IOT VE IIOT TEKNOLOJİLERİ İÇİN UZMAN SİSTEME DAYALI ANALİZ YÖNTEMİ

EXPERT SYSTEM BASED ANALYSIS METHOD FOR IOT AND IIOT TECHNOLOGIES

GÖKÇE KARACAYILMAZ

DOÇ. DR. HARUN ARTUNER

Tez Danışmanı

Hacettepe Üniversitesi

Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğinin

Adli Bilimler Anabilim Dalı için Öngördüğü

DOKTORA TEZİ olarak hazırlanmıştır.

Ağustos 2024

ÖZET

IOT VE IIOT TEKNOLOJİLERİ İÇİN UZMAN SİSTEME DAYALI ANALİZ YÖNTEMİ

Gökçe KARACAYILMAZ

Doktora, Adli Bilimler Anabilim Dalı

Tez Danışmanı: Doç. Dr. Harun ARTUNER

Ağustos 2024, 130 sayfa

Endüstri 4.0 süreciyle büyük ivme kazanan bilgi toplumuna geçiş ile birlikte, insan hayatına büyük esneklik, hız ve verimlilik sağlayan bilgi teknolojileri beraberinde yeni saldırı yüzeylerini de ortaya çıkarmıştır. Özellikle IoT ve IIoT altyapısının kullanıldığı başta kritik altyapılar olmak üzere, akıllı şebekler, akıllı evler de dahil olmak üzere siber güvenlik analizleri gerçekleştirilmeden kullanıma geçilmiştir. Süreç içerisinde yaşanan siber güvenlik saldırıları ile birlikte sistemlerin güvenlik analizlerinin önemi ortaya çıkmıştır. Bu tez çalışması, IoT ve IIoT sistemlerinin güvenlik açıklarını incelemek ve bu açıkların giderilmesine yönelik bir uzman sistem modeli geliştirmek üzerine odaklanmıştır. Çalışmanın ilk aşamasında, IoT ve IIoT sistemlerinin ağ topolojilerindeki güvenlik zafiyetleri detaylı bir şekilde incelenmiştir. Analizler kapsamında, çeşitli saldırı senaryoları üzerinden incelemeler yapılmış ve IIoT sistemlerine yönelik potansiyel tehditlerin doğasını anlamak amacıyla derinlemesine bir bakış sunulmuştur. Çalışmanın odak noktası, uzman sistem tabanlı bir saldırı tespit yönteminin araştırılması, geliştirilmesi ve bu yaklaşımın etkinliğinin değerlendirilmesidir.

Anahtar Kelimeler: IoT, IIoT, Siber Güvenlik, Uzman Sistem, Makine Öğrenmesi, Yapay Zeka

ABSTRACT

EXPERT SYSTEM BASED ANALYSIS METHOD FOR IOT AND IIOT TECHNOLOGIES

Gökçe KARACAYILMAZ

Doctor of Philosophy, Department of Forensic Sciences

Supervisor: Doç. Dr. Harun ARTUNER

August 2024, 130 pages

The transition to an information society, accelerated by the advancements brought about by Industry 4.0, has introduced significant flexibility, speed, and efficiency into human life through information technologies. However, this transition has also exposed new attack surfaces. Particularly in critical infrastructures where IoT and IIoT architectures are utilized, including smart grids and smart homes, these technologies have often been deployed without comprehensive cybersecurity analyses. The occurrence of cyberattacks over time has highlighted the critical importance of security assessments in these systems. This thesis focuses on examining the security vulnerabilities within IoT and IIoT systems and developing an expert system model aimed at mitigating these vulnerabilities. The initial phase of the study involves a detailed examination of the security weaknesses in the network topologies of IoT and IIoT systems. The analysis includes a review of various attack scenarios, providing an in-depth understanding of the nature of potential threats to IIoT systems. The core focus of the research is the investigation, development, and evaluation of an expert system-based attack detection method, assessing its effectiveness in addressing these security challenges.

