ANKARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

NESNELERİN İNTERNETİ CİHAZLARI İÇİN MAKİNE ÖĞRENMESİ YÖNTEMLERİYLE SALDIRI TESPİT SİSTEMİNİN GELİŞTİRİLMESİ

Hasan YILMAZ

ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI

ANKARA
2025

ÖZET

Yüksek Lisans Tezi

NESNELERİN İNTERNETİ CİHAZLARI İÇİN MAKİNE ÖĞRENMESİ YÖNTEMLERİYLE SALDIRI TESPİT SİSTEMİNİN GELİŞTİRİLMESİ

Hasan YILMAZ

Ankara Üniversitesi
Fen Bilimleri Enstitüsü
Elektrik-Elektronik Mühendisliği Anabilim Dalı

Danışman: Doç. Dr. Burak ÖZBEY

Nesnelerin interneti (IoT), birbirleriyle ve insanlarla etkileşim kurarak veri alışverişi yapan cihazlardan oluşan bir ekosistem olarak tanımlanabilir. IoT cihazları, geniş kullanım alanlarına sahip olmakla birlikte, zayıf güvenlik önlemleri nedeniyle siber saldırılara karşı savunmasızdır. Bu durum, IoT sistemlerinin güvenliğini sağlamak için yeni yöntemlerin geliştirilmesini gerekli hale getirmektedir. Bu tezde, IoT cihazlarına yönelik siber saldırıların tespit edilmesi amacıyla makine öğrenmesi yöntemlerinin kullanımı incelenmiştir. IoT ağlarındaki tehditlerin etkin bir şekilde tespit edilmesinde, makine öğrenmesi tekniklerinin çözüm sunduğu düşünülmektedir. Çalışmada, IoT cihazlarına yönelik çeşitli saldırı türlerinin tespitine yönelik bir saldırı tespit sistemi geliştirilmesi hedeflenmiştir. İlk olarak, ağ verisi toplanmış ve bu veri doğrudan makine öğrenmesi algoritmalarına sunulmadan önce analiz edilip uygun hale getirilmiştir. Veriler uygun hale getirildikten sonra, IoT ağlarında olabilecek potansiyel saldırıları tespit edebilmek için çeşitli makine öğrenmesi modelleri kullanılmış ve bu modellerin doğruluk oranları karşılaştırılmıştır. Tez çalışmasında, IoT cihazlarının güvenliğini artırmak amacıyla makine öğrenmesi yöntemleri ele alınmış ve IoT ağlarındaki güvenlik açıklarını tespit etmek için kullanılan yöntemlere katkı sağlanması hedeflenmiştir.

Ocak 2025, 79 sayfa

Anahtar Kelimeler: IDS, IoT, IoT Güvenliği, Makine Öğrenmesi, Nesnelerin İnterneti, Saldırı Tespit Sistemi, Siber Güvenlik

ABSTRACT

Master Thesis

DEVELOPMENT OF INTRUSION DETECTION SYSTEM WITH MACHINE LEARNING METHODS FOR INTERNET OF THINGS DEVICES

Hasan YILMAZ

Ankara University
Graduate School of Natural and Applied Sciences
Department of Electrical and Electronics Engineering

Supervisor: Assoc. Prof. Burak ÖZBEY

The Internet of Things (IoT) can be defined as an ecosystem of devices that interact with each other and with people to exchange data. While IoT devices have a wide range of applications, they are vulnerable to cyber attacks due to weak security measures. This situation requires the development of new methods to ensure the security of IoT systems. In this thesis, the use of machine learning methods to detect cyber attacks on IoT devices has been investigated. It is believed that machine learning techniques offer solutions for effective threat detection in IoT networks. The goal of the study is to develop an attack detection system to identify different types of attacks on IoT devices. First, network data was collected, analyzed, and prepared before being fed directly into machine learning algorithms. Once the data was prepared, different machine learning models were applied to detect potential attacks in IoT networks and the accuracy rates of these models were compared. This thesis focuses on the application of machine learning methods to improve the security of IoT devices, and aims to contribute to the methods used to detect security vulnerabilities in IoT networks.

January 2025, 79 pages

Key Words: Cyber Security, IDS, Internet of Things, Intrusion Detection System, IoT, IoT Security, Machine Learning

TEŞEKKÜR

Bu tez çalışmasının her aşamasında yenilikçi fikirlere olan açıklığı, rehberliği, sürekli desteği ve güçlü iletişimiyle bana yol gösteren danışmanım Doç. Dr. Burak ÖZBEY'e en içten teşekkürlerimi sunarım.

Hayatım boyunca yanımda olan ve desteğini hiçbir zaman esirgemeyen sevgili aileme, her adımda sağladığınız güç ve motivasyon için teşekkür ederim.

Bu süreçte sabrı, anlayışı ve sevgisiyle en büyük destekçim olan eşim Zehra'ya ve hayatıma anlam katan, her anımı güzelleştiren sevgili oğlum Ömer'e teşekkür ederim.

Hasan YILMAZ
Ankara, Ocak 2025

İÇİNDEKİLER

KISALTMALAR DİZİNİ

6LoWPAN	Düşük Güçlü Kablosuz Kişisel Alan Ağları Üzerinden IPv6 (IPv6 over Low-Power Wireless Personal Area Networks)
AUC	Eğri Altındaki Alan (Area Under the Curve)
CNN	Evrişimli Sinir Ağları (Convolutional Neural Networks)
CoAP	Kısıtlı Uygulama Protokolü (Constrained Application Protocol)
DDoS	Dağıtık Hizmet Dışı Bırakma Saldırısı (Distributed Denial of Service)
DNS	Alan Adı Sistemi (Domain Name System)
DoS	Hizmet Dışı Bırakma Saldırısı (Denial of Service)
ENISA	Avrupa Birliği Siber Güvenlik Ajansı (The European Union Agency for Cybersecurity)
GBM	Gradyan Artırıcı Makineler (Gradient Boosting Machines)
GDPR	Avrupa Birliği Genel Veri Koruma Yönetmeliği
GMM	Gaussian karışım model (Gaussian Mixture Model)
HTTP	Üst Metin Transfer Protokolü (Hyper Text Transfer Protocol)
IDS	Saldırı Tespit Sistemlerinde (Intrusion Detection Systems)
IEEE	Elektrik-Elektronik Mühendisleri Enstitüsü (Institute of Electrical and Electronics Engineers)
IoT	Nesnelerin İnterneti (Internet of Things)
IP	İnternet Protokolü (Internet Protocol)
IPv6	İnternet Protokolü Sürüm 6 (Internet Protocol Version 6)
ISO	Uluslararası Standardizasyon Kurumu (International Standardisation Organization)
ITU	Uluslararası Telekomünikasyon Birliği (International Telecommunication Union)
KNN	K-en yakın komşu (k-nearest neighbors)
LoRaWAN	Uzun Menzilli Geniş Alan Ağı (Long Range Wide Area Network)
LSTM	Uzun Kısa Süreli Bellek (Long Short-Term Memory)
M2M	Makineler Arası İletişim (Machine-to-Machine)
MIT	Massachusetts Teknoloji Enstitüsü (Massachusetts Institute of Technology)
MQTT	Mesaj Kuyruğu Telemetri Aktarımı (Message Queue Telemetry Transport)
NIST	Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards
ReLU	Doğrultulmuş Lineer Birim (Rectified Linear Unit)
RFID	Radyo Frekansı ile Tanımlama (Radio Frequency Identification)
RNN	Tekrarlayan Sinir Ağı (Recurrent Neural Network)
ROC	Alıcı İşlem Karakteristiği (Receiver Operating Characteristic)
SMOTE	Sentetik Azınlık Aşırı Örnekleme Tekniği (Synthetic Minority Over-sampling Technique)
SSH	Güvenlik Kabuk (Secure Shell)
SVM	Destek Vektör Makineleri (Support Vector Machines)
TCP	Geçiş Kontrol Protokolü (Transmission Control Protocol)
WPAN	Kablosuz Kişisel Alan Ağları (Wireless Personal Area Networks)
YSA	Yapay Sinir Ağları

ŞEKİLLER DİZİNİ

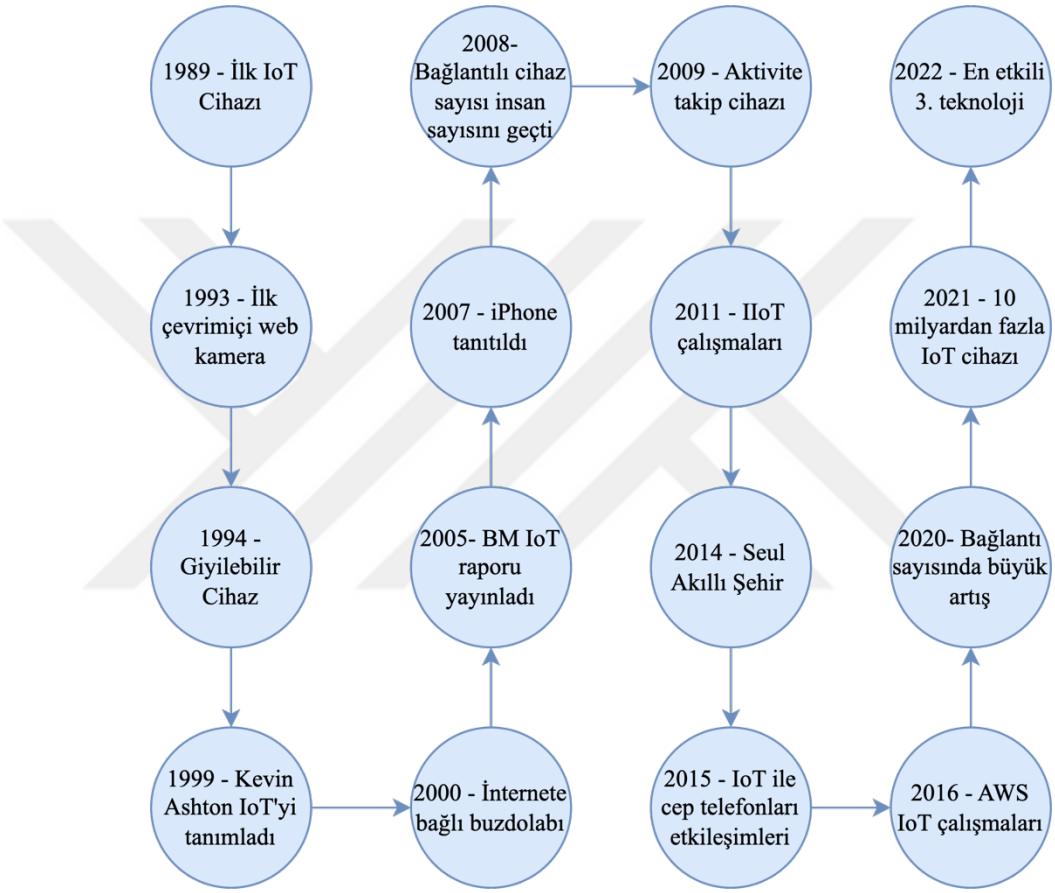
ÇİZELGELER DİZİNİ

1. GİRİŞ

Nesnelerin interneti (Internet of Things - IoT) terimi ilk kez 1999 yılında, Kevin Ashton'ın tedarik zinciri yönetimine ilişkin gerçekleştirdiği bir sunumda kullanılmıştır (Ashton 2009). Ashton, bilgi işlem, internet ve akıllı cihazların veri üretme hızındaki ilerlemeler nedeniyle, fiziksel dünyayla etkileşim şeklimiz ve yaşam biçimimizin köklü bir şekilde yeniden ele alınması gerektiğine inancına sahipti. Massachusetts Teknoloji Enstitüsünün (Massachusetts Institute of Technology - MIT) Auto-ID Merkezinde yönetici direktör olarak görev yaptığı dönemde Ashton, Radyo Frekansı ile Tanımlama (Radio Frequency Identification - RFID) teknolojisinin daha geniş alanlarda uygulanmasına önemli katkılarda bulunarak, günümüzdeki IoT vizyonunun temellerinin atılmasını sağlamıştır.

IoT teknolojisi, yıllar içinde hızla gelişmiş ve yaşamımızın her alanında büyük değişimlere zemin hazırlamıştır. 2000'lerin başında, IoT, RFID ve sensör ağları ile ilgili araştırmalar desteklenmeye başlanmıştır (Roberti 2004). Uluslararası Telekomünikasyon Birliği (International Telecommunication Union - ITU) tarafından, 2005 yılında IoT terimi kabul edilerek bu kavramı resmi olarak tanımlayan bir rapor yayımlanmıştır (ITU 2005). 2008 yılına gelindiğinde, bağlı cihazların sayısının dünyadaki insan sayısını geçtiği belirtilmiştir. Bu durum, IoT'nin gerçek anlamda doğuşu olarak kabul edilmiştir. Çünkü bağlı cihazların sayısı, dünyadaki tüm verilerin gerektiğinde toplanabileceği bir aşamaya ulaşmıştır. 2010'lu yıllarda, IoT teknolojisinin hızla ilerlediği gözlemlenmiştir. Bu dönemde endüstriyel IoT uygulamaları, akıllı şehirler, telefonlar ve saatler ortaya çıkmıştır. IoT teknolojisi, birçok işletmenin ilgisini çekecek düzeyde kazançlı bir hale gelmiş ve bu nedenle IoT platformları ortaya çıkmaya başlamıştır. Amazon Web Hizmetleri tarafından IoT hizmetinin 2015'te başlatıldığı ve 2016 yılında tamamen kullanıma sunulduğu bildirilmiştir. Bu gelişmeler, 2016'da Azure IoT Hub ve 2017'de Google IoT hizmeti tarafından yakından takip edilmiştir. Sonraki yıllarda, işletmelerin IoT projelerini basitleştirmelerine ve IoT alanına daha kolay bir şekilde genişlemelerine olanak tanıyan başka IoT platformları piyasaya sürülmüştür. Bu durumun doğrudan bir sonucu olarak, 2021'de bağlı cihazların sayısının dünya çapında bağlı olmayan cihazların sayısını geçtiği açıklanmıştır. Dünya Ekonomik Forumu, IoT teknolojisinin giderek artan

etkisi dikkate alınarak, IoT'yi 2022'nin en etkili üç teknolojik gelişmesinden biri olarak kabul etmiştir (Anonymous 2022a). IoT'nin gelişimi, teknolojik yenilikler ve endüstriyel uygulamalarla desteklenerek hızla devam etmektedir. Gelecekte daha da entegre ve akıllı sistemlerle IoT'nin yaşamın her alanında etkisini artırması beklenmektedir. Şekil 1.1'de IoT'nin yıllara göre gelişimi özetlenmektedir.



Şekil 1.1 IoT'nin yıllara göre gelişimi (Anonymous 2022a)

IoT günümüzde her ne kadar yaygın olarak kullanılsa da tanımı üzerinde bir fikir birliği bulunmamaktadır. IoT için sunulan hizmetler, hedeflenen amaçlar ve kullanılan mimari çerçevesinde çeşitli tanımlamalar yapılabilmektedir (Minerva vd. 2015). Basit bir ifadeyle IoT, nesnelerin birbirleriyle ve insanlarla akıllı bir şekilde etkileşime girebilecekleri şekilde bağlandıkları bir sistem olarak kabul edilebilmektedir (Iqbal vd. 2021). Ayrıca, aşağıda çeşitli kuruluşlar tarafından IoT hakkında kullanılan bazı tanımlamalara aşağıda yer verilmektedir (Minerva vd. 2015):

- Elektrik-Elektronik Mühendisleri Enstitüsü (Institute of Electrical and Electronics Engineers - IEEE): “IoT, her şeyin internette bir temsilinin ve varlığının olduğu bir çerçevedir. Daha spesifik olarak IoT, fiziksel ve sanal dünyalar arasında köprü kuran yeni uygulamalar ve hizmetler sunmayı amaçlamaktadır; bu kapsamda Makineler Arası İletişim (Machine-to-Machine - M2M), nesneler ve buluttaki uygulamalar arasındaki etkileşimleri sağlayan temel iletişimi temsil etmektedir.”
- Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology - NIST): “Siber fiziksel sistemler, bazen nesnelerin interneti (IoT) olarak da adlandırılmaktadır - ulaşım, enerji, üretim ve sağlık hizmetleri gibi çeşitli sektörlerdeki akıllı cihazların ve sistemlerin temelde yeni yollarla birbirine bağlanmasını içermektedir. Akıllı Şehirler/Topluluklar, operasyonlarının verimliliğini ve sürdürülebilirliğini artırmak ve yaşam kalitesini iyileştirmek için siber fiziksel sitemler ile IoT teknolojilerini giderek daha fazla benimsemektedir.”
- Uluslararası Standardizasyon Kurumu (International Standardisation Organization - ISO): “Birbirine bağlı nesneler, insanlar, sistemler ve bilgi kaynakları ile bunların fiziksel ve sanal dünyanın bilgilerini işlemesine ve tepki vermesine olanak tanıyan akıllı hizmetlerden oluşan bir altyapıdır.”
- ITU: “IoT her yerde, her zaman, her şey ve herkes tarafından kullanılabilen bir ağ türüdür.”

İnternet ile teknolojik gelişmelerin birleşmesi sonucunda, hayatımızın birçok alanında yenilikler meydana gelmiştir. Günümüzde IoT uygulamalarının endüstriyel üretim, ulaşım, enerji ve sağlık sektörlerinde yaygın bir şekilde kullanıldığını görülmektedir. Ayrıca, IoT kavramı, akıllı kelimesiyle özdeşleşmiş pek çok uygulamada karşımıza çıkmaktadır. IoT uygulamaların akıllı şehirler, akıllı evler ve akıllı enerji gibi alanlarda daha fazla benimsenmesi beklenmektedir. IoT cihazlarının yaygınlaşmasıyla birçok sektörde önemli avantajlar sağlanmakta ve operasyonel verimliliği artırarak enerji, zaman ve maliyet tasarrufu elde edilmesine olanak tanımaktadır. Toplanan veriler aracılığıyla kullanıcı davranışları ve operasyonel süreçler hakkında derinlemesine analiz imkanı sunulmaktadır. Günlük yaşamın birçok alanında kullanıcıların hayatını kolaylaştırıcı otomasyon ürünleri sağlanarak kullanıcılara zaman kazandırılmaktadır. IoT, sunduğu imkanlarla akıllı ve bağlı bir dünya yaratma potansiyeline sahiptir. Bu teknoloji, bireysel

kullanıcılar için olduğu kadar işletmeler ve kamu hizmetleri için de büyük faydalar sunmaktadır.

Ancak, sayıları ve kullanım alanı giderek artan IoT cihazları beraberinde önemli güvenlik tehditlerini de getirmektedir. Bir sektör tahminine göre, dünya çapında IoT cihazlarının toplam sayısı 2022'de 13,2 milyardan 2028'de 34,7 milyara çıkarak iki kattan fazla artacağı tahmin edilmektedir (Anonymous 2023b). Dünya genelinde IoT siber saldırılarının sayısı 2022 yılında 112 milyonu aşmıştır ve bu rakam, 2018'de tespit edilen yaklaşık 32 milyon vakadan önemli ölçüde artış göstermektedir. Özellikle 2022 yılında IoT kötü amaçlı yazılım olaylarının sayısındaki artış, bir önceki yıla göre %87 oranında olmuştur (Anonymous 2023c).

Avrupa Birliği Siber Güvenlik Ajansı (The European Union Agency for Cybersecurity - ENISA) tarafından yayımlanan rapora göre geleneksel Dağıtık Hizmet Dışı Bırakma Saldırısı (Distributed Denial of Service - DDoS), mobil ağlar ve IoT cihazlarına doğru ilerlemektedir. IoT cihazları, sınırlı kaynakları ve genellikle zayıf güvenlik önlemleri nedeniyle DDoS saldırıları için uygun hedefler haline gelmiştir. IoT cihazları, genellikle zayıf veya varsayılan şifrelerle piyasaya sürüldüğünden, saldırganlar için kolay hedefler oluşturmaktadır. Ayrıca, kullanıcıların güvenlik becerilerinin eksikliği de bu cihazların savunmasızlığını artırmaktadır. IoT cihazlarının ve mobil ağların artan karmaşıklığı, kullanıcıların güvenlik bilgisi eksikliğini daha belirgin hale getirmektedir. DDoS saldırıları, hem IoT bileşenlerinin kullanılabilirliğini tehdit etmekte, hem de diğer ağların veya sistemlerin işleyişini bozabilmekte ve kullanıcıların güvenliğini tehlikeye atabilmektedir. Buluta bağlı cihaz ve uygulamaların sayısındaki artış, saldırganlara daha geniş bir hedef yelpazesi sunmaktadır. Bu durum, DDoS saldırılarının IoT cihazları aracılığıyla sürekli olarak arttığını ve daha karmaşık hale geldiğini göstermektedir (Anonymous 2023a).

IoT cihazlarının güvenlik açıkları, siber suçluların dikkatini çekmekte ve bu cihazlara izinsiz erişim sağlamalarına, veri çalmalarına ve hatta cihazların kontrolünü ele geçirerek daha büyük saldırılar düzenlemelerine olanak tanımaktadır. Özellikle sağlık, enerji ve ulaşım gibi kritik altyapılarda kullanılan IoT cihazlarının güvenliği büyük önem

taşımaktadır. Bu cihazların hedef alınması durumunda, toplumun genel güvenliği tehlikeye girebilmekte ve büyük çaplı ekonomik kayıplar yaşanabilmektedir. IoT tabanlı saldırıları zamanında tespit ederek bu saldırılara müdahale etmek, günümüzün dijital dünyasında kritik bir öneme sahiptir. IoT cihazlarının ağ davranışlarını izleyerek ve gerektiğinde müdahale ederek, ağın bu cihazlardan kaynaklanabilecek potansiyel tehditlere karşı korunması sağlanabilmektedir. Bu sayede, normal ağ trafiği etkilenmeden kesintisiz bir şekilde devam edebilmektedir. Makine öğrenmesi teknikleri; sınıflandırma, tahmin ve tespit gibi işlemler için etkili bir araç sunmaktadır.

Bu tezin amacı, makine öğrenmesi yöntemleri kullanarak IoT saldırılarının tespit edilebilmesini sağlamaktır. Makine öğrenmesi yöntemlerinin başarılı bir şekilde uygulanabilmesi için uygun veri setlerine ihtiyaç duyulmaktadır. İlk aşamada ağ verisi toplanmaktadır. Daha sonra, ağ trafik paketleri için gerekli analiz ve dönüşüm işlemleri gerçekleştirilip, makine öğrenmesi için uygun hale getirilmektedir. Ardından, bu veriler için makine öğrenmesi modelleri belirlenmektedir. Makine öğrenmesinde doğru modelin seçilmesi, başarılı sınıflandırma veya tahmin yapılabilmesi açısından büyük önem taşımaktadır. Bu tez çalışması, öncelikle IoT cihazlarına yönelik potansiyel saldırı yöntemlerini incelemeyi amaçlamaktadır. Mevcut saldırı tespit teknikleri değerlendirildikten sonra, makine öğrenmesi algoritmalarının IoT ağlarındaki saldırıları tespit etme yeteneklerine odaklanılmaktadır. Tez çalışmasında, farklı makine öğrenmesi yöntemlerinin IoT ağlarında saldırıları tespit etme kapasite ve doğruluk oranları karşılaştırılmaktadır. Bu çalışma ile, IoT ağlarındaki güvenlik açıklarını tespit etmek ve potansiyel saldırılara karşı etkili bir korunma sağlamak amacıyla makine öğrenmesi tabanlı saldırı tespit sistemi geliştirilmesi hedeflenmektedir.

Tez çalışmasının ana odağı, IoT cihazlarının güvenliği olup, ilk olarak çeşitli IoT cihaz türlerine yönelik siber saldırılara odaklanılmaktadır. Ayrıca, akıllı ev eşyalarına yönelik saldırılar da ele alınmaktadır. Çalışma kapsamında IoT ağlarındaki saldırıların tespitinde kullanılabilecek makine öğrenmesi yöntemleri değerlendirilmekte, IoT cihazlarına yönelik belirli saldırı türleri üzerinde durulmaktadır. Bunlar arasında Hizmet Dışı Bırakma (Denial of Service - DoS) saldırıları, kaba kuvvet (brute force) saldırıları, sensör ve kamera ile etkileşim, ağ trafiği yakalama, zararlı yazılım ve zafiyet tarama yöntemleri

yer almaktadır. Çalışmanın genel amacı, bahse konu cihaz ve saldırı türlerinin yanı sıra, bu saldırıların tespitine yönelik makine öğrenmesi tabanlı sistemlerin geliştirilmesidir. Çalışmanın sonuçları, IoT cihazlarının güvenlik açıklarının daha iyi anlaşılması ve bu cihazlara yönelik siber saldırılara karşı etkili savunma mekanizmalarının oluşturulması açısından katkı sunmayı amaçlamaktadır.

Tez yapısı şu şekildedir: Birinci bölümde giriş yapılarak tez konusuna ilişkin genel bilgilere yer verilmekte, ikinci bölümde literatürde yer alan incelemeler sunulmaktadır. Üçüncü bölümde materyal ve yöntem açıklamaları, dördüncü bölümde çalışma sürecinde elde edilen bulgular detaylı bir şekilde sunulmaktadır. Son olarak beşinci bölümde sonuçlar değerlendirilmektedir.

2. KURAMSAL TEMELLER VE/VEYA KAYNAK ÖZETLERİ

Bu bölümde, nesnelerin interneti, makine öğrenmesi ve saldırı tespit sistemlerine ilişkin kuramsal temeller ele alınmış ve bu konularda literatürde yer alan çalışmalara değinilmiştir.

2.1 Nesnelerin İnterneti

IoT uygulamaları ve teknolojileri, kullanım alanlarına göre çeşitlilik arz etmektedir. Bu nedenle, farklı kullanım amaçlarına yönelik olarak çeşitli mimari modeller ve protokoller geliştirilmiş, bu doğrultuda pek çok yenilikçi teknoloji ortaya konulmuştur.

2.1.1 IoT mimarileri

IoT mimarileri, Geçiş Kontrol Protokolü (Transmission Control Protocol - TCP) ve İnternet Protokolü'ne (Internet Protocol - IP) dayalı çok katmanlı bir teknoloji olarak geliştirilmiştir. Bu mimariler, işlemci, sensör/aktüatör ve iletişim birimi ile donatılmış milyarlarca akıllı nesnenin anlamlı iletişimini sağlamak amacıyla tasarlanmıştır. IoT'nin temel amacı, farklı donanım cihazlarının çeşitli uygulama alanlarına bağlanmasını mümkün kılmaktır. Ancak, bu süreçte heterojenlik, ölçeklenebilirlik, birlikte çalışabilirlik, güvenlik/gizlilik ve hizmet kalitesi gibi önemli zorluklarla karşılaşılmaktadır. Bu zorluklar, IoT sistem mimarilerini doğrudan etkilemektedir (Iqbal vd. 2021).

Literatürde, farklı işlevselliklere ve teknik terminolojilere sahip çeşitli IoT mimarileri önerilmiştir. Ancak, bu mimariler arasında tam anlamıyla bir standartlaşma sağlanamamış, dolayısıyla farklı IoT sistemleri arasında birlikte çalışabilirlik sınırlı kalmıştır. Bu nedenle, tüm IoT projeleri için merkezi ve katmanlı bir mimarinin geliştirilmesine ihtiyaç duyulmaktadır. Bu bağlamda, IoT mimarileri genellikle üç, beş, altı ve yedi katmanlı yapılandırmalar olarak ele alınmaktadır (Iqbal vd. 2021).

Üç katmanlı IoT mimarisi, en basit IoT mimarilerinden biridir ve algılama, ağ ve uygulama katmanlarından oluşmaktadır. Algılama katmanı, fiziksel sensörler aracılığıyla çevresel verileri toplamaktan sorumludur. Toplanan veriler, ağ katmanı üzerinden uygulama katmanına aktarılmaktadır. Uygulama katmanı, bu verileri işleyerek kullanıcılara farklı hizmetler sağlamaktadır. Örneğin, sıcaklık, nem, hava basıncı gibi veriler bu katman aracılığıyla analiz edilip kullanıcılara sunulmaktadır. Üç katmanlı mimarinin basitliği, IoT sistemlerinin temel işlevselliklerini sağlamada yeterli olmasına rağmen, daha karmaşık ve büyük ölçekli uygulamalar için genellikle ek katmanlara ihtiyaç duyulmaktadır (Iqbal vd. 2021).

