T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

NESNELERİN İNTERNETİ UYGULAMALARI İÇİN SALDIRI TESPİT YÖNTEMLERİNİN GELİŞTİRİLMESİ

Rojbin TEKİN

Yüksek Lisans Tezi

ADLİ BİLİŞİM MÜHENDİSLİĞİ ANABİLİM DALI

Adli Bilişim Mühendisliği Bilim Dalı

HAZİRAN 2022

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Adli Bilişim Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

NESNELERİN İNTERNETİ UYGULAMALARI İÇİN SALDIRI TESPİT YÖNTEMLERİNİN GELİŞTİRİLMESİ

Tez Yazarı
Rojbin TEKİN

Danışman
Dr. Öğr. Üyesi Orhan YAMAN

HAZİRAN 2022
ELAZIĞ

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Adli Bilişim Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

Başlığı:	Nesnelerin İnterneti Uygulamaları için Saldırı Tespit Yöntemlerinin Geliştirilmesi
Yazarı:	Rojbin TEKİN
İlk Teslim Tarihi:	23.05.2022
Savunma Tarihi:	24.06.2022

TEZ ONAYI

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına göre hazırlanan bu tez aşağıda imzaları bulunan jüri üyeleri tarafından değerlendirilmiş ve akademik dinleyicilere açık yapılan savunma sonucunda OYBİRLİĞİ ile kabul edilmiştir.

	İmza	
Danışman:	Dr. Öğr. Üyesi Orhan YAMAN Fırat Üniversitesi, Teknoloji Fakültesi	Onayladım
Başkan:	Dr. Ögr. Üyesi Gülşah KARADUMAN Fırat Üniversitesi, Mühendislik Fakültesi	Onayladım
Üye:	Dr. Öğr. Üyesi Taha MÜEZZİNOĞLU Munzur Üniversitesi, Mühendislik Fakültesi	Onayladım

Bu tez, Enstitü Yönetim Kurulunun ...../...../20..... tarihli toplantısında tescillenmiştir.

İmza

Prof. Dr. Kürşat Esat ALYAMAÇ
Enstitü Müdürü

BEYAN

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım "Nesnelerin İnterneti Uygulamaları için Saldırı Tespit Yöntemlerinin Geliştirilmesi" Başlıklı Yüksek Lisans Tezimin içindeki bütün bilgilerin doğru olduğunu, bilgilerin üretilmesi ve sunulmasında bilimsel etik kurallarına uygun davrandığımı, kullandığım bütün kaynakları atıf yaparak belirttiğimi, maddi ve manevi desteği olan tüm kurum/kuruluş ve kişileri belirttiğimi, burada sunduğum veri ve bilgileri unvan almak amacıyla daha önce hiçbir şekilde kullanmadığımı beyan ederim.

24.06.2022

Rojbin TEKİN

ÖNSÖZ

Çalışmalarım yönlendiren, çalışma aşamasında desteklerini esirgemeyen ve beni motive eden danışman hocam sayın Dr.Ögr.Üyesi Orhan Yaman'a teşekkür ederim. Çalışmalarımın gerçekleşmesinde katkıları olan Fırat Üniversitesi Adli Bilişim Mühendisliği Anabilim Dalı öğretim üyelerine teşekkür ederim.

Ayrıca bu süreçte özverili bir şekil de yanımda olan ve maddi manevi desteklerini esirgemeyen aileme özellikle de annem Zinet Tekin'e teşekkür ederim.

Bu tez çalışması, Fırat Üniversitesi Bilimsel Araştırma Projeleri Koordinasyon Birimi (FÜBAP) tarafından **TEKF.21.18** protokol numaralı proje ile desteklenmiştir.

Rojbin TEKİN
ELAZIĞ, 2022

İÇİNDEKİLER

Sayfa

ÖZET

Nesnelerin İnterneti Uygulamaları için Saldırı Tespit Yöntemlerinin Geliştirilmesi

Rojbin TEKİN

Yüksek Lisans Tezi

FIRAT ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü

Adli Bilişim Mühendisliği Anabilim Dalı

Haziran 2022, Sayfa: xiv + 65

İnternettin gelişmesiyle birlikte IoT cihazları günümüzde birçok alanda kolaylık sağlamaktadır. Bu kolaylıklar insanların yaşam kalitesini arttırmaktadır. İnsanlar akıllı şehir, akıllı ev ve diğer akıllı platformları uzaktan izlemek ve yönetmek istemektir. Uzaktan izlenen ve yönetilen uygulamalar avantajlarının yanı sıra güvenlik sorunları gibi problemlere neden olmaktadır. IoT platformlarının artmasıyla birlikte saldırganların hedef noktası haline gelmiştir. Bu tür saldırıların tespit edilebilmesi ve güvenlik açıklarının önüne geçilmesi IoT teknolojisinin kullanım oranını daha da arttıracaktır. IoT kullanıcıları, saldırganların en çok tercih ettiği ağ saldırılarından dolayı mağdur olmaktadır. Bu mağduriyetin yanı sıra insanların kişisel verilerine erişim söz konusu olduğu için IoT platformlarındaki talebi olumsuz etkilemektedir.

Bu tez çalışmasında, DDoS, DoS ve Brute Force gibi saldırı türleri incelenmiş ve IoT saldırılarını tespit etmek için yöntemler geliştirilmiştir. Tez kapsamında iki temel katkı sunulmuştur. İlk olarak akıllı ev platformunu oluşturmak için Home Assistant teknolojisini kullanan bir laboratuvar kurulmuştur. Bu laboratuvar ortamında IoT cihazlarına Brute Force FTP, Brute Force SSH, DoS HTTP Flood, DoS ICMP Flood, DoS Syn Flood, Syn Scan ve UDP Scan, olmak üzere yedi saldırı gerçekleştirilmiştir. Toplanan veri setine XGBOOST algoritması uygulanarak saldırı türleri tespit edilmiştir. İkinci olarak, literatürde yaygın olarak kullanılan Bot-IoT veri setine Karar Ağacı algoritması uygulanmıştır. Tez kapsamında kullanılan veri setlerine diğer makine öğrenmesi yöntemleri uygulanarak sonuçlar karşılaştırılmıştır.

Anahtar Kelimeler: Nesnelerin İnterneti, Makine Öğrenmesi, Nesnelerin İnternetinde Güvenlik, IoT Katman Saldırıları, IoT Güvenliği

ABSTRACT

Development of Intrusion Detection Methods for Internet of Things Applications

Rojbin TEKİN

Master's Thesis

FIRAT UNIVERSITY
Graduate School of Natural and Applied Sciences

Department of Digital Forensic Engineering

June 2022, Pages: xiv + 65

With the development of the Internet, IoT devices provide convenience in many fields today. These conveniences increase people's quality of life. People want to remotely monitor and manage the smart city, smart home, and other smart platforms. Remotely monitored and managed applications cause problems such as security problems as well as their advantages. With the increase of IoT platforms, it has become the target point of attackers. Detecting such attacks and preventing security vulnerabilities will increase the rate of use of IoT technology. IoT users are suffered because of network attacks, which are the most preferred by attackers. Besides this suffering, it negatively affects the demand for IoT platforms, as there is access to people's data.

In this thesis, attack types such as DDoS, DoS, and Brute Force were examined and methods were developed to detect IoT attacks. Two main contributions were made within the scope of the thesis. First, a laboratory was established using Home Assistant technology to create the smart home platform. In this laboratory environment, seven attacks, namely Brute Force FTP, Brute Force SSH, DoS HTTP Flood, DoS ICMP Flood, DoS Syn Flood, Syn Scan, and UDP Scan, were carried out on IoT devices. Attack types were determined by applying the XGBOOST algorithm to the collected data set. Secondly, the Decision Tree algorithm was applied to the Bot-IoT dataset, which is widely used in the literature. The results were compared by applying other machine learning methods to the data sets used in the thesis.

Keywords: Internet of Things, Machine Learning, Internet of Things Security, IoT Layer Attacks, IoT Security

ŞEKİLLER LİSTESİ

Sayfa

TABLOLAR LİSTESİ

Sayfa

KISALTMALAR

AES	: Advanced Encryption Standard (Gelişmiş Şifreleme Standardı)
AI	: Artificial Intelligence (Yapay Zeka)
AMQP	: Advanced Message Queuing Protocol (Gelişmiş Mesaj Kuyruk Protokolü)
AP	: Access Point (Erişim Noktası)
ARP	: Address Resolution Protocol (Adres Çözümleme Protokolü)
ASF	: Anonymous Secure Framework (Anonim Güvenli Çerçeve)
BLE	: Bluetooth Low Energy (Bluetooth Düşük Enerji)
CAV	: Connected And Autonomous Vehicle (Bağlı Otonom Araç)
CNC	: Command and Control (Komuta ve Kontrol)
CoAP	: Constrained Application Protocol (Kısıtlı Uygulama Protokolü)
DDoS	: Distrubuted Denial of Service Attack (Dağıtık Hizmet Engelleme)
DDS	: Data Distribution Service (Veri Dağıtım Hizmeti)
DES	: Data Encryption Standard(Veri Şifreleme Standardı)
DL	: Deep Learning (Derin Öğrenme)
DNS	: Domain Name System (Alan Adı Sistemi)
DoS	: Denial of Service (Hizmet Reddi)
DRL	: Deeply Reinforced Learning (Derin Pekiştirmeli Öğrenme)
DTLS	: Datagram Transport Layer Security (Datagram Aktarım Katman Güvenliği)
FTP	: File Transfer Protocol (Dosya Transfer Protokolü)
IBM	: International Business Machines (Uluslararası İş Makineleri)
ICMP	: Internet Control Message Protocol (İnternet Kontrol Mesajı Protokolü)
ICS	: Industrial Control Systems (Endüstriyel Kontrol Sistemleri)
IETF	: Internet Engineering Task Force (İnternet Mühendisliği Görev Gücü)
IIoT	: Industrial Internet of Things (Endüstriyel Nesnelerin İnterneti)
IoT	: Internet of Things
IP	: Internet Protocol (İnternet Protokolü)
IPv4	: Internet Protocol Version 4 (İnternet Protokolü Versiyon 4)
IPv6	: Internet Protocol Version 6 (İnternet Protokolü Versiyon 6)
KNN	: K-Nearest Neighbor (K-En Yakın Komşuluk, K-NN)
LAN	: Local Area Network (Yerel Alan Ağları)
LPWAN	: Low Power Wide Area Network (Düşük Güçlü Geniş Alan Ağı)
LR	: Logistic Regression (Lojistik Regresyon)
LTE	: Long Term Evolution
MDMK	: Makine Öğrenme Tabanlı Algılama Çerçevesi
MDA	: Makine Öğrenime Tabanlı Algoritması
MDAE	: Makine Öğrenime Dayalı İyileştirme
MiTM	: Man in The Middle (Ortadaki Adam Saldırısı)
ML	: Machine Learning (Makine Öğrenmesi)
MQTT	: Message Queuing Telemetry Transport (Mesaj Kuyruk Telemetri Aktarımı)
M2M	: Machine to Machine (makineden makineye)
NFC	: Near Field Communication (Yakın Alan İletişimi)
PLC	: Programmable Logic Controller (Programlanabilir Mantıksal Denetleyici)
REST	: Representational state transfer (Temsili Durum Transferi)
RF	: Random Forest (Rastgele Orman)

RFID: : Radio Frequency Identification (Radyo Frekanslı Tanımlama)
RINA : Recursive Internetworking Architecture (Yinelemeli İnternet Çalışma Mimarisi)
RPL : Routing Protocol for Low-Power and Lossy Networks (Düşük Güçlü ve Kayıplı Ağlar için Yönlendirme Protokolü)
RTOS : Real Time Operating System (Gerçek Zamanlı İşletim Sistemi)
SASL : Simple Authentication and Security Layer (Basit Yetkilendirme ve Güvenlik Katmanı)
SNMP : Simple Network Management Protocol (Basit Ağ Yönetimi Protokolü)
SSL : Secure Sockets Layer (Güvenli Yuva Katmanı)
SVM : Support Vector Machines (Destek Vektör Makinesi)
TCP : Transmission Control Protocol
TLS : Transport Layer Security (Taşıma Katmanı Güvenliği)
UDP : User Datagram Protocol (Kullanıcı Datagram Protokolü)
YSA : Yapay Sinir Ağları
ZB : ZegaByte
WAN : Wide Area Network (Geniş Alan Ağları)

1. GİRİŞ

Bilgisayar ve ağ teknolojilerinde yaşanan gelişmeler ile günümüzde internet çok önemli bir noktaya gelmiştir. İnternettin günümüzde çok önemli noktaya gelmesi ile birlikte hayatımızın hemen hemen her alanında bize katkı sağlamaktadır (televizyon, bulaşık makinesi, akıllı ev sistemleri, ulaşım araçları, kameralar vs.). İnternete bağlı cihaz sayısındaki bu artış, Nesnelerin İnterneti (IoT) kavramının doğmasına sebep olmuştur.

Nesnelerin İnterneti, fiziksel nesnelerin birbiriyle bağlantılı olup günlük görevlerimizi iyileştirmek için hem fiziksel hem de dijital nesneleri entegre eder. Bununla beraber günümüzde gelişmekte olan internet ve internet ile bağlantılı olan cihazlar saldırganların hedef noktası haline gelmiştir.

Nesnelerin İnterneti (IoT) özellikli cihazlarda ve ortamda güvenlik, davetsiz misafirlerin veya kötü niyetli kullanıcıların, yeterli güvenlik önlemlerinin eksikliğinde IoT özellikli sistemleri tehlikeye atma kabiliyetleri nedeniyle önemli bir konudur [1]. Son birkaç yıldan beri IoT, IoT ağ anormalliği ve saldırı tespiti alanında büyük ilgi görmekte ve araştırmacılar bu sorunun üstesinden gelmek için çeşitli çalışmalar yapmaktadırlar [2].

Günümüzde 10-11 milyar cihazın internete bağlı olduğuna inanılmakta ve bu sayının 2022 yılına kadar 50 milyara çıkması beklenmektedir. Araştırmalara göre; dünyada kişi başına bağlı cihaz oranı 2003 yılında 0,08 iken, 2022 yılında bu oran yaklaşık 6,48d olarak tahmin edilmektedir. Ayrıca 20 ev cihazının 2022'de 2008'de üretilen tüm internet trafiğinden daha fazla web trafiği oluşturması beklenmektedir [3].

Ericsson raporuna göre [3], IoT bağlantıları, derin öğrenme gibi yapay zekâ (AI) algoritmaları kullanarak algılama verileri, analiz ederek akıllı olabilir 2026 IoT sistemleri tarafından 26,9 milyar ulaşacak [4] , [5] , derin pekiştirmeli öğrenme (DRL) [6] , vb. Örneğin, Amazon Alexa, insanların konuşmasını anlayabilir ve akıllı bir ev sisteminde akıllı bir yardımcı görevi gören bir yanıt verebilir [7].

1.1. Çalışmanın Amacı ve Konusu

Nesnelerin sürekli haberleşme halinde olması ve ağ bağlantılarının olması siber saldırılara olanak tanımaktadır [8] [9]. IoT güvenliğinde yeterli istihdam olmamasına rağmen işletmeler ekonomik nedenlerle ve büyük ölçekte bu IoT cihazlarını üretmeye devam ettikçe IoT'de gizlilik ve güvenlik yönetiminin önemi artmaktadır. Herhangi bir ihmalin olumsuz sonuçları olmaktadır [10]. Yüksek lisans çalışmasında, IoT sistemlerde meydana gelen ağ saldırılarının tespiti için makine öğrenmesi tabanlı yöntemlerin geliştirilmesi amaçlanmıştır.

1.2. Literatür Özeti

Literatürde IoT saldırılarının tespiti için makine öğrenmesi ve derin öğrenme tabanlı birçok yöntem geliştirilmiştir. Zhang ve diğ., IoT ağ ortamı üzerinden DDoS saldırısı için hafif bir savunma algoritması önerilmiş ve farklı ağ düğümleri arasındaki etkileşimli iletişimi incelemek için çeşitli senaryolara karşı test etmişlerdir [11].

Gupta ve diğ. [8], IoT bulunan zorluklardan, IoT ağındaki güvenlik ihtiyaçlarından ve IoT güvenliğinde devam eden araştırma ve zorlukları ele almışlardır. Ayrıca IoT için herhangi bir çözüm tasarlarken dikkate alınması gereken tasarım yönergelerini tartışmışlardır [8].

Kumar ve diğ. [9], çalışmasında önerilen çerçeve, verimli kimlik doğrulama ve anahtar anlaşması sağlar ve cihazların (kimlik ve veri) anonimliğini ve bağlantısının kesilmesini sağlar. Tek seferlik oturum anahtarı ilerlemesi, akıllı cihazlar için oturum anahtarını düzenli olarak yeniler ve ASF (Anonymous Secure Framework)'de ele geçirilmiş bir oturum anahtarı kullanma riskini azaltır. Güvenlik önemli ölçüde iyileştirilirken, önerilen çerçevenin hesaplama karmaşıklığının mevcut şemalara kıyasla düşük olduğu gösterilmiştir. Tek seferlik oturum anahtarı ilerlemesi, akıllı cihazlar için oturum anahtarını düzenli olarak yeniler ve ASF'de ele geçirilmiş bir oturum anahtarı kullanma riskini azaltır. Güvenlik önemli ölçüde iyileştirilirken, önerilen çerçevenin hesaplama karmaşıklığının mevcut şemalara kıyasla düşük olduğu gösterilmiştir. Tek seferlik oturum anahtarı ilerlemesi, akıllı cihazlar için oturum anahtarını düzenli olarak yeniler ve ASF'de ele geçirilmiş bir oturum anahtarı kullanma riskini azaltır. Güvenlik önemli ölçüde iyileştirilirken, önerilen çerçevenin hesaplama karmaşıklığının mevcut şemalara kıyasla düşük olduğu gösterilmiştir [9].

Mohammadi ve diğ. [4], IoT alanında analitiği ve öğrenmeyi kolaylaştırmak için derin öğrenme (DL) olarak bilinen gelişmiş makine öğrenimi tekniklerinin kullanımına ilişkin kapsamlı bir genel bakış sağlamışlardır. IoT verileri için iki ana iyileştirme belirleyerek başlanmıştır, yani IoT büyük veri analizi ve IoT akış veri analizi. IoT veri analitiği için ortaya çıkan DL tekniklerini kullanma potansiyeli daha sonra tartışılmıştır ve zorlukları sunulmuştur. Gelecekteki zorluklar ve potansiyel yönlere değinilmiştir [4].

Hussein ve diğ. [12], genel uygulamalar, özellikle gerçek zamanlı sistemler için kritik uygulamalar için bir IoT Platformu için tasarım ve uygulama önermişlerdir. Ayrıca, basit bir iletişim protokolü sunulmuş, çoklu konu özelliğini destekleyerek çok konulu mesajlaşma için gerekli olan trafiği ve gecikmeyi artıracak, önerilen RTOS protokolü için MQTT'ye karşı bir performans analizi gerçekleştirilmiştir. Analiz sonucu önerilen protokol, MQTT'den daha fazla ek konu için daha düşük bayt ekleyen çoklu konu özelliği nedeniyle MQTT protokolünden daha düşük gecikme ve trafik sağlamaktadır. [12].

Yavuz ve diğ. [13], derin öğrenme tabanlı güvenlik sistemi sunmuştur. Derin öğrenme de kullanılacak veri seti Cooja simülatörü ile hazırlamıştır. Çalışmada, Cooja IoT simülatörü, 1000

düğüme kadar değişen IoT ağlarında yüksek kaliteli saldırı verilerinin oluşturulması için kullanılmıştır. Eğitilen veri seti ile %99 kadar sonuç alınmıştır [13].

IoT ağlarda, ağ varlıklarının ağ ortamının belirsizliği altında ağ performansını en üst düzeye çıkarmak için yerel olarak kararlar alması gerekir. Luong ve diğ. [6], iletişim ve ağ iletişiminde Derin Pekiştirmeli Öğrenme (DRL) uygulamaları hakkında kapsamlı bir literatür taraması sunulmuş ve DRL eksikliklerin üstesinden gelmek için pekiştirmeli öğrenme ile derin öğrenme kombinasyonu geliştirmiştir [6].

Deniz yapmış olduğu tez çalışmasında, güvenlik yönetimi ihlallerine karşı alınması gereken temel önlemleri, daha önce yapılmış araştırmalardan yararlanılarak açıklamıştır. Ayrıca, üretici tarafından üretilen düğümlerin tek bir noktadan yönetilmesini sağlamak, mevcut IoT ağlarına yeni düğümler ekleme güvenliğini artırmak ve oluşabilecek güvenlik açıklarının kapatılmasına yardımcı olmak için yeni bir model önermiştir [10].

Irmak yapmış olduğu tez çalışmasında veri göndermek için bir IoT donanım bileşeni tasarlamış ve gerçek zamanlı veri toplama ve makine öğrenimi uygulamaları sağlayan bir yazılım geliştirmiştir. Kullanılan makine öğrenmesi algoritmaları incelenmiş ve başarı oranı ve işlem süresi açısından karşılaştırılmıştır. Destek vektör regresyonu ve yığın regresyonu dışında hesaplama süresinin çok hızlı olduğu gözlemlemiştir. Hava kalitesi indeksinin tahmin edilmesi için başarı kriterleri incelendiğinde, en iyi algoritmanın rastgele orman regresyonu olduğu hesaplamıştır [14].

Gürkan yapmış olduğu tez çalışmasında, IoT cihazlarda güvenli mesajlaşma için kullanılan DTLS ve CoAP protokolleri kullanan IoT cihazları için başarılı bir güvenlik uzantısı geliştirmiştir [15].

Yönem yapmış olduğu tez çalışmasında, sezgisel yöntemlerden, arıların yiyecek arama davranışlarını modelleyerek geliştirilen yapay arı kolonisi algoritması zaman serileri için başarılı sonuçlar üreten tekrarlayıcı sinir ağlarının eğitiminde kullanmıştır. Gerçekleştirilen model örnek bazı verilerinin analizinde kullanılmıştır. Bu çalışma ile yapay arı koloni algoritmasının nesnelerin interneti verilerinin analizinde etkin bir şekilde kullanılabileceği gösterilmiştir [16].

Arslan yapmış olduğu çalışmasında, akıllı cihazların buluta gönderdiği ve buluttan aldığı verilerin gerektiğinde aynı şekilde ulaşarak güvenli bir gönderme yeri bırakması sorununa odaklanmıştır. Bu anlamda gönderilecek veriler şifreleme modülü üzerinden gönderilerek şifreli olarak buluta gönderilerek depolanır. Aynı verinin şifrelenmiş versiyonunun şifresi, buluttan çekilerek çözülür ve kullanıcıların orijinal versiyona güvenli erişimini sağlar. AES, DES ve RSA algoritmalarını içeren şifreleme için bir uygulama geliştirilmiştir. IoT verilerini almak için bir simülatör tasarlanır ve yakalanan IoT verilerinden farklı boyutlar elde edilerek performans değerlendirilir [17].

Erhan yapmış olduğu tez çalışmasında, IoT sistem geliştiricilerine, ürünlerinin güvenlik risklerini ilgili güvenlik zafiyetleri kapsamında değerlendirebilmeleri için Secure IoT Design

Environment (Güvenli IoT Tasarım Ortamı), SIDE adlı bir ortam sunulmaktadır İlgili güvenlik açığının kapsamı tasarım aşaması. SIDE, tasarım kararlarıyla ilgili tehditleri tespit etmede ve bilinen güvenlik açıklarına dayalı alternatif çözümlerin güvenliğini değerlendirmede pratik ve kullanışlı olduğunu kanıtlamıştır [18].

Koroniotis ve diğ. [19], çalışmasında, meşru ve simüle edilmiş IoT ağ trafiğinin yanı sıra çeşitli saldırı türlerini birleştiren Bot-IoT adı verilen yeni bir veri kümesi önerilmiştir. BoT-IoT veri kümesinin güvenilirliğini, karşılaştırma ve diğer veri kümelerine kıyasla adli bilişim amaçlı farklı istatistiksel ve makine öğrenimi yöntemleri kullanılarak değerlendirilmiştir. Tam özellikli veri kümesinde eğitilmiş SVM modelinden en yüksek doğruluğu ve geri çağırmayı gözlemlenmiştir, en iyi 10 özellikli veri kümesi sürümünün SVM modelinden en yüksek hassasiyet ve en düşük düşüş göstermiştir [19].

Hasan ve diğ. [20], IoT sistemlerindeki saldırıları ve anormallikleri doğru bir şekilde tahmin etmek için birkaç makine öğrenimi modelinin performansları karşılaştırılmıştır. Burada kullanılan makine öğrenimi (ML) algoritmaları Lojistik Regresyon (LR), Destek Vektör Makinesi (SVM), Karar Ağacı (DT), Rastgele Orman (RF) ve Yapay Sinir Ağı'dır (YSA). Performans karşılaştırmasında kullanılan değerlendirme ölçütleri doğruluktur, Hassasiyet, geri çağırma, f1 puanı ve Alıcı Çalışma Karakteristik Eğrisi altındaki alan. Sistem Karar Ağacı, Rastgele Orman ve YSA için%99,4 test doğruluğu elde edilmiştir [20].

López ve diğ. [21] çalışmasında, cihazların karmaşıklığı ve hesaplama gücünden bağımsız olarak, çeşitli Nesnelerin İnterneti (IoT) kablosuz ağlarındaki tüm düğümlerin farklı iletişim katmanlarını etkileyebilecek sıkışma saldırılarının yayılmasını incelemek için salgın bir yaklaşımın kullanımını açıklamaktadır [21].

Alladi ve diğ [22]. çalışmasında, Endüstriyel Kontrol Sistemlerine (ICS'ler) yapılan büyük saldırıların örnek olay incelemelerini sunulmuştur. Bu saldırıların her biri için, kullanılan saldırı metodolojisini açıklanmış ve bu tür saldırıları önlemek için olası çözümler önerilmiştir [22].

Okegbile ve diğ. [1] IoT cihazlarda meydana gelen DDoS (Denial of Service) saldırıları ele alınarak model önermiştir. Bu model saldırganların sistemdeki davranışını karakterize etmektedir. Model güven listesi tablosu, kötü niyetli düğümlerin tespitini daha da iyileştirerek meydana gelecekte veya şu an gelen saldırılar için önlem oluşturmaktadır [1].

Hatalı özellik seçimi nedeniyle makine öğrenimi teknikleri, güvenli akıllı uygulamalar için akıllı IoT ağındaki bir dizi kötü amaçlı trafiği yanlış sınıflandırır. Bundan dolayı Shafiq ve diğ. çalışmasında, ilk olarak etkili özellik seçimi için bijective soft set uygulanmıştır ve ardından yeni bir CorrACC özellik seçim metrik yaklaşımı önerilmiştir. Önerilen yaklaşımları değerlendirmek için BoT-IoT veri setinde dört farklı ML sınıflandırıcı kullanılmış ve algoritma ile elde edilen deneysel sonuçlar ve%95'in üzerinde doğruluk saylamamıştır [2].

Genetik programlamanın temel kavramlarını kullanan Qureshi ve diğ., RPL tabanlı IoT ve IIoT (Industrial internet of things) ağlarında güvenlik tehditlerinin varlığını tespit etmek için yeni ve güvenli bir çerçeve önermektedir. Önerilen çerçeve, HELLO-Flood saldırısı, Sürüm numarası saldırısı, Sinkhole saldırısı ve Kara delik saldırısını tespit etme yeteneğine sahiptir. Önerilen çerçevenin performansı, saldırı algılama doğruluğu, gerçek pozitif oran, yanlış pozitif oranı, iş hacmi ve uçtan uca gecikme dahil olmak üzere çeşitli performans parametrelerinde değerlendirilir. Olumlu sonuçlar önerilen çerçeveyi destekliyor gibi görünmektedir ve onu RPL tabanlı IIoT ortamları için en iyi seçim haline getirmektedir [23].

