aracılığıyla gerçekleştirilir. Kullanılan başlıca protokoller şunlardır [58]:

- DSRC: V2V ve araçlarla yol kenarı birimleri arasında (V2I) kısa menzilli, yüksek hızlı ve düşük gecikmeli iletişim sağlayan bir kablosuz protokoldür. DSRC, özellikle güvenlikle ilgili kritik mesajların iletilmesinde kullanılmaktadır.
- Hücresel Araçtan Her şeye Ağ (C-V2X): Hücresel ağ altyapısını (4G/5G) kullanarak araçların hem kendi aralarında hem de diğer katılımcılarla (yol kenarı birimleri, yayalar, ağ altyapısı) iletişim kurmasını sağlayan bir protokol ailesidir.
- WAVE (Wireless Access in Vehicular Environments): DSRC ile birlikte kullanılan ve IEEE 802.11p standardına dayanan bir protokol kümesidir. WAVE, araç ağlarında çok kanallı işlem, yüksek hızlı arayüz değişimi ve yayın tabanlı iletişim gibi özellikleri desteklemektedir.
- MQTT: Yayınla/abone ol esasına dayalı, hafif bir mesajlaşma protokolüdür. IoV sistem bağlamında, araçların sensör verilerini bulut platformlarına göndermesi ve buluttan komut ve bildirim alması için kullanılmaktadır.

Tablo 1.2, IoV protokollerinin temel özelliklerini ve uygulama alanlarını özetlemektedir.

Tablo 1.2. Yaygın IoV protokollerinin temel özelliklerini ve uygulama alanları [59].

Protokol	**Frekans Bandı**	**Veri Hızı**	**Menzil**	**Gecikme**	**Uygulama alanları**
DSRC	5.9 GHz	3-27 Mbps	300-1000 m	<10 ms	Güvenlik mesajları, V2V, V2I
C-V2X	Hücresel	100 Mbps(4G)	Hücresel Kapsama Alanı	<100 ms (4G)	V2X(araçlar,altyapı,yayalar, ağlar),eğlence verimlilik
WAVE	5.9 GHz	3-27 Mbps	300-1000 m	<10 ms	V2V, V2I, güvenlik, internet erişimi
MQTT	Uyg.katmanı	-	Kapsama alanı	Ayarlanabilir	V2I, V2N, V2C, izleme ve kontrol

IoV sistemlerinin hızla gelişen ve yayılan ekosistemi, otonom araçlar, 5G ve ötesi iletişim ağları, yapay zeka ve derin öğrenme gibi trend olan teknolojilerin etkisiyle sürekli değişim göstermektedir. Gelecekte, akıllı ve birbirleriyle bağlantılı araçların, ulaşım altyapısına tam entegre olduğu, sıfır kaza, sıfır emisyon ve sıfır trafik sıkışıklığı hedeflerine ulaşıldığı bir IoV perspektifi kestirilmektedir [60].

1.3.2. IoV Uygulama Alanları

IoV sistemleri, ulaşım ve lojistik sektörlerinde geniş bir uygulama alanına sahiptir ve önemli faydalar sağlamaktadır. Aşağıda, IoV'un başlıca uygulama alanları ve ilgili örnekler verilmektedir.

1. Akıllı Trafik Yönetimi: IoV sistemlerinin teknolojileri, trafik sıkışıklığını azaltmak, seyahat güvenliğini artırmak ve seyahat sürelerini optimize etmek için kullanılır. Örneğin, gerçek zamanlı trafik verileri toplanarak, trafik ışıklarının yanma süreleri dinamik olarak ayarlanabilir ve sürücüler alternatif farklı güzergahlar hakkında bilgi sahibi olabilir. [50].
2. Otonom Araçlar: IoV, kendi kendini süren otonom araçların geliştirilmesinde kilit bir rol oynamaktadır. Araçlar, sensörler, kameralar ve iletişim teknolojileri aracılığıyla çevrelerini algılayabilir, birbirleriyle ve altyapıyla iletişim kurabilir, böylece daha güvenli ve verimli bir sürüş deneyimi sağlayabilir [61].
3. Araç Veri Analizi: IoV sistemleri, araçlardan toplanan verileri analiz ederek sürüş davranışlarını, yakıt tüketimini ve araç performansını izleyebilir. Bu veriler, araç bakımını optimize etmek, sürüş güvenliğini artırmak ve yakıt verimliliğini iyileştirmek için kullanılabilir [62].
4. Akıllı Park Sistemleri: IoV sistemleri, sürücülere gerçek zamanlı park alanı bilgileri sağlayarak park yeri arama süresini kısaltır ve park alanlarının optimize şekilde kullanılmasını sağlar. Otonom park sistemleri, sürücülerin park etme stresini ortadan kaldırır ve park alanından maksimum yararlanmayı sağlar [63].
5. Yaya ve Bisikletli Güvenliği: IoV sistemleri, yayalar ve bisikletliler için gelişmiş güvenlik özellikleri sunar. Araçlarda bulunan sensörler, yayaları ve bisikletlileri algılayabilir, sürücülere olabilecek tehlikeler karşısında bilgi verebilir ve gerektiğinde otomatik frenleme yapabilir. Bu akıllı sistem ile sürüş ve yol güvenliğini önemli ölçüde artar. [64].

Sonuç olarak, IoV sistemleri ulaşım ve lojistik sektörlerini dönüştürme potansiyeline sahiptir. Ancak, IoV'un geniş çapta benimsenmesi için mevcut zorlukların üstesinden gelinmesi gerekmektedir. Bunlar arasında, standartlaştırma, altyapı uyumluluğu, veri güvenliği ve düzenleyici çerçeveler yer almaktadır.

1.3.3. IoV Güvenlik Sorunları ve Açık Problemler

IoT teknolojilerinin ulaşım sektöründe kullanılması, beraberinde önemli güvenlik ve gizlilik sorunlarını da getirmiştir. IoV ekosisteminin çeşitliliği, dağıtık sistem yapısı ve kritik görevleri, onu geleneksel bilgi teknoloji sistemlerine göre siber saldırılara karşı daha kırılgan kılmaktadır[65].

IoV'a yönelik başlıca güvenlik tehditleri şunları içerir:

1. Sistemlere Yetkisiz Erişim ve Müdahale: Art niyetli kişilerin araçların kontrol sistemlerine sızarak frenleri devre dışı bırakması, direksiyonun kontrolünün ele geçirmesi veya hız sınırını aşması gibi somut tehditler oluşturabilir [12].
2. Veri Mahremiyeti İhlalleri: Aracın konum, rota, sürüş davranışı gibi hassas verilerinin izinsiz toplanması, paylaşılması veya açığa çıkarılması sürücülerin ve yolcuların gizliliğini tehdit edebilir [66].
3. Sahte/Aldatıcı Bildirimler: Trafik sıkışıklığı, hava durumu veya acil durum uyarılarının bilinçli olarak değiştirilmesi veya gerçek dışı bilgilerin dahil edilmesi, kazalara veya trafiğin akışının tamamen durmasına sebep olabilir [67].
4. Hizmet Engelleme(DoS(Denial of Service)): Önemli iletişim kanallarının veya bulut sağlayıcılarının aşırı trafik veya sahte isteklerle bilinçli olarak tıkanması, IoV sistemlerinin hizmetlerinin aksamasına veya durmasına yol açabilir [68].
5. Yazılımsal/Donanım Açıkları: Araçların işletim sistemlerindeki, haberleşme protokollerindeki veya sensör/aktüatör aygıtlarındaki tasarım yanlışlıkları ve açıklar, saldırganlar tarafından kötüye kullanılabilir [69].
6. Güvensiz Şifreleme: Kolayca kırılabilir şifreleme algoritmalarının kullanılması, kriptografik anahtarların güvenli şekilde korunmaması veya rastgele sayı üretiminde oluşan hatalar, IoV sistemlerinin şifrelerinin çözülmesine veya kırılmasına neden olabilir[70].

Bahsedilen tehlikelerin gerçekleşmesi durumunda, maddi kayıpların, yaralanmaların ve hatta ölümlerin yaşanması söz konusu olabilmektedir. Örneğin, 2015 yılında, güvenlik araştırmacıları uzaktan bir Jeep marka bir arazi aracının kontrolünü ele geçirmiş ve aracı yoldan çıkarabilmeyi başarmıştır [71].

IoV sistemlerinin güvenliğinin sağlanması için aşağıdaki hususlara dikkat edilmesi önerilmektedir [72]:

- Güvenli araç içi ağların tasarımı Kontrol Alan Ağı(CAN(Controller Area Network)), Medya Odaklı Sistemler Taşıması(MOST(Media Oriented Systems Transport)), FlexRay vb.)
- Güvenli V2X iletişim protokollerinin oluşturulması (DSRC, C-V2X, WAVE vb.)
- Yazılım ve donanım bileşenlerinin düzenli olarak güncellenmesi ve hatalarının giderilmesi
- Güçlü ve güvenilir kimlik doğrulama, yetkilendirme ve erişim kontrolü mekanizmaları
- Kriptografik protokollerin ve anahtar yönetimlerinin standartlara uygun gerçekleştirilmesi
- Saldırıların tespiti, önlenmesi ve olaya müdahale sistemlerinin geliştirilmesi
- Gizlilik koruyucu veri toplama, işlenme ve paylaşılma politikalarının benimsenmesi
- Düzenleyici devlet kurumları ve standart kuruluşlarıyla işbirliği ve uyum sağlanması

Ayrıca, blok zinciri, yapay zeka ve makine öğrenmesi gibi yeni nesil teknolojilerin IoV sistemlerinin güvenliğinde kullanılması da umut edici sonuçlar ortaya koymaktadır. Örneğin, blok zinciri aracılığıyla dağıtık ve değiştirilemez bir veri defteri oluşturularak verilerin bütünlüğü sağlanabilir ve güvenilirliği artırılabilir [73]. Yapay zeka ve makine öğrenmesi algoritmaları ise ağ trafiğindeki anomalileri gerçek zamanlı olarak tespit ederek sıfırıncı gün saldırılarına karşı öngörülü bir koruma sağlayabilir [74].

Bununla beraber, IoV sistemlerinin güvenliğinin tam olarak sağlanabilmesi için araştırma kurumları, üniversiteler, endüstriyel işletmeler ve resmi kurumlar arasında ortak çalışma ve uyumun sağlanması şarttır. Ortak standartların, düzenleyici yasaların ve sertifika programlarının geliştirilmesi, IoV sistemlerine olan güveni artıracak ve genel kabulü hızlı kılacaktır [75]. Toplumun bilinçlenmesi ve kullanıcı eğitimleriyle desteklenen bütünleşik bir IoV güvenlik stratejisi, akıllı ve bağlantılı araçların faydalarından güvenle yararlanılmasına olanak tanıyacaktır.

1.4. IoMT Tanımı ve Temel Kavramlar

IoMT, IoT teknolojilerinin sağlık hizmetleri ve tıp alanına uyumlu hale getirilmesiyle ortaya çıkan bir kavramdır. IoMT, hastaların, sağlık çalışanlarının ve sağlık kuruluşlarının, tıbbi cihazlar ve sağlık sistemleri aracılığıyla birbirleriyle ve internetle iletişim kurmasını ifade etmektedir [4]. Bu iletişim ağı sağlık verilerinin gerçek zamanlı olarak toplanmasını, iletilmesini, işlenmesini ve analiz edilmesini sağlayarak, tanı, tedavi ve bakım süreçlerinin verimli hale getirilmesine olanak tanır.

IoMT sistemlerinin temel gayesi, verilen sağlık hizmetlerinin kalitesini, erişilebilirliğini ve verimliliğini artırmak, aynı zamanda maliyetleri optimize etmektir. IoMT sistemlerinin teknolojileri, hastalar için daha kişiye özel, tahminleyici ve etkileşimli bir sağlık deneyimi sunarken, sağlık çalışanları için daha etkili karar verme ve bakım planlaması oluşturur [76]. Akıllı hastaneler, tele tıp, giyilebilir sağlık cihazları, dijital ilaçlar ve robotik cerrahi gibi uygulamalar, IoMT sistemlerinin sağlık hizmetleri alanındaki değişim yaratma gücünü kanıtlamaktadır. Tablo 1.3. IoMT cihazlarının sağlık hizmetlerindeki uygulama örneklerini göstermektedir.

Tablo 1.3. IoMT cihazlarının sağlık hizmetlerindeki uygulama örnekleri.

IoMT Cihaz Türü	**Uygulama Alanları**
Giyilebilir Sensörler	Hasta takibi, fitness izleme, kronik hastalık yönetimi
Akıllı İlaç Kutuları	İlaç takibi, dozaj hatırlatmaları
Teletıp Cihazları	Uzaktan teşhis ve tedavi, görüntüleme, veri analizi

IoMT sistemleri pazarının gün geçtikçe hızla büyümesi beklenmektedir. Şekil 1.4'te gösterildiği üzere Towards Healthcare raporlarının tahminlerine göre, küresel IoMT pazarı 2032 yılına kadar 305 milyar dolara ulaşacak ve 2022-2025 döneminde yıllık %19,7 büyüme oranı gösterecektir [77]. Bu büyümenin arkasındaki temel tetikleyici etmenler arasında, nüfusun yaşlanması, kronik hastalıkların artması, sağlık harcamalarındaki artış, teknolojik gelişmeler ve sağlık farkındalığının artması yer almaktadır.



Şekil 1.4. Küresel IoMT pazarının yıllara göre büyüklüğü ve 2032 yılına kadar yapılan tahminler (milyar dolar) [77].

1.4.1. IoMT Mimarisi ve Protokolleri

IoMT, tıbbi cihazların ve sağlık uygulamalarının internet aracılığıyla birbirine bağlanarak veri alışverişi yaptığı bir ekosistemi ifade etmektedir. Bu ekosistem, hastaların, sağlık profesyonellerinin, sağlık kuruluşlarının ve tıbbi akıllı cihazların birbirleriyle etkileşimini içermektedir. [78].

IoMT'nin temel bileşenleri şunlardır:

1. Tıbbi Cihazlar: Vücut sensörleri, giyilebilir cihazlar, implantlar, akıllı ilaç kutuları, tıbbi görüntüleme cihazları ve robotik sistemler gibi, veri sağlayan veya sağlık hizmetlerinde bulunan akıllı cihazlardır [79].
2. İletişim Ağı Altyapısı: Tıbbi cihazları birbirine ve internete bağlayan kablolu ve kablosuz iletişim teknolojilerini içerir. Wi-Fi, Bluetooth, hücresel ağlar (4G/5G), Zigbee, Yakın Alan İletişimi(NFC(Near Field Communication)) ve Radyo Frekansı ile Tanımlama(RFID(Radio Frequency Identification)) gibi protokoller bu alanda yaygın olarak kullanılmaktadır [80].
3. Veri Platformları: IoMT sistemlerinin verilerini toplayan, işleyen, analiz eden ve saklayan bulut tabanlı veya yerinde çalışan bilgi işlem sistemleridir. Bu platformlar, yapay zeka, makine öğrenmesi ve büyük veri madenciliği gibi teknolojileri kullanarak verilerden değerli çıktılar üretir [35].

4. Sağlık Uygulamaları: Sistemden sağlanan verileri kullanarak sağlık hizmetlerini sunan yazılım çözümleridir. Tele tıp, kişiselleştirilmiş tıp, kronik hastalık yönetimi, hasta izleme, ilaç yönetimi ve sağlık karar destek sistemleri gibi uygulamaları içermektedir [81].
5. Katılımcılar: Hastalar, sağlık profesyonelleri, sigorta şirketleri, ilaç firmaları, düzenleyici kurumlar ve teknoloji sağlayıcıları gibi, IoMT ekosistemindeki tüm aktörleri kapsar [82].

IoMT cihazları, çeşitli fizyolojik parametreleri (ör. kalp atış hızı, kan basıncı, solunum hızı, vücut sıcaklığı) ve çevresel faktörleri (ör. konum, aktivite, uyku) ölçerek, objektif ve gerçek zamanlı sağlık verileri sunar. Bu veriler, elektronik sağlık kayıtlarıyla entegre edilerek, hastaların kapsamlı bir profili oluşturulabilmektedir [83]. Ek olarak, IoMT cihazlarının verileri, halk sağlığı yönetimi gözetimi ve klinik araştırmalar içinde değerli bir kaynak oluşturmaktadır.

IoMT sistemlerinin sağladığı faydalar arasında özellikle şunlar öne çıkmaktadır [84]:

- Erken tanı ve önleyici bakım: IoMT sistemleri, hastalıkların belirtilerini erken tespit ederek ve risk faktörlerini izler, ileriye yönelik ve önleyici sağlık hizmetlerine olanak tanır.
- Kronik hastalık yönetimi: Diyabet, hipertansiyon, kalp, astım gibi kronik rahatsızlıkları olan hastaların uzaktan takibi ve yönetilmesi, hastalıkların semptomların kontrol altında kalmasını ve istenmeyen durumların önlenmesini sağlar.
- İlaç takibinin iyileştirilmesi: Akıllı ilaç kutuları ve hatırlatıcıları ile hastaların ilaçlarını zamanında ve doğru miktarlarda almalarına yardımcı olur.
- Hastaneye yatış oranı ve acil servis başvurularının azaltılması: Evde izleme ve tele tıp hizmetleri, hastaların gereksiz hastane yatışlarını ve acil durum başvurularını azaltır.
- Kişiye özgü tedavi: IoMT sistemlerinin verileri, hastaların eşsiz özelliklerine ve farklı ihtiyaçlarına göre uygun hale getirilmiş tedavi planları geliştirilmesini sağlar.
- Sağlık hizmetlerine erişimin artırılması: Tele tıp ve mobil sağlık uygulamaları, özellikle kırsal ve az hizmet alan bölgelerdeki hastalara sağlık hizmetlerine erişme imkanını arttırır.
- Maliyet verimliliği: IoMT cihazlarının teknolojileri, hastane yatışlarını, acil servis başvurularını ve gereksiz tahlilleri azaltarak sağlık harcamalarını azalmasını katkıda bulunur.

IoMT sistemlerinin etkin bir şekilde çalışabilmesi için aşağıdaki meselelerin dikkate alınması gerekmektedir [85]:

- Birlikte çalışabilirlik: Farklı üreticilerin IoMT cihazlarının ve sistemlerinin sorunsuz bir şekilde veri alışverişi yapabilmesi için ortak standartlar ve protokoller geliştirilmelidir.
- Veri güvenliği ve gizliliği: Hassas sağlık verilerinin yetkisiz erişim, sızıntı ve manipülasyondan korunması için güçlü güvenlik mekanizmaları ve veri koruma politikaları uygulanmalıdır.
- Yasal uyumluluk: IoMT cihazları ve uygulamaları, tıbbi cihaz yönetmelikleri (ör. Gıda ve İlaç İdaresi(FDA(Food and Drug Administration))), CE işareti) ve veri koruma yasaları (ör. Genel Veri Koruma Yönetmeliği(GDPR(General Data Protection Regulation)) ile uyumlu olmalıdır.
- Kolay kullanılabilirlik ve kullanıcı deneyimi: IoMT çözümleri, hasta ve sağlık çalışanları tarafından kolay ve sezgisel bir şekilde kullanılabilecek şekilde tasarlanmalıdır.
- Kanıta dayalı değerlendirme: IoMT müdahalelerinin klinik etkinliği ve maliyet verimliliği, kapsamlı klinik çalışmalarla değerlendirilmelidir.

1.4.2. IoMT Uygulama Alanları

IoMT sistemleri, sağlık hizmetlerinin hemen her alanında uygulanmakta ve önemli yararlar sağlamaktadır. Aşağıda, IoMT'nin başlıca uygulama alanları ve ilgili örnekler verilmektedir.

1. Uzaktan Hasta İzleme: Giyilebilir EKG cihazları ve akıllı saatler, hastaların kalp ritmini ve aktivitesini sürekli olarak izleyerek, kalp hastalıklarının erken teşhisine ve önlenmesine olanak tanır [86].
2. Tele tıp ve Sanal Sağlık Hizmetleri: Tele tıp platformları, özellikle kırsal ve az hizmet alan bölgelerdeki hastalara, uzman doktorlara erişim imkanı sunar. Ayrıca, COVID-19 salgını sırasında, bulaşma riskini azaltmak için tele tıp kullanımı önemli ölçüde artmıştır [87].
3. Akıllı Hastaneler ve Klinik Operasyonlar: Sağlık kuruluşlarında envanter yönetiminde RFID etiketleri ve sensörler kullanılarak, tıbbi cihazların ve ilaçların gerçek zamanlı takibi yapılabilir. Bu sayede, ekipman kullanılabilirliği artırılır, stok yönetimi optimize edilir ve hatalar azaltılır [88].

4. Bireye Özel ve Hassas Tıp Teknikleri: Giyilebilir cihazlar ve mobil uygulamalar, hastaların genetik, fizyolojik ve davranışsal verilerini toplayarak, kişiselleştirilmiş sağlık önerileri ve tedavi planları sunulmasını sağlar [89].
5. Tıbbi Robotik ve Yapay Zeka: Robot cerrahi sistemleri, daha yüksek hassasiyet, vücuda daha az müdahale gerektirme ve daha hızlı iyileşme avantajı sağlar. Yapay zeka uygulamaları ise tıbbi görüntülerin yorumlanmasında ve hastalık riskinin önlenmesinde doktorlara yardımcı olur [90].
6. Halk Sağlığı ve Salgın Yönetimi: IoMT sistemlerinin teknolojileri, salgınların erken tespit edilmesine, yayılmanın kontrol altına alınmasına ve risk altındaki toplumun belirlenmesine yardımcı olmaktadır. Örneğin yakın geçmişte, akıllı termal kameralar ve giyilebilir cihazlar, COVID-19 taşıyıcılarının belirlenmesinde kullanılmıştır [91].

Sonuç olarak, IoMT sistemlerinin uygulamaları sağlık hizmetlerinin her seviyesinde değer yaratmaktadır ve değiştirici bir güce sahiptir. Bununla beraber, IoMT sistemlerinin tam potansiyelinin kullanılması için önemli zorlukların aşılması gerekmektedir. Bunların başında, cihazların ve verilerin güvenliği, gizlilik, düzenleyici yasalar ve sağlık sistemlerinin teknolojik olarak olgunlaşması gelmektedir.

1.4.3. IoMT Güvenlik Sorunları ve Açık Problemler

IoMT sistemleri, sağlık hizmetlerinin kalitesini ve erişilebilirliğini artırırken, beraberinde önemli güvenlik ve gizlilik riskleri de getirmektedir. IoMT cihazları ve verileri, son derece hassas kişisel sağlık bilgilerini içerdiği için, bunların yetkisiz erişim, sızıntı, değiştirme ve istismardan korunması hayati değer taşımaktadır. Aşağıda, IoMT güvenliğinin başlıca sorunları ve açık problemleri ele alınmıştır.

1. Cihaz Güvenliği ve Donanım Açıkları: IoMT cihazlarının kısıtlı işlem gücü, bellek ve enerji kaynakları, geleneksel bilgi teknoloji sistemlerine kıyasla göre zayıf güvenlik önlemlerinin uygulanmasına neden olmaktadır [92]. Bunun yanında, IoMT cihazlarının uzun ömürlü olması ve sık güncellenememesi, zamanla yeni güvenlik açıklarının ortaya çıkmasına yol açmaktadır.
2. Ağ ve İletişim Güvenliği: IoMT cihazları genellikle kablosuz ağlar (Wi-Fi, Bluetooth, Zigbee vb.) üzerinden iletişim kurmaktadır. Bu ağların güvenlik açıkları, ağın test ve yayın

ortamlarının düzgün izole edilememesi, dışarıdan gelebilecek saldırılara açık olması, verilerin şifresiz iletilmesi ve yetkisiz erişime izin vermesi gibi risklere neden olabilmektedir [93].

3. Veri Gizliliği ve Mahremiyeti: IoMT verileri, hastaların tıbbi durumları, genetik bilgileri, davranışları ve konumları hakkında son derece hassas bilgiler içermektedir. Bu verilerin uygunsuz şekilde ele geçirilmesi veya kullanılması, hastaların mahremiyetini ihlal edebilir ve ayrımcılığa yol açmaktadır [94].
4. Düzenleyici Uyumluluk ve Standartlar: IoMT ekosisteminin küresel ve çok katılımcılı yapısı, yasal düzenleyici ihtiyaçların karmaşıklığını artırmaktadır. Farklı kanunlar içeren bölgelerdeki yasalara uyum sağlamak ve sektörel standartları takip etmek, IoMT sistemleri hizmet sağlayıcıları için zorlayıcı olabilmektedir [79].
5. İnsan Faktörü ve Sosyal Mühendislik: IoMT sistemlerine dahil olmuş olan, son kullanıcıların güvenlik davranışları ve tercihleri, IoMT sistemlerinin tamamlayıcı güvenliği üzerinde önemli bir etkiye sahiptir. Kullanıcıların bilinçlendirilmesi ve özellikle güvenlik konusunda eğitilmesi, kullanıcılardan kaynaklanan riskleri azaltmada önemli pay sahibi olmaktadır [95].

IoMT sistemlerinin güvenliğini artırmak için kapsamlı ve çok katmanlı bir koruma yaklaşım gerekmektedir. Bu yaklaşım, cihaz, ağ, uygulama ve veri katmanlarını kapsayan uçtan uca güvenlik önlemlerini içeren bir düzende olmalıdır [92]. Bazı temel öneriler şunlardır:

- Güvenli yazılım/donanım mimarisi ve yaşam döngüsü yönetimi
- Güçlü kimlik doğrulama, yetkilendirme ve erişim kontrolleri
- Uçtan uca şifreleme ve güvenli iletişim protokolleri (ör. TLS, DTLS)
- Düzenli risk kontrolü, güvenlik açığı yönetimi ve yazılım güncellemeleri
- Veri koruma ilkelerine uyum
- Siber güvenlik olaylarına müdahale ve iş sürekliliği planları
- Kullanıcıların güvenlik farkındalığını artırma ve eğitim programları

Ayrıca, blok zinciri, yapay zeka ve makine öğrenmesi gibi gelişen teknolojilerin IoMT güvenliğini iyileştirmedeki rolünün önemi de gün geçtikçe artmaktadır. Örneğin, blok zinciri, IoMT sistemlerinin verilerinin bütünlüğünü ve değiştirilemezliğini sağlamak için kullanılabilir [96]. Makine öğrenmesi algoritmaları ise IoMT sistemlerinin ağ trafiğindeki anormallikleri anlık olarak tespit ederek, sıfırıncı gün saldırılarına karşı savunma sağlayabilir [97].

Son olarak, IoMT sistemlerinin güvenliği, sağlık hizmetlerinin dijital dönüşümünde son derece kritik bir rol oynamaktadır. IoMT sistemlerinden tam olarak faydalanabilmek için siber risklerin öngörülebilen ve kapsamlı bir şekilde ele alınmasının sağlanması gerekmektedir. Bu, tüm katılımcıların (sağlık kuruluşları, doktorlar, hasta grupları, sigorta şirketleri, teknoloji firmaları, devlet kurumları vb.) birlikte çalışmasını ve ortak sorumluluğunu gerektiren zorluklarla dolu bir yoldur. Bununla birlikte, güvenli ve güvenilir IoMT sistemlerinin çözümlerinin geliştirilmesi, sağlık hizmetlerinin geleceği için kritik bir değere sahiptir.

1.5. Literatürde Yapılan Çalışmalar

IoV ve IoMT sistemlerinin güvenliği son yıllarda araştırmacıların ve endüstri profesyonellerinin artan ilgisini çekmektedir. Bu bölümde, IoV ve IoMT güvenliği alanlarındaki güncel akademik çalışmalar ve saldırı tespiti için önerilen derin öğrenme yaklaşımları detaylı olarak incelenecektir.

Literatür taramasının amacı, mevcut çalışmaların kapsamlı bir analizini sunmak, önemli bulguları vurgulamak, açık problemleri belirlemek ve gelecekteki araştırma yönlerini önermektir. Böylece, tez çalışmasının motivasyonu ve katkıları daha net bir şekilde ortaya konulabilecektir.

1.5.1. IoV Güvenliği Üzerine Yapılan Çalışmalar

Sakiz ve Sen [98], IoV ve VANET ağlarında karşılaşılan saldırı türlerini ve tespit yöntemlerini ayrıntılı bir şekilde incelemişlerdir. Yaptıkları bu çalışma, mevcut güvenlik çözümlerinin IoV'nin dinamik ve çeşitlilik gösteren yapısını tam olarak ele alamadığını vurgulamış ve uyarlanabilir, ölçeklenebilir savunma mekanizmalarına olan ihtiyacı ortaya koymuştur. Özellikle, makine öğrenmesi ve derin öğrenme tabanlı anomali tespit sistemlerinin bilinmeyen saldırıları yakalamada umut verici olduğu belirtilmiştir.

Alladi ve arkadaşları [99], IoV ağlarında araçların kötü niyetli davranışlarını tespit etmek için derin öğrenme tabanlı bir sınıflandırma modeli önermişlerdir. Sistem, araçların işlem birimlerinden gelen iletişim isteklerini yol kenarı birimleri tarafından işlemeden önce potansiyel kötü niyetli

araçları tespit etmeye odaklanmaktadır. Önerilen model, ikili ve üçlü olmak üzere iki farklı sınıflandırma yaklaşımı sunmakta ve Evrişimli Sinir Ağı (CNN(Convolutional Neural Network))-Uzun-Kısa Süreli Bellek(LSTM(Long Short-Term Memory)) hibrit mimarisi kullanmaktadır. Deneysel sonuçlar, özellikle ince taneli sınıflandırmanın hata ve saldırıları ayrı ayrı tespit etmede daha başarılı olduğunu göstermiştir.

Ahmed ve arkadaşları [100], IoV sistemlerinde araç içi ağların güvenliğini sağlamak için derin öğrenme tabanlı bir saldırı tespit sistemi önermişlerdir. CAN-bus protokolünü kullanan sistemde, VGG-16 mimarisi kullanılarak DoS ve Fuzzy saldırıları tespit edilmektedir. Model, araçların Araç İçi Teşhis(OBD(On-Board Diagnostics)) portuna gelen verileri analiz ederek saldırıları tespit etmekte ve geleneksel makine öğrenmesi yaklaşımlarına göre daha yüksek başarı göstermektedir. Önerilen sistem, araç içi ağların güvenliğini sağlamada etkili bir çözüm sunmaktadır.

Muhammad ve arkadaşları [101], IoV sistemlerinin güvenliğini, güvenilirliğini ve gizliliğini sağlamak için derin öğrenme tabanlı bir yaklaşım önermişlerdir. Araçlardan elde edilen verileri işlemek için tek boyutlu bir CNN mimarisi kullanan sistem, IoV verileri üzerinde düşük gecikmeli ve hafif bir çözüm sunmaktadır. Model, sıcaklık ve araç hızı gibi sensör verilerini gerçek zamanlı olarak analiz ederek, akıllı ulaşım sistemlerinde güvenlik tehditlerinin tespit edilmesine katkı sağlamaktadır.

Ullah ve arkadaşları [102], IoV sistemlerinde saldırı tespiti için LSTM ve Geçitli Tekrarlayan Birim(GRU(Gated Recurrent Unit)) tabanlı hibrit bir derin öğrenme modeli önermişlerdir. Model, araç içi ağlarda ve araçlar arası haberleşmede oluşabilecek DDoS, fuzzy ve spoofing gibi saldırıları tespit etmeyi amaçlamaktadır. Önerilen yaklaşım hem eğitim hem de yanıt süresini düşürürken, saldırı tespit performansını da önemli ölçüde artırmakta ve deneysel sonuçlarda yüksek başarı göstermektedir.

Arif ve arkadaşları [103], VANET'ler ve IoV (Internet of Vehicles) sistemleri için Yazılım Tanımlı Ağ(SDN(Software Defined Network)) ve sis bilişim tabanlı yeni bir mimari önermişlerdir. Önerilen mimari, yazılım tanımlı ağların sağladığı esneklik ve programlanabilirlik ile sis bilişimin konum tabanlı hizmetlerini birleştirmektedir. Sistem, V2V ve V2I iletişimi desteklerken, hibrit SDN mimarisi ve güvenlik katmanı ile güvenli haberleşme sağlamaktadır. Ayrıca akıllı trafik güvenlik sistemi de içeren yaklaşım, yapılan testlerde her iki iletişim türünde de başarılı sonuçlar göstermiştir.

Nie ve arkadaşları [104], Akıllı IoV sistemlerinde saldırı tespiti için DCNN tabanlı veri odaklı bir yaklaşım önermişlerdir. Geleneksel yöntemlerin aksine, trafik verilerini OBU'lardan değil RSU'lardan toplayarak sistem kaynaklarını daha verimli kullanmayı hedeflemişlerdir. Önerilen CNN mimarisi, bağlantı yükü davranışlarının özelliklerini çıkarmak ve RSU'lara yönelik saldırıları tespit etmek için 7 katmanlı bir yapı ve artık hata terimi içermektedir. Deneysel sonuçlar, önerilen yaklaşımın geleneksel makine öğrenmesi yöntemlerine kıyasla daha yüksek doğruluk ve daha düşük yanlış alarm oranı sağladığını göstermektedir.

Yang ve arkadaşları [105], IoV sistemlerinde hem bilinen hem de sıfır gün saldırılarını tespit edebilen çok katmanlı bir hibrit saldırı tespit sistemi önermişlerdir. Önerilen sistem, veri ön işleme ve öznitelik mühendisliği aşamalarını içeren ve dört katmanlı bir yapıdan oluşmaktadır. Bilinen saldırıları tespit etmek için ağaç tabanlı denetimli öğrenme modelleri, sıfır gün saldırılarını tespit etmek için ise k-means tabanlı denetimsiz öğrenme modeli kullanılmıştır. Deneysel sonuçlarda sistem hem araç içi hem de araçlar arası ağlarda yüksek saldırı tespit başarısı göstermiş, oldukça sağlam ve tutarlı sonuç elde etmiş ve düşük işlem süresiyle gerçek zamanlı çalışabildiğini kanıtlamıştır.

Korium ve arkadaşları [106], IoV sistemlerinde çoklu saldırı tipleri (DoS, DDoS, DrDoS, botnet, brute force vb.) için çok katmanlı bir hibrit saldırı tespit sistemi önermişlerdir. Model, veri ön işleme ve öznitelik mühendisliği aşamalarından sonra dört katmandan oluşmakta ve hem bilinen hem de sıfır gün saldırılarını tespit edebilmektedir. Deneysel sonuçlarda önerilen sistem yüksek saldırı tespit başarısı göstermiş ve düşük işlem süresiyle gerçek zamanlı çalışabildiğini kanıtlamıştır.

Man ve arkadaşları [107], IoV sistemlerinde yapay zeka tabanlı bir saldırı tespit sistemi önermişlerdir. Makale öncelikle IoV kavramını ve özelliklerini tanıtarak, IoV ağlarına yönelik güvenlik tehditlerini incelemekte ve ardından yapay zeka tabanlı saldırı tespit sistemleri üzerine yapılan güncel araştırmaları derlemektedir. Yazarlar ayrıca IoV'de saldırı tespitine yönelik açık zorlukları ve gelecek araştırma yönlerini tartışmışlardır.

1.5.2. IoMT Güvenliği Üzerine Yapılan Çalışmalar

Chaganti ve arkadaşları [108], IoMT sistemlerinde saldırı tespiti için PSO ve derin öğrenme tabanlı yeni bir yaklaşım önermişlerdir. Çalışmada, ağ trafiği ve hasta biyometrik verilerini birleştirerek daha etkili ve doğru bir saldırı tespit sistemi geliştirmeyi amaçlamışlardır. Önerilen PSO ve Derin Sinir Ağı(DNN(Deep Neural Network)) modeli, özellik seçimi için Parçacık Sürü Optimizasyonu (PSO) ve sınıflandırma için DNN kullanmaktadır. Model, literatürdeki diğer çalışmalarla karşılaştırıldığında %96'lık doğruluk oranıyla daha iyi performans göstermiştir.

Thamilarasu ve arkadaşları [109], IoMT sistemlerinde saldırı tespiti için mobil ajan tabanlı yeni bir saldırı tespit sistemi önermişlerdir. Önerilen sistem, ağ ve cihaz seviyesinde anormallik tespiti için makine öğrenmesi ve regresyon algoritmalarını kullanan hiyerarşik ve özerk bir yapıya sahiptir. Yazarlar, ağ topolojisini simüle ederek hastane ortamında kablosuz vücut alan ağları ve diğer bağlantılı tıbbi cihazlar için detaylı deneyler gerçekleştirmişlerdir. Minimum kaynak kullanımıyla son derece yüksek bir başarı oranında saldırı tespit doğruluğu elde etmişlerdir.

Zachos ve arkadaşları [110], IoMT sistemlerinde anormallik tabanlı saldırı tespiti için yeni bir mimari önermişlerdir. Önerilen sistem, IoMT cihazları ve ağ geçidi üzerinde dağıtık izleme ve veri toplama bileşenleri ile ağ geçidi üzerinde merkezi tespit bileşeninden oluşmaktadır. Sistem, makine öğrenmesi teknikleri kullanarak ağ ve cihaz seviyesinde %96 doğrulukla anormal davranışları tespit edebilmektedir. Yazarlar, değerlendirme sonucunda Karar Ağacı(DT(Decision Tree)), Rasgele Orman(RF(Random Forest)) ve K-En Yakın Komşu(KNN(K-Nearest Neighbors)) algoritmalarının anomali tespitinde en iyi performansı gösterdiğini belirlemişlerdir.

Ravi ve arkadaşları [111], IoMT sistemlerinde saldırı tespiti için derin öğrenme tabanlı yeni bir yaklaşım önermişlerdir. Önerilen sistem, ağ akışı ve hasta biyometrik verilerini kullanarak saldırıları tespit etmek için çok katmanlı bir derin öğrenme mimarisi ve global dikkat mekanizması içermektedir. Yazarlar, dengesiz veri problemini çözmek için maliyet duyarlı öğrenme yaklaşımını entegre etmişlerdir. Model, WUSTL EHMS 2020 veri setinde ağ özellikleri üzerinde %95, hasta biyometrikleri üzerinde %89 ve birleşik özellikler üzerinde %99 doğruluk elde etmiştir. Önerilen yaklaşım, diğer yöntemlerle karşılaştırıldığında IoMT saldırı tespit veri setinde %3,9 daha yüksek doğruluk göstermiştir.

Areia ve arkadaşları [112], IoMT sistemlerinde saldırı tespiti için kullanılabilecek yeni bir veri seti olan IoMT-TrafficData'yı önermişlerdir. Veri seti, paket tabanlı ve akış tabanlı olmak üzere iki alt

veri setinden oluşmakta ve IoMT ağlarında görülen sekiz farklı saldırı türünü içermektedir. Araştırmacılar çeşitli makine öğrenmesi ve derin öğrenme modellerini kullanarak veri seti üzerinde ikili ve çok sınıflı sınıflandırma deneyleri gerçekleştirmişlerdir. Deneysel sonuçlarda, modellerin zararlı trafiği tespit etmede %90'ın üzerinde F1-skor elde ettiği ve akış tabanlı özelliklerin paket tabanlı özelliklere göre %5'e varan daha iyi performans sağladığı gösterilmiştir.

Alsolami ve arkadaşları [113], IoMT sistemlerinde saldırı tespiti için topluluk öğrenme yöntemlerinin etkinliğini araştırmışlardır. Çalışmada, Random Forest ve Support Vector Machine tabanlı modelleri temel alarak Stacking, Bagging ve Boosting teknikleri WUSTL-EHMS-2020 veri seti üzerinde değerlendirilmiştir. Deneysel sonuçlarda Stacking yaklaşımı en yüksek başarıyı gösterirken, bunu sırasıyla Bagging ve Boosting yöntemleri takip etmiştir. Önerilen topluluk öğrenme yaklaşımlarının IoMT sistemlerindeki siber saldırıları tespit etmede yüksek başarı gösterdiği ve hassas sağlık verilerinin korunmasında etkili olduğu ortaya konmuştur.