Beş katmanlı IoT mimarisi, algılama, nesne soyutlama, hizmet yönetimi, uygulama ve iş katmanlarından oluşmaktadır. Algılama katmanı, fiziksel sensörler aracılığıyla çevresel verileri toplar ve nesne soyutlama katmanına iletilmektedir. Nesne soyutlama katmanı, bu verileri güvenli bir şekilde bilgi işlem sistemlerine iletmek için çeşitli iletişim teknolojilerini kullanmaktadır. Hizmet yönetimi katmanı ise IoT uygulamaları ile veriler arasındaki bağlantıyı sağlamakta ve bu verilerin işlenmesini organize etmektedir. Uygulama katmanı, kullanıcıların talep ettiği hizmetleri sunarken, iş katmanı IoT sisteminin genel faaliyetlerini yönetmekte ve iş modellerini geliştirmektedir. Beş katmanlı mimari, IoT sistemlerinin daha karmaşık işlevselliklerini desteklemeye yöneliktir ve daha geniş bir veri işleme kapasitesi sunmaktadır (Iqbal vd. 2021).

Altı katmanlı IoT mimarisi ise odak, biliş, iletim, uygulama, altyapı ve iş yeterliliği katmanlarından oluşmaktadır. Bu mimari, birden fazla IoT sisteminin entegrasyonunu ve bu sistemlerin iş değerine etkilerini analiz etmek amacıyla geliştirilmiştir. Odak katmanı, IoT sistemlerinin belirli unsurlarını tanımlamaktan sorumluyken, biliş katmanı bu unsurlardan veri toplamaktadır. İletim katmanı, toplanan verileri uygulama katmanına iletmekte, altyapı katmanı ise bu verilerin depolanması ve işlenmesi için bulut hizmetleri gibi teknolojileri kullanmaktadır. İş yeterliliği katmanı ise bu veriler üzerinden iş modelleri ve stratejiler geliştirilmesine olanak tanımaktadır (Iqbal vd. 2021).

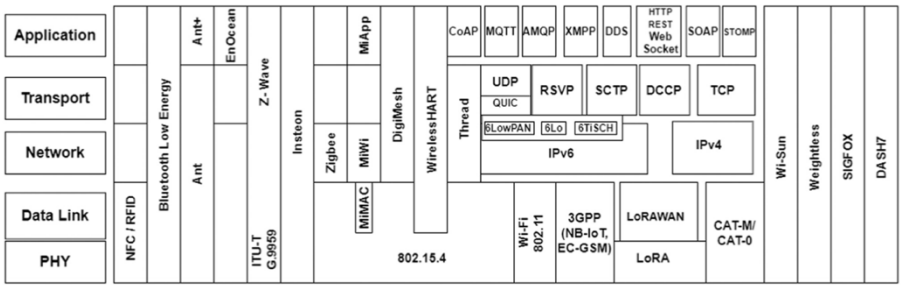
Yedi katmanlı IoT mimarisi, nesneler, bağlantı, kenar/bulut bilişim, veri birikimi, veri soyutlama, uygulama ve iş birliği katmanlarından oluşmaktadır. Bu mimari, IoT

sistemlerinin işlevselliğini anlamak ve yönetmek için en kapsamlı yapıyı sunmaktadır. Nesneler katmanı, IoT sistemine bağlı olan tüm cihazları içerir ve bu cihazlardan veri toplamaktadır. Bağlantı katmanı, bu verilerin zamanında ve güvenli bir şekilde iletilmesini sağlamaktadır. Kenar/bulut bilişim katmanı, verilerin analiz edilmesi ve işlenmesi için ilk aşamada işlem görmesini sağlamaktadır. Veri birikimi katmanı, verilerin depolanması ve uygun şekilde organize edilmesini sağlamaktadır. Veri soyutlama katmanı, farklı veri formatlarının birleştirilmesi ve işlenmesi için gerekli işlemleri gerçekleştirmektedir. Uygulama katmanı, bu verileri kullanarak çeşitli IoT uygulamalarını çalıştırırken, iş birliği katmanı, kullanıcılar ve iş süreçleri arasında etkileşim sağlamaktadır. Sonuç olarak, IoT mimarileri, IoT sistemlerinin belirli gereksinimlerini karşılamak amacıyla çeşitli katmanlar ve işlevler sunmaktadır (Iqbal vd. 2021).

Bu mimariler, IoT'nin çeşitli zorluklarına yönelik farklı çözüm yolları sunmakta ve IoT sistemlerinin esnek, ölçeklenebilir ve güvenli bir şekilde çalışabilmesi için hayati bir öneme sahiptir (Iqbal vd. 2021).

2.1.2 IoT protokoller ve teknolojiler

IoT'nin etkin çalışması, çeşitli iletişim protokolleri sayesinde mümkün olmaktadır. Bu protokoller, cihazların veri alışverişini kolaylaştırmak ve çeşitli kullanım senaryolarında ihtiyaç duyulan performans, güvenlik ve enerji verimliliği gibi gereksinimlere cevap vermek için tasarlanmıştır. Her bir protokol, IoT ekosisteminin farklı bileşenlerinin bir arada sorunsuz bir şekilde çalışmasını sağlamak için belirli avantajlar sunmaktadır.



Şekil 2.1 IoT protokolleri (Bang vd. 2022)

Mesaj Kuyruğu Telemetri Aktarımı (Message Queue Telemetry Transport - MQTT) protokolü, düşük bant genişliği ve enerji tüketimi gerektiren ortamlar için geliştirilmiş hafif bir mesajlaşma protokolü olarak öne çıkmaktadır. Bu protokol, özellikle sınırlı kaynaklara sahip IoT cihazları arasında güvenilir veri aktarımını sağlamak amacıyla tasarlanmıştır. MQTT, "yayın-abonelik" modeli üzerine kurulu olup, cihazların sadece gerekli olduğunda veri göndermesine olanak tanımakta, bu da ağ trafiğini ve enerji tüketimini minimumda tutmaktadır. Bu nedenle MQTT, uzaktan izleme, ev otomasyonu ve sağlık takibi gibi IoT uygulamalarında yaygın olarak kullanılmaktadır (Gerodimos vd. 2023).

Kısıtlı Uygulama Protokolü (Constrained Application Protocol - CoAP), düşük veri iletim hızı ve hafif yapısı sayesinde kısıtlı cihazlar ve ağlar için ideal bir seçenek olarak değerlendirilmektedir. CoAP, Üst Metin Transfer Protokolü'nün (Hyper Text Transfer Protocol - HTTP) IoT cihazlarına uyarlanmış bir versiyonu olarak düşünülebilir; ancak, çok daha az kaynak tüketimi ile çalışmaktadır. Bu protokol, özellikle düşük güçlü cihazların enerji verimliliğini artırmak amacıyla tasarlanmıştır ve M2M uygulamalarında yaygın olarak kullanılmaktadır. CoAP'nin web tabanlı yapısı, internet ve IoT cihazları arasında kolay entegrasyon sağlamakta, bu da onu endüstriyel otomasyon ve akıllı enerji sistemleri gibi uygulamalar için ideal hale getirmektedir (Gerodimos vd. 2023).

ZigBee, düşük güç tüketimi ve kısa mesafe iletişim için tasarlanmış bir kablosuz protokoldür. Bu protokol, özellikle akıllı ev otomasyonu, enerji yönetimi ve akıllı aydınlatma sistemleri gibi uygulamalarda tercih edilmektedir. ZigBee'nin mesh ağ yapısı, geniş bir alana yayılan çok sayıda cihazın birbirine bağlanmasını ve verilerin bu cihazlar

arasında güvenli bir şekilde iletilmesini sağlamaktadır. Ayrıca, ZigBee, düşük veri iletim hızına rağmen, uzun pil ömrü gerektiren uygulamalar için ideal bir çözüm sunmaktadır (Gerodimos vd. 2023).

Uzun Menzilli Geniş Alan Ağı (Long Range Wide Area Network - LoRaWAN), düşük enerji tüketimi ve geniş alan kapsama kapasitesi sunan bir protokol olarak öne çıkmaktadır. Bu protokol, özellikle geniş coğrafi alanlarda dağınık halde bulunan sensör ağları için ideal bir çözüm sunmaktadır. LoRaWAN, düşük bant genişliği gerektiren IoT uygulamalarında uzun mesafeli veri iletimi sağlamak amacıyla tasarlanmıştır. Bu özellikleriyle, tarım, çevresel izleme ve akıllı şehir uygulamalarında, enerji verimliliğini korurken geniş alanlarda veri toplamayı mümkün kılmaktadır (Gerodimos vd. 2023).

Wi-Fi ve Bluetooth gibi teknolojiler ise, IoT cihazlarının internete bağlanması ve birbirleriyle iletişim kurması için yaygın olarak kullanılmaktadır. Wi-Fi, yüksek veri aktarım hızı ve geniş ağ kapsamı ile öne çıkarken, özellikle ev ve ofis ağlarında IoT cihazlarının merkezi bir ağa bağlanmasını sağlamaktadır. Wi-Fi'nin yüksek bant genişliği gerektiren uygulamalarda kullanılması, büyük veri miktarlarının hızlı bir şekilde iletilmesini mümkün kılmaktadır. Bluetooth, düşük enerji tüketimi ve kısa mesafeli iletişim yetenekleri ile özellikle taşınabilir cihazlar ve giyilebilir teknolojilerde tercih edilmektedir. Bluetooth'un enerji verimliliği, IoT cihazlarının pil ömrünü uzatmakta ve sürekli bağlantı gerektiren uygulamalarda güvenilir bir iletişim sunmaktadır (Bang vd. 2022).

IoT'nin temelini oluşturan teknolojiler, cihazların uyumlu bir şekilde çalışmasını sağlayan standartlar ve altyapılar üzerine kurulmaktadır. Bu teknolojiler arasında, IoT cihazlarının sayısındaki artışa yanıt verebilmek için geliştirilen IPv6 (İnternet Protokolü sürüm 6 - Internet Protocol Version 6) öne çıkmaktadır. IPv6, cihazların özebir (unique) adreslerle internete bağlanmasını sağlayarak, IoT ağlarının ölçeklenebilirliğini artırmaktadır. 6LoWPAN (Düşük Güçlü Kablosuz Kişisel Alan Ağları Üzerinden IPv6 - IPv6 over Low-Power Wireless Personal Area Networks), IPv6'yı düşük güçlü kablosuz kişisel alan ağlarına (Wireless Personal Area Networks - WPAN) entegre eden bir protokol olarak, düşük enerji tüketimi ve yüksek verimlilik sunmakta, böylece IoT

cihazlarının geniş bir yelpazede uyumlu bir şekilde çalışmasına olanak sağlamaktadır. Ayrıca, Kenar ve Sis Bilişim teknolojileri, IoT cihazlarının ürettiği büyük veri miktarlarının merkezden ziyade veriye yakın noktalarda işlenmesini sağlamaktadır. Bu yaklaşım, ağ üzerindeki yükü azaltmakta ve veri işleme sürelerini kısaltarak, IoT sistemlerinin gerçek zamanlı uygulamalarda daha verimli çalışmasını mümkün kılmaktadır. Bu teknolojiler, IoT'nin performansını ve esnekliğini artırırken, aynı zamanda enerji tüketimini optimize ederek sürdürülebilirlik hedeflerine de katkı sağlamaktadır (Bang vd. 2022).

2.2 IoT'de Güvenlik

IoT teknolojisinin hızla yaygınlaşması, günlük yaşamın birçok alanında önemli kolaylıklar sağlamaktadır. Ancak bu genişleme, beraberinde ciddi güvenlik endişelerini de getirmektedir. IoT cihazlarının sınırlı işlem gücü ve enerji kapasiteleri, geleneksel güvenlik önlemlerinin uygulanmasını zorlaştırmakta ve bu durum, çeşitli siber saldırılara karşı savunmasız bir ortam oluşturmaktadır (Fei vd. 2023).

IoT güvenliği, küresel ölçekte uyum gerektiren bir konudur. Farklı ülkelerde farklı güvenlik standartlarının uygulanması, IoT cihazlarının güvenliğini sağlama konusunda zorluklar oluşturmaktadır. Bu nedenle, uluslararası düzeyde güvenlik standartlarının belirlenmesi ve bu standartların tüm ülkelerde uygulanması, IoT güvenliğini artırmak için önemli bir adım olarak değerlendirilmektedir (Schiller vd. 2022).

Gizlilik politikaları da IoT güvenliğinin önemli bir bileşenidir. Avrupa Birliği Genel Veri Koruma Yönetmeliği (GDPR) gibi düzenlemeler, IoT cihazları tarafından toplanan verilerin korunmasını zorunlu kılmaktadır. Ancak bu düzenlemelerin uygulanması, IoT cihazlarının doğası gereği zor olabilmektedir. IoT cihazlarının sürekli veri toplaması ve bu verilerin farklı hizmet sağlayıcılar arasında paylaşılması, bu verilerin izlenmesi ve gerektiğinde silinmesi sürecini karmaşık hale getirmektedir (Schiller vd. 2022).

IoT güvenliği, cihazların tasarımından uygulamasına ve yönetimine kadar birçok aşamada ele alınması gereken çok katmanlı bir konudur. IoT cihazlarının güvenliğinin sağlanması, yalnızca teknik bir gereklilik değil, aynı zamanda kullanıcı güvenini artırmak ve bu teknolojinin geniş kitleler tarafından güvenle kullanılabilmesini sağlamak açısından da kritik öneme sahiptir (Schiller vd. 2022). Bu nedenle, IoT ürün ve uygulamalarının güvenliğini sağlamak için bütünleşik ve kapsamlı bir yaklaşım benimsenmelidir.

2.2.1 Açıklar ve zafiyetler

IoT cihazlarının tasarımındaki kısıtlamalar, güçlü güvenlik mekanizmalarının uygulanmasını engellemektedir. Zayıf şifreleme tekniklerinin kullanılması, verilerin cihazlar arasında aktarılırken korunamamasına yol açmaktadır. Güçlü şifreleme algoritmalarının eksikliği, verilerin yetkisiz kişiler tarafından ele geçirilmesine ve manipüle edilmesine zemin hazırlamaktadır. Özellikle cihazlar ile bulut servisleri arasındaki iletişimde yeterli şifrelemenin sağlanmaması, kullanıcı verilerinin güvenliğini tehdit etmektedir (Fei vd. 2023).

Kimlik doğrulama mekanizmalarındaki yetersizlikler de önemli bir zafiyet olarak ortaya çıkmaktadır. IoT cihazlarının kısıtlı işlem gücü ve enerji kapasiteleri nedeniyle karmaşık kimlik doğrulama süreçlerinin uygulanamaması, cihazların siber saldırganlar tarafından ele geçirilme riskini artırmaktadır. Varsayılan şifrelerin değiştirilmemesi ve güvenli olmayan kimlik doğrulama yöntemlerinin kullanılması, bu cihazların yetkisiz erişimlere karşı savunmasız kalmasına neden olmaktadır (Fei vd. 2023).

Güncelleme ve yama yönetimi konusunda da ciddi eksiklikler bulunmaktadır. IoT cihazlarının düzenli olarak güncellenmemesi, zamanla bu cihazların güvenlik açıkları içeren eski sistemlerle çalışmasına neden olmaktadır. Eski yazılımların kullanıldığı IoT sistemleri, siber saldırganların kolayca hedef alabileceği zayıf noktalar oluşturmaktadır (Schiller vd. 2022). Ayrıca, erişim kontrol mekanizmaları da zayıf kalmakta, yetkisiz kişilerin bu cihazlara erişim sağlamasına ve gizli bilgilere ulaşmasına neden olmaktadır. Özellikle, sağlık sektöründeki IoT cihazlarına yetkisiz erişimlerin meydana gelmesi, hastaların tıbbi verilerinin tehlikeye girmesine neden olabilmektedir (Fei vd. 2023).

Deniz (2019) tarafından yapılan çalışmada, ZigBee gibi yaygın olarak kullanılan teknolojilerde ağa katılım sırasında oluşabilecek güvenlik açıklarına dikkat çekilmiş ve bu açıkların kapatılmasına yönelik yeni bir bulut tabanlı güvenlik yöntemi önerilmiştir. Çalışmada, bulut üzerinden merkezi güvenlik yönetimi sağlanarak düğümlerin güvenli bir şekilde ağa katılımı sağlanmıştır. Bu yöntemle, düğüm bilgileri bulut sistemine kaydedilerek ağdaki güvenlik açıklarının minimize edilmesi hedeflenmiştir.

Fiziksel güvenlik açısından da IoT cihazları önemli zafiyetler barındırmaktadır. Bu cihazların çoğunlukla uzak ve korunmasız ortamlarda bulunması, fiziksel saldırılara karşı savunmasız kalmalarına yol açmaktadır. Cihazların fiziksel olarak ele geçirilmesi, donanım seviyesinde manipülasyon yapılmasına ve cihazın işlevselliğinin bozulmasına neden olabilmektedir (Fei vd. 2023).

Üretici hataları da IoT cihazlarının güvenlik zafiyetlerine sebep olabilmektedir. Birçok cihaz, güvenlik önlemleri yetersiz veya eksik olarak üretilmekte ve piyasaya sürülmektedir. Pazar rekabeti nedeniyle üreticiler, ürünlerini hızlıca piyasaya sürmeye çalışmakta, bu da güvenlik açısından yeterince test edilmemiş cihazların yaygınlaşmasına neden olmaktadır (Schiller vd. 2022).

Binglaw (2021) tarafından yapılan çalışmada, IoT sistemlerinde karşılaşılan güvenlik gereksinimleri, yaygın saldırı türleri ve bu saldırılara karşı uygulanabilecek önlemler kapsamlı bir şekilde ele alınmıştır. Algılama, ağ ve uygulama katmanlarına yönelik saldırılar analiz edilmiş ve bu katmanlardaki güvenlik açıklarına karşı önerilen karşı önlemler sunulmuştur. Ayrıca, akıllı ev uygulamaları örnek olarak ele alınmış ve bu uygulamaların maruz kalabileceği saldırılar ile ilgili çeşitli öneriler geliştirilmiştir. Çalışmada, IoT teknolojisinin geniş çapta benimsenmesi açısından güvenliğin kritik olduğu vurgulanmıştır.

2.2.2 Siber saldırılar

IoT sistemlerinde meydana gelen siber saldırılar, bu sistemlerin güvenliğini ciddi şekilde tehdit etmektedir. Farklı katmanlarda gerçekleşen bu saldırılar, IoT cihazlarının işleyişini bozarak veri kaybına, hizmet kesintilerine ve güvenlik ihlallerine neden olmaktadır. Her bir saldırı türü, farklı yöntemlerle IoT sistemlerini hedef almakta ve sistemlerin güvenilirliğini zedelemektedir. En çok karşılaşılan IoT saldırı tipleri, saldırıların gerçekleştirildiği IoT katmanına göre Çizelge 2.1'de sıralanmaktadır.

Çizelge 2.1 IoT saldırılarının sınıflandırılması (Fei vd. 2023)

Katman	**Olası IoT Saldırıları**
Algılama Katmanı	- Kötü niyetli düğüm saldırısı (Malicious node attack)
	- Yan kanal saldırısı (Side channel attack)
	- Yanlış veri enjeksiyonu saldırısı (False data injection attack)
	- Dinleme (Eavesdropping)
	- Donanım arızası (Hardware malfunctioning)
	- Pil boşaltma saldırısı (Battery drainage attack)
	- Cihaza yetkisiz erişim (Unauthorized admittance)
Ağ Katmanı	- Dağıtılmış Hizmet Engelleme Saldırısı (DDoS) / Hizmet Engelleme Saldırısı (DoS)
	- Dinleme (Eavesdropping)
	- Yönlendirme saldırısı (Routing attack)
	- Ortadaki adam saldırısı (Man-in-the-Middle - MITM attack)
	- Kimlik sahtekarlığı (Spoofing attack)
	- Kötü niyetli düğüm saldırısı (Malicious node attack)
	- Erişim kontrol saldırısı (Access control attack)
Ara Katman	- SQL enjeksiyonu saldırısı (SQL injection attack)
	- Ortadaki adam saldırısı (MITM attack)
	- Taşkın saldırısı (Flooding attack)
	- Bulut zararlı yazılım enjeksiyonu (Cloud malware injection)
	- İmza sarma saldırısı (Signature wrapping attack)
Uygulama Katmanı	- DDoS/DoS saldırısı
	- Erişim kontrol saldırısı (Access control attack)
	- Yanlış veri enjeksiyonu saldırısı (False data injection attack)
	- Kaba kuvvet/sözlük saldırısı (Brute force/dictionary attack)
	- Dinleme saldırısı (Sniffing attack)
Diğer (Gateway)	- Uçtan uca şifreleme (End-to-End encryption)
	- Ekstra arayüzler (Extra interfaces)
	- Donanım yazılımı güncellemeleri (Firmware updates)

Algılama katmanına yönelik saldırılar aşağıda açıklanmıştır:

- Kötü Niyetli Düğüm Saldırısı (Malicious Node Attack), ağda yer alan bir düğümün diğer düğümlere hizmet vermeyi reddetmesiyle gerçekleşmektedir. Bu saldırı sırasında düğümler veri paketlerini manipüle etmekte, yanlış yönlendirmekte ya da tamamen silmektedir. Böyle bir durumda ağın performansı düşmekte ve veri kaybı yaşanmaktadır. Bu saldırılar, ağın işleyişini bozarak hizmet kesintilerine neden olmaktadır.
- Yan Kanal Saldırısı (Side Channel Attack), cihazların fiziksel özelliklerinden faydalanılarak gerçekleştirilen bir saldırı türüdür. Saldırı sırasında cihazın güç tüketimi, zamanlama ya da elektromanyetik sinyaller gibi yan bilgiler kullanılarak şifreleme anahtarlarına erişilmektedir. Yan kanal saldırıları, şifreleme algoritmalarının uygulandığı cihazlarda gizli bilgilerin açığa çıkmasına yol açmaktadır.
- Yanlış Veri Enjeksiyonu Saldırısı (False Data Injection Attack), sisteme hatalı verilerin enjekte edilmesiyle gerçekleşmektedir. Bu saldırı türünde sistem yanlış veri işlemekte ve hatalı sonuçlar üretmektedir. Yanlış veri enjeksiyonu, sistemin çökmesine ya da yanlış kararlar alınmasına neden olabilmektedir.
- Dinleme Saldırısı (Eavesdropping/Sniffing Attack), güvenli olmayan ağ trafiğinin izlenmesi ile gerçekleştirilmektedir. Saldırganlar, şifrelenmemiş ya da yetersiz koruma sağlanmış ağlardan veri çalmakta ve gizli bilgilere erişmektedir. Bu tür saldırılar, kullanıcıların özel bilgilerini ele geçirerek büyük bir güvenlik riski oluşturmaktır.
- Donanım Arızası (Hardware Malfunctioning), IoT cihazlarının donanımsal zayıflıklarından yararlanılarak yapılmaktadır. Donanım arızaları, cihazların performansını olumsuz etkilemekte ve özellikle kritik sistemlerde cihazların işlevsiz hale gelmesine neden olmaktadır. Bu saldırılar, geniş çaplı hizmet kesintilerine yol açabilmektedir.
- Pil Boşaltma Saldırısı (Battery Drainage Attack), IoT cihazlarının pilini bitirmek amacıyla sürekli istek gönderilmesi ya da cihazın güç tüketiminin artırılması ile gerçekleştirilmektedir. Bu tür saldırılar, özellikle düşük enerjili cihazların işlevlerini kaybetmesine neden olmaktadır.

- Cihaza Yetkisiz Giriş (Unauthorized Admittance to the Device), IoT cihazlarına yetkisiz erişim sağlanarak cihazların kontrol edilmesiyle gerçekleşmektedir. Saldırganlar, cihazın işlevlerini ele geçirmek ya da gizli verileri çalmak için bu tür saldırıları gerçekleştirmektedir (Fei vd. 2023).

Ağ katmanına yönelik saldırılar aşağıda açıklanmıştır:

- Dağıtılmış Hizmet Engelleme Saldırısı (DDoS/DoS Attack), ağ kaynaklarının aşırı yüklenmesi sonucunda sistemin hizmet veremez hale gelmesine yol açmaktadır. DDoS saldırılarında birden fazla kaynaktan gelen trafik, sistemin çökmesine ve hizmetlerin durmasına neden olmaktadır.
- Yönlendirme Saldırısı (Routing Attack), ağ trafiğinin yanlış yönlendirilmesi ile yapılmaktadır. Bu saldırılar sonucunda veri paketleri yanlış düğümlere iletilmekte ve ağdaki veri iletimi kesintiye uğramaktadır. Yönlendirme saldırıları, ağın verimliliğini düşürmekte ve iletişim hatalarına yol açmaktadır.
- Ortadaki Adam Saldırısı (Man-in-the-Middle - MITM Attack), iki sistem arasındaki iletişimin kesilerek verilerin değiştirilmesi ya da yakalanması ile gerçekleştirilmektedir. Bu saldırılar, özellikle IoT cihazları arasında paylaşılan hassas bilgilerin ele geçirilmesine neden olmaktadır.
- Kimlik Sahtekarlığı (Spoofing Attack), saldırganların kendilerini başka bir cihaz ya da kişi gibi göstererek sistemlere sızdığı bir saldırı türüdür. Bu saldırılarda kimlik doğrulama süreçlerindeki zayıflıklardan yararlanılmakta ve yetkisiz erişim sağlanmaktadır.
- Erişim Kontrol Saldırısı (Access Control Attack), IoT cihazlarına zayıf erişim kontrol mekanizmaları kullanılarak gerçekleştirilmektedir. Bu tür saldırılar, gizli verilere yetkisiz erişim sağlamakta ve veri sızıntılarına yol açmaktadır (Fei vd. 2023).

Ara katmana yönelik saldırılar aşağıda açıklanmıştır:

- SQL Enjeksiyonu Saldırısı (SQL Injection Attack), veri tabanlarına zararlı SQL

komutları enjekte edilerek yapılmaktadır. Bu saldırılar, veri tabanına yetkisiz erişim sağlamakta ya da verileri manipüle etmektedir.

- Taşkın Saldırısı (Flooding Attack), hedef sisteme aşırı sayıda paket gönderilerek sistemin kaynaklarının tüketilmesi yoluyla gerçekleştirilmektedir. Bu tür saldırılar, sistemin yavaşlamasına ya da hizmet veremez hale gelmesine neden olmaktadır.
- Bulut Zararlı Yazılım Enjeksiyonu (Cloud Malware Injection), bulut sistemlerine zararlı yazılım enjekte edilmesiyle yapılmaktadır. Bu saldırılar sonucunda bulut hizmetlerinde gizli verilere erişilmekte ya da zararlı yazılım barındırılmaktadır.
- İmza Sarma Saldırısı (Signature Wrapping Attack), XML imza algoritmalarındaki güvenlik açıklarının kullanılarak mesajların manipüle edilmesiyle gerçekleştirilmektedir. Bu saldırılar, güvenlik önlemlerini atlatmak amacıyla yapılmaktadır (Fei vd. 2023).

Uygulama katmanına yönelik saldırılar aşağıda açıklanmıştır:

- Kaba Kuvvet/Sözlük Saldırısı (Brute Force/Dictionary Attack), farklı şifre ve kullanıcı adı kombinasyonlarının denenmesi yoluyla yapılmaktadır. Bu saldırılar, özellikle zayıf şifreleme sistemleri ile korunan cihazlarda etkili olmaktadır.
- Ekstra Arayüz Saldırıları (Extra Interfaces Attack), IoT ağ geçitlerinde kullanılan ekstra portlar üzerinden gerçekleştirilen saldırılardır. Bu saldırılar, cihazların arka kapıdan kontrol edilmesine ya da bilgi çalınmasına yol açmaktadır.
- Uçtan Uca Şifreleme Saldırısı (End-to-End Encryption Attack), IoT cihazları arasındaki şifrelenmiş veri iletişimlerini hedef alan saldırılardır. Şifreleme protokollerindeki zayıflıklar kullanılarak verilere yetkisiz erişim sağlanmaktadır.
- Donanım Yazılımı Güncelleme Saldırıları (Firmware Update Attacks), IoT cihazlarının donanım yazılımlarına yapılan müdahalelerle gerçekleştirilmekte ve cihazların kontrol edilmesine neden olmaktadır. Saldırganlar, cihazlara zararlı yazılım yükleyerek sistemleri hedef almaktadır (Fei vd. 2023).

Bu saldırılar, IoT sistemlerinin farklı katmanlarında ciddi güvenlik tehditleri oluşturmakta ve IoT cihazlarının güvenliği sağlanmadığı takdirde veri bütünlüğü, gizlilik ve hizmet sürekliliğini sekteye uğratmaktadır.