Shafiq ve diğ. [24], IoT cihazlarda meydana gelen saldırıları tespit etmek için en etkili makine öğrenmesi modelinin nasıl seçilmesi gerektiği üzerine bir model geliştirilmiştir. Modelde hangi ML (Makine Öğrenmesi) algoritmasının etkili olduğunu ve IoT anormalliği ve izinsiz giriş trafiği tanımlamasını seçmek için kullanılması gerektiğini bulmak için, önyargılı bir yazılım küme yaklaşımı ve algoritması uygulanmıştır [24].

Li ve diğ., gelecekteki nesnelerin internetini üç aşamada inceleyip belirtilen konu başlıkları ("Elektrikli cihazlarla nesnelerin interneti", "Her cihazla nesnelerin interneti" ve "Yapay Zekâ Nesnelerin İnterneti") hakkında öneriler sunulmuştur [25].

Kök yapmış olduğu tez çalışmasında IoT'nin veri ve mimari zorluklarını gidermek için derin öğrenmeye (Deep Learning / DL) dayalı çözümler geliştirilmiştir. IoT verilerinin gelecek değerlerini tahmin eden ikili DL (Deep Learning) değeri önerilmiştir. Önerilen DL modelleri kullanılarak özgün bir hava kalitesi tahmin sistemi geliştirilmiştir. Deneysel sonuçlar, geliştirilen hava kalitesi tahmin sisteminin gelecekteki hava kalitesi seviyelerini %94,9 başarı oranıyla tahmin ettiğini göstermiştir [26].

IoT cihazlarındaki saldırı modelleri bu makalede açıklanmıştır. Bazı modeller kural kümeleri tarafından tespit edilebilirken diğerleri yapay sinir ağı yaklaşımıyla analiz edilmeyebilir ve bu nedenle analiz edilebilir: IoT paket dizisi kalıpları eğitilir ve potansiyel olarak saldırıya açık paketler tanımlanmıştır. Yoon makale çalışmasındaki katkısı; IoT saldırılarının karakterizasyonu, IoT saldırı modellerini eğitmek için sinir ağı düğümlerinin oluşturulması ve gerçek zamanlı ağ akışı verilerini analiz etmek için eğitilmiş modellerin yerleştirilmesidir. IoT paket dizisi modelleri eğitilip ve potansiyel olarak saldırıya açık paketler tanımlanmıştır [27].

Zhang ve diğ. [28] çalışmasında, tam işlevli bir Mirai botnet ağ mimarisi kurularak ve Mirai botnet sunucusunda kapsamlı bir adli analiz gerçekleştirilmiştir. Saldırganın terminalinde, komuta ve kontrol (CNC) sunucusunda, veritabanı sunucusunda, tarayıcı alıcısında ve yükleyicisinde ve bunlardan gelen ağ paketlerinde kalan yapılar adli bilişim açısından incelenmiştir. Saldırganın bu saldırılardan bazılarını uzaktan nasıl elde edebileceği tartışılmış ve botnet sunucusuna doğrudan fiziksel erişim olmadan erişebileceği tespit edilmiştir [28].

Rizvi ve diğ. [29] çalışmada, IoT (Nesnelerin İnterneti) cihazlarını kullanan ağlar için bir saldırı yüzeyi tanımlanmış ve bir tehdit modeli önermişlerdir. Önerilen model olası riskleri azaltmak için güvenlik çözümleri sistematik olarak analiz edilmiştir. Önerilen model, ağ güvenliği uzmanlarının yeni IoT cihazlarını uygulama risklerini tahmin etmeleri için bir yöntem sağlamış ve olası çözümleri belirlemek için bir araç sağlanmıştır [29].

Zhang ve diğ. [7], gelecekte yapay zekâ destekli IoT'ler için hesaplama ve veri iletimi açısından dinamik bir ortamda güvenlik destekleri ile iş birliğine dayalı bilgi işlem sağlamıştır. Donanım asistanı için güvenilir yürütme ortamı teknolojisi ile geliştirilmiş güvenilir bir iş birliği çerçevesi önerilmiş ve uygulanmıştır. Deney sonuçları, çerçevesini düşük ek yük ile esnek ve dinamik iş birliği sağladığı gösterilmiştir. CAV (Connected And Autonomous Vehicle)'lerdeki iş birliğinin vaka çalışması, çerçevenin gelecekteki AI (Artificial Intelligence) destekli IoT'ler için iş birliğine dayalı yapay zekayı etkili bir şekilde destekleyebileceğini göstermektedir [7].

Choi ve diğ. [30], akıllı ev-Nesnelerin İnterneti alanındaki araştırma makalelerini analiz etmek için, önemli uluslararası konferanslarda sunulan ve saygın dergilerde yayınlanan makaleleri çıkararak bir bibliyometrik yaklaşım izlemişlerdir. Burada sunulan bulgular, akıllı ev-Nesnelerin İnternet'inin gelecekteki yönleri için önemli bilgiler sunar ve öğrenme noktalarına vurgu yapar. Dahası, akıllı ev-Nesnelerin İnterneti'nin hem temel eğilimleri hem de bilgi alanları sunulmuştur [30].

Srinadh ve diğ. [31], IoT uygulamalarındaki güvenlik tehditlerine ve tehdit kaynaklarına kapsamlı bir genel bakış sunmuştur. Ek olarak, IoT güvenliği araştırmasının mevcut durumu ve IoT güvenliği ve gizliliği ile ilgili gelecekteki araştırma bilgileri burada ele alınmıştır [31].

Niraja ve diğ. [32] çalışmasında, Gelişmiş Yapay Zekâ (AI) tabanlı Siber Saldırı Algılama (AAI-CAD) olarak bilinen hibrit bir algoritma tasarlamıştır. Derin otomatik kodlayıcı ve özellik çıkarma entegrasyonuna dayanır. Deneysel sonuçlar, önerilen algoritmanın IoT kullanım durumlarında siber saldırıların neredeyse gerçek zamanlı olarak tespit edilmesinde etkili olduğunu ortaya koyulmuştur [32].

Snehi ve diğ. [33] makalede, yazılımla tanımlanmış Siber-Fiziksel Sistemin mimari ayrıntılarını anlatılmakta ve bir dizi güvenlik açığının üstesinden gelmek için mimari katmanlardan biri olarak Sis Hesaplamanın birleştirilmesini önermiştir. Sis, performans iyileştirme ve bulut adına devredilen görevleri yürütme için algı ve bulut arasında bir katman olarak önerilmiştir. DDoS / IoT-DDoS algılama ve azaltma alanında önerilen çözümler incelenip temel oluşturabilecek güvenlik açığı analizi özetlemeye çalışılmıştır [33].

Lawal ve diğ. [34] çalışmasında, hızlı ve doğru saldırı algılamasını sağlamak için sis hesaplama kullanan IoT için bir DDoS azaltma çerçevesi önermiştir. Sis, azaltma çerçevesinin etkili bir şekilde yerleştirilmesi için kaynaklar sağlar, bu, kısıtlı kaynak IoT cihazlarının kaynaklarındaki açıkları çözer. Azaltma çerçevesi, anormallik tabanlı bir saldırı algılama yöntemi ve bir veri tabanı

kullanılmıştır. Veri tabanı, önceden tespit edilen saldırıların imzalarını saklarken, anormallik tabanlı tespit şeması, DDoS saldırılarını tespit etmek için K-NN sınıflandırma algoritması kullanır. K-NN sınıflandırma algoritmasının DDoS saldırılarının tespiti için %99 oranında doğruluk sağladığı sonucuna varılmıştır [34].

Yang ve diğ. [35] çalışmasında, kötü niyetli düğümlerin yalnızca belirli komşulara gönderilen paketlere saldırdığı, seçici uçlu paket saldırısı adı verilen gelişmiş bir saldırı tanıtılmıştır. Seçici saldırı paketleri nedeniyle, saldırı, geleneksel paket saldırısından daha gizlidir ve bu da mevcut algılama algoritmalarının tespit edilmesini zorlaştırır. Seçici uçlu paket saldırısını tespit etmek için, iletişim bağlantılarının ve düğümlerinin itibarını değerlendirmek için regresyon algoritması ve kümeleme algoritmasını kullanan ve buna göre kötü amaçlı düğümleri tespit eden çerçeveye dayalı makine öğrenimi tabanlı algılama çerçevesi (MDMK) ve makine öğrenimi tabanlı algılama algoritması (MDA) önerilmiştir. Algılama performansını daha da iyileştirmek için, yönlendirme yolunu optimize edilerek makine öğrenimine dayalı iyileştirme (MDAE) tabanlı algılama algoritması tasarlanmıştır. Deneysel sonuçlar, mevcut algılama algoritmaları ile karşılaştırıldığında, farklı durumlarda MDA ve MDAE'nin doğruluğunun yaklaşık olarak %7-%30 oranında arttığı sonucuna varılmıştır [35].

Samyuel ve diğ. [36] çalışmada, ağ yığınındaki tüm ağ kusurlarını ele alan güvenli bir ağ mimarisi sağlanmak amaçlamıştır. Birkaç yıldan beri araştırmacılar tarafından RINA (Recursive Internetworking Architecture) mimarisi geliştirilmiştir. Ancak bu çalışma için yeni bir yöntem geliştirilmiştir. Önerilen yöntem, LAN (Local Area Network) gibi kapalı ortamda RINA mimarisi ile geliştirilmiş. RINA'nın geleneksel ağ mimarisine göre ağ akışı saldırıları riskini etkili bir şekilde azaltabileceği sonucuna varılmıştır [36].

Ahmed ve diğ. [37], yakın zamandaki zaman korumasına ilişkin farkındalığı artırmayı ve nesnelerin interneti sistemlerinin mevcut korumasındaki boşlukları son kısıtlamalarla doldurmayı amaçlamıştır [37]. Ullah ve diğ. [38] çalışmada, IoT ağları için anormallik tabanlı yeni bir saldırı tespit modeli tasarlamıştır. Saldırı tespit modeli 1B, 2B ve 3B olarak evrişimli sinir ağları kullanılarak uygulama mantığına göre hazırlanmıştır. Evrişimli sinir ağı modeli için BoT-IoT, IoT Network Instrusion, MQTT-IoT-IDS2020 ve IoT-23 saldırı tespit veri kümeleri kullanarak doğrulamıştır [38].

Shen ve diğ. çalışmada, IoT sistemlerde zararlı yazılım yayılımı kullanıcıların sistemine ciddi bir şekilde zarar vermektedir. Sorunun çözümü için sinyal oyununa dayalı optimal IoT zararlı yazılım yayma stratejisi tahmin etmiştir. Daha sonra, IoT kötü amaçlı yazılım yayılımını pratikte yansıtacak ve IoT sistem düğümlerinin kötü amaçlı yazılımdan başarıyla etkilenme olasılığını makul bir şekilde ifade edecek olan sinyalleşme IoT kullanılabilirlik değerlendirme oyununun çözümünü elde etmek için bir algoritma geliştirmiştir [39].

Chaudhary ve diğ. [40] çalışmasında, akıllı IoT sisteminde bulunan gömülü cihazları XSS saldırılarına karşı korumaya yönelik yaklaşımlar geliştirmiştir. Bu yaklaşımlar enjekte edilen dizileri kara listeye almak için saldırı vektörleri ile karşılaştırarak tanımlama yapar ve filtreleme yöntemini optimize bir şekilde uygulayarak zararlı etkilerini azaltır. İki IoT cihaz da saldırı sömürüleri gerçekleştirilip test edilmiştir. Deneysel sonuçlar, her iki test edilen platformda da 0,9 ve üzeri bir doğruluk elde edilmiştir [40]. Vu ve diğ. [41] birden fazla IoT cihazdan toplanan ve etiketlenmemiş verilerden öğrenmeye izin veren derin transfer öğrenme yöntemi önerilmiştir. Deneysel sonuçlar, önerilen DTL modelinin IoT saldırılarını tespit etme doğruluğunu yüksek bir oranda geliştirdiğini göstermektedir [41].

Stellios ve diğ [42]. Çalışmasında 2010 yılından beri tüm uygulama alanlarında bulunan IoT özellikli siber saldırları araştırmıştır. Kritik altyapılarda ve hizmetlerde gerçekleştirilen saldırılar ve bu saldırılar sonucu alınması gereken önlemleri incelemiştir [42]. Yeni geliştirilen IoT saldırılarına uyum sağlayabilmek için, saldırı modelini otomatik olarak öğrenebilen ve tanıyabilen öğrenme tabanlı saldırı algılama modeli geliştirilmiştir. Bu modelle IoT saldırılarını daha az insan müdahalesi ile algılamaya olanak sağlanmıştır. Gerçek bir IoT saldırı veri seti üzerinde kapsamlı deneyler yapılmıştır ve IoT saldırı tespit etkinliği anlatılmıştır [42].

Andy ve diğ. [43] çalışmasında, yeterli güvenlik mekanizmasını uygulamayan IoT sistemlerin olmasının nedenlerini tartışmaktadır. Ayrıca saldırı senaryoları kullanılarak MQTT protokolünde nasıl saldırılacağını gösterilip analiz edilmiştir. Analiz sonucunda MQTT protokolü için güvenlik farkındalığı anlatılmıştır [43].

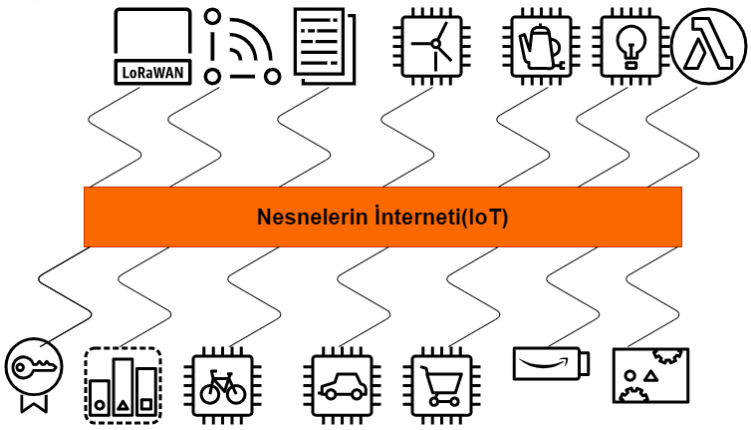
Arthi ve diğ. [44] çalışmasında mevcut veri kümelerinin IoT etkisi incelemiştir ardından IoT'deki DNS yükseltme saldırıları için gerçek zamanlı bir veri toplama çerçevesi ve DDoS saldırısı gerçekleştiren paketleri yansıtma yoluyla yakalamak hedeflemiştir [44].

2. NESNELERİN İNTERNETİ

Bu bölüm Nesnelerin İnternetinin tarihsel gelişimi, kullanım alanları, bileşenleri ve teknolojileri, bileşenleri protokolleri ve uygulama alanlarından oluşmaktadır.

2.1. Tarihsel Gelişim

İlk IoT cihazı olarak kabul edilen John Romkey, Ekim ‘89 INTEROP konferansı için internet üzerinden açılıp kapatılabilen bir ekmek kızartma makinesi geliştirmiştir. Interop Başkanı Dan Lynch, Romkey’e, Romkey’in "internette ekmek kızartma makinesini kaldırması" halinde, cihaza konferanstaki tüm kattaki katılımcılara yıldız yerleştirme verileceğine söz verdi. Ekmek kızartma makinesi, TCP/IP ağına sahip bir bilgisayara bağlandı. Daha sonra gücü açmak için bir bilgi tabanı (SNMP MIB) kullandı [45]. 1989 John Romkey yaptığı ekmek kızartması aslında bir IoT cihazıydı ama henüz IoT olarak adlandırılmamıştı. Daha sonrasın da 1999’da IoT kavramı ilk olarak bir Radyo Frekansı Tanımlama (RFID) üyesi tarafından önerildi [31]. Önerilmesinin ardından IoT kavramı gelişen teknolojilere ayak uydurarak bugün evimize ve elimizin altına kadar geldi. Artık bulunduğumuz her nokta da kullandığımız her cihazda IoT bulunmaktadır. Şekil 2.1’de günümüzde gelişen IoT teknolojisi görsel olarak sunulmuştur.



Şekil 2.1. IoT kullanımı

2.2. IoT Kullanım Alanları

Çeşitli IoT uygulamaları, farklı görevleri otomatikleştirmeye odaklanır ve cansız fiziksel nesnelerin herhangi bir insan müdahalesi olmadan hareket etmesini sağlamaya çalışır [46]. IoT uygulamalarına örnek verecek olursak günümüzde pek çok alana yayılmıştır; akıllı şehirler, akıllı çevre, akıllı ölçüm ve akıllı şebekeler, güvenlik ve acil durumlar, akıllı perakende, akıllı tasarım ve hayvan çiftliği, ev otomasyonu. Kullandığımız bu teknoloji her yerde yayılmaktadır. Gartner

tarafından hazırlanan bir rapor, gelecekte tüm teknolojilerdeki bağlantılı cihazların 20,6 milyar adede ulaşacağını belirtmiştir. Bağlı Cihazlar, yaşamın, toplumun, endüstrilerin ve iş dünyasının yaşam kalitesini, üretkenliğini ve yaşamı daha çok kolaylaştırdığı için fiziksel ve dijital dünya arasındaki boşluğu doldurur.

2.3. IoT Bileşenleri ve Teknolojileri

Nesne bileşenleri, fiziksel olarak birbirine ve İnternete bağlı cihazlardan oluşur. İnsan bileşeni, IoT ile aktif bir bağlantı sağlayan bileşendir. Veri kısmı, nesneler ve insanlar tarafından üretilen bilgilerden oluşur. Elde edilen bu veriler analiz edilerek bilgi olarak kullanılabilir veya insanlara veya makinelere iletilebilir. Bu sayede daha verimli kararlar alınabilir ve daha iyi sonuçlar alınabilir. Proses bileşenleri, diğer bileşenler arasındaki etkileşimleri gösterir ve doğru zamanda doğru kişilere veya ekipmana erişim sağlar [47].

2.3.1. Nesne Bileşeni

IoT uygulamalar tasarımcının barındırmak istediği her tür nesneyi içerir. IoT uygulamalar da bulunan bu nesneler haberleşmeyi sağlamak için gömülü sistemleri kullanırlar. Nesne bileşeni, internete ve birbirine bağlanmak için ağ üzerinden iletişime geçen nesneleri ifade eder. Önemli olan nesne bileşenleri şu şekildedir:

Sensörler

Nesneden farklı verileri alınmasını sağlayan cihazlardır. Işık, ısı, hareket, nem, basınç gibi birçok çevresel faktörden elde edebildiği bilgiyi verileri ekran veya ağ üzerinden başka bir yapıya ileten bileşenlerdir.

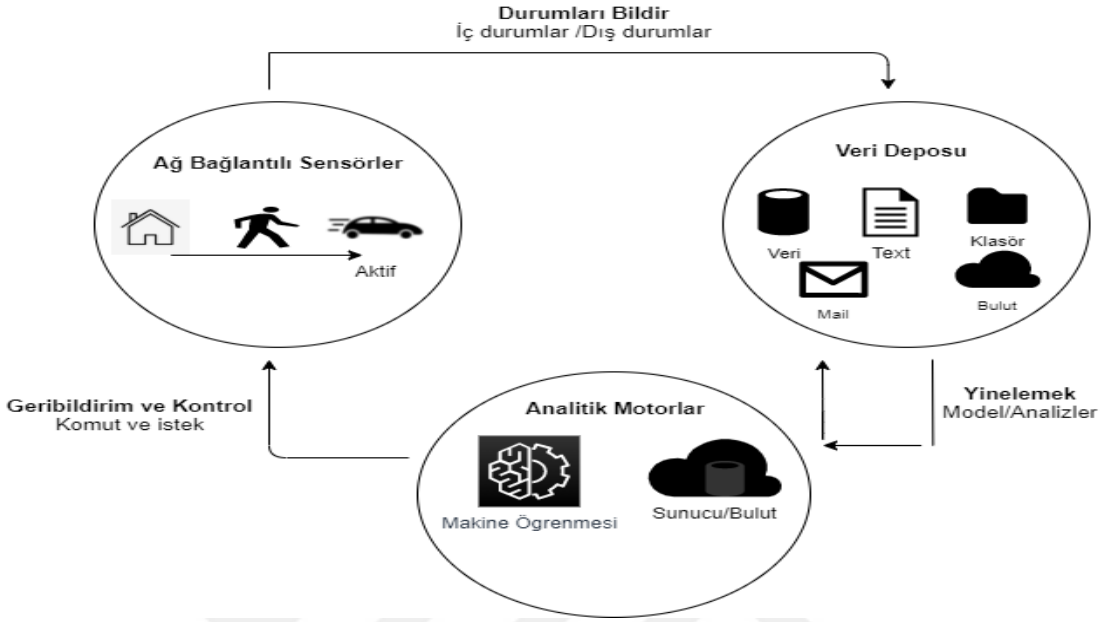
Kontrolörler

Sensörler, ortamdan alınan ölçümleri sinyallere dönüştürür ve toplanan bu verileri kontrolör adı verilen ana cihaza gönderir. Kontrolörler, topladıkları verileri buluttaki herhangi bir cihaza/aktivatöre gönderebilir. Kontrolörün görevi, sensörlerden veri toplamak ve bir internet bağlantısı sağlamaktır [47].

2.3.2. Veri Bileşeni

Veriler toplandıktan ve buluta ulaştığında, yazılım toplanan veriler üzerinde işlem yapar. Ancak veriler bazen tek başlarına bir anlam ifade etmeyebilirler. Veri yorumlandığında, ilişkilendirildiğinde, üzerinde işlem yapıldığında veya karşılaştırıldığında veri daha çok anlam

kazanır. Anlamlandırılan veri, bilgi haline dönüşür [47]. Veri işleme modeli Şekil 2.2'de sunulmuştur.



Şekil 2.2. Veri işleme modeli

2.3.3. Ağ Bileşeni

Sensör ve başka algılayıcılar ile elde edilen veriler, bellekte tutulurken aynı zamanda nesneler arasındaki başka ağlar arasında veriler taşınır.

2.3.4. Bulut Bileşeni

Sensörler aracılığıyla toplanan veriler çok büyüt boyutlarda ulaşmaktadır. Bu büyüklükte veriler depolamak için bulut teknolojisi kullanılmaktadır.

2.3.5. Analiz Bileşeni

Cihazların ve sensörlerin analog verileri gerçek zamanlı olarak dijital verilere dönüştürülür. Analiz, sistem veya cihazların çalışma anında meydana gelebilecek sorunların önceden belirlenmesini ve meydana gelebilecek problemlerin önüne geçilmesidir.

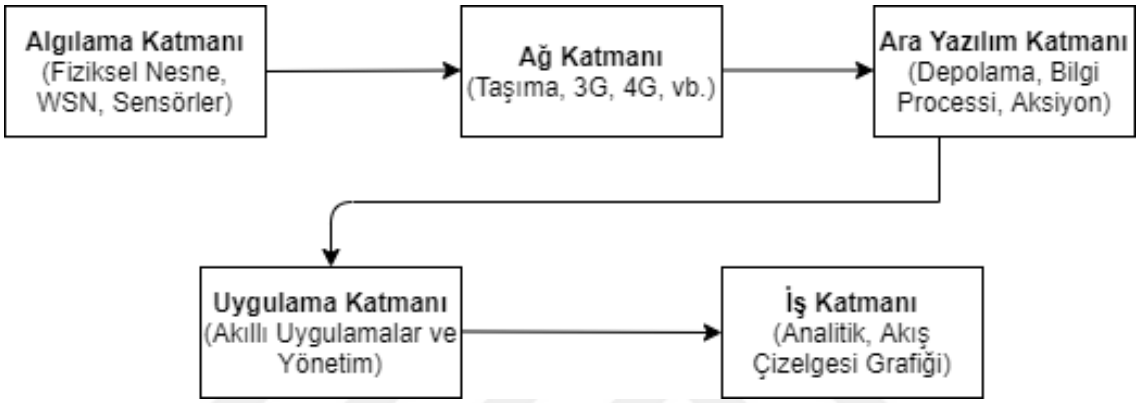
2.3.6. Kullanıcı Bileşeni

İnsanların ve cihazların erişemediği büyük miktarda veri tek başına anlamsızdır. Doğru kararlar alabilmek ve doğru aksiyonları alabilmek için bu verilerin insanların kullanabileceği

faydalı bilgilere dönüştürülmesi gerekmektedir [47]. Nesne ile aramızdaki ilişkiyi kontrol edebilecek bir uygulama (web sitesi, buton, arayüz vb.) geliştirilerek son kullanıcıya sunulur.

2.4. IoT Bileşenleri Protokolleri

IoT'nin katmanları dünyadaki her IoT sisteminin temellerini tanımlar. Birçok ileri teknolojiler ve büyük uygulama alanlarının çalışmalarına göre, 5 katmanlı mimari kabul edilir. Şekil 2.3'te beş katmanlı mimari gösterilmiştir.



Şekil 2.3. IoT katman mimarisi

2.4.1. Algılama Katmanı

Algılama katmanı IoT mimarisinin ilk katmanıdır. Bu katman analog sinyalleri dijital forma veya tam tersine dönüştürür. Bu katmanın ana işlevi, çerçeveden bilgi alarak başka katmana verileri iletmektir.

2.4.2. Ağ Katmanı

Bu katman algılama katmanından veri alır verileri ağ oluşturma teknolojileri kullanarak ara katmana iletir. Bu katmandaki iletişimler iki türlü gerçekleşir. İlk olarak TCP veya UDP/IP, ikinci olarak ağ geçitleri LAN (Local Area Network) ve WAN (Wide Area Network) bağlantıları arasında çalışır. Bu katmanda kullanılan protokoller Tablo 2.1'de verilmiştir.

Tablo 2.1. Ağ katman protokolleri

Ethernet	Bluetooth
NFC	LPWAN
ZigBee	Hücresel Ağlar
DDS	AMQP
COAP	MQTT

2.4.3. Ara Yazılım Katmanı

Ara yazılım katmanı, diğer iki katmandan gelen tüm veri setini depolar ve cihaz ad ve adresine uygun verileri verir. Bu sayede kullanılan uygulamalarda veri dağıtım aşamasında herhangi bir karışıklık yaşanmamaktadır.

2.4.4. Uygulama Katmanı

Uygulama katmanı tüm sürecini ara katman katmanından gelen verilere göre yönetir. Bu uygulama klima açmayı, güvenlik sistemlerini devreye almayı, cihazın hangi anda durup hangi anda çalışacağı gibi işlemler yönetilir.