Manimurugan ve arkadaşları [114], IoMT sistemlerinde saldırı tespiti için Derin İnanç Ağı(DBN(Deep Belief Network)) tabanlı derin öğrenme yöntemini önermişlerdir. CICIDS 2017 veri seti kullanılarak gerçekleştirilen deneylerde önerilen model, Botnet, Brute Force, DDoS, Infiltration, Port Scan ve Web saldırıları gibi farklı saldırı türlerini başarıyla tespit etmiştir. Geleneksel makine öğrenmesi yöntemleriyle karşılaştırıldığında DBN tabanlı yaklaşımın tüm saldırı türlerinde yüksek performans gösterdiği ve IoMT sistemlerinde saldırı tespiti için güvenilir bir çözüm sunduğu görülmüştür.

1.5.3. CICIoV2024 Veri Seti Kullanılan Çalışmalar

Amirudin ve Abdulkadir [115], IoV sistemlerinde saldırı tespiti için LightGBM, XGBoost, CatBoost ve Yerel Kaskad Kompozisyon Diferansiyel Evrimi(LCCDE(Local Cascade Composition Differential Evolution)) algoritmalarının karşılaştırmalı analizini yapmışlardır. CICIoV2024 veri setini kullanan çalışma, araç içi ağlarda DoS ve spoofing saldırılarının tespitine odaklanmaktadır. Önerilen yaklaşımda, veri ön işleme aşamasında Z-score normalizasyonu, k-means kümeleme ve Sentetik Azınlık Aşırı Örnekleme Tekniği(SMOTE(Synthetic Minority Over-sampling Technique)) teknikleri kullanılmıştır. Deneysel sonuçlarda tüm modeller %100 doğruluk, hassasiyet, duyarlılık ve F1-skoru elde etmiştir. Çalışma sonuçları, gelişmiş makine öğrenmesi tekniklerinin IoV sistemlerinin güvenliğini sağlamada etkili olduğunu göstermektedir.

Nakayiza ve arkadaşları [116], IoV sistemlerinde araç içi veri sahtekarlığının tespiti için farklı makine öğrenmesi algoritmalarının (RF, Saf Bayes(NB(Naive Bayes)), Destek Vektör Makinesi(SVM(Support Vector Machine)), Lojistik Regresyon(LR(Logistic Regression)), Adaptif Güçlendirme (AB(AdaBosst)), DNN, Tekrarlayan Sinir Ağı(RNN(Recurrent Neural Network)), KNN) performansını analiz etmişlerdir. CICIoV2024 veri setini kullanan çalışmada, veri ön işleme aşamasında eksik değerlerin ortalama ile doldurulması, özelliklerin standartlaştırılması ve kategorik değişkenlerin one-hot encoding ile sayısallaştırılması teknikleri uygulanmıştır. Hem ikili hem de çok sınıflı sınıflandırma deneylerinde, önerilen yaklaşım %95-100 arasında doğruluk, hassasiyet, duyarlılık ve F1-skoru elde etmiştir. Çalışma, etkili veri ön işlemenin model performansını önemli ölçüde artırdığını göstermiştir.

Rafrastara ve arkadaşları [117], IoV sistemlerinde saldırı tespiti için Naive Bayes, Decision Tree ve Logistic Regression algoritmalarının performansını analiz etmişlerdir. CICIoV2024 veri setini kullanan çalışmada, araç içi ağlardaki DoS ve spoofing saldırılarının tespitine odaklanılmıştır. 10 katlı çapraz doğrulama kullanılan çalışmada, Naive Bayes algoritması %98.1 doğruluk ve %98 F1-skoru ile en iyi performansı göstermiştir. Çalışma sonuçları, basit makine öğrenmesi algoritmalarının daha karmaşık Deep Neural Network ve Random Forest gibi yöntemlere kıyasla daha etkili olabileceğini göstermiştir.

Gul ve Bakir [118], IoV sistemlerinde saldırı tespitinin doğruluğunu artırmak için genetik algoritma tabanlı hiper parametre optimizasyonu yaklaşımı önermişlerdir. CICIoV2024 veri setini kullanan çalışmada, Logistic Regression, AdaBoost, Deep Neural Network ve Random Forest algoritmaları için hiper parametreler genetik algoritma ile optimize edilmiştir. Deneysel sonuçlarda en iyi performansı %99.64 doğruluk oranı ile Random Forest algoritması göstermiştir. Önerilen yaklaşım, orijinal çalışmaya kıyasla tüm algoritmalarda iyileştirme sağlamış ve özellikle AdaBoost'ta %4.76'lık bir performans artışı elde edilmiştir.

Merzouk ve arkadaşları [119], Derin Pekiştirmeli Öğrenme(DRL(Deep Reinforcement Learning)) tabanlı saldırı tespit sistemlerinin düşmanca örneklere karşı dayanıklılığını sistematik olarak analiz etmişlerdir. CICIoV2024, UNSW-NB15 ve NSL-KDD veri setlerini kullanan çalışmada, DRL algoritmaları Derin Q-Ağı(DQN(Deep Q-Network)), Proksimal Politika Optimizasyonu(PPO(Proximal Policy Optimization)), Güven Bölgesi Politika Optimizasyonu(TRPO(Trust Region Policy Optimization)), Avantaj Aktör Kritik(A2C(Advantage

Actor-Critic)), QRDQN), sinir ağı derinliği ve genişliği gibi hiper parametrelerin sistemin performansı ve dayanıklılığı üzerindeki etkileri incelenmiştir. Araştırma sonuçları, A2C algoritmasının düşmanca örneklere karşı en dayanıklı model olduğunu ve TRPO'nun da yakın performans sergilediğini göstermiştir. Ayrıca, sinir ağı mimarisinin seçimi ve verilerin karmaşıklık seviyesinin sistemin dayanıklılığını önemli ölçüde etkilediği tespit edilmiştir.

Aswal ve Pathak [120], IoV sistemlerinde CAN ağlarının güvenliğini artırmak için Çok Katmanlı Algılayıcı(MLP(Multi-Layer Perceptron)) tabanlı bir derin öğrenme çözümü önermişlerdir. Model, araç içi haberleşme sisteminde oluşabilecek DoS ve spoofing gibi saldırıları tespit etmeyi amaçlamaktadır. Önerilen yaklaşım, %99.99 doğruluk oranı ile saldırı tespiti yapabilmekte ve literatürdeki diğer çalışmalara kıyasla daha yüksek başarı göstermektedir. Model ayrıca düşük kaynak kullanımı ve gerçek zamanlı tespit yeteneği ile öne çıkmaktadır.

Khan ve Shivabasappa [121], IoT ortamlarında gelişen siber tehditleri tespit etmek için Konsept-Kayma XGBoost (CD-XGB) adı verilen yeni bir derin öğrenme modeli önermişlerdir. Model, değişen saldırı kalıplarını belirlemek ve bunlara uyum sağlamak için Geliştirilmiş Konsept-Kayma Tanımlama (ICDI) adlı ek bir algoritma içermektedir. CD-XGB modeli CICIoV2024 kullanılarak test edilmiş %99.96 doğruluk oranlarına ulaşmıştır. Model, konsept kaymasını etkili bir şekilde ele alırken çeşitli siber saldırı türlerinde yüksek tespit doğruluğunu koruyarak mevcut yaklaşımlardan daha iyi performans göstermiştir.

Mahdi ve arkadaşları [122], IoT ağlarında DDoS ve spoofing saldırılarını tespit etmek için derin öğrenme ve makine öğrenmesi yaklaşımlarını birleştiren hibrit bir metodoloji önermişlerdir. Yazarlar, özellik seçimi için korelasyon katsayısı ve sıralı özellik seçici tekniklerinin birleşiminden oluşan hibrit bir yöntem kullanmışlardır. Model, derin öğrenme (LSTM katmanları) ve makine öğrenmesi sınıflandırıcısını (Naive Bayes) birleştiren hibrit bir yapıya sahiptir. Metodolojinin performansı CICIoV2024 veri seti kullanılarak test edilmiş ve %99.77 doğruluk oranına ulaşılmıştır. Model, konsept kaymasını etkili bir şekilde ele alırken çeşitli siber saldırı türlerinde yüksek tespit doğruluğunu koruyarak mevcut yaklaşımların ötesinde performans göstermiştir.

1.5.4. CICIoMT2024 Veri Seti Kullanılan Çalışmalar

Hernandez-Jaimes ve arkadaşları [123], IoMT ortamlarında fidye yazılımı tespiti için Nilsimsa parmak izi tabanlı yeni bir makine öğrenmesi yaklaşımı önermişlerdir. Bu yaklaşım, mevcut ML Makine Öğrenmesi(ML(Machine Learning)) tabanlı saldırı tespit yöntemlerinde karşılaşılan özellik bağımlılığı sorununu ele almaktadır. Model, iki IoMT veri seti (ICE ve CICIoMT2024) kullanılarak test edilmiş ve klasik özellik çıkarımı tabanlı yöntemlere kıyasla daha iyi performans göstermiştir. CICIoMT2024 veri setinde %99.44 hassasiyet ve %98.59 F1-skor elde edilmiştir. Önerilen yaklaşım, özellikle eğitim verimliliği ve yanlış alarm oranını azaltma konusunda başarılı sonuçlar vermiştir.

Mohammadi ve arkadaşları [124], IoMT sistemlerinde siber saldırıları tespit etmek için CNN tabanlı yeni bir derin öğrenme modeli önermişlerdir. CICIoMT2024 veri seti üzerinde test edilen model, 18 farklı siber saldırı türünü tespit edebilmekte ve ikili, kategorik ve çok sınıflı sınıflandırma görevlerinde %99 doğruluk oranına ulaşmaktadır. Önerilen CNN modeli, Lojistik Regresyon, AdaBoost, DNN ve Random Forest gibi geleneksel makine öğrenmesi yöntemlerinden daha yüksek performans göstermektedir. Model özellikle karmaşık saldırı türlerini ayırt etmede ve gerçek zamanlı tehdit tespitinde başarılı sonuçlar vermektedir.

Sohail ve arkadaşları [125], IoMT sistemlerinde saldırı tespiti için XGBoost, AdaBoost ve CatBoost olmak üzere üç farklı boosting algoritması kullanan açıklanabilir bir saldırı tespit sistemi önermişlerdir. CICIoMT-2024 veri seti üzerinde yapılan deneylerde, XGBoost sınıflandırıcısı %95.01, AdaBoost %92.89 ve CatBoost %88.37 doğruluk oranı elde etmiştir. Önerilen sistemde Açıklanabilir Yapay Zeka(XAI(Explainable Artificial Intelligence)) teknikleri kullanılarak modellerin karar verme süreçleri şeffaf hale getirilmiş ve özellik önem grafikleri ile hangi ağ özelliklerinin saldırı tespitinde daha etkili olduğu gösterilmiştir. Çalışma, IoMT ortamlarında çoklu saldırı türlerinin sınıflandırılması konusunda boosting algoritmalarının etkinliğini ortaya koymuştur.

Naeem ve arkadaşları [126], IoMT sistemlerinin güvenliğini artırmak için veri artırma (data augmentation), öznitelik seçimi ve topluluk öğrenme tekniklerini birleştiren kapsamlı bir yaklaşım önermişlerdir. Transformer tabanlı sinir ağları, self-attention Derin Evrişimli Sinir Ağı(DCNN(Deep Convolutional Neural Network))'ler ve LSTM ağlarını içeren derin öğrenme modellerinden oluşan bir topluluk modeli geliştirmişlerdir. BAT algoritmasıyla veri artırma ve

Özyinelemeli Öznitelik Eleme(RFE(Recursive Feature Elimination)) teknikleri kullanılarak modelin genelleştirme performansı artırılmıştır. WUSTL-EHMS-2020 ve CICIoMT2024 veri setleri üzerinde yapılan deneylerde önerilen yaklaşım, sırasıyla %100 ve %99 doğruluk oranlarına ulaşarak saldırı tespitinde üstün performans göstermiştir. Ayrıca SHAP Shapley Katkısal Açıklamalar(SHAP(SHapley Additive exPlanations)) ve Tekdüze Manifold Yaklaşımı ve Projeksiyon(UMAP(Uniform Manifold Approximation and Projection)) görselleştirmeleriyle modelin karar verme süreci açıklanabilir hale getirilmiştir.

Misbah ve arkadaşları [127], IoMT sistemlerinde siber güvenliği artırmak için "SmartEdge" adında ölçeklenebilir ve adaptif bir çerçeve önermişlerdir. Çalışmada, sistematik ön işleme, gelişmiş özellik seçimi, kontrollü örnekleme ve yenilikçi model birleştirme teknikleri kullanılarak IoMT verilerinin işlenmesi ve analizi optimize edilmiştir. CICIoMT2024 veri seti üzerinde yapılan deneylerde, önerilen yaklaşım boyut indirgeme ile hesaplama yükünü %95 azaltırken, siber saldırı tespitinde 0.99'un üzerinde doğruluk oranı elde etmiştir. 10 kenar modeli sadece 55 saniyede eğitilmiş ve sıfıra yakın birleştirme süresiyle etkili sonuçlar alınmıştır.

Ullah ve arkadaşları [128], tüketiciler için sağlık cihazlarında siber güvenliği artırmak için Federe Öğrenme(FL(Federated Learning)) ve ağ trafiği örneklerini kullanan yeni bir kenar zekası yaklaşımı önermişlerdir. Çalışmada, ağ trafiği verilerinden görüntü tabanlı özellikler çıkarılarak ayırt edici bir veri seti oluşturulmuştur. Aralıklı istemci davranışı nedeniyle dengesiz veri setleri problemi ele alınmış ve giriş verilerinde bozulmalar oluşturan dört farklı saldırı yöntemi kullanılarak gürbüz veri setleri oluşturulmuştur. İşbirlikçi FL mimarisi veri güvenliği, gizliliği ve kenar zekasını sağlamıştır. Önerilen yöntem CICIoMT2024 ve Edge-IIoT olmak üzere iki standart veri seti üzerinde test edilmiş ve sırasıyla %97.45 ve %96.7 tespit doğruluğu elde edilmiştir.

Chen ve arkadaşları [129], IoT sistemlerinde saldırı tespiti için bilgi damıtma (knowledge distillation) ve federe proksimal öğrenme (federated proximal learning) tabanlı FedKD-Prox adında etkili bir federe öğrenme çerçevesi önermişlerdir. Önerilen yaklaşım, kısıtlı kaynaklara sahip IoT cihazlarında model eğitiminin verimini artırmak ve heterojen veri sorunlarını hafifletmek için, sunucu-cihaz iletişiminde model bilgisi paylaşımı ve yerel modeller üzerinde uyarlanabilir ceza stratejileri kullanmaktadır. CICIoT2024 ve Edge-IIoT veri setleri üzerinde yapılan deneyler, FedKD-Prox'un diğer federe öğrenme algoritmalarına kıyasla daha yüksek tespit doğruluğu ve daha hızlı yakınsama sağladığını göstermiştir.

Suarez Gomez ve arkadaşları [130], IoT sistemlerinde sınırlı hesaplama kapasitesine sahip cihazlar için anormal davranış tespitine dayalı bir Saldırı Tespit Sistemi(IDS(Intrusion Detection System)) önermişlerdir. Çalışmada, derin öğrenme tabanlı çözümlerin düşük kaynaklı IoT cihazları için uygun olmadığı belirtilerek İzolasyon Ormanı(IForest(Isolation Forest)), Yerel Aykırı Değer Faktörü(LOF(Yerel Aykırı Değer Faktörü)) ve Küme Tabanlı Yerel Aykırı Değer Faktörü(CBLOF(Cluster-Based Local Outlier Factor)) olmak üzere üç farklı anormal davranış tespit algoritması değerlendirilmiştir. CICIoMT2024 veri seti üzerinde yapılan deneysel sonuçlarda, IForest algoritması 0.85 Eğri Altındaki Alan(AUC(Area Under Curve)) Alıcı İşletim Karakteristiği(ROC(Receiver Operating Characteristic)) skoru ile normal ve anormal ağ trafiğinin ayırt edilmesinde en iyi performansı göstermiştir.

2. MATERYAL VE YÖNTEM

2.1. Kullanılan Veri Setleri

Bu tez çalışmasında IoV ve IoMT sistemleri için iki adet açık kaynaklı güncel veri seti kullanılmıştır. Bunlar CICIoV2024 ve CICIoMT2024 veri setleridir. Bu bölümde bu veri setlerinin özellikleri, nasıl oluşturuldukları ve içerdikleri veriler ayrıntılı olarak bahsedilecektir.

2.1.1. CICIoV2024 Veri Seti

CICIoV2024 veri seti, Kanada Siber Güvenlik Enstitüsü(CIC(Canadian Institute for Cybersecurity)) tarafından IoV sistemleri için güvenlik sistemlerinin oluşturulması ve geliştirilmesi için kapsamlı bir şekilde hazırlanmış gerçek cihazlardan sağlanan verileri içeren kapsamlı karşılaştırma veri setidir. Bu veri setinin tasarlanma amacı, araç içi iletişim sistemlerindeki güvenlik ve gizlilik zafiyetlerini tespit etmek ve bu tehditlere karşı geliştirilecek olan savunma mekanizmalarının oluşturmaktır. Veri seti, 2019 model bir Ford marka aracın, bütün Elektronik Kontrol Ünitesi(ECU(Electronic Control Unit))'lerinin dahil olduğu gerçek iç yapısındaki işlemler sonucunda oluşturulmuştur. Gerçek bir aracın iç yapısı kullanılmış olsa da, gerçekleşebilecek tehlikelerin önüne geçmek için, iç yapı araçtan sökülmüş ve araç hareketsiz hale getirilmiştir. Yapılan tüm deneyler Şekil 2.1'de gösterildiği üzere kontrollü bir laboratuvar ortamında gerçekleştirilmiştir.



Şekil 2.1. Ford model aracın kontrol ünitelerinin laboratuvar ortamına aktarılması [21]

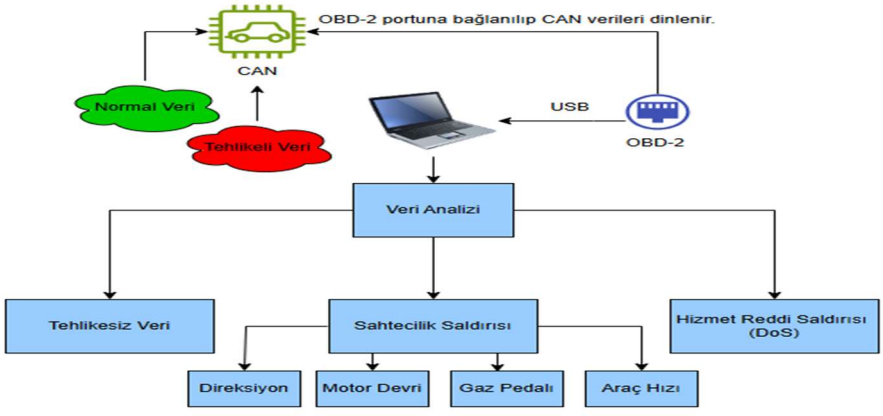
Denetleyici Alan Ağı (CAN) protokolü, araç içi seri veri yolu iletişiminde kullanılmakta ve bahsedilen veri setinin temelini oluşturmaktadır. Temel yapısı Tablo 2.1'de görüldüğü gibidir. CAN protokolü yüksek ve düşük hızlı iki farklı seri veri yolundan oluşur. Yüksek hızlı veri seri yolunun, veri iletim hızı 1 Mbps' e kadar yükselebilmekte, bu veri seri yolu daha çok kritik motor kontrol sistemlerinde (fren vb.) ve güvenlik sistemleri için kullanılmaktadır. Aydınlatma ve kapı

kilitleri daha az kritik sistemler için, hızı 40 Kbps ile 250 Kbps arasında olan düşük hızlı veri seri yolu kullanılır [21].

Tablo 2.1. CAN Protokolü Paket Yapısı [21]

Sıra	Adı	Boyut	Sıra	Adı	Boyut
1	Çerçeve Başlangıcı	1 bit	5	Veri Alanı	64 bit
2	Arbitrasyon ID	11 veya 29 bit	6	Yedek Kontrol Alanı	16 bit
3	Uzak İletim Alanı	1 bit	7	Onay Alanı	2 bit
4	Kontrol Alanı	6 bit	8	Çerçeve Sonu	7 bit

CAN protokolünde verinin iletilmesi belirli bir paket düzeniyle gerçekleştirilmektedir. Her bir CAN paketi, 1 bitlik çerçeve başlangıç alanıyla başlar ve ardından mesajın önceliğini belirleyen Arbitrasyon ID alanı gelir. Bu ID'nin düşük olması, önceliğin yüksek olduğunu gösterir. Paketin devamında 1 bitlik uzaktan iletim alanı, ardından paketin doğruluğunun kontrolünü sağlayan kontrol alanı bulunur. Pakette iletmek istenilen veri 64 bit boyutundaki veri alanında taşınır. Veriden sonra ise yedek kontrol alanı ve iletin verinin iletilip iletilmediği tutan onay alanından sonra çerçeve sonu ile paketin bittiği bildirilir. Bu paket yapısı sayesinde araçlar içerisindeki tüm iletişim, son derece düzenli ve kontrollü bir biçimde gerçekleşmektedir.



Şekil 2.2. Veri setinin oluşturulması için kullanılan test ortamı. [21]

Veri setinin güvenli şekilde oluşturulması için, test ortamı, hem tüm ağ trafiğini kaydedebilecek, hem de güvenli bir şekilde erişim sağlayacak şekilde tasarlanmıştır. Bu test ortamını oluşturmak için bir kaç farklı özelleştirilmiş donanım kullanılmıştır. CAN veri yoluna bağlanmak için, USB Evrensel Seri Veriyolu(USB(Universal Serial Bus)) arayüzü sağlayan Evrensel Seri Veri Yolu'ndan Kontrol Alan Ağı'na(USB2CAN(Universal Serial Bus to Controller Area Network)) cihazı,OBD-2 standardı üzerinden, araç verilerine Bluetooth üzerinden kablosuz erişimi sağlayan Gömülü Hafif Modül 32(ELM32(Embedded Lightweight Module)) cihazı ve açık kaynaklı bir otomotiv bağlantı arayüzü sunan Macchina M2 geliştirme kartı, bu donanımların öne çıkanlarındandır. Macchina M2 kartına çeşitli bağlantı modülleri eklenebilmesi, test ortamına büyük bir esneklik kazandırmıştır. Ek olarak, aracın ağ trafiğinin, sürekli ve performans sorunu oluşmadan bilgisayara kaydedilebilmesi için özel bir ağ donanımı kullanılmıştır [21].

Test ortamı oluşturulurken, kullanılan donanımlar kadar, kullanılan yazılımlarda veri toplama sürecinin önemli bir parçasını oluşturmaktadır. Kullanılan SocketCAN isimli yazılım, aracın CAN arayüzüne standart soket ağı üzerinden erişim sağlamıştır. Aracın CAN arayüzüne, Can-utils isimli, yazılım paketi içerisindeki cansniffer isimli araç ile paket yakalama işlemi, cansend isimli araç ile paket gönderme işlemi, candump isimli araç ile gönderilen paketleri kaydetme işlemi, canplayer isimli araç ile ise test amaçlı kullanım için rastgele paket üretme işi gerçekleştirilmiştir. Buna ek olarak, test ve geliştirme aşamalarında sanal CAN arayüzü oluşturmak için Sanal Kontrol Alan Ağı(VCAN(Virtual Controller Area Network)) sürücüsü kullanılırken, kaydedilen paketlerin detaylı analizi için Wireshark isimli yazılım kullanılmıştır[21].

Veri setini oluşturmak için, test ortamında iki ana kategoride saldırı gerçekleştirilmiştir. Bunlardan ilk olan DoS, CAN veri yolunun arbitrasyon alanı hedef alınmıştır. DoS saldırı türünde, sisteme sürekli sahte ve yüksek öncelikli paketler gönderilerek, mevcut gerekli iletişimin engellenip önüne geçilmesi hedeflenmiştir. Bu sayede CAN ağı aşırı yüklenir ve sürekli sahte mesajlar işlenerek, ECU'ların veri yoluna erişimi engellenmiş olur. Ek olarak, iletim hızının oynanmasıyla belirli iletişim kanalları engellenerek, sistemin kullanılabilirliği tehlikeye atılır.

İkinci saldırı kategorisi olan sahtecilik saldırılarında, dört farklı hedef belirlenmiştir. Direksiyon simülasyonu saldırısında, direksiyonun özel id'sini içeren paketle direksiyon pozisyonu 0.1 derece manipüle edilmiş ve ardından test edilip veriler kaydedilmiştir. Motor devri simülasyonunda, devir kısmının özel id'sini içeren paketle motor devri manipüle edilerek, ardından test edilip veriler

kaydedilmiştir. Hız simülasyonunda ise, araç hızı saldırı ile manipüle edilerek saldırı senaryoları düzenlenmiş ve test verileri kaydedilmiştir. Son saldırı türünde ise gaz pedalının konumu ile oynanmış ve test verileri kaydedilmiştir [21]. Bu eklenen veriyle birlikte oluşan veri setinin örnek sayısı dağılımı Tablo 2.2.'de gösterilmektedir.

Tablo 2.2. CICIoV2024 veri setindeki bulunan sınıflar ve örnek sayıları [21]

Etiket	**Kategori**	**Sınıf**	**Örnek Sayısı**
Normal Trafik	-	-	1.223.737
Saldırı Trafiği	Hizmet Reddi Saldırısı	-	74.663
	Sahtecilik Saldırısı	Gaz Pedalı	9991
		Direksiyon	19.977
		Araç Hızı	24.951
		Motor Devri	54.900

Oluşturulmuş olan veri setinde normal trafik verisi ve saldırı trafiği olmak üzere, iki ana kategoride veri toplanmıştır. Gerçek bir aracın günlük operasyon verilerini yansıtan temiz yani tehlikesiz trafik kategorisinde 1.223.737 örnek bulunurken, DoS saldırı trafiğinde ise 74.663 örnek bulunmaktadır. Sahtecilik saldırıları ise 4 farklı alt kategoriye ayrılmıştır. Direksiyon manipülasyonu için 19.977 örnek, motor devri manipülasyonu için 54.900 örnek, hız manipülasyonu için 24.951 örnek ve son olarak gaz pedalı konumu manipülasyonu için 9.991 örnek kaydedilmiştir [21].

CICIoV2024 veri seti literatüre üç farklı veri formatında sunulmuştur. Bunlar aynı verinin ikili tabanda, onluk tabanda ve on altılık tabanda gösterimi olarak ifade edilmesidir. Üç farklı formatta sunulmasının temel medeni farklı makine öğrenmesi tekniklerinin, performanslarını değerlendirmek için önemli bir özellik sağlamaktadır. İkili tabanda özellikle veri alanları, bit seviyesinde ayrılarak ayrıntılı analiz için sağlanmıştır. Onlu tabandaki tüm veriler ise, onluk sisteme çevrilmiş halde sunulmuştur. On altılık tabanda sağlanan veriler ise CAN protokolünün orijinal veri formatının türünü yansıtmaktadır.

Veri setinde her bir örnek için belirli özellikler bulunmaktadır. Arbitrasyon ID alanı mesajın önceliğini ve taşınan verinin türünü belirtmektedir. DATA_0 alanında DATA_7 alanına kadar olan 8 kolonluk alan pakette taşınan bilginin baytlarını içermektedir. Label alanı, trafik örneğinin, tehlikeli veya tehlikesiz olduğunu belirtmektedir. Category alanı ise trafik örneğinin hangi kategoriye ait olduğunu göstermektedir. Son olarak ise specific_class alanıysa, örnek trafiğin hangi özel alt alana ait olduğunu bildirir [21].

Tablo 2.3. CICIoV2024 veri setindeki sunulan özellikler [21]

Özellik Adı	**Açıklama**
ID	Mesajın önceliğini ve taşıdığı veri türünü belirtir.
DATA_0	İletilen verinin ilk baytı.
DATA_1	İletilen verinin 1. baytı.
DATA_2	İletilen verinin 2. baytı.
DATA_3	İletilen verinin 3. baytı.
DATA_4	İletilen verinin 4. baytı.
DATA_5	İletilen verinin 5. baytı.
DATA_6	İletilen verinin 6. baytı.
DATA_7	İletilen verinin 7. baytı.
Label	Zararsız veya zararlı ağ trafiğinin tanımlanması.
Category	Trafiğin ait olduğu kategorinin tanımlanması.
Specific_class	Trafiğin belirli sınıfının tanımlanması

CICIoV2024 veri seti, literatürde bulunan diğer veri setlerinden önemli farklılıklar içermektedir. Gerçek bir araç CAN ağında gerçekleştirilmiş saldırılar içermesi, farklı saldırı senaryolarını kapsaması, CAN protokolünün hem hızlı hem de yavaş seri veri yollarının özellikleri test etmesi,

paket ve saldırı konfigürasyonlarının detaylı olması, son olarak kapsamlı bir şekilde normal ve saldırı trafiği örnekleri içermesi bu veri setini özgün kılmıştır. Bu bahsedilen özellikleriyle CICIoV2024, IoV güvenlik çalışmaları için değerli bir kaynak oluşturmaktadır.

2.1.2. CICIoMT2024 Veri Seti

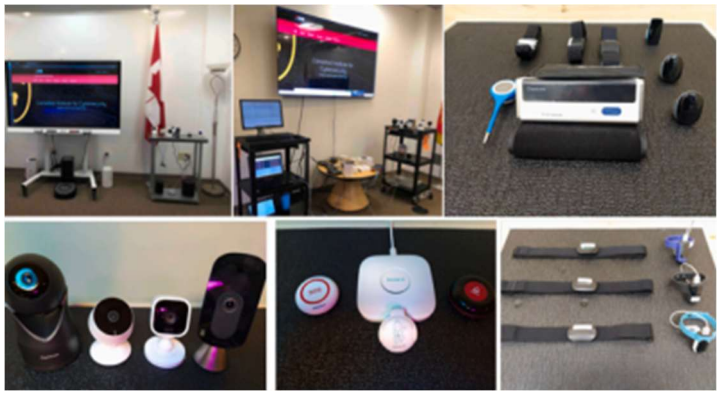
CICIoMT2024 veri seti, IoMT sistemlerinin güvenlik değerlendirmesi için sunulmuş kapsamlı bir karşılaştırma veri setidir. Bu veri setinin temel gayesi, sağlık hizmetlerinde özelleşmiş olarak kullanılan IoT cihazlarının güvenlik açıklarını bulmak ve bu saldırılara karşı savunma sistemleri ve yazılımları geliştirmektir. Veri seti, gerçek IoMT cihazları ve simüle edilmiş cihazlardan oluşan, kapsamlı bir test ortamında toplanan verilerden oluşmaktadır [22].

IoMT sistemlerinde genel olarak 3 temel protokol kullanılmaktadır. Wi-Fi protokolünde TCP/IP tabanlı veri iletimi gerçekleştirilirken, MQTT protokolü ise özelikle IoT cihazları için tasarlanmış, kaynak kullanım düşük yayın/abone yöntemiyle çalışmaktadır. Diğer bir temel protokol olan BLE Düşük Enerjili Bluetooth(BLE(Bluetooth Low Energy)) ise düşük güç tüketimli yakın mesafe iletişimi için kullanılmaktadır. Tablo 2.4. bu protokollerin temel özellerini göstermektedir.

Tablo 2.4. IoMT protokollerinin temel özellikleri[22]

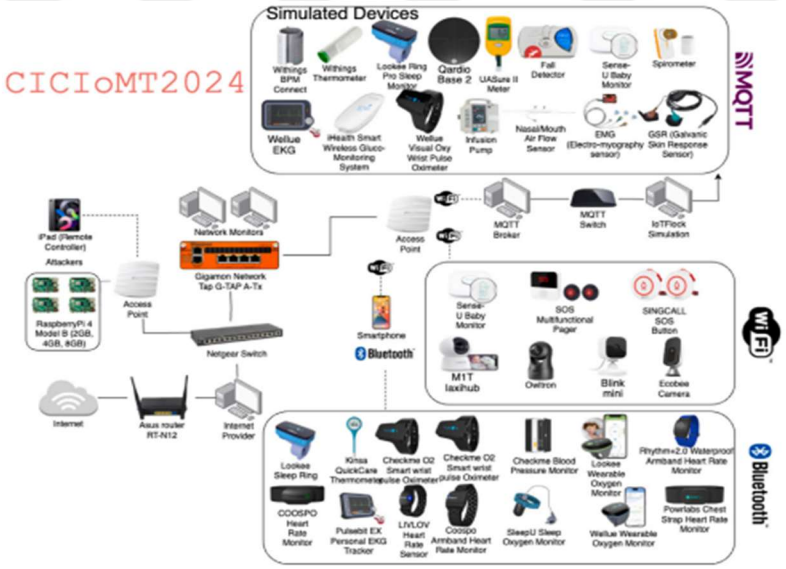
Protokol	İletişim Tipi	Kullanım Alanı	Temel Özellikler
Wi-Fi	Ip Tabanlı ağ iletişimi	Genel ağ bağlantısı	Yüksek bant genişliği, geniş kapsama alanı
MQTT	Yayın/Abone modeli	Sensör veri iletimi	Düşük bant genişliği, hafif protokol yapısı
BLE	Kısa Mesafe Kablosuz	Yakın mesafe sensör verisi	Düşük güç tüketimi, basit paket yapısı

Verilerin toplanması için kurulan test ortamı, CIC laboratuvarında Şekil 2.3'te görüldüğü şekilde kurulmuştur. Laboratuvar ortamı, çeşitli IoMT cihazları, ağ donanımları ve test ekipmanlarıyla donatılmıştır. Test düzeneğinde, ağ trafiğinin düzgün şekilde yakalanabilmesi için özel raflar ve güç bağlantıları kullanılmıştır.



Şekil 2.3. Veri setinin oluşturulması için kullanılan test ortamı. [22]

Test ortamında, 25'i gerçek ve 15'i simüle edilmiş toplamda 40 adet IoMT cihazı kullanılarak veri elde edilmiştir. İletişim ağı topolojisi ile Şekil 2.4'te gösterildiği şekilde yapılandırılmıştır. Topolojide bir iPad marka tablet uzaktan kontrolör olarak kullanılmış ve dört adet Raspberry Pi saldırgan cihaz olarak konumlandırılmıştır. Ağ trafiğinin kayıpsız yakalanması için, Gigabayte Network Tap cihazıyla gerçek zamanlı paket kopyalama sağlanmıştır [22].



Şekil 2.4. CICIoMT2024 Ağ Topolojisi [22]

MQTT protokolünün trafiği için yerel bir broker bağlantısı kurulmuş , IoTFlock simülasyon platformu kullanılmış ve bu platform üzerinde 15 farklı IoMT cihazı simüle edilmiştir. Yapılmış olan Bluetooth deneyleri için özel bir Faraday kalesi kullanarak, dış sinyallerin test senaryosunu ve verisini bozması engellenmiştir.

Veri setinde beş ana kategoride toplam 18 farklı saldırı gerçekleştirilmiştir.

1. DDoS Saldırıları: TCP, İnternet Kontrol Mesaj Protokolü(ICMP(Internet Control Message Protocol)), Senkronizasyon(SYN(Synchronize)) ve UDP flood saldırıları
2. DoS Saldırıları: TCP, ICMP, SYN ve UDP flood saldırıları
3. Keşif Saldırıları: Port tarama, İşletim Sistemi(OS(Operating System)) tarama, Ping sweep ve güvenlik açığı taraması
4. MQTT Saldırıları: Bağlantı flood, Yayın flood ve kötü biçimlendirilmiş veri saldırıları
5. Sahtecilik Saldırıları: Adres Çözümleme Protokolü (ARP(Address Resolution Protocol)) sahteciliği

Toplanan veriler Paket Yakalama(PCAP(Packet Capture)) formatında kaydedilmiş ve sonrasında sunulmak üzere Virgülle Ayrılmış Değerler(CSV(Comma-Separated Values)) formatına dönüştürülmüştür. Dönüştürme işlemi için TCPDUMP [21], Veri Paketi(DPKT(Data Packet)) ve Pandas [21] araçları kullanılmıştır. Veri setinde her örnek için şu özellik grupları çıkarılmıştır. Tüm özellikler Ayrıntılı bir şekilde Tablo 2.5'te gösterilmiştir.

1. Header Length: Transport katmanı başlık uzunluklarının ortalaması
2. Time-To-Live: Paketlerin yaşam süresi
3. Rate: Pencere içindeki paket iletim hızı
4. Protocol Type: Pencerede bulunan protokollerin modu
5. Paket Bayrakları: Bitiş(FIN(Finish)), SYN, Sıfırlama(RST(Reset)), İtme(PSH(Push)), Onay(ACK(Acknowledgment)) vb. bayrakların oranları
6. Protokol İstatistikleri: İnternet Grup Yönetim Protokolü(IGMP(Internet Group Management Protocol)), Güvenli Hiper Metin Transfer Protokolü(HTTPS(Hypertext Transfer Protocol Secure)), HTTP, Alan Adı Sistemi(DNS(Domain Name System)) vb. protokollerin ortalamaları
7. Paket Özellikleri: Toplam uzunluk, minimum, maksimum, ortalama ve standart sapma

Tablo 2.5. CICIoMT2024 veri setindeki sunulan özellikler [21]

Özellik Adı	Açıklama
Header Length	İletişim katmanındaki Header Uzunluklarının Ortalaması
Time-To-Live	Yaşam Süresi
Rate	Bir pencere içindeki paket iletim hızı (paket/s)
fin flag number	Penceredeki FIN bayraklı paketlerin oranı
syn flag number	Penceredeki SYN bayraklı paketlerin oranı
rst flag number	Penceredeki RST bayraklı paketlerin oranı
psh flag number	Penceredeki PSH bayraklı paketlerin oranı
ack flag number	Penceredeki ACK bayraklı paketlerin oranı
ece flag number	Penceredeki ECN-Yankı(ECE(ECN-Echo)) bayraklı paketlerin oranı
cwr flag number	Penceredeki Tıkanıklık Penceresi Azaltıldı(CWR(Congestion Window Reduced)) bayraklı paketlerin oranı
syn count	Paketlerdeki Syn bayrağı oluşum sayısı
ack count	Paketlerdeki Ack bayrağı oluşum sayısı
fin count	Paketlerdeki Fin bayrağı oluşum sayısı
rst count	Paketlerdeki Rst bayrağı oluşum sayısı
IGMP	Penceredeki ortalama IGMP sayısı
HTTPS	Penceredeki ortalama HTTPS sayısı
HTTP	Penceredeki ortalama HTTP paket sayısı
Telnet	Penceredeki ortalama Telnet paket sayısı

DNS	Penceredeki ortalama DNS paket sayısı
SMPT	Penceredeki ortalama Basit Posta Transfer Protokolü(SMTP(Simple Mail Transfer Protocol)) paket sayısı
SSH	Penceredeki ortalama Güvenli Kabuk(SSH(Secure Shell)) paket sayısı
IRC	Penceredeki ortalama İnternet Aktarmalı Sohbet(IRC(Internet Relay Chat)) paket sayısı
TCP	Penceredeki ortalama TCP paket sayısı
UDP	Penceredeki ortalama UDP paket sayısı
DHCP	Penceredeki ortalama Dinamik Ana Bilgisayar Yapılandırma Protokolü(DHCP(Dynamic Host Configuration Protocol)) paket sayısı
ARP	Penceredeki ortalama ARP paket sayısı
ICMP	Penceredeki ortalama ICMP paket sayısı
Ipv	Penceredeki ortalama İnternet Protokolü versiyonu(Ipv(Internet Protocol version)) paket sayısı
LLC	Penceredeki ortalama Mantıksal Bağlantı Kontrolü(LLC(Logical Link Control)) paket sayısı
Tot Sum	Penceredeki toplanan paketlerin toplam(TOT(total)) uzunluğu
Min	Toplanan paketler arasındaki minimum(MIN(Minimum)) paket uzunluğu (pencere)
Max	Toplanan paketler arasındaki maksimum(MAX(Maximum)) paket uzunluğu (pencere)
AVG	Toplanan paketlerdeki paket uzunluğunun ortalama(AVG(Avarage)) (pencere)
Std	Toplanan paketlerdeki paket uzunluğunun standart sapma(STD(Standard Deviation))'si (pencere)

Tot Size	Paketin ortalama uzunluğu
IAT	Penceredeki Varışlar Arası Süre(IAT(Inter-Arrival Time)) mevcut ve önceki paket arasındaki ortalama aralık
Number	Penceredeki toplam paket sayısı
Variance	Penceredeki paket uzunluklarının varyansı
Protocol Type	Pencerede bulunan protokollerin tipi

Test ortamında, ayrıca cihazların farklı durumlardaki davranışlarını anlamak için güç açma/kapama, boşta çalışma ve aktif kullanım durumları gibi farklı senaryolarda test edilmiştir. Bu sayede IoMT cihazlarının normal yaşam döngüleri boyunca oluşturdukları normal yani tehlikesiz trafik örnekleri de veri setine dahil edilmiştir. Bu eklenen veriyle birlikte oluşan veri setinin örnek sayısı dağılımı Tablo 2.6. da gösterilmektedir.