2.2.3 Güvenlik gereksinimleri

IoT sistemlerinde güvenlik gereksinimleri, donanım, yazılım ve iletişim teknolojilerindeki sınırlamalardan kaynaklanmaktadır. IoT cihazlarının sınırlı işlem gücü, bellek kapasitesi ve enerji kaynakları nedeniyle, bu cihazlarda güçlü güvenlik önlemlerinin uygulanması zorlaşmaktadır. Güvenlik gereksinimleri, IoT sistemleri için üç ana kategoride sınıflandırılmaktadır: bilgi düzeyi, erişim düzeyi ve fonksiyonel düzey güvenlik gereksinimleri.

Bilgi düzeyi güvenlik gereksinimleri, IoT sistemlerinde üretilen ve paylaşılan verilerin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunmasına odaklanmaktadır. Bu bağlamda, verilerin yetkisiz erişimlerden korunması ve değiştirilmesi ihtimaline karşı güvence altına alınması ve sistemlerin için sürekli erişilebilir olması hedeflenmektedir (Iqbal vd. 2021).

Erişim düzeyi güvenlik gereksinimleri, IoT sistemlerine ve verilere yalnızca yetkili kişilerin erişebilmesini sağlamayı amaçlamaktadır. Bu gereksinimler, kullanıcı kimlik doğrulaması, yetkilendirme mekanizmaları ve erişim kontrolü gibi önlemleri içermektedir. IoT cihazlarının farklı kullanıcılar tarafından erişilebilmesi, bu sistemlerde güçlü bir kimlik doğrulama ve yetkilendirme mekanizmasına ihtiyaç duyulduğunu göstermektedir (Iqbal vd. 2021).

Özkal (2021) tarafından yapılan çalışmada, IoT cihazları arasındaki iletişimin güvenliğinin artırılmasına yönelik bir protokol geliştirilmiştir. Çalışmada, IoT sensörleri ile ağ geçitleri arasındaki iletişimde gizlilik zafiyetlerini ortadan kaldırmak amacıyla karşılıklı kimlik doğrulama sağlayan beş aşamalı bir iletişim protokolü önerilmiştir. Protokol, IoT cihazlarına yönelik bilinen saldırılara karşı test edilmiş ve “Scyther” aracı

kullanılarak formal güvenlik analizleri gerçekleştirilmiştir. Gerçekleştirilen analizler, önerilen protokolün bilinen saldırılara karşı dayanıklı olduğunu ve yüksek seviyede bilgi güvenliği sağladığını ortaya koymuştur.

Fonksiyonel güvenlik gereksinimleri ise IoT sistemlerinin, saldırılar karşısında dahi doğru ve kesintisiz şekilde çalışmasını hedeflemektedir. Bu gereksinimler, sistemlerin işlevselliğinin korunmasını, sistem çökmesi veya bozulmasının önlenmesini ve saldırılar sırasında bile hizmetlerin sürekliliğinin sağlanmasını içermektedir (Iqbal vd. 2021). Özellikle kritik görevleri olan IoT sistemlerinde, bu tür fonksiyonel güvenlik önlemleri hayati önem taşımaktadır.

Saleh (2022) tarafından yapılan çalışmada, IoT veri gizliliğini koruma yöntemlerinin makine öğrenmesi algoritmaları üzerindeki etkileri incelenmiştir. K-anonimlik, l-çeşitlilik ve t-yakınlığı gibi anonimleştirme yöntemlerinin çeşitli makine öğrenmesi modelleri üzerindeki etkileri karşılaştırılmıştır. Ayrıca, federe öğrenme çerçevesine anonimleştirilmiş verilerin entegrasyonu ile gizlilik korunurken minimum bilgi kaybı sağlanabileceği ve her iki yaklaşımın avantajlarının birleştirilerek etkin bir sistem kurulabileceği gösterilmiştir. Çalışmanın sonuçları, anonimleştirme yöntemlerinin gizlilik düzeyini artırırken, modellerin performansı üzerinde farklı derecelerde bilgi kaybına yol açtığını ortaya koymuştur.

2.3 Makine Öğrenmesi

Makine öğrenmesi, bilgisayarların veri analizi yoluyla öğrenme kabiliyeti kazanmasını sağlayan bir süreç olarak tanımlanmakta ve bu süreçte, mevcut verilerden örüntüler çıkarılarak gelecekteki durumlar hakkında tahminlerde bulunulmaktadır. Alpaydın'a göre, makine öğrenmesinin temel amacı, büyük veri setlerinden anlamlı ve genellenebilir modeller çıkarmaktır (Alpaydın 2014). Bu modeller hem tahminsel hem de betimleyici amaçlarla kullanılabilmekte olup, farklı uygulama alanlarında başarılı sonuçlar elde edilmesini sağlamaktadır. Makine öğrenmesi süreci, şu temel adımlardan oluşmaktadır: veri toplama, veri ön işleme, model seçimi ve tasarımı, model eğitimi, model değerlendirme ve doğrulama. Veri toplama aşamasında, öğrenme süreci için gerekli olan

veriler, çeşitli kaynaklardan toplanmakta ve işlenmektedir. Daha sonra bu verilerden öğrenilecek modelin parametreleri belirlenmekte ve model eğitilmektedir. Model eğitimi, modelin doğru tahminler yapabilme kapasitesini artırmayı hedeflemektedir. Modelin eğitimi sonrası performansı, test verileri ile değerlendirilmekte ve modelin genel performansı ölçülmektedir. Bu süreçler, makine öğrenmesi modellerinin etkinliği ve doğruluğu için kritik öneme sahiptir. Alpaydın, bu sürecin her adımının dikkatle planlanması ve uygulanması gerektiğini vurgulamaktadır, çünkü her aşama, nihai modelin başarısını doğrudan etkilemektedir (Alpaydın 2014).

Makine öğrenmesi algoritmaları, veri yapısına ve problem türüne göre farklı kategorilere ayrılmakta olup, en yaygın olarak kullanılan kategoriler arasında denetimli öğrenme (supervised learning), denetimsiz öğrenme (unsupervised learning) ve pekiştirmeli öğrenme (reinforcement learning) yer almaktadır. Her bir kategori, belirli veri yapılarına ve problem türlerine uygun algoritmaları içermekte ve bu algoritmalar, çeşitli uygulama alanlarında etkin bir şekilde kullanılmaktadır. Denetimli öğrenme, etiketlenmiş veri setleri üzerinde çalışan ve bu verilerden öğrenen algoritmalar tarafından gerçekleştirilmektedir. Bu yöntem, girdi veri kümesi ile bu veriye karşılık gelen çıktı etiketleri arasındaki ilişkiyi öğrenmekte ve öğrendiklerini yeni verilere uygulayarak tahminlerde bulunmaktadır. Denetimli öğrenme, genellikle iki ana problem türünde kullanılmaktadır: sınıflandırma ve regresyon. Sınıflandırma probleminde, modelin çıktısı sınırlı sayıda kategoriden biri olarak belirlenmektedir: örneğin, bir e-posta mesajının spam veya spam değil olarak sınıflandırılması gibi. Regresyon probleminde ise, modelin çıktısı sürekli bir değer olarak belirlenmektedir: örneğin, bir evin fiyatının tahmin edilmesi gibi. Denetimli öğrenme algoritmalarına destek vektör makineleri, karar ağaçları, lojistik regresyon ve yapay sinir ağları gibi yöntemler örnek olarak gösterilebilmektedir. Alpaydın, denetimli öğrenmenin, veri etiketlerinin mevcut olduğu durumlarda en yaygın kullanılan öğrenme türü olduğunu ve bu yöntemin özellikle doğruluğu yüksek tahminler yapmak için uygun olduğunu belirtmektedir (Alpaydın 2014).

Denetimsiz öğrenme, etiketlenmemiş veriler üzerinde çalışan ve veri kümesindeki örüntüleri veya yapıları ortaya çıkarmayı amaçlayan bir öğrenme türü olarak

tanımlanmaktadır. Bu yöntemde, model eğitim verileri üzerinde belirli kalıpları keşfetmek için çalışır, ancak sonuçlar daha az belirgin olabilmektedir. Denetimsiz öğrenme, veri kümesinde gizli yapıları ortaya çıkarmak, veri kümesini segmentlere ayırmak veya boyutlarını azaltmak için kullanılmaktadır. Alpaydın, denetimsiz öğrenmenin, özellikle veri kümelerinde sıkça rastlanan yapıların ve örüntülerin tespit edilmesinde etkili olduğunu belirtmektedir. Denetimsiz öğrenme algoritmalarına örnek olarak K-ortalama kümeleme, hiyerarşik kümeleme ve ana bileşen analizi verilmektedir. Pekiştirmeli öğrenme ise, bir ajanın bir ortamda belirli bir görev veya problemle ilgili deneyim kazandıkça öğrenme sürecini ifade eden bir öğrenme türü olarak tanımlanmaktadır. Bu süreçte, ajan belirli eylemleri gerçekleştirerek ödüller veya cezalar almakta ve bu geri bildirimlere dayanarak gelecekteki kararlarını optimize etmektedir. Alpaydın, pekiştirmeli öğrenme yöntemlerinin özellikle oyun teorisi, robotik ve otonom sistemler gibi alanlarda yaygın olarak kullanıldığını vurgulamaktadır. Bu öğrenme türü, ajanın çevresiyle sürekli etkileşim içinde bulunarak kendi stratejilerini geliştirmesini sağlar. Pekiştirmeli öğrenme algoritmaları arasında Q-öğrenme ve derin pekiştirmeli öğrenme gibi yöntemler yer almaktadır. Bu algoritmalar, ajanın en iyi eylemi seçmesini ve ödülünü maksimize etmesini hedeflemektedir (Alpaydın 2014).

Makine öğrenmesi modellerinin performansını değerlendirmek amacıyla çeşitli metrikler kullanılmaktadır. Bu metrikler, modelin doğruluğunu, kesinliğini, duyarlılığını ve genel başarımını ölçmek için önemli bir rol oynamaktadır. Aşağıda, makine öğrenmesi modellerinde kullanılan başlıca performans metrikleri ve bu metriklerin formülleri yer almaktadır (Özdoğan 2024).

Karmaşıklık matrisi (confusion matrix), makine öğrenmesi ve veri bilimi alanlarında, sınıflandırma algoritmalarının performansını ölçmek ve değerlendirmek için en yaygın kullanılan araçlardan biridir. Modelin sınıflandırma sonuçlarını detaylandırarak doğru ve yanlış sınıflamaları ayrıntılı bir şekilde ortaya koymaktadır. Karmaşıklık matrisi, özellikle ikili sınıflandırma problemlerinde yaygın olarak kullanılmasına rağmen, çok sınıflı sınıflandırma problemlerinde de uygulanabilmektedir. Bu matris, modelin gerçek ve tahmin edilen sınıflarını karşılaştırarak dört temel değeri ölçmektedir: doğru pozitif (TP), doğru negatif (TN), yanlış pozitif (FP) ve yanlış negatif (FN). Doğru pozitif, gerçek

pozitif olan ve model tarafından doğru bir şekilde pozitif olarak sınıflandırılmış örnekleri ifade ederken; doğru negatif, gerçek negatif olan ve model tarafından doğru bir şekilde negatif olarak sınıflandırılmış örnekleri ifade etmektedir. Yanlış pozitif, gerçek negatif olan ancak model tarafından yanlış bir şekilde pozitif olarak sınıflandırılan örneklerdir ve bu hata türü "Type I error" olarak da bilinmektedir. Yanlış negatif ise gerçek pozitif olan fakat model tarafından yanlış bir şekilde negatif olarak sınıflandırılan örneklerdir ve "Type II error" olarak adlandırılmaktadır.

Doğruluk (accuracy), modelin doğru şekilde sınıflandırdığı örneklerin, toplam örneklere oranını gösteren bir ölçüttür. Bu metrik, sınıflandırma problemlerinde sıklıkla kullanılmakta ve modelin genel başarı oranını yansıtmaktadır. Doğruluk, şu formülle hesaplanmaktadır:

$$Doğruluk = \frac{TP + TN}{TP + TN + FP + FN} \tag{2.1}$$

Bu formülde:

- TP (Doğru Pozitif), pozitif olarak doğru sınıflandırılan örnekleri,
- TN (Doğru Negatif), negatif olarak doğru sınıflandırılan örnekleri,
- FP (Yanlış Pozitif), pozitif olarak yanlış sınıflandırılan örnekleri,
- FN (Yanlış Negatif) ise negatif olarak yanlış sınıflandırılan örnekleri ifade eder.

Kesinlik (precision), modelin pozitif olarak sınıflandırdığı örneklerin ne kadarının gerçekten doğru olduğunu belirleyen bir değerlendirme metriğidir. Kesinlik, özellikle hatalı pozitif sınıflandırmaların önemli olduğu durumlarda kullanılmaktadır. Kesinlik şu formül ile hesaplanmaktadır:

$$Kesinlik = \frac{TP}{TP + FP} \tag{2.2}$$

Duyarlılık (recall), modelin pozitif sınıfa ait örnekleri ne kadar başarılı bir şekilde tespit ettiğini ölçen bir değerlendirme metriğidir. Gerçek pozitiflerin ne kadarının doğru bir şekilde sınıflandırıldığını ölçmektedir. Duyarlılık, aşağıdaki formül ile hesaplanmaktadır:

$$Duyarlılık = \frac{TP}{TP + FN} \tag{2.3}$$

F1-Skoru (F1-Score), kesinlik ve duyarlılığın harmonik ortalamasını veren bir metriktir. Dengesiz veri kümelerinde, kesinlik ve duyarlılık arasındaki dengeyi sağlamak için kullanılmaktadır. F1-Skoru şu formülle hesaplanmaktadır:

$$F1 - Skoru = 2 \times \frac{Kesinlik\ x\ Duyarlık}{Kesinlik + Duyralık} \tag{2.4}$$

ROC (Receiver Operating Characteristic) eğrisi, modelin pozitif sınıfı ayırt etme yeteneğini görsel olarak ifade etmektedir. ROC eğrisinde, doğru pozitif oranı ile yanlış pozitif oranı grafiğe dökülmektedir. Eğri altındaki alan olan AUC (Area Under the Curve) değeri ise modelin genel performansını özetlemektedir. AUC değeri 0.5 ile 1 arasında değişmekte olup 1, en iyi performansı, 0.5 ise rastgele tahmini göstermektedir (Özdoğan 2024).

Bu performans metrikleri, makine öğrenmesi modellerinin etkinliğini değerlendirmek ve farklı modelleri karşılaştırmak açısından büyük önem taşımaktadır. Her bir metrik, modelin güçlü ve zayıf yönlerini belirlemek için kullanılmaktadır.

Makine öğrenmesi, güvenlik alanında geniş bir uygulama yelpazesine sahip olup, siber tehditlerin tespiti, sınıflandırılması ve önlenmesi gibi çeşitli görevlerde kullanılmaktadır. Makine öğrenmesi algoritmalarının, büyük veri setleri üzerinde öğrenme yaparak, bilinen ve bilinmeyen tehditleri tespit edebilme yeteneği kazandığı belirtilmektedir. Bu algoritmalar, saldırı tespit sistemlerinde (Intrusion Detection Systems - IDS), zararlı yazılım tespitinde, anomali algılamada ve veri sızıntısı önleme sistemlerinde yaygın olarak kullanılmaktadır. Makine öğrenmesi, geleneksel imza tabanlı güvenlik

çözümlerinin sınırlarını aşmak için geliştirilmiş anomali tabanlı tespit yöntemleri ile birleştirilmiştir. Bu yöntemler, sürekli değişen siber tehditlere karşı daha dinamik ve proaktif bir savunma mekanizması sunmaktadır. Ayrıca, büyük veri setlerinin analizi yoluyla, makine öğrenmesi tabanlı sistemler, bilinmeyen tehditlerin erken aşamada tespit edilmesini sağlamaktadır. Siber güvenlikte makine öğrenmesinin kullanımı, saldırı tespitinde daha yüksek doğruluk oranları elde edilmesine olanak tanımaktadır. Özellikle, anomali tespiti alanında kullanılan makine öğrenmesi algoritmaları, normal davranışlardan sapmaları tespit ederek potansiyel tehditleri belirleyebilmektedir. Bu yaklaşım hem bilinen saldırılara hem de sıfırıncı gün (zero-day) saldırılarına karşı etkili bir koruma sağlayabilmektedir.

IoT cihazlarının güvenliği için makine öğrenmesi, önemli bir çözüm olarak benimsenmiştir. IoT ağlarında güvenliği sağlamak için kullanılan makine öğrenmesi algoritmaları, anomali algılama, saldırı sınıflandırma ve güvenlik durumu değerlendirmesi gibi çeşitli görevlerde kullanılmaktadır. IoT ortamlarında saldırıların sürekli değişim geçirmesi nedeniyle, makine öğrenmesi tabanlı saldırı tespit ve saldırı önleme sistemleri, IoT ağlarının güvenliğini artırmak için kritik öneme sahiptir. Bu sistemler, ağ trafiğini analiz ederek, normal ve anormal davranışları öğrenmekte ve bu sayede, yeni ortaya çıkan tehditlere karşı etkili bir savunma sağlamaktadır. Makine öğrenmesi, IoT güvenliğinde sürekli öğrenme ve adaptasyon yetenekleri sunarak, güvenlik açıklarının zamanında tespit edilmesini ve IoT cihazlarının güvenliğinin sağlanmasını mümkün kılmaktadır. IoT güvenliğinde makine öğrenmesi, özellikle düşük kaynak tüketimi ve yüksek doğruluk oranları sağlama konusundaki avantajları nedeniyle tercih edilmektedir. IoT cihazlarının sınırlı işlem gücü ve enerji kaynakları, makine öğrenmesi algoritmalarının optimize edilmesini gerektirmekte olup, bu optimizasyonlar sayesinde saldırı tespit sistemlerinin performansı artırılmaktadır. Bu bağlamda, makine öğrenmesi, IoT cihazlarının korunmasında proaktif bir güvenlik çözümü sunmaktadır.

Çekmez (2022) tarafından yapılan çalışmada, IoT ağlarına yönelik yapılan çeşitli saldırıların derin öğrenme ile tespit edilmesi için veri odaklı bir ağ saldırı sınıflandırma sistemi geliştirilmiştir. Model, CICIDS2017 veri seti üzerinde test edilmiş ve ağırlıklı ortalama %99.94 F1-Skoruna ulaşmıştır.

Çıkmazel (2022) tarafından yapılan çalışmada, IoT verilerindeki anomalilerin tahmin edilmesi için Çok Çözünürlüklü Seviyeler Arası İyileştirme adlı yeni bir mimari geliştirilmiştir. Mimarinin performansı, Elektrik Tüketimi ve New York City Taksi Yolcu verileri üzerinde test edilmiş ve diğer modellere göre daha iyi performans sergilediği görülmüştür.

Emeç (2022) tarafından yapılan çalışmada, IoT cihazları arasındaki iletişim güvenliğini artırmak amacıyla hibrit bir derin öğrenme modeli geliştirilmiştir. CIC-IDS-2018 ve BoT-IoT veri setleri kullanılarak saldırı tespit sistemleri tasarlanmış ve önerilen modelin doğruluk ve F1-Skoru gibi performans metriklerinde başarılı olduğu ortaya konulmuştur.

Ergün (2023) tarafından yapılan çalışmada, şifreli trafikte bile IoT cihazlarının paket boyutlarından sınıflandırılabileceği gösterilmiştir. Bu sınıflandırmaya karşı savunma yöntemleri olarak "Dolgu (Padding)" ve "Diferansiyel Mahremiyet (Differential Privacy)" yaklaşımları kullanılmıştır. XGBoost ve LSTM (Long Short-Term Memory) algoritmaları ile yapılan saldırı tespit modelleri yüksek doğruluk oranlarına ulaşmış ve "Fourier Pertürbasyon Algoritması" yönteminin "mahremiyet-fayda" dengesi açısından diğer dolgu yöntemlerinden daha etkili olduğu sonucuna varılmıştır.

Kolukısa (2024) tarafından yapılan çalışmada, IoT tabanlı araç tipi sınıflandırması ve ağ anomali tespiti için makine öğrenmesi yaklaşımları geliştirilmiş ve %92.92 doğruluk oranına ulaşılmıştır. Ayrıca, siber güvenlik risklerini azaltmak için lojistik regresyon modeli ve yapay arı kolonisi algoritması kullanılarak yeni bir ağ saldırı tespit modeli önerilmiştir.

Salati (2024) tarafından yapılan çalışmada, ağ güvenliği için makine öğrenmesi yöntemlerini kullanan yeni bir izinsiz giriş tespit sistemi geliştirilmiştir. Evrişimli sinir ağları (Convolutional Neural Networks - CNN) ile birleştirilmiş metasezgisel tabanlı bir öznitelik seçme yöntemi kullanılarak saldırı tespiti gerçekleştirilmiş ve yüksek doğruluk oranlarına ulaşılmıştır.

Yaraş (2024) tarafından gerçekleştirilen çalışmada, IoT ağlarında meydana gelen DDoS saldırılarının büyük veri ortamında analiz edilmesi ve tespit edilmesi amacıyla derin öğrenme yöntemleri kullanılmıştır. Hibrit bir derin öğrenme algoritması olan CNN ve LSTM modelleri birleştirilmiş ve %99.995 doğruluk oranı elde edilmiştir.

Bu çalışmalar, makine öğrenmesi ve derin öğrenme yöntemlerinin IoT ağlarındaki siber tehditleri tespit etmedeki başarılarını ortaya koymaktadır. Makine öğrenmesi, IoT güvenliğinde sürekli öğrenme ve adaptasyon yetenekleri sunarak, güvenlik açıklarının zamanında tespit edilmesini ve IoT cihazlarının güvenliğinin sağlanmasını mümkün kılmaktadır. IoT güvenliğinde makine öğrenmesi, özellikle düşük kaynak tüketimi ve yüksek doğruluk oranları sağlama konusundaki avantajları nedeniyle tercih edilmektedir.

2.4 Saldırı Tespit Sistemleri

Siber güvenlik dünyasında saldırı tespit sistemleri (IDS), ağlar ve sistemler üzerindeki potansiyel tehditleri ve saldırıları tespit etmek için kullanılan kritik araçlardır. IDS, siber saldırıları önlemek için proaktif bir güvenlik katmanı sağlamakta ve ağ trafiğini veya sistem davranışlarını sürekli izleyerek, anormal veya kötü niyetli etkinlikleri tanımlamaya çalışmaktadır (Özdoğan 2024).

IoT cihazlarının yaygınlaşmasıyla birlikte, bu cihazların güvenliğini sağlamak için geleneksel güvenlik yaklaşımları yetersiz kalmaya başlamıştır. Bu bağlamda, IDS, IoT ağlarının korunmasında kritik bir rol oynamaktadır. Geleneksel IDS sistemlerinin genellikle imza tabanlı olduğu ve bilinen saldırı kalıplarına dayandığı bilinmektedir. Ancak, IoT ortamlarının dinamik yapısı ve saldırıların sürekli değişmesi, imza tabanlı sistemlerin etkinliğini sınırlamaktadır (Özdoğan 2024).

Kuriş (2019) tarafından yapılan çalışmada, IoT ekosisteminde yapay zeka tabanlı bir saldırı tespit sistemi geliştirilmiştir. Çalışmada, IoT cihazlarının güvenliğini sağlamak amacıyla anomali tabanlı saldırı tespit sistemlerinin kullanılmasının önemi

vurgulanmıştır. Yapay zeka algoritmaları kullanılarak IoT cihazlarına yönelik güncel ve bilinmeyen siber saldırıların tespit edilmesi hedeflenmiştir.

Yavuz (2020) tarafından yapılan çalışmada, IoT tabanlı ağlarda yönlendirme saldırılarının tespiti için derin öğrenme tabanlı bir model geliştirilmiş ve Decreased Rank, Hello Flood ve Version Number gibi üç farklı yönlendirme saldırısı üzerinde durulmuştur. Derin öğrenme modelleri çeşitli veri kümeleri üzerinde test edilerek yüksek başarı oranları elde edilmiş, özellikle Hello Flood saldırısında %99 F1-Skoru ile en yüksek performansın elde edildiği belirtilmiştir. Ayrıca, bu modellerin farklı ağ topolojilerine uyarlanabilirliği ve ölçeklenebilirliği de ele alınmıştır.

Amarouche (2021) tarafından yapılan çalışmada, IoT için saldırı tespitinde makine öğrenmesi ve derin öğrenme yöntemlerinin performansları karşılaştırılmıştır. UNSW-NB15 veri kümesi üzerinde yapılan deneylerde, klasik makine öğrenmesi yöntemleri ve derin öğrenme yöntemleri uygulanmış ve derin öğrenme modellerinin daha yüksek doğruluk oranlarına ulaştığı tespit edilmiştir. CNN-LSTM modeli %87,34 doğruluk oranına sahipken, klasik makine öğrenmesi yöntemlerinden Rastgele Orman %87,09 doğruluk oranına ulaşmıştır. Bu çalışma özelinde IoT saldırı tespit sistemlerinde derin öğrenme algoritmalarının daha etkili olduğu sonucu elde edilmiştir.

Balcı (2021) tarafından yapılan çalışmada, IoT ekosisteminde yapay zeka destekli bir saldırı tespit sistemi geliştirilmiştir. IoT cihazlarının düşük işlemci gücü ve güvenlik açıkları gibi zorlukları ele alınmış ve bu cihazlara yönelik saldırıların tespiti için makine öğrenmesi yöntemleri kullanılmıştır. Yapay sinir ağları, K-en yakın komşular ve karar ağaçları gibi algoritmalar kullanılarak bir saldırı tespit sistemi geliştirilmiş ve sistemin performansı, sıfırıncı gün saldırılarına karşı test edilmiştir.

Adamu (2022) tarafından yapılan çalışmada, IoT ağ cihazları üzerindeki siber saldırıların tespiti ve analizi için bir yöntem geliştirilmiştir. Geleneksel imza tabanlı izinsiz giriş tespit sistemlerinin modern saldırı türlerini tespit edememesi üzerine, IoT ağ trafiğinin analiz edilmesine dayanan makine öğrenmesi algoritmalarının kullanımı önerilmiştir.

Aydın (2022) ise IoT botnetleri ile gerçekleştirilen DDoS saldırılarının tespiti için çevrim içi bir ağ saldırı tespit sistemi geliştirmiştir. CNN tabanlı bir model kullanılarak ağ verilerinin zamansal ve konumsal özelliklerinden yararlanılmıştır. Sistem, özellikle IoT botnetlerinden gelen kötü niyetli trafiği hızlı ve doğru bir şekilde tespit etmeyi amaçlamaktadır.

Taş (2022) tarafından yapılan çalışmada, IoT için akıllı saldırı tespit sistemleri geliştirilmiştir. "Metasezgisel Optimizasyon" algoritmaları ile "Topluluk Öğrenme" algoritmaları bir arada kullanılarak bir saldırı tespit modeli önerilmiştir. NSL-KDD ve BoT-IoT veri setleri üzerinde yapılan testlerde, önerilen model %99.63 doğruluk oranına ulaşmıştır.

Tekin (2022) tarafından yapılan çalışmada, IoT uygulamaları için saldırı tespit yöntemlerinin geliştirilmesi üzerine odaklanılmıştır. DDoS, DoS ve kaba kuvvet gibi saldırı türleri incelenmiş ve makine öğrenmesi algoritmaları kullanılarak tespit modelleri oluşturulmuştur. Deneysel sonuçlar, önerilen yöntemlerin saldırı tespitinde yüksek doğruluk oranlarına ulaştığını göstermektedir.

Kwaider (2023) tarafından yapılan çalışmada, IoT ağlarında siber saldırıları tespit etmek amacıyla makine öğrenmesi algoritmaları kullanılmış ve yüksek doğruluk oranı elde edilmiştir. Sultan (2023) ise IoT ve siber fiziksel sistemlerde saldırı tespiti için denetimli makine öğrenmesi algoritmalarını kullanmıştır.

Bu çalışmalar, IDS'nin IoT güvenliğindeki kritik rolünü ve makine öğrenmesi tabanlı yaklaşımların etkinliğini ortaya koymaktadır. IoT ağlarında meydana gelen DDoS, yönlendirme saldırıları ve sıfırıncı gün saldırıları gibi yaygın tehditlerin tespit edilmesinde geliştirilen modellerin başarı oranları yüksek olup, farklı ağ topolojilerine uyarlanabilirlik ve ölçeklenebilirlik gibi yönleri incelenmiştir.