2.4.5. İş Katmanı

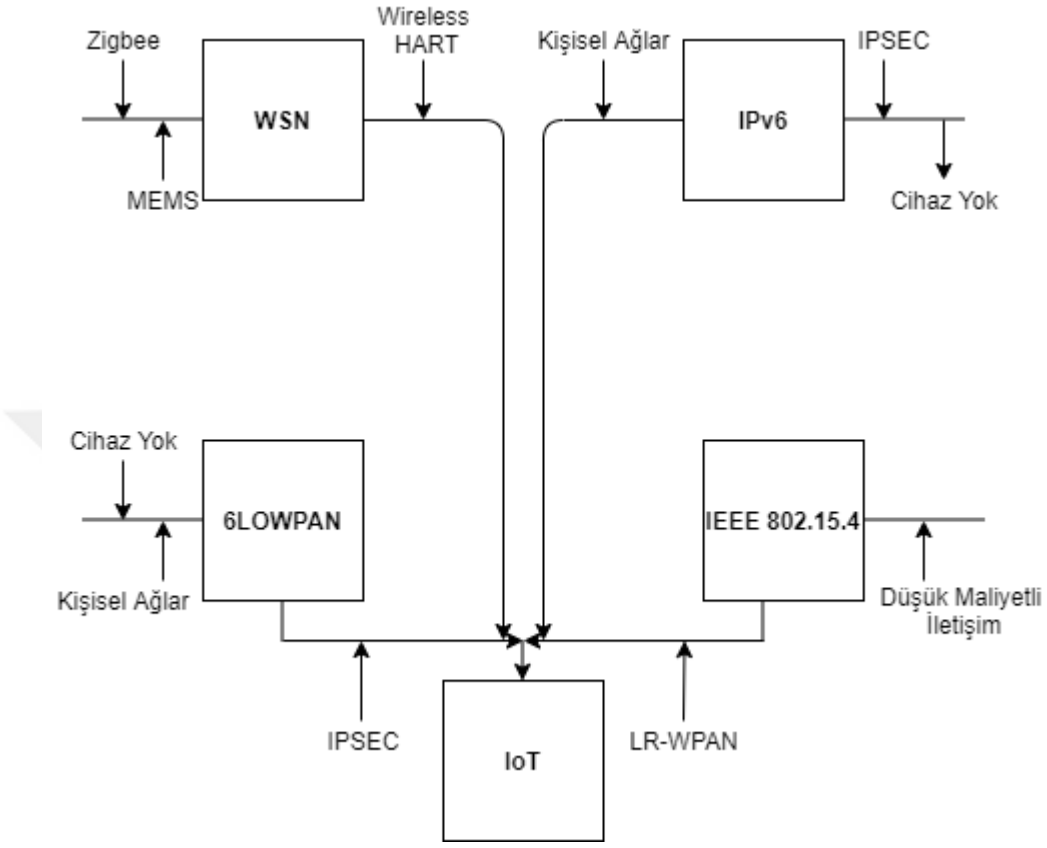
Bu katmanda IoT verileri toplanarak iş planlaması ve stratejileri için kullanılmaktadır. Uygulama tasarımcıları geleceği planlamak için geçmiş ve mevcut verilerden faydalanırlar.

2.5. IoT Teknolojileri Protokolleri

IoT sistemlerinde, kullanılan protokoller tüm sistemi etkileyebilecek güvenlik açıklarına [1] sahip olabilir. IoT cihazları, temel güvenlik protokollerinden yoksun olmaları nedeniyle siber suçlular ve saldırganlar için savunmasız hedeflerdir. Bu, kuruluşlara karşı DDoS başlatmak için kullanılan botnetler tarafından saldırıya uğrayabilecekleri ve saldırıya uğrayabilecekleri anlamına gelir [48].

Her defasında gönderilecek veri boyutu, enerji tüketimi, veriyi üretecek ve gönderecek cihazın sınırlı olması, veri güvenliği, kullanılacak bağlantı türüne bağlı olarak bant genişliği, verinin iletilemediği durumlardaki tepkiler vb. birçok etmenin veri iletiminde göz önünde bulundurulması gerekmektedir. Bu etmenlere bağlı olarak farklı kullanım senaryolarına sahip farklı haberleşme modelleri ve protokolleri oluşturulmuştur [49].

Bu bölümde protokollerin genel tanımları yer almaktadır. IoT protokollerinin arka planda haberleşme mantığı Şekil 2.4 de gösterilmiştir.

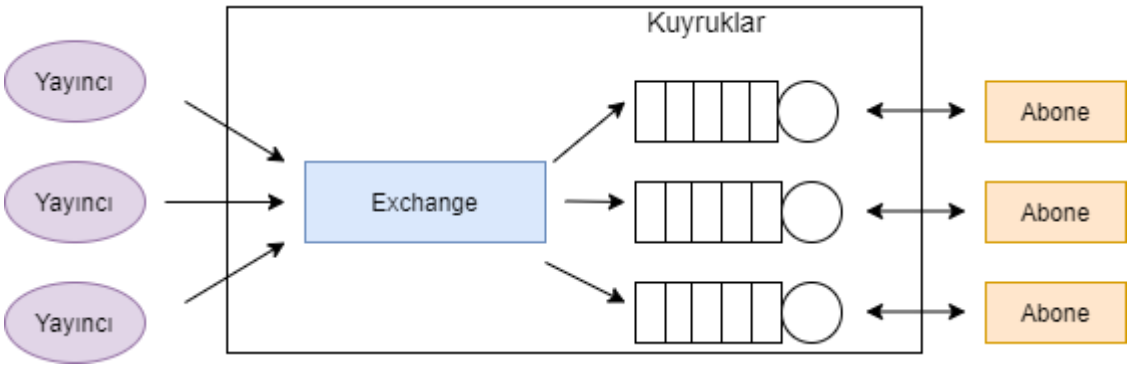


Şekil 2.4. Protokollerin arka planda çalışma mantığı [50]

2.5.1. AMQP

AMQP (Gelişmiş İleti Sıraya Alma Protokolü), açık standart uygulama protokolüdür [49]. Mesajlaşma ara yazılımları arasında çalışan uygulama katmanı protokoldür AMQP protokolü Şekil 2.5'te gösterilmiştir. AMQP, uygulamaların anlık mesajlaşma veya mail uygulamaları gibi birbirlerine mesaj göndermesi ya da almasını sağlar. AMQP mesajların nasıl iletileceği ve bu iletim aşamasında kullanılan güvenlik, tutarlılık ve performans alanlarında çeşitli tercihler sunmasıyla diğer IoT protokollerinden farklılaşır [51].

AMQP varsayılan haberleşme kanalı olarak TCP'yi, güvenlik için ise SSL/TLS ve SASL kullanır. SASL (Simple Authentication and Security Layer) basit yetkilendirme ve güvenlik katmanı anlamına gelir ve istemci veya sunucuların bir kullanıcı adı/parola ya da bir sertifika ile yetkilendirilmesine olanak sağlar. SSL/TLS ise mesaj yükünü şifrelemek için kullanılır [52].

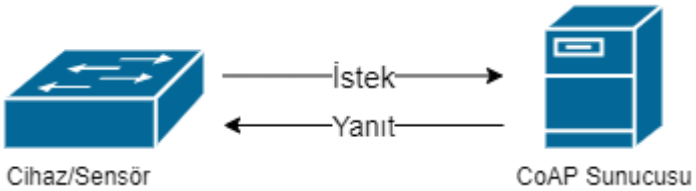


Şekil 2.5. AMQP protokolü

2.5.2. CoAP

CoAP (Kısıtlı Uygulama Protokolü), kısıtlı düğümler ve kısıtlı ağlarla kullanılan web aktarım protokolüdür. Protokol M2M(makineden makineye) uygulamalar için tasarlanmıştır. REST (Respresentational State Transfer) modeline dayanır. CoAP hem cihazlarda hem de ağda kaynak kullanımını daha aza indirmek için tasarlanmıştır. CoAP, 10 KİB RAM ve 100KİB kod alanı ile mikro denetleyicilerle çalışmak için tasarlanmıştır. IP üzerinden UDP ile çalışır. CoAP protokolü haberleşme modülü Şekil 2.6'da verilmiştir.

CoAP, IETF (İnternet Mühendisliği Görev Gücü) tarafından tasarlanmış bir uygulama katmanı protokolüdür [49].



Şekil 2.6. CoAP haberleşme modülü

2.5.3. DDS

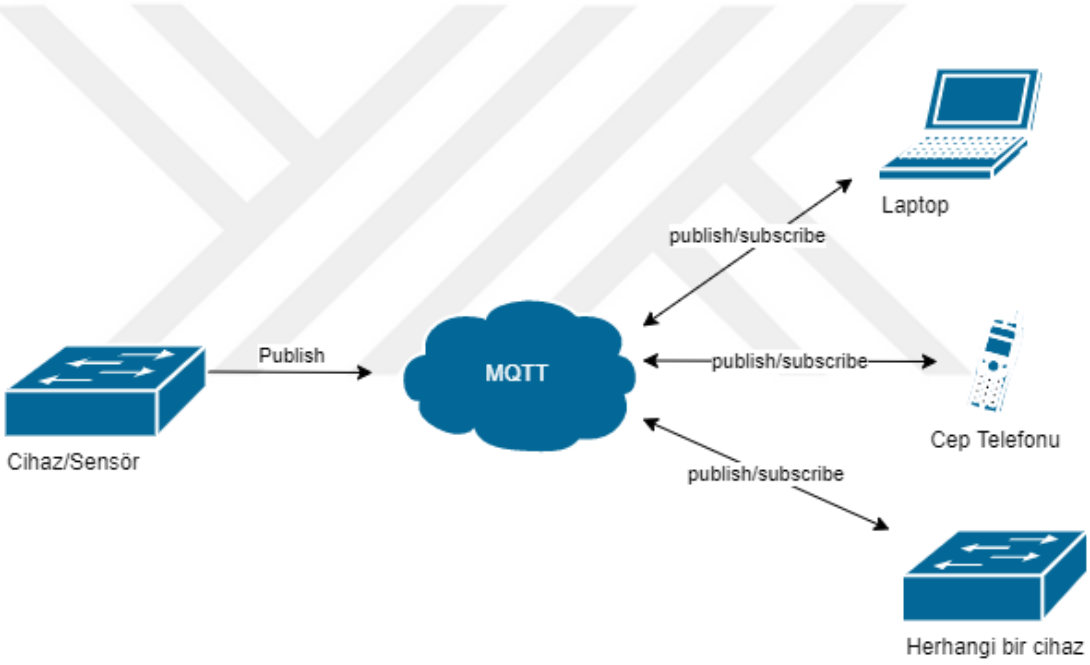
DDS (Veri Dağıtım Hizmeti), ara katmanı dağıtık ortamda çalışan gerçek zamanlı sistemlerde veri iletimi için kullanılır. Savunma, havacılık endüstriyel nesnelerin interneti, sağlık ve otomotiv alanlarında kullanılmaktadır. UDP tabanlı bir protokol kullanmaktadır. DDS ara katmanı mimari olarak yayımla-abone ol tasarım kalıbını temel almaktadır.

Yayımla abone-ol mimarisi veriyi sağlayan uygulama ile veriye erişen uygulamanın birbirinden bağımsız hale gelmesini sağlamaktadır. Veriyi oluşturan bileşen veriyi ara katman üzerinden yayımlar. Veriyi yayımlayan bileşenin veriyi kime iletmesi gerektiğini bilmesi gerekmemektedir. Ara katman veriyi bu veriye abone olan diğer bileşenlere iletmekten sorumludur [53].

2.5.4. MQTT

MQTT (Message Queue Telemetry Transport-Mesaj Sırası Telemetri Aktarımı), makineden makiye(M2M) iletişim için tasarlanmış ve uzak noktalardaki düşük bant genişliğine sahip bağlantılarda kullanılan protokoldür. Verimli bant genişliği gerektiren cihazlar için kullanılır ve yayınlama abone-olma modelini kullanmaktadır.

MQTT protokolü 1999 yılında IBM ve Arcom (Eurotech) tarafından tanıtılmasına karşın 2013'te OASIS tarafından standartlaştırılmış ve 2016 yılında ISO tarafından ISO/IEC 20922:2016 olarak onaylanmış bir IoT haberleşme protokolüdür. MQTT protokolü, IoT cihazların bulut (internet) ile bağlantılarını sağlamak üzere TCP/IP protokolü kullanmaktadır. MQTT haberleşmesi TCP protokolünün üçlü el sıkışma yapısında çalışır. TCP üzerinden gönderilen herhangi bir mesaj TCP paketi olarak gönderilir [49]. MQTT haberleşme modülü Şekil 2.7'de verilmiştir.



Şekil 2.7. MQTT haberleşme modülü

2.5.5. TCP

TCP (Transmission Control Protocol), İnternet ağlarının çoğunda iletişim sırasında bu protokol kullanılır. Bilgisayar ağlarında paket anahtarlamalı bilgisayar iletişiminde paketlerin kaybolmadan veri gönderimi sağlayabilmesi için bu protokol kullanılmaktadır.

2.5.6. UDP

UDP (User Datagram Protocol), işlemler arası iletişim kuran ve IP üzerinden iletişim sağlayan bir iletişim protokolüdür. Bu protokolde veriler bağlantı kurmadan yollanır kayıpsız veri aktarımı gerektiren uygulamalar için kullanılır.

2.5.7. IP

IP (İnternet Protokolü), veri paketlerinin ağ iletişiminde doğru alıcıya gidebilmesi için paketleri yönlendiren ve adresleyen protokoldür. Ağda dolaşan paketlere alıcının ip bilgileri eklenip paketin doğru hedefe ulaşması amaçlanır. İnternete bağlanan her cihaz ip adresi alır, alınan ip adresleri paketlere ekli yönlendirilince paketler doğru hedefe ulaşırlar.

IP paketi, her veri paketine ip başlığı eklenerek oluşturulan pakettir. IP adreslerinin IPv4 ve IPv6 versiyonları bulunmaktadır. Günümüzde birçok yerde ve geçmişte kullandığımız bütün IP adresleri IPv4 versiyonuna sahiptir. Ancak internetin gelişip ilerlemesi ve interneti tüketen çok sayıda cihazın olmasından dolayı IPv4 yetersiz kalmış ve IPv6 versiyonu yavaş yavaş kullanılmaya başlanmıştır.

2.5.8. 6LoWPAN

6LoWPAN (Ipv6 Over Low Power Wireless Personel Networks), IETF (Internet Engineering Task Force)'nin internet alanındaki bir çalışma grubunun ismidir. Bu protokol genellikle düşük güç kullanımlı cihazlar için uygundur. IEEE'nin 801.15.4 standartlarına uygun olarak çalışır. Birden fazla cihazla iletişime geçer ve daha çok alana yayılan veri tiplerinin kullanabilmesine olanak sağlar.

2.5.9. IEEE 802.15.4

802.15.4-2003 standardı, bir kişisel alan ağında radyo iletişimleriyle birbirine bağlanan cihazları ve temel protokolleri tanımlar. Star, noktadan noktaya gibi topolojileri destekler. Medya erişimi bağlantı tabanlıdır. IEEE 802.15.4 ağları, ağ yöneticileri olarak tam özellikli cihazlar gerektirir, ancak sistem maliyetini azaltmak için uç nokta cihazları, azaltılmış özellikli cihazlar olabilir [54].

Düşük hızlı kablosuz iletişim ağlarında kullanılan bir standarttır. Kablosuz ağlar oluşturmak için Zigbee, 6LoWPAN gibi standartlarla kullanılır.

2.5.10. LPWAN

LPWAN (Low-Power Wide Area Network), kablosuz veri iletişimi için kullanılan bir radyo teknolojisidir. Düşük güç tüketimi için kullanılan bir protokoldür. Sabit olmayan verilerin düzenli olarak taşınmasını sağlar. Daha düşük maliyetle çalışmaktadır.

2.5.11. BLE

Bu, kısa menzilli radyo frekansı sinyallerini kullanan ve 1994 yılında Ericsson tarafından geliştirilen bir kablosuz iletişim protokolüdür. 2 ana amaç için kullanılır. Bağlantı ve iletişim ekipmanı. Kablosuz dosya aktarımını etkinleştirin. Bu iki amaç için, Bluetooth modülü iletişim kurduğunda, birincil konumdaki modül, iletişimi organize etmekten sorumludur ve veri göndericidir. Cihaz lokasyonundan gelen cihaz, bu iletişimde verilerin gönderildiği adrestir.
BLE (Bluetooth Low Energy), maliyeti güç tüketimini azaltıp bluetooth iletişim sağlamaktadır. Uzun batarya ömrü ve az maliyetle tüketicilerin en çok tükettiği elektronik haline gelmiştir.
Türkiye'de en yaygın kullanılan 2 BLE modülü bulunmaktadır.

HM10

TI'nin CC2541 yongasını kullanan HM10, BLE 4.0 protokolünü desteklemesi nedeniyle ucuzdur ve çok az güç tüketir. 2.4 GHz frekansında haberleşme sağlar ve Arduino gibi mikrodenetleyiciler ile rahatlıkla kullanılabilir.

DBM01

Modül BLE 4.0 protokolünü destekler ve 2.4 GHz frekansında iletişim kurar. Küçük boyutu insanların dikkatini çekmiştir ve giyilebilir teknoloji ürünlerinde ve prototiplemede kullanılabilir.

2.5.12. Ethernet

Ethernet IoT cihazlara kablolu bağlantı, hızlı veri bağlantısı ve veri iletimini hızlı bir şekilde sunan iletişim protokolüdür.

Çerçeve, Ethernet ağ sisteminin çekirdeğidir. Ağ cihazları, bilgisayarlar veya siteler arasında bilgi aktarımı veya bilgi aktarımı. Bu nedenle, Ethernet çerçevesinin yapısal dinamik özellikleri resmi olarak kullanılır. Ethernet çerçevesindeki bitler, belirli alanlarda ve dolayısıyla zaman dilimlerinde ortaya çıkarak bir form oluşturur. Ethernet çerçeve yapısı Şekil 2.8'de verilmiştir [55].

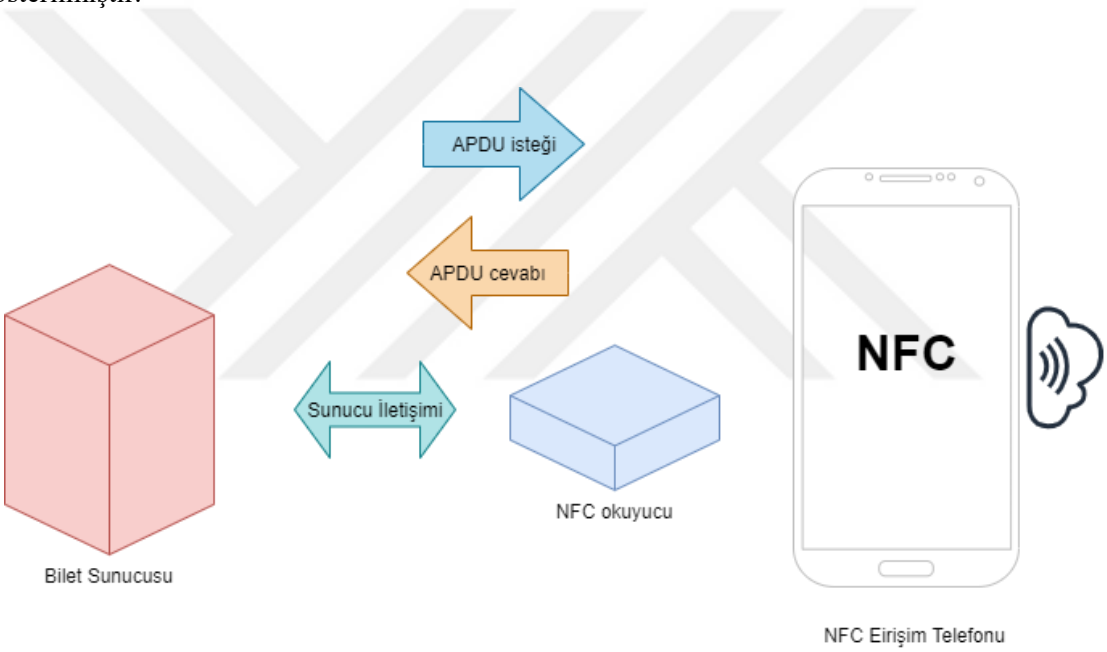
Şekil 2.8. Ethernet çerçeve yapısı

2.5.13. LTE

LTE (Long Term Evolution), Bölüm 2.3'te belirttiğimiz kullanıcı bileşenleri kısmında en çok kullanılan protokoldür. Gelişen teknolojiyle birlikte telefonlarımıza gelen LTE, mobil cihazlarda yüksek hızlı mobil internete verilen addır. LTE, kablosuz ağların ve çok noktaya yayın alımını ve hızını iyileştirir.

2.5.14. NFC

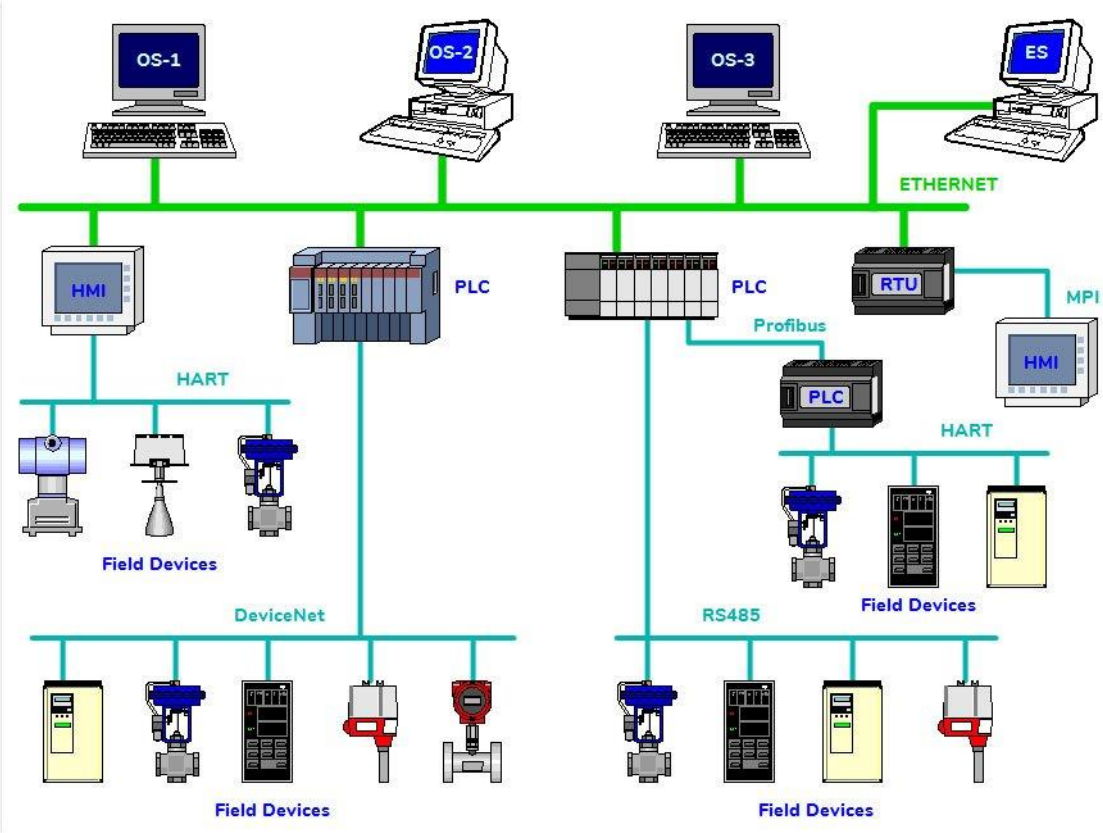
NFC (Near-Field Communication), elektromanyetik alanları kullanarak cihazların iletişime izin veren bir iletişim protokolüdür. Genellikler mobil ödemelerde, temassız ödemelerde, elektronik biletlerde akıllı biletlerde kullanılır. Şekil 2.9 NFC protokolünün çalışma yapısı gösterilmiştir.



Şekil 2.9. NFC haberleşme protokolü

2.5.15. PLC

PLC (Programmable Logic Controller), mevcut güç kabloları üzerinden veri gönderen ve veri alan bir iletişim teknolojisidir. Bundan dolayıda PLC'ler farklı saha cihazları, programlama cihazları ve diğer PLC'ler olan kontrolörler, HMI'lar SCADA'lar ile haberleşmek için kullanılan protokoldür. PLC'ler, aynı kablo üzerinden IoT cihazlarına güç vermenizi ve kontrol etmenizi sağlar [56]. Şekil 2.10'da PLC iletişim protokolü verilmiştir.



Şekil 2.10. PLC iletişim protokolü [57]

2.5.16. RFID

Radyo frekansı kullanarak nesneleri tanıma yöntemine sahiptir. Kimlik doğrulama bilgilerine erişerek eriştiği bilgi doğrultusunda RFID etiketlere güç ve iletişim sağlar.

2.5.17. Z-Wave

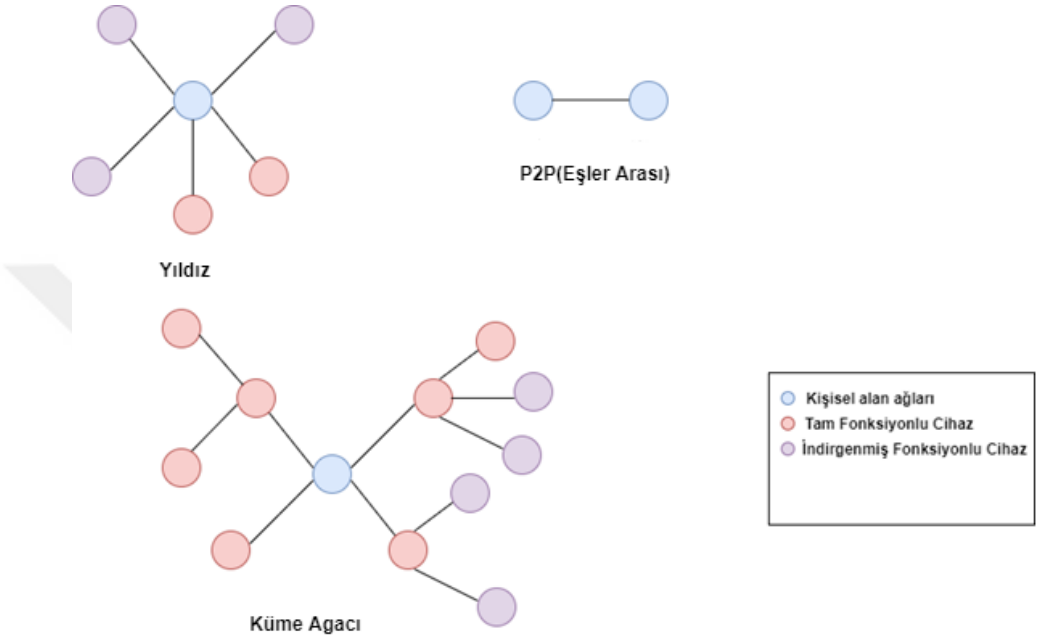
Z-Wave, ev otomasyonları için kullanılan kablosuz ağ teknolojisidir. Bu teknoloji kullanıcıların ev otomasyon cihazlarını uzaktan kontrol etmek ve izlemek için geliştirilmiştir. Ev cihazları arasında iletişim kurmak için düşük enerjili radyo dalgalarını kullanan bir ağdır [56].

2.5.18. ZigBee

Endüstride kullanılan cihazlar arasındaki fikir birliği, kablosuz iletişimin daha düşük bant genişliklerinde daha az karmaşıklık getirdiği ve çoğu durumda pil ömründen kaynaklanan sorunları çözdüğü yönündedir. Ancak, düğümler pille çalışıyorsa, düşük güç tüketimi kullanabilirler. WiFi ve Bluetooth bu ihtiyaçları karşılamak için çok çalışıyor (hepsi değil, bazıları). 1999 yılında "Firefly" çalışma grubu, ZigBee olarak bilinen teknolojiyi tasarlamaya başladı. Geliştirme

aşamasında, önce IEEE 802.15.4-2003, ardından Aralık 2004'te ZigBee Alliance'ın ZigBee protokolü temel alındı [54].