Tablo 2.6. CICIoMT2024 veri setindeki saldırı türleri ve örnek sayıları [28]

Etiket	**Kategori**	**Sınıf**	**Örnek Sayısı**
Normal Trafik	-	-	230.339
	Sahtecilik	ARP Sahteciliği	17.791
	Keşif Saldırıları	Ping Sweep	926
		Güvenlik Açığı Taraması	3207
		OS Tarama	20.666
		Port Tarama	106.603
	MQTT Saldırıları	Bozulmuş Veri	6.877
		DoS Bağlantı Seli	15.904
		DDoS Yayın Seli	36.039

Saldırı Trafiği		DoS Yayın Flood	52.881
		DoS Yayın Flood	241.952
	DoS Saldırıları	DoS TCP Protokolü	462.480
		DoS ICMP Protokolü	514.724
		DoS SYN Protokolü	540.498
		DoS UDP Protokolü	704.503
	DdoS Saldırıları	DDoS SYN Protokolü	947.359
		DDoS TCP Protokolü	987.063
		DDoS ICMP Protokolü	1.887.175
		DDoS UDP Protokolü	1.998.026

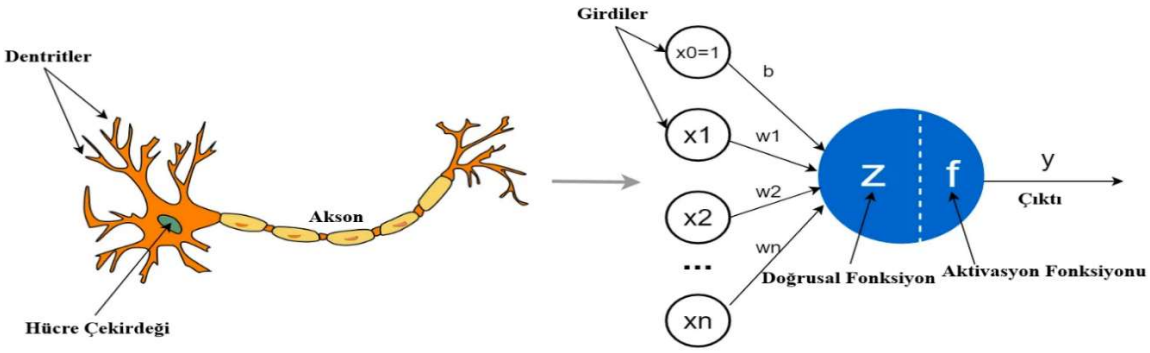
CICIoMT2024 veri seti, literatürde bulunan diğer IoMT güvenliği veri setlerinden önemli farklılıklar göstermektedir. Gerçek ve simüle edilmiş cihazların hibrit şekilde kullanımı, Wi-Fi, MQTT ve Bluetooth gibi çoklu protokollerin desteklenmesi, çeşitli ve detaylı saldırı senaryolarının uygulanması bu veri setini özgün kılmıştır. Ayrıca cihazların profilleme verilerinin de dahil edilmesi ve yüksek kaliteli ve performanslı veri kaydetme altyapısının kullanılması, veri setinin kalitesini arttıran diğer öne çıkan özelliklerin başında gelmektedir. Bu özellikleriyle CICIoMT2024 literatüre, IoMT sistemlerinin güvenlik değerlendirmesi ve makine öğrenmesi tabanlı saldırı tespit sistemlerinin geliştirilmesi için değerli bir kaynak oluşturmaktadır.

2.2. Derin Öğrenme

Derin öğrenme, yapay sinir ağlarının birden fazla katmandan oluşan hiyerarşik yapıları temel alan, verilerdeki soyut ve karmaşık örüntüleri tanıyıp öğrenmesini sağlayan, bir makine öğrenmesi alt dalıdır [131]. Klasik makine öğrenmesi tekniklerinden farklı olarak, derin öğrenme modelleri, işlenmemiş veriden kabul edilebilir anlamlar çıkarabilir ve özellik mühendisliğine olan ihtiyacı azaltır. Derin öğrenme, bilgisayarla görme, doğal dil işleme, seslerin tanınması ve zaman serisi incelenmesi gibi birçok farklı alanda, önemli derecede isabetli sonuçlar elde etmiştir [132].

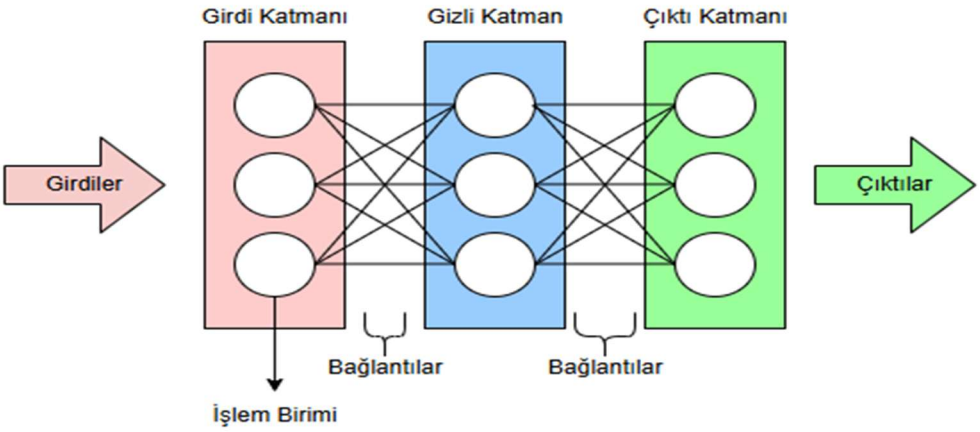
2.2.1 Yapay Sinir Ağları

Derin öğrenme mimarisinin temelini oluşturan Yapay Sinir Ağları(YSA(Artificial Neural Networks)), Şekil 2.5' te görüldüğü üzere insan beyninin bilgiyi işlemesinden ilham alan, derin öğrenmenin en küçük yapı taşıdır. YSA'lar birbiriyle ilişkili birçok işlem biriminin paralel ve dağıtık çalışmasıyla karmaşık işlevleri, tıpkı canlıların vücudunda bulunan biyolojik sinir ağlarındaki gibi gerçekleştirebilirler [133]



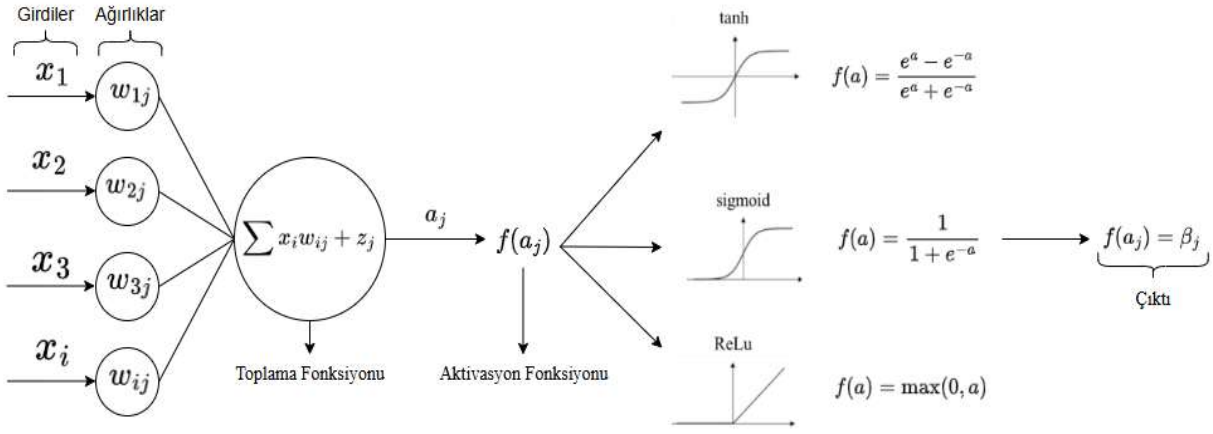
Şekil 2.5. Biyolojik Sinir Hücresi ve Yapay Sinir Hücresi [133]

Yapay sinir ağları Şekil 2.6'da görüldüğü şekilde, girdi katmanı, gizli katmanlar ve çıktı katmanından oluşan çok katmanlı bir mimariye sahiptir. Girdi katmanının görevi, dış dünyadan gelen veriyi almak ve gizli katmanlara iletmektir. Çıktı katmanı ise, sinir ağının son kararını yani çıktısını verir ve bir sınıflandırma veya regresyon sonucu üretir [134].



Şekil 2.6. Bir yapay sinir ağının genel yapısı [134]

Yapay sinir ağlarında veri işleme süreci şu şekilde gerçekleşir: İlk olarak, ham veriler sistemin giriş noktası olan giriş katmanına beslenir. Bu giriş verileri, ağın temel işlem birimleri aracılığıyla bir sonraki aşama olan gizli katmana aktarılır. Gizli katmanda, veriler çeşitli matematiksel işlemlerden geçerek işlenir. Son olarak, gizli katmanda işlenmiş olan bu bilgiler çıkış katmanına ulaşır ve burada nihai sonuçlar oluşturulur. Bu süreç, tıpkı bir fabrikanın üretim hattı gibi, verilerin adım adım işlenmesini ve dönüştürülmesini sağlar [134].



Şekil 2.7. Bir yapay nöronun yapısı ve matematiksel gösterimi [134]

Şekil 2.7.'de görüldüğü üzere, oklar üzerinde bulunan ve bilginin nasıl aktığını gösteren sayısal değerlere girdi adı verilir. Her yapay nöronda, bu girdilerin hücre üzerindeki etkisi ve önemi, w sembolüyle gösterilen ağırlıklar tarafından kontrol edilir. Bir ağırlığın değeri ne kadar büyükse, o girdinin sistem üzerindeki etkisi de o kadar güçlü olur. Giriş katmanındaki nöronlar sadece tek bir girdi alabildiğinden, bu nöronların çıktısı aldıkları girdinin belirli bir ağırlıkla çarpılmasıyla elde edilir. Tüm girdiler ilgili ağırlıklarla çarpıldıktan sonra, her katmanda bulunan bias (önyargı) değerleri (z) bu toplama eklenir ve toplama fonksiyonu kullanılarak α sembolü ile gösterilen net girdi değeri hesaplanır. Elde edilen bu net girdi değeri, daha sonra nöronun karakteristik özelliği olan aktivasyon fonksiyonundan geçirilir. Sonuç olarak, çıktı değeri β sembolüyle gösterilmiştir. Yapay sinir ağının gizli katmanlarındaki her bir düğümün matematiksel ifadesi, g_i fonksiyonu olarak adlandırılır ve bu fonksiyon, f aktivasyon fonksiyonu kullanılarak aşağıdaki biçimde tanımlanmıştır [135]. g_i fonksiyonu formül 2.1'de ifade edilmiştir.

$$gi(x) = f\,(xTw + z) \tag{2.1}$$

Yapay nöronların ağırlıkları uygun şekilde düzenlendiğinde, belirli girdiler için hedeflenen çıktılar elde edilebilir. Ancak, bir yapay sinir ağı yüzlerce veya binlerce nörondan oluştuğunda, bu ağırlıkların manuel olarak belirlenmesi son derece karmaşık ve zor bir hal alır. Bu zorluğun üstesinden gelmek için, özel algoritmalar kullanılarak ağın ağırlıkları otomatik olarak ayarlanabilir. Bu otomatik ağırlık ayarlama işlemine eğitim veya öğrenme süreci adı verilir. Bu süreç rastgele seçilen ağırlıklarla başlar ve temel amacı, ağın hata oranını minimum seviyeye indirecek şekilde ağırlıkları optimize etmektir [136].

2.2.2 İleri Besleme

İleri besleme mekanizmalı sinir ağları, yapay sinir ağlarının en basit şekillerinden biridir. Bu tür bir ağda bilgi, girdi katmanından, çıktı katmanına doğru tek yönlü akarak ilerler. Her bir nöron, kendinden sonra gelen katmandaki tüm nöronlara bağlı durumdadır. Bu bağlantıların her birinde bir ağırlık değeri bulunmaktadır. Nöronlar, bağlantı üzerinden kendilerine gelen bu toplamı bir aktivasyon fonksiyonundan geçirerek kendi çıkışlarını oluşturmaktadır. İstenen çıktı üretilecek hale gelene kadar bu işlem aşama aşama devam eder ve ağ boyunca ilerler [131].

2.2.3 Kayıp Fonksiyonu

Yapay sinir ağlarında kayıp fonksiyonu, modelin yaptığı tahminlerin gerçek değerlerden ne kadar uzaklaştığını belirleyen matematiksel bir ölçüm aracıdır. Bu fonksiyon, ağın ürettiği sonuçların beklenen değerlerden sapmasını rakamsal olarak değerlendirir. Modelin eğitim sürecinde asıl hedef, bu sapma değerini en aza indirgemektir. Geriye yayılım algoritması, kayıp fonksiyonundan elde edilen bilgileri kullanarak ağın ağırlıklarını ve bias değerlerini yeniler. Problemin türüne göre farklı kayıp fonksiyonları tercih edilir; sınıflandırma görevlerinde çapraz entropi kaybı öne çıkarken, regresyon problemlerinde ortalama kare hata tekniği yaygın olarak kullanılır. Her tekrarda kayıp değeri yeniden hesaplanır ve buna göre model parametreleri ince ayara tabi tutulur, böylece ağın öğrenme kapasitesi sürekli olarak geliştirilir [137].

2.2.4 Geriye Yayılım Algoritması

Yapay sinir ağlarının eğitiminde kilit rol oynayan geriye yayılım algoritması, temel bir optimizasyon yaklaşımı sunar. Bu algoritma, çıktı katmanında tespit edilen hata değerini, giriş katmanına doğru sistematik bir şekilde yayar. Matematiksel olarak zincir kuralını temel alan bu süreçte, her bir nöronun nihai çıktıya katkısı değerlendirilir ve bu bilgi ışığında ağırlıkların

güncelleme stratejisi şekillenir. Algoritma, gradyan iniş yöntemiyle entegre çalışarak, her tekrarda ağın ağırlık ve bias değerlerini hassas bir şekilde ayarlar. Önceden belirlenen öğrenme oranı doğrultusunda, hata değerini en aza indirecek şekilde parametreler yenilenir ve böylece ağın öğrenme süreci kontrollü bir şekilde ilerler. Bu mekanizma sayesinde model, eğitim verilerini daha iyi yorumlayarak tahmin performansını sürekli olarak geliştirir [138].

2.2.5 Aktivasyon Fonksiyonları

Yapay sinir ağlarının temel yapı taşlarından olan aktivasyon fonksiyonları, nöronlara doğrusal olmayan özellikler kazandıran matematiksel işlemlerdir. Bu fonksiyonlar, nöronlara gelen ağırlıklı girdileri özel aralıklara dönüştürüp işler. En yaygın kullanılan aktivasyon fonksiyonlarından Doğrultulmuş Doğrusal Birim(ReLU(Rectified Linear Unit)), negatif girdileri eleyip sıfıra dönüştürürken pozitif değerleri değiştirmeden iletir; sigmoid fonksiyonu tüm çıktıları 0-1 aralığında normalize ederken, tanh fonksiyonu değerleri -1 ile +1 arasında ölçeklendirir. Bu matematiksel dönüşümler sayesinde, ağ karmaşık ve doğrusal olmayan yapıları başarıyla modelleyebilmektedir. Aktivasyon fonksiyonun seçilmesi, ağın öğrenme kapasitesini ve genel başarısını büyük ölçüde belirlemektedir. Bu fonksiyonlar aynı zamanda, gradyanların ağ içindeki akışını düzenleyerek derin yapıların eğitimini mümkün kılar ve gradyan kaybı/patlaması gibi problemleri engeller [139].

2.2.6 Mini-batch Boyutu

Mini-batch boyutu yapay sinir ağlarının eğitim sürecinde belirleyici rol oynayan temel hiper parametrelerden biridir. Bu değişken, her bir eğitim adımında ağın işleme alacağı veri örneği miktarını tanımlayarak sistemin başarımını etkiler. Düşük batch boyutları seçildiğinde, model ağırlıklarının güncellenmesi daha sık gerçekleşir ve lokal minimumlarda takılma olasılığı düşer; ancak bu durum, dalgalı ve parazitli gradyanların ortaya çıkmasına yol açabilir. Buna karşılık, yüksek batch boyutları dengeli gradyanlar üreterek eşzamanlı hesaplamaları mümkün kılar, lakin hafıza tüketimini yükseltir ve modelin genelleştirme yetisini zayıflatabilir. En verimli mini-batch boyutunun seçimi, mevcut bilgisayar kapasitesi, veri kümesinin hacmi ve ele alınan problemin zorluğu gibi etkenlere göre şekillenir. Bu sebepten ötürü, eğitim aşamasında optimum mini-batch boyutunun test edilerek belirlenmesi kritik bir adımdır [140].

2.2.7 Optimizasyon Algoritmaları

Yapay sinir ağlarının eğitiminde kayıp fonksiyonunu minimize etmeyi hedefleyen optimizasyon algoritmaları, öğrenme sürecinin temel bileşenlerini oluşturur. En temel yaklaşımlardan biri olan SGD (Stokastik Gradyan İnişi), gradyanın ters yönünde değişmeyen bir öğrenme hızıyla hareket eder. Fakat modern uygulamalarda, daha karmaşık ve ileri düzey algoritmalara yönelim artmaktadır. Değişim bazlı teknikler, önceki gradyanları göz önünde bulundurarak lokal minimumlardan sıyrılma becerisini yükseltir. Her bir değişken için özelleştirilmiş öğrenme oranları kullanan Uyarlanabilir Moment Tahmini(Adam(Adaptive Moment Estimation)) algoritması, hızlı yakınsama özelliğiyle dikkat çeker ve yaygın kullanım alanı bulur. Adam'ın bir türevi olan AdaMax, L∞ normunu kullanarak daha dengeli parametre güncellemeleri gerçekleştirir. RMSprop algoritması ise gradyan karelerinin kayar ortalamasını baz alarak öğrenme oranını sürekli olarak günceller. Bu çeşitli optimizasyon yaklaşımları, farklı problem tiplerine göre kendine özgü üstünlükler sağlayarak eğitim prosedürünü belirgin şekilde etkilemektedir [141].

2.2.8 Epoch Zamanı

Yapay sinir ağlarının eğitiminde epoch, veri setindeki tüm örneklerin modele tek seferde gösterildiği öğrenme döngüsünü tanımlar. Her epoch döneminde, eğitim örnekleri mini-batch adı verilen parçalara ayrılarak işleme alınır ve bu süreçte ağın parametreleri yenilenir. Eğitim için gerekli epoch miktarının doğru tespiti, modelin öğrenme yeteneğini ciddi şekilde etkiler; düşük sayıda epoch kullanıldığında model yeterince öğrenememe (underfitting) problemiyle karşılaşabilirken, aşırı sayıda epoch kullanımı ezberleme (overfitting) problemine yol açabilir. Bu durumda, doğrulama hata oranının izlenmesi ve erken sonlandırma (early stopping) gibi tekniklerle en uygun epoch sayısı tespit edilir. İhtiyaç duyulan epoch miktarı, eğitim verilerinin hacmi, ağın yapısal karmaşıklığı ve kullanılabilir bilgi işlem gücü gibi değişkenlere bağlı olarak şekillenir. Bunun yanı sıra, her epoch tamamlandığında modelin başarımı ölçülerek eğitimin sürdürülüp sürdürülmeyeceği belirlenir [142].

2.3 Derin Öğrenme Modelleri Performans Metrikleri

Derin öğrenme modellerinin başarı seviyesini ölçmek ve oluşturulan modeli test etmek, eğitilen modellerin işlevselliğinin ve gerçek hayattaki kullanılabilirliğini görmek için gerekli bir aşamadır. Bir derin öğrenme modelinin, ne kadar etkili olduğunu belirlemek için farklı değerlendirme yöntemleri kullanılır. Bu kullanılan yöntemler, eğitilen modelin tahminlerin tutarlılığını,

güvenilirliğini ve başarısını farklı açılardan incelememizi sağlamaktadır. Doğru değerlendirme yöntemlerinin seçimi ve yorumlanması, model geliştirme sürecindeki aşamaları yönlendirmede ve modelin gerçek uygulamalardaki başarısını belirlemede kritik rol oynar [137].

2.3.1 Karmaşıklık Matrisi

Sınıflandırma modellerinin başarı ölçümünde kullanılan karmaşıklık matrisi, modelin tahmin kabiliyetini dikkatli bir şekilde gözlemleme ve değerlendirme imkanı veren çok yönlü bir ölçme yöntemidir. Bu değerlendirme yöntemi, gerçek sonuçlar ile tahmin edilen sonuçların örnek sayısını karşılaştırarak oluşabilecek dört farklı durumu gösterir. Olumlu tahminlerin doğruluğu Doğru Pozitif(TP(True Positive)), olumsuz tahminlerin doğruluğu Doğru Negatif(TN(True Negative)), yanlış olumlu sonuçlar Yanlış Pozitif(FP(False Positive)) ve yanlış olumsuz sonuçlar Yanlış Negatif(FN(False Negative)) bu durumları oluşturmaktadır. Özellikle ikili sınıflandırma problemi için 2x2 boyutunda bir tablo formatında sunulan bu yapı, modelin her sınıf için gösterdiği başarı ve başarısızlık durumunu açıkça ifade etmektedir. Karmaşıklık matrisi, doğruluk, kesinlik ve duyarlılık gibi başka önemli performans metriklerinin hesaplanmasında önemli rol oynar [143].

Tablo 2.7. Karmaşıklık Matrisi [143].

	Pozitif Tahmin	**Negatif Tahmin**
Gerçek Pozitif	TP	FN
Gerçek Negatif	FP	TN

2.3.2 Doğruluk Performans Metriği

Doğruluk performans metriği, derin öğrenme modellerinin başarı değerlendirmesinde kullanılan en temel ölçütlerden bir tanesidir. Bu değer, bir modelin toplam tahminlerindeki, doğru tahminlerin oranını gösterir ve (2.2)'deki formül ile hesaplanır. Doğruluk ölçümü, özellikle eşit sınıf sayısına sahip dengeli veri setlerinde modelin genel başarısı hakkında hızlı ve anlaşılır bir fikir vermektedir. Dengesiz veri setlerinde yanıltıcı sonuçlar verebilir. Örnek olarak, bir hastalık tespiti yapan derin öğrenme modelinde 1000 örnekten sadece 10 hasta örneği varsa, model hiç

hastalık teşhisi koymasa bile %99 doğruluk oranı gösterebilir. Bu sebeple, doğruluk performans metriği tek başına değil, diğer performans metrikleriyle beraber değerlendirilmelidir [131]. Doğruluk performans metriği, formül 2.2 ile ifade edilmiştir.

$$\text{Doğruluk} = \frac{TP + TN}{TP + TN + FP + FN} \tag{2.2}$$

2.3.3 Kesinlik Performans Metriği

Kesinlik performans metriği, bir sınıflandırma modelinin pozitif tahmin ettiği sınıf örnekleri arasından, gerçekten pozitif olanların oranını hesaplayan önemli performans metriklerinden bir tanesidir. Matematiksel olarak (2.3)'teki formül ile hesaplanmaktadır. Bu metrik, modelin pozitif sınıf tahminlerindeki güvenilirliğini ölçer. Özellik FP, önemli sonuçlar çıkarabileceği durumlarda büyük önem taşır. Örneğin, bir eposta istenmeyen mail filtreleme sisteminde normal bir epostanın yanlışlıkla, istenmeyen bir mail olarak gösterilmesi, ciddi iletişim problemlerine yol açabilmektedir. Bu sebeple, kesinlik metriği, özellikle yanlış pozitiflerin maliyetinin yüksek olduğu sistemlerdeki modellerin performansını analiz etmede önemli rol oynamaktadır [144]. Kesinlik performans metriği, formül 2.3 ile ifade edilmiştir.

$$\text{Kes}\mathit{in}\text{lik} = \frac{TP}{TP + FP} \tag{2.3}$$

2.3.4 Duyarlılık Performans Metriği

Duyarlılık performans metriği, bir sınıflandırma modelinin, gerçekte pozitif olan örnekleri doğru saptama yeteneğini ölçen temel bir performans metriğidir. (2.4)'teki formül ile hesaplanmaktadır. Bu metrik, modelin pozitif sınıfa ait örnek sınıflarını tespit etme başarısını göstermektedir. Yanlış negatiflerin (FN) tespitinin, kritik sonuçlar doğurabileceği durumlarda kritik öneme sahiptir. Örnek olarak, bir işletmedeki üretim bandındaki kusurlu ürünlerin gözden kaçırılması gibi önemli sorunlara neden olabilir. Bundan dolayı, duyarlılık metriği, özellikle pozitif sınıf örneğinin bulunmasının çok kritik olduğu ve gözden kaçırılmaması gereken sistemlerde modelin etkinliğinin ölçülmesinde önemli rol oynamaktadır [145]. Duyarlılık performans metriği, formül 2.4 ile ifade edilmiştir.

$$\text{Duyarlılık} = \frac{TP}{TP + FN} \tag{2.4}$$

2.3.5 F1-skoru Performans Metriği

F1-skoru performans metriği, duyarlılık ve kesinlik metriklerinin harmonik ortalamasın alıp bu önemli iki metriği, tek bir değerde birleştiren dengeli bir performans ölçütüdür. (2.5)'teki formül ile hesaplanmaktadır. Bu metrik, bir sınıflandırma modelinin başarısını daha kapsamlı şekilde değerlendirmektedir. Özel olarak, dengesiz veri setlerinde tek başına doğruluk değerinin yanıltıcı olabileceği durumlarda kullanışlıdır. Bu bağlamda, bir sosyal medya platformundaki zararlı içerik tespit edici bir sistemde, hem zararlı içeriklerin tespitini kaçırmamak (yüksek duyarlılık), hem de normal içerikleri yanlışlıkla zararlı olarak engellemekten kaçınmak (yüksek kesinlik) önemlidir. Özetle, F1-skoru, bu iki önemli metrik arasında bir hesaplama yapıp modelin genel başarısını bir değerle ifade etmeyi sağlamaktadır [146]. F1-Skoru performans metriği, formül 2.5 ile ifade edilmiştir.

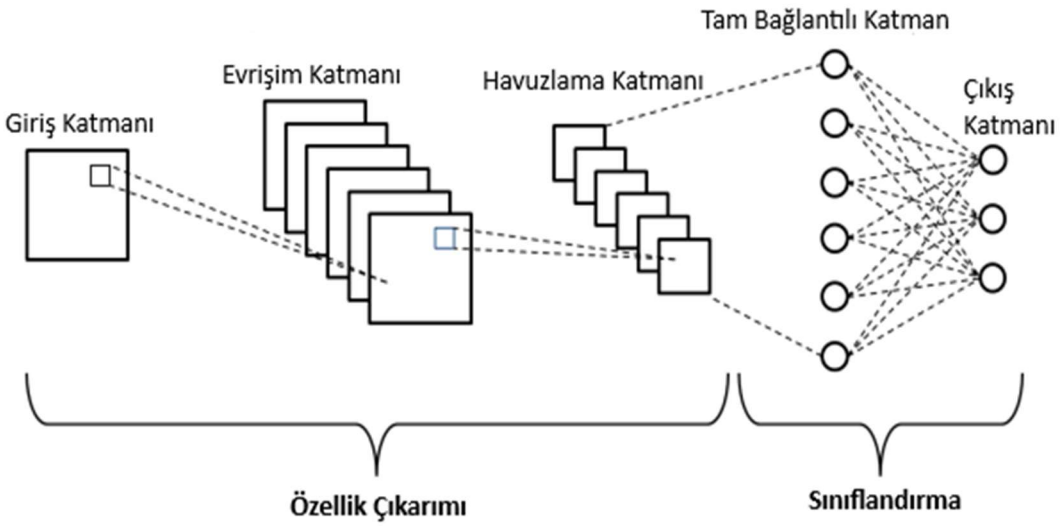
$$\text{F1} - \text{Skoru} = 2 * \frac{Kesinlik * Duyarlılık}{Kesinlik + Duyarlılık} \tag{2.5}$$

2.4. Tez Çalışmasında Kullanılan Derin Öğrenme Mimarileri

Bu tez çalışmasındaki deneylerde, en popüler derin öğrenme mimarilerinden olan, CNN, DNN, LSTM kullanılmıştır.

2.4.1 Evrişimli Sinir Ağları (CNN) Mimarisi

Evrişimli sinir ağları, özellikle görüntü işlem ve analizi alanında, yüksek başarılar sağlamış, derin öğrenme mimarilerinden biridir [131]. CNN'ler, insanın görme yapısından ilham alınarak oluşturulmuştur. CNN mimarisinin, görsel verilerdeki konumsal ilişkileri otomatik olarak öğrenme yeteneği bulunmaktadır. Bu mimari, klasik yapay sinir ağlarından ayrışarak, görüntülerdeki lokal özellikleri bulabilen özel katmanlar içermektedir [147].



Şekil 2.8. CNN Mimarisi [148]

CNN mimarisinin temel yapısı Şekil 2.8'de görüldüğü üzere, evrişim katmanları, havuzlama katmanları ve tam bağlantılı katmanlardan oluşmaktadır. Evrişim katmanları, görüntü üzerinde filtreleri aşama aşama kaydırarak, görüntüdeki önemli özellikleri tespit edebilmektedir. Bu kullanılan filtreler, dokular, kenarlar, şekiller gibi diğer özelliklerden daha düşük seviyedeki özelliklerden başlayarak, ağın daha derin katmanlarında nesne veya insan yüzü gibi daha yüksek seviyedeki özellikleri öğrenebilmektedir [149].

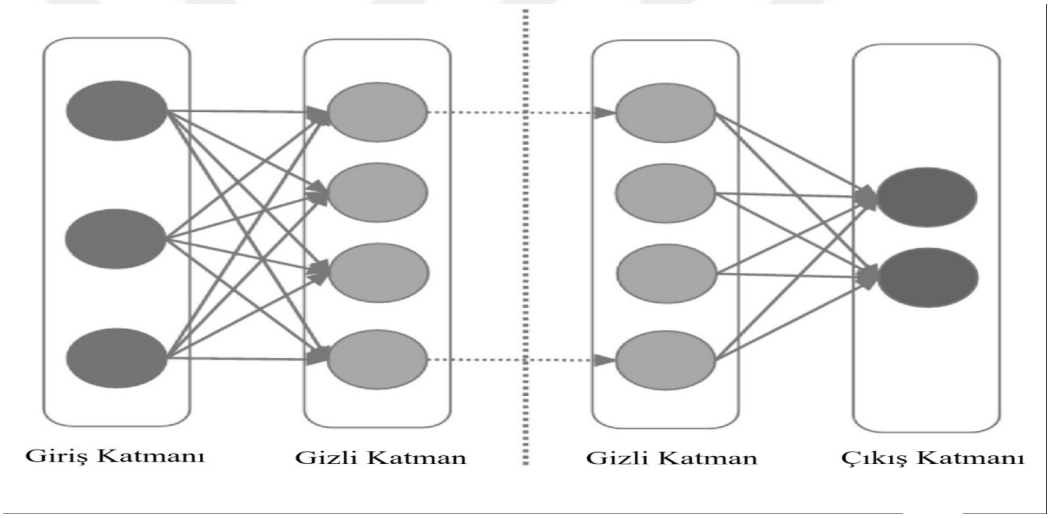
Son olarak tam bağlantılı kavramlar, CNN mimarisinin son kademesinde yer almakta olup, kendinden önceki katmanlardan çıkarılan özellikleri kullanıp sınıflandırma işlemini gerçekleştirmektedir [150]. Bu tam bağlantılı katmanlar, evrişim ve havuzlama katmanlarından çıkarılan özellikleri harmanlayarak, kesin tahminleri ortaya koymaktadır. Ek olarak, CNN mimarilerinde, modelin yanlış sonuçlar vermesine sebep olabilen aşırı öğrenmesini engellemek için dropout ve batch normalization gibi düzenleme teknikleri de kullanılmaktadır.

Günümüzde CNN modelleri, sadece görüntü sınıflandırma alanında değil, obje tespiti, semantik segmentasyon, yüz tanıma ve medikal görüntü analizi gibi birçok alanda başarıyla uygulanmaktadır [131]. AlexNet [147] ve GoogLeNet [151] gibi ünlü CNN mimarileri, görüntü işleme alanında son derece başarılı sonuçlar elde etmiş ve derin öğrenme alanının ilerlemesinde önemli katkılar sağlamıştır.

2.4.2 Derin Sinir Ağları (DNN) Mimarisi

Derin Sinir Ağları mimarisi, yapay sinir ağlarının çok katmanlı ve karmaşık bir formu olup, günümüzdeki yapay zeka uygulamalarının temelini oluşturan önemli bir bileşendir [137]. DNN modelleri, birden çok gizli katman içerir ve her katmanda çok sayıda sinir ağı birbirine bağlı durumdadır. Bu mimari, insan beynin biyolojik sinir ağlarından ilham alınarak geliştirilmiştir ve karmaşık örüntüleri tespit etme ve öğrenme kabiliyetine sahiptir.

DNN'ler, birden fazla gizli katman içeren ve her katmanda çok sayıda nöronun birbirine bağlı olduğu yapılardır. Bu mimari, beynin nöral ağlarından esinlenilerek geliştirilmiş olup, karmaşık örüntüleri öğrenme ve temsil etme yeteneğine sahiptir [132].



Şekil 2.9. DNN Mimarisi [152]

DNN mimarisi temelde, Şekil 2.9'da görüldüğü üzere, bir giriş katmanı, bir çıkış katmanı ve çok fazla sayıda gizli katmandan oluşur. Her bir katmandaki nöronlar, bir aktivasyon fonksiyonuyla elde ettiği sonucu diğer katmana iletir. Gizli katmanlarda veri ilerledikçe, daha soyut ve yüksek seviyede özellikleri çıkarmaya başlar [131]. Örnek olarak bir ses tanıma uygulamasını ele aldığımızda, ilk katmanlar en başta basit ses desenlerini algılayabilirken, katmanlar derinleştikçe model kelimeleri ve cümleleri öğrenmeye başlayabilir. Günümüzde modern DNN mimarileri ReLu, sigmoid ve tanh gibi çeşitli aktivasyon fonksiyonları kullanmaktadır. Bu sayede gradyan kaybı problemi minimize edilmektedir [140].

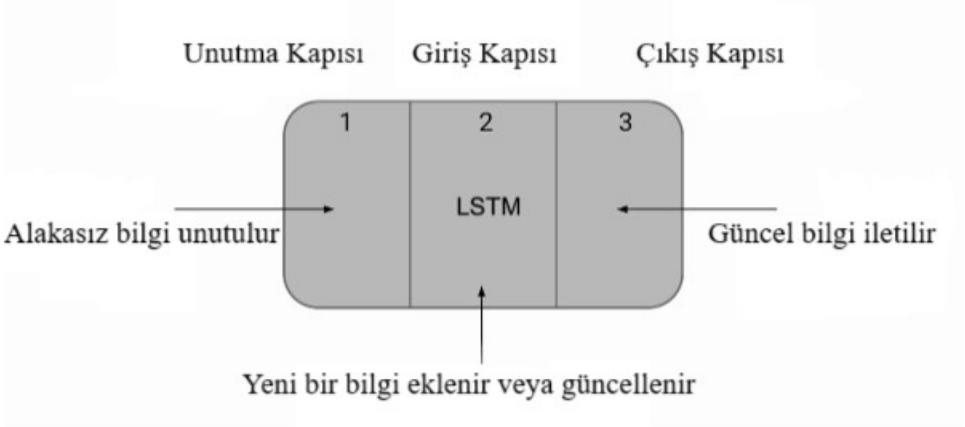
DNN modelinin eğitim süresince, hesaplanan ağırlıkların optimizasyonları için geri yayılım algoritmasının yanında, çeşitli optimizasyon teknikleri kullanılmaktadır. Bu tekniklerden biri olan

gradyan inişi, eğitim süreci boyunca ağın parametrelerini güncelleme de bulunarak modeli optimize eder [138]. Benzer şekilde, modelin eğitim sürecindeki aşırı öğrenmeyi en aza indirmek için, dropout, Katman 1/Katman 2(L1/L2(Layer 1/Layer 2)) optimizasyonu ve erken durdurma gibi teknikler uygulanabilir. Bunun yanında batch normalization gibi işlemler, eğitim sürecini hızlandırabilir ve modelin sınıflandırma yeteneğini arttırmak için kullanılabilir [153].

Günümüzde DNN mimarisi, ses tanıma, doğal dil işleme, finansal fiyat tahmini gibi birçok sektörde başarıyla uygulanmaktadır. Gelişmiş donanım seçenekleri ve gün geçtikçe büyüyen veri setleri sayesinde derin öğrenme modelleri giderek daha karmaşık problemlerde daha başarılı sonuçlar vermeye başlamıştır. Aynı şekilde farklı problem türlerine göre kendi içinde özelleşen farklı DNN modelleri de bulunmaktadır [137].

2.4.3 Uzun-Kısa Süreli Bellek (LSTM) Mimarisi

Uzun-Kısa Süreli Bellek mimarisi, sıralı veri işleme ve zaman serisi verisi analizinde ön plana çıkmakta olan özel bir tekrarlayan sinir ağı (RNN) türüdür [154]. LSTM mimarisi, standart RNN mimarisinin uzun süreli bilgileri öğrenmede yaşadığı kaybolan gradyan problemine çözüm olarak geliştirilmiştir. LSTM mimarisi, içindeki özel kapı mekanizması aracılığıyla, uzun süreli bilgiyi seçici bir şekilde unutma ve hatırlama becerisine sahiptir [155].



Şekil 2.10. LSTM Hücresi Mimarisi [154]

LSTM mimarisi temelinde, Şekil 2.10'da görüldüğü üzere unutma kapısı, giriş kapısı ve çıkış kapısı olarak üç ana kapı mekanizmasından oluşur. Hücrede hangi bilgilerin unutulacağına, unutma kapısı karar vermektedir. Yeni gelen bilgilerin hücre durumuna eklenmesini, giriş kapısı

belirlemektedir. Hücre durumundan, hangi kısımların çıktı olacağını ise çıkış kapısı kontrol etmektedir. Bahsedilen bu mekanizmalar, sigmoid ve tanh aktivasyon fonksiyonlarıyla her bir zaman adımında güncellenmektedir [156].

Hücre durumu adı verilen özel bileşen, LSTM hücresinin bellek yönetiminden sorumludur. Hücre durumu kendine aktarılan bir bilgiyi uzun süre saklayabilir ve bu bilgi kapı mekanizmaları tarafından kontrol edilir [157]. Kurulan bu yapı sayesinde, LSTM modelleri uzun vadeli bağımlılıkları öğrenip sıradaki verilerdeki uzak ilişkileri tespit edebilir. Ayrıca, gözetleme deliği optimizasyonu gibi ek bağlantılar ile modelin performansı daha da artırılabilir [158].