3. MATERYAL VE YÖNTEM

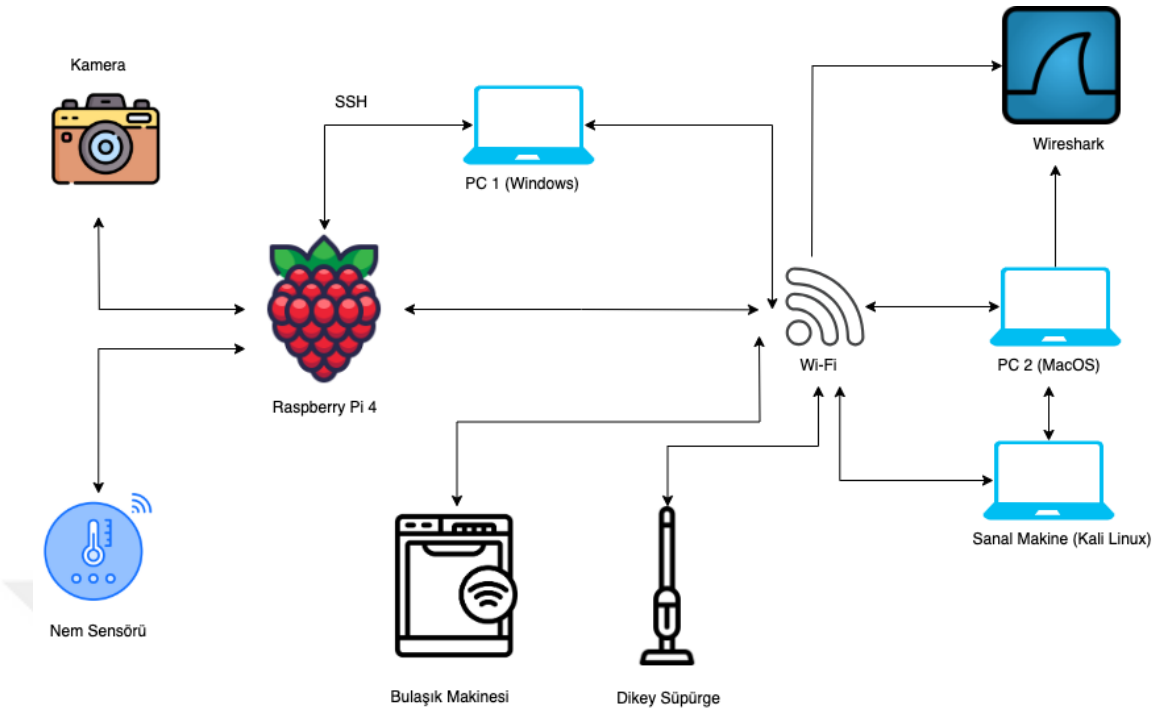
Bu bölümde, çalışma sırasında kullanılan materyaller ve çalışmanın uygulanmasında izlenen yöntemler ayrıntılı bir şekilde sunulmaktadır. Ayrıca, IoT cihazlarına yönelik çeşitli siber savunma stratejileri ile makine öğrenmesi ve derin öğrenme algoritmaları kullanılarak tasarlanan bir saldırı tespit sistemi bu bölümde açıklanmıştır.

3.1 Materyal

Bu çalışma, IoT cihazlarından elde edilen ağ trafiği verilerini kullanarak bir saldırı tespit sistemi geliştirmeyi amaçlamaktadır. Deneysel ortam, aşağıdaki bileşenlerden oluşmaktadır:

- IoT cihazları ve ağ yapısı: Raspberry Pi 4 cihazına SSH (Secure Shell) protokolü aracılığıyla uzaktan bağlantı kurulmuştur. Bu sayede Raspberry Pi cihazı tamamen komut satırı aracılığıyla kontrol edilebilir hale gelmiştir. Bu noktada cihaz üzerinde dosya işlemleri, sistem ayarları ve yazılım yüklemeleri gibi işlemler gerçekleştirilebilmektedir. Raspberry Pi cihazı hem internete bağlanarak bir IoT işlevi görmekte ayrıca kendine has donanımsal özellikleri sayesinde bilgisayar işlevi görebilmektedir. Raspberry Pi cihazına ayrıca kamera ve nem sensörü entegre edilmiştir.
- Akıllı ev cihazları: Wi-Fi ile ortak ağa bağlanabilen Bosch marka bulaşık makinesi ve LG marka elektrikli süpürge de bu çalışma kapsamında ele alınmıştır.
- Veri toplama araçları: Çalışmada, Wireshark ile ağ trafiği dinlenmiş ve elde edilen veriler pcap formatında kaydedilmiştir.
- Saldırı simülasyonu: Çalışmada, Kali Linux aracılığıyla çeşitli siber saldırı araçları kullanılmıştır.

Çalışmada veri elde etmek üzere oluşturulan ortam mimarisi Şekil 3.1’de gösterilmektedir.



Şekil 3.1 IoT ortam mimarisi

3.2 Yöntem

Bu çalışmada, IoT cihazlarına yönelik siber saldırıların tespiti amacıyla saldırgan perspektifinden bir saldırı tespit sistemi geliştirilmesi hedeflenmiştir. Çalışma, IoT ortamını simüle ederek, gerçek dünya senaryolarına uygun şekilde saldırganların kullanabileceği teknikleri incelemek üzere yapılandırılmıştır. İlk aşamada, Kali Linux sanal makinesi üzerinde, ağ güvenliği ve sızma testlerinde yaygın olarak kullanılan araçlar yardımıyla Raspberry Pi cihazı ve bu cihaza bağlı IoT cihazlarına yönelik çeşitli siber saldırılar gerçekleştirilmiştir. Saldırı süresince, ağ trafiği Wireshark programı ile ayrıntılı olarak izlenmiş ve tüm ağ paketleri pcap formatında kaydedilmiştir. Bu ham veri, daha sonraki analizler için önemli bir kaynak oluşturmuştur. Toplanan pcap dosyaları, Python programlama dili kullanılarak geliştirilen özel bir yazılım aracılığıyla işlenmiş ve csv formatına dönüştürülerek yapısal bir veri setine dönüştürülmüştür. Oluşturulan veri seti, makine öğrenmesi ve derin öğrenme algoritmaları kullanılarak analiz edilmiş ve IoT cihazlarına yönelik saldırıların tespiti için bir saldırı tespit sistemi geliştirilmiştir. Bu kapsamda, farklı sınıflandırma ve anomali tespit yöntemleri denenmiş, sistemin başarım

oranını artırmak amacıyla çeşitli özellik çıkarımı ve optimizasyon teknikleri uygulanmıştır. Daha sonra aynı işlemler akıllı ev ortamına bağlı cihazlar için de gerçekleştirilmiştir.

3.3 Çalışma Kapsamında Gerçekleştirilen Siber Saldırılar

Siber güvenlik alanında, IoT cihazlarına yönelik gerçekleştirilen saldırılar, bu cihazların sınırlı kaynakları ve genellikle yetersiz güvenlik önlemleri nedeniyle ciddi tehditler oluşturmaktadır. Brute force saldırıları, bu tür cihazlara yönelik olarak yaygın bir şekilde kullanılmaktadır. Brute force saldırısı, sistemin kimlik doğrulama mekanizmasına yönelik çok sayıda kullanıcı adı ve şifre kombinasyonunun denenmesiyle gerçekleştirilmekte ve doğru kimlik bilgileri bulunana kadar bu deneme süreci devam etmektedir. IoT cihazlarının çoğunlukla varsayılan veya zayıf şifrelerle korunması, bu cihazları brute force saldırılarına karşı savunmasız hale getirmektedir. Saldırganlar, bu zafiyetten faydalanarak yetkisiz erişim elde edebilir ve sistemin kontrolünü ele geçirebilir.

Bu çalışmada, brute force saldırılarının simülasyonu amacıyla "Hydra aracı" kullanılmıştır. Hydra, SSH protokolü üzerinden brute force saldırıları gerçekleştirmek için tercih edilen bir araçtır. Çalışmada, IoT cihazları ve akıllı ev aletlerine yönelik bir brute force saldırısı gerçekleştirilmiştir. "GitHub" adlı platformda, açık kaynak olarak yayımlanan ve yaygın kullanıldığı düşünülen 10.000 satırlık bir şifre listesi ile sıkça kullanılan kullanıcı adları kullanılarak gerçekleştirilen bu saldırıda, sistemin zayıf şifreleme mekanizmaları hedef alınmıştır (Anonymous 2024). Bu saldırı yöntemi, öncelikle hedef sistemin IP adresinin ve SSH servisinin açık olup olmadığının tespit edilmesiyle başlatılmıştır. Daha sonra, Hydra aracı kullanılarak belirlenen hedef IP adresine karşı kullanıcı adı ve şifre kombinasyonlarının denenmesi sürecine geçilmiştir.

Port tarama saldırıları, bir sistemdeki açık portların ve bu portlar üzerinde çalışan hizmetlerin belirlenmesi amacıyla yapılmaktadır. Saldırganlar, açık portları ve savunmasız hizmetleri tespit ettikten sonra, bu zafiyetlerden faydalanarak sisteme erişim

sağlamaya çalışırlar. IoT cihazlarının sürekli çevrim içi olması ve açık portlar barındırması, bu cihazları port tarama saldırılarına karşı savunmasız hale getirmektedir.

Çalışma kapsamında, port tarama işlemleri "Nmap" aracı kullanılarak gerçekleştirilmiştir. IoT cihazları ve akıllı ev aletleri üzerinde yapılan bu port taraması ile açık portlar ve çalışan hizmetler tespit edilmiştir. Bu aşamada, saldırı tespit sisteminin tarama girişimlerini izleyip tespit etmesi amaçlanmıştır. Port tarama saldırıları, sistemdeki güvenlik açıklarının tespit edilmesi açısından önemli olup, erken fark edilmesi güvenlik açısından kritik öneme sahiptir. IoT cihazları ve akıllı ev aletleri üzerinde yapılan nmap taraması ile açık portlar ve çalışan hizmetler tespit edilmiştir. Bu süreçte, saldırı tespit sisteminin tarama girişimlerini izleyip tespit etmesinin sağlanması amaçlanmıştır. Port tarama işlemleri, sistemdeki güvenlik açıklarının belirlenmesi açısından önemli olarak değerlendirilmiştir.

Zafiyet taramaları, bilinen güvenlik açıklarının tespit edilmesi ve bu açıkların kullanılarak sistemlere sızılması amacıyla gerçekleştirilen saldırılardır. Saldırganlar, sistemdeki güvenlik açıklarını belirleyerek yetkisiz erişim elde edebilir ve bu cihazlar üzerinde çeşitli işlemler gerçekleştirebilir. IoT cihazları, genellikle güncellenmemiş yazılımlar ve yetersiz güvenlik yapılandırmaları nedeniyle zafiyet taramalarına karşı savunmasızdır.

Bu çalışmada zafiyet taraması yapmak amacıyla "Metasploit Framework" kullanılmıştır. "DNS/bind_tkey" zafiyeti üzerinden yapılan bu taramada, IoT cihazları ve akıllı ev aletlerinin DNS hizmetlerindeki güvenlik açıkları tespit edilmeye çalışılmıştır. Metasploit aracı kullanılarak yapılan bu saldırıda, DNS sunucusuna yönelik zafiyetler analiz edilmiş ve saldırı tespit sisteminin bu tür girişimleri tespit etmesi amaçlanmıştır.

DoS saldırıları, hedef cihaz veya ağın aşırı yüklenerek hizmet veremez hale getirilmesi amacıyla gerçekleştirilen saldırılardır. Bu tür saldırılarda, saldırganlar hedef sisteme aşırı miktarda veri göndererek kaynakların tükenmesine ve hizmet aksamasına yol açmaktadır. IoT cihazları, sınırlı kaynaklara sahip olmaları nedeniyle DoS saldırılarına karşı daha savunmasızdır.

Çalışmada DoS saldırıları “hping” aracı kullanılarak gerçekleştirilmiştir. IoT cihazlarına yönelik yapılan bu saldırıda, cihaza aşırı miktarda trafik gönderilmiş ve cihazın hizmet veremez hale getirilmesi amaçlanmıştır. Saldırı tespit sistemi, trafik hacmindeki bu artışı izleyerek DoS saldırılarını tespit etmeye yönelik olarak yapılandırılmıştır. DoS saldırılarının erken tespiti, IoT cihazlarının sürekli işleyişinin korunması açısından önem taşımaktadır.

Kamera erişimi saldırıları, saldırganların güvenlik kameralarına veya diğer görüntüleme cihazlarına izinsiz erişim sağlama amacıyla gerçekleştirilen saldırılardır. Bu tür saldırılar, gizli görüntülerin ele geçirilmesine veya cihazların kontrolünün saldırganlara geçmesine neden olabilmektedir. Bu çalışmada, kamera erişim saldırısı “wget” aracı kullanılarak gerçekleştirilmiştir. Raspberry Pi’ye bağlı bir güvenlik kamerasına izinsiz erişim sağlanmaya çalışılmış ve bu girişim saldırı tespit sistemi tarafından izlenmiştir. Kamera ve benzeri IoT cihazlarının güvenliği, kişisel gizliliğin korunması açısından önemlidir ve bu tür saldırılara karşı önlem alınması gerekmektedir.

Sensör verilerine izinsiz erişim saldırıları, saldırganların IoT cihazlarındaki sensörlerden gelen verileri manipüle etmeye çalıştığı saldırılardır. Sensör verilerinin manipüle edilmesi, cihazların doğru çalışmasını engelleyebilir ve sistemin genel güvenliğini tehlikeye atabilir. Çalışmada, “Flask” aracı kullanılarak sensör verilerine izinsiz erişim sağlanmaya çalışılmıştır. Bu girişimde, sensör verilerinin manipüle edilip edilemeyeceği test edilmiş ve saldırı tespit sisteminin bu girişimleri tespit etmesi sağlanmıştır. Sensör verilerinin güvenliği, IoT cihazlarının işleyişi ve güvenliği açısından kritik önem taşımaktadır.

Son olarak, zararlı yazılım (malware) saldırıları, IoT cihazlarına kötü amaçlı yazılım yükleyerek saldırganın cihazın kontrolünü ele geçirmesine olanak tanımaktadır. Bu tür saldırılar, saldırganın cihazı tamamen ele geçirmesine ve ağa yayılan tehditler oluşturmasına neden olabilmektedir. Bu çalışmada, Metasploit Framework kullanılarak IoT cihazlarına zararlı yazılım yerleştirilmeye çalışılmıştır. Zararlı yazılım saldırılarının erken tespit edilmesi, IoT cihazlarının ağ güvenliğini sağlamak açısından kritik bir öneme sahiptir.

3.4 Veri Seti

Çalışma kapsamında, Raspberry Pi cihazı, internete bağlanabilen bulaşık makinesi ve süpürgeye yönelik gerçekleştirilen saldırılar kaydedilmiş ve bu saldırılara ilişkin veri elde edilmiştir. Elde edilen veriler Python programı ile etiketleme yapılarak veri seti haline getirilmiştir. Tez çalışmasında kullanılan veri seti, Çizelge 3.1'deki öznitelikleri içermektedir:

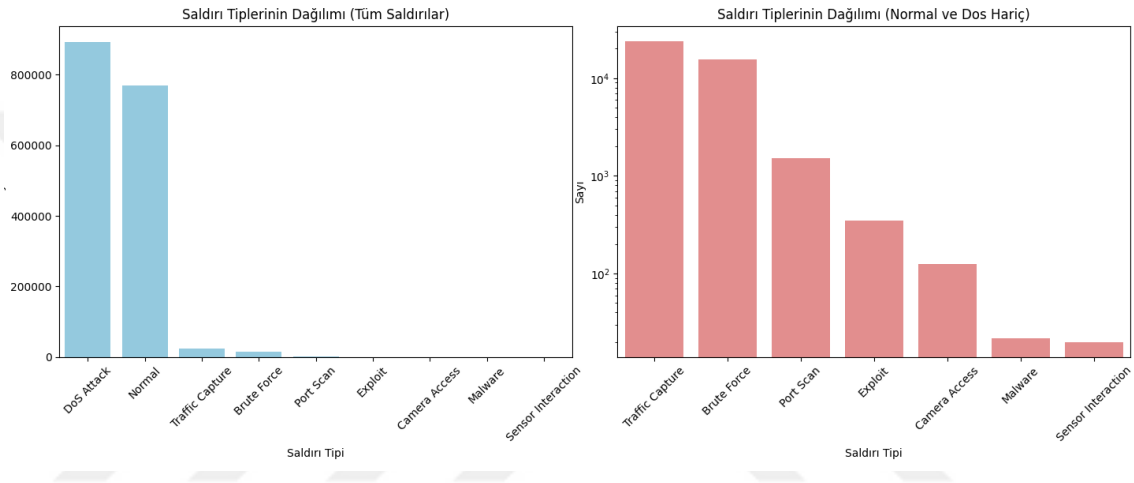
Çizelge 3.1 Veri seti öznitelikleri

Öznitelik No	Öznitelik	Tanım
1	No.	Kayıt numarası, her bir kaydın özebir numarasıdır
2	Time	Paketlerin kaydedildiği zaman damgası
3	Source	Paketi gönderen kaynak IP adresi
4	Destination	Paketi alan hedef IP adresi
5	Protocol	İletişim protokolü
6	Length	Paket boyutu
7	Info	Paket hakkında ayrıntılı bilgi (TCP bayrakları, port numaraları vb.)
8	attack_type	Saldırı türü (Port Scan, Brute Force, Exploit, Traffic Capture, Camera Access, Sensor Interaction, DoS Attack, Malware, Normal)

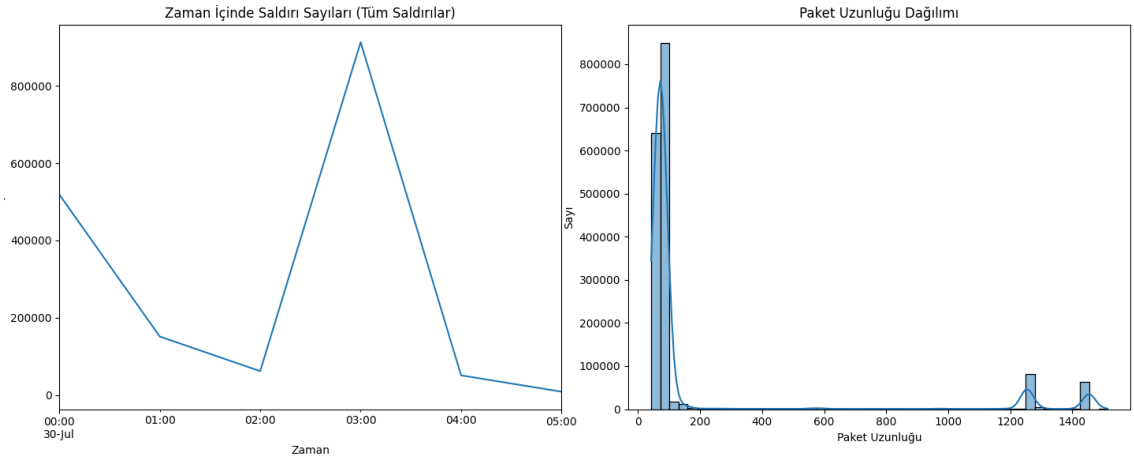
Veri setinde toplam 1.705.085 satır ve 8 sütun bulunmaktadır. Saldırı tiplerinin dağılımı incelendiğinde, en yüksek sayıya sahip kategori DoS saldırısı olup toplamda 893.536 adet ile en yaygın saldırı tipi olarak karşımıza çıkmaktadır. Normal kategorisi ise 769.903 adet ile ikinci sırada yer almaktadır. Diğer saldırı tipleri arasında, Trafik Yakalama 24.005 adet, Brute Force 15.609 adet, Port Tarama 1.514 adet, Zafiyet Tarama 350 adet, Kamera Erişimi 126 adet, Zararlı Yazılım 22 adet ve Sensör Etkileşimi 20 adet olarak

sıralanmaktadır. Bu dağılım, özellikle DoS Saldırısı ve Normal kategorilerinin diğer kategorilere kıyasla oldukça yüksek sayılara ulaştığını göstermektedir.

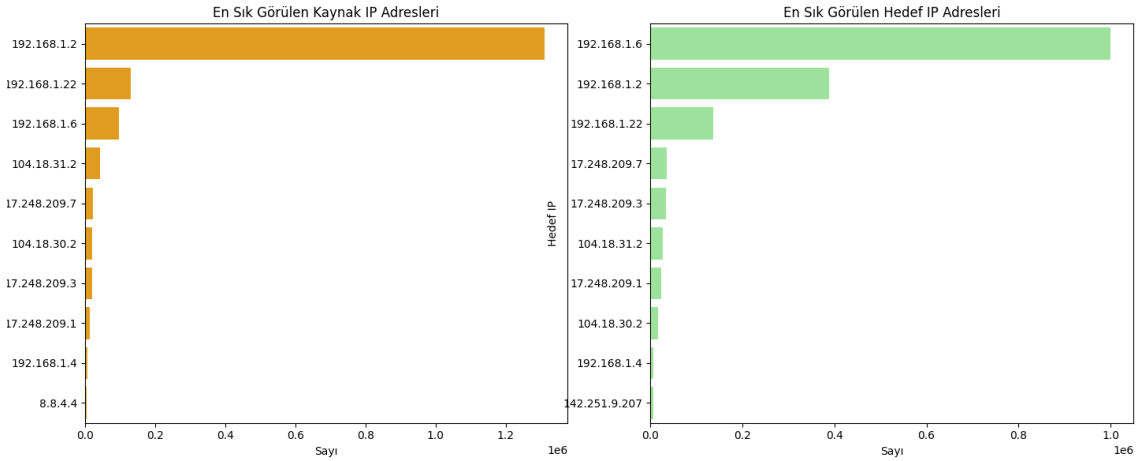
Trafik analizi sonuçlarına göre, toplam trafik hacmi 335.252.271 byte olarak hesaplanmıştır. Paket uzunlukları incelendiğinde, ortalama paket uzunluğu 196,62 byte olarak belirlenmiş, minimum paket uzunluğu 42 byte ve maksimum paket uzunluğu ise 1.514 byte olarak tespit edilmiştir. Veri setine ilişkin görseller aşağıda yer almaktadır.



Şekil 3.2 Saldırı sayıları



Şekil 3.3 Saldırıların zamana göre dağılımı ve paket uzunlukları



Şekil 3.4 En sık görülen IP adresleri

3.5 Kullanılan Yazılım ve Kütüphaneler

Bu tez çalışmasında, programlama dili olarak Python tercih edilmiştir. Python, yüksek seviyeli ve genel amaçlı bir programlama dili olarak, prosedürel, fonksiyonel ve nesne yönelimli programlama yaklaşımlarını destekleyen çok paradigmalı bir yapıya sahiptir. Çalışma kapsamında Python programlama dilinin 3.9.19 sürümü tercih edilmiş ve geliştirme ortamı olarak Visual Studio Code kullanılmıştır.

Tez çalışmasında kullanılan kütüphaneler ve işlevleri şu şekildedir:

- Pandas kütüphanesi, veri işleme ve analiz amacıyla kullanılmıştır. “DataFrame” yapısı sayesinde verilerin yüklenmesi, işlenmesi ve analiz edilmesi kolay hale getirilmiştir. Özellikle csv dosyalarından veri okuma ve bu veriler üzerinde manipülasyonlar yapmak için tercih edilmiştir.
- Numpy kütüphanesi, bilimsel hesaplamalar ve sayısal veri işlemleri için kullanılmıştır. Diziler ve matrisler üzerinde yüksek performanslı işlemler gerçekleştiren bu kütüphane, sayısal değerlere dönüştürülme ve matematiksel işlemlerde rol oynamıştır.
- Matplotlib kütüphanesi, veri görselleştirme amacıyla kullanılmıştır. İki boyutlu grafikler, karmaşıklık matrisi ve ROC eğrisi gibi grafiklerin oluşturulmasında bu

kütüphane tercih edilmiştir. Verilerin görselleştirilmesi, modelin performansını daha net analiz etme imkanı sunmuştur.

- Seaborn kütüphanesi ise Matplotlib tabanlı bir veri görselleştirme kütüphanesi olarak kullanılmıştır. Grafiklerin daha estetik ve açıklayıcı hale getirilmesi amacıyla özellikle karmaşıklık matrisi ve scatter plot gibi grafiklerin görselleştirilmesinde faydalanılmıştır.
- Scikit-learn kütüphanesi, makine öğrenmesi algoritmalarını içeren popüler bir kütüphanedir. Bu tez çalışmasında veri işleme, model oluşturma, model seçimi ve değerlendirme işlemlerinde kullanılmıştır.
- Imbalanced-learn kütüphanesi, dengesiz veri kümelerinde sınıf dengesizliklerini gidermek amacıyla kullanılmıştır. Bu tez çalışmasında, özellikle aşırı örnekleme (oversampling) ve az örnekleme (undersampling) işlemleri yapılmıştır.
- XGBoost kütüphanesi, veri madenciliği ve makine öğrenmesi için kullanılan güçlü bir ağaç tabanlı algoritma içermektedir. Gradyan artırımı ile çalışan bu sınıflandırıcı (XGBClassifier), hızlı ve yüksek doğruluklu sonuçlar elde etmek amacıyla kullanılmıştır. Hiperparametre optimizasyonunda GridSearchCV ile kullanılarak modelin performansı artırılmıştır.
- TensorFlow/Keras kütüphanesi, derin öğrenme modellerinin oluşturulması için kullanılmıştır. Keras, TensorFlow üzerinde çalışan bir yüksek seviye arayüz olarak, yapay sinir ağı ve derin öğrenme mimarilerini oluşturma ve eğitim süreçlerinde rol oynamıştır.
- Scipy kütüphanesi, bilimsel hesaplamalar ve istatistiksel işlemler için kullanılmıştır. Hiperparametre optimizasyonunda, özellikle rastgele sayı dağılımlarının belirlenmesinde etkili olmuştur.

Bu kütüphaneler, verilerin işlenmesi, makine öğrenmesi ve derin öğrenme modellerinin geliştirilmesi, sınıf dengesizliklerinin giderilmesi, model optimizasyonu ve sonuçların görselleştirilmesi gibi süreçlerin etkin bir şekilde gerçekleştirilmesini sağlamıştır.

3.6 Veri Ön İşleme Adımları

Bu çalışmada kullanılan veri seti, modelleme süreçlerine uygun hale getirilmek amacıyla bir dizi detaylı veri ön işleme adımından geçirilmiştir. İlk olarak, veri seti csv formatında bir dosyadan okunmuş ve Pandas kütüphanesi kullanılarak tablo yapısına dönüştürülmüştür. Veri seti üzerinde yapılacak analiz ve modelleme işlemlerine başlamadan önce, verilerin doğru ve eksiksiz olduğundan emin olmak amacıyla çeşitli işlemler gerçekleştirilmiştir.

Veri setinde yer alan IP adresleri, metin formatında olduğundan, bu verilerin sayısal hale getirilmesi gerekmektedir. Sayısal dönüşüm işlemi, makine öğrenmesi algoritmalarının sayısal veriler üzerinde çalışması zorunluluğundan kaynaklanmaktadır. Bu işlemde, her bir IP adresi dört parçaya ayrılmış ve her parça belirli bir katsayı ile çarpılarak sayısal bir değer elde edilmiştir. Bu şekilde IP adresleri sayısal formatta modele uygun hale getirilmiştir. Bununla birlikte, bu dönüşümün ardından eksik veri bulunma ihtimaline karşı veri temizleme işlemi yapılmıştır.

Kategorik veriler, makine öğrenmesi algoritmalarında doğrudan kullanılabilir olmadığından, sayısal değerlere dönüştürülmüştür. Veri setinde yer alan Protocol ve attack_type gibi kategorik değişkenler, sayısal değerlere çevrilmiştir. Bu işlemde, “LabelEncoder” kullanılarak her kategorik değişken belirli bir sayı ile eşleştirilmiştir. Kategorik verilerin sayısal hale getirilmesi, modelin bu veriler üzerinde daha sağlıklı bir şekilde çalışmasına olanak sağlamaktadır.

Veri seti, modelde kullanılmak üzere özellikler (bağımsız değişkenler) ve hedef değişken (bağımlı değişken) olarak ayrıştırılmıştır. Bu çalışmada hedef değişken olarak attack_type seçilmiş ve veri setindeki diğer özellikler modelde kullanılmak üzere belirlenmiştir. Ayrıca, Info sütunu metin içerdiğinden modelleme sürecine dahil edilmemiştir. Özellikler ve hedef değişkenin ayrılması, makine öğrenmesi ve derin öğrenme modellerinin bu verilere dayalı olarak çalışabilmesi için gerekli bir adımdır.