ZigBee, IEEE 802 standartlarına göre küçük, düşük güçlü radyo dalgalarını kullanarak kısa mesafe kablosuz ağ standardı olarak tanımlanan iletişim protokolüdür. ZigBee protokolü Şekil 2.11'de gösterilmiştir.



Şekil 2.11. ZigBee protokolü

2.6. Uygulama Alanları

Gelişen teknoloji ile IoT teknolojileri günümüzde birçok alana yayılmakta ve hayatımızı kolaylaştırmaktadır. IoT, sensörler ve akülatörlerle zenginleştirildiğinde, üretim/endüstriyel, ulaşım/mobilite, enerji, perakende, şehirler, sağlık, tedarik zinciri, tarım, binalar gibi teknolojileri kapsayan siber-fiziksel teknoloji sınıfı haline gelir.

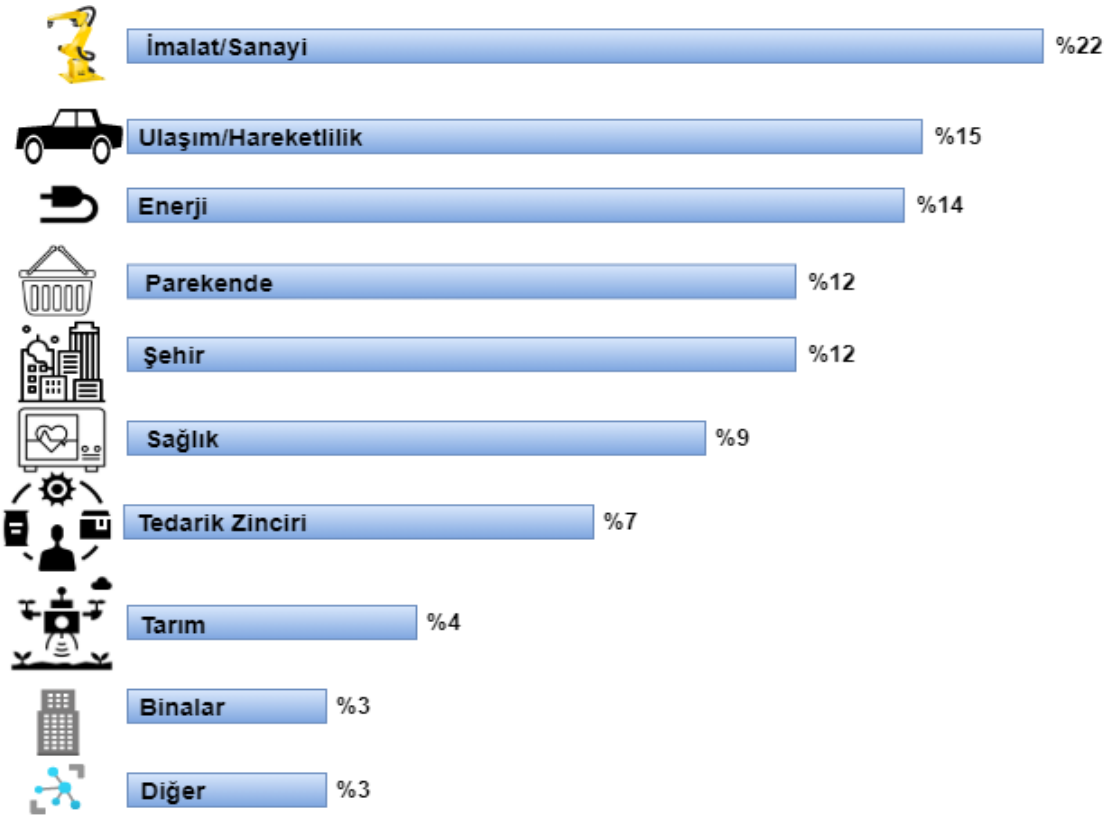
Bina ve evlerde IoT kullanımı; doğal gaz sensörleri, su, duman, yangın, alarm ve gözetleme sistemleri gibi alanda yer almakta ve kolaylık sağlamaktadır.

Endüstride, IoT kullanımı kontrol sistemleri, makine ağı gibi alanlarda kullanılır endüstride genel olarak bir örnek verilirse SCADA sistemler örnek verilebilir. IoT cihazlar burada, işin işleyişine ve hızının artmasına yardımcı olur. Sistemlerin birbiriyle iletişime geçip veri alışverişi yaparak sürecin kısalmasına katkıda bulunurlar. İnsan faktörü işin işine girseydi süreç daha uzun zaman alır ve iş trafiğinin aksamasına sebep olurdu.

Enerji sektöründe, IoT cihazların enerji tüketimini en aza indirip ve enerji kontrolünü sağlamak için uzaktan kontrol sistemlerini yönetmektedir. Sağlık sektöründe hastanın vücut

değerlerinin takibi, çalışanların işlerini veri toplama analiz etme, tıbbi cihazlar, giyilebilir akıllı cihazlar, vb. alanlarda kullanılmaktadır. Ulaşım sektöründe navigasyon yönetimi, akıllı park, trafik izleme, güvenlik gibi sistemlerde kullanılmaktadır.

Tarım sektöründe tarlanın ihtiyacı olan su miktarının, gübre oranın doğruluğuna kadar birçok alanda kolaylık sağlayarak tarlaların verimliliği ve gıdaların besin kalitesinin artırılmasına olanak sağlamaktadır. Şekil 2.12 IoT uygulama alanlarının 2020 yılına göre dağılımı verilmiştir.



Şekil 2.12. IoT uygulama alanları grafik dağılımı [58]

3. IOT SALDIRILARI

Ahmed ve diğ.[37] çalışmasında, nesnelerin interneti için yeni sistemler, bir rakibin hedeflerine ve sistemine bağlı olarak farklı şekillerde birçok tehditle karşı karşıyadır. Satıcılara dayalı bir model kullanılarak yapılan bir sistemde, katkıda bulunan satıcılardan biri kötü niyetle hareket edebileceği ve potansiyel olarak güvenilmeyen satıcı, sistemin görevlerine çeşitli nefret kötü işlevler ekleyebileceğinden bahsetmiştir [37].

Sriandh ve diğ.[31] bahsettiği gibi, nesnelerin İnterneti (IoT) milyarlarca ara bağlantı, bilgi paylaşımı ve yararlı veri cihazları, kişiler ve hizmetlerden oluşan bir ağdır. Artan konfor, performans ve kullanıcı otomasyonu, IoT uygulamalarında güçlü bir şekilde onaylanmıştır. Otomatik IoT ortamını güçlendirmek için, yüksek düzeyde güvenlik ve gizlilik, kimlik doğrulama ve saldırılardan kurtarma gereklidir [31].

Nesnelerin İnterneti ekolojisi oluşturulduktan sonra, güvenlik açısından da zorluklarla karşılaşacaktır. Örneğin, bir kullanıcı bir IoT cihazını ağa bağlamak için sıradan bir ev tipi yönlendirici kullanmayı seçerse, özellikle birçok ailenin zayıf şifreleri olduğunda veya hatta bir şifre belirleme alışkanlığına sahip olmadığında, herhangi bir zamanda saldırıya uğrama riski vardır. Kablosuz ağ ortamları için şifre. Bu durumda saldırgan, yönlendiriciyi istila ederek evin tüm IoT sistemini kolayca kontrol edebilir. Mevcut İnternet esas olarak sanal içerik sunar ve bilgisayar korsanlarının saldırılarına uğradığında genellikle yalnızca veriler kaybolur. Ancak, Nesnelerin İnterneti ağı ağa bağlar gerçek nesneler. Yasadışı bir şekilde kontrol edildiğinde, maddi hasara neden olabilir ve hatta kişisel güvenliği tehdit edebilir. Bu nedenle, Nesnelerin İnternetinin güvenliğini sağlamaktan kimin sorumlu olduğunu bulmak da önemlidir [25].

Endüstriler, zayıf veya kolayca elde edilebilen varsayılan kimlik bilgilerini ve genellikle zayıf güvenlik özelliklerini içerebilen varsayılan yapılandırmalar sağlayarak üretim maliyetlerini en aza indirmeye çalışır. Bu zayıflıklar, çeşitli kötü niyetli hedeflere ulaşmak için güvenlik zayıflıklarından yararlanan Mirai gibi büyük ölçekli botnet'lerin ortaya çıkmasına yol açmıştır. Dahası, botnetlerin gelişmekte olduğunu gözlemlemek kolay olsa da giderek daha karmaşık ve daha etkili hale geliyor, IoT botnetlerinin işlevleri hakkında güvenilir bilgiler genellikle mevcut değil. Bilgi mevcut olduğunda, genellikle heterojen bir şekilde sağlanır ve botlar arasında karşılaştırmayı zorlaştırır [59].

3.1. IoT Saldırı Türleri

IoT, günümüzde her yerde evimizin, arabamızın, işyerimizin vb. alanlarda bizlerle. Bu durumda bize mahremiyetimizin ne kadar ihlal edildiğinin bir kanıtıdır aslında. Mahremiyetimin

korunması ve yaşanan bu olayların önüne geçmek için gizlilik yönetimi ve kimlik yönetimi çok önemli faktör oynamaktadır.

3.1.1. Fiziksel Saldırılar

IoT cihazlar herkes tarafından erişebilir olduğunda fiziksel saldırılar meydana gelir. Fiziksel saldırılar genellikle saldırganın kötü amaçlı kodu yaymak için usb takıp sisteme uzaktan erişmesi sağlanır.

3.1.2. Şifreleme Saldırıları

Şifrelenmemiş IoT cihazların veya karmaşık şifre ile şifrelenmemiş cihazlar saldırganın hedef noktası haline gelebilir. Saldırgan ağı koklayarak bu cihaza uzaktan erişip şifreleme saldırıları başlatabilir.

3.1.3. DoS(Hizmet Reddi)

Saldırgan internete bağlı IoT cihazı geçici veya süresiz olarak ağı aksatarak kullanıcının asıl alması gereken pakete erişmesini engelleyip ağ trafiğini doldurur. DoS saldırıları, web sunucuları, bankacılık, ticaret, hükümet ve medya kuruluşlarını hedef alır. DoS saldırıları için iki yöntem kullanılır sel veya çökertme saldırıları. En çok kullanılan kabuk (Shell) saldırıları:

Arabellek Taşması Saldırısı

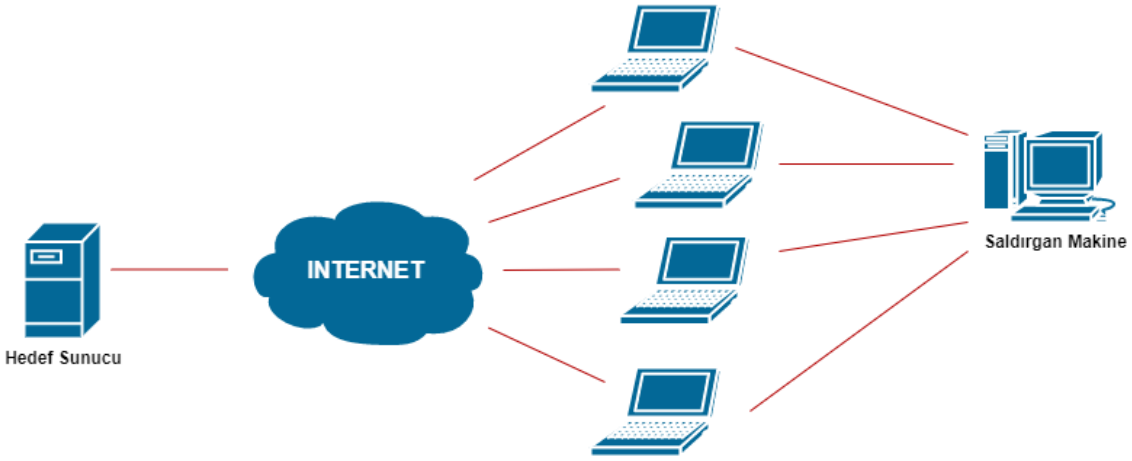
Ağ adresine çok fazla trafik gönderilir, ağ iletişiminin aksamasına neden olur.

ICMP flood

Bir makine yerine ağdaki tüm bilgisayarlara ping paketi göndererek ağ trafiğini doldururlar.

SYN flood

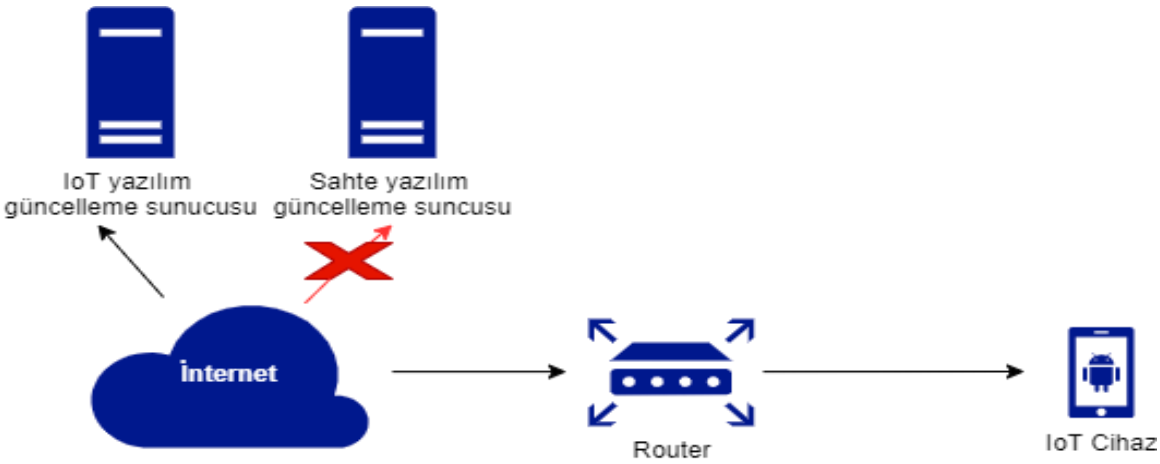
Sunucuya bağlanmak için istek gönderilir, paket hiçbir zaman yerine ulaşmaz. Tüm açık bağlantılar isteklerle doldurularak asıl kullanıcının bağlanmaması sağlanır. Gelişen teknoloji DoS saldırılarına karşı savunma mekanizması geliştirmiştir fakat DDoS benzersiz özellikleri nedeniyle yüksek bir tehdit oluşturur. Şekil 3.1’de DoS saldırısı gösterilmiştir.



Şekil 3.1. DoS saldırısı

3.1.4. Firmware Hijackging

Firmware saldırısı sisteme saldırgan tarafından hazırlanan kodun entegre edilmesidir. IoT uygulamaları için gelen güncellemenin doğru kaynaktan geldiğine emin olunmalıdır aksi taktirde saldırganın hazırladığı zararlı yazılım indirilip sisteme entegre edilebilir. Kullanılan Firmware güvenliğini önemli kılan nedenlerden bazıları elektronik cihazların web kameraları, ses kartları vb. ürünler ürün yazılımı ile doludur, bu ürünler için herhangi bir zararlı yazılım ile güncelleme sistemi ciddi şekilde tehdit eder. Ek olarak yazılım için gelen yamalar güncel tutulmalıdır. Şekil 3.2'de gösterilen kırmızı ile çizilen sunucudan güncelleme yapılırsa saldırganın hazırladığı zararlı kod sisteme entegre olur.

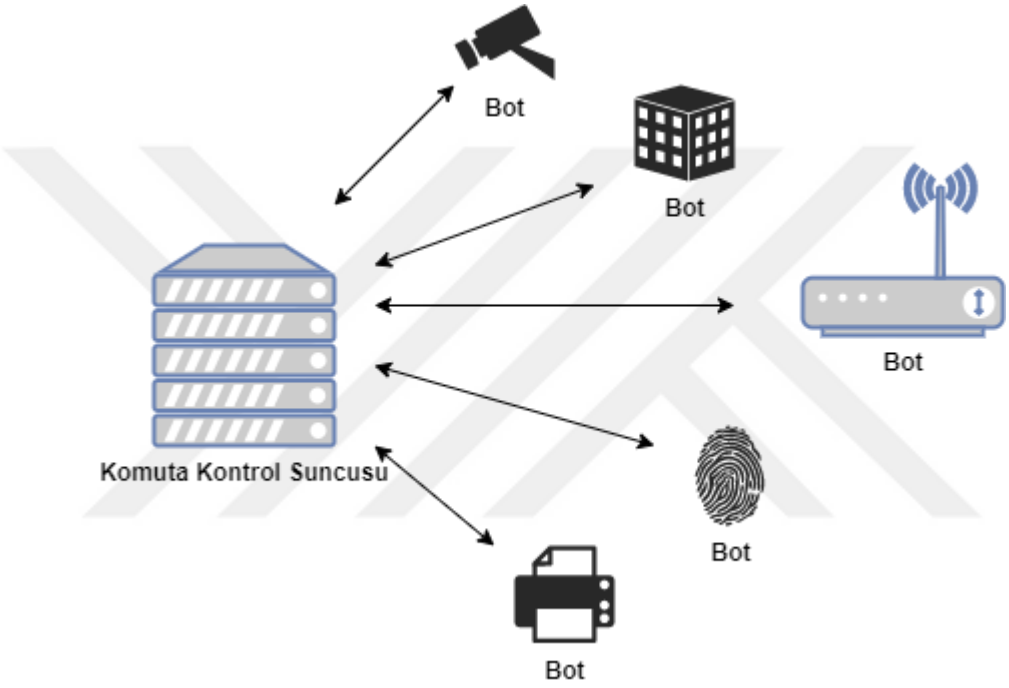


Şekil 3.2. Firmware Hijacking

3.1.5. Bot Ağları

Botnet, saldırganın kurban sisteme uzaktan erişip komuta kontrol sunucularını kullanarak bot ağlarını kontrol edip sunucudan elde ettiği bilgileri para karşılığında satmaya çalışmasıdır. Şekil 3.3 de botnet saldırısı gösterilmiştir.

Mirai botnet, saldırısı bu örneklerden biridir. Açık telnet bağlantı noktaları için ip adreslerinin büyük blokları taranıp ele geçirilen şifrelerle oturum açmaya çalışılmıştır. Bu şekilde mirai botnet oluşturulmuş. Bu saldırı 12 Ekim 2016'da Amerika'da gerçekleştirilmiştir.



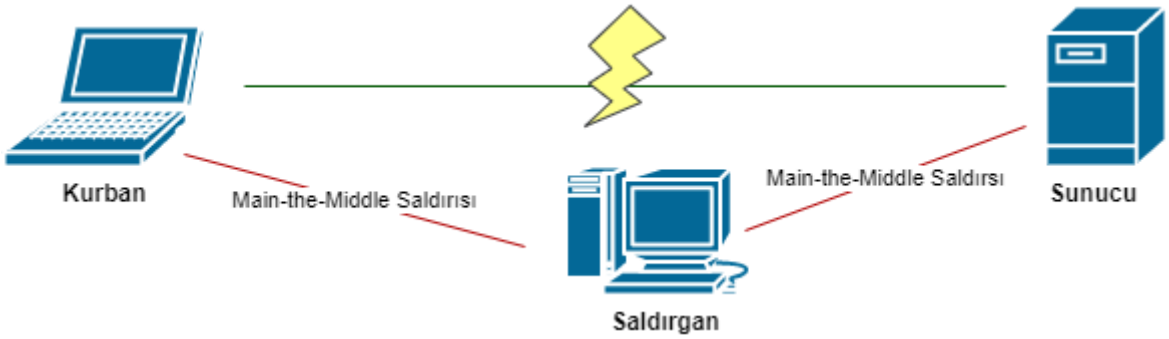
Şekil 3.3. Botnet saldırısı

3.1.6. Ortadaki Adam Saldırısı

Ortadaki adam saldırısı (Man in The Middle - MiTM) istemci-sunucu arasındaki iletişim dinlendiğinde gerçekleşir. Bu saldırıda istemci-sunucu arasındaki iletişim yakalandığında alıcının doğru paketi almaması alıcının saldırganın ilettiği paketi alması sağlanır. Özellikle broadcast alınan paketler ağda ki tüm makineler tarafından görünür. IoT cihazlarının güvenliğinin ihlal edilmesi için bu yöntem kullanılır.

Saldırı yöntemi, ARP zehirlenmesi yaparak ARP tablosu doldurulur. Yönlendirici gelen ARP isteklerine cevap veremez hale gelir. Sonrasın da ARP isteği paketleri broadcast olarak gönderilir. Ağda yönlendirici arayan bilgisayar saldırganı yönlendirici bilgisayar olarak tanır. Ağ üzerindeki paketler saldırganın bilgisayarı üzerinden gönderilecektir. Tüm paketler saldırgan tarafında okunur ve değiştirilir duruma gelecektir.

Bu tür saldırılardan korunmak için TLS gibi açık anahtar altyapısı ağı ortadaki adam saldırısına karşı koruyabilir veya kullanıcılar gelen yanıt sürelerdeki tutarsızlıkları kontrol etmelidir. Şekil 3.4'te ortadaki adam saldırısı gösterilmiştir.



Şekil 3.4. Ortadaki adam saldırısı

3.1.7. Fidye Yazılımı

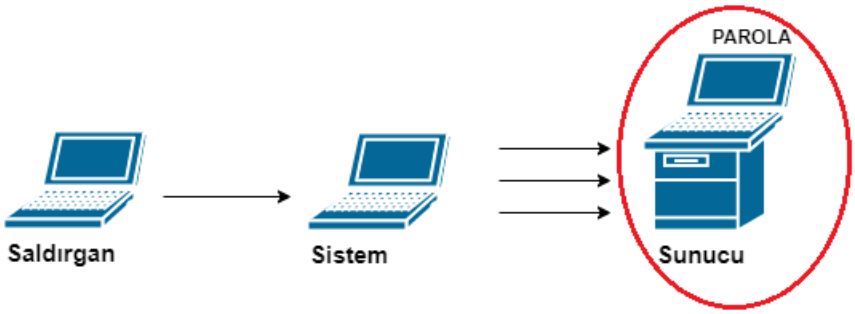
Fidye yazılımı, saldırganın eriştiği cihazdaki dosyaları şifreleyip erişimi engelleten kötü amaçlı bir yazılım türüdür. Saldırganlar, kullanıcının veya kurumun dosyalarına erişebilmesi için şifre çözme anahtarını satarlar. Bu durum günlük işlerin sekteye uğramasına sebep olur.

3.1.8. Ayrıcalık Yükseltme

Saldırgan IoT cihazlarda keşfettiği güvenlik açığıyla sisteme erişip yetki yükselterek kötü amaçlı yazılım çalıştırıp sistemde önemli olan bilgileri ele geçirebilir.

3.1.9. Kaba Kuvvet Saldırısı

Saldırgan doğru olanı tahmin etme umuduyla IoT cihazlarda parola deneme saldırıları gerçekleştirir. Çeşitli kullanıcı adı ve şifre deneme kombinasyonları ile denen bir saldırı türüdür. Bu saldırı da çok sayıda ardışık parola deneme isteği var ise kaba kuvvet (brute force) saldırısı diyebiliriz. Saldırganlar elde ettikleri parola ile ayrıcalık yükseltip, dosyalara erişim sağlayabilirler. Şekil 3.5'te kaba kuvvet saldırısı gösterilmiştir.



Şekil 3.5. Kaba kuvvet saldırısı

3.2. IoT Katman Saldırıları

Bu saldırılar, sistemler üzerinde kötü niyetli eylemlerde bulunmak ve böylece yetkili kullanıcılara verilen hizmetleri kesintiye uğratmak için tasarlanır ve yürütülür. Bu saldırılar, gizliliği ve sistem bütünlüğünü tehlikeye atar.

3.2.1. Fiziksel Katman Saldırıları

Parazit Yapma: Bu saldırıda saldırgan güçlü bir anten ile sinyal oluşturarak iletişimde parazit yapabilir.

Etiket: Etiket saldırılarında saldırgan sahte bir etiket oluşturarak kullanıcılara sahte bir istek atıp kullanıcıları istemedikleri yere yönlendirilir.

Düğüm: Böyle saldırılarda fiziksel bir düğüm kopyalanarak IoT ağında birden fazla noktaya yerleştirilerek kullanıcıların gitmek istedikleri düğümler yerine saldırganlar tarafından oluşturulan sahte düğümlere gitmesi hedef alınır.

3.2.2. Veri Bağı Katmanı Saldırıları

Fiziksel bir düğüm etrafındaki IoT cihazlara kendini birden çok düğümmüş gibi tanıtarak çok kimlikli saldırılarda birden çok mantıksal düğüm gibi davranırlar.

ITU IoT çalışmasında, çukur saldırısında saldırgan düğüm komşularını yönlendirme parametreleriyle etkileyerek bilgilendirir. Saldırgan komşuları tarafından istenilen düğüm olarak seçerek mesajları o düğüme yönlendirir. Bu tür saldırılar bir arada gerçekleştiğinde, birçok komşu düğüm, mesajlarını saldırgan düğüme iletir. Paketleri yönlendirebilen saldırgan sisteme saldırılarda bulunabilmektedir [60].

ITU IoT çalışmasında, bir düğümün kök düğüme göre konumunu belirlemek için RPL düzeyi parametresi kullanılır ve paketler, düğümler arasında düzeye göre yönlendirilir ve kök düğüme iletilir. Seviye değerine göre kök düğümden her düğüme iletilir. Seviye topolojilerinde oluşan döngüleri engeller. Seviye değerleri, saldırganlar tarafından baskın konumları işaretlemek ve döngüyü önlemek için kullanılır. Hatalar ve istisnalar meydana geldiğinde, sürüm numarasını kullanan kök düğüm, yeni bir topoloji oluşturmaya bağlıdır. Saldırgan, sürüm numarasını kullanarak RPL ağını yeni bir topoloji kurmaya zorlar. Topoloji güncellemesinin neden olduğu mesaj trafiği nedeniyle düğümlerin gereksiz kaynakları kullanmaya zorlandığını ve böylece ağın ömrünün kısaldığını gösterir [60].

3.2.3. İletim Katmanı Saldırısı

Saldırgan IoT ağına birden çok paket göndererek ağdaki trafiğin dolmasına ve asıl alıcının paketi alamamasına sebep olur. Senkoronizasyona yönelik saldırılarda ip paket başlık bilgisi değiştirilerek seğmenlerin zamanlaması bozulur, yerine ulaşamayan seğmenlerin tekrar gönderilmesine yol açar.

3.2.4. Uygulama Katmanı Saldırısı

Internet üzerinden gerçekleştirilen saldırılar bu katmana aittir. Uygulama katmanı, web, protokol işleme, url işleme vb. güvenlik açıkları bulunmaktadır.

3.3. IoT Güvenliği

IoT cihazları tehlikeli olamayacak kadar küçük veya özel görünse de, bunların saldırganlar tarafından ele geçirilebilecek ve IoT güvenliğinin ötesinde sorunlara neden olabilecek ağ bağlantılı genel amaçlı bilgisayarlar olma riski vardır. En basit cihaz bile İnternet üzerinden saldırıya uğradığında çok tehlikeli olabilir. Örneğin bebek monitörleri izlenebilir veya hayat kurtaran sağlık ekipmanlarının kullanımı engellenebilir. Saldırganlar kontrolü ele geçirdikten sonra verileri çalabilir, hizmetleri bozabilir veya herhangi bir bilgisayarda gerçekleştirebilecekleri diğer siber suçları işleyebilirler. Saldırganların IoT altyapısını ele geçirmesinin neden olduğu hasar, veri ihlalleri ve hizmet kesintileri ile sınırlı değildir. Bu insanlar sistemlere fiziksel zarar verebilir ve daha da kötüsü, onları kullanan insanlara zarar verebilirler.