LSTM mimarisi günümüzde doğal dil işleme, ses tanıma, makine çevirisi, müzik oluşturma ve finansal tahmin gibi birçok alanda sıkça kullanılmaktadır. Özellikle metin üretimi, duygu analizi ve dil modelleme gibi sektörlerde iyi sonuçlar göstermektedir [159]. Bidirectional LSTM ve Stacked LSTM gibi çeşitleri, farklı problem türlerine özgü çözümler sunmaktadır [160].

2.5. Deney Ortamı

Bu tez çalışmasında yapılan tüm deneyler, Windows 11 işletim sistemi [161] yüklü masaüstü bilgisayarda gerçekleştirilmiştir. Bahsedilen bilgisayar, işlemci olarak AMD Ryzen 5 5500 3.60 GHz modelini kullanmaktadır. Ekran kartı olarak NVIDIA GeForce GTX 1650 SUPER (4 GB) kullanan bilgisayarın Rastgele Erişimli Bellek(RAM(Random Access Memory)) boyutu 32 GB'dir.

Yapılan deneylerde Python programlama dili ve çeşitli derin öğrenme kütüphaneleri kullanılmıştır. Bu kütüphaneler aşağıdaki şekildedir.

1. Tensorflow [162]: Derin öğrenme modellerinin oluşturulması, eğitilmesi ve dağıtılması için geliştirilmiş açık kaynaklı bir kütüphanedir.
2. Keras [163]: Tensorflow üzerinden geliştirilmiş, derin öğrenme modellerini hızlı bir şekilde prototiplemek ve geliştirmek için kullanılan üst düzey bir sinir ağları kütüphanesidir.
3. Pandas [164]: Verilerin analizi ve işlenmesi için yüksek performanslı ve kullanımı kolay veri yapıları sağlayan bir Python kütüphanesidir.
4. Numpy [165]: Büyük ve çok boyutlu diziler ve matrislerle işlem yapabilmeye olanak tanıyan bir Python kütüphanesidir.

5. Scikit-learn [166]: Makine öğrenimi için kullanılan açık kaynaklı bir Python kütüphanesidir. Sınıflandırma, regresyon ve kümeleme gibi çeşitli algoritmaları içinde barındırmaktadır.
6. Matplotlib [167]: Görselleştirme ve grafik oluşturma için kullanılan Python tabanlı bir çizim kütüphanesidir.
7. Seaborn [168]: Matplotlib tabanlı bir görselleştirme kütüphanesidir. İstatiksel grafikler oluşturmak için yüksek düzeyli bir programlama arayüzü sağlar.

Yukarıda açıklanan kütüphaneler ve bağımlılıklar, Anaconda [169] dağıtımı kullanılarak oluşturulmuş sanal bir conda ortamı içinde bağımlılık versiyonları yönetilmiş ve izolasyonu sağlanmıştır. Bununla birlikte, deneylerin tekrarlanabilirliğini sağlamak ve olası uyumsuzlukları ortadan kaldırmak için tutarlı ve izole bir deney ortamı oluşturulması amaçlanmıştır.

Veri ön işleme, model eğitimi ve test süreci boyunca, ana donanım olarak Grafik İşlem Birimi(GPU(Graphics Processing Unit))'nun gücünden yararlanılıp, hesaplama süreleri minimize edilmiştir. Tüm deneyler boyunca, deterministik ve tutarlı sonuçlar oluşturmak için, aynı bir rastgele tohum değeri kullanılmış ve aynı veri setleri üzerinde, veri setinin tamamı kullanılarak çalışılmıştır. Batch size boyutu ve katman sayısını optimum performans metriklerine ulaşılana kadar değiştirilerek test edilmiş ve en uygun sonuca göre modelin parametreleri bulunmuştur.

2.6. CICIoV2024 Veri Seti Üzerinde Yapılan Deneyler

Tez çalışmasının bu bölümünde, CICIoV2024 veri seti üzerinde önce yapılan ön işleme anlatılmakta ardından önerilen CNN, DNN ve LSTM modeli mimarilerinin ayrıntıları verilmektedir.

2.6.1. Veri Ön İşleme

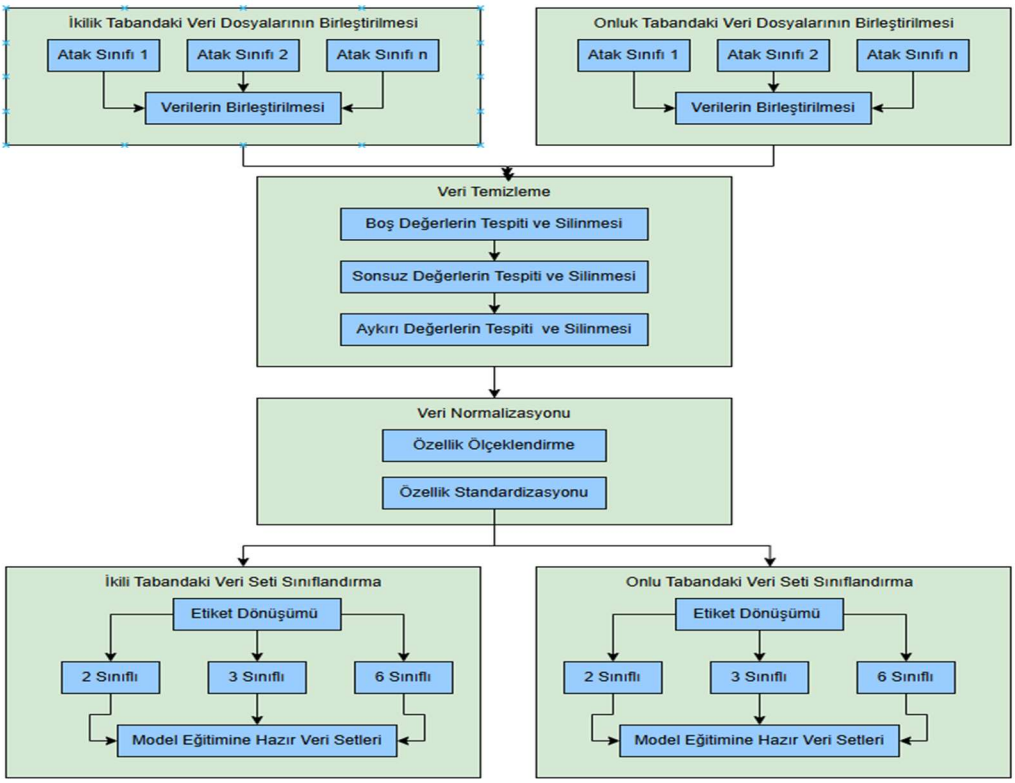
Veri seti dosyalarının eğitim modellerine uygun hale getirilmesinde aşağıdaki adımlar izlenmiş ve Şekil 2.11de akış olarak gösterilmiştir.

CICIoV2024 veri setinin ikili ve onluk tabanda olarak iki farklı formatı bulunmaktadır. Veri işleme süreci, iki farklı veri formatı için birleştirme aşamasıyla başlar. İkili ve onluk tabandaki veri dosyaları iki dosyada birleştirilirken, her iki yapıda da değişik atak sınıflarından (Atak Sınıfı 1, 2 ve n) gelen veriler kendi içlerinde birleşir.

Sürecin ikinci aşaması olan temizlik aşamasında iki dosyadaki bu birleştirilmiş veri, ortak bir bilgi temizleme sürecinden geçmektedir. Bu aşamada üç temel işlem yapılmaktadır: Önce boş değerlerin bulunması ve silinmesi sağlanmakta, sonra sonsuz değerler tespit edilerek çıkarılmakta ve en son aykırı değerler bulunarak veri setinden çıkarılmaktadır.

Üçüncü aşamada ise, iki veri grubu için de özellikler ayarlama ve özellikler standart hale getirme işlemleri yapılmaktadır. Bu işlemler, farklı tiplerde olan verilerin karşılaştırılabilir duruma gelmesini sağlamaktadır.

Normalizasyon işleminden sonraki son aşamada ise, iki farklı formattaki veri seti içinde, eğitim modeline sunmak üzerine, ikili, üçlü ve altılı sınıflı olmak üzere üç farklı dosyaya bölünmektedir. Bu ayırma işlemleri sonrası, her iki tabandaki veriler de model eğitimine hazır bir şekilde gelinmektedir. Son olarak model eğitimine hazır olan veriler üçe bölünerek, eğitim, doğrulama ve test veri setlerine ayrılmıştır.



Şekil 2.11. CICIoV2024 veri setinin ön işleme adımları.[21]

2.6.2. Önerilen CNN Modeli

Tablo 2.8. Önerilen CNN Modelinin Katmanları.

Katman	Parametreler	Aktivasyon Fonksiyonu
Conv1D	32, kernel_size = 2, padding = 'same'	ReLU [139]
Batch Normalization	0	-
Conv1D	64, kernel_size = 2, padding = 'same'	ReLU
Batch Normalization	0	-
Dropout	0.3	-
Conv1D	128, kernel_size = 2, padding = 'same'	ReLU
Batch Normalization	0	-
Dropout	0.2	-
Flatten	0	-
Batch Normalization	0	-
Dropout	0.2	-
Dense	sınıf sayısı	İkili:Sigmoid [140] Çoklu:Softmax [137]

Tablo 2.9. Önerilen CNN Modelinin Hiper Parametreleri.

Parametre	Değer
Batch Size (Batch Boyutu)	128
Epochs (Dönem)	10

Optimizasyon Fonksiyonu	Adam
Kayıp Fonksiyonu	İkili:BinaryCrossentropy [139] Çoklu:Categorical CrossEntropy [139]

2.6.3. Önerilen DNN Modeli

Tablo 2.10. Önerilen DNN Modelinin Katmanları.

Katman	**Parametreler**	**Aktivasyon Fonksiyonu**
Dense	256	ReLU
Batch Normalization	0	-
Dropout	0.3	-
Dense	128	ReLU
Batch Normalization	0	-
Dropout	0.3	-
Dense	64	ReLU
Batch Normalization	0	-
Dropout	0.2	-
Dense	32	ReLu
Batch Normalization	0	-
Dropout	0.2	-
Dense	sınıf sayısı	İkili:Sigmoid Çoklu:Softmax

Tablo 2.11. Önerilen DNN Modelinin Hiper Parametreleri

Parametre	**Değer**
Batch Size (Batch Boyutu)	128
Epochs (Dönem)	10
Optimizasyon Fonksiyonu	Adam[137]
Kayıp Fonksiyonu	İkili:BinaryCrossentropy [140] Çoklu:Categorical CrossEntropy [137]

2.6.4. Önerilen LSTM Modeli

Tablo 2.12. Önerilen LSTM Modelinin Hiper Parametreleri.

Katman	**Parametreler**	**Aktivasyon Fonksiyonu**
LSTM	32, return_sequences = True	tanh
Batch Normalization	0	-
Dropout	0.3	-
LSTM	64, return_sequences = False	tanh
Batch Normalization	0	-
Dropout	0.3	-
Dense	32	ReLU
Batch Normalization	0	-
Dropout	0.2	-

Dense	sınıf sayısı	İkili:Sigmoid Çoklu:Softmax

Tablo 2.13. Önerilen LSTM Modelinin Hiper Parametreleri.

Parametre	**Değer**
Batch Size (Batch Boyutu)	256
Epochs (Dönem)	10
Optimizasyon Fonksiyonu	Adam[137]
Kayıp Fonksiyonu	İkili:BinaryCrossentropy Çoklu:Categorical CrossEntropy [137]

2.7. CICIoMT2024 Veri Seti Üzerinde Yapılan Deneyler

Tez çalışmasının bu bölümünde, CICIoMT2024 veri seti üzerinde önce yapılan ön işleme anlatılmakta ardından önerilen CNN, DNN ve LSTM modeli mimarilerinin ayrıntıları verilmektedir.

2.7.1. Veri Ön İşleme

Veri seti dosyalarının eğitim modellerine uygun hale getirilmesinde aşağıdaki adımlar izlenmiş ve Şekil 2.12'de akış olarak gösterilmiştir.

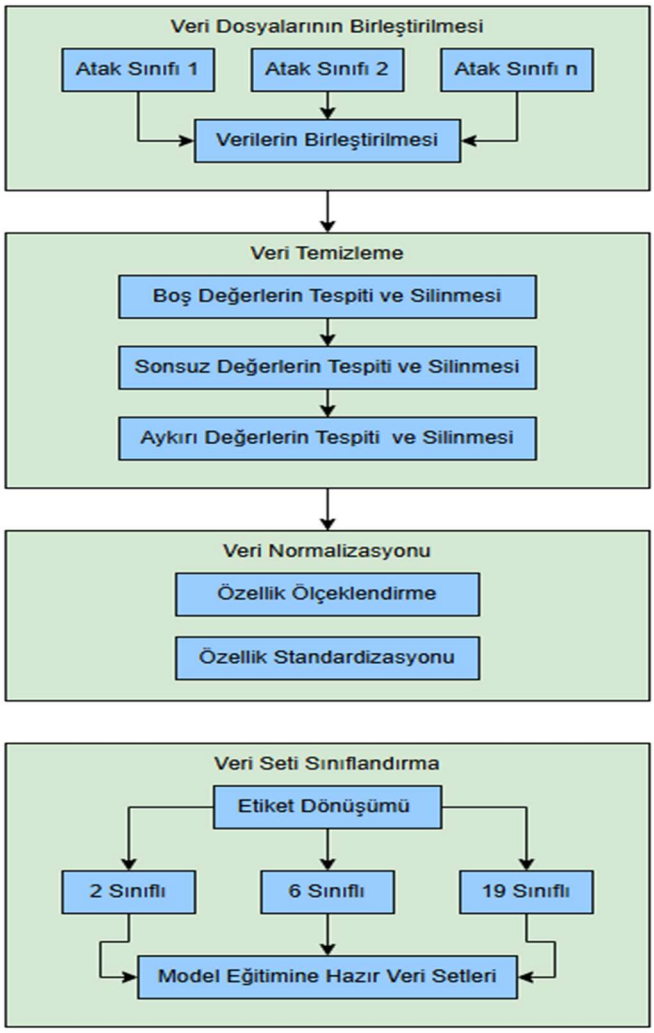
Ön işleme sürecinde, dört ana aşama vardır. İlk aşama veri dosyalarının birleştirilmesidir, farklı atak türlerinden (Atak Türü 1, 2 ve n) gelen veriler farklı dosyalar tek bir dosya içinde toplanır. Bu birleşim işlemi verilerin düzgün bir şekilde incelenmesi ve işlenmesi için çok önemlidir.

İkinci aşama veri temizleme işleminde, üç ana temel işlem yapılmaktadır. Öncelikle boş değerler bulunmakta ve silinmektedir. Ardından sonsuz değerler tespit edilip veri setinden çıkarılmaktadır.

Son olarak aykırı olan veriler tespit edilip veri setinden çıkarılmaktadır. Bu aşama verinin kalitesini ve güvenilirliğini artırmak için önemlidir.

Üçüncü aşama olan, veri düzeltme aşamasında, özelliklerin boyut ayarı ve standart hale getirme işleri yapılır. Bu işler, değişik boyutlardaki verilerin standart duruma gelmesini sağlar.

Son adımda ise veri seti sınıflandırma sürecinde, ilk olarak etiket değiştirme yapılmaktadır. Bu değişim sonrası veriler 2 sınıf, 6 sınıf ve 19 sınıf olarak üç farklı grup olarak ayrı dosyalara bölünmektedir. Bu sınıflama işleminden sonra elde edilen veriler model eğitimi için hazır duruma getirilmektedir. Son olarak model eğitimine hazır olan veriler üçe bölünerek, eğitim, doğrulama ve test veri setlerine ayrılmıştır.



Şekil 2.12. CICIoMT2024 veri setinin ön işleme adımları [22]

2.7.2. Önerilen CNN Modeli

CICIoMT2024 veri setinin eğitimi için kullanılan CNN mimarisin katmanları Tablo 2.14'teki gibidir. İkili, altılı ve on dokuz sınıflı modelde aynı mimari ve Tablo 2.15'te görüldüğü üzere aynı hiper parametreler kullanılmıştır.

Tablo 2.14. Önerilen CNN Modelinin Katmanları.

Katman	**Parametreler**	**Aktivasyon Fonksiyonu**
Conv1D	128	ReLU
MaxPooling1D	0	-
Conv1D	6208	ReLU
MaxPooling1D	0	-
Flatten	0	-
Dense	flatten_çıkış_katmanı_boyutu × 128 + 128	ReLU
Dense	128 × sınıf_sayısı + sınfı sayısı	İkili:Sigmoid Çoklu:Softmax

Tablo 2.15. Önerilen CNN Modelinin Hiper Parametreleri.

Parametre	**Değer**
Batch Size (Batch Boyutu)	256
Epochs (Dönem)	10
Optimizasyon Fonksiyonu	Adam[137]

Kayıp Fonksiyonu	İkili:BinaryCrossentropy Çoklu:Categorical CrossEntropy [137]

2.7.3. Önerilen DNN Modeli

CICIoMT2024 veri setinin eğitimi için kullanılan DNN mimarisin katmanları Tablo 2.16'daki gibidir. İkili, altılı ve on dokuz sınıflı modelde aynı mimari ve Tablo 2.17'de görüldüğü üzere aynı hiper parametreler kullanılmıştır.

Tablo 2.16. Önerilen DNN Modelinin Katmanları.

Katman	**Parametreler**	**Aktivasyon Fonksiyonu**
Dense	256	ReLU
Droput	0.3	-
Dense	128	ReLU
Dropout	0.3	-
Dense	64	ReLU
Dense	sınıf sayısı	İkili:Sigmoid Çoklu:Softmax

Tablo 2.17. Önerilen DNN Modelinin Hiper Parametreleri.

Parametre	**Değer**
Batch Size (Batch Boyutu)	128

Epochs (Dönem)	10
Optimizasyon Fonksiyonu	RMSprop[137]
Kayıp Fonksiyonu	İkili:BinaryCrossentropy Çoklu:Categorical CrossEntropy [137]

2.7.4. Önerilen LSTM Modeli

CICIoMT2024 veri setinin eğitimi için kullanılan LSTM mimarisin katmanları Tablo 2.18'deki gibidir. İkili, altılı ve on dokuz sınıflı modelde aynı mimari ve Tablo 2.19'da görüldüğü üzere aynı hiper parametreler kullanılmıştır.

Tablo 2.18. Önerilen LSTM Modelinin Katmanları.

Katman	**Parametreler**	**Aktivasyon Fonksiyonu**
LSTM	128, return_sequences = True	Tanh
BatchNormalization	0	-
Dropout	0.3	-
LSTM	64, return_sequences = True	Tanh
BatchNormalization	0	-
Dense	64	ReLU [139]
Dropout	0.2	-
Dense	sınıf sayısı	İkili:Sigmoid [140] Çoklu:Softmax [137]

Tablo 2.19. Önerilen LSTM Modelinin Hiper Parametreleri

Parametre	**Değer**
Batch Size (Batch Boyutu)	256
Epochs (Dönem)	10
Optimizasyon Fonksiyonu	RMSprop[137]
Kayıp Fonksiyonu	İkili:BinaryCrossentropy Çoklu:Categorical CrossEntropy [137]

3. BULGULAR VE TARTIŞMA

Tez çalışmasının bu bölümünde, yapılan deneylerden elde edilen sonuçlar ayrıntılı bir biçimde anlatılacak ve ilgili literatürdeki diğer çalışmalarla karşılaştırılacaktır. Deneysel veriler; oluşturulan karmaşıklık matrisi ve grafik incelemeleri ile düzenli bir şekilde gözden aktarılacaktır. Elde edilen bilgilerinin analizi ve açıklanması, çalışmanın ana amaçlarıyla hedeflenen çıktılar doğrultusunda genişçe ele alınmıştır.

3.1. CICIoV2024 Deney Sonuçları

CICIoV2024 veri seti üstünde yapılan tüm deneysel çalışmaların sonuçları Tablo 3.1'de ayrıntılı olarak gösterilmiştir. Yapılan deneylerde önerilen CNN, DNN ve LSTM modellerinin her biri için ikili ve onlu tabanlı veri formatlarında sınıflandırma yöntemleri sınanmıştır. Tüm modeller ikili, üçlü ve altılı sınıflandırma işlemleri için doğruluk, kesinlik, duyarlılık ve F1-skoru yönünden performans metrikleri yönünden değerlendirilmiştir.

Tablo 3.1'deki sonuçlara bakıldığında, iki ve üçlü sınırlandırma türlerinde tüm modeller mükemmel performans göstermiştir. Bu durum, önerilen modellerin yalın ve orta derecede karmaşıklıkta olan sınıflama deneylerinde açık ara çok başarılı olduğunu açıkça göstermektedir. Önerilmiş olan CNN, DNN, ve LSTM modellerinin her biri hem ikili hem de onlu formatlarda benzer şekilde üstün performans göstermiştir.

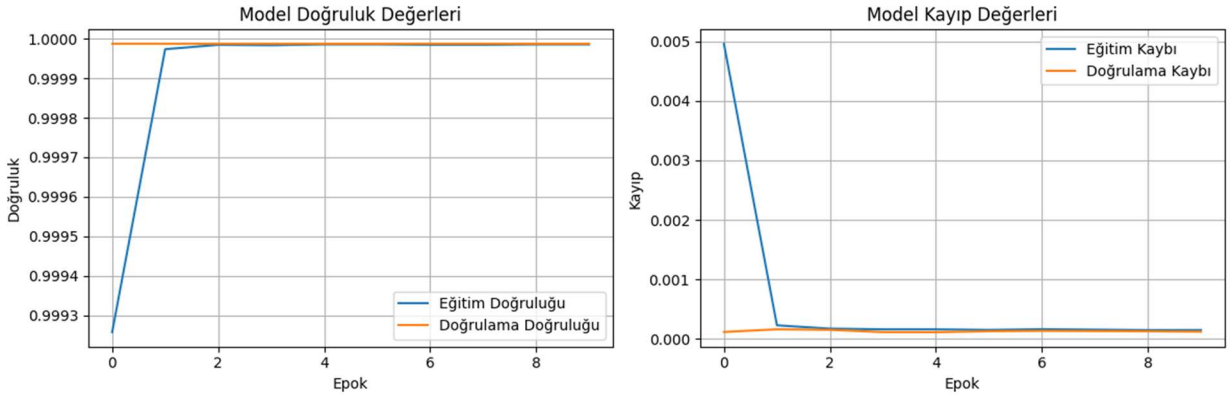
Altılı sınıflandırma sonuçlarına bakıldığında, performansta küçük bir azalma görülmekle birlikte, tüm modeller hâlâ çok yüksek başarı oranı elde etmeye deam etmiştir. Deney sonuçlarında CNN modelinde ikili tabanda %96-99 arası, DNN modelinde %97-99 arası ve LSTM modelinde %96-99 arası değerler alınmıştır. Bu sonuçlar karmaşıklık seviyesi yükseldikçe modellerin performansında az bir düşüş olmuş olsa da önerilen yöntemlerin çoklu IoV cihaz sınıflandırma sorunlarında da epey etkili olduğunu göstermektedir.

Tablo 3.1. CICIoV2024 veri setinin deney sonuçları.

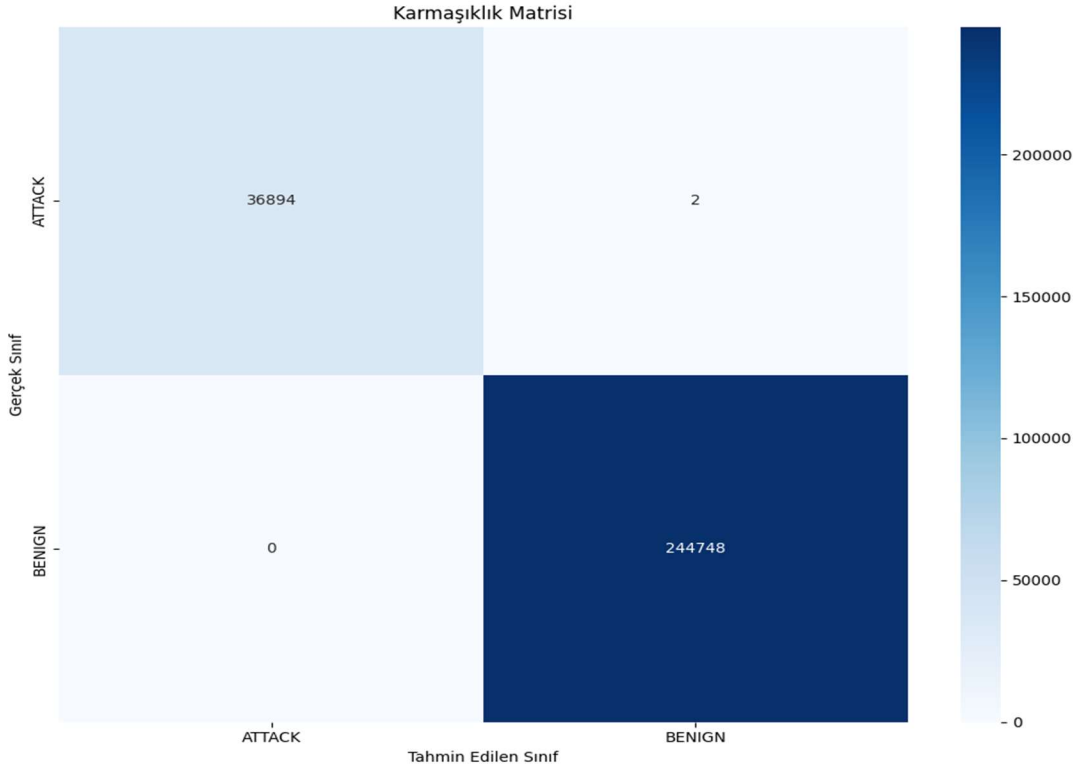
Model	Sınıflandırma	Veri Formatı (Taban)	Performans Metrikleri (%)			
			Doğruluk	Kesinlik	Duyarlılık	F1-Skor
CNN	İkili	İkili	1	1	1	1
		Onlu	1	1	1	1
	Üçlü	İkili	1	1	1	1
		Onlu	1	1	1	1
	Altılı	İkili	0.99	0.96	0.98	0.98
		Onlu	0.99	0.97	0.98	0.98
DNN	İkili	İkili	1	1	1	1
		Onlu	1	1	1	1
	Üçlü	İkili	1	1	1	1
		Onlu	1	1	1	1
	Altılı	İkili	0.99	0.97	0.98	0.98
		Onlu	0.99	0.99	0.96	0.97
LSTM	İkili	İkili	1	1	1	1
		Onlu	1	1	1	1
	Üçlü	İkili	1	1	1	1
		Onlu	1	1	1	1
	Altılı	İkili	0.99	0.99	0.96	0.97
		Onlu	0.99	0.99	0.96	0.97

3.1.1 CNN Modeli Sonuçları

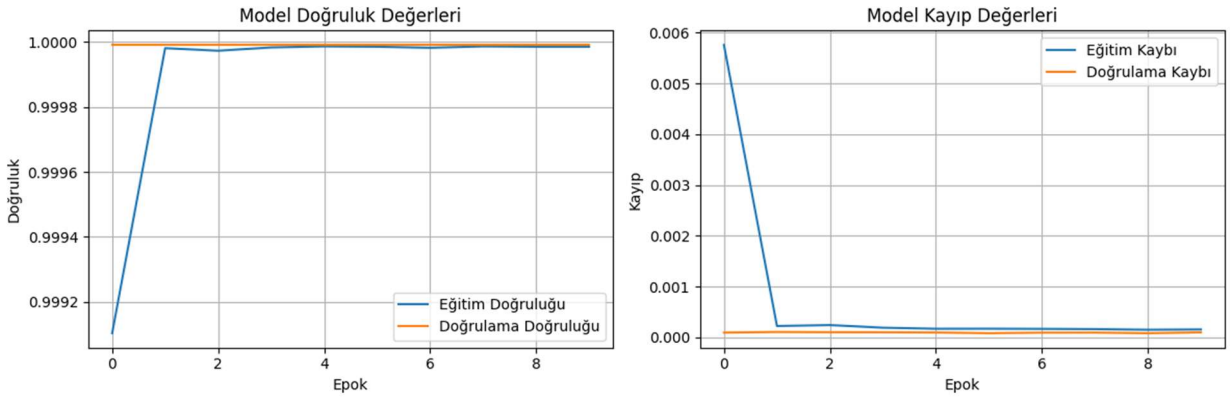
Önerilen CNN modeli, CICIoV2024 veri setinin hem iki hem de onlu tabandaki formatında, ikili, üçlü ve altılı sınıflandırma deneylerinde kusursuza yakın başarı sağlamıştır. Aşağıdaki şekillerde Model doğruluk, model kayıp grafikleri ve karmaşıklık matrisi gösterilmektedir.



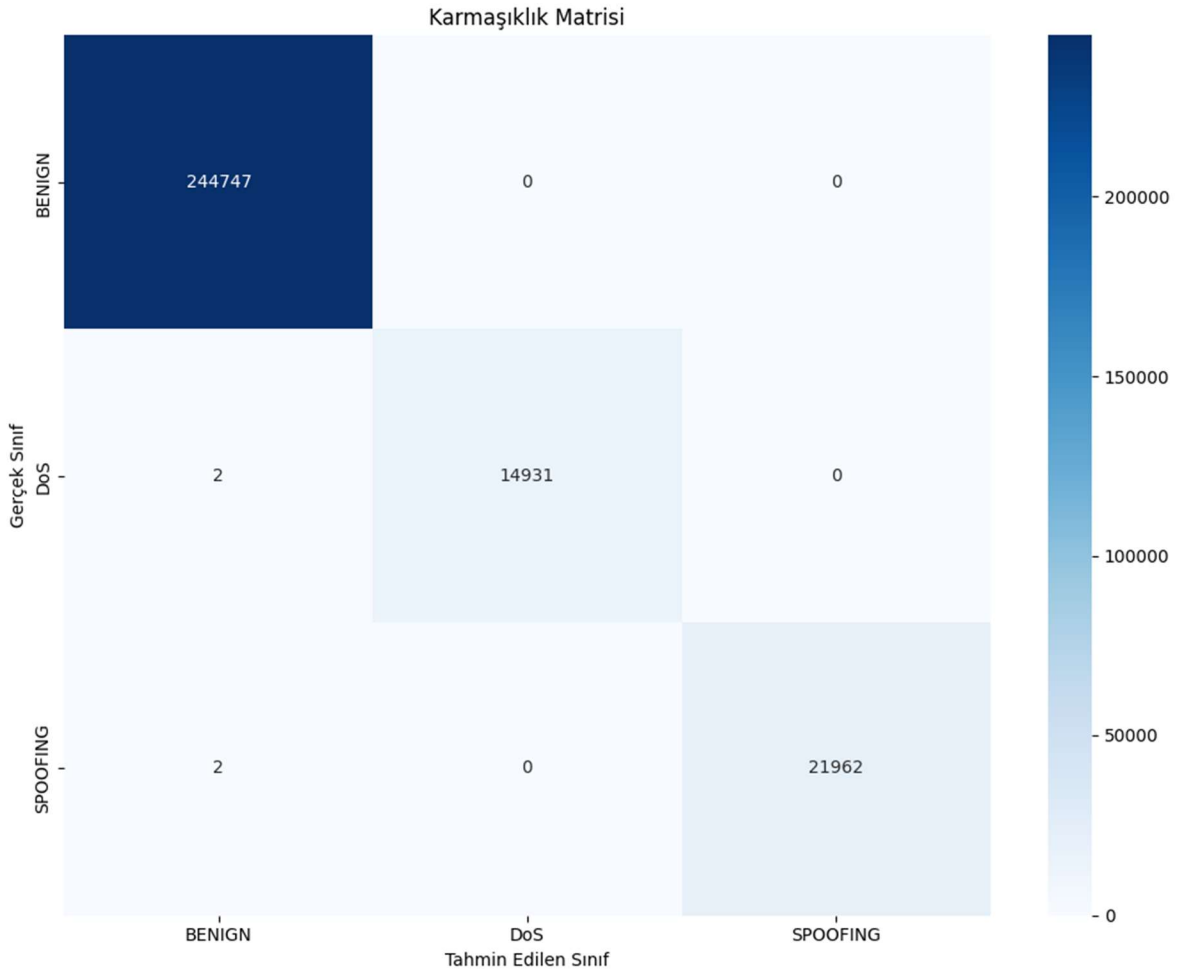
Şekil.3.1. İkili tabandaki veri setinin ikili sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



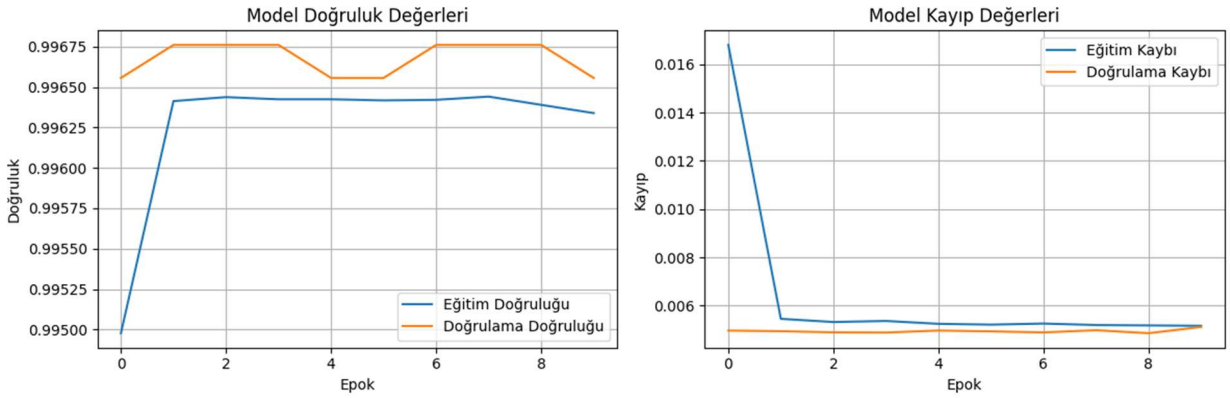
Şekil.3.2. İkili tabandaki veri setinin ikili sınıflandırma testinin karmaşıklık matrisi



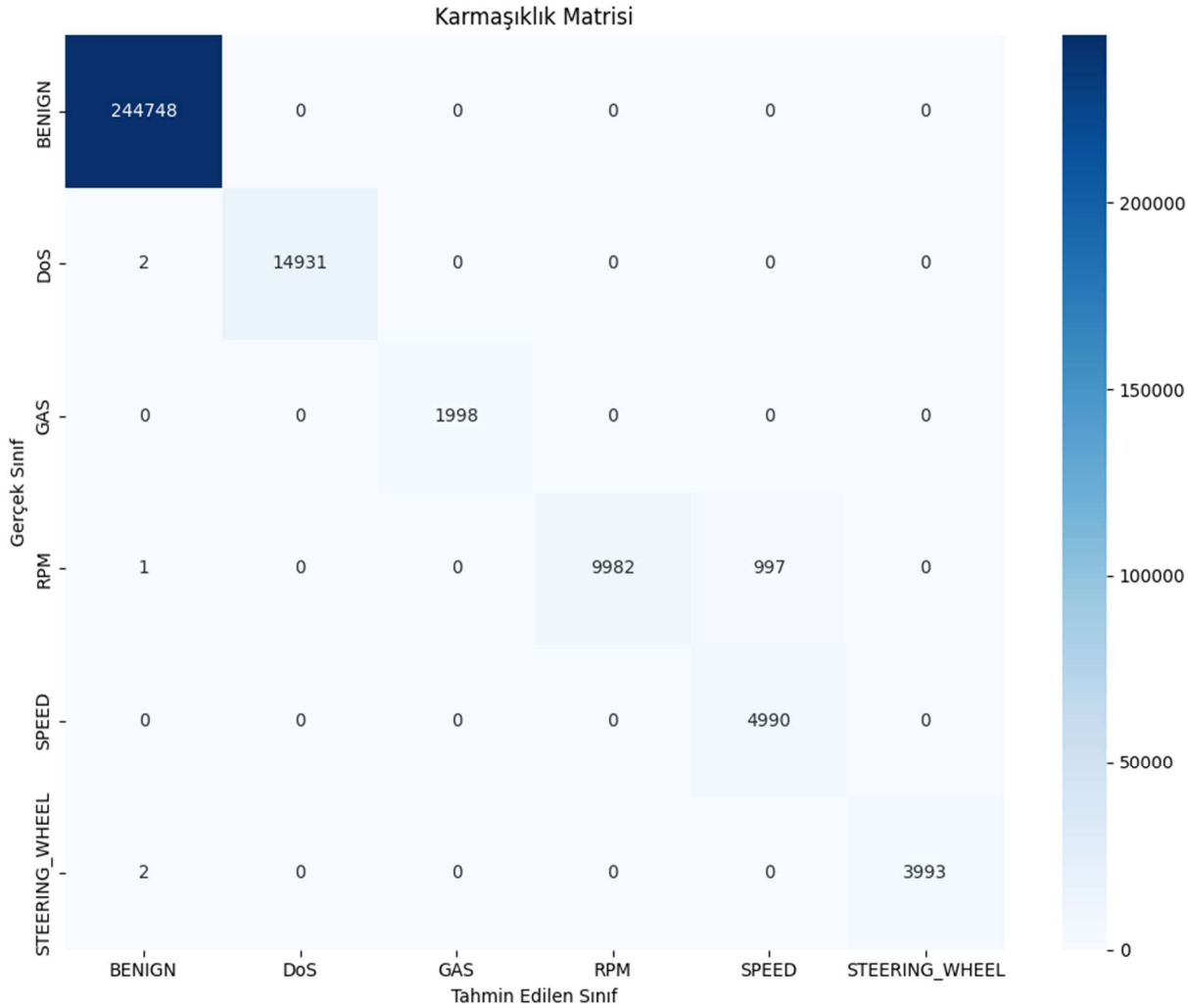
Şekil.3.3. İkili tabandaki veri setinin üçlü sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



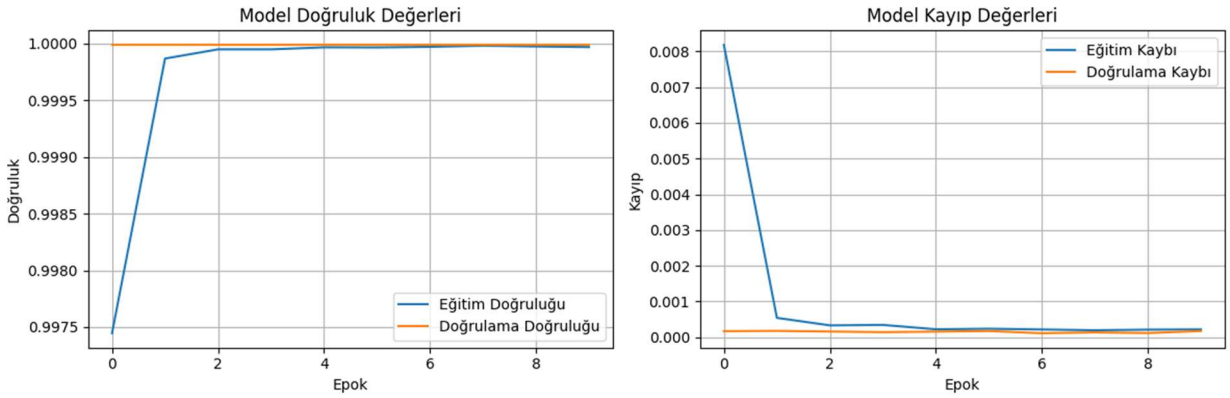
Şekil.3.4. İkili tabandaki veri setinin üçlü sınıflandırma testinin karmaşıklık matrisi