Modelleme sürecine başlamadan önce, veri seti eğitim ve test setlerine ayrılmalıdır. Veri seti, %80 eğitim ve %20 test olacak şekilde ikiye ayrılmıştır. Bu işlem, modelin eğitilmesi ve test edilmesi için gereklidir. Eğitim sırasında kullanılan verilerle model öğrenme sürecini tamamlarken, test seti modelin performansını değerlendirmek için kullanılmaktadır. Ayrıca, hedef değişkenin sınıf dağılımı korunarak eğitim ve test setlerine ayrılmıştır. Bu sayede, eğitim ve test setlerinde sınıf dengesizlikleri minimize edilmiştir.

Verilerin farklı ölçeklerde olması, model performansını olumsuz etkileyebilmektedir. Bu nedenle, tüm özellikler aynı ölçek seviyesine getirilmiştir. Özelliklerin ölçeklendirilmesi, özellikle mesafeye dayalı algoritmalar ve sinir ağları gibi modellerde büyük bir önem taşımaktadır. Bu çalışmada, "StandardScaler" kullanılarak veriler ölçeklendirilmiştir. Ölçeklendirme işlemi, her bir özelliğin ortalaması sıfır, standart sapması bir olacak şekilde standartlaştırılmasını sağlamıştır.

Sınıf dengesizliği problemi, sınıflar arasında dengesiz dağılımlar olduğunda ortaya çıkmakta ve bu durum makine öğrenmesi modellerinin performansını olumsuz etkileyebilmektedir. Sınıf dengesizliği sorununu çözmek amacıyla, "SMOTE (Synthetic Minority Over-sampling Technique)" ve "RandomUnderSampler" yöntemleri kullanılmıştır. SMOTE, küçük sınıflara ait örnek sayısını artırarak, sınıf dengesizliğini giderirken; RandomUnderSampler ise fazla örneklemli sınıfların sayısını azaltmak için kullanılmıştır. Bu sayede, sınıflar arasında denge sağlanmış ve modelin daha dengeli bir şekilde eğitim alması sağlanmıştır.

Hedef değişken çok sınıflı bir yapıya sahip olduğundan, derin öğrenme modelleri için uygun hale getirilmesi amacıyla kategorik forma dönüştürülmüştür. Bu işlem, "to_categorical" fonksiyonu kullanılarak gerçekleştirilmiştir. Çok sınıflı veri setlerinde, sınıfların birden fazla kategorik etiket ile temsil edilmesi, özellikle sinir ağı gibi modellerde gerekmektedir. Bu adım sayesinde model, hedef değişken üzerinde doğru sınıflandırma yapabilir hale gelmiştir.

Bu adımlar ile veri seti, eksiksiz, temiz ve modelleme süreçleri için hazır hale getirilmiştir. Uygulanan veri ön işleme teknikleri, modelin veriyi daha iyi anlamasına ve performansının artmasına olanak sağlamıştır.

3.7 Makine Öğrenmesi Yöntemleri ile Sınıflandırma

Tez çalışması kapsamında, veri setlerine yönelik veri ön işleme adımlarının tamamlanmasının ardından çeşitli makine öğrenmesi algoritmaları uygulanmıştır. Sınıflandırma çalışmaları için yaygın olarak kullanılan makine öğrenmesi yöntemleri tercih edilmiştir. Makine öğrenmesi ile ilgili detaylı bilgilere 2. bölümde yer verilmiştir. Bu bölümde ise tez çalışması kapsamında kullanılan makine öğrenmesi yöntemleri açıklanmıştır.

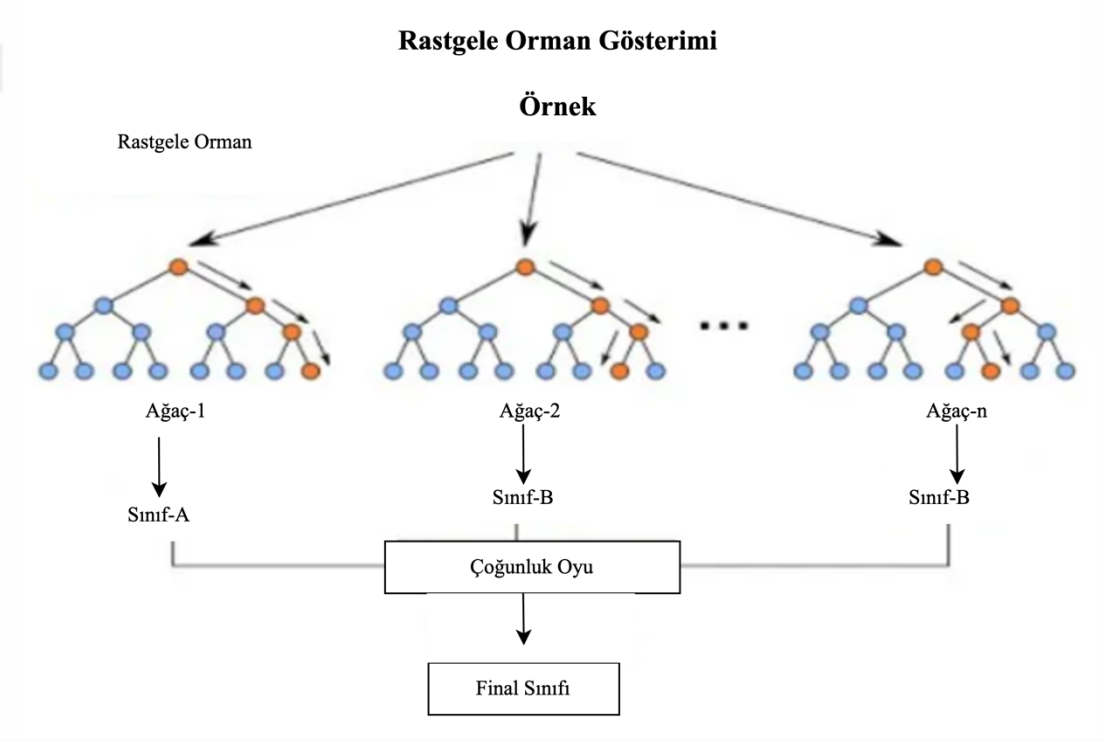
3.7.1 Rastgele orman sınıflandırma algoritması

Leo Breiman tarafından (2001) yılında yayımlanan Rastgele Orman (Random Forest) makalesi, makine öğrenmesi alanında önemli bir dönüm noktası olmuştur. Bu çalışmada, Rastgele orman algoritması, çok sayıda karar ağaçları oluşturarak bu ağaçların tahminlerini birleştiren bir topluluk öğrenme yöntemi olarak tanımlanmaktadır. Breiman, algoritmanın temel iki bileşenini, yani “bagging (Bootstrap Aggregating)” ve rastgele özellik seçimini vurgulamaktadır. Her bir karar ağacı, eğitim verisinin bir “bootstrap” örneği üzerinde eğitilirken, her bir düğümde rastgele bir özellik alt kümesi dikkate alınmaktadır (Breiman 2001).

Breiman’ın çalışmasında, Rastgele Orman algoritmasının genelleme hatasını azaltmada etkili olduğu belirtilmiştir. Yöntemin genelleme kapasitesini artırdığı, çok sayıda ağacın kullanılmasıyla birlikte doğruluğun önemli ölçüde iyileştirildiği ifade edilmiştir. Ayrıca, Rastgele Orman algoritmasının, özellik öneminin belirlenmesinde de başarılı bir yöntem olduğu vurgulanmıştır. Bu bağlamda, algoritma her bir özelliğin modeldeki katkısını değerlendirerek, çok boyutlu verilerde hangi özelliklerin daha önemli olduğunu saptamada kullanışlı bir araç sunmaktadır. Yapılan deneylerde, Rastgele Orman

algoritmasının hem sınıflandırma hem de regresyon problemlerinde yüksek doğruluk oranları ile üstün performans gösterdiği ortaya konmuştur (Breiman 2001).

Breiman, algoritmanın yüksek doğruluk ve aşırı öğrenme kontrolü sağlama konusundaki yeteneklerini vurgulamaktadır. Ayrıca, algoritmanın büyük ve yüksek boyutlu veri setleri ile etkili bir şekilde çalışabilme kapasitesi, onu pek çok uygulama alanında tercih edilen bir yöntem haline getirmiştir. Rastgele Orman çalışma prensibi Şekil 3.5'te gösterilmektedir.



Şekil 3.5 Rastgele Orman çalışma prensibi (Ren ve Cao 2022).

3.7.2 Karar ağaçları algoritması

Karar Ağaçları (Decision Trees), sınıflandırma ve regresyon problemlerinde sıklıkla kullanılan, karar süreçlerini temsil eden ağaç yapısına dayalı bir modelleme tekniğidir. Bu yöntem, verilerin belirli özelliklere göre bölünmesiyle çalışmaktadır ve her bir düğümde bir karar alınarak nihai tahminler yapılmaktadır. Karar ağacı, genellikle

görselleştirilebilen ve anlaşılması kolay bir modeldir, bu nedenle kullanıcılara modelin nasıl çalıştığı hakkında net bir anlayış sunulmaktadır (Anonymous 2022b).

Veri seti, karar ağacı algoritması tarafından en uygun şekilde bölünecek şekilde ayrılmaktadır. Bu bölme işlemi, genellikle "Gini impurity" veya "Entropy" gibi kriterlere göre gerçekleştirilmektedir. Gini impurity, her bir bölmeden sonra kalan veri alt kümelerinin homojenliğini ölçerken, Entropy ise veri alt kümelerinin düzensizliğini ifade etmektedir. Her bir bölme adımında, en düşük Gini impurity veya en yüksek bilgi kazancı sağlayan özellik seçilerek, her bir alt küme daha homojen hale getirilmektedir (Anonymous 2022b).

Karar ağaçlarının önemli bir avantajı, modelin açıklanabilir olmasıdır. Modelin her bir adımı, kullanılan özelliklere dayalı olarak açıkça tanımlanmakta ve görselleştirilebilmektedir. Bu sayede, karar ağaçları, modelin nasıl çalıştığı hakkında kullanıcıya net bir anlayış sunmaktadır. Ancak, karar ağaçları genellikle aşırı öğrenme sorunuyla karşılaşabilmektedir. Çok derin ağaçlar, eğitim verisine aşırı uyum sağlamakta ve test verisi üzerinde düşük performans sergileyebilmektedir. Bu nedenle, ağacın derinliği sınırlanmakta veya "pruning (budama)" yöntemleriyle modelin karmaşıklığı azaltılmaktadır (Anonymous 2022b).

3.7.3 Gradyan artırıcı makineler sınıflandırma algoritması

Gradyan Artırıcı Makineler (Gradient Boosting Machines - GBM), istatistiksel modelleme ve makine öğrenmesi alanlarında yaygın olarak kullanılan bir teknik olup, özellikle tahmin gücü yüksek modellerin geliştirilmesinde önemli bir rol oynamaktadır. Friedman (2001), GBM'yi, zayıf öğrenicilerin ardışık olarak bir araya getirilmesiyle güçlü bir model oluşturma süreci olarak tanımlamaktadır. Bu yöntemin temel prensibi, her yeni modelin, önceki modellerin tahmin hatalarını düzeltmeye yönelik olarak optimize edilmesidir (Friedman 2001).

GBM, temel olarak iki aşamadan oluşmaktadır: modelin tahmin hatalarının hesaplanması ve yeni bir modelin bu hataları düzeltmek amacıyla oluşturulması. İlk olarak, mevcut modelin tahmin ettiği değerler ile gerçek değerler arasındaki hata hesaplanmaktadır. Bu hata, "kalıntı (residual)" olarak adlandırılmakta ve yeni modelin öğrenmesi gereken hedef değişken olarak kullanılmaktadır. İkinci aşamada ise, bu hataları minimize etmek için gradyan iniş algoritması uygulanmaktadır. Her iterasyonda, önceki modelin hatalarını düzeltmek üzere yeni bir model eklenmektedir. Bu süreç, modelin genel performansını artırırken, aşırı uyum riskini de yönetme imkanı sunmaktadır (Friedman 2001).

Friedman, GBM'nin birçok avantajını vurgulamaktadır. Bunlar arasında, karmaşık veri setleri üzerinde etkili bir şekilde çalışabilme yeteneği, esnekliği ve modelin yapılandırılabilirliği yer almaktadır. GBM hem regresyon hem de sınıflandırma problemlerinde kullanılabilen ve "hiperparametre" ayarları ile performansı optimize edilebilen güçlü bir makine öğrenmesi yöntemidir. Ayrıca, değişkenlerin önem derecelerini belirleme yeteneği, GBM'yi açıklanabilirliği yüksek bir model haline getirmektedir (Friedman 2001).

Bu yöntemin uygulama alanları oldukça geniştir. Finansal tahminler, sağlık verileri analizi, pazarlama stratejileri ve çeşitli mühendislik problemleri gibi birçok alanda GBM kullanılmaktadır. Friedman'ın çalışmaları, bu yöntemin matematiksel temellerini ve uygulama pratiklerini detaylandırarak, araştırmacılara ve uygulayıcılara önemli bir kaynak sağlamaktadır. GBM, güçlü tahmin yetenekleri, esnek yapılandırma seçenekleri ve uygulama çeşitliliği ile modern istatistiksel analizlerde ve makine öğrenmesi alanında öne çıkan bir yöntemlerden biridir.

3.7.4 XGBoost algoritması

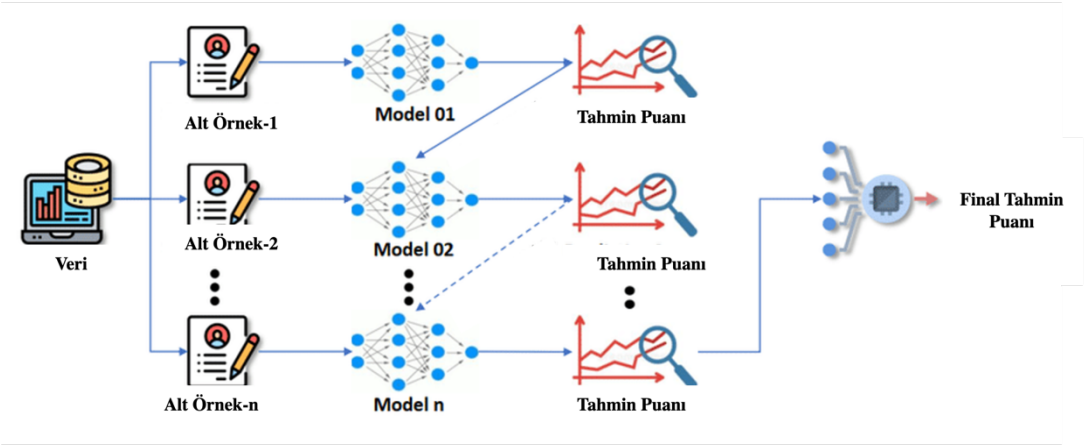
XGBoost, Chen ve Guestrin (2016) tarafından geliştirilmiş, ağaç artırma algoritmalarını optimize eden ve yüksek performansı ile öne çıkan bir makine öğrenmesi yöntemidir. Bu sistem, özellikle büyük veri setlerinde yüksek performans sağlamak amacıyla tasarlanmıştır. XGBoost, geniş çaplı makine öğrenmesi uygulamalarında yaygın olarak kullanılmakta ve birçok yarışmada en iyi sonuçları elde etmek için tercih edilmektedir.

XGBoost'un en önemli özelliklerinden biri, verilerin "dağınık (sparse)" yapısını etkili bir şekilde işleyebilmesidir. Bu özellik, sistemin, eksik verilere veya sıklıkla sıfır değerlerine sahip verilerle başa çıkmasına olanak tanımaktadır. Sistem, bu tür verilerdeki belirsizlikleri azaltmak için bir varsayılan yönlendirme mekanizması kullanmaktadır. Eksik verilerin bulunması durumunda, verinin hangi yöne yönlendirileceği öğrenilmekte ve böylece modelin genelleme yeteneği artırılmaktadır (Chen ve Guestrin 2016).

XGBoost ayrıca, verileri işlemek için kullanılan blok yapıları sayesinde "bellek dışı (out-of-core)" hesaplamaları desteklemektedir. Bu blok yapıları, verilerin bellekte saklanması yerine diskte depolanmasına ve gerektiğinde okunmasına olanak tanımaktadır. Bu sayede, sistem, çok büyük veri kümeleri üzerinde çalışabilmekte ve bellek sınırlamalarını aşabilmektedir (Chen ve Guestrin 2016).

XGBoost, mevcut diğer popüler ağaç artırma sistemlerine kıyasla on kat daha hızlı çalışabildiği gösterilmiştir. Bu hız, sistemin paralel ve dağıtık hesaplama yeteneklerinden kaynaklanmaktadır. XGBoost, birden fazla işlemci çekirdeğini kullanarak hesaplama süresini önemli ölçüde azaltmakta ve böylece modellerin daha hızlı bir şekilde keşfedilmesine olanak tanımaktadır. Sistem, aynı zamanda veri erişim desenlerini optimize ederek, önbellek kullanımını artırmakta ve bellek erişim sürelerini minimize etmektedir. Bu özellik, özellikle büyük veri setlerinde işlemci kaynaklarının etkili bir şekilde kullanılmasını sağlamaktadır (Chen ve Guestrin 2016).

XGBoost, sunduğu yenilikçi algoritmalar ve sistem tasarımı ile büyük veri analizi için güçlü bir araç haline gelmiştir. Veri bilimcileri ve araştırmacılar, XGBoost'u kullanarak karmaşık veri bağımlılıklarını modelleme ve büyük veri setlerinden etkili bir şekilde öğrenme fırsatına sahip olmaktadırlar. XGBoost'un sağladığı avantajlar ve uygulama potansiyeli hakkında daha derin bir anlayış geliştirmeyi amaçlamaktadır (Chen ve Guestrin 2016). XGBoost'un çalışma prensibi Şekil 3.6'da gösterilmektedir.



Şekil 3.6 XGBoost çalışma prensibi (Rahaman vd. 2022)

3.7.5 Destek vektör makineleri sınıflandırma algoritması

Destek Vektör Makineleri (Support Vector Machine - SVM), hem sınıflandırma hem de regresyon problemlerinde kullanılan güçlü bir denetimli öğrenme algoritmasıdır. Bu algoritmanın temel amacı, verileri sınıflar arasındaki farkı en iyi şekilde ayıracak bir hiper düzlem oluşturmak ve sınıflar arasındaki marjı maksimize etmektir. SVM, sınıflar arasındaki sınırı belirlemek için yalnızca destek vektörleri olarak adlandırılan belirleyici veri noktalarını kullanmaktadır. Veriler doğrusal olarak ayrılamadığında, "kernel" fonksiyonları kullanılarak veriler daha yüksek boyutlu bir uzaya dönüştürülmekte ve bu sayede doğrusal olarak ayırma işlemi mümkün hale getirilmektedir. Kullanılan kernel fonksiyonları arasında lineer, polinomial, radyal temel fonksiyonu ve sigmoid fonksiyonları yer almaktadır. Kernel fonksiyonlarının doğru seçilmesi, sınıflandırma performansını önemli ölçüde etkilemektedir (Ioannou ve Vassiliou 2021).

SVM'nin IoT ağlarında saldırı tespiti sistemlerinde kullanımı, cihazların güvenliği açısından kritik öneme sahiptir. SVM algoritması, olası saldırıların erken tespit edilmesi ve güvenlik tehditlerine karşı hızlı önlem alınması açısından güçlü bir araç olarak kabul edilmektedir. Özellikle bilinmeyen ve yeni saldırıların tespiti açısından önemli avantajlar sağlamaktadır. Ancak, başarılı bir SVM modelinin uygulanabilmesi için veri setine uygun

kernel fonksiyonunun doğru bir şekilde seçilmesi ve modelin doğru biçimde eğitilmesi gerekmektedir (Ioannou ve Vassiliou 2021).

3.7.6 K-en yakın komşular algoritması

K-en yakın komşular (k-nearest neighbors - KNN) algoritması, makine öğrenmesi alanında kullanılan temel denetimli öğrenme yöntemlerinden biri olarak bilinmektedir. Hem sınıflandırma hem de regresyon problemlerinde kullanılabilen bu algoritma, bir veri noktasının sınıfını veya değerini, en yakın "K" komşusunun sınıflarına veya değerlerine dayanarak belirlemektedir (Cover ve Hart 1967). Algoritmanın temelinde, benzer veri noktalarının birbirine yakın konumlandığı ve bu noktalar arasındaki mesafelerin kullanılarak sınıflandırma ya da tahmin yapılabileceği varsayımı bulunmaktadır. KNN algoritması, herhangi bir öğrenme süreci gerektirmemesiyle diğer algoritmalardan farklılaşmakta, yeni bir veri noktasının değerlendirilmesi sırasında eğitim veri kümesindeki tüm noktalarla mesafe hesaplanarak tahmin yapılmaktadır (Mitchell 1997).

KNN algoritmasının önemli avantajları arasında basitliği ve eğitim süreci gerektirmemesi yer almaktadır. Algoritma, öğrenme süreci olmadan, tüm veri noktalarını bellekte saklayarak, her yeni veri için hızlı tahminler yapabilmektedir (Cunningham ve Delany, 2007). Bu nedenle, özellikle küçük ve orta ölçekli veri setlerinde etkili bir şekilde kullanılabilmektedir. Ancak, büyük veri kümelerinde, her yeni veri noktası için tüm veri setiyle mesafe hesaplanması gerektiğinden, algoritmanın yavaş çalışabileceği ve hesaplama maliyetlerinin artabileceği bilinmektedir (Hastie vd. 2009). Ayrıca, veri setleri dengesiz olduğunda, KNN algoritmasının çoğunluk sınıfına eğilim gösterebileceği ve az sayıda örneği olan sınıflarda düşük performans gösterebileceği değerlendirilmektedir.

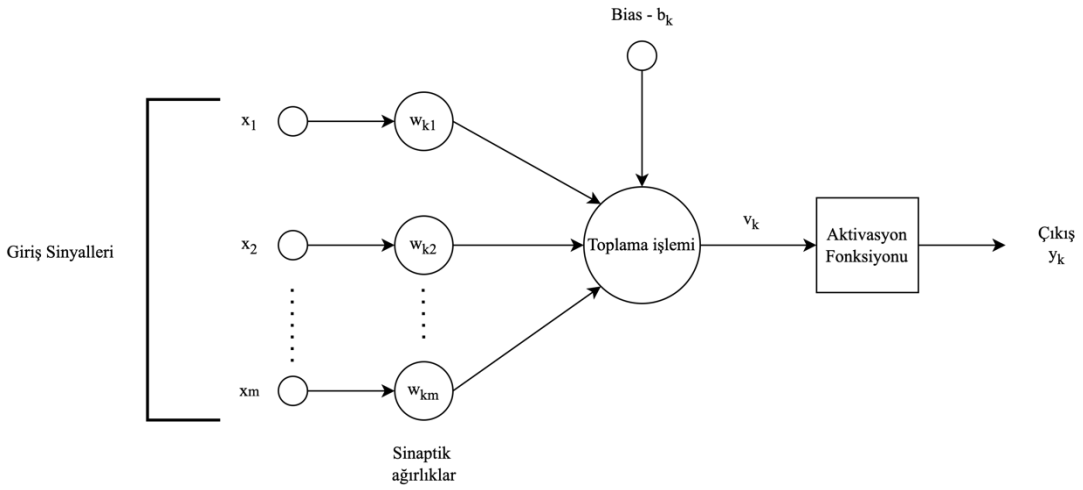
3.8 Yapay Sinir Ağları

Yapay sinir ağları (YSA), biyolojik nöronların matematiksel modelleri olarak tanımlanmaktadır. Bu ağlar, birbirine bağlı çok sayıda yapay nörondan oluşmakta olup, her bir nöron girdileri belirli ağırlıklarla çarparak toplamaktadır. Toplanan değer, bir

aktivasyon fonksiyonuna uygulanarak çıktı elde edilmektedir. Böylece karmaşık örüntüler işlenmekte ve öğrenilmektedir. Özellikle doğrusal olmayan aktivasyon fonksiyonlarının kullanılması, ağın daha karmaşık ilişkileri modelleyebilmesini sağlamaktadır (Haykin 2009).

Bir nöron, sinir ağlarının temelini oluşturan ve bilgi işleme görevini üstlenen en küçük birimdir. Şekil 3.7'deki diyagram, bir sinir ağı ailesinin tasarımına temel teşkil eden bir nöron modelini göstermektedir. Bu modelde, sinir ağının üç temel unsuru tanımlanmaktadır:

1. Her biri, kendine özgü bir ağırlık veya güç değeriyle tanımlanan bir dizi sinaps veya bağlantı. Özel olarak, k nöronuna bağlı j sinapsının girişindeki bir x_j sinyali, w_{kj} sinaptik ağırlığı ile çarpılır. w_{kj}'deki ilk alt simge söz konusu nöronu, ikinci alt simge ise ağırlığın atıfta bulunduğu sinapsın giriş ucunu ifade etmektedir. Beyindeki sinaps ağırlıklarından farklı olarak, yapay nöronlarda sinaptik ağırlığın hem pozitif hem de negatif değerler alabileceği görülmektedir.
2. Nöronun, ilgili sinaptik ağırlıklarla çarpılan giriş sinyallerini toplamak amacıyla bir toplayıcı içerdiği ifade edilmektedir. Bu işlemin doğrusal bir birleştirici işlevi oluşturduğu belirtilmektedir.
3. Nöronun çıkış sinyalinin genliğini sınırlamak için bir aktivasyon fonksiyonunun kullanıldığı görülmektedir. Aktivasyon fonksiyonunun, çıkış sinyalini belirli bir genlik aralığına sınırlayarak sinyali sıkıştırdığı ve bu nedenle "ezme fonksiyonu" olarak da adlandırıldığı belirtilmektedir.



Şekil 3.7 Nöron modeli (Haykin 2009)

Tipik olarak, bir nöronun çıkışının genliği, normalleştirilmiş bir değer aralığına sınırlanır ve bu aralık genellikle [0,1] veya [-1,1] şeklinde ifade edilmektedir. Şekil 3.7'de gösterilen nöron modeli ayrıca, b_k ile gösterilen ve harici olarak uygulanan bir yanlılık (bias) terimini de içermektedir. Bu yanlılık, aktivasyon fonksiyonunun net girdisini, işaretine bağlı olarak artırma veya azaltma etkisi yapmaktadır. Matematiksel olarak, Şekil 3.7'de verilen k nöronu aşağıdaki denklemlerle tanımlanmaktadır:

$$u_k = \sum_{j=1}^{m} w_{kj} x_j \tag{3.1}$$

$$y_k = \varphi(u_k + b_k) \tag{3.2}$$

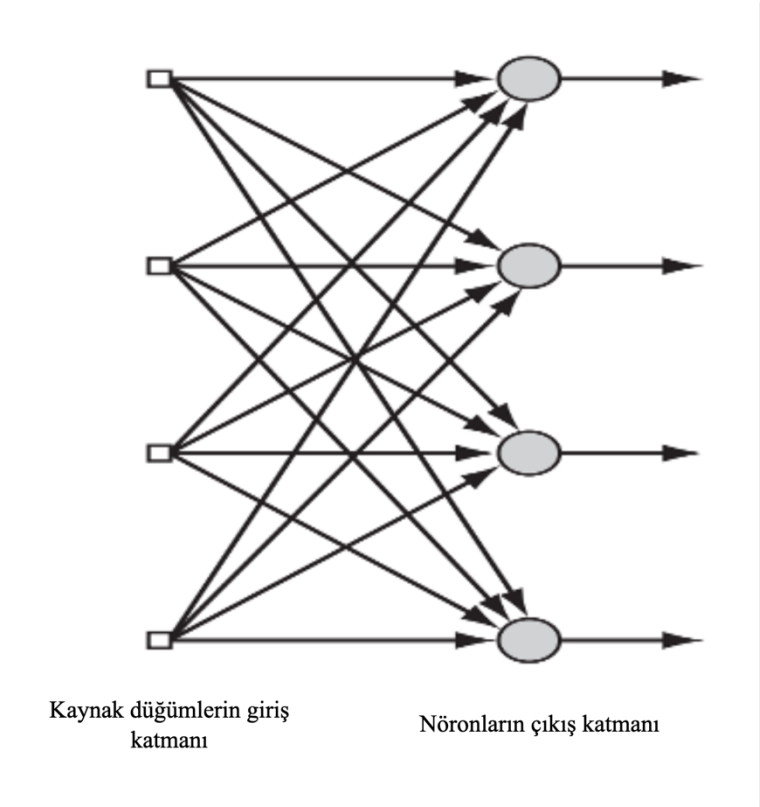
Burada, $x_1, x_2, \ldots, x_m$ giriş sinyallerini; $w_{k1}, w_{k2}, \ldots, w_{km}$ ise k nöronunun ilgili sinaptik ağırlıklarını temsil etmektedir. u_k, giriş sinyalleri nedeniyle doğrusal birleştirici çıktısıdır; b_k yanlılık içermektedir; φ aktivasyon fonksiyonudur ve y_k nöronun çıkış sinyalidir. b_k'nin kullanılması Şekil 3.7'deki modelin doğrusal birleştiricinin çıktısı olan u_k'ye bir dönüşüm uygulama etkisine sahiptir ve aşağıdaki gibi gösterilmektedir:

$$v_k = u_k + b_k \tag{3.3}$$

Öğrenme sürecinde, çoğunlukla denetimli öğrenme prensibi benimsenmektedir. Bu süreçte eğitim verisi ağdan geçirilmekte ve elde edilen çıktı, hedefle karşılaştırılarak hata hesaplanmaktadır. Hesaplanan hata, geri yayılım algoritması ile ağırlıklara dağıtılmakta ve gradyan inişi yöntemiyle minimize edilmektedir. Bu optimizasyon, ağın iterasyonlar boyunca kendini optimize etmesine olanak tanıyarak veri örüntülerini daha doğru öğrenmesini sağlamaktadır (Haykin 2009).