Srinadh ve diğ.[31] makalesinde, IoT dünyası hızla yükseliyor ve sosyal ve iş hayatı üzerinde büyük bir etkiye sahip. Bağlı cihazlar bu ortam aracılığıyla çok büyük miktarda veri üretir. Sahinaslan'a (2019) göre ağ üzerinden 2020 yılına kadar alınıp verilen verilerin 44 ZettaBytes (ZB) üzerinde olması bekleniyor. Dünyadaki bağlantılı her birey (o zamanın toplam nüfusunun yaklaşık %75'i) 2025'e kadar her gün yaklaşık 18 saniyede bir olmak üzere 4.900'den fazla dijital veri

etkileşimine sahip olacak. 2025'te IoT cihazları tarafından 90 ZB'nin üzerinde veri üretildiği bahsedilmiştir [31].

Bu hızlı gelişme risk ve tehditleri beraberinde getirmektedir. Güvenli anahtar yönetimini sağlamak için ileri teknikler geliştirilmeli ve kullanılmalıdır. IoT güvenliğini sağlamak için genel gereksinimler:

Veri Bütünlüğü

Verilerin yetkisiz kullanıcı veya saldırgan tarafından manipülasyona karşı korunmasına odaklanır. IoT özellikli bulut tabanlı bir sistemde, gönderen ve alıcı arasındaki değişime dâhil olan her düğümde bir bütünlük kontrolü gerçekleştirilebilir. Cilt izleme sisteminde bütünlük çok önemlidir sanki cilt hastalığı verileri tahrif edilmiş, yanlış teşhis ve tedavi yapılabilir, bu da yan etkilere, bazen de cilt kanserine neden olur. Bütünlüğe ulaşmak için, veri bütünlüğünü artırma mekanizmalarının geliştirilmesi gerekmektedir [61].

Kullanılabilirlik

Amaçlanan verilerin, hizmetlerin ve cihazların yetkili kullanıcılar için erişilebilir olmasını sağlar. IoT ve bulut tabanlı platformda yetkisiz kullanıcıların iletişimi kesintiye uğratmasına veya etkilemesine izin verilmemelidir. IoT tabanlı cilt bakımı sistemi çoğunlukla gerçek zamanlı veriler ve hizmetler üzerinde çalışır, bu nedenle zamanında kaliteli teslimat şarttır. Ayrıca herhangi bir zararlı reaksiyon durumunda, sistem gerçek zamanlı çözümler ve hizmetler sağlamalıdır. IoT'de kullanılabilirliği sağlamak için verilerin kullanılamaz hale gelmesini önlemek için gelişmiş teknikler uygulanmalıdır [61].

Kimlik Doğrulama ve Tanımlama

Yalnızca kimliği doğrulanmış kullanıcı bilgi ve hizmetlere erişmelidir. Doğruluk, kullanıcının korumalı bilgilere erişimini denetler ve kısıtlar. Yetkisiz cihaz bağlantılarının veya sistemdeki uygulamanın engellenmesi Tanımlama ile sağlanmaktadır. Kimlik doğrulama, verilerin ağ üzerinden yasal olarak teslim edilmesini sağlar. IoT sistemi çok sayıda heterojen cihaz içerdiğinden, kimlik doğrulamayı işlemek için verimli mekanizmalar gereklidir [61].

Kaynak Yönetimi

IoT tabanlı sistemler heterojen cihazlardan oluşur, bu nedenle kaynak yönetimi, ilgilenilmesi gereken önemli bir husustur. Verimliliği artırmak ve veri fazlalığını azaltmak, kaynak yönetimindeki konulardır. Kaynakları verimli bir şekilde yönetmek için verimli mekanizmalar gereklidir [61].

Tazelik

Bilginin taze olduğunu ve eski mesajların herhangi bir düşman tarafından tekrarlanamayacağını doğrular [62].

İletim gizliliği

Bir IoT algılama düğümü ağdan çıkarsa, çıkışından sonra gelecekteki tüm mesajlar yasaklanmalıdır [62].

Geriye dönük gizlilik

Ağa yeni bir IoT algılama düğümü eklenirse, daha önce iletilen herhangi bir mesajı okumamalıdır [62].

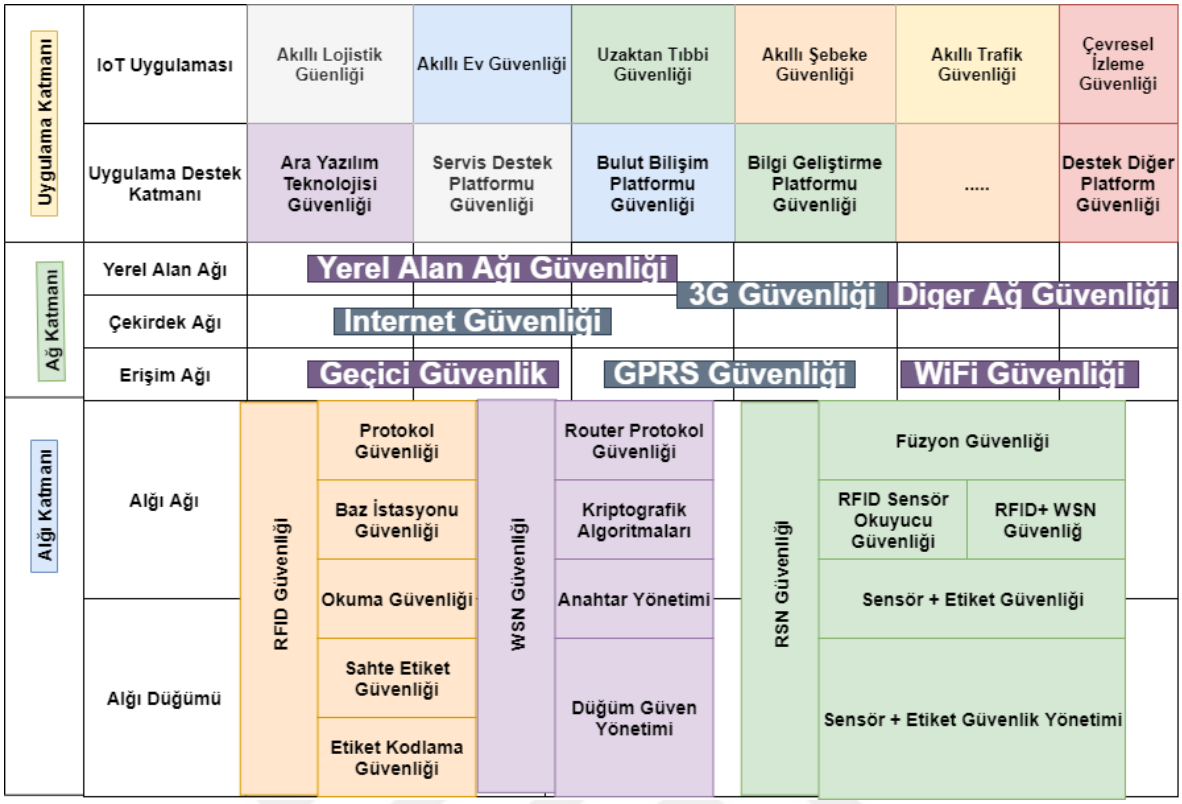
Yetkilendirme

Yalnızca meşru IoT algılama (akıllı) cihazların ağ hizmetlerine bilgi sağlayabileceğini doğrular [62].

Hırsız Algılama

IoT cihazlarının hizmetinde, mevcut modellerin çoğu davetsiz misafirleri teşhis etmede düşük verimliliğe sahiptir. Gerçekleşen izinsiz girişleri yeterince tanımlayacak böyle bir sistem tasarlamak karmaşıktır. Son olarak, IoT cihazı büyük ölçekte yetkin bir şekilde çalışabilen bir sistem gerektirir [50].

Mardiana ve diğ.(2019) yaptıkları çalışmada, IoT uygulamaların güvenliğini artırmak için, Şekil 3.6'de gösterildiği gibi tüm IoT katmanlarındaki güvenlik mimarisini kapsaması gerektiğini söylemişlerdir [63].



Şekil 3.6. IoT mimarisi [63]

3.4. IoT Güvenliği İçin Kullanılan Kriptografi Algoritmaları

Gün geçtikçe gelişen teknoloji interneti güvenli bir şekilde kullanmamız için bizi uyarıyor. Gelişen IoT teknolojilerinin sağladığı kullanım kolaylığına ek olarak güvenliğinde bir o kadar önemli bir hale gelmektedir. Bunun için IoT haberleşmelerinde veriler kriptografik algoritmalarla şifrelenir bunun sebebi IoT cihazlar arasında iletişimi güvenli bir şekilde şifrelemek ve oluşabilecek güvenlik tehditlerinin önüne geçmektir.

Kriptografi, şifreleme algoritmaları kullanarak verileri şifreleyerek ağda iletirken bir mesajı (e-posta mesajları, kredi kartı bilgileri vb.) Güvenli tutma sanatı ve bilimidir. Ağ güvenliğinde birçok şifreleme algoritması kullanılmaktadır. Üç temel türe ayrılırlar: Simetrik algoritmalar, Asimetrik (veya açık anahtar) algoritmalar ve Kriptografik protokoller. Şifreleme ve şifre çözmede kullanılan anahtarların sayısına göre, bunlar şu şekilde sınıflandırılır: Verileri şifrelemek ve şifresini çözmek için bir anahtarın kullanıldığı simetrik algoritmalar (veya gizli anahtar şifreleme) ve iki anahtar (ör. Özel) kullanan asimetrik (veya açık anahtar) algoritmalar ve genel anahtarlardır. Şifreleme için genel anahtar kullanılır ve şifre çözme için özel anahtar kullanılır [64].

3.4.1. CLEFİA Blok Şifreleme

Clefia 2007 yılında sony tarafından geliştirilen güvenli bir blok şifreleme algoritmasıdır. Blok uzunluğu 128 bittir ama 128 bit, 192 bit ve 256 bit anahtar boyutları da seçilebilir. Clefia IoT cihazlarda yüksek güvenlik sağlarken donanım ve yazılım uygulama yetenekleri sağlamaktadır. Sony yaptığı açıklamaya göre; LEFIA, büyük ölçekli saldırılara karşı bağışıklık sağlayan bir yayılma anahtarlama mekanizması kullanır. Ek olarak, veri işleme bölümü ile kritik programlama bölümü arasındaki işlevlerin paylaşımı, kapı boyutu küçüldükçe maliyetlerin düşmesi anlamına gelir. Aynı zamana da hafif sıklet algoritması olarak bilinmektedir Aslan [65] makalesinde anlattığı gibi, hafif sıklet algoritmaları; Hafif sıklet kriptografinin amacı, kısıtlı kaynaklar (alan, güç tüketimi, enerji tüketimi) kullanılarak bilgi güvenliğini sağlayan algoritmalar sunmaktır [65]. Bundan dolayı IoT haberleşmede hafif sıklet algoritmaları tercih edilmektedir.

3.4.2. PRESENT Blok Şifreleme

PRESENT, Fransa Orange Labs, Almanya Ruhr Üniversitesi ve Danimarka Teknik Üniversitesi tarafından 2007 yılında geliştirilen bir blok şifredir. Tasarımcıları A. Bogdanov, A. Poschmann, C. Paar, C. Vikkelsoe, G. Leander, L.R. Knudsen, M.J.B. Robshaw ve Y. Seurin'dur. CLEFIA gibi ISO/IEC 29192-2:2012 dokümanı ile hafif sıklet blok şifreleme algoritması olarak standartlaşmıştır[65]. Blok boyutu 64 bittir anahtar uzunluğu 80 bit veya 128 bit olabilir. 4 bitlik S-box'tan oluşmaktadır. Present algoritmasında şifreleme ve şifre çözmek için 80 ve 128 bitlik anahtarlar kullanılmaktadır.

3.4.3. Blowfish

Blowfish bir blok şifrelemedir ve simetrik anahtar şifrelemenin bir parçasıdır. Verileri 8 baytlık bloklar halinde şifreler. Algoritma iki bölümden oluşur; bir anahtar uzantısı bölümü ve bir veri şifreleme bölümü. Anahtar uzantısı, maksimum 56 bayt (448 bit) uzunluğundaki bir anahtarı, toplam 4168 baytlık alt anahtarlara sahip birkaç tabloya dönüştürür [66].

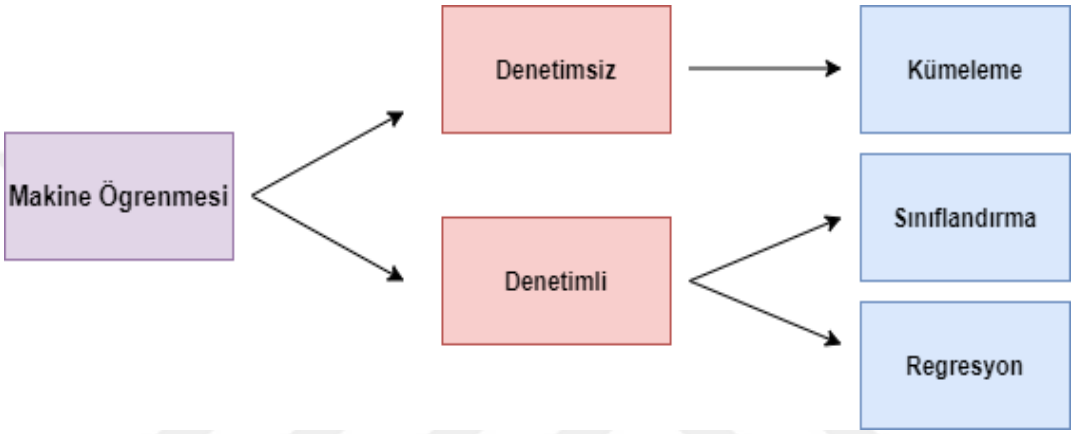
3.4.4. Hafif Kriptografi Algoritmaları

Yaygın olarak kullanılan kriptografik algoritmalar, CPU zamanı, bellek ve pil gücü gibi çok fazla bilgi işlem kaynağı tüketmektedir. Bu nedenle, kaynak kısıtlı bir cihaz olarak, Nesnelerin İnternet'inin ana zorluğu hafif, kaynak verimli kriptografik algoritmalardır. Kaynak kısıtlı ortamlar için uygun algoritmalar. Bunlar, geleneksel şifreleme ve şifre çözme algoritmalarından daha enerji verimli olan ve optimize edilmiş şifreleme algoritmaları tarafından desteklenen hızlı yanıt algoritmalarını içermektedir [64].

Son derece düşük kaynaklı cihazlarda kullanılan kriptografik algoritmaların tasarım standartları, yaygın olarak kullanılanlardan farklıdır. Bu nedenle, son derece düşük gereksinimlere sahip hafif bir şifreleme algoritması geliştirilmiştir. Hafif şifreleme algoritmaları için tanımlanmış kesin bir standart olmamasına rağmen, özellikler genellikle; Donanım uygulamaları için gereken minimum boyut, Mikro işlemcilerden veya mikro denetleyicilerin düşük hesaplama gücü, düşük uygulama maliyeti ve iyi güvenlik özelliklerini içerir [64].

4. MAKİNE ÖĞRENMESİ

Tez çalışmasında kullanılan veri setleri üzerinde makine öğrenme yöntemleri ile sınıflandırma yapılmıştır. Makine öğrenmesi, analitik modellerin yetersiz olduğu durumlarda sorunları çözmek için kullanılmaktadır. Makine öğrenimi algoritmaları, insan müdahalesi olmadan deneyimlerle gerçekleştirilen programlardır. Makine öğrenme yöntemleri kategorize edilmiş hali Şekil 4.1'de gösterilmiştir.



Şekil 4.1. Makine ögrenmesi yöntemleri

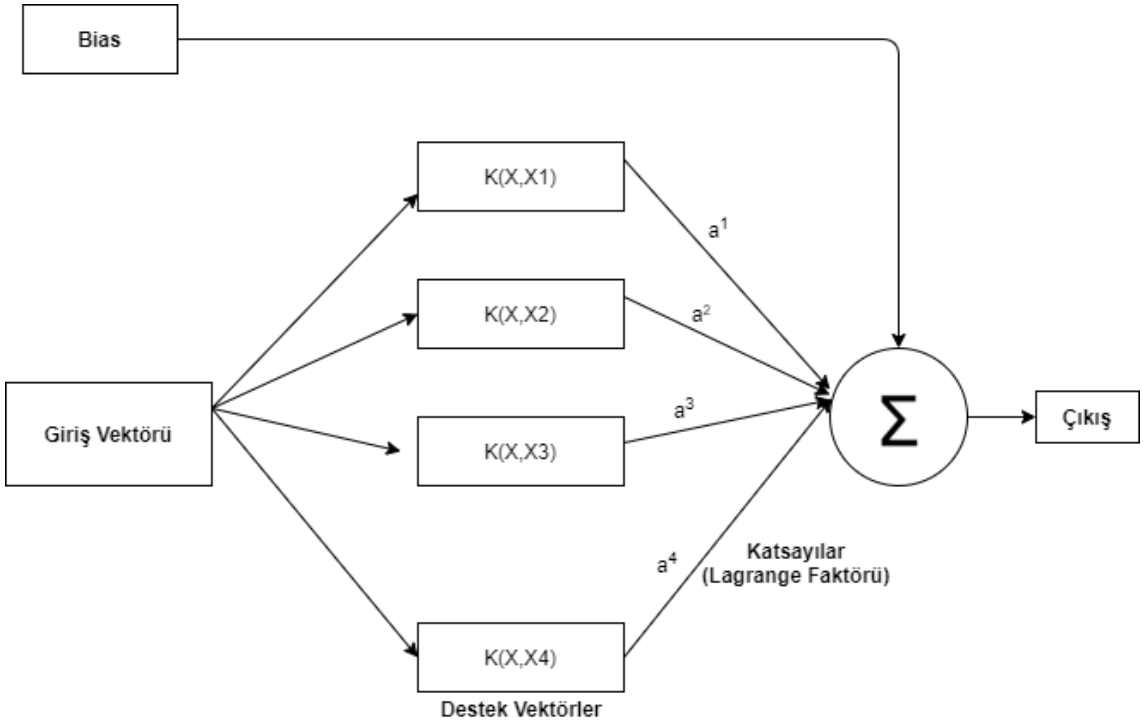
Denetimsiz öğrenme, denetlemeye ihtiyaç duyulmayan bir makine öğrenme tekniğidir. Modeli analiz edilmesi için modelin kendi başına çalışmasına izin verilmelidir. Denetimsiz öğrenmede sistem öğretilmez, verilerden öğrenilir ve verilerde bilinmeyen her türlü paterni bulur. Kümeleme bir nesne kümesini gruplama yöntemidir. Önceden bir bilgi verilmemiş bir yapıya model bulunur. Ek olarak algoritmaların kaç kümeyi tanımlaması gerektiğini ayarlayabiliriz. K-Means ve Hiyerarşik kümeleme en çok kullanılan yöntemlerdir ve mesafe olarak yakın olan kümeler birleştirilerek yeni bir küme oluşturulur. Bütünden parçaya da tam tersidir.

Denetimli öğrenmede, algoritmalar etiketli örnekleri kullanarak tahmin yaparlar. Geliştirilen tahmin modelleri sınıflandırma ve regresyon teknikleri kullanır.

Girdi verileri kategorilere ayrılır. Veriler etiketlenir, kategorilere ayrılır veya belirli gruplara sınıflara ayrılırlar. Sınıflandırma yapmak için kullanılan algoritmalar, Destek Vektör Makineleri (DVM – Support Vector Machine (SVM)), Karar Ağaçları, K-En Yakın Komşuluk (K-Nearest Neighbor - KNN), Naive Bayes, Diskriminant Analizi, Lojistik Regresyon ve Yapay Sinir Ağlarını içerir.

4.1. Destek Vektör Makineleri

Veri noktalarını belirgin bir şekilde sınıflandırıp N boyutlu bir uzayda bir hiper düzlem bulunmaktadır. Bulduğu hiperdüzlem üzerindeki noktaları ayırmak için bir çizgi çizer ve amacı çizginin iki noktası arasındaki mesafeyi maksimize etmektir. SVM zamanda doğrusal ve doğrusal olmayan verilerde sınıflandırılabilir. Karmaşık, küçük ve orta ölçekteki veri setleri için kullanılır. SVM algoritması 4.1 denkleminde verilmiştir. Şekil 4.2'de SVM yapısı verilmiştir.



Şekil 4.2. Destek vektör yapısı [67]

Şekil 4.1'de verilen vektör yapısı incelenirken çekirdek fonksiyonu ve alfa Lagrange çarpanları görüntülenir. Girdinin iç ürünü, çekirdek işleviyle hesaplanır. Lagrange çarpanları ağırlıkları temsil eder. Örneğin, bir SVM'de çıktı değeri, nokta çarpımların bağımsız kombinasyonlarının ve girdinin Lagrange çarpanlarının toplamına eşittir [67].

$$K(x,y) =< x,y >\div \sqrt{(< x,x >< y,y >)} \tag{4.1}$$

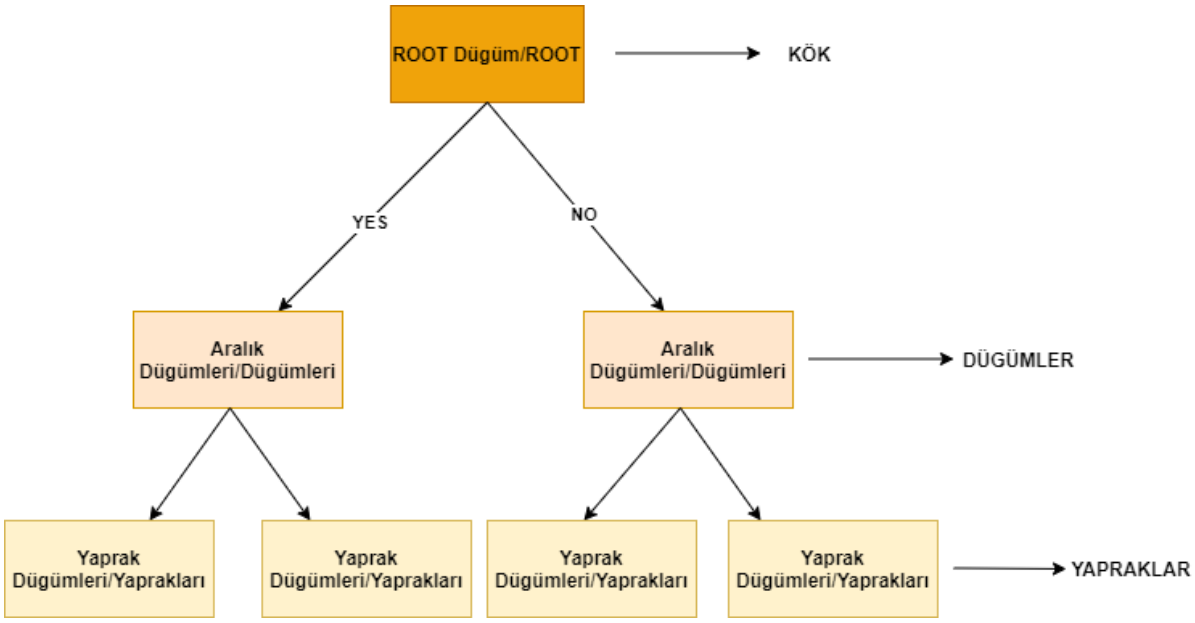
$$< x,y >= PolyKernel(x,y) \tag{4.2}$$

SVM modeli, yapay sinir ağını ve SVM'yi bağlamak için sigmoid çekirdek işlevini kullanır; iki katmanlı bir ileri beslemeli sinir ağına sahiptir. Destek Vektör Makinelerinin özellikleri; ampirik risk minimizasyonu, veri seti üzerindeki ortalama hata karesinin minimize edilmesiyle elde edilir

ve istatistiksel öğrenme teorisinde yapısal risk minimizasyonu çalışmasıdır. SVM'nin temel varsayımlarından biri, eğitim setindeki tüm örneklerin bağımsız ve benzer şekilde dağılmış olmasıdır. SVM, sınıflandırma ve regresyon veri kümeleri için uygundur [68].

4.2. Karar Ağaçları

Karmaşık veri setlerinde tercih edilmektedir. Genellikle sınıflandırma ve regresyon yöntemlerinde kullanılmaktadır. Karar ağacı yapısı Şekil 4.3'te gösterilmiştir.



Şekil 4.3. Karar ağacı yapısı

Karar ağacının tepesine kök (kök veya kök düğüm) adı verilir. Her gözlem, kök durumuna göre "evet" veya "hayır" olarak sınıflandırılır. Kök hücrenin alt kısmında düğümler bulunur. Düğüm sayısı arttıkça model daha karmaşık hale gelir. Son olarak ağacın en alt kısmında yapraklar bulunur yapraklar bize sonucu verir.

Kökü seçerken veri setinde en önemli etken seçilir. Köke bizler karar vermiyoruz, karar vermek için gini algoritmasını kullanabiliriz 4.3 denklemde gini algoritması verilmiştir. Gini değeri 0 ile 1 arasında bir değer elde eder, elde edilen değer 0 ne kadar yakınsa o kadar iyi bir sonuç elde edilmiş diyebiliriz.

$$Gini = 1 - \sum_j p_j^2 \tag{4.3}$$

4.3. K-En Yakın Komşu Algoritması

K-NN en çok kullanılan ve en kolay sınıflandırma algoritmasıdır. K-NN tembel bir öğrenme algoritmasıdır. Eğitim verilerini öğrenmez, verilerini ezberler. Tahmin yapılmak istendiğinde, tüm veri setine en yakın komşular aranır. Uzaklık hesaplama işleminde genelde öklid(4.4), manhattan(4.5), minkowski(4.6), chebyschev(4.7) ve dilca(4.8) fonksiyonları kullanılabilir.

$$\sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \tag{4.4}$$

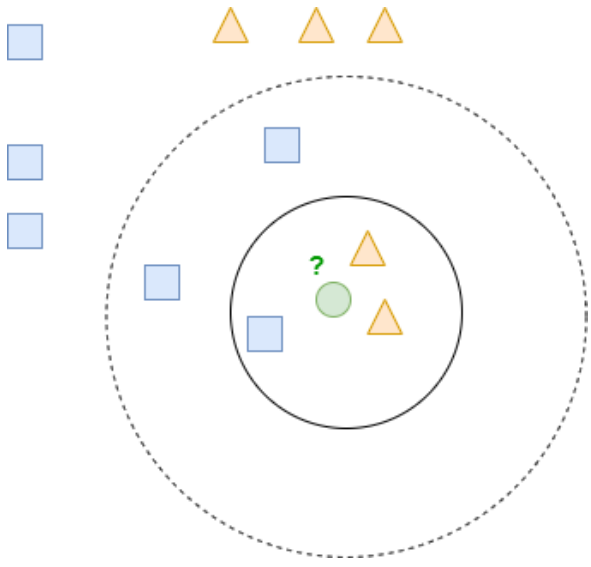
$$\left(\sum_{i=1}^{n}|x_i - y_i|\right) \tag{4.5}$$

$$\left(\sum_{i=1}^{n}|x_i - y_i|^p\right)^{1/p} \tag{4.6}$$

$$\lim_{p\to\infty}\left(\sum_{i=1}^{n}|x_i - y_i|^p\right)^{1/p} = \max_{i=1}^{n}|x_i - y_i| \tag{4.7}$$

$$\mathrm{SU}(symmetrical\ uncertainty) = 2x\left[\frac{IG}{H(Y)+H(X)}\right] \tag{4.8}$$

Sınıflandırma kısmında, tanımlı bir sabittir ve etiketlenmemiş bir vektör (sorgu veya test), bu sorgu noktasına en yakın k eğitim örnekleri arasında en çok görülen etiket seçilerek sınıflandırılır. K-NN sınıflandırma modeli Şekil 4.4'te verilmiştir.