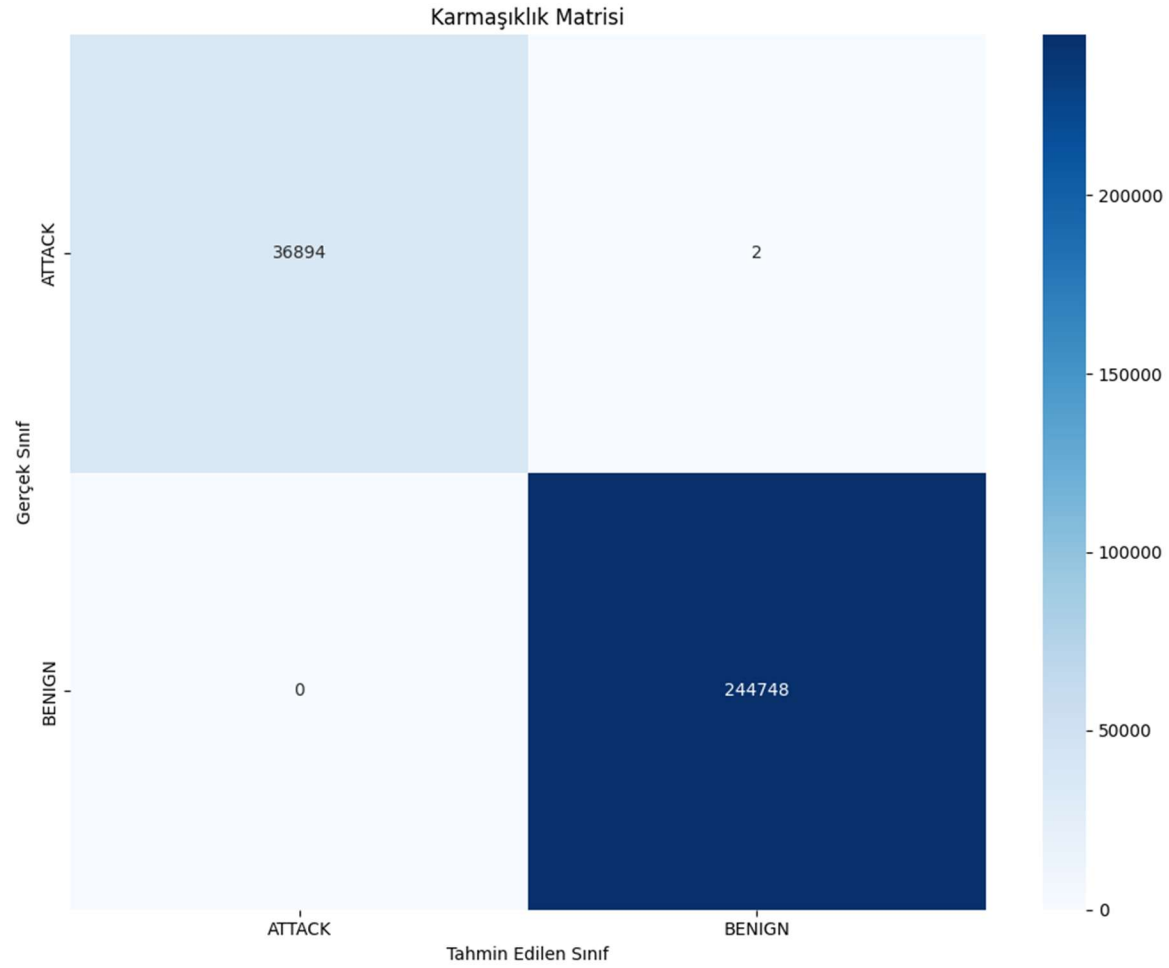
Şekil.3.5. İkili tabandaki veri setinin altılı sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



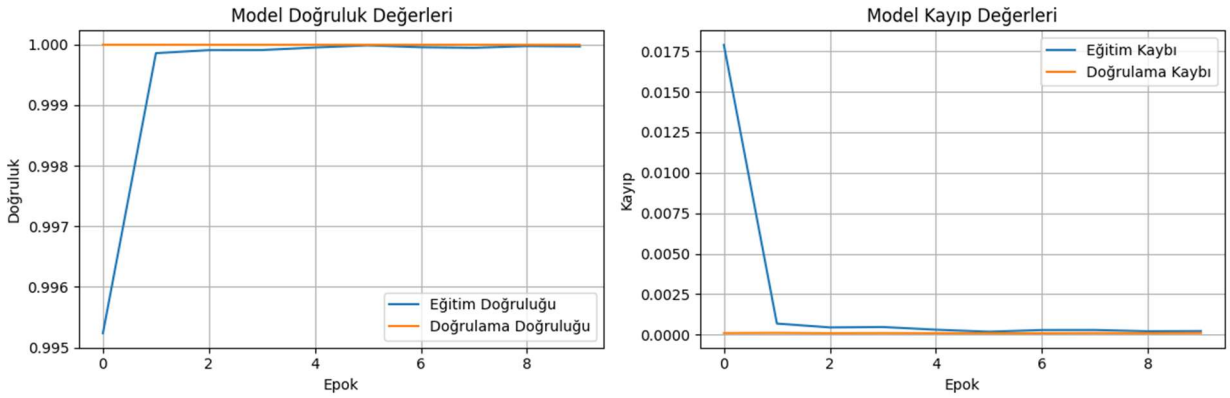
Şekil.3.6. İkili tabandaki veri setinin altılı sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



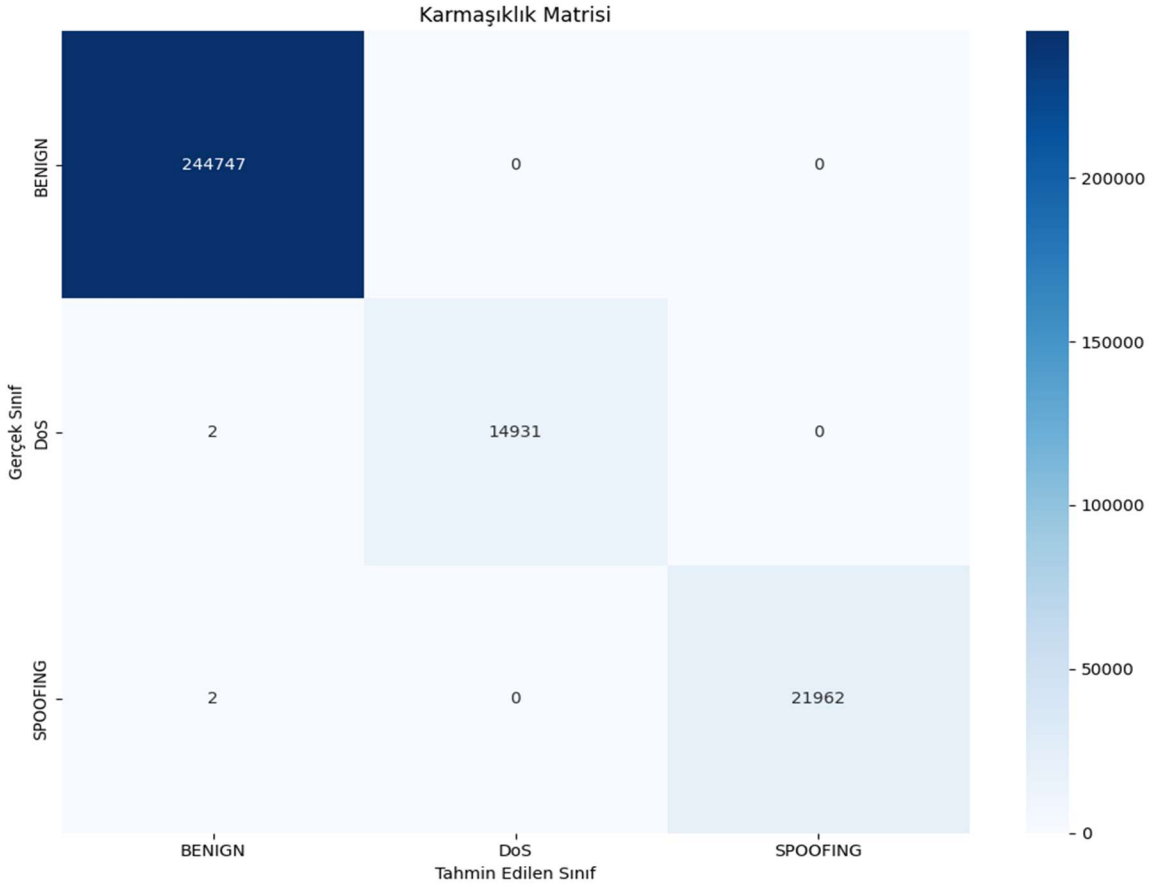
Şekil.3.7. Onluk tabandaki veri setinin ikili sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



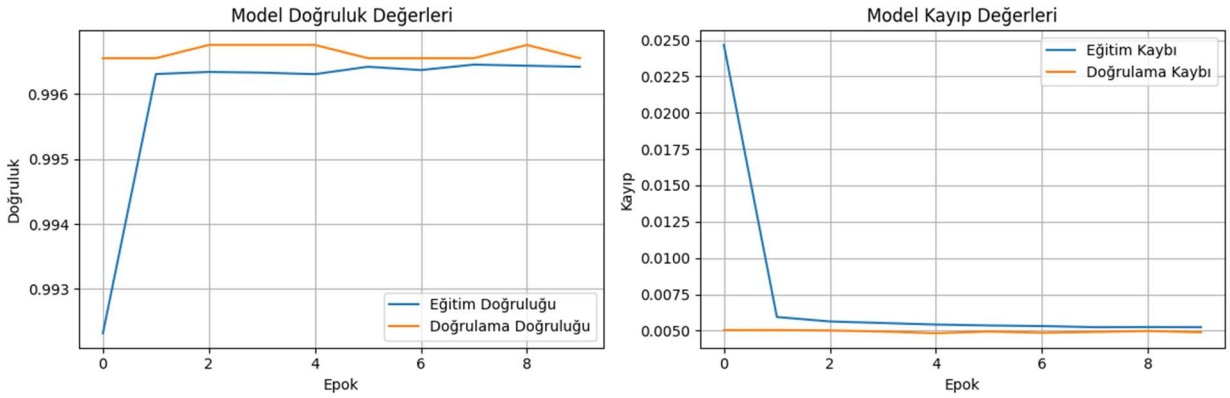
Şekil.3.8. Onluk tabandaki veri setinin ikili sınıflandırma testinin karmaşıklık matrisi



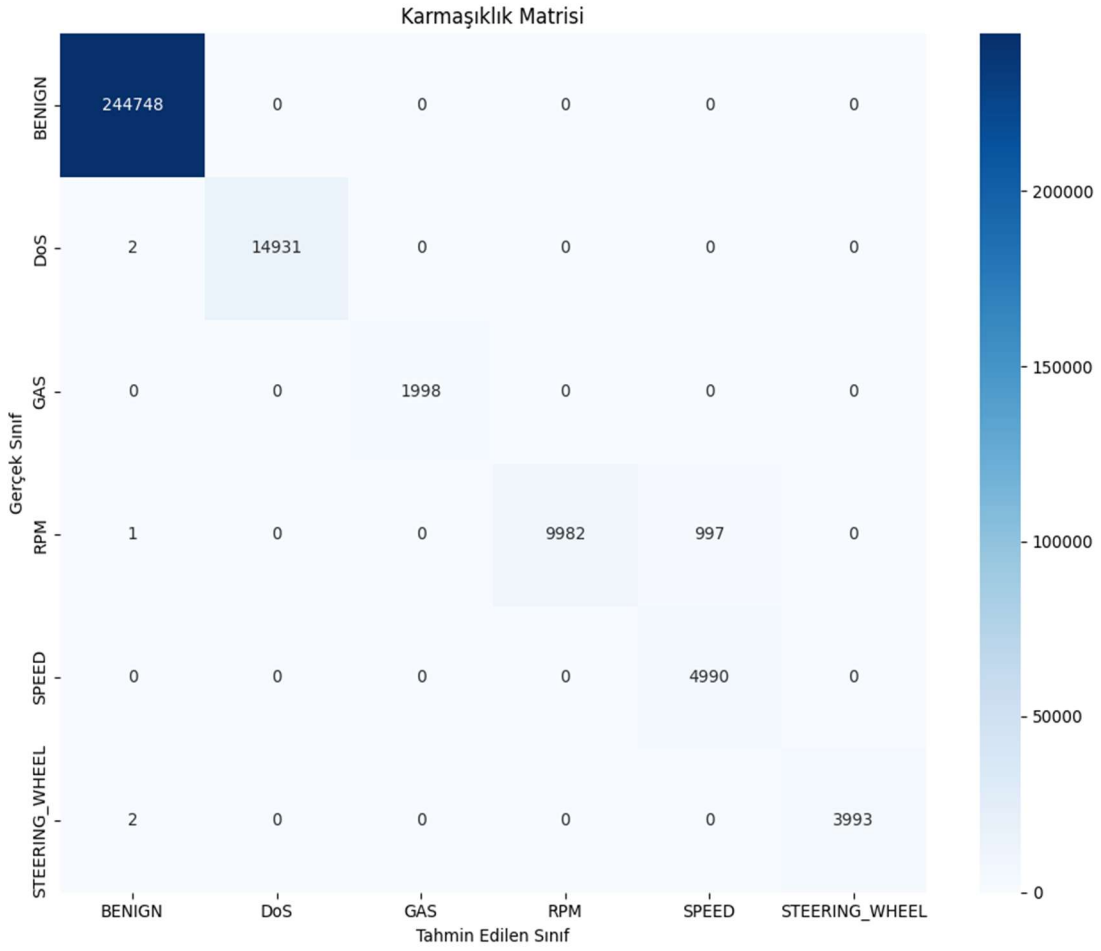
Şekil.3.9. Onluk tabandaki veri setinin üçlü sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



Şekil.3.10. Onluk tabandaki veri setinin üçlü sınıflandırma testinin karmaşıklık matrisi



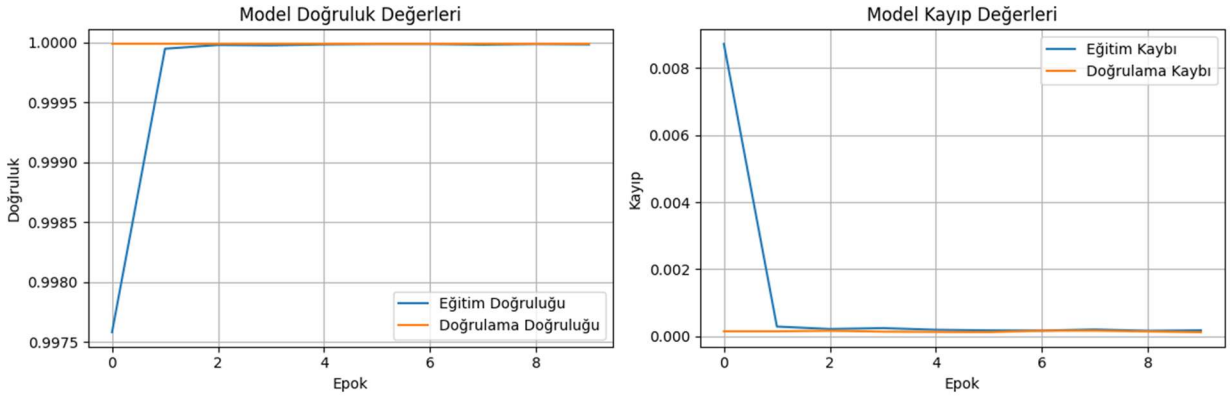
Şekil.3.11. Onluk tabandaki veri setinin altılı sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



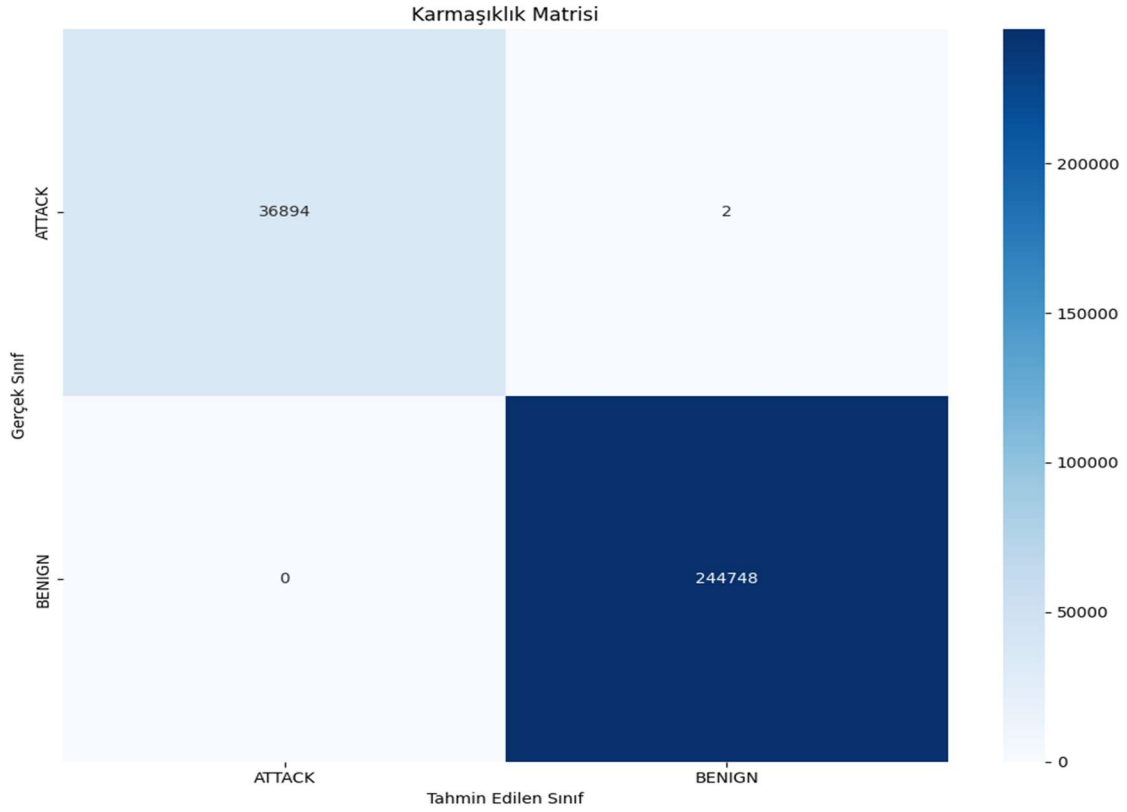
Şekil.3.12. Onluk tabandaki veri setinin altılı sınıflandırma testinin karmaşıklık matrisi

3.1.2 DNN Modeli Sonuçları

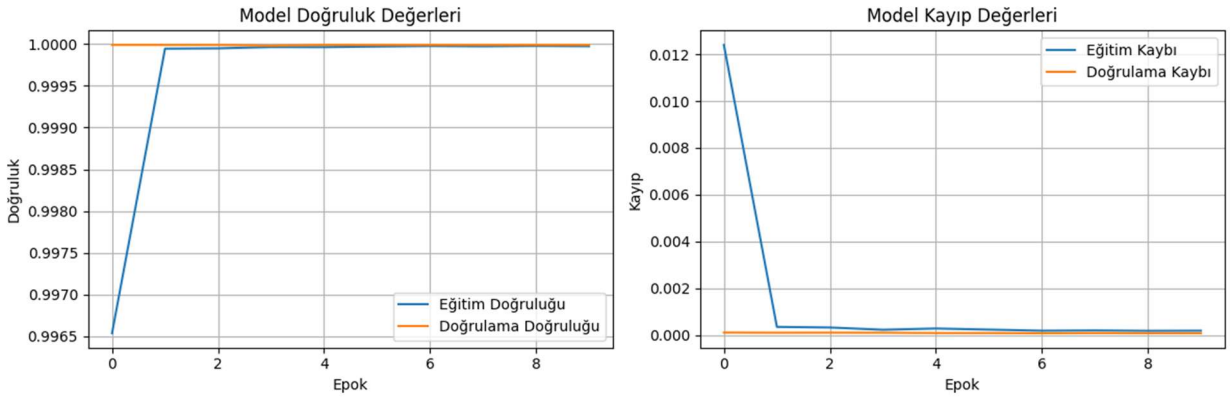
Önerilen DNN modeli, CICIoV2024 veri setinin hem iki hem de onlu tabandaki formatında, ikili, üçlü ve altılı sınıflandırma deneylerinde kusursuza yakın başarı sağlamıştır. Aşağıdaki şekillerde Model doğruluk, model kayıp grafikleri ve karmaşıklık matrisi gösterilmektedir.



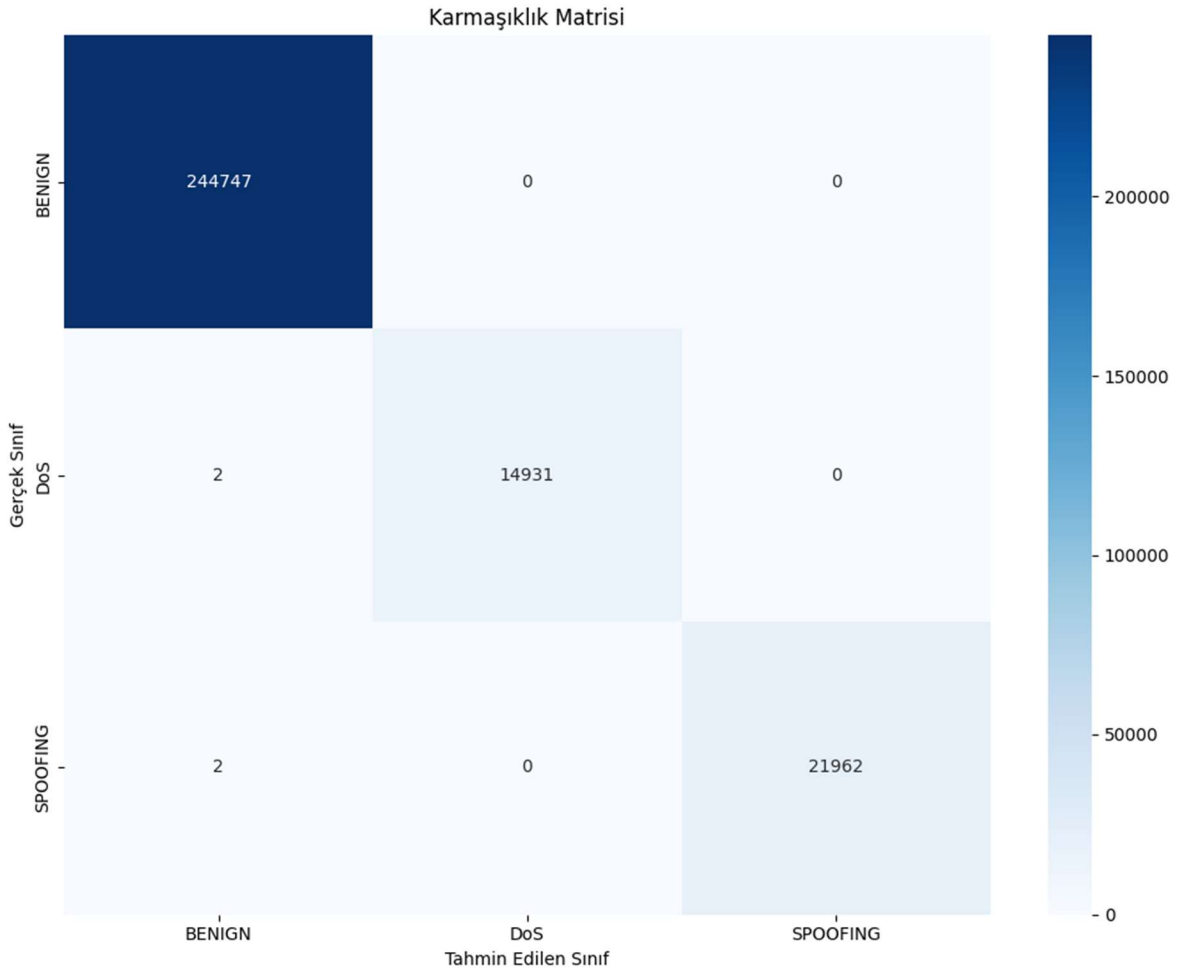
Şekil.3.13. İkili tabandaki veri setinin ikili sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



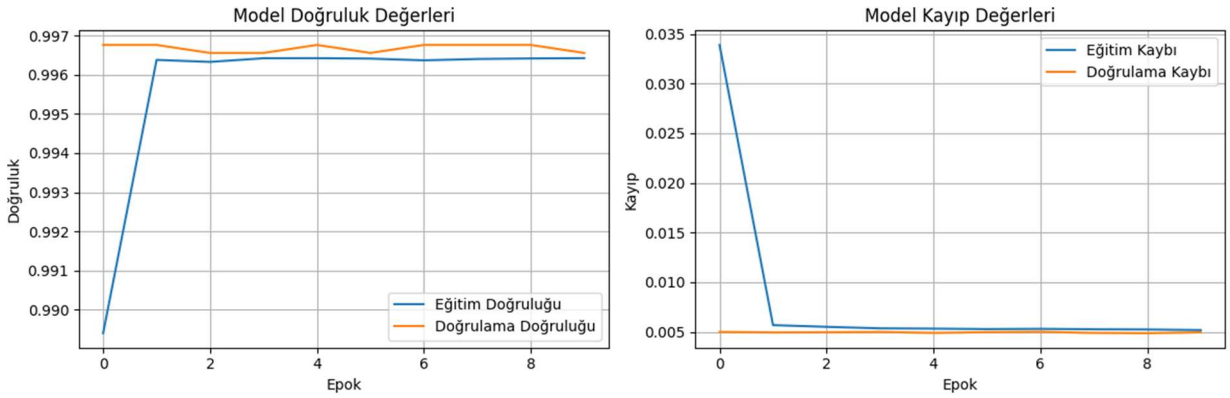
Şekil.3.14. İkili tabandaki veri setinin ikili sınıflandırma testinin karmaşıklık matrisi



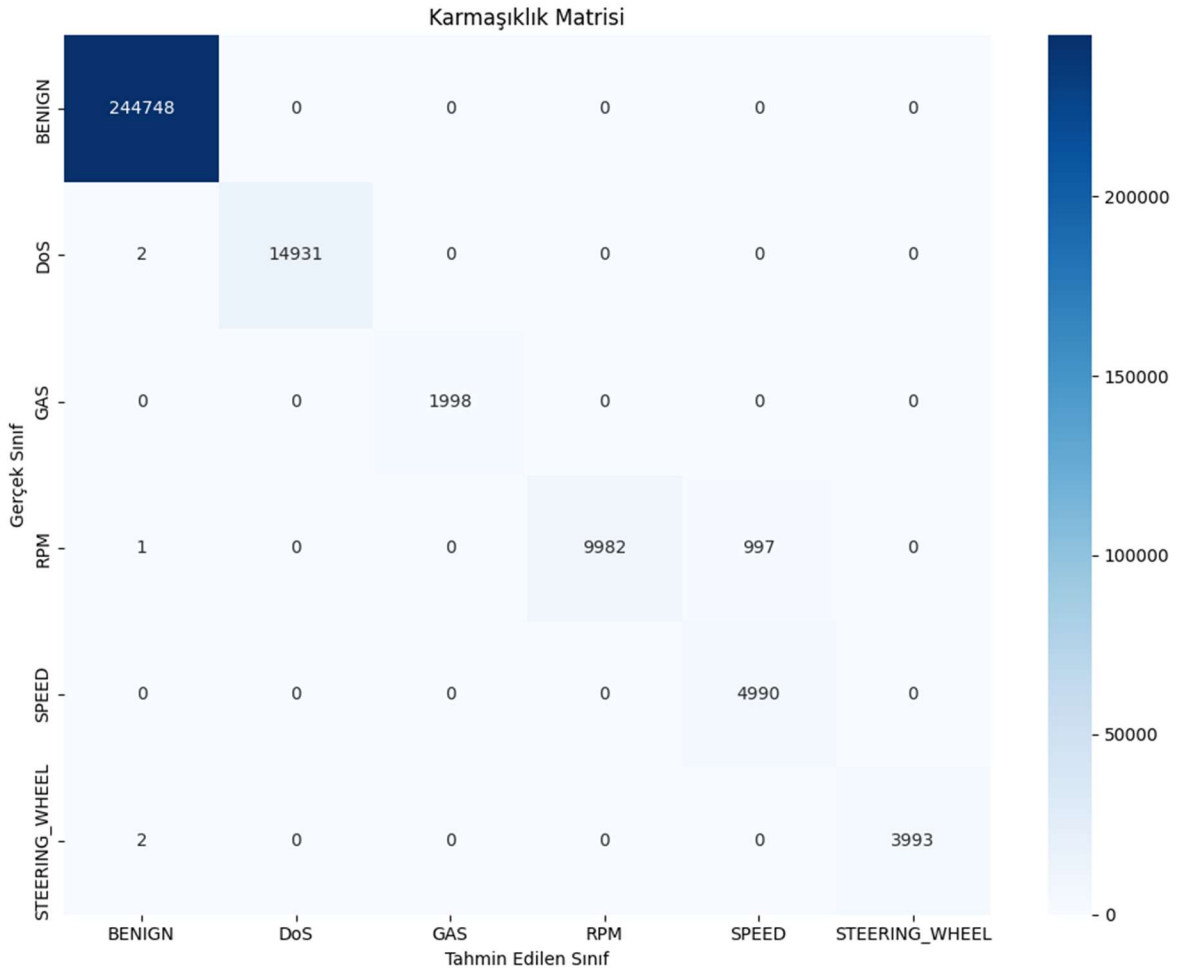
Şekil.3.15. İkili tabandaki veri setinin üçlü sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



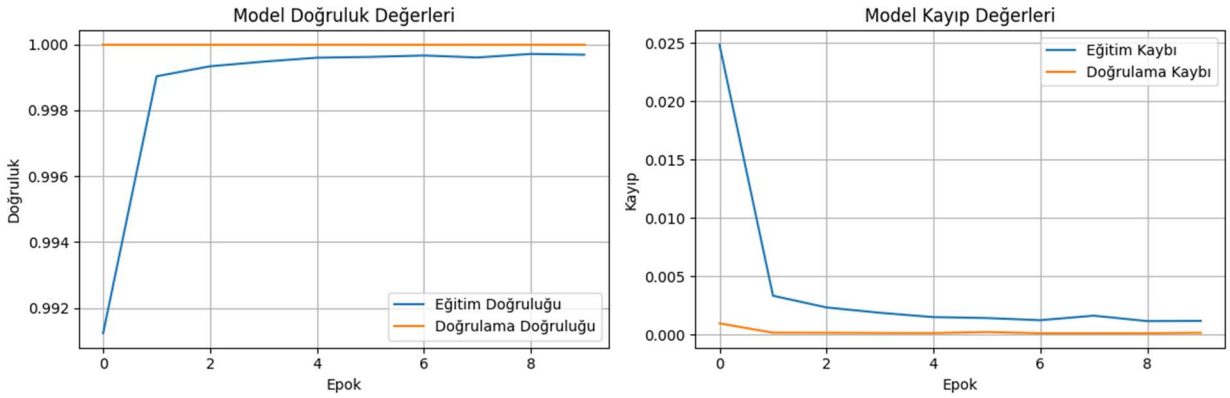
Şekil.3.16. İkili tabandaki veri setinin üçlü sınıflandırma testinin karmaşıklık matrisi



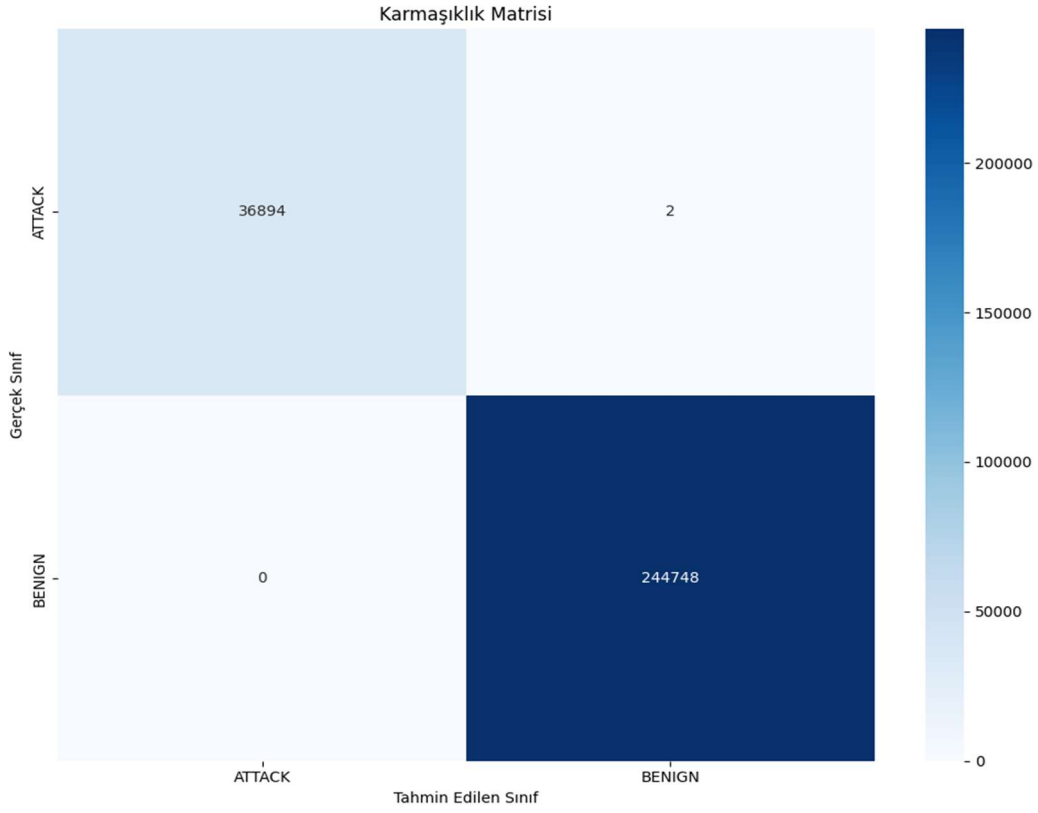
Şekil.3.17. İkili tabandaki veri setinin altılı sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



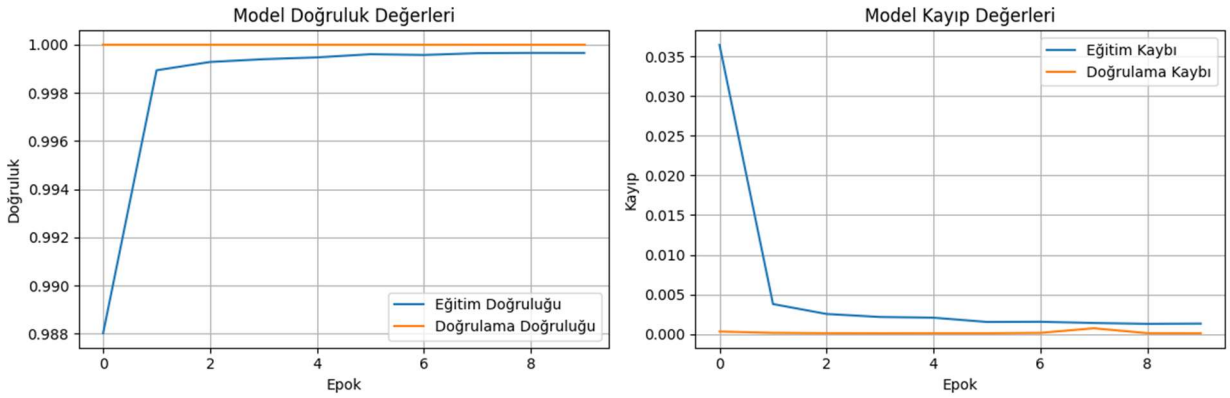
Şekil.3.18. İkili tabandaki veri setinin altılı sınıflandırma testinin karmaşıklık matrisi



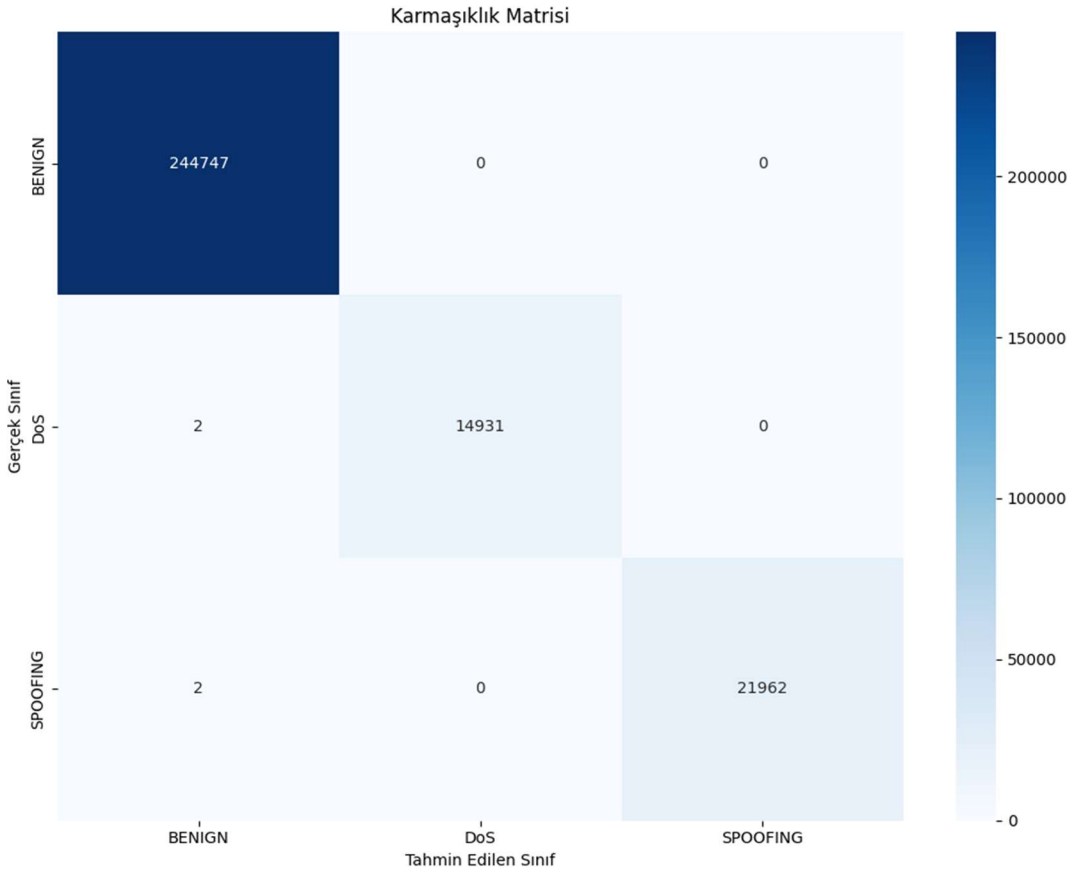
Şekil.3.19. Onluk tabandaki veri setinin ikili sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



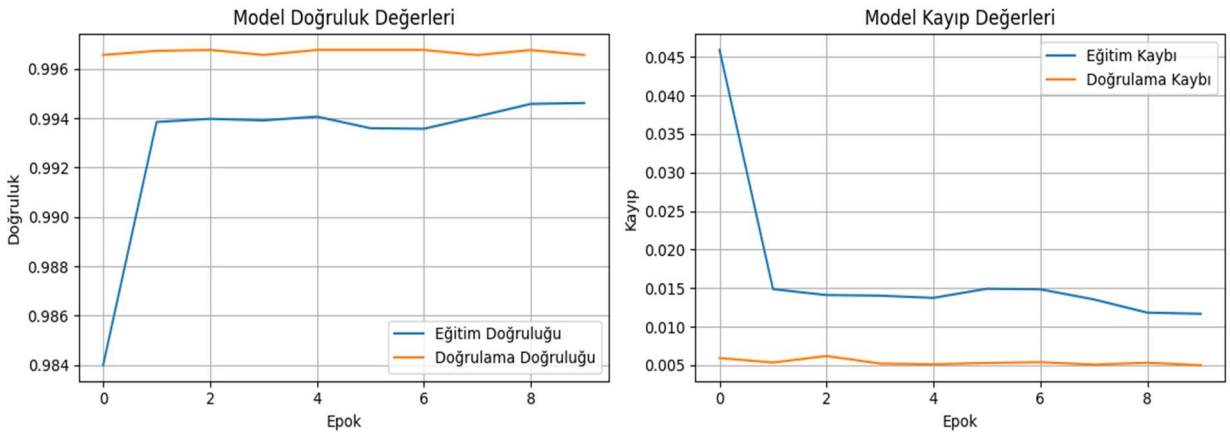
Şekil.3.20. Onluk tabandaki veri setinin ikili sınıflandırma testinin karmaşıklık matrisi