Sinir ağı mimarilerinin, tek katmanlı yapılardan çok katmanlı derin yapılara kadar geniş bir yelpazede çeşitlilik gösterdiği belirtilmektedir. Çok katmanlı algılayıcılar, doğrusal olmayan verileri modellemede başarı göstermekte olup özellikle sınıflandırma ve regresyon problemlerinde etkili sonuçlar sunmaktadır. Görüntü işleme için geliştirilen CNN, verinin özniteliklerini çıkarmada katmanlı yapısından yararlanmakta ve küçük bölgesel filtreler kullanarak bilgi kaybını minimize etmektedir (Haykin 2009).

Katmanlı bir sinir ağında, nöronlar belirli katmanlar halinde düzenlenmiştir. En basit formunda, giriş katmanındaki kaynak düğümleri, doğrudan çıktı katmanına projeksiyon yapmaktadır. Ancak bu projeksiyon, ters yönde gerçekleşmez. Başka bir ifadeyle, bu yapı tamamen ileri beslemeli (feedforward) bir ağ türüdür. Şekil 3.8, hem giriş hem de çıktı katmanında dört düğümün bulunduğu bir durumu göstermektedir. Bu tür bir ağ, tek katmanlı bir ağ olarak adlandırılmaktadır. Burada, “tek katman” terimi, yalnızca nöronlardan oluşan çıktı katmanını ifade etmektedir. Kaynak düğümlerden oluşan giriş katmanı hesaplama yapmadığı için katman sayısına dahil edilmemektedir (Haykin 2009).

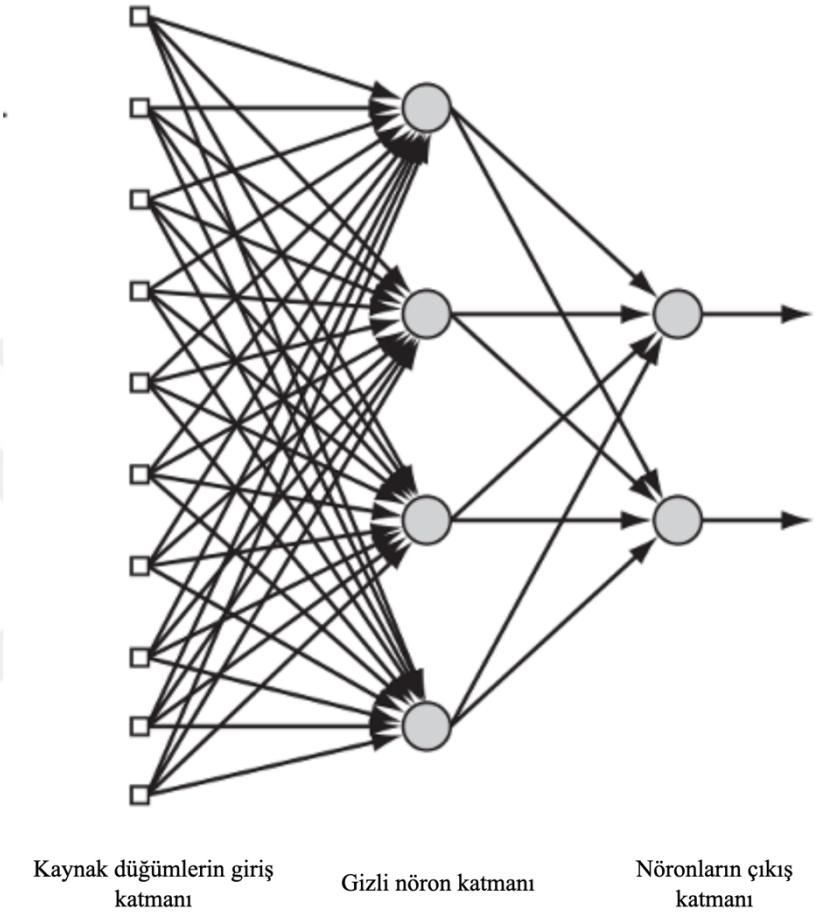


Şekil 3.8 Tek katmanlı nöron içeren ileri beslemeli ağ yapısı (Haykin 2009)

İleri beslemeli sinir ağlarının ikinci türü, bir veya daha fazla gizli katmanın (hidden layers) varlığı ile tanımlanmaktadır. Bu katmanlarda bulunan hesaplama düğümleri, gizli nöronlar veya gizli birimler olarak adlandırılmaktadır. Gizli terimi, bu katmanların ağın giriş veya çıkış katmanından doğrudan gözlemlenmediğini ifade etmektedir. Gizli nöronların işlevi, ağın dış girdisi ile çıktısı arasında etkileşim sağlamak ve girdilerden daha yüksek dereceli istatistiksel özelliklerin çıkarılmasını mümkün kılmaktır. Bu bağlamda, sinir ağı yerel bağlantılara sahip olsa da ek sinaptik bağlantılar ve nöronlar arasındaki etkileşimlerin oluşturduğu ek boyut, sistemi analiz etmek ve anlamak için daha geniş bir perspektif, yani küresel bir bakış açısı gerektirmektedir (Haykin 2009).

Ağın giriş katmanında bulunan kaynak düğümler, ağın ikinci katmanında (ilk gizli katman) yer alan nöronlara uygulanan giriş sinyallerini sağlamaktadır. Her katmandaki nöronlar, yalnızca bir önceki katmandan gelen çıkış sinyallerini girdi olarak almaktadır. Ağın çıktı katmanındaki nöronların sinyalleri, ağın giriş katmanında yer alan kaynak

düğümlerinden sağlanan aktivasyon desenine karşılık gelen genel çıktıyı oluşturmaktadır (Haykin 2009).



Şekil 3.9 Gizli katman ve çıkış katmanına sahip ileri beslemeli ağ (Haykin 2009)

YSA'nın genelleme kapasitesinin korunmasında, aşırı öğrenmenin (overfitting) engellenmesi önem taşımaktadır. Aşırı öğrenme problemi, modelin eğitim verisine fazla uyum göstermesi sonucu yeni veriler üzerinde düşük performans sergilemesi olarak tanımlanmaktadır. Bu durumu önlemek için düzenleme teknikleri, çapraz doğrulama ve "dropout" gibi yöntemler kullanılmaktadır. Bu teknikler, modelin genelleme kapasitesini koruyarak yeni verilere daha iyi uyum sağlamasını hedeflemektedir (Haykin 2009).

YSA'nın geniş bir uygulama alanı olduğu ifade edilmektedir. Bu ağlar, finansal analiz, piyasa tahmini, sağlık sektörü ve doğal dil işleme gibi alanlarda kullanılmaktadır. Örneğin, çok katmanlı algılayıcılar finansal tahminlerde, doğal dil işleme alanında ise dil modelleri ve otomatik çeviri sistemleri geliştirilmiştir. Bu çeşitlilik, YSA'nın veri işleme kapasitesini ve problem çözme esnekliğini ortaya koymaktadır (Haykin 2009).

Bu çalışmada kullanılan yapay sinir ağı modeli, çok sınıflı sınıflandırma problemine uygun olarak tasarlanmıştır. Model, bir giriş katmanı, üç gizli katman ve bir çıkış katmanından oluşmaktadır. Giriş katmanında, veri setindeki özellik sayısı kadar nöron bulunmakta ve bu katmanda ReLU aktivasyon fonksiyonu kullanılmıştır. Gizli katmanlar, sırasıyla 256, 128 ve 64 nörondan oluşmaktadır. Tüm gizli katmanlarda ReLU aktivasyon fonksiyonu tercih edilmiştir. Ayrıca, modelin aşırı öğrenme (overfitting) riskini azaltmak amacıyla her gizli katmanda %30 oranında sönümleme (dropout) uygulanmıştır. Çıkış katmanı, veri setindeki sınıf sayısı kadar nörona sahiptir ve bu katmanda çok sınıflı sınıflandırma problemlerine uygun olan "Softmax" aktivasyon fonksiyonu kullanılmıştır. Modelin eğitimi sırasında kayıp fonksiyonu olarak kategorik çapraz entropi (categorical crossentropy) tercih edilmiştir. Optimizasyon algoritması olarak ise "Adam yöntemi" kullanılmıştır. Modelin performansı, doğruluk metriği üzerinden değerlendirilmiştir. Eğitim sürecinde modelin erken durdurma yöntemi ile aşırı öğrenme ve gereksiz fazla eğitimin önlenmesi hedeflenmiştir. Erken durdurma yöntemi, doğrulama kaybı (validation loss) metriği izlenerek uygulanmıştır ve sabır süresi 10 "epoch" olarak belirlenmiştir. Model, maksimum 100 epoch ile eğitilmiş olup her iterasyonda 128 veri örneği (batch size) kullanılmıştır.

3.9 Derin Öğrenme

Derin öğrenme (Deep Learning - DL), çok katmanlı yapay sinir ağları aracılığıyla verilerden anlamlı temsilciler öğrenmeyi sağlayan güçlü bir makine öğrenmesi tekniği olarak öne çıkmaktadır. Bu teknik, bilgisayar görüsü, konuşma tanıma ve doğal dil işleme gibi alanlarda yüksek başarı oranları elde etmiş ve özellikle duygu analizi gibi spesifik uygulama alanlarında popülerlik kazanmıştır. Duygu analizi, insanların ürünler, hizmetler, organizasyonlar ve olaylar hakkındaki düşünce ve duygularını analiz etmeye

odaklanır ve büyük veri ile sosyal medya platformlarının yaygınlaşmasıyla birlikte geniş bir uygulama alanı bulmuştur (Zhang vd. 2018).

Derin öğrenme, biyolojik beyne benzer bir yapıdaki çok sayıda bilgi işleme biriminden (nöronlardan) oluşan yapay sinir ağlarının kullanımıyla çalışmaktadır. Bu ağlar, veri akışını sağlayan katmanlardan oluşur. Her katmanda, veriler üzerinde farklı seviyelerde öğrenme gerçekleştirilmektedir. Temel olarak, ağlar ileri beslemeli sinir ağları ve geri dönüşümlü sinir ağları gibi kategorilere ayrılmaktadır. Bu yapı sayesinde derin öğrenme, daha önce yalnızca sınırlı katmanlar ve veri ile pratik olan sinir ağlarından daha geniş bir öğrenme kapasitesine sahiptir (Zhang vd. 2018).

İleri beslemeli ağlar, her katmandaki nöronların çıktısının bir sonraki katmanın girişine aktarılması prensibiyle çalışmaktadır. Giriş verisi, ağ boyunca işlendikçe bir dizi matris çarpımı ve aktivasyon fonksiyonundan geçmektedir. Her bir nöronun çıktısı, diğer nöronlardan aldığı girişlerin ağırlıklarla çarpılması ve ardından "bias" değerinin eklenmesiyle hesaplanmaktadır.

$$z = W.x + b \tag{3.4}$$

Burada z nöronun çıktısı, W nöron ağırlıklarını, x giriş verilerini ve b bias değerini ifade etmektedir. Bu işlem sonucunda elde edilen çıktı, doğrusal olmayan bir aktivasyon fonksiyonundan geçirilerek sonuca ulaşılmaktadır. Aktivasyon fonksiyonları, modelin doğrusal olmayan ilişkileri öğrenmesine olanak tanıyarak daha karmaşık veri yapılarını temsil etmesini sağlamaktadır. Sıkça kullanılan aktivasyon fonksiyonları arasında "sigmoid", "tanh" ve "ReLU (Rectified Linear Unit)" yer almaktadır. Bu fonksiyonlardan bazıları aşağıdaki gibi tanımlanmaktadır:

Sigmoid fonksiyonu:

$$f(z) = \frac{1}{1 + e^{-z}} \tag{3.5}$$

Tanh fonksiyonu:

$$f(z) = \tanh(z) = \frac{e^z - e^{-z}}{e^z + e^{-z}} \tag{3.6}$$

ReLU fonksiyonu:

$$f(z) = \max(0, z) \tag{3.7}$$

ReLU fonksiyonu, hesaplama kolaylığı ve daha hızlı öğrenme sağlaması nedeniyle özellikle derin ağlarda yaygın olarak tercih edilmektedir.

Sinir ağlarının eğitimi, her bir katmandaki ağırlık ve bias terimlerinin uygun değerlerinin bulunması sürecini kapsamaktadır. Bu süreç genellikle "stokastik gradyan inişi (stochastic gradient descent)" ile "geri yayılım (backpropagation)" algoritmalarının kullanımıyla gerçekleştirilmektedir. Geri yayılım, ağın çıktısının hatasını hesaplayarak bu hatayı minimuma indirmeye yönelik bir yaklaşım sunmaktadır. Bu işlemde, "kayıp fonksiyonu (loss function)" türevlenerek her bir bağlantı ağırlığının nasıl güncelleneceği belirlenmektedir. Ağ parametrelerinin güncellenmesi şu formüle göre yapılır:

$$W = W - n\frac{\partial L}{\partial W} \tag{3.8}$$

Burada, n öğrenme oranını (learning rate) temsil ederken, $\frac{\partial L}{\partial W}$ kayıp fonksiyonunun ağırlıklar üzerindeki gradyanını göstermektedir. Bu güncelleme işlemi, modelin hata oranını düşürerek her bir eğitim adımında daha doğru tahminler yapmasına yardımcı olmaktadır.

Derin öğrenme, yapay sinir ağlarının çok katmanlı yapıları sayesinde veri analizinde yüksek başarı oranlarına ulaşmaktadır. Özellikle büyük veri ve gelişmiş donanım imkanları ile bu teknolojinin daha da gelişmesi beklenmektedir.

Bu çalışmada kullanılan derin öğrenme modeli, çok sınıflı sınıflandırma problemi için uygun şekilde tasarlanmıştır. Model, bir giriş katmanı, iki gizli katman ve bir çıkış katmanından oluşmaktadır. Giriş katmanında, veri setindeki özellik sayısı kadar nöron bulunmakta ve bu katmanda ReLU aktivasyon fonksiyonu kullanılmaktadır. Gizli katmanlardan ilki 256, ikincisi ise 128 nörondan oluşmaktadır. Her iki katmanda da ReLU aktivasyon fonksiyonu tercih edilmiştir. Ayrıca, aşırı öğrenme riskini azaltmak amacıyla, her iki gizli katmanda %50 oranında sönümleme uygulanmıştır. Çıkış katmanı, veri setindeki sınıf sayısı kadar nörona sahiptir ve çok sınıflı sınıflandırma problemleri için uygun olan Softmax aktivasyon fonksiyonu kullanılmıştır. Modelin eğitimi sırasında, kayıp fonksiyonu olarak kategorik çapraz entropi tercih edilmiş ve optimizasyon algoritması olarak "Adam yöntemi" kullanılmıştır. Modelin performansı, doğruluk metriği üzerinden değerlendirilmiştir. Eğitim sürecinde, aşırı öğrenme ve gereksiz fazla eğitimin önlenmesi amacıyla erken durdurma yöntemi uygulanmıştır. Erken durdurma işlemi, doğrulama kaybı metriği izlenerek gerçekleştirilmiş ve sabır süresi 10 epoch olarak belirlenmiştir. Model, maksimum 100 epoch ile eğitilmiş olup, her eğitim iterasyonunda 128 veri örneği kullanılmıştır. Modelin öğrenme sürecinde ödül-ceza mekanizması dolaylı olarak kayıp fonksiyonu ve geri yayılım yöntemi aracılığıyla devreye girmiştir. Doğru tahminler, modelin kayıp değerini azaltarak ödüllendirilmesini sağlarken; yanlış tahminler, kaybı artırarak bir ceza mekanizması işlevi görmüştür. Ayrıca, sönümleme yöntemi, modelin belirli nöronlara aşırı bağımlı hale gelmesini engellemiş ve genelleme yeteneğini artırmıştır. Bu süreçler, modelin ağırlıklarının güncellenmesinde dengeleyici bir rol oynayarak daha doğru sınıflandırmalar yapmasına katkıda bulunmuştur. Bu sayede, modelin performansının optimize edilmesi ve aşırı öğrenme riskinin azaltılması hedeflenmiştir.

4. ARAŞTIRMA BULGULARI

Bu bölümde, tez çalışmasında kullanılan makine öğrenmesi algoritmaları, yapay sinir ağları ve derin öğrenme modelleri ile elde edilen sonuçlar detaylı bir şekilde incelenmektedir. Algoritmaların performansları, karmaşıklık matrislerinden elde edilen doğruluk değerleri, F1 skorları, kesinlik (precision) ve duyarlılık (recall) değerleri ile değerlendirilmiştir. Ayrıca, saldırılar özelinde algoritmaların metrikleri karşılaştırılmış ve algoritmaların çalışma süreleri incelenmiştir.

4.1 Elde Edilen Sonuçlar

IoT cihazları için geliştirilen saldırı tespit sistemi üzerinde çeşitli algoritmalar test edilmiştir. Her bir algoritmanın doğruluk oranı, sınıflandırma raporları ve karmaşıklık matrisleri incelenmiştir. Aşağıda yer alan Çizelge 4.1'de elde edilen sonuçlar özetlenmektedir:

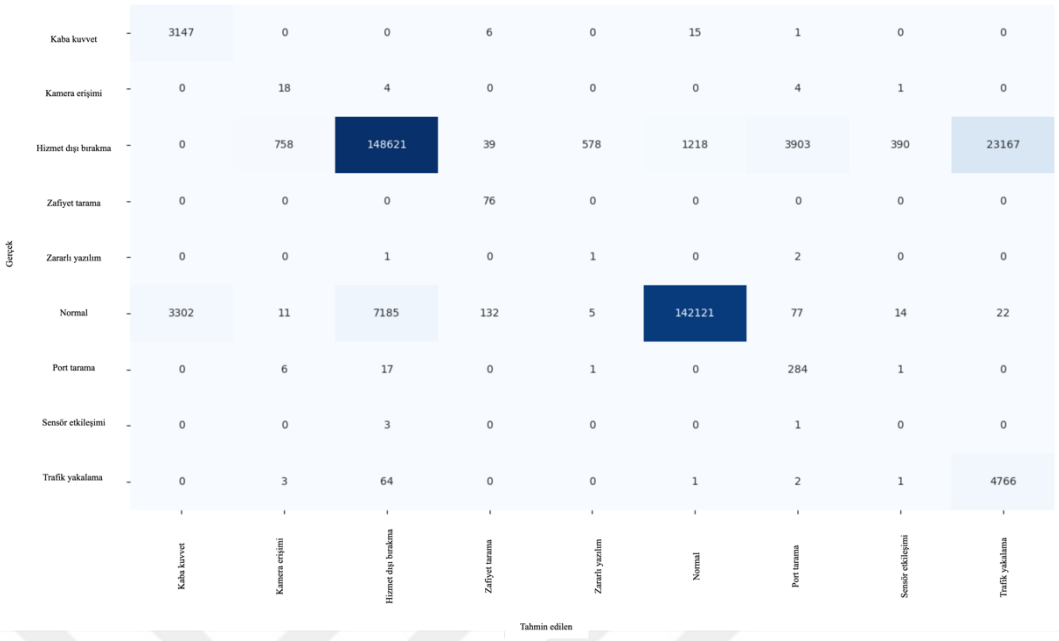
Çizelge 4.1 Elde edilen sonuçlar

Algoritma	**Doğruluk (%)**	**F1-Skoru**	**Kesinlik**	**Duyarlılık**
Rastgele Orman (RF)	87,96	0,91	0,95	0,88
Karar Ağaçları (DT)	87,67	0,90	0,95	0,88
Gradyan Artırıcı Makine (GBM)	88,99	0,92	0,96	0,89
XGBoost	88,32	0,91	0,96	0,88
Destek Vektör Makineleri (SVM)	72,84	0,71	0,74	0,73
K-en Yakın Komşular (KNN)	87,82	0,90	0,94	0,88
Yapay Sinir Ağları (YSA)	87,92	0,91	0,95	0,88
Derin Öğrenme (DL)	88,28	0,91	0,95	0,88

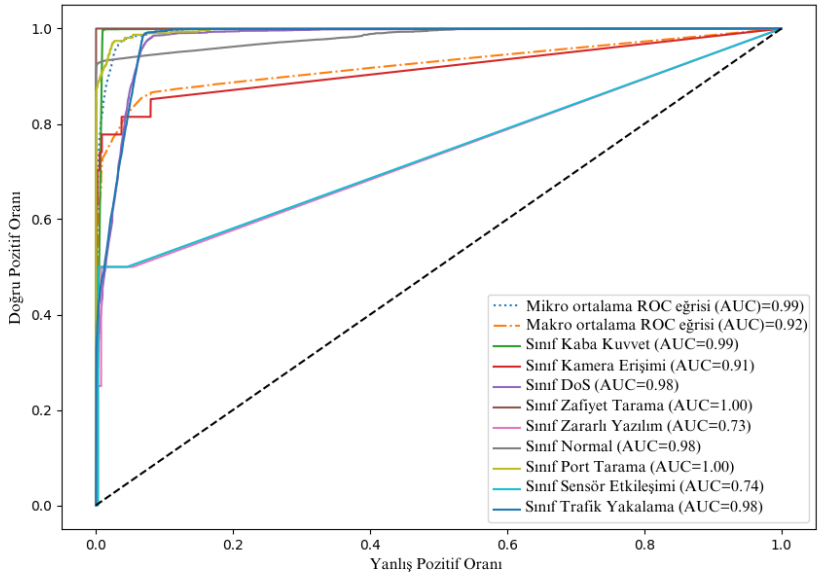
Çizelge 4.1'de yer alan sonuçlara göre, Gradyan Artırıcı Makine (GBM) algoritması %88,99 doğruluk oranı ile en yüksek başarıyı elde etmiştir. GBM, yüksek F1-skoru (0,92), kesinlik (0,96) ve duyarlılık (0,89) değerleri ile dikkat çekmektedir. Bir diğer yüksek performans gösteren algoritma XGBoost (%88,32 doğruluk), GBM'yi takip etmektedir ve benzer şekilde iyi sonuçlar elde etmiştir. Bu algoritmanın da F1-skoru 0,91, kesinliği 0,96 ve duyarlılığı 0,88 olup, yüksek doğruluk oranı ile başarılı bir sınıflandırma performansı görülmektedir. Yapay Sinir Ağları (YSA) ve Derin Öğrenme (DL) algoritmaları ise sırasıyla %87,92 ve %88,28 doğruluk oranları ile iyi bir performans sergilemiştir. Diğer algoritmalar arasında, Rastgele Orman (RF) ve Karar Ağaçları (DT) sırasıyla %87,96 ve %87,67 doğruluk oranları ile dikkat çekmektedir. Her iki algoritma da yüksek kesinlik ve duyarlılık değerlerine sahip olup, başarılı bir sınıflandırma performansı sergilemiştir. K-en Yakın Komşular (KNN) algoritması da %87,82 doğruluk oranı ile etkili bir şekilde çalışmaktadır. Destek Vektör Makineleri (SVM) algoritması, %72,84 doğruluk oranı ile bu çalışmada diğer algoritmaların gerisinde kalmıştır.

4.2 Karmaşıklık Matrisleri ve ROC Eğrileri

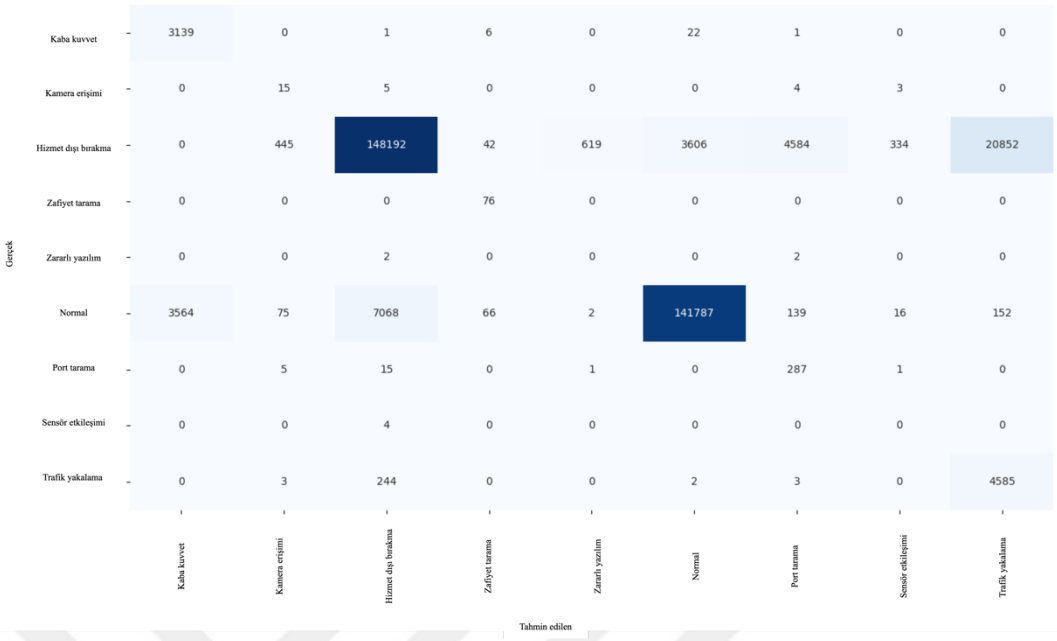
Aşağıdaki şekillerde, her bir algoritmanın farklı saldırı türleri için karmaşıklık matris değerleri ve ROC eğrileri sunulmaktadır. Karmaşıklık matrisi, gerçek ve tahmin edilen sınıflar arasındaki ilişkiyi detaylı bir şekilde ortaya koyarak sınıflandırma performansının analiz edilmesini sağlamaktadır. Matris içerisinde Doğru Pozitif, Doğru Negatif, Yanlış Pozitif ve Yanlış Negatif değerleri yer almaktadır. Bu değerler aracılığıyla modelin doğru sınıflandırma oranları ve yapılan hatalar belirlenmektedir. ROC eğrisi ise, Doğru Pozitif Oranı ile Yanlış Pozitif Oranı arasındaki ilişkiyi ortaya koyarak modelin ayırt edicilik yeteneği değerlendirilmektedir. Eğri altındaki alanın büyüklüğü, modelin sınıflandırma başarısının bir göstergesi olarak kullanılmaktadır.