Şekil 4.4. K-NN sınıflandırma modeli

4.4. Naive Bayes Algoritması

1812 yılında Thomas Bayes tarafından bulunmuştur. Koşullu olasılık hesaplama formülü 4.9 denkleminde verilmiştir.

$$P(A/B) = \frac{P(B/A)\,P(A)}{P(B)} \quad (4.9)$$

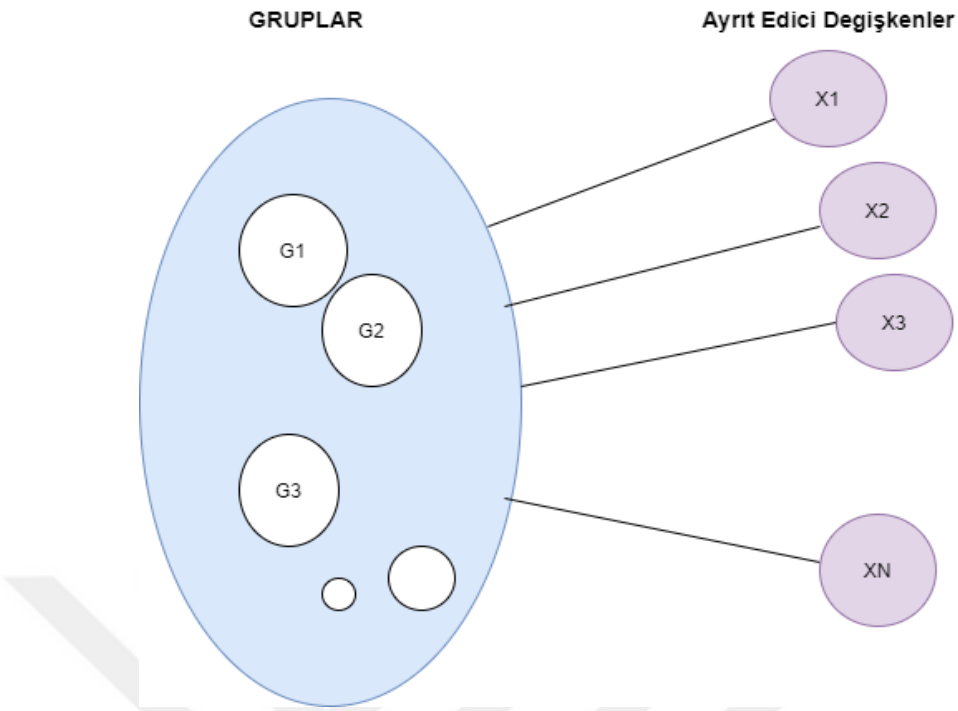
Naive Bayes algoritması da K-NN algoritması gibi tembel bir öğrenme algoritmasıdır ancak dengesiz veri kümelerinde çalışabilir. Algoritmanın çalışma yapısı bir değer için bütün durumların olasılığı hesaplanır ve olasılık değeri en yüksek olan algoritmaya göre sınıflandırılır. Eğitim kümesinde beklenmeyen bir değer var ise olasılık sonucu 0 verir yani tahmin yapamaz. Kullanım alanları; gerçek zamanlı tahmin, spam filtreleme, duyarlılık analizi ve metin sınıflandırma sistemleri bunlara örnektir.

4.5. Diskiriminant Analizi

Atakan ve dig. [69] çalışmalarında, diskriminant analizi, üstünden ölçüm alınan birim sonlu sayıda bilinen ayrımlı kitlelerden birine atanmasını gerçekleştiren istatistiksel analiz tekniği tanımlamışlardır. Bir hücre ait olduğu yapıdan farklı bir yapıya atandığında, atama sırasında aldığı gözlemlere göre hata oluşur. Diskriminant analizinde bu hataya hata oranı veya yanlış sınıflandırma olasılığı denir. Diskriminant analizinde atama işleminin minimum hata ile yapılması gerektiği anlatılmaktadır. [69].

Diskriminant fonksiyonları olarak adlandırılan denklemler, birbirine benzer grupların belirlenmesine izin vererek grupların ortak özelliklerini belirlemek için kullanılır. Grupları ayırt etmek için kullanılan özelliklere diskriminant değişkenler denir [70].

Diskriminant analizi genel olarak Şekil 4.5'te ki gibi gösterilebilir. Diskriminant analizinin amaçları; diskriminant analizi gruplar arasındaki farklılıkları analiz eder, gözlemlerin gruplara ayrılıp ayrılmadığını kontrol eder, yeni bireyler için grup üyelikleri saptanır.



Şekil 4.5. Diskriminant analizi

4.6. Lojistik Regresyon

Lojistik regresyon, sonuç belirler. Lojistik regresyon, bir veya daha fazla bağımsız değişken içeren veri kümelerini analiz etmek için kullanılır. Lojistik regresyon yalnızca 1 veya 0 değerini içerir. 1 değeri doğru olarak kabul edilir 0 değeri ise yanlış olarak kabul edilmektedir. Regresyon modelinde maksimum olasılık tahmini yapılır, ancak verilerin dağıtımı hakkında varsayımlarda bulunur. Örnek olarak varsayılan sınıf için kadın 1'e en yakın değeri ve diğer sınıf da erkek 0 yakın bir değer sonuçlandırılır. Lojistik regresyon denklemleri 4.10, 4.11 ve 4.12'de gösterilmiştir.

$$P = \frac{e^{a+bX}}{1+e^{a+bX}} \tag{4.10}$$

$$\text{odds} = \frac{p}{1-p} \tag{4.11}$$

$$\text{logit}(p) = \ln\left(\frac{p}{1-p}\right) \tag{4.12}$$

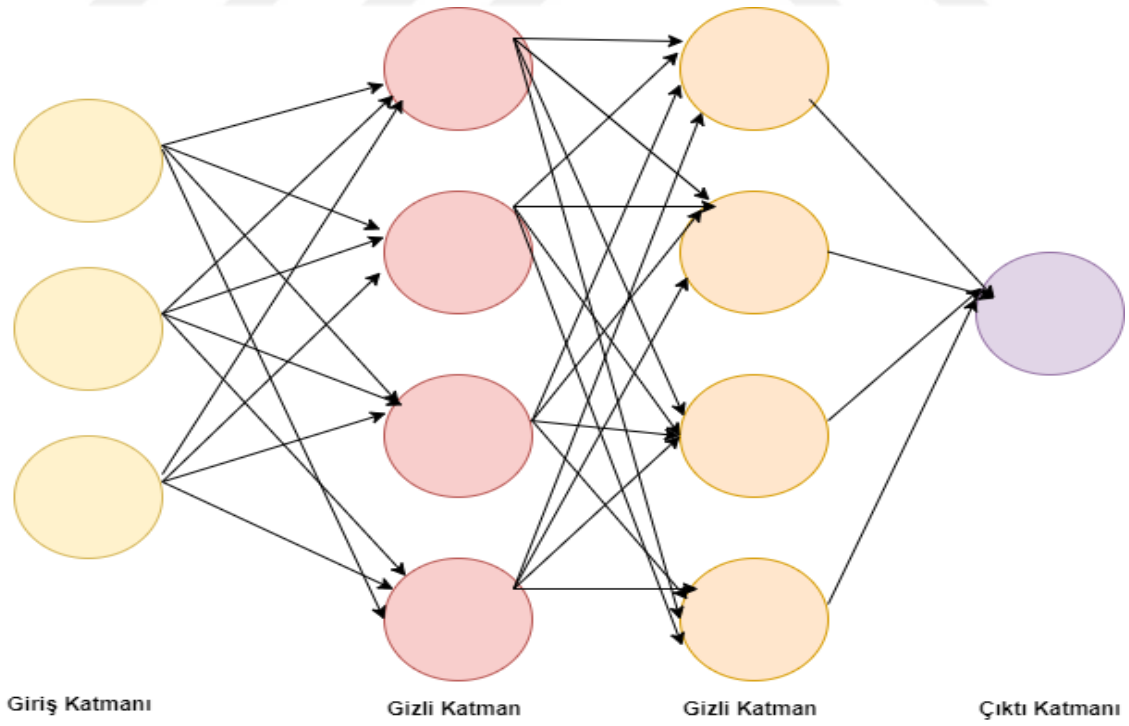
4.7. Yapay Sinir Ağları

İnsan beyninin gelişmiş özellikleri, bilim insanlarını onu incelemeye ve beynin nörofiziksel yapısından esinlenerek matematiksel bir model oluşturmaya zorlamıştır. Beynin tüm davranışlarını belirlemek için fiziksel bileşenlerin doğru bir şekilde modellenmesi gerektiği fikriyle farklı yapay hücre ve ağ modelleri geliştirilmiştir. Bu sayede günümüz bilgisayar algoritmalarının hesaplama yönteminden farklı bir yapay sinir ağı ortaya çıkmıştır [71].

Sinir ağları oluşturulurken insan beyni baz alınmıştır. Sinir ağları insan veya istatiksel standartlara göre imkânsız olan sorunları çözer. Sinir ağları daha fazla bilgi elde ettikçe daha iyi sonuçlar elde ederler.

Yapay Sinir Ağlarının (YSA) bilgi işleme ve hesaplama gücünü, koşut dağılmış modelinden, Öğrenme ve genelleme yeteneğinden kaynaklandığı söylenir. Genelleme, öğrenme veya eğitim sırasında karşılaşılmayan girdilere YSA'nın uygun yanıtı olarak tanımlanır. Bu özellikler yapay sinir ağlarının karmaşık problemleri çözme yeteneğini göstermektedir. [72].

Yapay sinir ağları Şekil 4.6.'da gösterildiği gibi tanımlanabilir. Katmandaki her düğüm, diğer katmandaki bütün düğümlere bağlıdır. Gizli katman sayısı artırılarak yapay sinir ağları derinleştirilebilir. Düğümlerin denklemi 4.13 ve 4.14'te verilmiştir. Sinir ağlarını eğitmek, tüm uçlarla ilişkisi ağırlıklar öğrenilmelidir.



Şekil 4.6. Sinir ağları

$$z = f(x.w) = f(\sum_{i=1}^{n} x_i w_i) \quad (4.13)$$

$$x \in d_{1xn}, \omega \in d_{nx1} z \in d_{1x1} \quad (4.14)$$

Giriş Katmanı: Bu, dış dünyadan gelen girdinin yapay sinir ağına girdiği katmandır. Bu katmanda, dış dünyadan giriş sayısı kadar birim vardır ve giriş genellikle herhangi bir işlem yapılmadan alt katmana aktarılır [16].

Gizli (Ara) Katman: Giriş katmanından gelen bilgiler bu katmana ulaşır. Ara katmanların sayısı ağdan ağa değişebilir. Bazı yapay sinir ağları ara katmanlara sahip değildir ve bazı yapay sinir ağları birçok ara katmana sahip olabilir. Orta katmandaki nöron sayısının girdi ve çıktı sayısıyla ilgisi yoktur. Birden fazla ara katmanı olan bir ağda, ara katmanlar arasındaki hücre sayısı da farklı olabilir. Orta katmandaki ve bu katmanlardaki nöron sayısındaki artış, hesaplama karmaşıklığını ve zamanı artıracak olsa da daha karmaşık problemleri çözmek için yapay sinir ağları da kullanılabilir. Bu katman sayısını belirlerken bazı varsayımlar olsa da henüz kesin bir bilgi yoktur. Problemin amacına ve uygulama alanına göre en uygun nöron tabakası ve sayısını seçmeye çalışarak en uygun nöron tabakasını ve sayısını belirlemektedir. [16].

Çıkış Katmanı: Orta katmandan gelen bilgileri işleyerek ağ çıktısı üreten bir katmandır. Bu katmanda üretilen çıktı, dış dünyaya gönderilir. Geri bildirim ağında, katmanda üretilen çıktı yeniden kullanılarak ağın yeni ağırlık değeri hesaplanır [16].

4.8. Gradient Boosting Machine Algoritması

Gradient Boosting Machine (GBM) algoritması, güçlendirme algoritması olarak bilinmektedir. Güçlendirme zayıf olan algoritmaları güçlü öğrenmeye dönüştüren bir algoritmadır. GBM, birçok modeli sırasıyla, ekleyerek eğitir. GBM algoritması kayıp fonksiyonundaki gradyanları kullanarak eksikleri belirler.

4.9. Extreme Gradient Boosting Algoritması

Extreme Gradient Boosting (XGBOOST), GBM algoritmasının yenilenmiş yüksek performanslı halidir. Bu algoritmanın en önemli özelliği yüksek tahmin gücü, fazla öğrenmenin önüne geçmesi, boş verileri yönetmesidir.

4.10. Light Gradient Boosting Machine Algoritması

Light GBM (LGBM), ağaç tabanlı öğrenme algoritması kullanan gradyan artırma çerçevesidir. Bu algoritma da ağaçlar yatay olarak büyütülür. Büyüme için maksimum delta kaybını seçer. LGBM hızlı olduğu için büyük boyutlu veri setlerini işler ve çalıştırmak için az işlemci gücü kullanır.

4.11. Category Boosting Algoritması

Category Boosting (Catboost) algoritması, karar ağaçlarında gradyan artırmak için kullanılan bir algoritmadır. Yandex araştırmacıları tarafından geliştirilen bir algoritmadır. Catboost, tahmin süresi fazla olan bir algoritmadır.

4.12. Çok Katmanlı Algılayıcı Algoritması

Çok katmanlı Algılayıcı (Multi Layer Perception - MLP) girdi ve çıktı arasındaki eşleşmenin doğrusal olmadığı bir sinir ağıdır. MLP, giriş ve çıkış katmanlarına ve birçok nöron birden fazla katmana sahiptir.

4.13. Adaboost Algoritması

Adaboost, bütün gözleme eşit ağırlık verilen bir karar ağacını eğitir. Sınıflandırılması zor olan verilerin ağırlıkları artırılır, sınıflandırılması kolay olan verilerin ağırlıkları azaltılır. İkinci ağaç ağırlıklı veriler üzerinde büyütülür. Buradaki amaç ilk ağacın tahminlerini geliştirmektir. Burada oluşan model ilk ağaç+ ikinci ağaçtır. Oluşturulan iki ağaç üzerinden sınıflandırma hatası hesaplanır ve düzeltilen artıkları tahmin etmek için üçüncü ağaç oluşturulur. Bu işlem belirli sayıda tekrar ettikten sonra ağaçların iyi sınıflandırılamamış gözlemi sınıflandırmaya yardımcı olur.

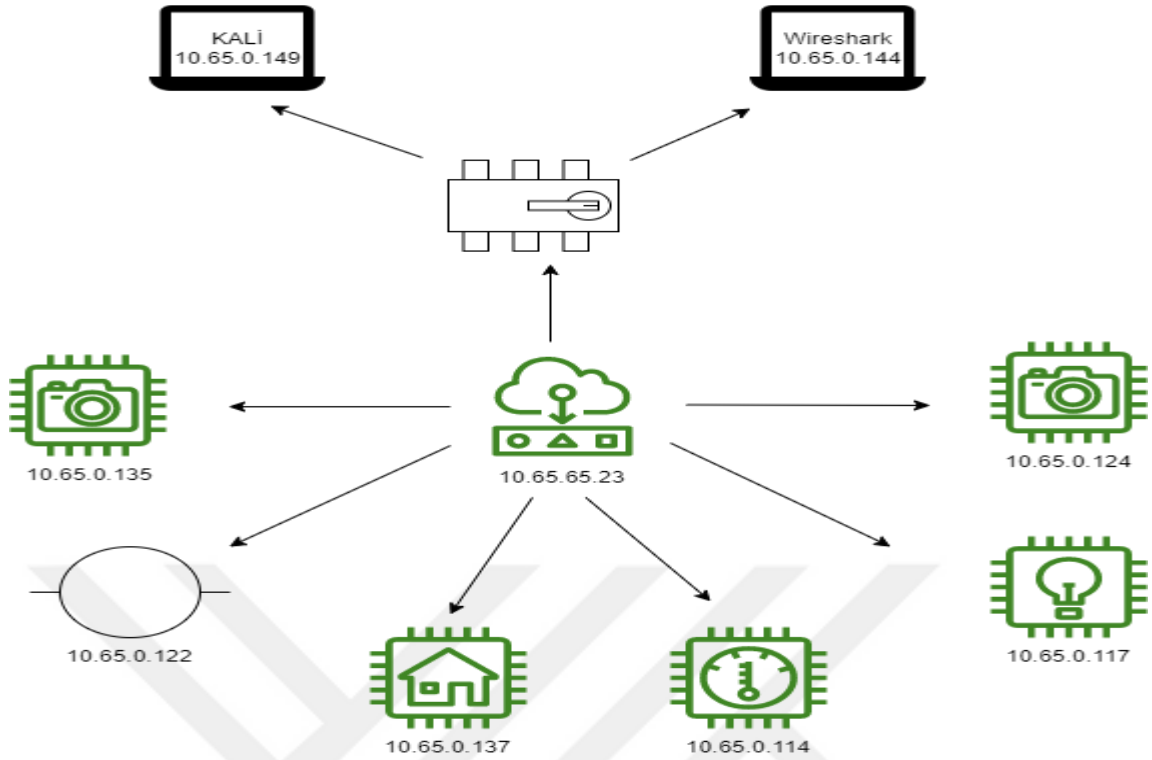
5. NESNELERİN İNTERNETİNDE XGBOOST İLE TESPİT YÖNTEMİ

5.1. Giriş

Bu çalışmada akıllı ev platformlarına yapılabilecek muhtemel saldırı türlerinin tespit edilebilmesi için makine öğrenmesi tabanlı bir yöntem önerilmiştir. Akıllı ev platformunu oluşturmak için Home Assistant teknolojisini kullanan bir laboratuvar kurulmuştur. Bu laboratuvar ortamında IoT (Nesnelerin İnterneti) cihazlarına Brute Force FTP, Brute Force SSH, DoS HTTP Flood, DoS ICMP Flood, DoS Syn Flood, Syn Scan ve UDP Scan olmak üzere yedi saldırı gerçekleştirilmiştir. Toplanan veri seti normal paketlerle birlikte sekiz sınıftan oluşmaktadır. Sekiz sınıf için toplamda 435815 örnek elde edilmiştir. Toplanan veri setine XGBOOST algoritması uygulanarak Hold-out 80:20 eğitim test verisi için %92,55 ve Hold-out 70:30 eğitim test verisi için %92,55 ve %92,49 doğruluk hesaplanmıştır. XGBOOST algoritması ile elde edilen sonuçlar diğer sınıflandırma algoritmaları ile karşılaştırılmış ve XGBOOST algoritmasının başarısının yüksek olduğu görülmüştür.

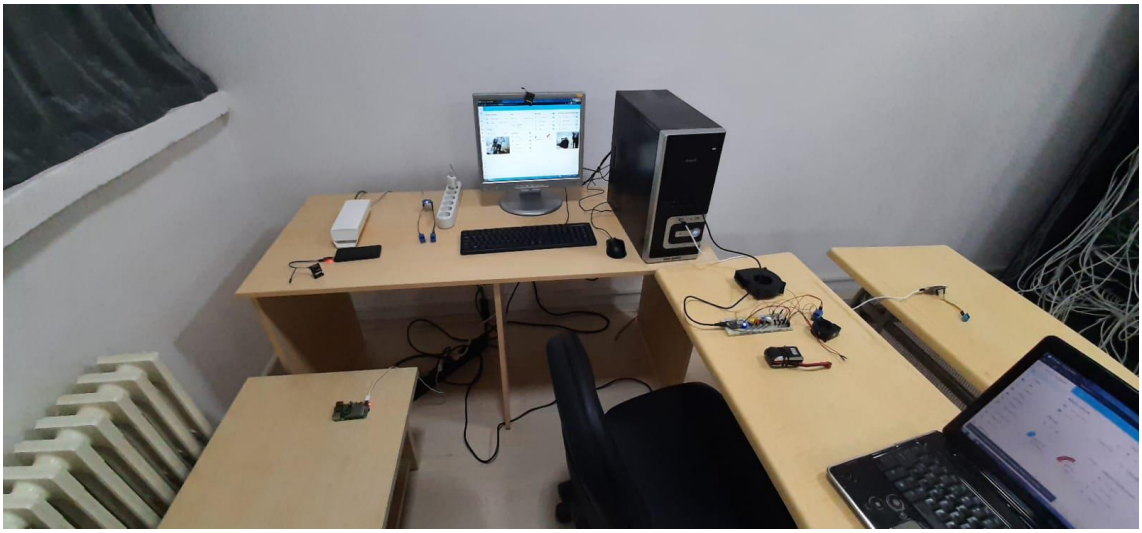
5.2. Materyal

Bu çalışmada, IoT tabanlı akıllı ev laboratuvarından veri seti toplamak için Şekil 5.1'de verilen mimari oluşturulmuştur. Laboratuvar ortamımızda Linux işletim sistemli bir makine, ağda ki paketleri toplamak için wireshark yüklü olan Windows işletim sistemi yüklü bilgisayar, akıllı switch, IoT cihazları ve IoT cihazlardan gelen verileri toplanmak için AP kullanılmıştır.

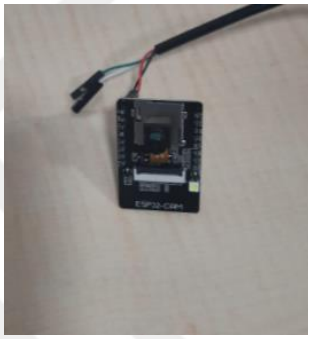


Şekil 5.1. IoT akıllı ev laboratuvar mimarisi

Şekil 5.1'de önerilen test ortamı proje kapsamında alınan IoT ürünleri ile oluşturulmuştur. Akıllı ev ortamı oluşturularak sensor düğümlerinden oluşan bir laboratuvar alt yapısı kurulmuştur. Bu çalışma kapsamında oluşturulan akıllı ev laboratuvar görüntüleri Şekil 5.2'de görülmektedir.



(a)

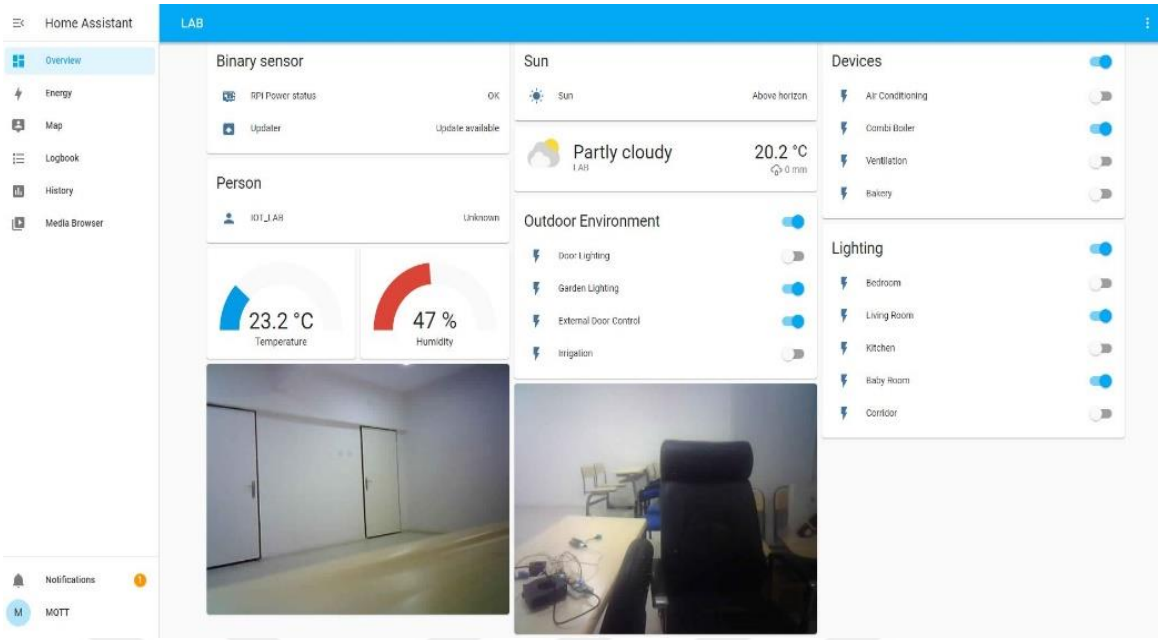


(b) (c) (d)

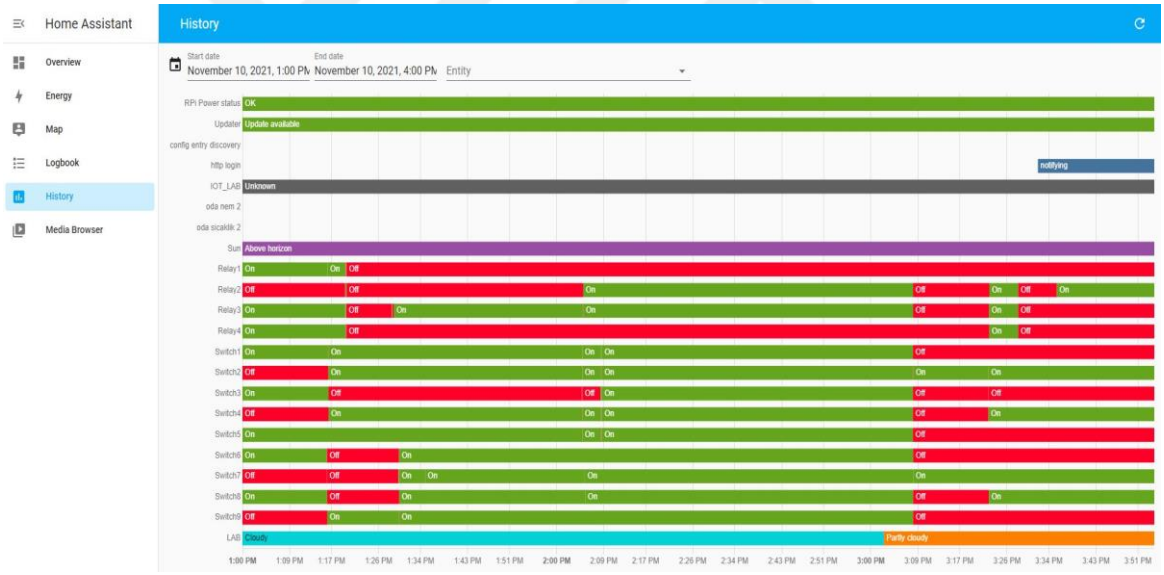
Şekil 5.2. Oluşturulan akıllı ev laboratuvar görüntüleri

Şekil 5.2'de görülen akıllı ev ortamının uzaktan izlenmesi ve kontrol edilebilmesi için "Home Assistant" teknolojisi kullanılmıştır.