Şekil.3.21. Onluk tabandaki veri setinin üçlü sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



Şekil.3.22. Onluk tabandaki veri setinin üçlü sınıflandırma testinin karmaşıklık matrisi



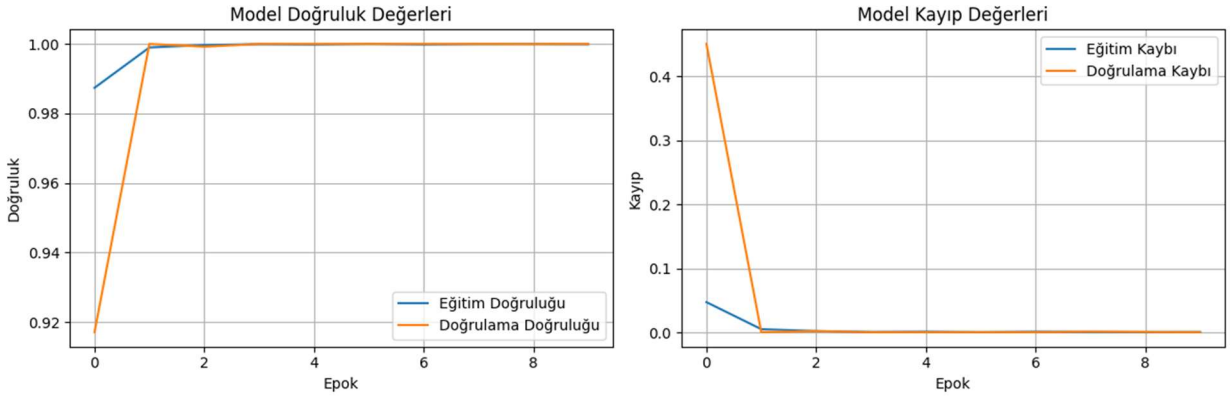
Şekil.3.23. Onluk tabandaki veri setinin altılı sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



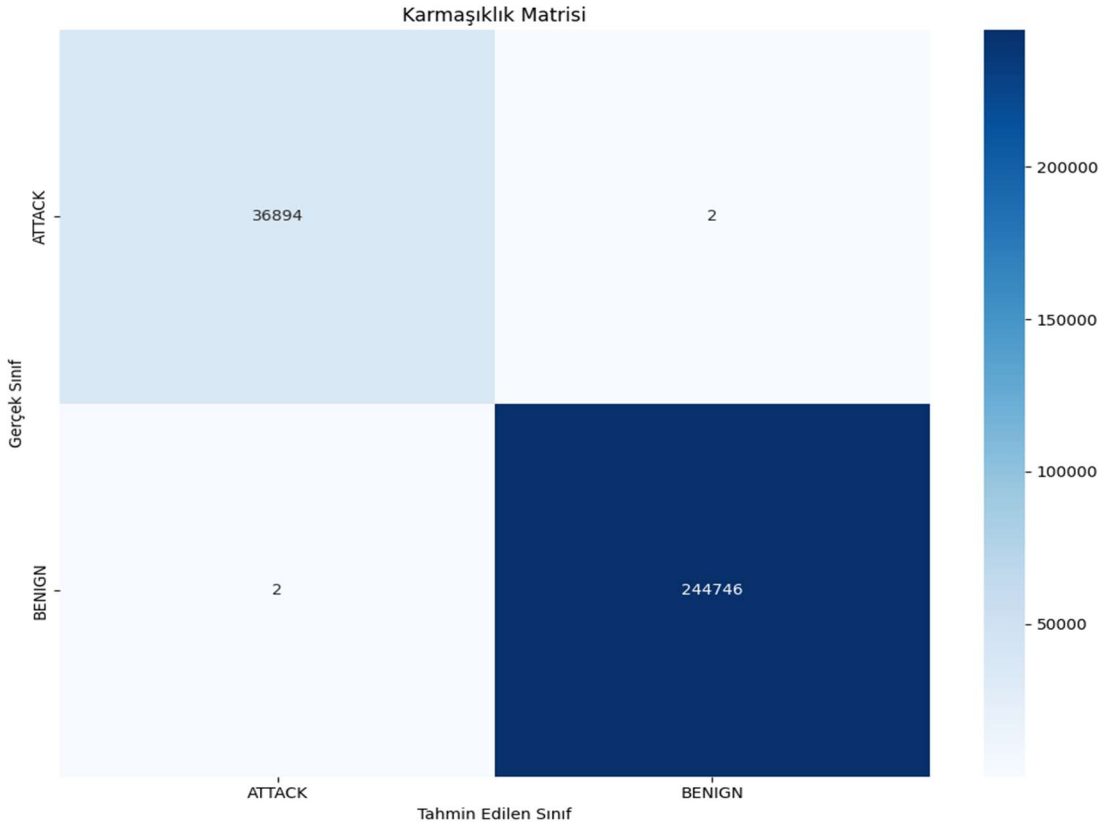
Şekil.3.24. Onluk tabandaki veri setinin altılı sınıflandırma testinin karmaşıklık matrisi

3.1.3 LSTM Modeli Sonuçları

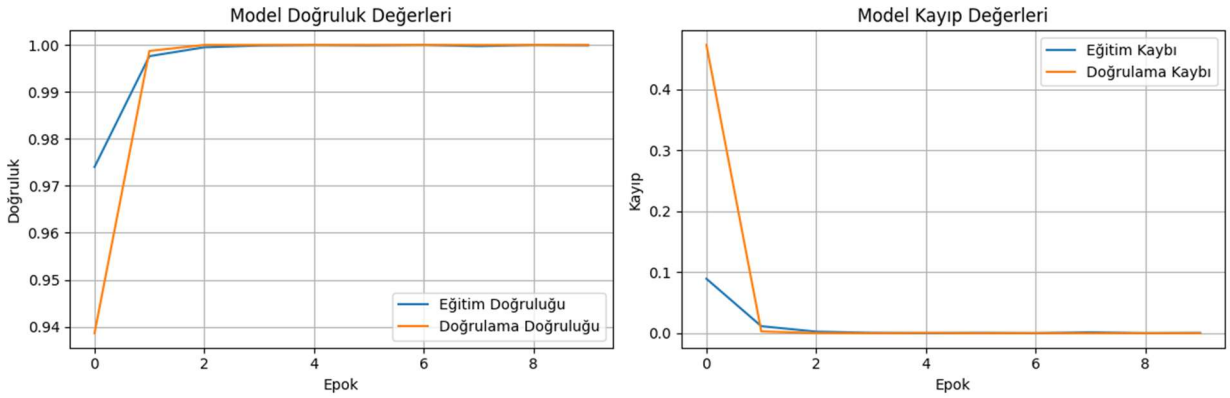
Önerilen LSTM modeli, CICIoV2024 veri setinin hem iki hem de onlu tabandaki formatında, ikili, üçlü ve altılı sınıflandırma deneylerinde kusursuza yakın başarı sağlamıştır. Aşağıdaki şekillerde Model doğruluk, model kayıp grafikleri ve karmaşıklık matrisi gösterilmektedir.



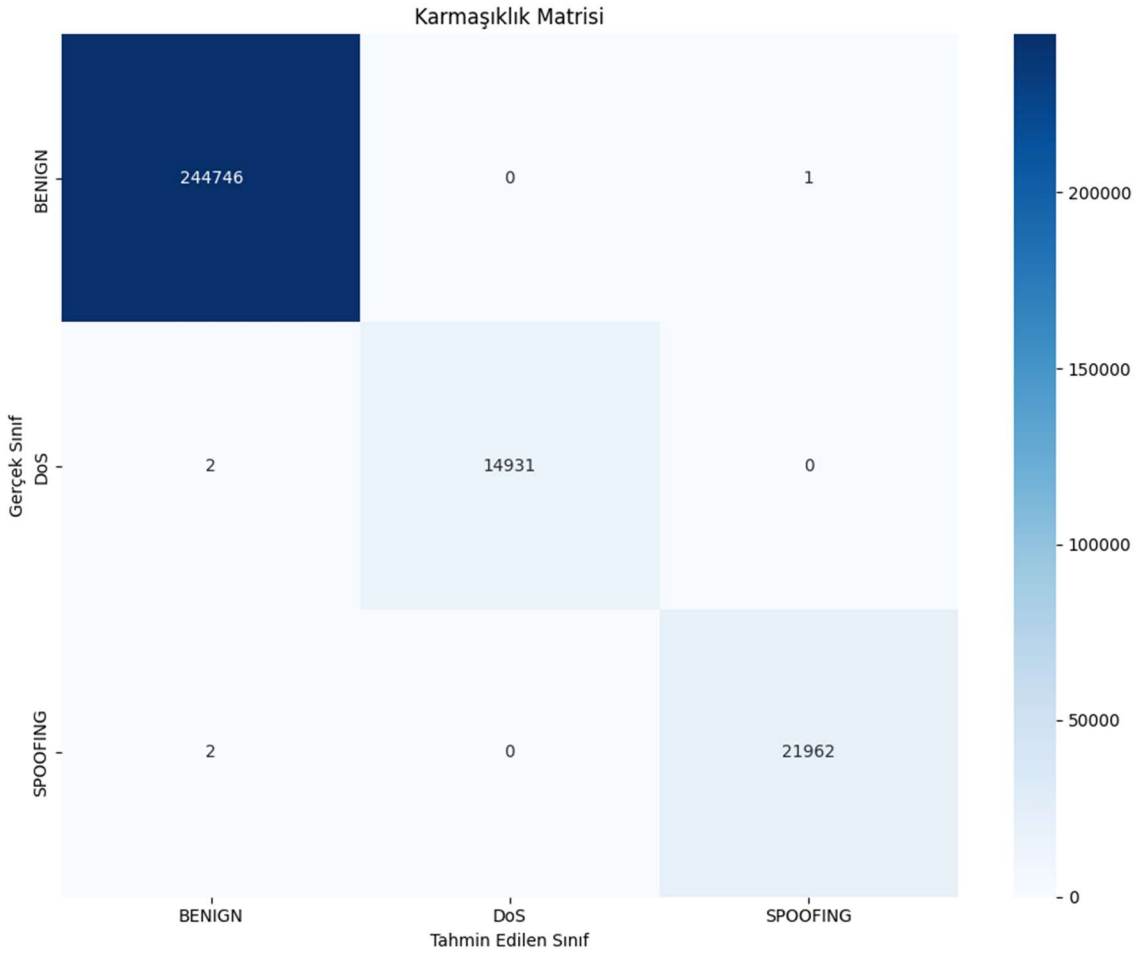
Şekil.3.25. İkili tabandaki veri setinin ikili sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



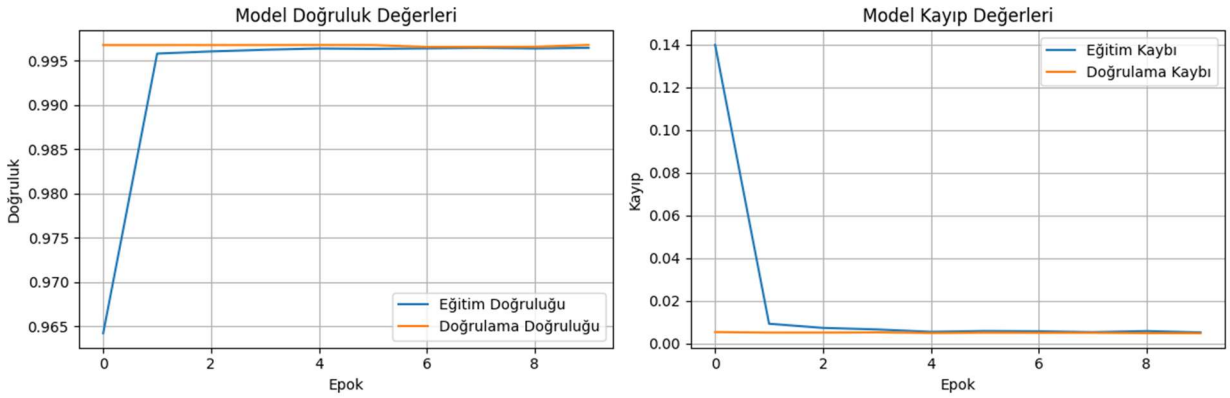
Şekil.3.26. İkili tabandaki veri setinin ikili sınıflandırma testinin karmaşıklık matrisi



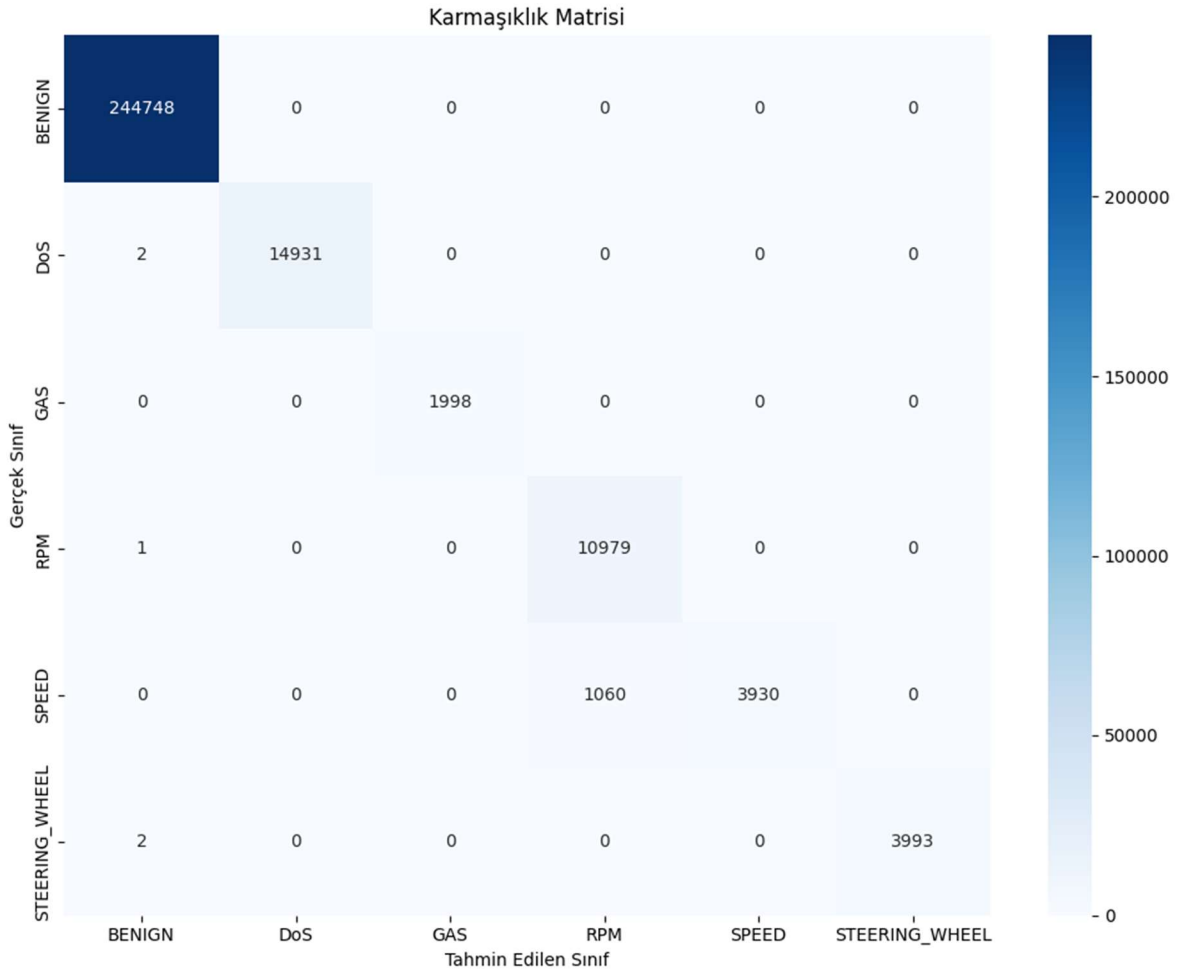
Şekil.3.27. İkili tabandaki veri setinin üçlü sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



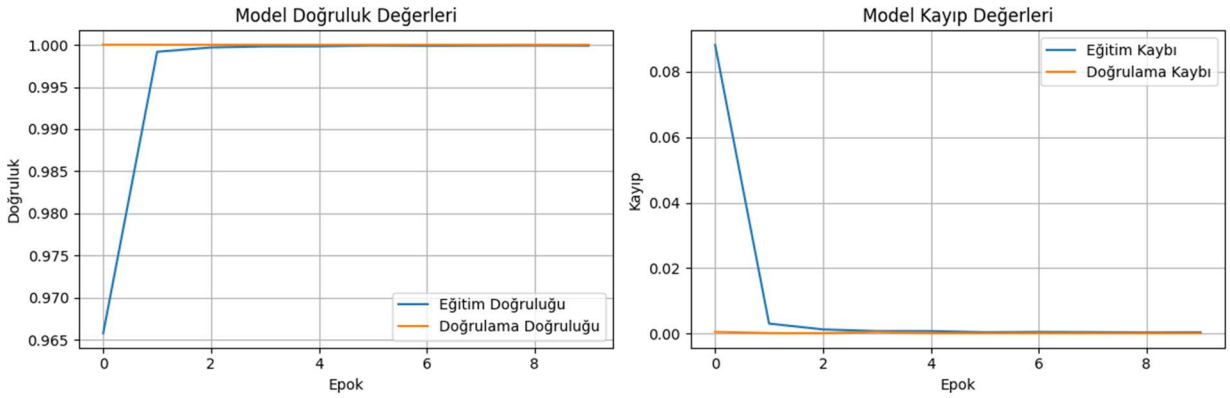
Şekil.3.28. İkili tabandaki veri setinin üçlü sınıflandırma testinin karmaşıklık matrisi



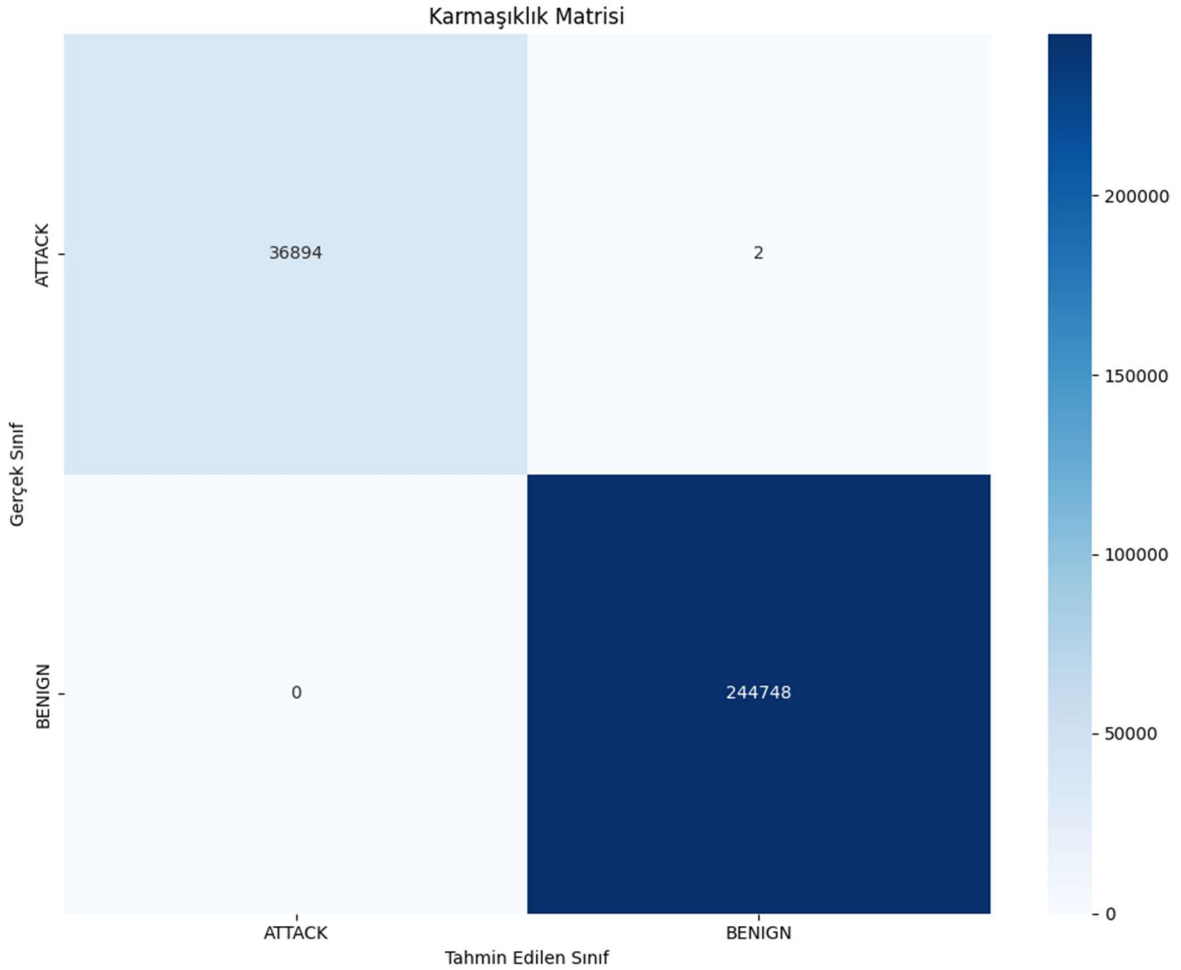
Şekil.3.29. İkili tabandaki veri setinin altılı sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



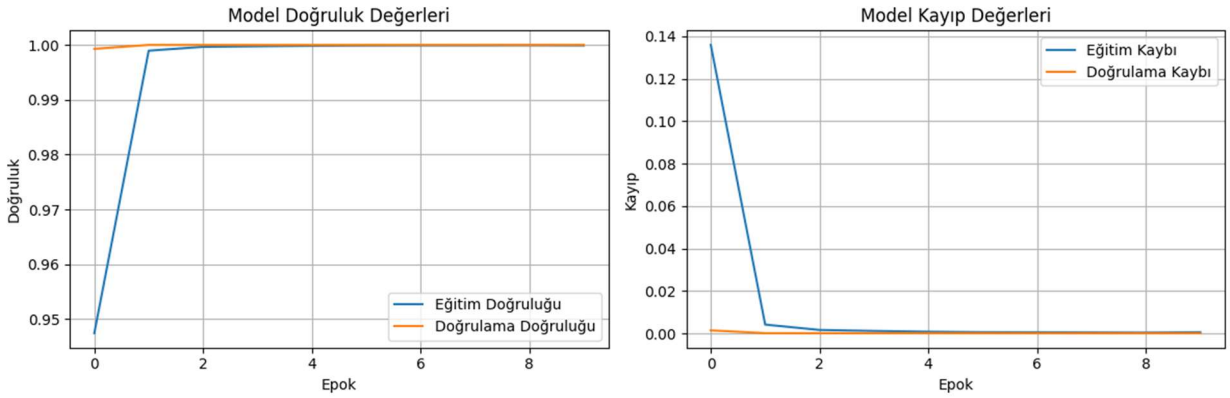
Şekil.3.30. İkili tabandaki veri setinin altılı sınıflandırma testinin karmaşıklık matrisi



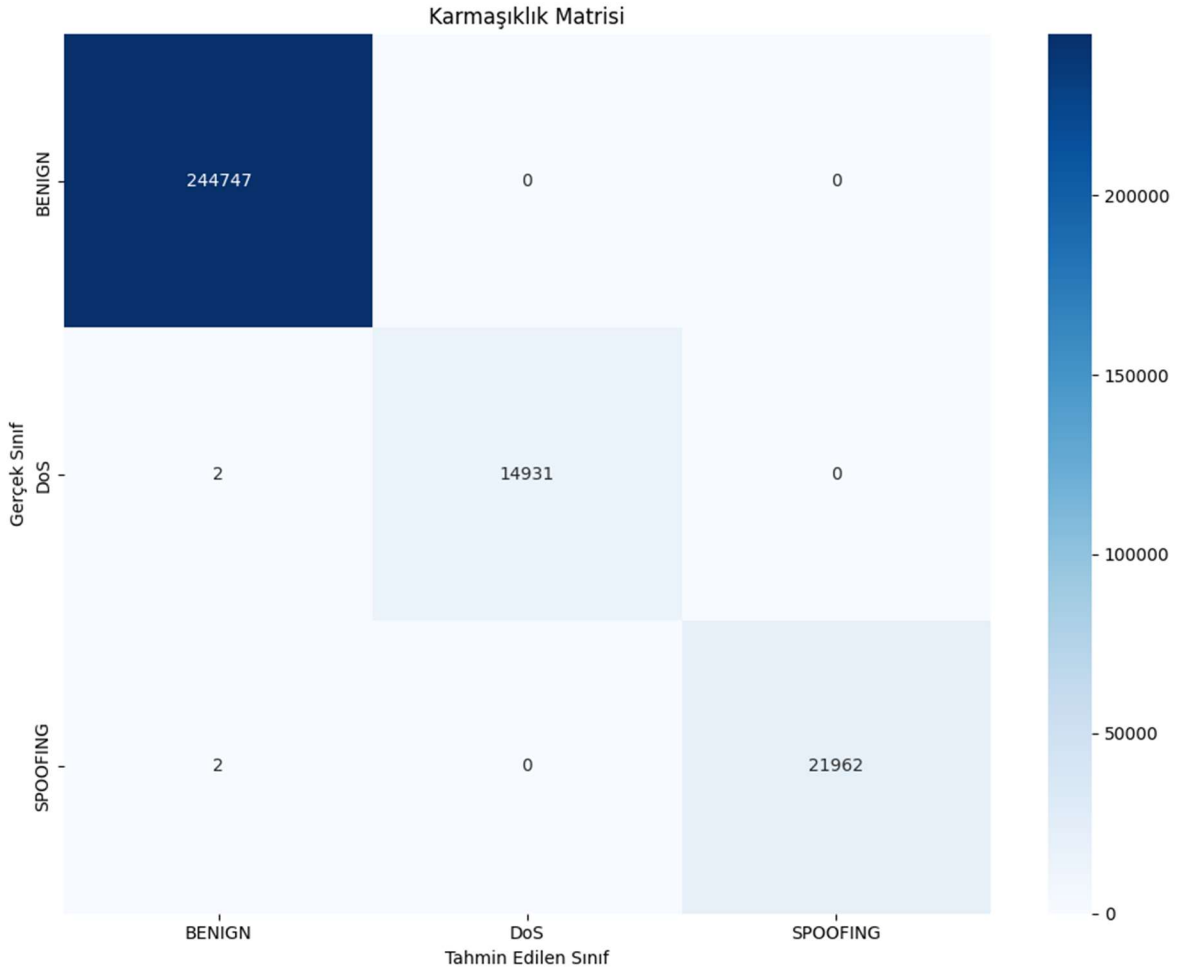
Şekil.3.31. Onluk tabandaki veri setinin ikili sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



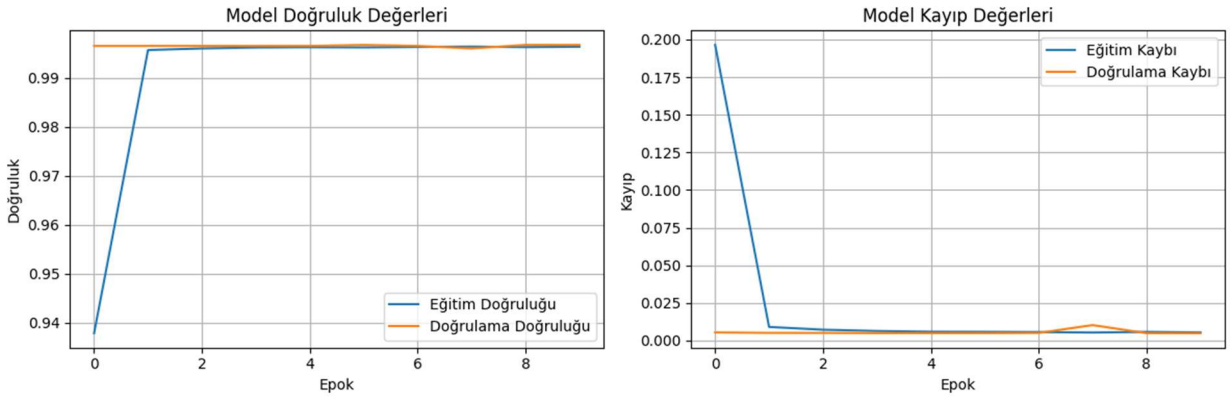
Şekil.3.32. Onluk tabandaki veri setinin ikili sınıflandırma testinin karmaşıklık matrisi



Şekil.3.33. Onluk tabandaki veri setinin üçlü sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



Şekil.3.34. Onluk tabandaki veri setinin üçlü sınıflandırma testinin karmaşıklık matrisi



Şekil.3.35. Onluk tabandaki veri setinin altılı sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



Şekil.3.36. Onluk tabandaki veri setinin altılı sınıflandırma testinin karmaşıklık matrisi

3.2. CICIoMT2024 Deney Sonuçları

CICIoMT2024 veri seti üstünde yapılan tüm deneysel çalışmaların sonuçları Tablo 3.2'de ayrıntılı olarak gösterilmiştir. Yapılan deneylerde önerilen CNN, DNN ve LSTM modellerinin her biri için sınıflandırma yöntemleri eğitilmiş ve test edilmiştir. Tüm modeller ikili, altılı ve on dokuzlu sınıflandırma işlemleri için doğruluk, kesinlik, duyarlılık ve F1-skoru yönünden performans metrikleri yönünden değerlendirilmiştir.

İkili sınıflandırma deneylerinde, önerilen tüm modeller oldukça yüksek ve başarılı performans göstermektedir. Deneyde kullanılan CNN, DNN ve LSTM modelleri, tüm performans metriklerinde mükemmele yakın bir başarı elde etmiştir. Bu sonuçla, bu veri setindeki ikili sınıflandırma deneyinde model seçiminin kritik bir faktör olmadığını ve tüm modellerin problemi neredeyse aynı başarıyla çözebildiği gözlenmektedir.

Altılı sınıflandırmada deneylerinde, önerilen tüm modeller arasında küçük performans farklılıkları görülmektedir. Deneyde kullanılan LSTM modeli, F1-skoru açısından en iyi başarılı modeli gösterirken, bunu sırasıyla DNN modeli ve CNN modeli takip etmiştir. Deneyde kullanılan LSTM modelinin daha fazla başarı oranıyla duyarlılık ve kesinlik performans metriklerinde diğer modellere göre daha başarılı bir performans göstermesi, önerilen LSTM modelinin sıralı veri yapılarını işlemedeki üstünlüğünü göstermektedir.

On dokuzlu sınıflandırma deneylerinde ise, önerilen tüm modeller benzer performans seviyelerinde kalmıştır. CNN ve DNN modelleri 0.71'lik F1-skoru elde etmiş ve LSTM modeli de aynı seviyede performans göstermiştir. Karşılaşılan bu durum, veri setindeki sınıf örneklerinin sayısının dengesiz dağılması ve artan sınıf sayısının getirdiği karmaşıklıktan kaynaklanmaktadır. Bu durumun, model mimarisine bakılmaksızın sınıflandırma başarısını olumsuz bir şekilde etkilediğini göstermektedir.

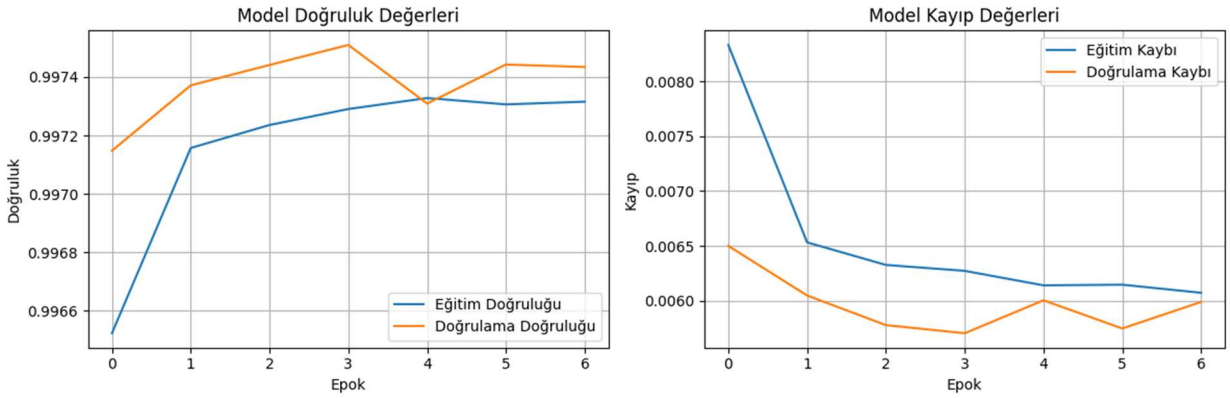
Son olarak genel bir performans değerlendirilmesi yapıldığında, önerilen tüm modeller basit sınıflandırma görevlerinde son derece yüksek başarı sağlarken, sınıf sayısı arttıkça performansta düşüş görülmektedir. Deneyde kullanılan LSTM modelinin özellikle altılı sınıflandırma deneyinde gösterdiği diğer modellere görece üstün performans, genellemeleri yakalama kabiliyetinin bu tür orta karmaşıklıktaki görevlerde avantaj sağladığını göstermektedir.

Tablo 3.2. CICIoMT2024 veri setinin deney sonuçları.

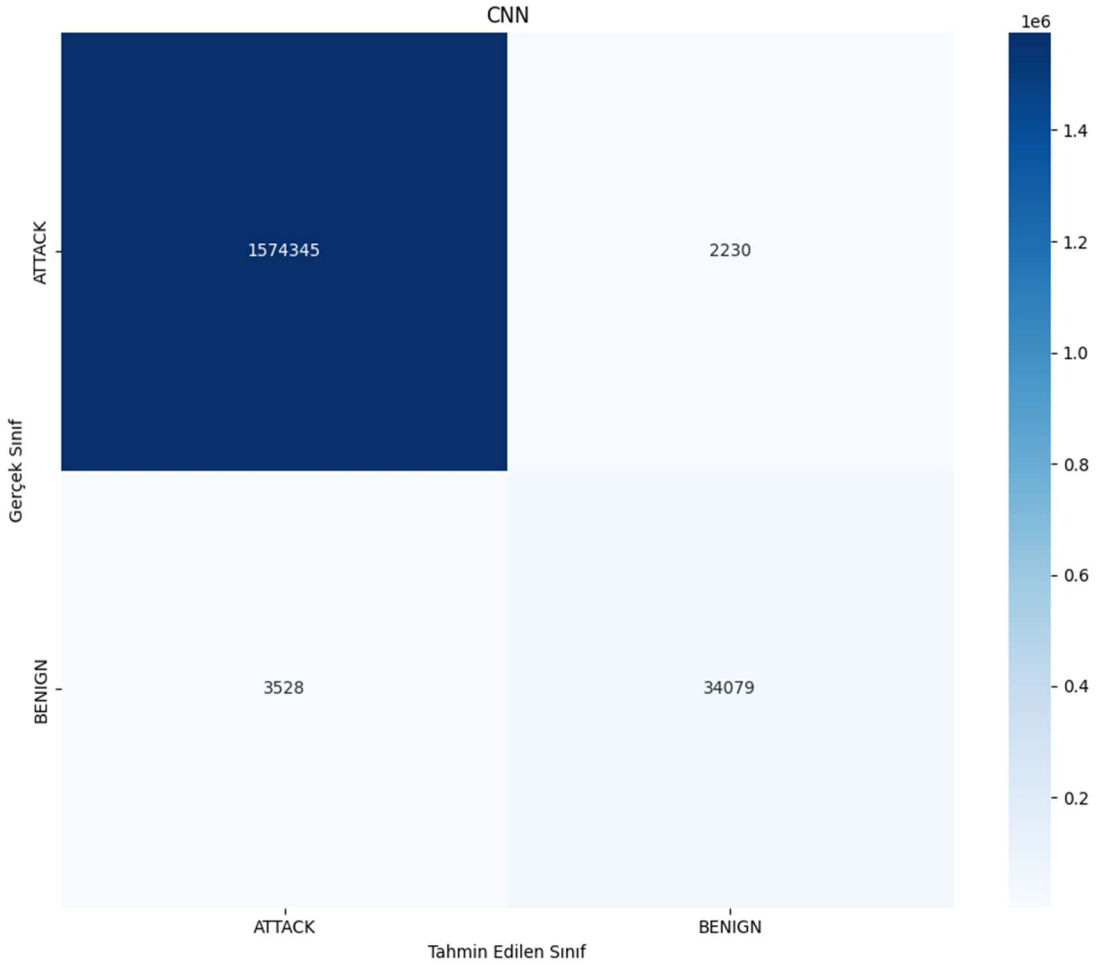
Model	Sınıflandırma	Performans Metrikleri (%)			
		Doğruluk	**Kesinlik**	**Duyarlılık**	**F1-Skor**
CNN	**İkili**	0.99	0.99	0.99	0.99
	Altılı	0.78	0.77	0.77	0.72
	On Dokuzlu	0.77	0.74	0.77	0.71
DNN	**İkili**	0.99	0.99	0.99	0.99
	Altılı	0.78	0.77	0.77	0.75
	On Dokuzlu	0.77	0.75	0.77	0.71
LSTM	**İkili**	0.99	0.99	0.99	0.99
	Altılı	0.79	0.78	0.79	0.76
	On Dokuzlu	0.78	0.71	0.78	0.71

3.2.1 CNN Modeli Sonuçları

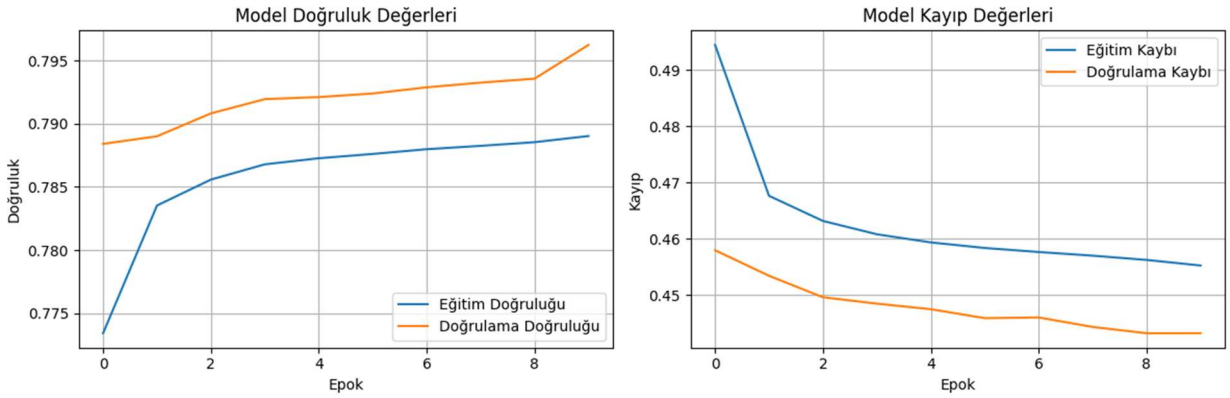
Önerilen CNN modeli, CICIoMT2024 veri setinde özellikle ikili sınıflandırma deneylerinde yüksek başarı sağlamıştır. Ancak veri setinin dengesiz dağılımından ve sınıf sayısının fazlalığından altılı ve on dokuzlu sınıflandırma deneylerinde bir miktar doğruluk metriğinde düşüş gözlenmektedir. Aşağıdaki şekillerde önerilen modelin doğruluk, kayıp grafikleri ve karmaşıklık matrisi gösterilmektedir.