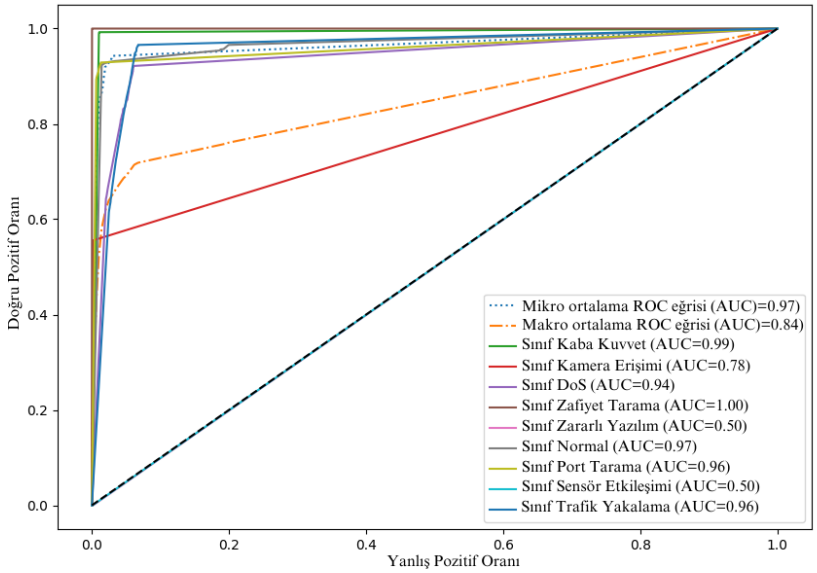
Şekil 4.1 Rastgele Orman karmaşıklık matrisi



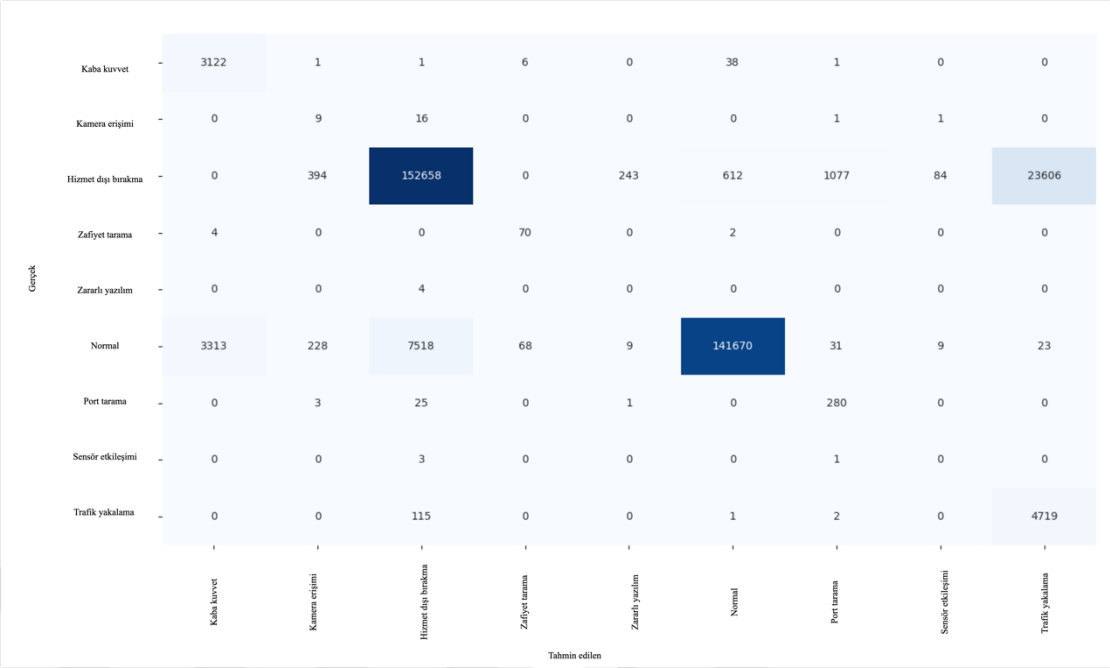
Şekil 4.2 Rastgele Orman ROC eğrisi



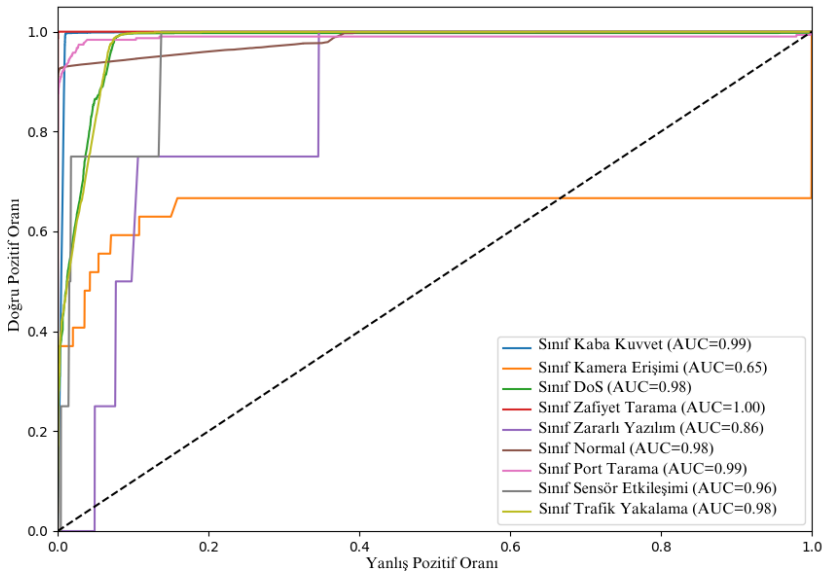
Şekil 4.3 Karar Ağaçları karmaşıklık matrisi



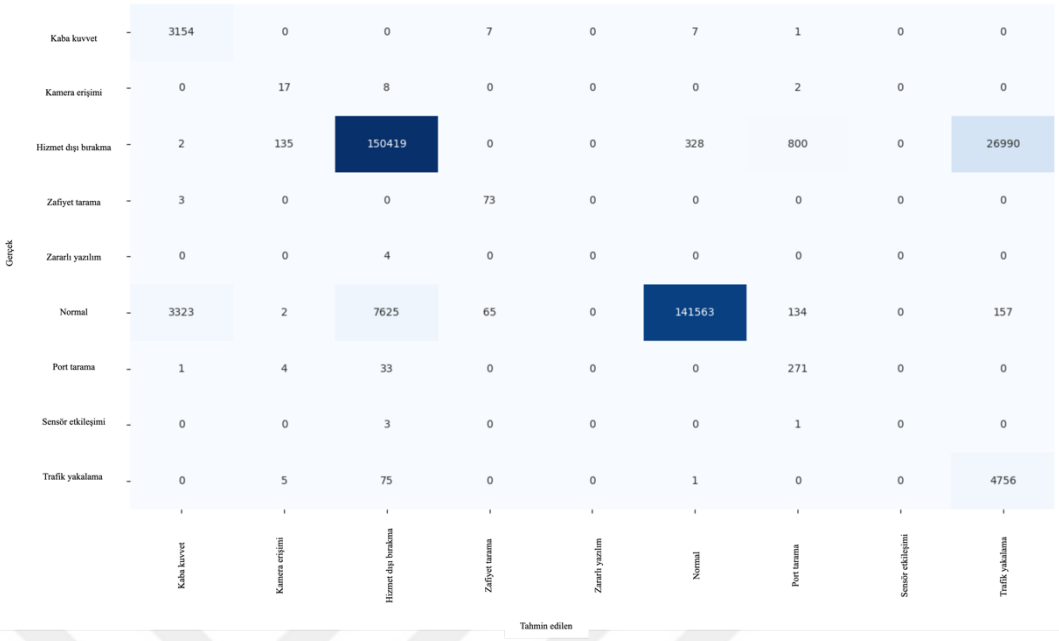
Şekil 4.4 Karar Ağaçları ROC eğrisi



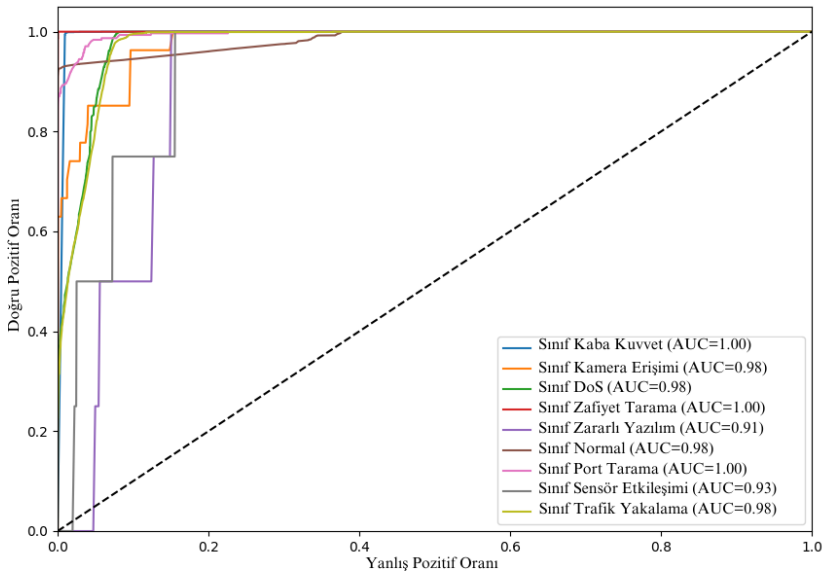
Şekil 4.5 GBM karmaşıklık matrisi



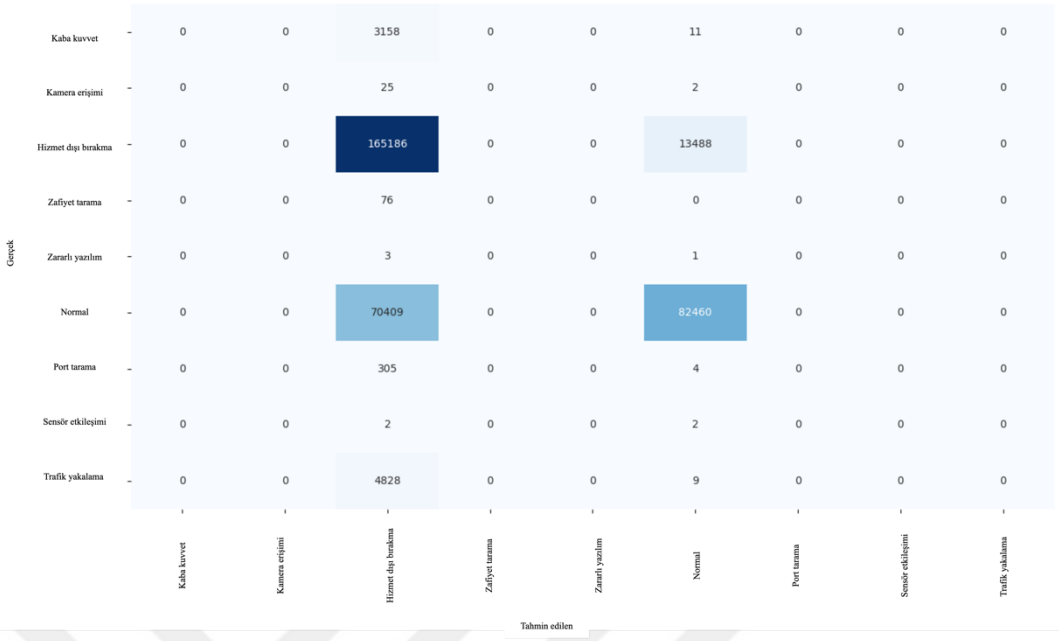
Şekil 4.6 GBM ROC eğrisi



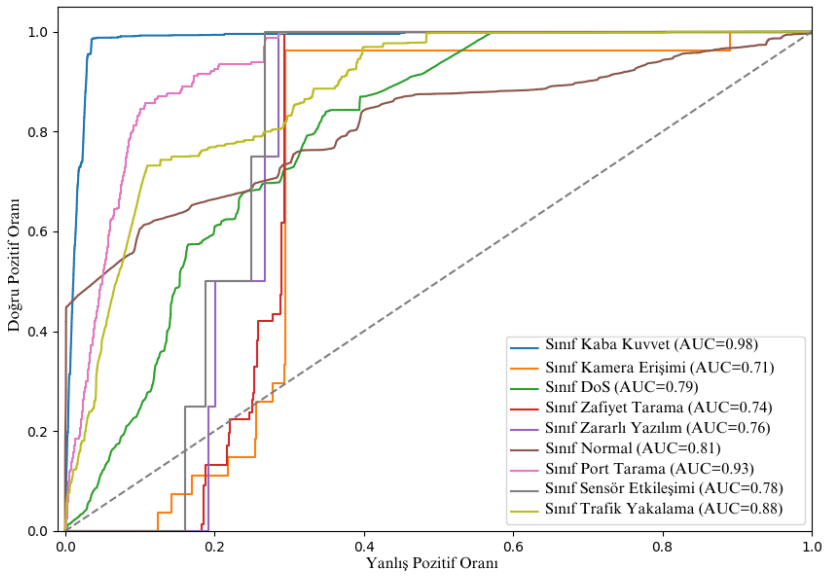
Şekil 4.7 XGBoost karmaşıklık matrisi



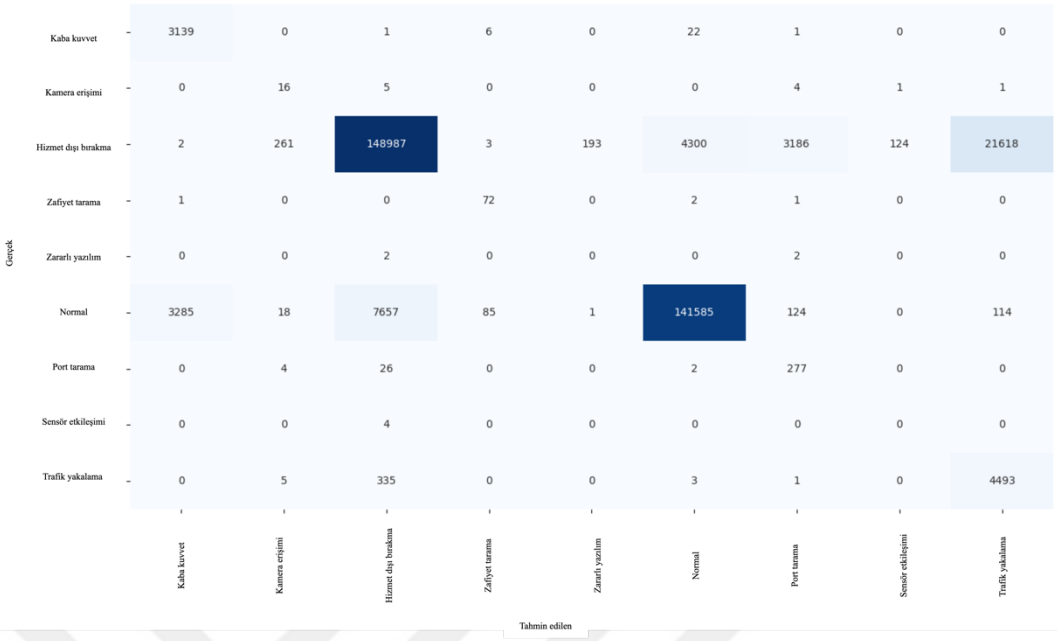
Şekil 4.8 XGBoost ROC eğrisi



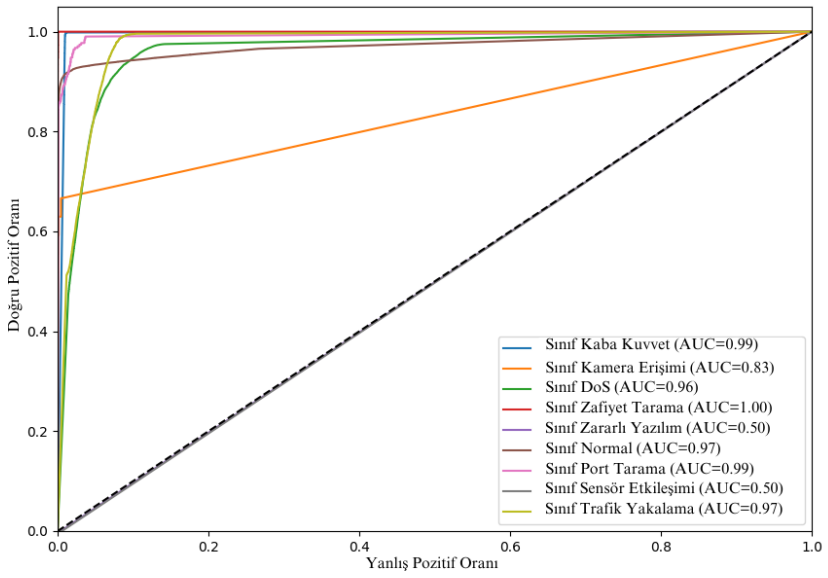
Şekil 4.9 SVM karmaşıklık matrisi



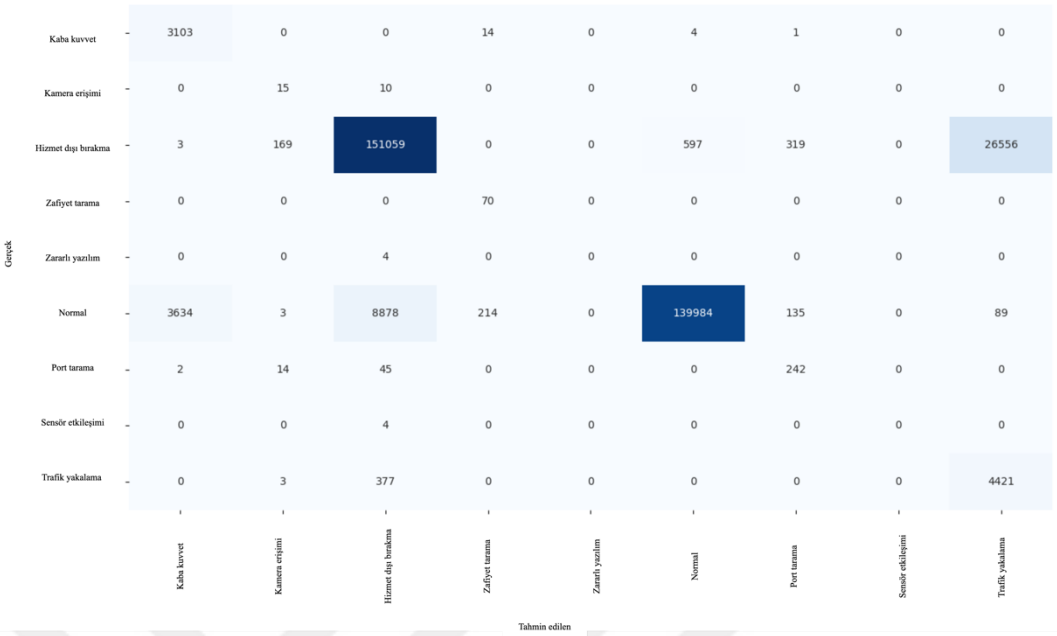
Şekil 4.10 SVM ROC eğrisi



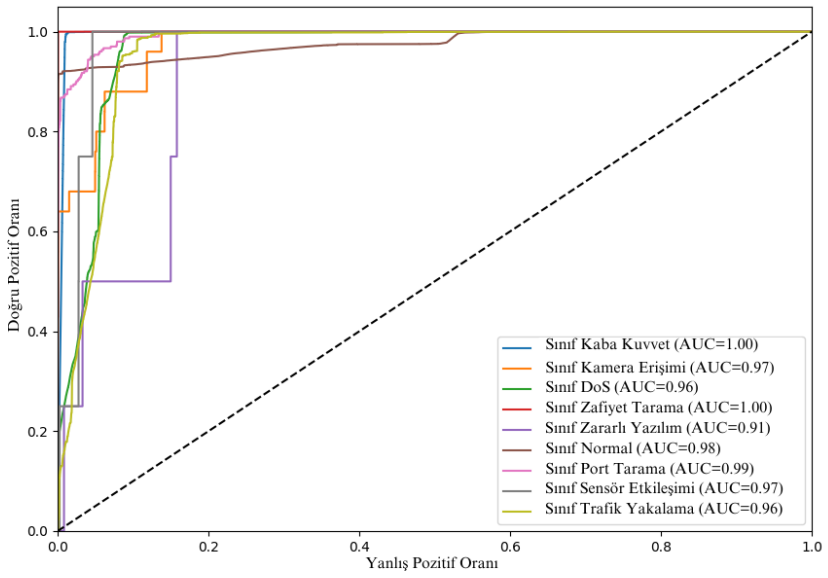
Şekil 4.11 KNN karmaşıklık matrisi



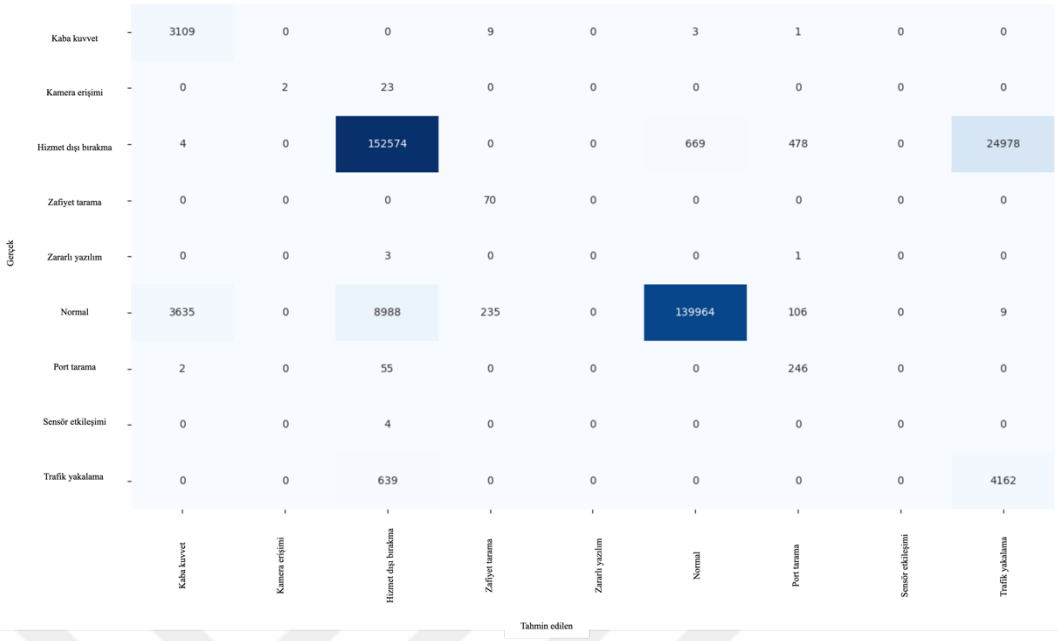
Şekil 4.12 KNN ROC eğrisi



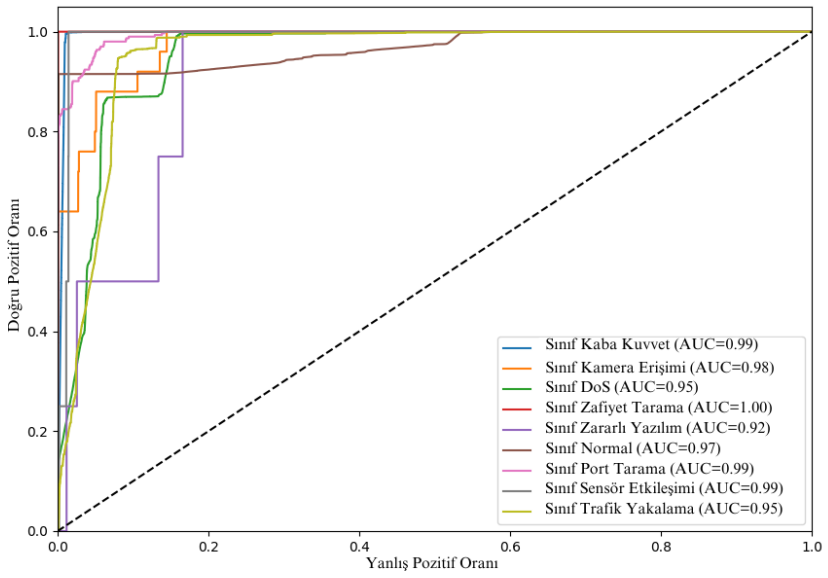
Şekil 4.13 YSA karmaşıklık matrisi



Şekil 4.14 YSA ROC eğrisi



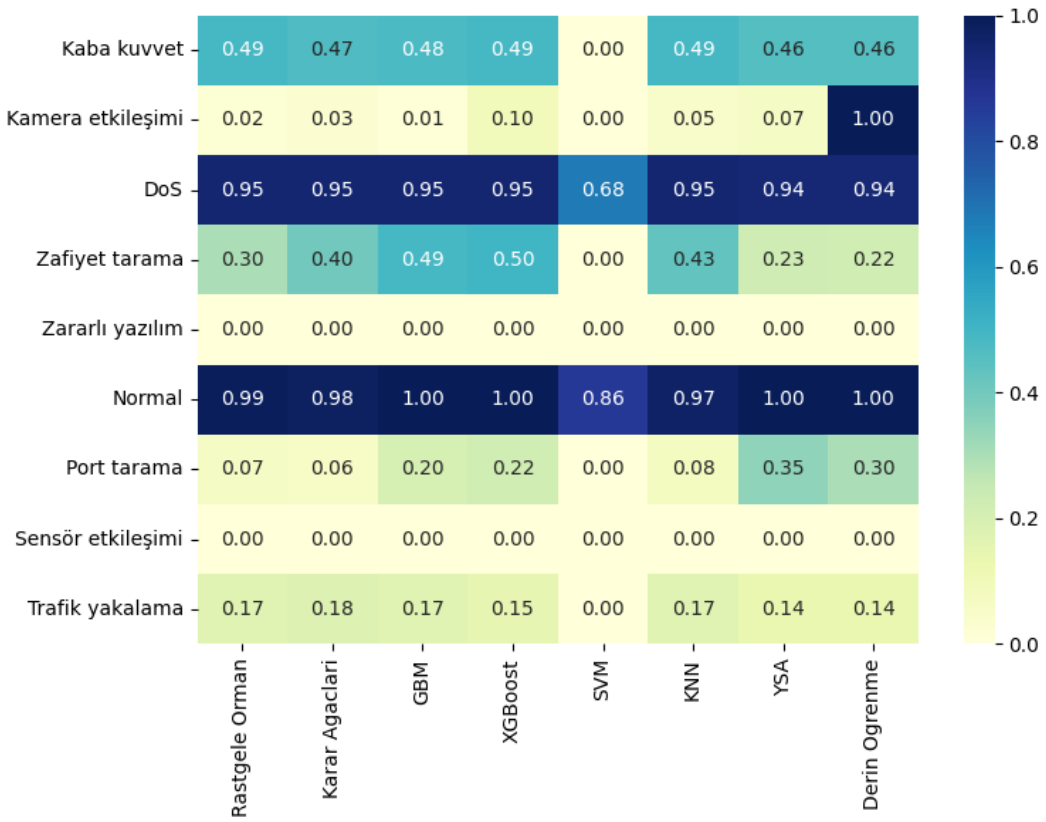
Şekil 4.15 Derin öğrenme karmaşıklık matrisi



Şekil 4.16 Derin öğrenme ROC eğrisi

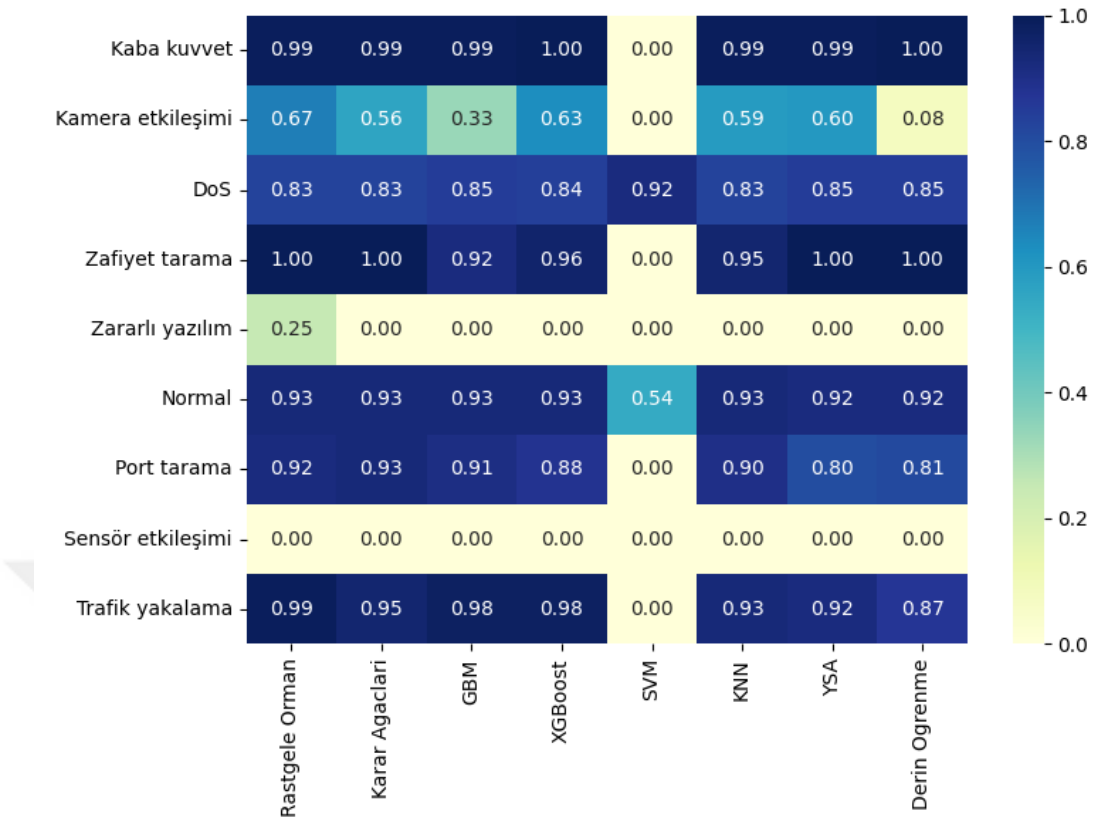
4.3 Kesinlik, Duyarlılık ve F1-Skor Metrikleri

Bu bölümde, model performansının değerlendirilmesinde yaygın olarak kullanılan kesinlik, duyarlılık ve F1-skoru metrikleri sunulmuştur. Kesinlik, bir algoritmanın pozitif olarak sınıflandırdığı olaylardan ne kadarının gerçekten doğru (gerçek saldırılar) olduğunu gösteren bir metriktir. Bu metrik, pozitif tahminlerin doğruluğunu ve algoritmaların hangi saldırı türlerinde daha etkili olduğunu daha net bir şekilde ortaya koymaktadır. Şekil 4.17'de her bir algoritmanın her bir saldırı türü için kesinlik değerlerine ilişkin bir matris sunulmaktadır. Elde edilen sonuçlar, algoritmaların pozitif sınıflandırma doğruluklarını ve farklı saldırı türlerindeki etkinliklerini değerlendirme imkânı sunmaktadır. Normal trafik ve DoS saldırıları için genel olarak yüksek kesinlik değerleri (genellikle %95 ve üzeri) elde edilmiştir. Ancak, kamera etkileşimi, sensör etkileşimi ve zararlı yazılımların test verilerinin yetersizliği nedeniyle bu alanlarda daha düşük kesinlik oranları gözlemlenmiştir. Bunun yanı sıra, XGBoost ve Karar Ağaçları algoritmalarının bazı saldırı türlerinde diğer yöntemlere kıyasla daha yüksek kesinlik değerleri sağladığı tespit edilmiştir. Öte yandan, Derin Öğrenme yönteminin özellikle kamera etkileşimi sınıfında belirgin bir başarı gösterdiği belirlenmiştir. Genel olarak, sonuçlar, algoritmaların farklı saldırı türlerindeki performansları arasındaki belirgin farkları açıkça ortaya koymaktadır.