Keywords: IoT, IIoT, Cybersecurity, Expert Systems, Machine Learning, Artificial Intelligence

TEŞEKKÜR

Tezin hazırlanması aşamasında bana her türlü desteği veren, her zaman ama özellikle doktora sürecimin en zor dönemlerinde hoşgörü ve sabırla desteğini hiç eksik etmeyen, değerli hocam, tez danışmanım Doç. Dr. Harun ARTUNER'e,

Tez izleme ve savunma aşamasında çok değerli yorum ve önerileriyle tezin gelişmesine ve son halini almasına yardımcı olan, tez izleme komitesi ve savunma jüri üyesi hocalarım Prof. Dr. Ercan Nurcan YILMAZ, Prof.Dr. Sevil ŞEN AKAGÜNDÜZ, Doç. Dr. Kayhan M. İMRE'ye ve Dr. Serkan GÖNEN'e

Tezin her aşamasında değerli katkılarını esirgemeyen arkadaşım M.Ali BARIŞKAN'a,

Desteklerini benden esirgemeyen mesai arkadaşlarıma,

Bu süreçte ve hep yanımda olan, beni destekleyen, büyük sevgisini ve anlayışını hiçbir zaman benden esirgemeyen hayat arkadaşım Nurver ile çocuklarım Efe ve Alp'e,

Hayatımın her aşamasında hep yanımda olan, sevgi ve desteklerini hiç eksik etmeyen çok sevgili annem ve kardeşime,

Canı gönülden sonsuz teşekkür ederim.

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

KISALTMALAR

AI Yapay Zeka (Artificial Intelligence)

AMP İleri Üretim Ortaklığı (Advanced Manufacturing Partnership)

AMQP Gelişmiş Mesaj Kuyruk Protokolü (Advanced Message Queuing Protocol)

AR Artırılmış Gerçeklik (Augmented Reality)

ARP Adres Çözümleme Protokolü (Address Resolution Protocol)

BLE Bluetooth Düşük Enerji (Bluetooth Low Energy)

CNN Geleneksel Sinirsel Şebeke (Convolutional Neural Network)

COAP Kısıtlı Uygulama Protokolü (Constrained Application Protocol)

CPU Merkezi İşlem Birimi (Central Process Unit)

DDoS Dağıtık Hizmet Reddi (Distrubuted Denial of Service)

DDS Veri Dağıtım Hizmeti (Data Distribution Service)

DL Derin Öğrenme (Deep Learning)

DNP3 Dağıtık Ağ Protokolü 3 (Distributed Network Protocol 3)

DNN Derin Sinirsel Şebeke (Deep Neural Network)

DODAG Hedef Odaklı Yönlendirilmiş Döngüsel Çizge (Destination Oriented Directed Acyclic Graph)

DoS Hizmet Reddi (Denial of Service)

EDR Uç Nokta Tehdit Algılama ve Yanıt (Endpoint Detection and Response)

EKS Endüstriyel Kontrol Sistemleri

GPU Grafik İşlemci Birimi (Graphics Processing Unit)

HMI İnsan Makine Arayüzü (Human Machine Interface)

HTTP Hiper Metin Transfer Protokolü (Hypertext Transfer Protocol)

IDS Saldırı Tespit Sistemi (Intrusion Detection System)

IPS Saldırı Önleme Sistemi (Intrusion Prevention System)

IIoT Endüstriyel Nesnelerin İnterneti (Industrial Internet of Things)

INT Enterferans (Interference)

IoT Nesnelerin İnterneti (Internet of Things)

LoRa Uzun Mesafeli (Long Range)

LoRaWAN Uzun Mesafeli Geniş Alan Ağı (Long Range Wide Area Network)

M2M Makineden Makineye (Machine to Machine)

MitM Ortadaki Adam (Man in the Middle)

ML Makine Öğrenmesi (Machine Learning)

MQTT Mesaj Kuyruğu Telemetri Aktarımı (Message Queuing Telemetry Transport)

NN Sinirsel Şebeke (Neural Networks)

ON Çalışmada (in Operation)

OPC UA Açık Platform İletişimi Birleşik Mimarisi (Open Platform Communications Unified Architecture)

OSI Açık Sistemler Bağlantısı (Open Systems Interconnection)

OT Operasyonel Teknoloji (Operational Technology)

PCA Temel Bileşen Analizi (Principal Component Analysis)

PLC Programlanabilir Mantık Denetleyicisi (Programmable Logic Controller)

PROFIBUS Süreç Alan Veriyolu (Process Field Bus)

ReLU Doğrultulmuş Lineer Birim (Rectified Linear Unit)

RPL Düşük Güçlü ve Kayıplı Ağlar İçin Yönlendirme Protokolü (Routing Protocol for Low-Power and Lossy Network)

RTU Uzak Terminal Birimi (Remote Terminal Unit)

SCADA Denetimsel Kontrol ve Veri Toplama (Supervisory Control and Data Acquisition)

STP Korumalı Çift Örme (Shielded Twisted Pair)

SVM Destek Vektör Makinesi (Support Vector Machine)

TANH Hiperbolik Tanjant

UTP Korumasız Çift Örme (Unshielded Twisted Pair)