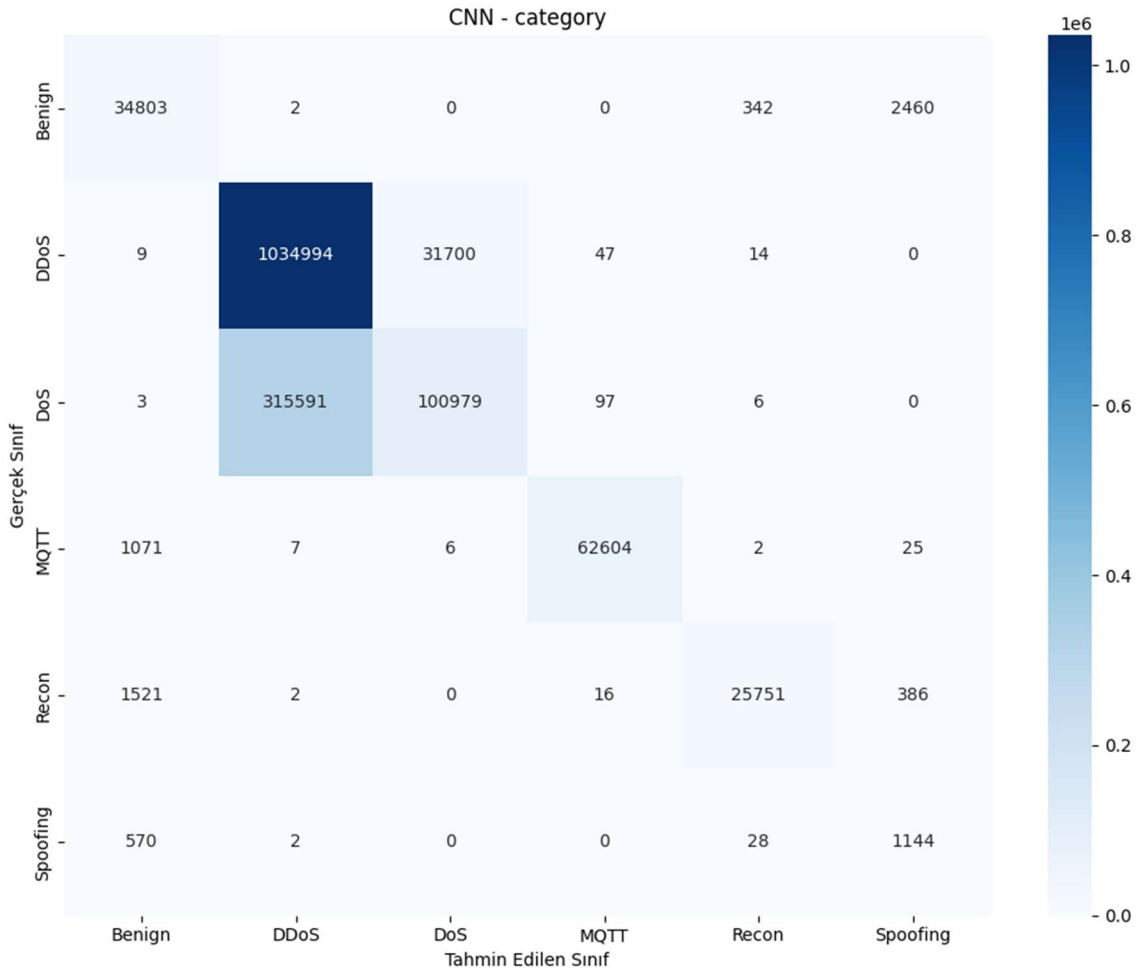
Şekil.3.37. İkili sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



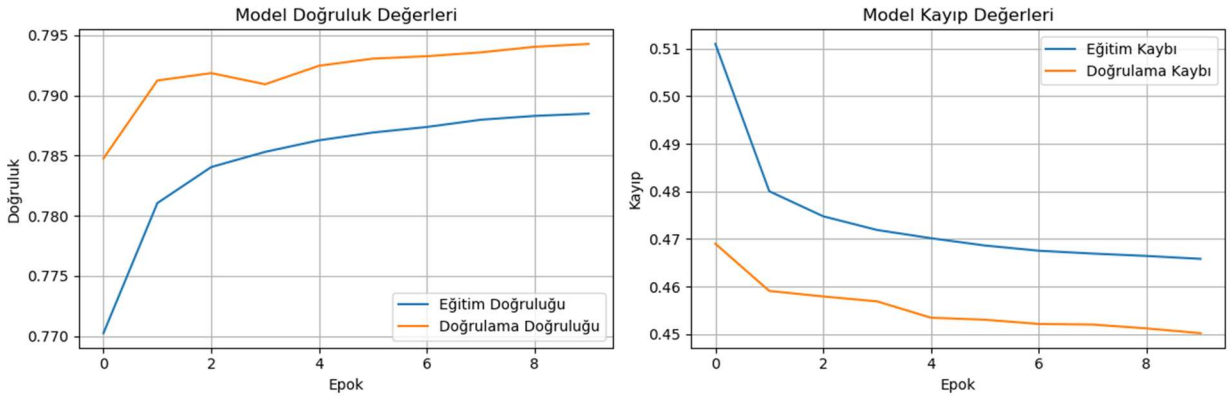
Şekil.3.38. İkili sınıflandırma testinin karmaşıklık matrisi



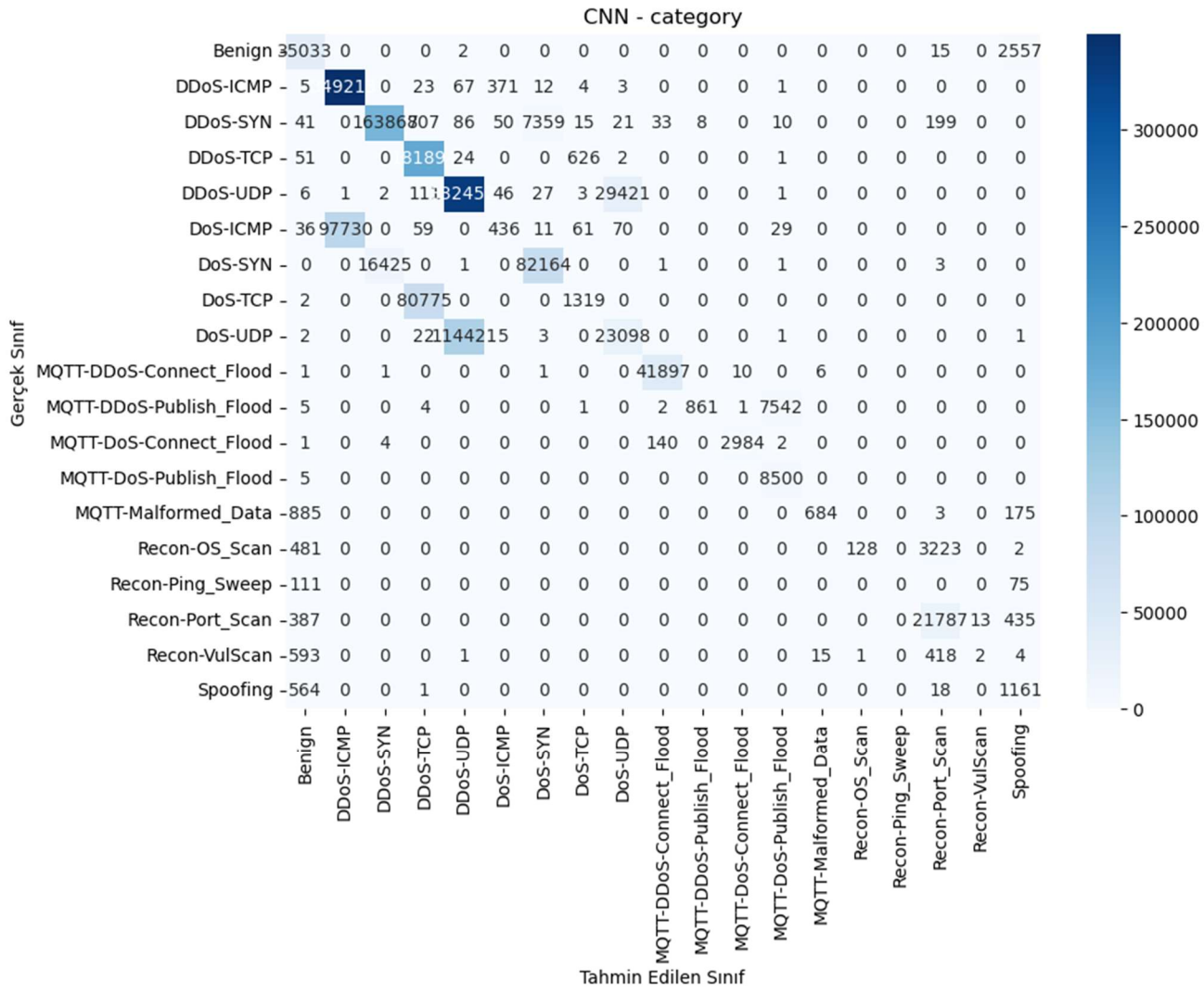
Şekil.3.39. Altılı sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



Şekil.3.40. Altılı sınıflandırma testinin karmaşıklık matrisi



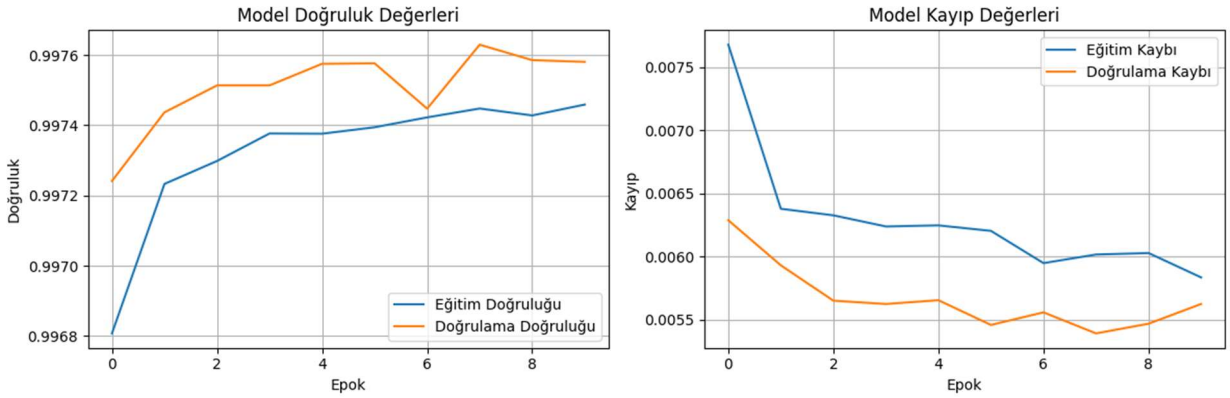
Şekil.3.41. On dokuzlu sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



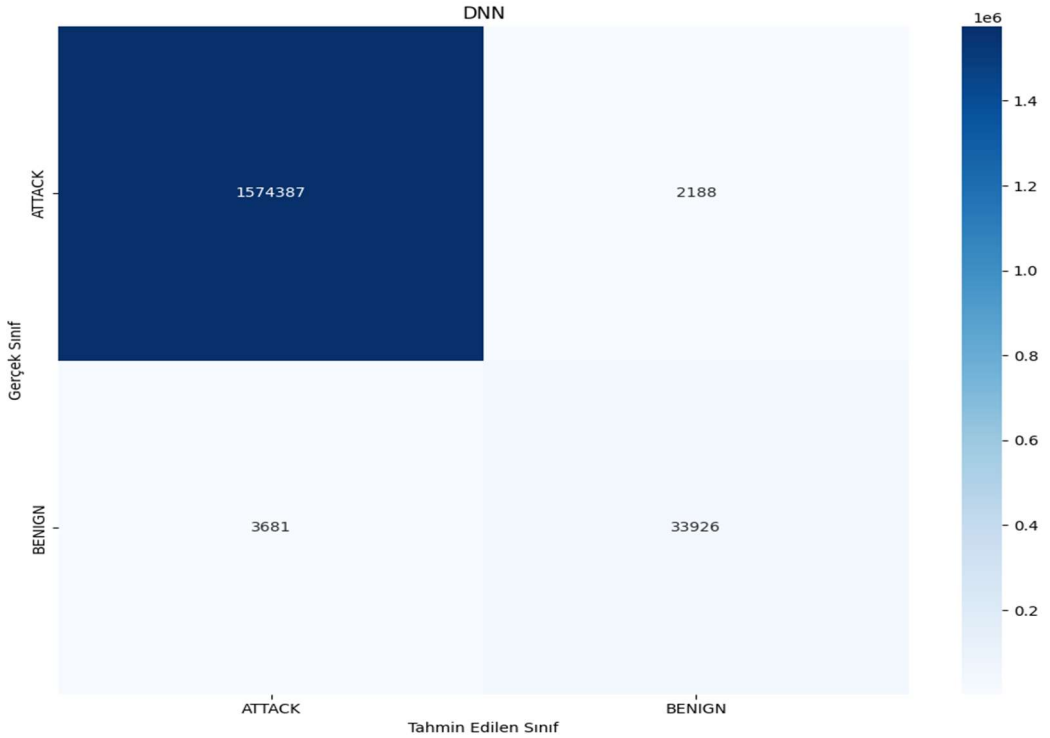
Şekil.3.42. On dokuzlu sınıflandırma testinin karmaşıklık matrisi

3.2.2 DNN Modeli Sonuçları

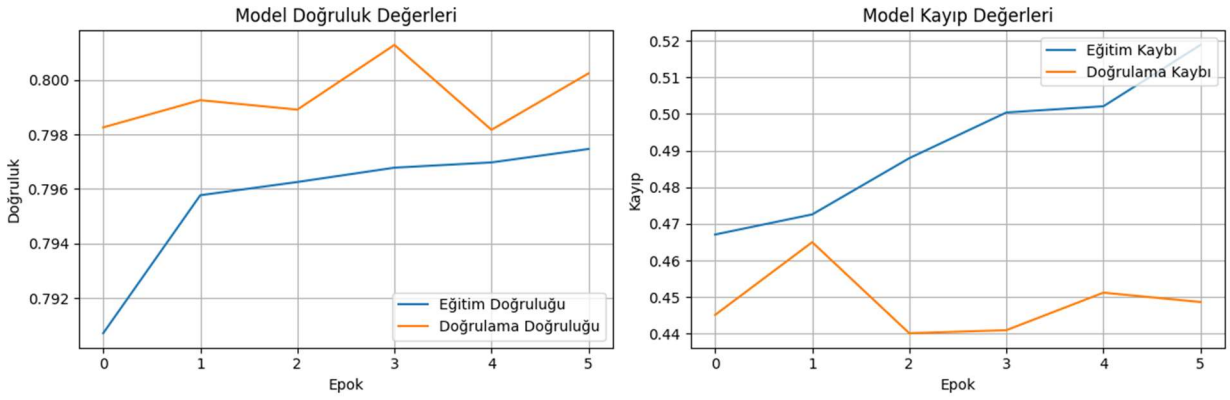
Önerilen DNN modeli, CICIoMT2024 veri setinde özellikle ikili sınıflandırma deneylerinde yüksek başarı sağlamıştır. Ancak veri setinin dengesiz dağılımından ve sınıf sayısının fazlalığından altılı ve on dokuzlu sınıflandırma deneylerinde bir miktar doğruluk metriğinde düşüş gözlenmektedir. Aşağıdaki şekillerde önerilen modelin doğruluk, kayıp grafikleri ve karmaşıklık matrisi gösterilmektedir.



Şekil.3.43. İkili sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



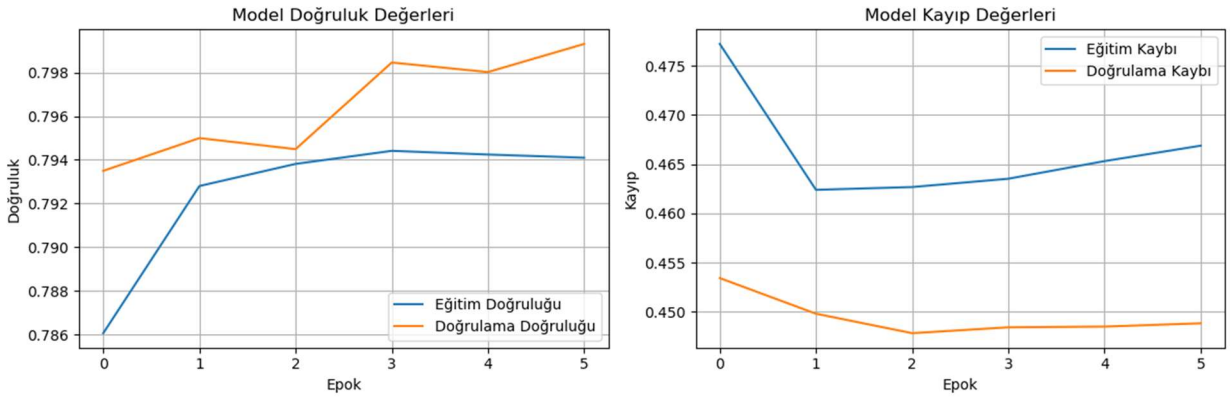
Şekil.3.44. İkili sınıflandırma testinin karmaşıklık matrisi



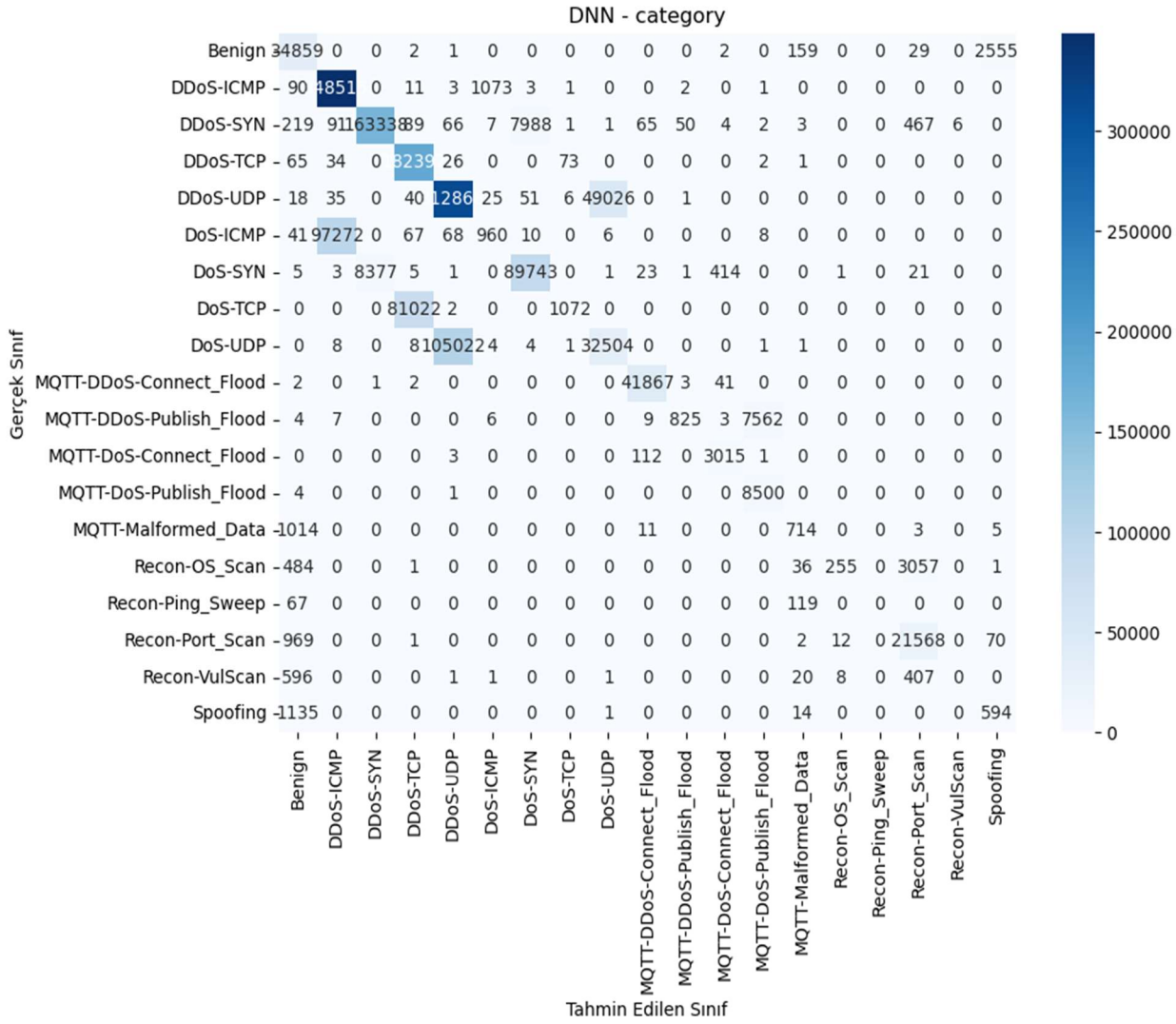
Şekil.3.45. Altılı sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



Şekil.3.46. Altılı sınıflandırma testinin karmaşıklık matrisi



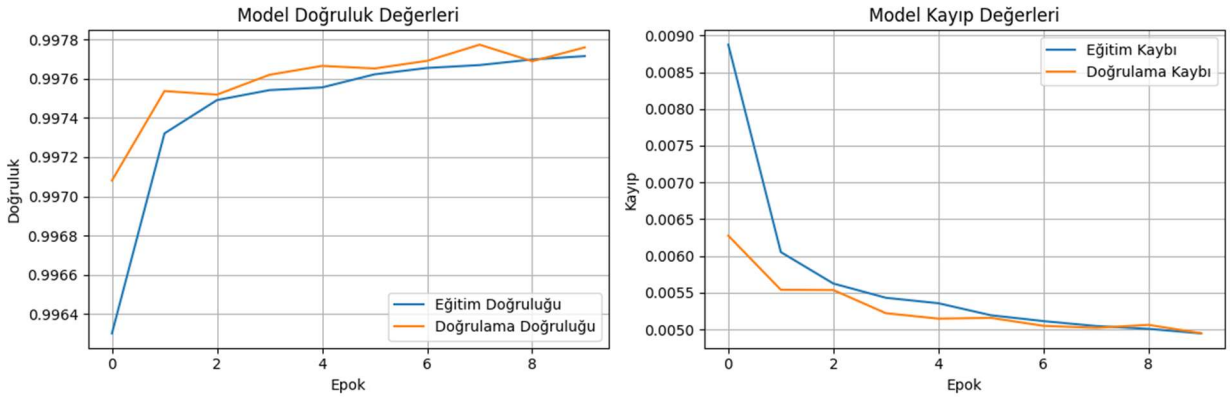
Şekil.3.47. On dokuzlu sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



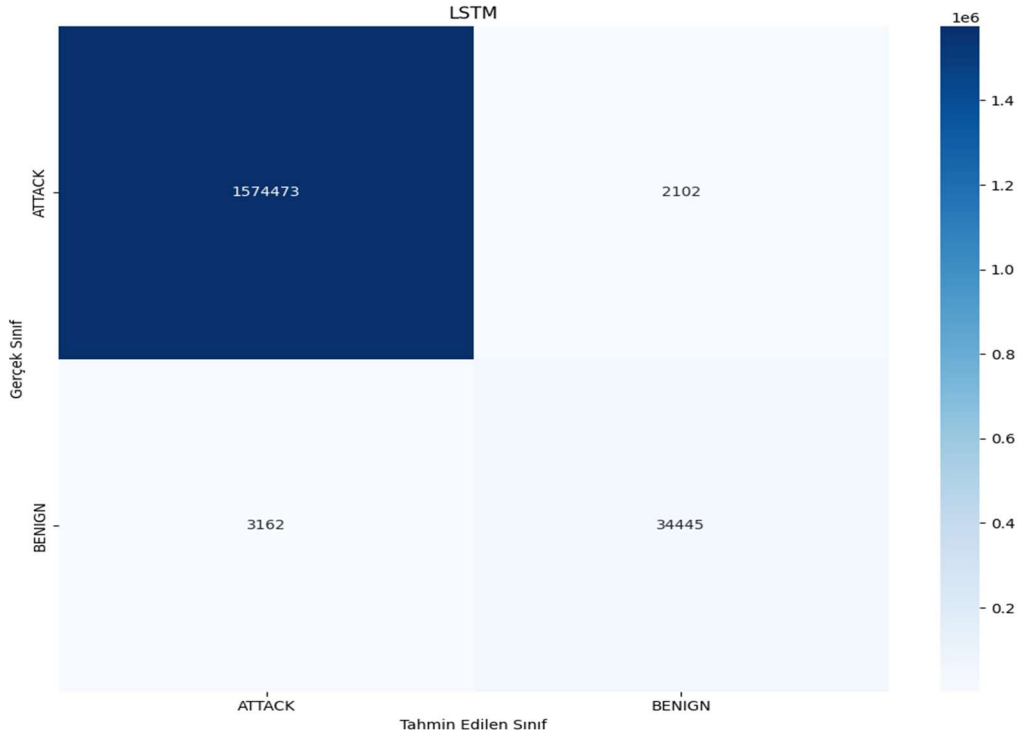
Şekil.3.48. On dokuzlu sınıflandırma testinin karmaşıklık matrisi

3.2.3 LSTM Modeli Sonuçları

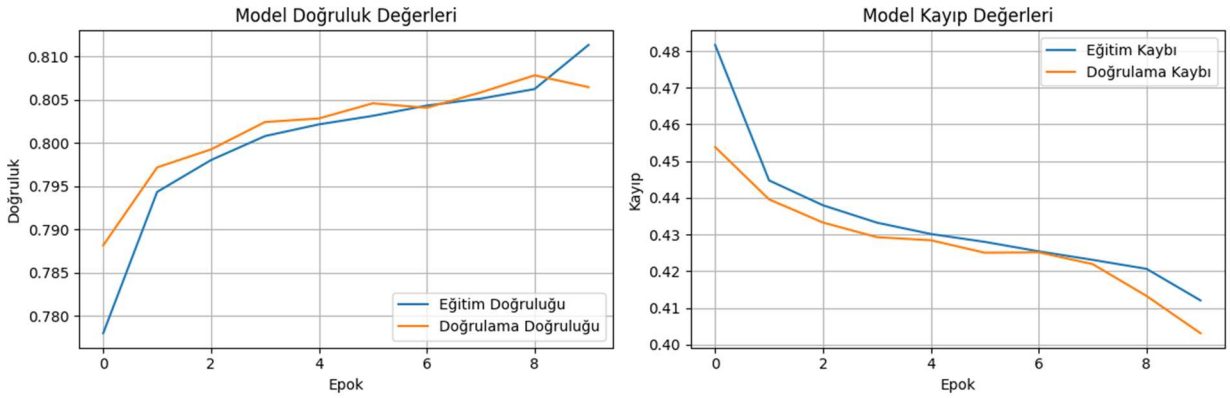
Önerilen LSTM modeli, CICIoMT2024 veri setinde özellikle ikili sınıflandırma deneylerinde yüksek başarı sağlamıştır. Ancak veri setinin dengesiz dağılımından ve sınıf sayısının fazlalığından altılı ve on dokuzlu sınıflandırma deneylerinde bir miktar doğruluk metriğinde düşüş gözlenmektedir. Aşağıdaki şekillerde önerilen modelin doğruluk, kayıp grafikleri ve karmaşıklık matrisi gösterilmektedir.



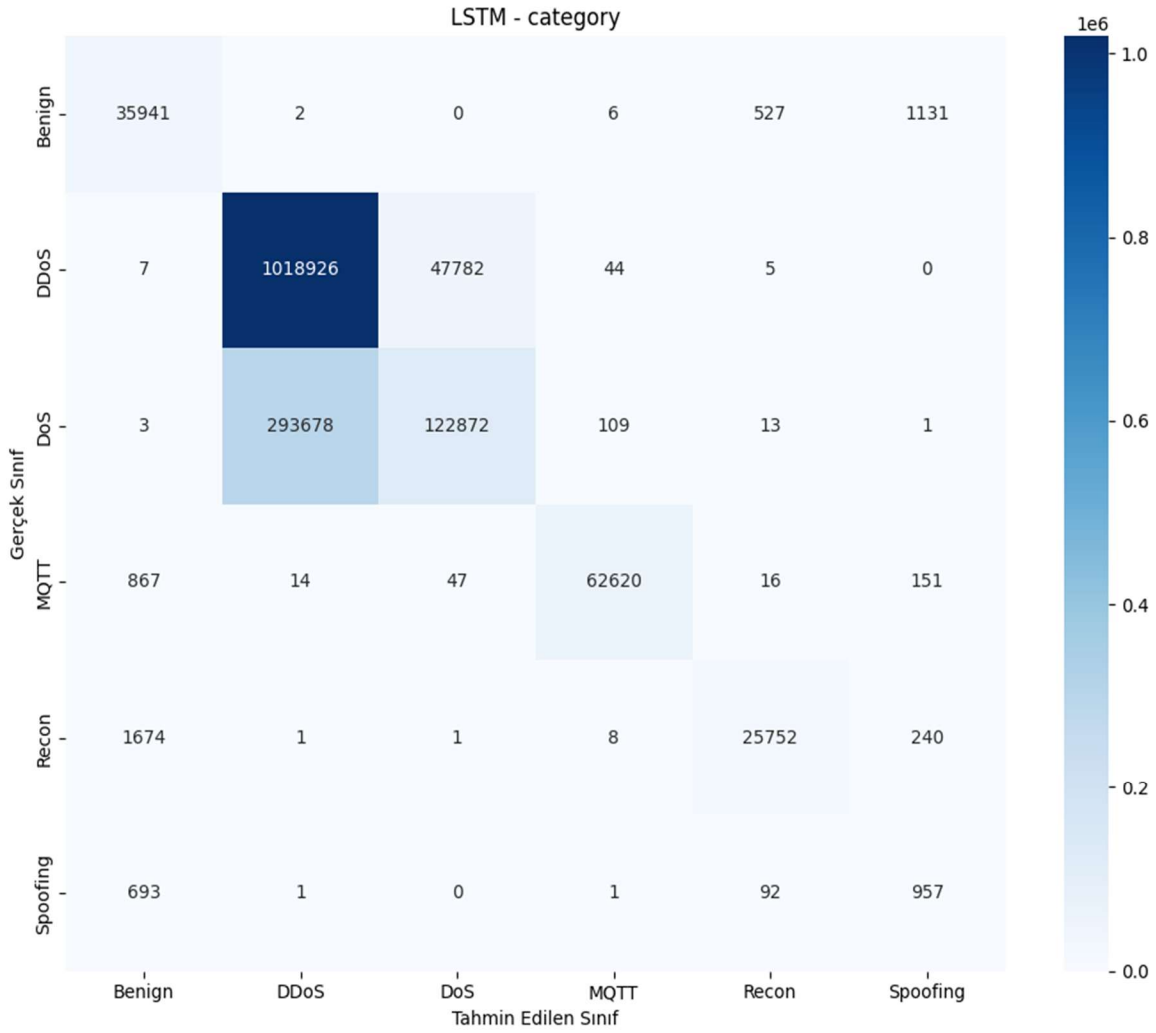
Şekil.3.49. İkili sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



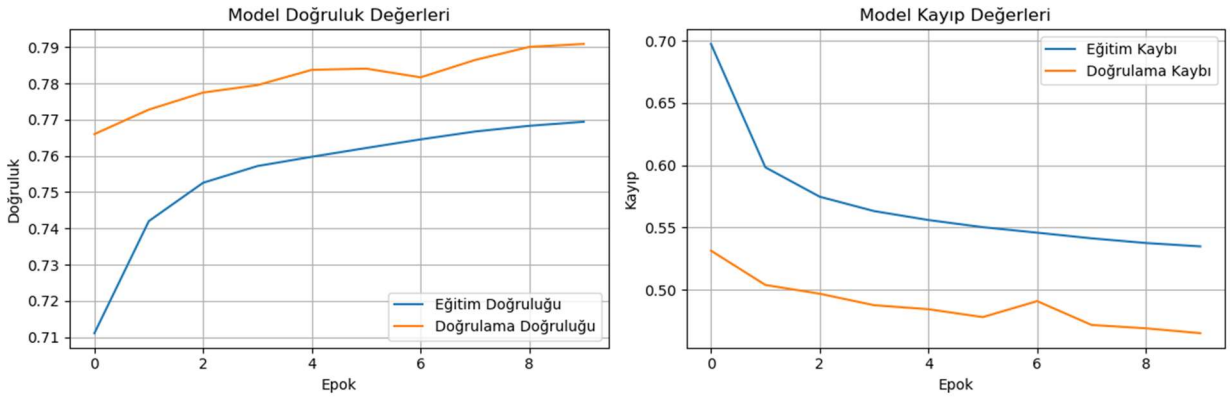
Şekil.3.50. İkili sınıflandırma testinin karmaşıklık matrisi



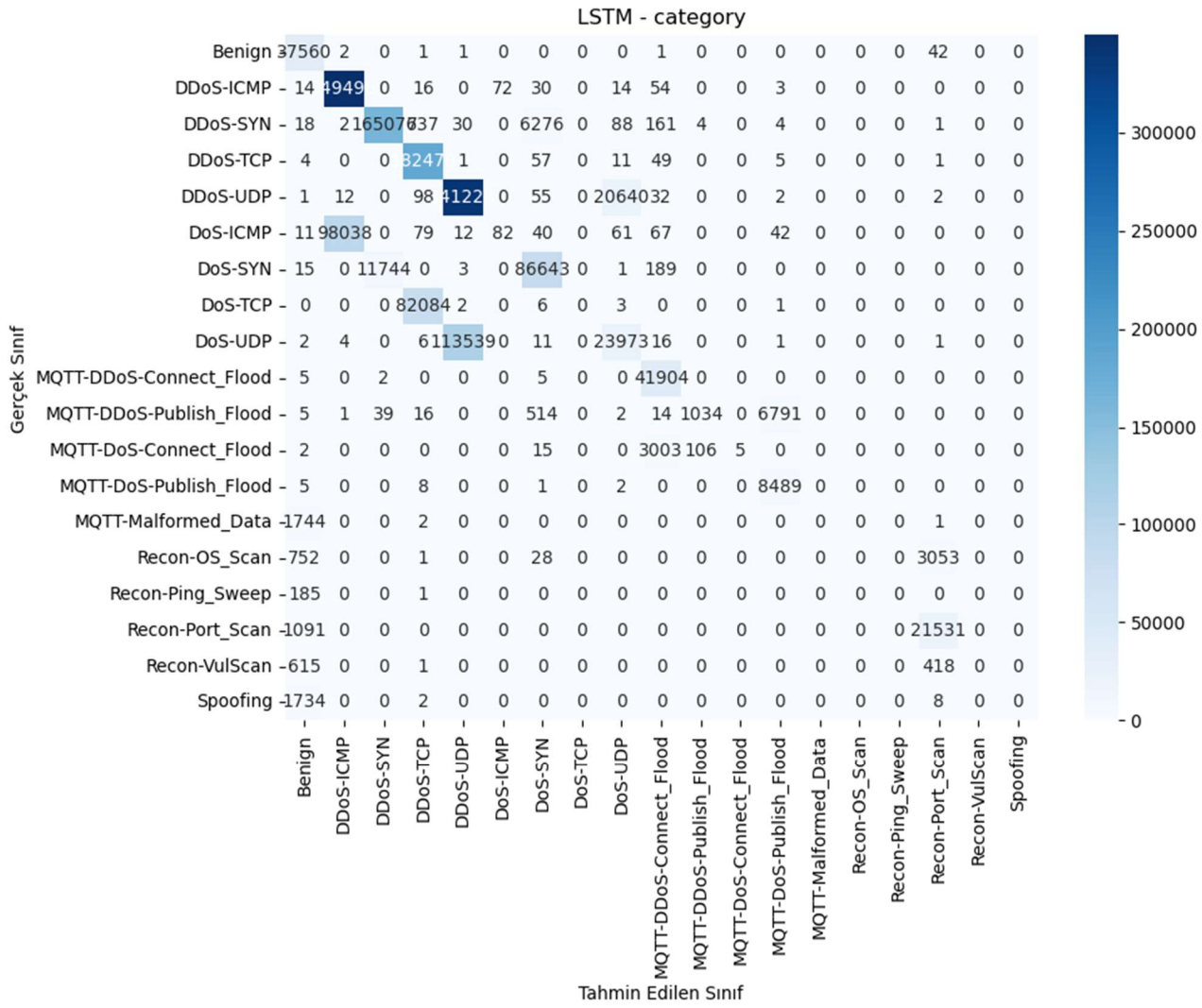
Şekil.3.51. Altılı sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



Şekil.3.52. Altılı sınıflandırma testinin karmaşıklık matrisi



Şekil.3.53. On dokuzlu sınıflandırma eğitiminin doğruluk ve kayıp grafikleri



Şekil.3.54. On dokuzlu sınıflandırma testinin karmaşıklık matrisi

3.3. Literatürdeki Sonuçlarla Karşılaştırma

3.3.1 CICIoV2024 Veri Seti

CICIoV2024 veri setinin oluşturulduğu çalışmada [21], derin öğrenme tekniklerinden sadece DNN modeli üzerinde ikili, üçlü ve altılı sınıflandırma yaptığı gözlenmektedir. Tablo 3.3'te bahsedilen çalışma ve önerilen modellerdeki sonuçlar gösterilmiştir.

Tablo 3.3. CICIoV2024 veri seti üzerinde yapılan çalışma ile önerilen modeli karşılaştırma.

Model	Sınıflandırma	Veri Formatı (Taban)	Performans Metrikleri (%)			
			Doğruluk	Kesinlik	Duyarlılık	F1-Skor
Neto ve ark. [21]	İkili	İkili	1	1	1	1
		Onlu	0.98	0.99	0.93	0.95
	Üçlü	İkili	1	1	1	1
		Onlu	0.95	0.99	0.85	0.90
	Altılı	İkili	0.95	0.74	0.68	0.63
		Onlu	0.96	0.83	0.76	0.78
Önerilen model	İkili	İkili	1	1	1	1
		Onlu	1	1	1	1
	Üçlü	İkili	1	1	1	1
		Onlu	1	1	1	1
	Altılı	İkili	0.99	0.97	0.98	0.98
		Onlu	0.99	0.99	0.96	0.97

CICIoV2024 veri seti üzerinde yapılan karşılaştırmalı analiz sonuçları, önerilen modelin literatürdeki mevcut çalışmaya göre önemli bir performans artışı sağladığını göstermektedir. Neto

ve ark. [21] tarafından sunulan DNN modeli ile önerilen model arasındaki en önemli fark, özellikle üçlü ve altılı sınıflandırma deneylerinde görülmektedir.

İkili sınıflandırma deneylerinde iki model de, benzer ve yüksek sonuçları vermiş olsa da, önerilen model üçlü ve altılı sınıflandırma deneylerinde daha başarılı performans göstermiştir. Özellikle altılı sınıflandırmadaki performans metriğindeki farklar, önerilen modelin daha karmaşık sınıflandırma deneylerinde bile literatürdeki çalışmaya göre daha tutarlı olduğunu ve yüksek performansa sahip olduğunu göstermektedir.

Bu tez çalışmasında değerlendirmelerde kullandığımız duyarlılık performans metriğinde ise, özellikle altılı sınıflandırmada önerilen model çok daha başarılı sonuç elde etmiştir. Bundan dolayı önerilen model, özellikle çok sınıflı sınıflandırma görevlerinde daha güçlü ve genellenebilir yapıya sahip olduğunu göstermiştir.

3.3.2 CICIoMT2024 Veri Seti

CICIoMT2024 veri setinin oluşturulduğu çalışmada [22], derin öğrenme tekniklerinden sadece DNN modeli üzerinde ikili, altılı ve on dokuzlu sınıflandırma yaptığı gözlenmektedir. Tablo 3.4.'te bahsedilen çalışma ve önerilen modellerdeki sonuçlar gösterilmiştir.