Şekil 4.17 Kesinlik değerleri matrisi

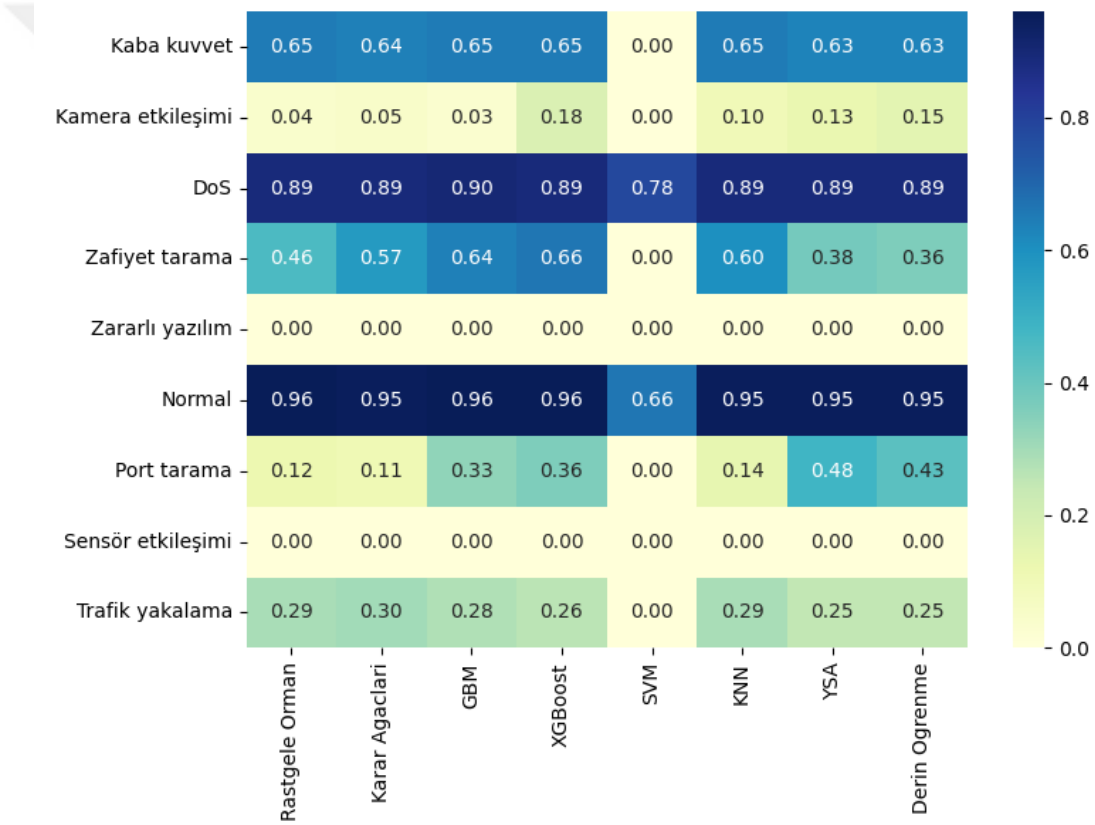
Duyarlılık, bir algoritmanın tüm gerçek saldırılardan (gerçek pozitifler) ne kadarını doğru şekilde tespit ettiğini gösteren bir metriktir. Yani, duyarlılık yüksek olduğunda, algoritma daha fazla gerçek saldırıyı yakalamış demektir. Bu metrik, algoritmaların hangi saldırı türlerinde daha fazla başarı gösterdiğini ve hangi saldırıların algılanmasında zorluk yaşandığını açıkça göstermektedir. Şekil 4.18'de her bir algoritmanın her bir saldırı türü için duyarlılık değerlerine ilişkin bir matris yer almaktadır. Matrisin incelenmesi sonucunda, Rastgele Orman, Derin Öğrenme ve XGBoost algoritmalarının birçok saldırı türünde yüksek duyarlılık değerleri sergilediği görülmektedir. Özellikle kaba kuvvet, zafiyet tarama ve trafik yakalama saldırılarında bu algoritmaların oldukça başarılı olduğu tespit edilmiştir. Bununla birlikte, sensör etkileşimi ve zararlı yazılım saldırı türlerinde düşük test verisi nedeniyle tüm algoritmaların düşük duyarlılık değerleri sergilediği gözlemlenmiştir. Ayrıca, Rastgele Orman algoritmasının genel olarak yüksek ve tutarlı duyarlılık değerleri sunduğu görülmüştür.



Şekil 4.18 Duyarlılık değerleri matrisi

F1-Skoru, kesinlik ve duyarlılık metriklerinin dengelenmiş bir ölçüsüdür. Yüksek bir F1-Skoru, algoritmanın hem yüksek doğrulukla hem de yüksek duyarlılıkla sınıflandırma yaptığını göstermektedir. F1-Skoru, özellikle dengesiz veri setlerinde ve sınıflar arasında önemli farklar olduğunda, kesinlik ve duyarlılık arasındaki dengeyi göz önünde bulundurarak daha doğru bir değerlendirme sunmaktadır. Bu metrik, algoritmaların genel sınıflandırma performansını ve hangi saldırı türlerinde daha etkili olduklarını yansıtmaktadır. Şekil 4.19'da her bir algoritmanın her bir saldırı türü için F1-Skoru değerlerine ilişkin bir matris bulunmaktadır. Matris incelendiğinde, DoS ve normal gibi sınıflarda algoritmaların oldukça yüksek F1-Skor değerlerine ulaştığı ve bu türlerin hem duyarlılık hem de kesinlik açısından dengeli bir şekilde tespit edilebildiği görülmektedir. Bu durum, modellerin bu saldırı türlerini başarılı bir şekilde öğrenebildiğini ve test verisinde güçlü bir performans sergilediğini göstermektedir. Ayrıca, bazı algoritmaların zafiyet tarama gibi saldırılarda da nispeten iyi bir performans sunduğu dikkat çekmektedir. Bununla birlikte, zararlı yazılım, kamera etkileşimi ve sensör etkileşimi gibi

bazı saldırı türlerinde F1-Skor değerlerinin düşük olduğu görülmüştür. Ancak bu durum, modelin yetersizliğinden değil, bu saldırı türlerine ait sınırlı test verisinden kaynaklanmaktadır. Test verisinin azlığı, algoritmaların bu türleri tespit edebilme kapasitesini sınırlamış, dolayısıyla F1-Skor değerlerini olumsuz etkilemiştir. Bu durum, bu tür saldırıların tespiti için veri miktarının artırılmasının önemini vurgulamaktadır. Algoritmalar arasında değerlendirildiğinde, Rastgele Orman, XGBoost ve Derin Öğrenme algoritmalarının birçok saldırı türünde istikrarlı ve güçlü bir performans sergilediği gözlemlenmiştir. Özellikle kaba kuvvet, DoS ve trafik yakalama gibi saldırı türlerinde bu algoritmalar öne çıkmıştır.

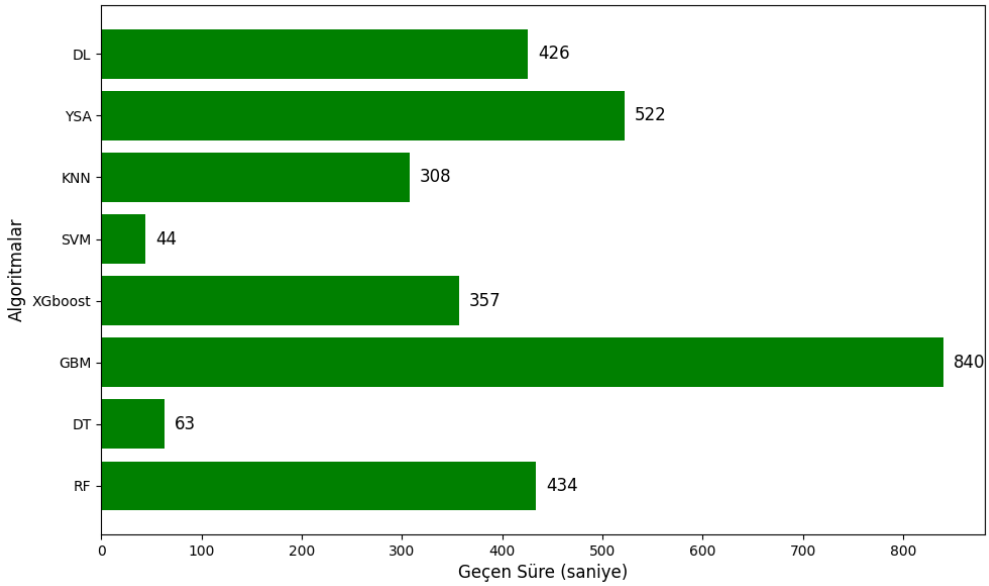


Şekil 4.19 F1-Skor değerleri matrisi

4.4 Algoritmaların Çalışma Süreleri

Tez çalışma kapsamında algoritmaların toplam çalışma süreleri de ölçülmüştür. Şekil 4.20'de algoritmaların toplam çalışma süreleri sunulmaktadır. Kullanılan sistem, dört

çekirdekli ve 1,4 GHz hızında çalışan Intel Core i5 işlemciye sahiptir. Ayrıca, 8 GB RAM ile desteklenmiş ve macOS 15.1.1 işletim sistemi üzerinde çalıştırılmıştır. Bu sistem özellikleri, algoritmaların performanslarının değerlendirilmesinde referans olarak kullanılmıştır.



Şekil 4.20 Algoritmaların çalışma süreleri

Rastgele orman algoritmasının, 434 saniyede %87,96 doğruluk ile çalıştığı görülmektedir. Bu algoritmanın işlem süresi uzun olmakla birlikte karmaşık veri setlerinde etkili sonuçlar verdiği gözlemlenmiştir. KNN ise 308 saniyede %87,82 doğruluk ile benzer bir performans sergilemiştir. GBM, 840 saniyede %88,99 doğruluk ile en yüksek doğruluğu sağlarken, aynı zamanda işlem süresi de en uzun olmuştur. XGBoost, 357 saniyede %88,32 doğruluk ile çalışmış ve daha kısa sürede benzer doğruluk sunmuştur. SVM, 44 saniye ile en hızlı algoritma olup, %72,84 doğruluk sağlamıştır. Karar Ağaçları 63 saniye ile %87,67 hızlı ve yüksek doğruluk oranı sunmuştur. YSA %87,92 doğruluk ve 522 saniye işlem süresi ile yüksek doğruluk sağlarken, derin öğrenme %88,28 doğruluk ve 426 saniye işlem süresi ile benzer bir performans sergilemiştir.

5. TARTIŞMA VE SONUÇ

Günümüzde IoT cihazları, hayatın her alanında yaygın olarak kullanılmakta ve bu cihazlar, ağlara bağlanarak veri iletimi ve alımı gerçekleştirmektedir. Ancak bu durum, IoT cihazlarını çeşitli siber saldırılara açık hale getirmektedir. IoT cihazlarına yönelik saldırılar, ağ trafiği üzerinden tespit edilebilen anormal davranışlarla kendini gösterebilmektedir. Bu nedenle, ağ trafiği verilerinin kullanılarak IoT cihazlarına yönelik saldırıların tespit edilmesi, siber güvenlik alanında önemli bir araştırma konusu haline gelmiştir. Literatürde, IoT saldırılarının tespit edilmesi amacıyla genellikle makine öğrenmesi tekniklerinden yararlanıldığı görülmektedir.

Bu tez çalışmasında, IoT cihazları için makine öğrenmesi tabanlı bir saldırı tespit sistemi geliştirilmesi hedeflenmiştir. Literatürdeki çalışmalarda olduğu gibi, ağ trafiği üzerinden saldırı tespiti yapılmış, ancak bu tezde kullanılan veri setinin, IoT cihazları için en sık karşılaşılabilecek saldırı türlerini kapsamasına dikkat edilmiştir. Literatürde genellikle denetimli öğrenme algoritmalarına odaklanılırken, bu çalışmada farklı makine öğrenmesi algoritmalarının performansları karşılaştırılmış ve Rastgele Orman, SVM ve XGBoost gibi algoritmaların performansları analiz edilmiştir. Literatürde benzer algoritmalarla elde edilen sonuçlarla bu tezdeki bulguların benzerlik gösterdiği, özellikle XGBoost algoritmasının yüksek doğruluk oranı ve güçlü F1-Skoru gibi metriklerde etkili olduğu belirlenmiştir.

Çalışma sürecinde, özellik mühendisliği ve veri ön işleme süreçlerine odaklanılmış ve bu süreçlerin model doğruluğunu önemli ölçüde artırdığı sonucuna varılmıştır. Ayrıca, farklı makine öğrenmesi algoritmaları performans metrikleri açısından karşılaştırılmıştır. Çalışmada, etiketli veri üzerinden sınıflandırma işlemi gerçekleştirilmesi amacıyla ağırlıklı olarak denetimli öğrenme algoritmaları tercih edilmiştir. Bunun yanı sıra, pekiştirmeli öğrenme yöntemleri kapsamında derin öğrenme teknikleri de kullanılmıştır. Yapay Sinir Ağları ve Derin Öğrenme yöntemleri, çok sınıflı sınıflandırma problemlerine yönelik olarak başarıyla uygulanmıştır. Modellerde giriş, gizli ve çıkış katmanları özenle tasarlanmış ve uygun aktivasyon fonksiyonları tercih edilmiştir. Eğitim sürecinde, kategorik çapraz entropi kayıp fonksiyonu, Adam optimizasyon algoritması ve erken

durdurma yöntemi kullanılarak model performansı optimize edilmiştir. Ayrıca, sönümleme oranlarıyla aşırı öğrenme riski azaltılarak genelleme yeteneği artırılmıştır. Bu yöntemlerin birlikte kullanımı, sınıflandırma performansını artırarak veri setindeki karmaşık ilişkilerin modellenmesinde etkili sonuçlar sağlamıştır. Her iki yöntemin de başarılı sonuçlar elde ettiği görülmüştür.

Çalışma kapsamında yapılan analiz sonuçlarına göre, en yüksek doğruluk oranı (%88,99) ve F1-Skoru (0,92), GBM algoritması tarafından elde edilmiştir. GBM, aynı zamanda kesinlik (0,96) ve duyarlılık (0,89) metriklerinde de yüksek başarı göstermiştir. XGBoost algoritması ise %88,32 doğruluk oranı ve 0,91 F1-Skoru ile güçlü bir performans sergilemiştir. Derin Öğrenme %88,28 doğruluk ve 0,91 F1-Skoru ve Rastgele Orman algoritması %87,96 doğruluk ve 0,91 F1-Skoru ile dengeli bir performans sağlamıştır.

Orta seviyede performans sergileyen algoritmalar arasında YSA, KNN ve Karar Ağaçları yer almaktadır. Bu algoritmalar, yaklaşık %88 doğruluk oranı ile Rastgele Orman'a yakın sonuçlar sunmuştur. Daha düşük performans sergileyen algoritma olarak SVM yer almıştır. SVM algoritması %72,84 doğruluk oranı ve 0,71 F1-Skoru ile düşük bir performans göstermiştir.

Farklı algoritmaların doğruluk ve işlem süreleri karşılaştırıldığında, GBM en yüksek doğruluğu elde etmiş ancak en uzun işlem süresine sahip olmuştur. XGBoost benzer doğrulukla daha kısa sürede işlem yaparak işlem süresi açısından daha verimli bir seçenek sunmuştur. Rastgele Orman da benzer doğruluklarla daha uzun işlem süresi gerektirmiştir. Karar Ağaçları ile hızlı ve etkili sonuç edilmiştir. KNN benzer doğrulukla makul bir işlem süresi sergilerken, SVM en hızlı algoritma olmasına rağmen doğruluk oranı daha düşük kalmıştır. YSA ve Derin Öğrenme, uzun işlem sürelerine rağmen yüksek doğruluk sağlamış ve iyi performans göstermiştir. Çalışma kapsamında süre arttıkça lineer bir şekilde olmasa da doğruluk oranlarında da artış olduğu görülmüştür.

Sonuç olarak, GBM, XGBoost, Rastgele Orman ve Derin Öğrenme gibi algoritmalar, IoT cihazlarına yönelik saldırıların tespitinde yüksek doğruluk oranlarıyla öne çıkmıştır. Bu bulgular, IoT saldırı tespit sistemlerinin geliştirilmesinde algoritma seçiminin ve veri seti

yapısının kritik bir öneme sahip olduğunu ortaya koymaktadır. Daha dengeli ve güvenilir sonuçlar elde edebilmek için veri ön işleme ve özellik mühendisliği süreçlerinin titizlikle planlanması gerektiği anlaşılmıştır. Ayrıca, büyük veri setlerinde daha az temsil edilen sınıflarda oluşabilecek veri dengesizliğini önlemek için gerekli çalışmaların yapılmasının önem taşıdığı vurgulanmıştır. Bununla birlikte, kullanılan algoritmaların belirli saldırı türlerinde daha güçlü performans gösterdiği göz önünde bulundurularak, saldırı tespit modellerinin bu türlere göre optimize edilmesinin faydalı olacağı değerlendirilmektedir. Bu tez çalışması ile makine öğrenmesi algoritmalarının IoT güvenliği alanındaki etkinliği bir kez daha ortaya konulmuştur. Ayrıca, daha geniş kapsamlı saldırı türlerinin dahil edildiği veri setleriyle yapılacak gelecekteki çalışmaların bu alandaki ilerlemelere önemli katkılar sağlayacağı düşünülmektedir.

KAYNAKLAR

Adamu, B. Z. 2022. Detection and Analysis of Cyber-attacks on IoT Network Devices. Yüksek Lisans Tezi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Adli Bilişim Mühendisliği Anabilim Dalı, 58, Elazığ.

Alpaydın, E. 2014. Introduction to Machine Learning. The MIT Press, 640, Cambridge, MA.

Amarouche, S. 2021. Comparison of Intrusion Detection for the Internet of Things with Machine and Deep Learning Methods. Yüksek Lisans Tezi, Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, 65, Kocaeli.

Anonymous, 2022a. Web Sitesi: https://bytebeam.io/blog/a-brief-history-of-internet-of-things/, Erişim Tarihi: 03.08.2024.

Anonymous, 2022b. Web Sitesi: https://scikit-learn.org/1.5/modules/tree.html#, Erişim Tarihi: 02.12.2024.

Anonymous, 2023a. Web Sitesi: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023, Erişim Tarihi: 05.08.2024.

Anonymous, 2023b. Web Sitesi: https://www.ericsson.com/49dd9d/assets/local/reports-papers/mobility-report/documents/2023/ericsson-mobility-report-june-2023.pdf, Erişim Tarihi: 05.08.2024.

Anonymous, 2023c. Web Sitesi: https://www.statista.com/statistics/1377569/worldwide-annual-internet-of-things-attacks/, Erişim Tarihi: 05.08.2024.

Anonymous 2024. Web Sitesi: https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/10k-most-common.txt, Erişim Tarihi: 30.07.2024

Ashton, K. 2009. That 'Internet of Things' Thing. RFID Journal.

Aydın, E. 2022. An Online Network Intrusion Detection System for DDoS Attacks with IoT Botnet. Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, 84, İstanbul.

Balcı, Y. 2021. Nesnelerin İnterneti Ekosisteminde Yapay Zeka Destekli Saldırı Tespit Sistemi. Yüksek Lisans Tezi, Millî Savunma Üniversitesi, Hezârfen Havacılık ve Uzay Teknolojileri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, 40, İstanbul.

Bang, A. O., Rao, U. P., Visconti, A., Brighente, A., Conti, M. 2022. An IoT Inventory Before Deployment: A Survey on IoT Protocols, Communication Technologies, Vulnerabilities, Attacks, and Future Research Directions. Computers & Security, 123, 102914.

Binglaw, F. 2021. Security Issues in the Internet of Things: Requirements, Attacks, and Countermeasures. Yüksek Lisans Tezi, Atılım Üniversitesi, Fen Bilimleri Enstitüsü, Bilgi Teknolojileri Anabilim Dalı, 186, Ankara.

Breiman, L. 2001. Random Forests. Machine Learning 45, 5–32.

Chen, T., ve Guestrin, C. 2016. XGBoost: A scalable tree boosting system. arXiv preprint arXiv:1603.02754.

Cover, T. ve Hart, P. 1967. Nearest neighbor pattern classification. IEEE Transactions on Information Theory, 13(1), 21-27.

Cunningham, P. ve Delany, S. J. 2007. k-Nearest neighbour classifiers. Multiple Classifier Systems, 34(8), 1-17.

Çekmez, U. 2022. Nesnelerin İnterneti İçin Derin Öğrenme ile Veri Odaklı Ağ Saldırı Sınıflandırma Sistemi. Doktora Tezi, Marmara Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, 186, İstanbul.

Çıkmazel, R. O. 2022. Anomaly Prediction for the Internet of Things. Yüksek Lisans Tezi, Yaşar Üniversitesi, Fen Bilimleri Enstitüsü, Elektrik ve Elektronik Mühendisliği Anabilim Dalı, 94, İzmir.

Deniz, E. 2019. Nesnelerin İnternetinde Gizlilik ve Güvenlik Yönetimi. Yüksek Lisans Tezi, Ankara Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, 51, Ankara.

Emeç, M. 2022. Increasing Communication Security Among Internet of Things. Doktora Tezi, Dokuz Eylül Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, 186, İzmir.

Ergün, A. E. 2023. IoT Cihazlarının Sınıflandırılması ve IoT Trafik Analizine Karşı Mahremiyet-Fayda Dengesinin İyileştirilmesi. Yüksek Lisans Tezi, Ege Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, 95, İzmir.

Fei, W., Ohno, H., Sampalli, S. 2023. A Systematic Review of IoT Security: Research Potential, Challenges, and Future Directions. ACM Comput. Surv., 56(5), Article 111, 40 pages.

Friedman, J. H. 2001. Greedy function approximation: A gradient boosting machine. Annals of Statistics 29(5): 1189-1232.

Gerodimos, A., Maglaras, L., Ferrag, M. A., Ayres, N., Kantzavelou, I. 2023. IoT: Communication protocols and security threats. Internet of Things and Cyber-Physical Systems, 3(1), 1-13.

Hastie, T., Tibshirani, R. ve Friedman, J. 2009. Data mining, inference, and prediction, In: The Elements of Statistical Learning. Hastie, T., Tibshirani, R. ve Friedman, J. (eds), Springer, 83-119, New York.

Haykin, S. 2009. Neural Networks and Learning Machines. Pearson Prentice Hall, 906, New York.

Ioannou, C. ve Vassiliou, V. 2021. Network attack classification in IoT using support vector machines. Journal of Sensor and Actuator Networks, 10(3); 58.

Iqbal, M.A., Hussain, S., Xing, H. and Imran, M.A. 2021. Enabling the Internet of Things: Fundamentals, Design, and Applications. Wiley, 264, Chennai, India.

ITU. 2005. The Internet of Things. ITU Internet Reports.

Kolukısa, B. 2024. Machine Learning Approaches for Internet of Things Based Vehicle Type Classification and Network Anomaly Detection. Doktora Tezi, Abdullah Gül Üniversitesi, Fen Bilimleri Enstitüsü, Elektrik ve Bilgisayar Mühendisliği Anabilim Dalı, 132, Kayseri.

Kuriş, U. 2019. Nesnelerin İnterneti Ekosisteminde Yapay Zeka Tabanlı Saldırı Tespit Sistemi Geliştirilmesi. Yüksek Lisans Tezi, İstanbul Üniversitesi-Cerrahpaşa, Lisansüstü Eğitim Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, 72, İstanbul.

Kwaider, H. A. 2023. Makine Öğrenimini Kullanarak IoT Ağlarında Saldırı Tespiti. Yüksek Lisans Tezi, Mersin Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, 94, Mersin.

Minerva, R., Biru, A., and Rotondi, D. 2015. Towards a definition of the internet of things (IoT). IEEE Internet Initiative 1: 1-86.

Mitchell, T. M. 1997. Machine Learning. McGraw-Hill, 414, New York.

Özdogan, E. 2024. A Comprehensive Analysis of the Machine Learning Algorithms in IoT IDS Systems. IEEE Access, 12, 46785-46811.

Özkal, S. Y. 2021. Increasing Security in Communication Between IoT Devices. Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, 84, İzmir.

Rahaman, M. N., Chaki, S., Biswas, M. S., Biswas, M., Ahmed, S., Mahi, M. J. N., ve Faruqui, N. 2022. Identifying the signature of suicidality: A machine learning approach. THEETAS, EAI.

Ren, L. ve Cao, S. 2022. Application of Feature Selection Based on Elastic Network and Random Forest in the Evaluation of Sports Effects. Journal of Electrical and Computer Engineering, 1-9.

Roberti, M. 2004. Navy Revs Up RFID Sensors. RFID Journal.

Salati, M. 2024. Analysis of Network Security Using Machine Learning Methods. Doktora Tezi, Ankara Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, 132, Ankara.

Saleh, T. E. 2022. Comparison of the Effects of Data Privacy Preserving Methods on Machine Learning Algorithms in IoT. Yüksek Lisans Tezi, Marmara Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik ve Bilgisayar Mühendisliği Anabilim Dalı, 58, İstanbul.

Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., Stiller, B. 2022. Landscape of IoT security. Computer Science Review, 44, 100467.

Sultan, A. S. 2023. IoT and Physical Cyber Security Intrusion Detection Based on Supervised Machine Learning. Yüksek Lisans Tezi, Bahçeşehir Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, 42, İstanbul.

Taş, O. 2022. Nesnelerin İnterneti İçin Akıllı Saldırı Tespit Sistemleri Geliştirilmesi. Doktora Tezi, İstanbul Sabahattin Zaim Üniversitesi, Lisansüstü Eğitim Enstitüsü, Bilgisayar Bilimleri ve Mühendisliği Anabilim Dalı, 139, İstanbul.

Tekin, R. 2022. Nesnelerin İnterneti Uygulamaları İçin Saldırı Tespit Yöntemlerinin Geliştirilmesi. Yüksek Lisans Tezi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Adli Bilişim Mühendisliği Anabilim Dalı, 65, Elazığ.

Yaraş, S. 2024. IoT'de Meydana Gelen DDoS Saldırılarının Derin Öğrenme Yöntemleri Kullanılarak Büyük Veri Ortamında Analizi ve Tespiti. Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Bilgi Güvenliği Mühendisliği Anabilim Dalı, 85, Ankara.

Yavuz, F. Y. 2020. Deep Learning in Cyber Security for Internet of Things. Yüksek Lisans Tezi, Şehir Üniversitesi, Fen Bilimleri Enstitüsü, Siber Güvenlik Mühendisliği Anabilim Dalı, 190, İstanbul.

Zhang, L., Wang, S. ve Liu, B. 2018. Deep learning for sentiment analysis: A survey. arXiv (cs.CL), 1801.07883v2, 1-34.