VR Sanal Gerçeklik (Virtual reality)

WiMAX Mikrodalga Erişimi için Dünya Çapında Birlikte Çalışabilirlik (Worldwide Interoperability for Microwave Access)

WSN Kablosuz Sensör Ağı (Wireless Sensor Network)

XDR Genişletilmiş Algılama ve Yanıt (Extended Detection and Response)

1. GİRİŞ

İnsan yaşamının evrimini belirleyen, kritik öneme sahip çeşitli evreler bulunmaktadır. Bunlar genel olarak tarım, endüstri ve bilgi topluluğu başlıkları altında birleştirilmektedir. Tarım toplumu, endüstri toplumu ve bilgi toplumu kavramları, farklı üretim biçimleri, sosyal yapılar ile bilgi ve iletişim biçimleriyle karakterize edilen insan medeniyetinin farklı evrelerine atıfta bulunmaktadır. Tarım toplumu veya tarımsal toplum, ana üretim biçimi olarak kendi kendine yeten tarımı ve akrabalık bağları, aile ve klan birimleri etrafında sosyal örgütlenmeyi karakterize etmektedir. Bu toplum biçimi, düşük teknoloji seviyeleri, sınırlı iş bölümü ve düşük ticaret ve ticaret seviyeleri ile işaretlenmektedir. Sanayi devriminin yükselişi, on sekizinci ve on dokuzuncu yüzyılların sonlarında endüstriyel toplum yapısının da gelişimini sağlamıştır. İleri makineler, kömür ve buhar gücü gibi enerji kaynakları kullanarak malların toplu üretimini karakterize etmektedir. Bu da büyük şehir merkezlerinin gelişmesine, karmaşık iş bölümüne ve endüstriyel işçi sınıfı ve sermayedar sınıfı gibi yeni sosyal sınıfların ortaya çıkmasına yol açmıştır. Bilgi toplumu veya post-endüstriyel toplum ise ekonomik büyümenin ve sosyal değişimin anahtarı olarak bilgi ve iletişim teknolojilerinin merkezi olarak nitelendirilmektedir. Bu toplum biçimi, bilgiye dayalı bir ekonominin yükselişi, yeni sosyal örgütlenme ve iletişim biçimlerinin ortaya çıkması gibi özellikleriyle karakterizedir. Her bir toplum biçimi, farklı ekonomik, sosyal ve kültürel özelliklere sahip insan medeniyetinin farklı bir evresini temsil etmekte olup, bu da insan gelişimi ve ilerlemesi için farklı zorluklar ve fırsatlar sunmaktadır.

Hali hazırda içinde bulunduğumuz bilgi toplumu baş döndürücü hızla gelişen bilgi teknolojilerinin ışığında hayatımızın her alanında yaygın olarak kullanılmaya başlanmıştır. Bilgi teknolojilerinin yaygın kullanımı, son yıllarda insan yaşamının önemli bir parçası haline gelmiştir. İnternet, akıllı telefonlar, tabletler ve diğer cihazlar bilgiye erişim, iletişim ve eğlence için kullanılmaktadır. Bilgi teknolojilerinin bu yaygın kullanımı, hemen hemen tüm sektörlerde, özellikle eğitim, sağlık, iş dünyası ve devlet gibi alanlarda büyük faydalar sağlamıştır. Bilgi teknolojileri, eğitim alanında da önemli bir rol oynamaktadır. Öğrenciler internet aracılığıyla çevrimiçi kaynaklara erişebilir, uzaktan eğitim alabilir ve dijital öğrenme materyalleri kullanabilirler. Bunun yanı sıra, öğretmenler ve öğrenciler arasındaki iletişim, e-posta ve diğer dijital araçlar kullanılarak kolaylaştırılmaktadır. Sağlık sektörü de bilgi teknolojilerinin yaygın kullanımından

önemli faydalar sağlamaktadır. Elektronik sağlık kayıtları, hasta verileri ve tıbbi görüntüleme daha iyi tanı ve tedavi için kullanılabilir hale gelmiştir. Buna ek olarak uzaktan ilaç veya uzaktan tıp uygulamaları, uzak bölgelerde veya acil durumlarda hızlı bir şekilde tıbbi müdahale yapılmasına yardımcı olabilmektedir. İş dünyasında bilgi teknolojileri, iş süreçlerinin otomasyonu, verimliliğin artırılması, müşteri ilişkilerinin yönetimi ve işletme maliyetlerinin azaltılması için kullanılmaktadır. Örneğin, bulut bilişim teknolojisi, işletmelerin verilerini daha güvenli ve kolay bir şekilde yönetmelerine olanak tanımıştır. Devletler de vatandaşlarla daha iyi iletişim kurmak ve hizmet sunmak için bilgi teknolojilerine başvurmaktadır. Online vergi beyannameleri, çevrimiçi pasaport başvuruları ve e-devlet uygulamaları gibi diğer dijital hizmetler vatandaşların işlerini hızlı ve kolay bir şekilde gerçekleştirmelerine yardımcı olmuştur.