Tablo 3.4. CICIoMT2024 veri seti üzerinde yapılan çalışma ile önerilen modeli karşılaştırma

Model	**Sınıflandırma**	**Performans Metrikleri (%)**			
		Doğruluk	**Kesinlik**	**Duyarlılık**	**F1-Skor**
Dadkhah ve ark. [22]	**İkili**	0.99	0.96	0.95	0.95
	Altılı	0.73	0.73	0.69	0.67
	On Dokuzlu	0.72	0.65	0.55	0.53
Önerilen model	**İkili**	0.99	0.99	0.99	0.99
	Altılı	0.78	0.77	0.77	0.75
	On Dokuzlu	0.77	0.75	0.77	0.71

CICIoMT2024 veri seti üzerinde yapılan önerilen model ile literatür çalışması arasındaki karşılaştırmalı değerlendirme, önerilen modelin literatürdeki çalışmaya göre genel olarak daha başarılı bir performans ortaya koyduğunu göstermektedir. Dadkhah ve ark. [22] tarafından sunulan DNN modeli ile önerilen model arasındaki performans farklılıkları, sınıf sayısı arttıkça daha çok belirginleşmektedir.

İkili sınıflandırma deneyinde her iki model de yüksek performans göstermiştir. Bununla birlikte önerilen model tüm performans metriklerinde küçük bir iyileşme sağlamıştır. Altılı sınıflandırma senaryosunda, önerilmiş modelin F1-skoru ile literatür çalışmasındaki önerilen modelin F1-skoru arasında yaklaşık 0.08'lik bir puan artışı gözlemlenmiştir.

On dokuzlu sınıflandırma deneyinde ise önerilen model, Dadkhah ve ark.'nın [22] çalışmasındaki önerilmiş modelden önemli ölçüde daha iyi performans göstererek 0.71'lik bir F1-skoru elde etmiştir. Veri setindeki sınıfların örnek sayısının dengesiz dağılımı göz önüne alındığında, bu performans artışı özellikle dikkat çekmektedir. Kullanılan veri setindeki bazı sınıf örneklerinin diğerlerine göre çok daha az sayıda örneğe sahip olmasından dolayı, özellikle çok sınıflı deneylerde sınıflandırma performansını olumsuz etkilenmiştir. Buna rağmen önerilen model, veri dengesizliği probleminin üstesinden literatürdeki çalışmaya göre daha iyi gelerek literatürdeki çalışmadan daha iyi performans metriği sonuçları almayı sağlamıştır. Bu durum, modelin sınıf dengesizliği gibi gerçek dünya problemlerinde literatür çalışmasındaki önerilmiş modelden daha etkili sınıf tespiti yapabildiğini göstermektedir.

Bu tez çalışmasının değerlendirilmesinde kullanılan performans metriklerinden duyarlılık ve kesinlik metrikleri açısından benzer bir artış durumu gözlemlenmekte olup, bu da önerilen modelin veri setindeki dengesizliğe rağmen, sınıf sayısı arttıkça dahi tutarlı sonuçlar üretebildiğini göstermektedir. Bu sonuçlarla birlikte, önerilen modelin özellikle dengesiz veri dağılımına sahip, yüksek karmaşıklıktaki çok sınıflı sınıflandırma deneylerinde literatürdeki önerilmiş modele göre daha güçlü ve etkili olduğunu göstermektedir.

4.SONUÇLAR

Yapılan bu tez çalışmasında, IoV ve IoMT sistemlerinin güvenliğini sağlamak ve geliştirme üzere derin öğrenme mimarisi tabanlı üç farklı model (CNN, DNN ve LSTM) önerilmiş ve iki farklı CICIoV2024 ve CICIoMT2024 veri setleri üzerinde son derece kapsamlı deneylerle testi sağlanmıştır. Önerilen modellerin yaklaşımlarının hem ikili hem de çok sınıflı saldırı tespitinde yüksek başarı sağladığını yapılan deneysel çalışmalar göstermektedir.

İlk veri seti olan CICIoV2024 üzerinde gerçekleştirilen deneylerde, tez çalışmasında önerilen tüm modeller ikili ve üçlü sınıflandırma deneylerinde %100'e yakın doğruluk ve F1-skoru elde etmiştir. Elde edilen bu sonuçlar, modellerin normal ve saldırı trafiğini ayırt etmede son derece başarılı olduğunu göstermektedir. Altılı sınıflandırma deneyinde ise modeller %96-99 arasında doğruluk oranlarına ulaşmıştır. Özellikle önerilen modelimizle karşılaştırdığımız literatürdeki Neto ve ark. [21] çalışmasına kıyasla, önerilen modeller önemli bir performans artışı göstermiştir. Örnek olarak, altılı sınıflandırma deneyi sonucu olarak literatürdeki %78'lik F1-skoru, önerilen modellerle %98'e kadar yükseltilmiştir. Bu başarıda, önerilen modelin hiper parametre optimizasyonunun önemli katkısı olmuştur.

Bir diğer veri seti olan CICIoMT2024 üzerindeki deneylerde ise, ikili sınıflandırma deneylerinde önerilen tüm modeller %99 doğruluk oranına ulaşmıştır. Altılı sınıflandırma deneyinde ise %75-76, on dokuzlu sınıflandırma deneyinde ise %71 F1-skoru elde edilmiştir. Alından bu sonuçlarla, Dadkhah ve ark. [22] çalışmasına kıyasla belirgin bir iyileşme sağladığı görülmektedir. LSTM modeli özellikle, mimarisi gereği uzun vadeli bağımlılıkları yakalama yeteneği sayesinde karmaşık saldırı desenlerini genelleştirmede ve tespit etmede daha başarılı olmuştur. Veri setindeki sınıf dengesizliği problemi, özellikle çoklu sınıflandırma deneylerinde genel olarak modellerin başarısını olumsuz yönde etkilemiştir.

Bu tez çalışmasındaki deneylerin başarısını arttırmak için, gelecek çalışmalar için şu öneriler sunulabilir:

1. Model Optimizasyonu:
    - Yapay zeka modellerinin daha hızlı çalışması için, modeli küçültme ve önemli olmayan kısımları ayıklama teknikleri uygulanabilir.

- Model içindeki sayısal değerleri basitleştirme ve sıkıştırma teknikleriyle, bellek ve işlemci gibi kaynakların kullanımı iyileştirilebilir.
- Otomatik makine öğrenmesi yaklaşımları kullanılarak hiper parametre optimizasyonu otomatikleştirilebilir.

2. Veri İyileştirme:
    - SMOTE gibi gelişmiş veri dengeleme teknikleri kullanılabilir.
    - Veri çoğaltma işlemi için çekişmeli üretici ağlar temelli yöntemler geliştirilebilir.
    - Öznitelik çıkarma ve seçme işlemleri için otomatik yöntemler denenebilir.
3. Model Yorumlanabilirliği:
    - SHAP yöntemi gibi XAI teknikleri entegre edilebilir.
    - Saldırı tespitinde hangi özelliklerin daha belirleyici olduğunu anlamak için önem derecesi analizi gerçekleştirilebilir.
    - Sistemin nasıl karar verdiğini anlaşılır kılmak için, kararların dayandığı kuralları belirleyen teknikler sisteme dahil edilebilir.
4. Genelleştirme ve Adaptasyon:
    - Transfer öğrenme teknikleriyle farklı IoT uygulamalarına adaptasyon sağlanabilir.
    - Sürekli öğrenme stratejileri ile modeller güncellenebilir.
5. Güvenlik ve Mahremiyet:
    - İş birlikçi öğrenme yöntemiyle, verilerin farklı noktalarda kalmasına ve gizliliğin korunmasına olanak sağlayan bir eğitim süreci oluşturulabilir.
    - Kişisel verilerin korunması için, verilere kontrollü miktarda gürültü ekleyen özel gizlilik koruma teknikleri uygulanabilir.

Bu tez çalışması, IoV ve IoMT sistemlerinin siber güvenliğini artırmak için etkili ve ölçeklenebilir çözümler sunmaktadır. Önerilen derin öğrenme modelleri, gerçek dünya uygulamalarında kullanılabilecek yüksek doğruluk ve güvenilirlik seviyelerine ulaşmıştır. Gelecekte yapılacak çalışmalarla, bu modellerin performansı ve kullanılabilirliği daha da artırılabilir.

KAYNAKLAR

[1] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer Networks, 54(15), 2787-2805.

[2] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660.

[3] Jeschke, S., Brecher, C., Meisen, T., Özdemir, D., & Eschert, T. (2017). Industrial internet of things and cyber manufacturing systems. In Industrial Internet of Things (pp. 3-19). Springer, Cham.

[4] Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The internet of things for health care: A comprehensive survey. IEEE Access, 3, 678-708.

[5] Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the internet of things: A review. 2012 International Conference on Computer Science and Electronics Engineering (Vol. 3, pp. 648-651).

[6] Sajid, A., Abbas, H., & Saleem, K. (2016). Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. IEEE Access, 4, 1375-1384.

[7] Wen, Q., Dong, X., & Zhang, R. (2012). Application of dynamic variable cipher security certificate in internet of things. In 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems (Vol. 3, pp. 1062-1066).

[8] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125-1142.

[9] Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 38, 8-27.

[10] Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. IEEE Communications Surveys & Tutorials, 22(3), 1646-1685.

[11] Gerla, M., Lee, E. K., Pau, G., & Lee, U. (2014). Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. In 2014 IEEE World Forum on Internet of Things (WF-IoT) (pp. 241-246).

[12] Parkinson, S., Ward, P., Wilson, K., & Miller, J. (2017). Cyber threats facing autonomous and connected vehicles: Future challenges. IEEE Transactions on Intelligent Transportation Systems, 18(11), 2898-2915.

[13] Moosavi, S. R., Gia, T. N., Rahmani, A. M., Nigussie, E., Virtanen, S., Isoaho, J., & Tenhunen, H. (2015). SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. Procedia Computer Science, 52, 452-459.

[14] Vijayakumar, P., Azees, M., Kannan, A., & Deborah, L. J. (2016). Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks. IEEE Transactions on Intelligent Transportation Systems, 17(4), 1015-1028

[15] Hajar, M. S., Al-Kadri, M. O., & Kalutarage, H. K. (2021). A survey on wireless body area networks: Architecture, security challenges and research opportunities. Computers & Security, 104, Article 102211.

[16] Wazid, M., Das, A. K., Bhat, V., & Vasilakos, A. V. (2020). LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment. Journal of Network and Computer Applications, 150, Article 102496.

[17] Avatefipour, O., & Malik, H. (2017). State-of-the-art survey on in-vehicle network communication (CAN-Bus) security and vulnerabilities. International Journal of Computer Science and Network, 6(6), 720-727.

[18] Jiang, Q., Ni, J., Ma, J., Yang, L., & Shen, X. (2018). Integrated authentication and key agreement framework for vehicular cloud computing. IEEE Network, 32(3), 28-35.

[19] Ferrag, M. A., Maglaras, L., & Ahmim, A. (2017). Privacy-preserving schemes for ad hoc social networks: A survey. IEEE Communications Surveys & Tutorials, 19(4), 3015-3045.

[20] Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2017). ProfilIoT: A machine learning approach for IoT device identification based on network traffic analysis. In Proceedings of the Symposium on Applied Computing (pp. 506-509).

[21] Neto, E. C. P., Taslimasa, H., Dadkhah, S., Iqbal, S., Xiong, P., Rahman, T., & Ghorbani, A. A. (2024). CICIoV2024: Advancing realistic IDS approaches against DoS and spoofing attack in IoV CAN bus. Internet of Things, 26, Article 101209.

[22] Dadkhah, S., Pinto Neto, E. C., Ferreira, R., Molokwu, R. C., Sadeghi, S., & Ghorbani, A. A. (2024). CICIoMT2024: A benchmark dataset for multi-protocol security assessment in IoMT. Internet of Things, 28, Article 101351.

[23] Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engineering, 2017(1), Article 9324035.

[24] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

[25] Banks, A., & Gupta, R. (2014). MQTT version 3.1.1. OASIS Standard, 29, 89.

[26] Shelby, Z., Hartke, K., & Bormann, C. (2014). The constrained application protocol (CoAP). RFC 7252.

[27] Kushalnagar, N., Montenegro, G., & Schumacher, C. (2007). IPv6 over low-power wireless personal area networks (6LoWPANs): Overview, assumptions, problem statement, and goals. RFC 4919.

[28] Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the internet of things: A survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials, 17(3), 1294-1312.

[29] Rahman, M.A., Rashid, M.M., Hossain, M.S., Hassanain, E., Alhamid, M.F., & Guizani, M. (2019). Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City. IEEE Access, 7, 18611-18621.

[30] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395-411.

[31] Ray, P. P. (2018). A survey on Internet of Things architectures. Journal of King Saud University- Computer and Information Sciences, 30(3), 291-319.

[32] Sengupta, J., Ruj, S., & Das Bit, S. (2020). A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. Journal of Network and Computer Applications, 149, Article 102481.

[33] Lynggaard, P. (2014). Artificial intelligence and Internet of Things in a “smart home” context: A Distributed System Architecture.

[34] Yan, J., Meng, Y., Lu, L., & Li, L. (2017). Industrial Big Data in an Industry 4.0 Environment: Challenges, Schemes, and Applications for Predictive Maintenance. IEEE Access, 5, 23484-23491.

[35] Dhanvijay, M. M., & Patil, S. C. (2019). Internet of Things: A survey of enabling technologies in healthcare and its applications. Computer Networks, 153, 113-131.

[36] Pham, T. N., Tsai, M. F., Nguyen, D. B., Dow, C. R., & Deng, D. J. (2015). A Cloud-Based Smart-Parking System Based on Internet-of-Things Technologies. IEEE Access, 3, 1581-1591.

[37] Clement, S., McKee, D. W., & Xu, J. (2017). Service-oriented reference architecture for smart cities. In 2017 IEEE Symposium on Service-Oriented System Engineering (SOSE) (pp. 81-85).

[38] Farooq, M. S., Riaz, S., Abid, A., Abid, K., & Naeem, M. A. (2019). A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. IEEE Access, 7, 156237-156271.

[39] J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin, D. Aharon, "The Internet of Things: Mapping the value beyond the hype," McKinsey Global Institute, 3, 2015.

[40] Statista Research Department, "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025," Statista, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide (Erişim Tarihi: 11 Kasım 2024)

[41] Sisinni, E., Saifullah, A., Han, S., Jennehag, U., & Gidlund, M. (2018). Industrial internet of things: Challenges, opportunities, and directions. IEEE Transactions on Industrial Informatics, 14(11), 4724-4734.

[42] Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2017). Evaluating critical security issues of the IoT world: Present and future challenges. IEEE Internet of Things Journal, 5(4), 2483-2495.

[43] Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015). Internet of Things: Security vulnerabilities and challenges. In 2015 IEEE Symposium on Computers and Communication (ISCC) (pp. 180-187).

[44] De Donno, M., Dragoni, N., Giaretta, A., & Spognardi, A. (2018). DDoS-capable IoT malwares: Comparative analysis and mirai investigation. Security and Communication Networks.

[45] Greenberg, A. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world (Erişim tarihi: 13 Kasım 2024).

[46] Saxena, U., Sodhi, J., & Singh, Y. (2017). Analysis of security attacks in a smart home networks. In 2017 7th International Conference on Cloud Computing, IEEE Data Science & Engineering-Confluence (pp. 431-436).

[47] 116th Congress, "S.734 - Internet of Things Cybersecurity Improvement Act of 2020," 4 Dec 2020. https://www.congress.gov/bill/116th-congress/senate-bill/734 (Erişim tarihi: 13 Kasım 2024)

[48] ETSI, ETSI EN 303 645 V2.1.1 (2020-06) - Cyber Security for Consumer Internet of Things: BaselineRequirements,2020.https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf (Erişim tarihi: 15 Kasım 2024)

[49] Kaiwartya, O., Abdullah, A. H., Cao, Y., Altameem, A., Prasad, M., Lin, C. T., & Liu, X. (2016). Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects. IEEE Access, 4, 5356-5373.

[50] Contreras, J., Zeadally, S., & Guerrero-Ibanez, J. A. (2018). Internet of Vehicles: Architecture, Protocols, and Security. IEEE Internet of Things Journal, 5(5), 3701-3709.

[51] Zhu, L., Yu, F. R., Wang, Y., Ning, B., & Tang, T. (2019). Big Data Analytics in Intelligent Transportation Systems: A Survey. IEEE Transactions on Intelligent Transportation Systems, 20(1), 383-398.

[52] Sheikh, M. S., Liang, J., & Wang, W. (2020). An improved automatic traffic incident detection technique using a vehicle to infrastructure communication. Journal of Advanced Transportation, 2020, Article ID 9139074.

[53] Ejaz, W., Naeem, M., Sharma, S. K., Khattak, A. M., Ramzan, M. R., Ali, A., & Anpalagan, A. (2021). IoV-Based deployment and scheduling of charging infrastructure in intelligent transportation systems. IEEE Sensors Journal, 21(14), 15504-15514

[54] MacHardy, Z., Khan, A., Obana, K., & Iwashina, S. (2018). V2X Access Technologies: Regulation, Research, and Remaining Challenges. IEEE Communications Surveys & Tutorials, 20(3), 1858-1877.

[55] Boban, M., Kousaridas, A., Manolakis, K., Eichinger, J., & Xu, W. (2018). Connected roads of the future: Use cases, requirements, and design considerations for vehicle-to-everything communications. IEEE Vehicular Technology Magazine, 13(3), 110-123.

[56] Wahid, I., Ikram, A., Ahmed, M., Ali, S., & Ali, A. (2018). State of the Art Routing Protocols in VANETs: A Review. Procedia Computer Science, 130, 689-694.

[57] Xu, D., Li, T., Li, Y., Su, X., Tarkoma, S., Jiang, T., Crowcroft, J.A., & Hui, P. (2020). Edge Intelligence: Architectures, Challenges, and Applications. arXiv: Networking and Internet Architecture.

[58] Bazzi, A., Campolo, C., Masini, B. M., Molinaro, A., Zanella, A., & Berthet, A. O. (2018). Enhancing Cooperative Driving in IEEE 802.11 Vehicular Networks Through Full-Duplex Radios. IEEE Transactions on Wireless Communications, 17(4), 2402-2416.

[59] Li, Y. J. (2012). An Overview of the DSRC/WAVE Technology. In X. Zhang & D. Qiao (Eds.), Quality, Reliability, Security and Robustness in Heterogeneous Networks (pp. 544-558). Springer.

[60] Siegel, J. E., Erb, D. C., & Sarma, S. E. (2018). A Survey of the Connected Vehicle Landscape—Architectures, Enabling Technologies, Applications, and Development Areas. IEEE Transactions on Intelligent Transportation Systems, 19(8), 2391-2406.

[61] Yurtsever, E., Lambert, J., Carballo, A., & Takeda, K. (2020). A Survey of Autonomous Driving: Common Practices and Emerging Technologies. IEEE Access, 8, 58443-58469.

[62] Byttner, S., Nowaczyk, S., Prytz, R., & Rögnvaldsson, T. (2013). A field test with self-organized modeling for knowledge discovery in a fleet of city buses. 2013 IEEE International Conference on Mechatronics and Automation (ICMA) (pp. 1398-1403). IEEE.

[63] Nandugudi, A., Ki, T., Nuessle, C., & Challen, G. (2014). PocketParker: Pocketsourcing Parking Lot Availability. In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (pp. 963-973).

[64] Hussein, A., García, F., Armingol, J. M., & Olaverri-Monreal, C. (2016). P2V and V2P Communication for Pedestrian Warning on the basis of Autonomous Vehicles. In 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC) (pp. 2034-2039). IEEE.

[65] Perallos, A., Hernandez-Jayo, U., Onieva, E., & García-Zuazola, I. J. (2015). Intelligent Transport Systems: Technologies and Applications. John Wiley & Sons.

[66] Eiza, M., & Ni, Q. (2017). Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity. IEEE Vehicular Technology Magazine, 12(2), 45-51.

[67] Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H., & Zedan, H. (2014). A comprehensive survey on vehicular Ad Hoc network. Journal of Network and Computer Applications, 37, 380-392.

[68] Mejri, M. N., Ben-Othman, J., & Hamdi, M. (2014). Survey on VANET security challenges and possible cryptographic solutions. Vehicular Communications, 1(2), 53-66.

[69] Wolf, M., Lemke, K., & Paar, C. (2006). Secure In-Vehicle Communication. In Embedded Security in Cars: Securing Current and Future Automotive IT Applications (pp. 95-109). Springer.

[70] Groza, B., Murvay, S., van Herrewege, A., & Verbauwhede, I. (2012). LiBrA-CAN: A Lightweight Broadcast Authentication Protocol for Controller Area Networks. In J. Pieprzyk, A.-R. Sadeghi, & M. Manulis (Eds.), Cryptology and Network Security (CANS 2012) (pp. 185-200). Springer.

[71] Greenberg, A. (2015, July 21). Hackers Remotely Kill a Jeep on the Highway—With Me in It. Wired. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway (Erişim tarihi: 20 Kasım 2024)

[72] Fraiji, Y., Ben Azzouz, L., Trojet, W., & Saidane, L. A. (2018). Cyber security issues of Internet of electric vehicles. In 2018 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-6). IEEE.

[73] Yang, Z., Yang, K., Lei, L., Zheng, K., & Leung, V. C. M. (2019). Blockchain-based Decentralized Trust Management in Vehicular Networks. IEEE Internet of Things Journal, 6(2), 1495-1505.

[74] Dibaei, M., Zheng, X., Jiang, K., Abbas, R., Liu, S., Zhang, Y., Xiang, Y., & Yu, S. (2020). Attacks and defences on intelligent connected vehicles: A survey. Digital Communications and Networks, 6(4), 399-421.

[75] Mollah, M. B., Zhao, J., Niyato, D., Lam, K. Y., Zhang, X., Ghosh, A. M., Leung, V. C. M., & Wen, Y. (2021). Blockchain for Future Smart Grid: A Comprehensive Survey. IEEE Internet of Things Journal, 8(1), 18-43.

[76] Gatouillat, A., Badr, Y., Massot, B., & Sejdić, E. (2018). Internet of Medical Things: A Review of Recent Contributions Dealing With Cyber-Physical Systems in Medicine. IEEE Internet of Things Journal, 5(5), 3810-3822.

[77] Towards Healthcare. (2023). IoT in Healthcare Market Size (USD 305.55 Bn) Report by 2032. https://www.towardshealthcare.com/insights/iot-in-healthcare-market-size (Erişim tarihi: 25 Kasım 2024)

[78] Alsubaei, F., Abuhussein, A., Shandilya, V., & Shiva, S. (2019). IoMT-SAF: Internet of Medical Things Security Assessment Framework. Internet of Things, 8, Article 100123.

[79] Ahmadi, H., Arji, G., Shahmoradi, L., Safdari, R., Nilashi, M., & Alizadeh, M. (2019). The application of internet of things in healthcare: a systematic literature review and classification. Universal Access in the Information Society, 18(4), 837-869.

[80] Hasan, K., Biswas, K., Ahmed, K., Nafi, N. S., & Islam, M. S. (2019). A comprehensive review of wireless body area network. Journal of Network and Computer Applications, 143, 178-198.

[81] Tuli, S., Basumatary, N., Gill, S. S., Kahani, M., Arya, R. C., Wander, G. S., & Buyya, R. (2020). HealthFog: An ensemble deep learning based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in integrated IoT and fog computing environments. Future Generation Computer Systems, 104, 187-200.

[82] Ray, P. P., Dash, D., & De, D. (2019). Edge computing for Internet of Things: A survey, e-healthcare case study and future direction. Journal of Network and Computer Applications, 140, 1-22.

[83] Rahmani, A. M., Gia, T. N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M., & Liljeberg, P. (2018). Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. Future Generation Computer Systems, 78, 641-658.

[84] Sodhro, A. H., Pirbhulal, S., & de Albuquerque, V. H. C. (2019). Artificial Intelligence-Driven Mechanism for Edge Computing-Based Industrial Applications. IEEE Transactions on Industrial Informatics, 15(7), 4235-4243.

[85] Joyia, G. J., Liaqat, R. M., Farooq, A., & Rehman, S. (2017). Internet of medical things (IOMT): Applications, benefits and future challenges in healthcare domain. Journal of Communications, 12(4), 240-247.

[86] Pierleoni, P., Pernini, L., Belli, A., & Palma, L. (2014). An android-based heart monitoring system for the elderly and for patients with heart disease. International Journal of Telemedicine and Applications, 2014.

[87] Monaghesh, E., & Hajizadeh, A. (2020). The role of telehealth during COVID-19 outbreak: a systematic review based on current evidence. BMC Public Health, 20(1), Article 1193.

[88] Martínez Pérez, M., de la Torre Díez, I., García Zapirain, B., & López-Coronado Delgado, M. (2015). Privacy and Security in Mobile Health Apps: A Review and Recommendations. Journal of Medical Systems, 39(1), Article 181.

[89] Slade Shantz, J. A., & Veillette, C. J. (2014). The application of wearable technology in surgery: ensuring the positive impact of the wearable revolution on surgical patients. Frontiers in Surgery, 1, Article 39.

[90] Amin, S. U., & Hossain, M. S. (2021). Edge Intelligence and Internet of Things in Healthcare: A Survey. IEEE Access, 9, 45-59.

[91] Channa, A., Popescu, N., Skibinska, J., & Burget, R. (2021). The Rise of Wearable Devices during the COVID-19 Pandemic: A Systematic Review. Sensors, 21(17), Article 5787.

[92] Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., Rodriguez, J., & Lymberopoulos, D. (2020). A survey on security threats and countermeasures in internet of medical things (IoMT). Transactions on Emerging Telecommunications Technologies, 31(7), Article e4049.

[93] Das, A. K., Zeadally, S., & He, D. (2018). Taxonomy and analysis of security protocols for Internet of Things. Future Generation Computer Systems, 89, 110-125.

[94] Ahmed, S. F., Alam, M. S. B., Afrin, S., Rafa, S. J., Rafa, N., & Gandomi, A. H. (2024). Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions. Information Fusion, 102, Article 102060.

[95] Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society, 39, 283-297.

[96] Park, J. H. (2017). Blockchain security in cloud computing: Use cases, challenges, and solutions. Symmetry, 9(8), Article 164.

[97] Yeh, K.-H. (2016). A secure IoT-based healthcare system with body sensor networks. IEEE Access, 4, 10288-10299.

[98] Sakiz, F., & Sen, S. (2017). A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. Ad Hoc Networks, 61, 33-50.

[99] Alladi, T., Kohli, V., Chamola, V., & Yu, F. R. (2021). Securing the Internet of Vehicles: A Deep Learning-Based Classification Framework. IEEE Networking Letters, 3(2), 94-97.

[100] Ahmed, I., Jeon, G., & Ahmad, A. (2023). Deep Learning-Based Intrusion Detection System for Internet of Vehicles. IEEE Consumer Electronics Magazine, 12(1), 117-123.

[101] Muhammad, G., & Alhussein, M. (2022). Security, Trust, and Privacy for the Internet of Vehicles: A Deep Learning Approach. IEEE Consumer Electronics Magazine, 11(6), 49-55.

[102] Ullah, S., Khan, M. A., Ahmad, J., Jamal, S. S., e Huma, Z., Hassan, M. T., Pitropakis, N., Arshad, & Buchanan, W. J. (2022). HDL-IDS: A Hybrid Deep Learning Architecture for Intrusion Detection in the Internet of Vehicles. Sensors, 22(4), 1340.

[103] Arif, M., Wang, G., & Wang, T. (2018). SDN-based secure VANETs communication with fog computing. In International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage (pp. 46-59). Springer.

[104] Nie, L., Ning, Z., Wang, X., Hu, X., Cheng, J., & Li, Y. (2020). Data-driven intrusion detection for intelligent Internet of vehicles: A deep convolutional neural network-based method. IEEE Transactions on Network Science and Engineering, 7(4), 2219-2230.

[105] Yang, L., Moubayed, A., & Shami, A. (2022). MTH-IDS: A multitiered hybrid intrusion detection system for Internet of vehicles. IEEE Internet of Things Journal, 9(1), 616-632.

[106] Korium, M.S., Saber, M., Beattie, A., Narayanan, A., Sahoo, S., & Nardelli, P.H.J. (2024). Intrusion detection system for cyberattacks in the Internet of Vehicles environment. Ad Hoc Networks, 153, 103330.

[107] Man, D., Zeng, F., Lv, J., Xuan, S., Yang, W., & Guizani, M. (2023). AI-based intrusion detection for intelligence Internet of Vehicles. IEEE Consumer Electronics Magazine, 12(1), 109-116.

[108] Chaganti, R., Azrour, M., Vinayakumar, R., Naga, V., Dua, A., & Bhushan, B. (2022). A Particle Swarm Optimization and Deep Learning Approach for Intrusion Detection System in Internet of Medical Things. Sustainability, 14(19)

[109] Thamilarasu, G., Odesile, A., & Hoang, A. (2020). An Intrusion Detection System for Internet of Medical Things. IEEE Access, 8, 181560-181576.

[110] Zachos, G., Essop, I., Mantas, G., Porfyrakis, K., Ribeiro, J. C., & Rodriguez, J. (2021). An Anomaly-Based Intrusion Detection System for Internet of Medical Things Networks. Electronics, 10(21), 2562.

[111] Ravi, V., Pham, T. D., & Alazab, M. (2023). Deep Learning-Based Network Intrusion Detection System for Internet of Medical Things. IEEE Internet of Things Magazine, 2023, 50-54.

[112] Areia, J., Bispo, I. A., Santos, L., & Costa, R. L. D. C. (2024). IoMT-TrafficData: Dataset and Tools for Benchmarking Intrusion Detection in Internet of Medical Things. IEEE Access, 12, 115370-115385.

[113] Alsolami, T., Alsharif, B., & Ilyas, M. (2024). Enhancing Cybersecurity in Healthcare: Evaluating Ensemble Learning Models for Intrusion Detection in the Internet of Medical Things. Sensors, 24(18), 5937.

[114] Manimurugan, S., Al-Mutairi, S., Aborokbah, M. M., Chilamkurti, N., Ganesan, S., & Patan, R. (2020). Effective Attack Detection in Internet of Medical Things Smart Environment Using a Deep Belief Neural Network. IEEE Access, 8, 77396-77404.

[115] Amirudin, N. A., & Abdulkadir, S. J. (2024). Comparative study of machine learning algorithms using the CICIOV2024 dataset. Platform - A Journal of Science & Technology, 7(1), 1-8.

[116] Nakayiza, H. L., Ahakonye, L. A. C., Kim, D. S., & Lee, J. M. (2024). Machine Learning Algorithms for Detecting Intra-Vehicular Data Falsification.

[117] Rafrastara, F. A., Ghozi, W., & Wardoyo, A. (2024). Deteksi Serangan berbasis Machine Learning pada Internet of Vehicle. IN-FEST 2024: Seminar Nasional Informatika – FTI UPGRIS, 2, 1-9.

[118] Gul, M. F., & Bakir, H. (2024). Improving Attack Detection in IoV Systems using GA-based Hyperparameter Optimization. In 2024 8th International Artificial Intelligence and Data Processing Symposium (IDAP) (pp. 1-5). IEEE.

[119] Merzouk, M. A., Neal, C., Delas, J., Yaich, R., Boulahia-Cuppens, N., & Cuppens, F. (2024). Adversarial robustness of deep reinforcement learning-based intrusion detection. International Journal of Information Security, 23, 3625-3651.

[120] Aswal, K., & Pathak, H. (2024). Advancing Vehicle Security: Deep Learning based Solution for Defending CAN Networks in the Internet of Vehicles. EAI Endorsed Transactions on Internet of Things, 10(1), 1-14.

[121] Khan, F., & Shivabasappa, S. K. B. (2024). Detecting Evolving Cyber Threats in IoT Environments Using Machine Learning. International Journal of Intelligent Engineering and Systems, 17(6), 12-23. doi: 10.22266/ijies2024.1231.02

[122] Mahdi, Z. S., Zaki, R. M., & Alzubaidi, L. (2024). Advanced Hybrid Techniques for Cyberattack Detection and Defense in IoT Networks. Security and Privacy, 0(0), e471.

[123] Hernandez-Jaimes, M. L., Martínez-Cruz, A., Ramírez-Gutiérrez, K. A., & Guevara-Martínez, E. (2024). Enhancing Machine Learning Approach Based on Nilsimsa Fingerprinting for Ransomware Detection in IoMT. IEEE Access, 12, 153886-153897.

[124] Mohammadi, A., Aminian, M., Ghahramani, H., & Asghari, S. A. (2024). Securing Healthcare with Deep Learning: A CNN-Based Model for medical IoT Threat Detection. 2024 19th Iranian Conference on Intelligent Systems (ICIS), 1-7.

[125] Sohail, F., Bhatti, M. A. M., Awais, M., & Iqtidar, A. (2024). Explainable Boosting Ensemble Methods for Intrusion Detection in Internet of Medical Things (IoMT) Applications. 2024 4th International Conference on Digital Futures and Transformative Technologies (ICoDT2), 1-8.

[126] Naeem, H., Alsirhani, A., Alserhani, F. M., Ullah, F., & Krejcar, O. (2024). Augmenting Internet of Medical Things Security: Deep Ensemble Integration and Methodological Fusion. Computer Modeling in Engineering & Sciences, 141(3), 2186-2223.

[127] Misbah, A., Sebbar, A., & Hafidi, I. (2024). SmartEdge: A Scalable and Adaptive Framework for Cyber Resilience in IoMT. Security and Privacy

[128] Ullah, F., Mostarda, L., Cacciagrano, D., Alenazi, M. J., Chen, C. M., & Kumari, S. (2024). Federated Edge Intelligence for Enhanced Security in Consumer Intermittent Healthcare Devices using Adversarial Examples. IEEE Transactions on Consumer Electronics

[129] Chen, Y., Fang, F., Wang, B., & Zhang, L. (2024). An Efficient Federated Learning Framework for IoT Intrusion Detection. IEEE Vehicular Technology Conference (VTC2024-Fall)

[130] Suarez Gomez, A., Gutierrez Portela, F., & Diaz Triana, O. A. (2024). Intrusion Detection System for IoT using Anomaly Detection Techniques. IEEE VII Congreso Internacional en Inteligencia Ambiental, Ingeniería de Software y Salud Electrónica y Móvil (AmITIC)

[131] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436–444, 2015.

[132] J. Schmidhuber, "Deep learning in neural networks: An overview," Neural Networks, vol. 61, pp. 85–117, 2015.

[133] W. S. McCulloch and W. Pitts, "A logical calculus of the ideas immanent in nervous activity," Bulletin of Mathematical Biophysics, vol. 5, no. 4, pp. 115–133, 1943.

[134] S. Haykin, Neural Networks and Learning Machines, 3rd ed. Upper Saddle River, NJ, USA: Pearson, 2009.

[135] Graupe, D. (2013). Principles of artificial neural networks (Vol. 7). World Scientific.

[136] Gupta, N. (2013). Artificial Neural Network. Network and Complex Systems, 3(1), 24-28.

[137] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT press.

[138] Rumelhart, D. E., Hinton, G. E., & Williams, R. J. (1986). Learning representations by back-propagating errors. Nature, 323(6088), 533-536.

[139] Nair, V., & Hinton, G. E. (2010). Rectified linear units improve restricted boltzmann machines. In Proceedings of the 27th international conference on machine learning (ICML-10) (pp. 807-814).

[140] Keskar, N. S., Mudigere, D., Nocedal, J., Smelyanskiy, M., & Tang, P. T. P. (2017). On large-batch training for deep learning: Generalization gap and sharp minima.

[141] Kingma, D. P., & Ba, J. (2014). Adam: A method for stochastic optimization. arXiv preprint arXiv:1412.6980.

[142] Bengio, Y. (2012). Practical recommendations for gradient-based training of deep architectures. Neural networks: Tricks of the trade, 437-478.

[143] Sokolova, M., & Lapalme, G. (2009). A systematic analysis of performance measures for classification tasks. Information Processing & Management, 45(4), 427-437.

[144] Powers, D. M. (2008). Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation. Journal of Machine Learning Technologies, 2(1), 37-63.

[145] Saito, T., & 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.

[146] Chicco, D., & Jurman, G. (2020). The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation. BMC Genomics, 21(1), 1-13.

[147] Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). ImageNet classification with deep convolutional neural networks. Advances in Neural Information Processing Systems, 25, 1097-1105.

[148] Mutasa, S., Sun, S., & Ha, R. (2021). Understanding artificial intelligence based radiology studies: CNN architecture. Clinical Imaging, 80, 72-76.

[149] Simonyan, K., & Zisserman, A. (2015). Very deep convolutional networks for large-scale image recognition. 3rd International Conference on Learning Representations (ICLR 2015), 1–14.

[150] He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 770-778.

[151] Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S., Anguelov, D., & Rabinovich, A. (2015). Going deeper with convolutions. Proceedings of the IEEE conference on computer vision and pattern recognition, 1-9.

[152] Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. IEEE Access, 7, 41525-41550

[153] Ioffe, S., & Szegedy, C. (2015). Batch normalization: Accelerating deep network training by reducing internal covariate shift. International conference on machine learning, 448-456.

[154] Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. Neural computation, 9(8), 1735-1780.

[155] Graves, A., & Schmidhuber, J. (2005). Framewise phoneme classification with bidirectional LSTM and other neural network architectures. Neural networks, 18(5-6), 602-610.

[156] Greff, K., Srivastava, R. K., Koutník, J., Steunebrink, B. R., & Schmidhuber, J. (2016). LSTM: A search space odyssey. IEEE transactions on neural networks and learning systems, 28(10), 2222-2232.

[157] Gers, F. A., Schmidhuber, J., & Cummins, F. (2000). Learning to forget: Continual prediction with LSTM. Neural computation, 12(10), 2451-2471.

[158] Deng, B., Yan, J., & Lin, D. (2017). Peephole: Predicting Network Performance Before Training. ArXiv, abs/1712.03351.

[159] Sutskever, I., Vinyals, O., & Le, Q. V. (2014). Sequence to sequence learning with neural networks. Advances in neural information processing systems, 27.

[160] Atef, S., & Eltawil, A. B. (2020). Assessment of stacked unidirectional and bidirectional long short-term memory networks for electricity load forecasting. Electric Power Systems Research, 187, 106489.

[161] Microsoft Windows 11 Microsoft. https://www.microsoft.com/windows/windows-11(Erişim Tarihi: 11 Aralık 2024)

[162] TensorFlow Google. https://www.tensorflow.org (Erişim Tarihi: 12 Aralık 2024)

[163] Keras. GitHub. https://github.com/keras-team/keras (Erişim Tarihi: 12 Aralık 2024)

[164] Pandas https://pandas.pydata.org (Erişim Tarihi: 14 Aralık 2024)

[165] NumPy. GitHub. https://github.com/numpy/numpy (Erişim Tarihi: 14 Aralık 2024)

[166] Scikit-learn https://scikit-learn.org (Erişim Tarihi: 14 Aralık 2024)

[167] Matplotlib https://matplotlib.org (Erişim Tarihi: 15 Aralık 2024)

[168] Seaborn https://seaborn.pydata.org (Erişim Tarihi: 15 Aralık 2024)

[169] Anaconda https://www.anaconda.com (Erişim Tarihi: 16 Aralık 2024)

ÖZGEÇMİŞ

Adı Soyadı : Nadir Can KAVKAS

Yabancı Dil : İngilizce

Öğrenim Bilgileri

Derece	**Bölüm**	**Üniversite**	**Yıl**
Lisans	Bilgisayar Mühendisliği	İstanbul Üniversitesi	2012-2016
Yüksek Lisans	Bilgisayar Mühendisliği	Marmara Üniversitesi	2022-2024

İş Deneyimi

Yıl	**Firma/Kurum**	**Görevi**
2017-2020	Ekol Lojistik	Yazılım Geliştirme Uzmanı
2020-2021	Otelz.com	Kıdemli Yazılım Geliştirme Uzmanı
2021-2023	Aras Kargo	Yazılım Geliştirme Takım Lideri
2023-Halen	Papara	Kıdemli Yazılım Geliştirme Uzmanı