Home Assistant lokalde kontrolü ve gizliliği merkezine koyan açık kaynak kodlu bir akıllı ev otomasyonu teknolojisidir. Açık kaynak olması sayesinde tek bir kurum tarafından değil bu alanda ilgili olan herkes tarafından geliştirilebilmektedir. Bir Raspberry Pi üzerinde ya da mevcut sunucular üzerine kolaylıkla kurulabilmekte ve kullanılabilmektedir. Şekil 5.2'de (d) görüldüğü akıllı ev laboratuvar ortamı kurulurken Raspberry Pi kullanılmıştır. Bir Raspberry Pi'ye sahip olduktan sonra micro-SD vasıtasıyla Raspberry Pi tanıtılarak kurulum aşaması tamamlanmıştır.
Proje kapsamında kurulan deneysel ortam üzerinde Home Assistant uygulaması sonuçları Şekil 5.3'te gösterilmiştir. Home Assistant üzerinden IoT cihazlar yönetilmektedir Şekil 5.4'te gösterildiği gibi "on" ve "off" butonları ile yönetilebilmektedir. Aynı zamanda ortamın nem ve sıcaklık değerlerinin de kontrolü sağlanabilmektir. Şekil 5.5'te gösterilmiştir.



Şekil 5.3. Akıllı ev laboratuvar ortamında Home Assistant uygulaması sonuçları



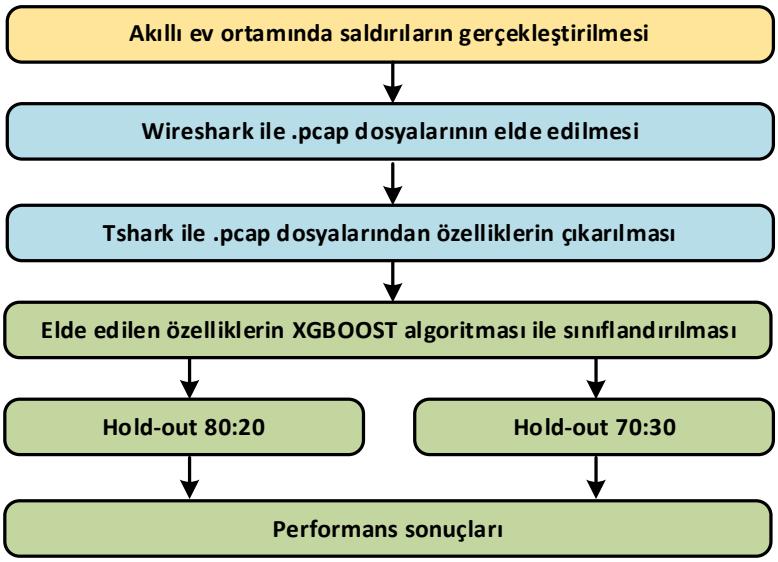
Şekil 5.4. Home Assistant'a bağlı cihazların açma ve kapama bilgisi

Şekil 5.5. Home Assistant sıcaklık ve nem değerleri

Akıllı ev laboratuvar ortamı kurulurken wifi modülleri(esp1, esp2, esp32) kullanılmıştır. Modüllerin Home Asistant ile iletişiminin saglanması için esp1, esp2, esp32 kartları ve mqtt protokolü kullanılmıştır. Esp modüllerinin kullanılmasının sebebi IoT cihazlarda ki internet trafigini izlemek ve cihazların internet ile iletişimini saglamak amaçlanmıştır. MQTT protokolü ise IoT sistemlerde kullanılan bir iletişim protokolüdür.

5.3. Önerilen Yöntem

Bu çalışmada akıllı ev ortamlarında oluşabilecek saldırıların hızlı ve yüksek doğrulukla tespit edilebilmesi için hafifsıklet bir yöntem önerilmiştir. Önerilen yöntemin blok şeması Şekil 5.6'da verilmiştir.

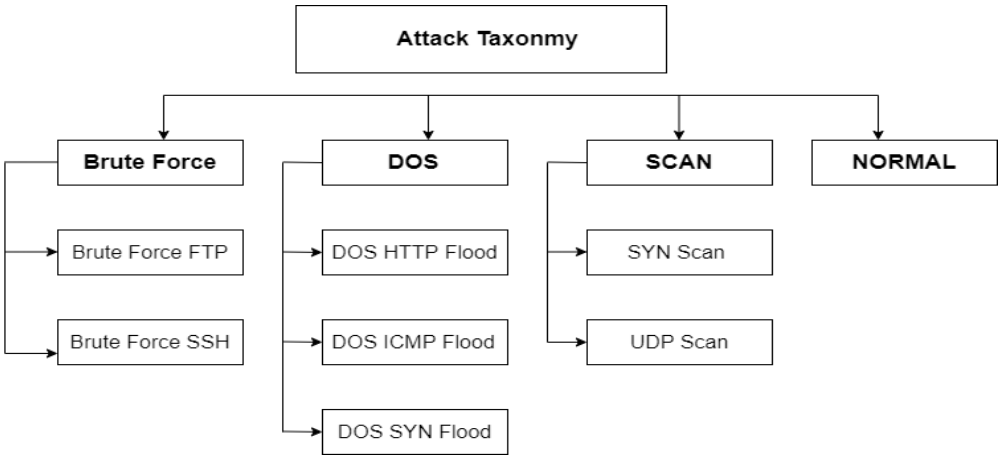


Şekil 5.6. Önerilen yöntemin blok şeması

Şekil 5.6'te de görülebileceği gibi önerilen yöntem üç aşamadan oluşmaktadır. İlk olarak akıllı ev ortamında saldırıların gerçekleştirilmesidir. Daha sonra veri setinin elde edilmesi ve XGBOOST algoritması kullanılarak sınıflandırılması aşamalarından oluşmaktadır.

5.4. Akıllı Ev Ortamında Saldırıların Gerçekleştirilmesi

IoT laboratuvar da saldırılar gerçekleştirilirken 10.65.0.194 ip adresli Linux işletim sistemi üzerinden brute force, dos ve scan olmak üzeri 3 farklı saldırı gerçekleştirilmiştir. Bu saldırılar Brute Force FTP, Brute Force SSH, DoS HTTP Flood, DoS ICMP Flood, DoS Syn Flood, Normal, Syn Scan ve UDP Scan olmak üzere 8 farklı şekilde gerçekleştirilmiştir. Bu saldırılar Şekil 5.7'de gösterilmiştir.



Şekil 5.7. Saldırı taksonomisi

Şekil 5.7'de verilen 'Brute Force' saldırılarının gerçekleştirilmesi için 'xHydra' aracı kullanılmıştır. 'DoS' saldırılarının uygulanması için 'Hping3' ve 'Scan' saldırılarının gerçekleştirilmesi için 'NMAP' araçları kullanılmıştır.

5.5. Veri Setinin Elde Edilmesi

Bu aşamada, ham ağ trafik paketleri toplanmıştır. Bu işlem, toplanan .pcap dosyalarından özellik çıkarılmasını sağlamaktadır. Bu çalışmada IoT laboratuvar ortamında gerçekleştirilen saldırılar wireshark ile dinlenmiştir. Wireshark ile elde edilen. pcap dosyalarından özellik çıkarılmıştır. .pcap dosyalarından özellik çıkarmak için tshark.exe kullanılmıştır. Çıkarılan özelliklerle ilgili bilgiler Tablo 5.1'de verilmiştir.

Tablo 5.1. Saldırı paketlerinden elde edilen özellikler

	Özellik adı	Özellik tanımı
1	ip.len	Ip adres uzunluğu
2	ip.flags.df	Datagramın parçalanma değeri
3	ip.flags.mf	Datagramın ek parça değeri
4	ip.ttl	Datagramın ömrünün değeri
5	ip.proto	Sonraki kapsüllenmiş protokol değeri
6	ip.version	Ip versiyon değeri
7	udp.port	UDP portu
8	tcp.windows_size	TCP pencere uzunluğu
9	tcp.ack	TCP onay numarası
10	tcp.seq	TCP sıra numarası
11	tcp.len	TCP başlık uzunluğu
12	tcp.stream	TCP akış değeri
13	tcp.analysis.ack_rtt	ACK'nin yakalanması arasındaki zaman değeri
14	tcp.reassembled.length	TCP birleştirme değeri uzunluğu
15	tcp.time_relative	TCP oturumunda ilk çerçeveyi aldığı andan geçen süre değeri
16	tcp.time_delta	TCP oturumunda önceki ve mevcut paket arasında geçen süre değeri
17	class	Saldırı yapılan değerler sınıflandırılmıştır.

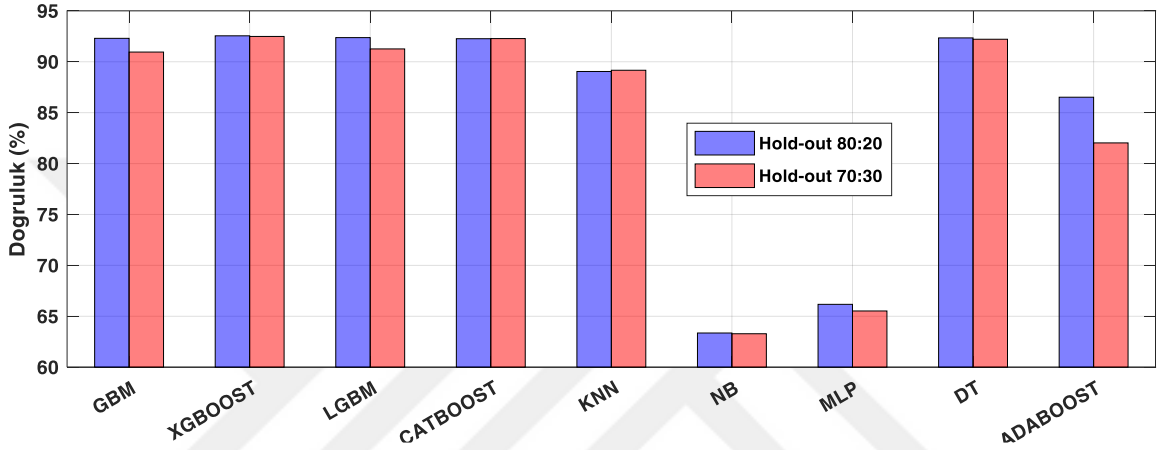
Bu veri setinde Tablo 1'de belirtilen 16 tane özellik ile 8 sınıf (Brute Force FTP, Brute Force SSH, DoS HTTP Flood, DoS ICMP Flood, DoS Syn Flood, Syn Scan, UDP Scan ve Normal) oluşturulmuştur. Oluşturulan bu veri seti XGBOOST algoritması kullanılarak sınıflandırılmıştır.

5.6. Sınıflandırma

XGBoost algoritması, gradyan artırma çerçevesi kullanan karar ağacı tabanlı makine öğrenme algoritmasıdır. XGBoost yapılandırılmış verileri içerir. İçerdiği yapılandırılmış veriler ile birçok algoritmayı geride bırakmaktadır. XGBoost Washington Üniversitesi'nde araştırma projesi olarak geliştirilen bir algoritmadır. XGBoost geniş bir uygulama alanı bulunmaktadır. Regresyon,

sınıflandırma, sıralama gibi problemleri çözmek için kullanılır. En kısa zaman da daha az kaynak tüketimi kullanarak yüksek değerli sonuçlar elde edilir. XGBOOST'un diğer algoritmalara göre daha iyi performans göstermesinin sebebi, gradyan iniş mimarilerini kullanarak zayıf öğrenenlere artırma ilkesi uygulanmasıdır.

Önerilen yöntemin belirlenmesi için GBM, XGBOOST, LGBM, CATBOOST, KNN, NB, MLP, DT, ADABOOST algoritmaları kullanılmıştır. Bu algoritmalar kullanılarak Hold-out 80:20 ve Hold-out 70:30 eğitim ve test verileri ile Şekil 5.8'de verilen sonuçlar hesaplanmıştır.

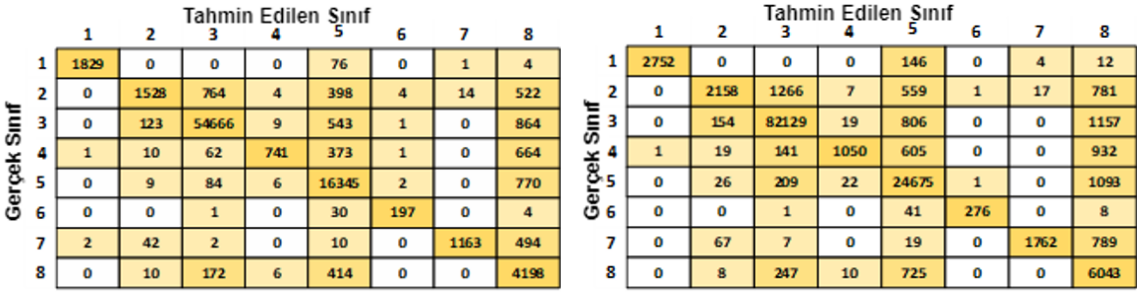


Şekil 5.8. GBM, XGBOOST, LGBM, CATBOOST, KNN, NB, MLP, DT, ADABOOST algoritmaları ile elde edilen sonuçlar

Şekil 5.8'de verilen sonuçlar incelendiğinde XGBOOST algoritmasının en yüksek doğruluk elde ettiği görülmüştür. XGBOOST algoritması ile Hold-out 80:20 eğitim test verisi için %92,55 ve Hold-out 70:30 eğitim test verisi için %92,55 ve %92,49 doğruluk hesaplanmıştır. Böylece bu çalışmada XGBOOST algoritması tercih edilmiştir.

5.7. Deneysel Sonuçlar

Bu çalışma Python 3.10 programı kullanılarak geliştirilmiştir. Oluşturulan akıllı ev platformu ile veri seti toplanmış ve özellik çıkarımı yapılmıştır. Elde edilen özellikler GBM, XGBOOST, LGBM, CATBOOST, KNN, NB, MLP, DT, ADABOOST sınıflandırıcılar ile sınıflandırılmıştır. Bu sınıflandırıcılar içerisinde en yüksek doğruluk XGBOOST ile hesaplanmıştır. XGBOOST sınıflandırıcısı sonucunda elde edilen hata matrisi Şekil 5.9'de sunulmuştur.



a) 80:20 eğitim test sonucu b) 70:30 eğitim test sonucu

Şekil 5.9. XGBOOST sınıflandırıcısı sonucunda elde edilen hata matrisi

XGBOOST sınıflandırıcısı kullanılarak Hold-out 80:20 ve Hold-out 70:30 eğitim test sonuçlarında elde edilen sınıf doğrulukları Tablo 5.2'de gösterilmiştir.

Tablo 5.2. XGBOOST sınıflandırıcı ile elde edilen sınıf doğrulukları

Sınıf	Sınıf adı	Doğruluk (%)	
		Hold-out 80:20	Hold-out 70:30
1	Brute Force FTP	95.75	94.44
2	Brute Force SSH	47.24	45.06
3	DoS HTTP Flood	97.26	97.46
4	DoS ICMP Flood	40.01	38.20
5	DoS SYN Flood	94.94	94.80
6	Normal	82.77	84.66
7	SYN Scan	67.89	66.64
8	UDP Scan	87.45	85.92

Tablo 5.2'de gösterildiği gibi Hold-out 80:20 eğitim test verileri kullanılarak en yüksek doğruluk %97,26 ile DoS HTTP Flood sınıfı için hesaplanmıştır. En düşük doğruluk ise %40.01 ile DoS ICMP Flood sınıfında elde edilmiştir. Hold-out 70:30 eğitim test verileri içinde en yüksek ve en düşük doğruluklar sırasıyla DoS HTTP Flood ve DoS ICMP Flood sınıflarında hesaplanmıştır.

5.8. Bölüm Değerlendirmesi

Nesnelerin interneti günümüzde birçok alanda kullanılmaktadır. Bu teknolojiler ile nesneler uzaktan izlenmekte ve yönetilmektedir. Bu teknolojinin uzaktan yönetilebilmesi beraberinde siber saldırıları da getirmektedir. Bu çalışmada IoT saldırıları türlerinin tespiti için XGBOOST sınıflandırıcı kullanılmıştır. Akıllı ev platformu oluşturulmuş ve veri seti toplanmıştır. Toplanan veri setinde 16 özellik olmak üzere toplamda 435815 örnek mevcuttur. Bu veri seti Brute Force FTP, Brute Force SSH, DoS HTTP Flood, DoS ICMP Flood, DoS Syn Flood, normal, Syn Scan ve

UDP Scan olmak üzere sekiz sınıftan oluşmaktadır. XGBOOST sınıflandırıcısı kullanılarak Hold-out 80:20 eğitim test verisi için %92,55 doğruluk hesaplanmıştır.

6. NESNELERİN İNTERNETİNDE KARAR AĞACI TABANLI SALDIRI TESPİT YÖNTEMİ

6.1. Giriş

Bilgisayar ve ağ teknolojilerindeki gelişmeler internet teknolojisini de olumlu yönde etkilemiştir. İnternetin gelişmesiyle birlikte IoT (Nesnelerin İnterneti) kavramı da gelişmiştir. Günümüzde IoT cihazları birçok alanda kolaylık sağlamaktadır. Bu kolaylıklar insanların yaşam kalitesini artırmaktadır. İnsanlar akıllı şehirleri, akıllı evleri ve diğer platformları uzaktan izlemek ve yönetmek istiyor. Uzaktan izlenen ve yönetilen uygulamalar, avantajlarının yanı sıra güvenlik sorunları gibi sorunları da beraberinde getirmektedir. IoT platformlarının artmasıyla saldırganların hedef noktası haline geldi. Bu tür saldırıları tespit etmek ve güvenlik açıklarını önlemek, IoT teknolojisinin kullanım oranını daha da artıracaktır. Bu çalışmada, Bot-IoT veri seti kullanılarak karar ağacı tabanlı saldırı tespiti gerçekleştirilmiştir. Dokuz saldırı türü için 3668443 veri kullanıldı. Karar Ağacı (DT) ile %97,43 doğruluk hesaplanmıştır.

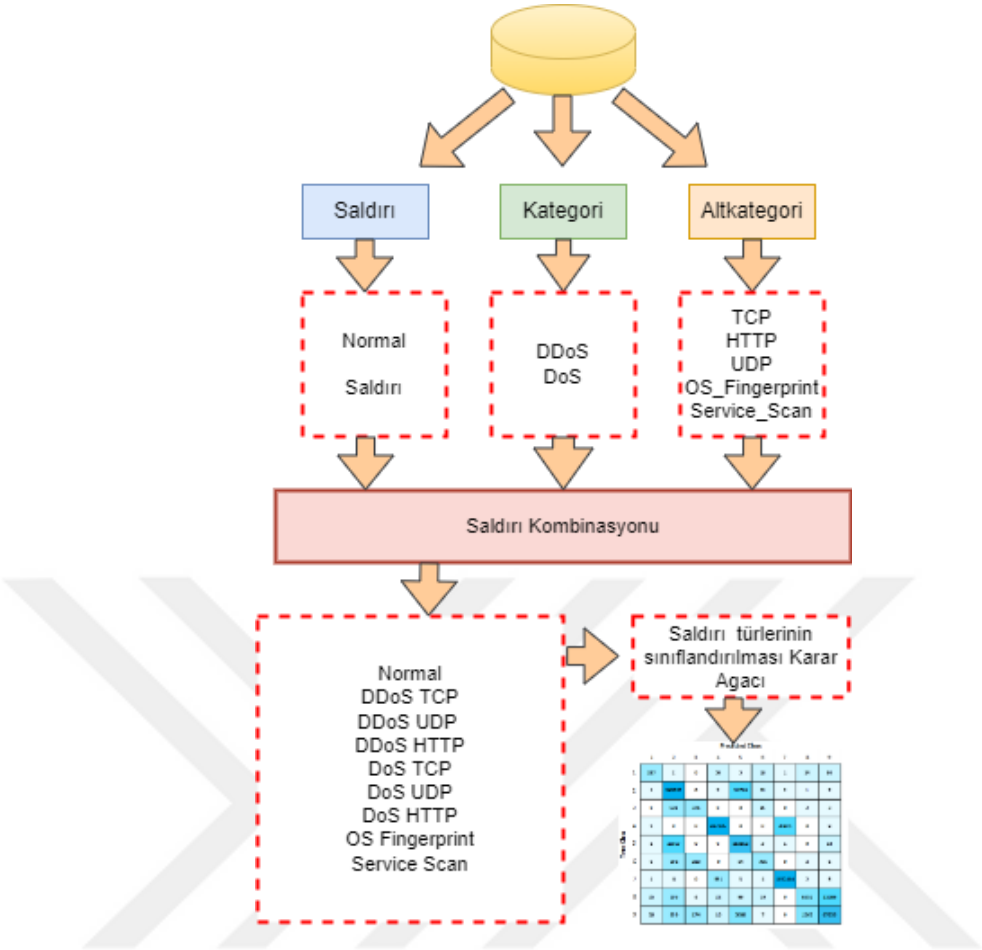
6.2. Materyal ve Metot

Bot-IoT veri seti bu çalışmada kullanıldı [19]–[37]. Bot-IoT veri seti laboratuvar ortamında oluşturulmuştur. Pcap dosyaları Argus aracıyla toplandı ve düzenlendi. Bot-IoT veri seti ile birçok özellik elde edilmiştir. Koroniotis ve diğ. [19] Bot-IoT, veri kümesindeki ilk 10 özelliği seçti ve kullandı. Bu çalışmada Bot-IoT veri setinde seçilen ilk 10 özellik kullanılmıştır. İlk 10 özellik ve açıklamaları Tablo 6.1'de gösterilmiştir.

Tablo 6.1. Bot-IoT veri kümesinin özellikleri ve açıklamaları [19]

Özellik	Tanım
srate	Saniyede kaynaktan hedefe paket sayısı
drate	Saniyede hedeften kaynağa paket sayısı
rate	İşlemde saniyede toplam paket sayısı
max	Birleştirilmiş kayıtların maksimum süresi
state_number	Özellik durumunun sayısal gösterimi
mean	Birleştirilmiş kayıtların ortalama süresi
min	Birleştirilmiş kayıtların minimum süresi
stddev	Birleştirilmiş kayıtların standart sapması
flgs_number	Özellik bayraklarının sayısal gösterimi
seq	Argus sıra numarası

Tablo 6.1'de sunulan Bot-IoT veri kümesindeki ilk 10 özellik kullanıldı. Önerilen yöntemin blok diyagramı Şekil 6.1'de görülebilir.



Şekil 6.1. Bot-IoT veri kümesi için önerilen yöntemin blok diyagramı

Şekil 6.1'de görüldüğü gibi, ilk 10 özellik karar ağacına göre sınıflandırılmıştır. Bot-IoT veri setinde "saldırı", "kategori" ve "alt kategori" sonuçları bulunmaktadır. "Saldırı" kategorisinde normal ve saldırı sınıfları bulunmaktadır. "Kategori" içerisinde DDoS ve DoS sınıfları bulunmaktadır. "Alt kategori" de TCP, HTTP, UDP, OS_Fingerprint ve Service_Scan sınıfları bulunmaktadır. Literatürde veri seti "saldırı", "kategori" ve "alt kategori" sonuçlarına göre ayrı ayrı sınıflandırılmaktadır. Bu çalışmada "saldırı", "kategori" ve "alt kategori" sonuçları birleştirilerek 9 sınıf oluşturulmuş ve sınıflandırılmıştır. Elde edilen sınıf türleri ve örnek sayıları Tablo 6.2'de gösterilmiştir.

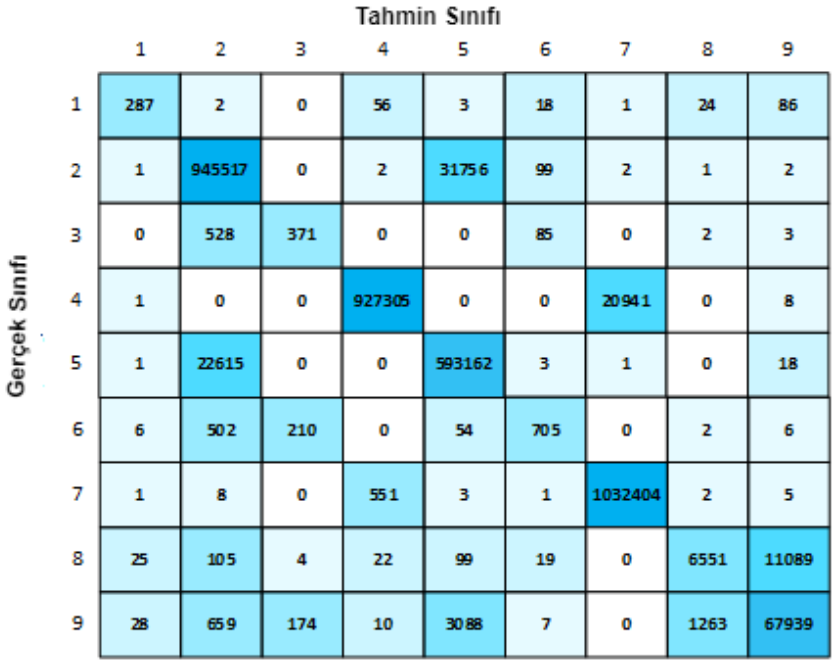
Tablo 6.2. "Saldırı", "kategori" ve "alt kategori" sonuçlarının birleştirilmesiyle elde edilen yeni sınıflar

Sınıf Sayısı	Sınıf Türü	Örnek Sayısı
1	Normal	477
2	DDoS TCP	977380
3	DDoS HTTP	989
4	DDoS UDP	948255
5	DoS TCP	615800
6	DoS HTTP	1485
7	DoS UDP	1032975
8	OS Fingerprint	17914
9	Service Scan	73168

Bu çalışmada Bot-IoT veri setini sınıflandırmak için MATLAB programında Classification Learner Toolbox kullanılmıştır. Veri kümesinin büyük boyutu, önerilen yöntemin test süresini etkiler. Bu nedenle derin öğrenme gibi algoritmalar yerine hızlı ve hesaplama karmaşıklığı düşük olan Karar Ağacı algoritması tercih edilmektedir.

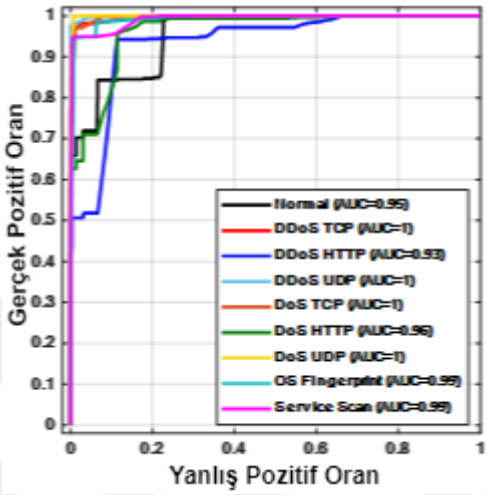
6.3. Deneysel Sonuçlar

Bu çalışmada kullanılan Karar Agacı sınıflandırıcısında "Split Criterion" parametresi "gdi" ve "Max Number of Splits" parametresi "100" olarak seçilmiştir. Sınıflandırma sonucunda elde edilen Hata Matrisi Şekil 6.2'de gösterilmiştir.