Nesnelerin İnterneti (IoT) ve Endüstriyel Nesnelerin İnterneti (IIoT) teknolojilerinin hızla yaygınlaşması, birçok sektörde devrim yaratırken, beraberinde ciddi siber güvenlik risklerini de getirmiştir. Kritik altyapılarda ve endüstriyel kontrol sistemlerinde yaygın olarak kullanılan bu cihazlar, büyük miktarda hassas veri üretmekte ve siber saldırılara karşı savunmasız kalmaktadır. IoT ve IIoT sistemlerinin güvenliğinin sağlanması hem bireyler hem de kuruluşlar için hayati bir önem taşımaktadır. Ancak, mevcut güvenlik yöntemleri bu dinamik ve çeşitli tehdit ortamında yetersiz kalmakta, bu da yeni ve etkili savunma stratejilerinin geliştirilmesini zorunlu kılmaktadır. Bu kapsamda, tezde sunulan uzman sisteme dayalı yöntemi, bu güvenlik açıklarını minimize etmeyi amaçlayan yenilikçi yaklaşımlar sunmaktadır. Özellikle, saldırı tespit ve önleme mekanizmalarının geliştirilmesi, bu sistemlerin güvenliğini sağlamada önemli bir rol oynamaktadır. Bu sayede, siber güvenlik uzmanı olmayan personelin bile bu kompleks sistemlerin güvenliğini sağlamalarına yardımcı olacak bir uzman sistem tasarımı önerilmiştir. Önerilen sistemde, yapay zeka algoritmaları kullanılarak kullanıcıların çeşitli siber tehditleri etkin bir şekilde tespit etmeleri ve bu tehditlere karşı kural tabanlı sistemleri kolaylıkla kullanabilmeleri hedeflenmiştir. Bu şekilde, IoT ve IIoT sistemlerinin korunması, siber güvenlik uzmanlığı gerektirmeden sağlanarak, söz konusu teknolojilerin güvenli ve verimli bir şekilde kullanılmasına katkıda bulunulmuştur.

Bu çalışmanın temel motivasyonu ve katkısı, Nesnelerin İnterneti (Internet of Things-IoT) ve IoT cihazları ile entegre edilmiş programlanabilir mantık denetleyicileri (Programmable Logic Controller-PLC) için yapay zeka algoritmaları kullanarak sürekli izleme ve saldırı tespitini birleştiren yeni bir uzman sistem yöntemi önermesidir. Önerilen

sistem, yüksek düzeyde doğruluk ve düşük yanlış pozitif değerler elde etmeyi hedefleyen, kural tabanlı yaklaşımlar ile makine öğrenimi metotlarının birleşiminden yararlanan hibrit bir yapı kullanmaktadır. Bu sayede, makine öğrenimi metodları kullanılarak belirlenen modeller kural yazımında uzman personel için yönlendirici olurken, uzman tarafından hazırlanan kurallar ile hızlı ve etkin bir şekilde saldırıların tespitinin sağlanarak sistem yöneticilerinin bilgilendirilmesi hedeflenmiştir. Önerilen sistemin performansı, endüstriyel kontrol sistemlerinde kullanılan gerçek cihazlar üzerinde değerlendirilmiştir.

Çalışma ile IoT ve IIoT sistemlerine yönelik saldırılar için siber güvenlik alanındaki araştırma ve uygulamaların ilerlemesine önemli katkılar sağlanmaktadır. Ağ üzerindeki cihazlardan toplanan IoT ve IIoT ağ trafiğine yönelik yaygın saldırılar (Man in the Middle-MitM, Distributed Denial of Service-DDoS, ve Başlat-Durdur gibi) gerçekleştirilmiştir. İşletim sistemlerine ek yük getirmemek ve ağın güvenliğini sağlamak amacıyla analizlerde yansıtma (mirroring) kullanılmıştır. Saldırı tespit aşamasında, yapay zeka tabanlı uzman sistem kullanılarak sürekli izleme ve saldırı tespiti birleştirilmiştir. Tespit aşamasında belirlenen özniteliklerin (feature) saldırıların tespitindeki etkisi değerlendirilerek "saldırı tespit modeli" oluşturulmuştur. Yapılan çalışma sonucunda, uzman sistem yüksek bir saldırı tespit başarı oranı göstermiştir.