Şekil 6.2. Karar Ağacı sınıflandırıcı ile elde edilen Hata Matrisi sonuçları

Tüm sınıfların ROC eğrileri ve AUC değerleri Şekil 6.3'te görülebilir. Şekil 6.3'te görüldüğü gibi en iyi sonuçlar "DDoS TCP", "DDoS UDP", "DoS TCP" ve "DoS UDP" sınıfları için hesaplanmıştır. Doğruluk, Kesinlik, Geri Çağırma, Geometrik Ortalama ve F1-Skor değerleri, önerilen yöntemin 100 iterasyonu çalıştırılarak hesaplanmıştır. Doğruluk, Kesinlik, Geri Çağırma, Geometrik Ortalama ve F1-Skor değerlerinin Maksimum, Minimum, Ortalama ve Standart Sapma değerleri Tablo 6.3'te verilmiştir.

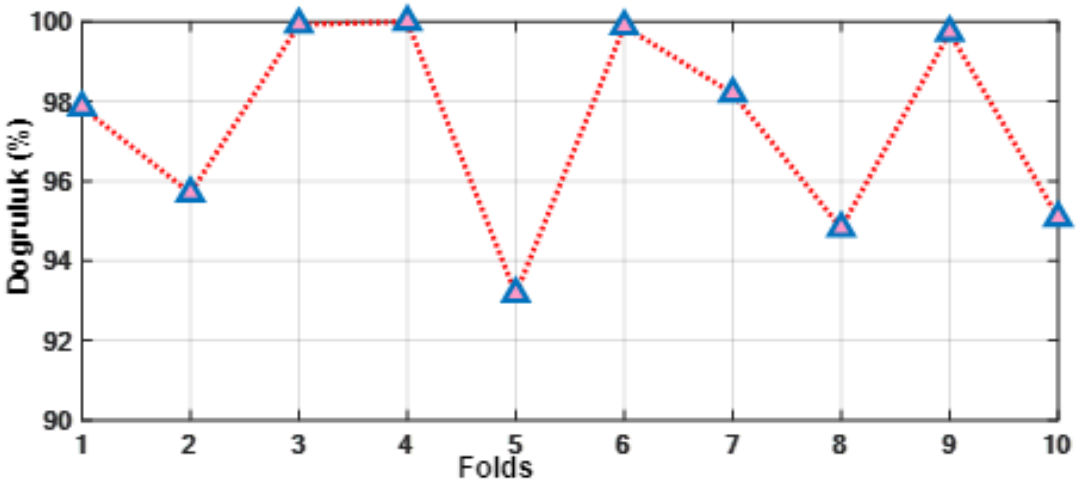


Şekil 6.3. Tüm sınıfın ROC Eğrisi

Tablo 6.3. Önerilen yöntemin 100 iterasyon performans değerleri

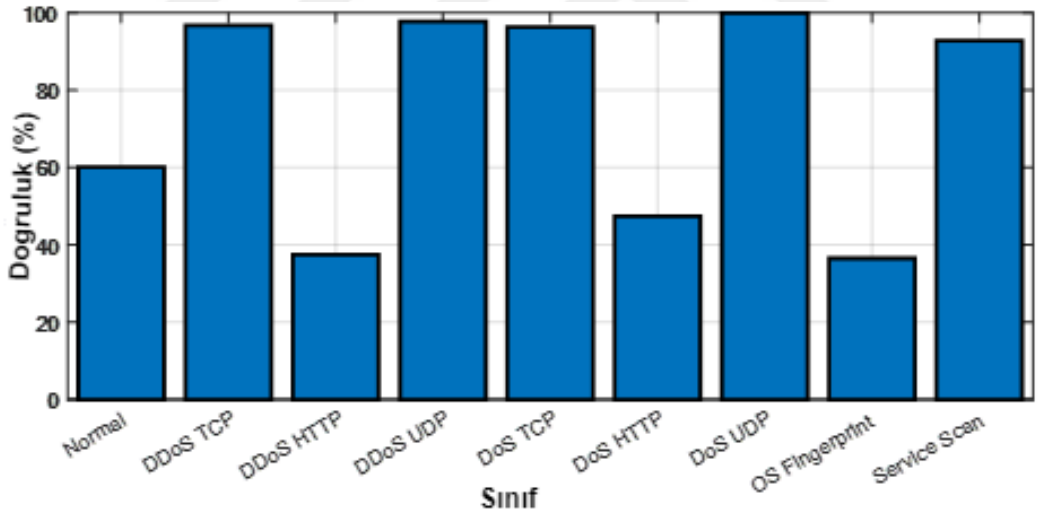
	Doğruluk	**Kesinlik**	**Duyarlılık**	**Geometrik Ortalama**	**F1-Skoru**
Maksimum	97.43	85.29	73.99	68.56	79.23
Minimum	97.42	84.98	73.92	68.48	79.08
Aritmetik Ortalama	97.41	85.06	73.93	68.49	79.11
Standart sapma	0.001	0.08	0.01	0.01	0.04

Tablo 6.3'te görüldüğü gibi en iyi %97,43 doğruluk Karar Ağacı sınıflandırıcı ile hesaplanmıştır. Bu sonuçlar 10 Kat çapraz doğrulama (Fold-Cross Validation) kullanılarak elde edilmiştir. Ayrıca önerilen yöntemde Fold-wise doğruluk değerleri hesaplanıp Şekil 6.4'te görülmektedir.



Şekil 6.4. Karar Ağacı sınıflandırıcı kullanılarak hesaplanan katlamalı doğruluklar

Şekil 6.4'te görüldüğü gibi, en yüksek sonuçlar Fold3, Fold4, Fold6 ve Fold9 (>%99,5 doğruluk) ile hesaplanmıştır. En düşük sonuç ise Fold5 ile %93,16 olarak hesaplandı. Önerilen yöntemin sınıf bazında sonuçları Şekil 6.5'te görülebilir.



Şekil 6.5. Karar Ağacı sınıflandırıcı kullanılarak hesaplanan sınıf bazında doğruluk

Şekil 6.5'te görüldüğü gibi en yüksek sonuçlar "DDoS TCP", "DDoS UDP", "DoS TCP" ve "DoS UDP" sınıfları için hesaplanmıştır. Doğruluk "DDoS TCP" için %96,73, "DDoS UDP" için %97,79, "DoS TCP" için %96,32 ve "DoS UDP" için %99,94'tür. En düşük sonuçlar "DDoS HTTP", "DoS HTTP" ve "OS Parmak İzi" sınıflarında hesaplanmıştır. Bot-IoT veri setinde yer alan örnek sayıları sonuçlarla karşılaştırıldığında, başarı oranının örnek sayıları ile ilişkili olduğu görülmektedir. "DDoS TCP", "DDoS UDP", "DoS TCP" ve "DoS UDP" sınıflarındaki örnek sayısı fazla olduğu için doğruluk değeri yüksek hesaplanmıştır.

6.4. Bölüm Değerlendirmesi

Bu çalışmada, Bot-IoT veri seti kullanılarak saldırı türleri sınıflandırılmıştır. Literatürde Bot-IoT veri seti ikili sınıflarda (Normal- DDoS HTTP, Normal- DDoS TCP, Normal- DDoS UDP vb.) değerlendirilmektedir. Bu ikili sınıflar için SVM, RNN ve LSTM tabanlı yöntemler önerilmiştir. Bot-IoT veri kümesinin büyük boyutu nedeniyle, yüksek özellikli bilgisayarlara ihtiyaç vardır. Bu nedenle Bot-IoT veri seti için hafif bir yöntem geliştirilmiştir. Ayrıca literatürdeki ikili sınıflar yerine 9 sınıf oluşturularak sonuçlar hesaplanmıştır. Karar Ağacı sınıflandırıcı ile %97,43 doğruluk hesaplanmıştır.

7. SONUÇLAR

İnternet, hayatı kolaylaştırmayı amaçladığı için günümüz hayatında çok önemli bir yere sahiptir. İnternet teknolojisinin gelişmesi sayesinde internet erişimi her yerden sağlanabilmektedir. Bu teknolojilerin örnekleri arasında mobil, kablosuz sensör ağları, uzaktan izleme ve kontrol sistemleri ve Nesnelerin İnterneti sayılabilir. Gelişen bu teknolojiler hayatı kolaylaştırsa da güvenlik açıklarına da yol açabilmektedir. Örneğin, büyük miktarda veri sızıntısının neden olduğu büyük miktarda veriye maruz kalmanın sonuçları ciddidir.

Yaygın olarak kullanılan internet teknolojilerinden biri olan Nesnelerin İnterneti, artık yaşamda çok önemli bir yere sahiptir. Akıllı nesneler birçok alanda kullanılmaya başlanmıştır. Herhangi bir ihlalin ciddi sonuçları nedeniyle, Nesnelerin İnternet'inde gizlilik ve güvenlik yönetiminin önemi artmaktadır. Ayrıca kritik sistemlerdeki güvenlik açıklarının daha fazla sonucu olacaktır. Tüm bu olumsuz etkiler göz önüne alındığında, bu teknolojideki gizlilik ve güvenlik yönetimi konuları daha da önemli hale gelmiştir. Tez çalışmasında, literatür de bulunan ve kendi oluşturduğumuz veri setleri kullanılarak IoT sistemlerde bulunan saldırılar incelenip makine öğrenme yöntemleri geliştirilerek doğruluk değerleri hesaplanmıştır.

Bu tez çalışmasında öncelikle Nesnelerin İnterneti tarihçesi, tanımı, haberleşme protokolleri, kullanım alanları ve makine öğrenmesi yöntemlerinden bahsedilmiştir. Ardından iki farklı çalışma gerçekleştirilmiştir. İlk çalışma kendi laboratuvar ortamımızda oluşturulan veri setleriyle gerçekleştirilmiştir. Bu çalışmada IoT saldırıları türlerinin tespiti için XGBOOST sınıflandırıcı kullanılmıştır. Akıllı ev ortamı oluşturulmuş ve akıllı ev ortamına saldırılar düzenlenerek veri seti toplanmıştır. Toplanan veri setinde 16 özellik olmak üzere toplamda 435815 örnek mevcuttur. XGBOOST sınıflandırıcısı kullanılarak Hold-out 80:20 eğitim test verisi için %92,55 doğruluk hesaplanmıştır.

Gerçekleştirilen diğer çalışmada ise literatürde Bot-IoT veri seti kullanılmıştır. Bu çalışmada 9 sınıf oluşturularak Karar Ağacı sınıflandırıcı ile %97,43 doğruluk değeri hesaplanıştır.

KAYNAKLAR

[1] S. D. Okegbile and O. I. Ogunranti, "Users emulation attack management in the massive internet of things enabled environment," *ICT Express*, vol. 6, no. 4, pp. 353–356, Dec. 2020, doi: 10.1016/j.icte.2020.06.005.

[2] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "IoT malicious traffic identification using wrapper-based feature selection mechanisms," *Computers and Security*, vol. 94, p. 101863, Jul. 2020, doi: 10.1016/j.cose.2020.101863.

[3] Ericsson, "Ericsson Mobility Report," 2020.

[4] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep learning for IoT big data and streaming analytics: A survey," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 4. Institute of Electrical and Electronics Engineers Inc., pp. 2923–2960, Oct. 01, 2018. doi: 10.1109/COMST.2018.2844341.

[5] J. Wang, J. Hu, G. Min, A. Y. Zomaya, and N. Georgalas, "Fast Adaptive Task Offloading in Edge Computing Based on Meta Reinforcement Learning," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 1, pp. 242–253, Jan. 2021, doi: 10.1109/TPDS.2020.3014896.

[6] N. C. Luong *et al.*, "Applications of Deep Reinforcement Learning in Communications and Networking: A Survey," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 4. Institute of Electrical and Electronics Engineers Inc., pp. 3133–3174, Oct. 01, 2019. doi: 10.1109/COMST.2019.2916583.

[7] Q. Zhang, H. Zhong, W. Shi, and L. Liu, "A trusted and collaborative framework for deep learning in IoT," *Computer Networks*, vol. 193, p. 108055, Jul. 2021, doi: 10.1016/j.comnet.2021.108055.

[8] K. Gupta and S. Shukla, "Internet of Things: Security challenges for next generation networks," in *2016 1st International Conference on Innovation and Challenges in Cyber Security, ICICCS 2016*, Aug. 2016, pp. 315–318. doi: 10.1109/ICICCS.2016.7542301.

[9] P. Kumar, A. Braeken, A. Gurtov, J. Iinatti, and P. H. Ha, "Anonymous Secure Framework in Connected Smart Home Environments," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 968–979, Apr. 2017, doi: 10.1109/TIFS.2016.2647225.

[10] E. Deniz, "Nesnelerin İnternetinde Gizlilik ve Güvenlik Yönetimi, Yüksek Lisans Tezi, Ankara Üniversitesi," Ankara, 2019.

[11] C. Zhang and R. Green, "Communication security in internet of thing: Preventive measure and avoid DDoS attack over IoT network," *Simulation Series*, vol. 47, no. 3, pp. 8–15, 2015.

[12] M. Hussein, M. Zorkany, and N. S. Abdel Kader, "Design and Implementation of IoT Platform for Real Time Systems," in *Advances in Intelligent Systems and Computing*, 2018, vol. 723, pp. 171–180. doi: 10.1007/978-3-319-74690-6_17.

[13] F. Y. Yavuz, "Deep Learning in Cyber Security for Internet of Things, Yüksek Lisans Tezi, Istanbul City University," 2018.

[14] E. M. Irmak, "Makine Ögrenmesi Regresyon Yöntemlerinin Nesnelerin İnterneti Verilerine Uygulanması, Yüksek Lisans Tezi, Harran Üniversitesi," p. 75, 2019.

[15] T. A. Gürkan, “Security Analysis of Coap and Dtls Protocols for Internet of Things Applications, Master of Science, Işık University,” p. 53, 2019.

[16] E. Yönem, “Nesnelerin Internetinde Veri Analizi İçin Tekrarlayıcı Sinir Ağları Yönetiminin Yapay Arı Koloni Algoritması İle Eğitilmesi, Erciyes Üniversitesi, Yüksek Lisans Tezi,” p. 124, 2019.

[17] K. Arslan, “Performance Evaluation of Iot Data Security on Cloud Computing, Master Science, Ankara Yıldırım Beyazıt University,” p. 65, 2019.

[18] M. Erhan, “It Security And Privacy Guidance Tool For IoT Designs And Products, Master Of Science, The Middle East Technical University,” vol. 8, no. 5, p. 127, 2019.

[19] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, “Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset,” *Future Generation Computer Systems*, vol. 100, pp. 779–796, Nov. 2019, doi: 10.1016/j.future.2019.05.041.

[20] M. Hasan, Md. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, “Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches,” *Internet of Things*, vol. 7, p. 100059, Sep. 2019, doi: 10.1016/j.iot.2019.100059.

[21] M. López, A. Peinado, and A. Ortiz, “An extensive validation of a SIR epidemic model to study the propagation of jamming attacks against IoT wireless networks,” *Computer Networks*, vol. 165, p. 106945, Dec. 2019, doi: 10.1016/j.comnet.2019.106945.

[22] T. Alladi, V. Chamola, and S. Zeadally, “Industrial Control Systems: Cyberattack trends and countermeasures,” *Computer Communications*, vol. 155. Elsevier B.V., pp. 1–8, Apr. 01, 2020. doi: 10.1016/j.comcom.2020.03.007.

[23] K. N. Qureshi, S. S. Rana, A. Ahmed, and G. Jeon, “A novel and secure attacks detection framework for smart cities industrial internet of things,” *Sustainable Cities and Society*, vol. 61, p. 102343, Oct. 2020, doi: 10.1016/j.scs.2020.102343.

[24] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, “Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city,” *Future Generation Computer Systems*, vol. 107, pp. 433–442, Jun. 2020, doi: 10.1016/j.future.2020.02.017.

[25] C. Z. E. Li and Z. W. Deng, “The embedded modules solution of household internet of things system and the future development,” in *Procedia Computer Science*, Jan. 2020, vol. 166, pp. 350–356. doi: 10.1016/j.procs.2020.02.086.

[26] İ. Kök, “Nesnelerin İnternetinde Derin Ögrenmeye Dayalı Veri Analizi ve Bilgi Çıkarımı, Doktora Tezi, Gazi Üniversitesi,” p. 155, 2020.

[27] J. Yoon, “Deep-learning approach to attack handling of IoT devices using IoT-enabled network services,” *Internet of Things*, vol. 11, p. 100241, Sep. 2020, doi: 10.1016/j.iot.2020.100241.

[28] X. Zhang, O. Upton, N. L. Beebe, and K.-K. R. Choo, “IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers,” *Forensic Science International: Digital Investigation*, vol. 32, p. 300926, Apr. 2020, doi: 10.1016/j.fsidi.2020.300926.

[29] S. Rizvi, R. Orr, A. Cox, P. Ashokkumar, and M. R. Rizvi, “Identifying the attack surface for IoT network,” *Internet of Things*, vol. 9, p. 100162, Mar. 2020, doi: 10.1016/j.iot.2020.100162.

[30] W. Choi, J. Kim, S. Lee, and E. Park, “Smart home and internet of things: A bibliometic study,” *Journal of Cleaner Production*, vol. 301, p. 126908, Jun. 2021, doi: 10.1016/j.jclepro.2021.126908.

[31] V. Srinadh, M. Srinivasa Rao, M. Ranjan Sahoo, and K. Rameshchandra, “An analytical study on security and future research of Internet of Things,” *Materials Today: Proceedings*, Mar. 2021, doi: 10.1016/j.matpr.2020.12.342.

[32] K. S. Niraja and S. Srinivasa Rao, “A hybrid algorithm design for near real time detection cyber attacks from compromised devices to enhance IoT security,” *Materials Today: Proceedings*, Mar. 2021, doi: 10.1016/j.matpr.2021.01.751.

[33] M. Snehi and A. Bhandari, “Vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks,” *Computer Science Review*, vol. 40, p. 100371, May 2021, doi: 10.1016/j.cosrev.2021.100371.

[34] M. A. Lawal, R. A. Shaikh, and S. R. Hassan, “A DDoS Attack Mitigation Framework for IoT Networks using Fog Computing,” *Procedia Computer Science*, vol. 182, pp. 13–20, Jan. 2021, doi: 10.1016/j.procs.2021.02.003.

[35] L. Yang, L. Liu, Z. Ma, and Y. Ding, “Detection of selective-edge packet attack based on edge reputation in IoT networks,” *Computer Networks*, vol. 188, p. 107842, Apr. 2021, doi: 10.1016/j.comnet.2021.107842.

[36] N. B. Samyuel and B. A. Shimray, “Securing IoT device communication against network flow attacks with Recursive Internetworking Architecture (RINA),” *ICT Express*, vol. 7, no. 1, pp. 110–114, Mar. 2021, doi: 10.1016/j.icte.2020.08.001.

[37] M. S. Ahmed, “Designing of internet of things for real time system,” *Materials Today: Proceedings*, Apr. 2021, doi: 10.1016/j.matpr.2021.03.527.

[38] I. Ullah and Q. H. Mahmoud, “Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks,” *IEEE Access*, vol. 9, pp. 103906–103926, 2021, doi: 10.1109/ACCESS.2021.3094024.

[39] Y. Shen, S. Shen, Z. Wu, H. Zhou, and S. Yu, “Signaling game-based availability assessment for edge computing-assisted IoT systems with malware dissemination,” *Journal of Information Security and Applications*, vol. 66, p. 103140, May 2022, doi: 10.1016/J.JISA.2022.103140.

[40] P. Chaudhary, B. B. Gupta, and A. K. Singh, “Securing Heterogeneous Embedded Devices against XSS Attack in Intelligent IoT System,” *Computers & Security*, p. 102710, Mar. 2022, doi: 10.1016/J.COSE.2022.102710.

[41] L. Vu, Q. U. Nguyen, D. N. Nguyen, D. T. Hoang, and E. Dutkiewicz, “Deep Transfer Learning for IoT Attack Detection,” *IEEE Access*, vol. 8, pp. 107335–107344, 2020, doi: 10.1109/ACCESS.2020.3000476.

[42] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, “A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services,” *IEEE Communications Surveys and Tutorials*, vol. 20, no. 4, pp. 3453–3495, Oct. 2018, doi: 10.1109/COMST.2018.2855563.

[43] S. Andy, B. Rahardjo, and B. Hanindhito, “Attack scenarios and security analysis of MQTT communication protocol in IoT system,” *International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, vol. 2017-December, Dec. 2017, doi: 10.1109/EECSI.2017.8239179.

[44] R. Arthi and S. Krishnaveni, “Design and development of iot testbed with DDoS attack for cyber security research,” *2021 3rd International Conference on Signal Processing and Communication, ICPSC 2021*, pp. 586–590, May 2021, doi: 10.1109/ICSPC51351.2021.9451786.

[45] J. Romkey, “Toast of the IoT: The 1990 Interop Internet Toaster,” *IEEE Consumer Electronics Magazine*, vol. 6, no. 1, pp. 116–119, Jan. 2017, doi: 10.1109/MCE.2016.2614740.

[46] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, “A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures,” *IEEE Access*, vol. 7. Institute of Electrical and Electronics Engineers Inc., pp. 82721–82743, 2019. doi: 10.1109/ACCESS.2019.2924045.

[47] M. Zekeriya Gündüz *et al.*, “Nesnelerin interneti: Gelişimi, bileşenleri ve uygulama alanları Internet of things (IoT): Evolution, components and applications fields,” *Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi*, vol. 24, no. 2, pp. 327–335, Apr. 2018, doi: 10.5505/pajes.2017.89106.

[48] P. Nimbalkar and D. Kshirsagar, “Feature selection for intrusion detection system in Internet-of-Things (IoT),” *ICT Express*, May 2021, doi: 10.1016/j.icte.2021.04.012.

[49] M. Ebleme, “Nesnelerin interneti uygulama katmanı haberleşme protokollerinin başarım analizi,” *Sakarya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar ve Bilişim Mühendisliği Ana Bilim Dalı Bilgisayar Mühendisliği Bilim Dalı,* 2019.

[50] J. Neeli and S. Patil, “Insight to security paradigm , research trend & statistics in internet of things(IoT),” *Global Transitions Proceedings*, vol. 2, no. 1, pp. 84–90, Jun. 2021, doi: 10.1016/j.gltp.2021.01.012.

[51] J. L. Fernandes, I. C. Lopes, J. J. P. C. Rodrigues, and S. Ullah, “Performance evaluation of RESTful web services and AMQP protocol,” in *International Conference on Ubiquitous and Future Networks, ICUFN*, 2013, pp. 810–815. doi: 10.1109/ICUFN.2013.6614932.

[52] M. Pohl, J. Kubela, S. Bosse, and K. Turowski, “Performance evaluation of application layer protocols for the internet-of-things,” in *Proceedings - 2018 6th International Conference on Enterprise Systems, ES 2018*, Dec. 2018, pp. 180–187. doi: 10.1109/ES.2018.00035.

[53] H. Kutluca, “Arakatmanlar -4. DDS Arakatmanı ile Sistem Geliştirme | by Huseyin Kutluca | Yazılım Mimarileri | Medium,” 2019. https://medium.com/yazılım-mimarileri/arakatmanlar-4-dds-arakatmanı-ile-sistem-geliştirme-81d5d3ebf36f (accessed May 08, 2021).

[54] B. Karasulu, L. Toker, and S. Korukoğlu, “ZigBee- IEEE 802.15.4 Standartı Temelli Kablosuz Algılayıcı Ağları,” *XIV. Türkiye’de İnternet Konferansı Bildirileri*, Dec. 13, 2009. http://inet-tr.org.tr/inetconf14/kitap/karasulu_toker_inet09.pdf (accessed May 17, 2021).

[55] G. Cansever, “Ethernet Tabanlı I/O Sistemleri ve Mobil Laboratuar Uygulaması Ethernet-Based I/O Systems and Mobile Laboratory Application,” 2012.

[56] Microsoft Azure, “IoT Teknolojileri ve Protokolleri | Microsoft Azure.” https://azure.microsoft.com/tr-tr/overview/internet-of-things-iot/iot-technology-protocols/ (accessed May 09, 2021).

[57] “30+ Most Useful PLC Communication Protocols.” https://instrumentationblog.com/plc-communication-protocols/ (accessed May 18, 2021).

[58] IoT Analytics, “IoT Analytics - Market insights for the Internet of Things.” https://iot-analytics.com/ (accessed May 07, 2021).

[59] B. Vignau, R. Khoury, S. Hallé, and A. Hamou-Lhadj, “The evolution of IoT Malwares, from 2008 to 2019: Survey, taxonomy, process simulator and perspectives,” *Journal of Systems Architecture*, vol. 116. Elsevier B.V., p. 102143, Jun. 01, 2021. doi: 10.1016/j.sysarc.2021.102143.

[60] “Internet of Thing (IOT).” https://bidb.itu.edu.tr/seyir-defteri/blog/2019/01/15/internet-of-thing-(iot) (accessed May 18, 2021).

[61] S. Juyal, S. Sharma, and A. Shankar Shukla, “Security and privacy issues in unified IoT-based skin monitoring system,” *Materials Today: Proceedings*, Feb. 2021, doi: 10.1016/j.matpr.2021.01.718.

[62] A. K. Das, S. Zeadally, and D. He, “Taxonomy and analysis of security protocols for Internet of Things,” *Future Generation Computer Systems*, vol. 89, pp. 110–125, Dec. 2018, doi: 10.1016/j.future.2018.06.027.

[63] M. binti Mohamad Noor and W. H. Hassan, “Current research on Internet of Things (IoT) security: A survey,” *Computer Networks*, vol. 148, pp. 283–294, Jan. 2019, doi: 10.1016/j.comnet.2018.11.025.

[64] S. Surendran, A. Nassef, and B. D. Beheshti, “A survey of cryptographic algorithms for IoT devices,” in *2018 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2018*, Jun. 2018, pp. 1–8. doi: 10.1109/LISAT.2018.8378034.

[65] F. Y. Aslan, “Nesnelerin interneti uygulamalarının güvenliği için hafif sıklet kriptografik algoritmaların analizi ve güvenli akıllı bir platform uygulaması,” *Trakya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Ana Bilim Dalı,* 2020.

[66] V. Goyal and A. Zafar, “A Cryptographic Approach for Securing IoT Devices,” *International Research Journal of Engineering and Technology*, 2020, Accessed: May 17, 2021. [Online]. Available: www.irjet.net

[67] S. Ayhan and Ş. Erdoğmuş, “Destek Vektör Makineleriyle Sınıflandırma Problemlerinin Çözümü İçin Çekirdek Fonksiyonu,” *Eskişehir Osmangazi Üniversitesi İktisadi ve İdari Bilimler Dergisi*, vol. 9, no. 1, pp. 175-201, Apr. 2014.

[68] İ. Kocaarslan, M. Taciddin Akçay, A. Akgündoğdu, and H. Tiryaki, “The Comparison of the ANN and SVM Methods for the Prediction of Voltage Drop on a Subway Line,” *Uluslararası Mühendislik Araştırma ve Geliştirme Dergisi*, vol. 10, no. 1, Nov. 2018, doi: 10.29137/umagd.352946.

[69] C. Atakan and İ. Karabulut, “Derinliğe Dayalı Diskriminasyon,” 2003.

[70] O. Cangul, “Diskriminant analizi ve bir uygulama denemesi,” *Bursa Uludag University*, 2006.

[71] B. Ataseven, “Yapay sinir ağları ile öngörü modellemesi,” *Öneri Dergisi,* vol. 10, no. 39, pp. 101-115. 2013.

[72] H. Ergezer, M. Dikmen, and E. Özdemir, “Yapay Sinir Ağları ve Tanıma Sistemleri.” Pivolka, vol. 2, no. 6, pp. 14-17, 2003.

ÖZGEÇMİŞ

Rojbin TEKİN

[redacted]