Bu çalışma, IoT ve IIoT sistemlerinin güvenliğini artırmaya yönelik stratejiler geliştirmek için önemli bir kaynak sunmakta ve gelecekteki araştırmalara yön veren değerli bilgiler sağlamaktadır. IoT ve IIoT teknolojilerinin güvenli bir şekilde entegrasyonunu sağlamak, bilgi toplumunun sürdürülebilirliği ve güvenliği açısından büyük önem taşımaktadır. Çalışmanın önemli katkıları aşağıdaki gibidir:

- Ağ üzerindeki cihazlardan toplanan IoT ve IIoT ağ trafiğine saldırganlar tarafından yaygın olarak (Man in the Middle-MitM-Ortadaki Adam, Distributed Denial of Service-DDoS ve Başlat-Durdur gibi) saldırılar gerçekleştirilmiştir.

- İşletim sistemlerine ek yük getirmemek ve ağın güvenliğini sağlamak amacıyla yapılan analizlerde yansıtma (mirroring) kullanılmıştır.

- Saldırı tespit aşamasında yapay zeka tabanlı uzman sistem kullanılmıştır. Bu uzman sistem, yapay zeka kullanarak sürekli izleme ve saldırı tespitini birleştirmektedir. Tespit aşamasında, belirlenen özniteliklerin (feature) saldırıların tespitindeki etkisi değerlendirilerek "saldırı tespit modeli" oluşturulmuştur. Yapılan çalışma sonucunda uzman sistem, belirgin şekilde yüksek bir saldırı tespit başarı oranı göstermiştir.

- Çalışma kapsamında çeşitli IoT ve IIoT sistemlerine yönelik saldırı analizleri gerçekleştirilmiş olsa da saldırı analizleri ve uzman sistem üzerinden saldırı tespitine yönelik akış diyagramlarında belirtilen adımlar izlenmesi halinde ağ üzerinde veri üreten diğer sistemlere de uygulanabilecektir.

Çalışmanın ikinci bölümde genel bilgiler verilmiştir. Üçüncü bölümde bu alanda yapılmış olan diğer çalışmalar incelenmiştir. Dördüncü bölümde, çalışma kapsamında oluşturulan sınama ortamı (örnek sistem) tanıtılmış, bileşenleri detaylı olarak açıklanmış ve oluşturulan sınama ortamı üzerinde gerçekleştirilen saldırı analizleri ile saldırıların sistem/sistemler üzerindeki etkisi değerlendirilmiştir. Beşinci bölümde çalışmanın temel odak noktası olan dördüncü bölümde gerçekleştirilen saldırıların uzman sistem aracılığıyla tespiti ele alınmış ve gerçekleştirilen saldırı ile tespit analizlerinden elde edilen çıkarımlar değerlendirilmiştir. Altıncı bölümde Sonuçlar tartışılmıştır. Yedinci bölüm olan yorumlar ve katkılar ile çalışma tamamlanmıştır.

2. GENEL BİLGİLER

2.1. Endüstri 4.0

Bilgi teknolojilerinin insan hayatının her alanında kullanılmaya başlamasıyla ortaya çıkan olgulardan bir de “akıllı sistemler”dir. Bu yapıda çeşitli isimlerle adlandırılan uygulamalar ortaya çıkmıştır. Bunların başında, akıllı evler, akıllı şehirler ve akıllı şebekeler son yıllarda büyük ilgi gören konular arasındadır. Bu sistemler, farklı cihazların birbirleriyle etkileşim halinde olduğu, verilerin toplandığı ve bu verilerin analiz edilerek çeşitli kararların alındığı sistemlerdir. Akıllı evler, evlerdeki cihazların internete bağlanması ve birbirleriyle iletişim kurması yoluyla ev sahiplerine farklı imkanlar sunmuştur. Bu sistemler sayesinde ev sahipleri, evlerini uzaktan kontrol edebilir, güvenlik kameralarını takip edebilir, evlerindeki ısıtma, aydınlatma, havalandırma gibi sistemleri otomatikleştirebilir. Ayrıca akıllı evler, enerji tasarrufu sağlamak için de kullanılabilmektedir. Örneğin akıllı termostatlar, evdeki sıcaklık ve nem seviyelerini ölçerek enerji tasarrufu sağlayacak şekilde akıllı ev sistemini ayarlayabilmektedir.

Akıllı şehirler, kentlerin farklı bileşenlerinin birbirleriyle iletişim kurduğu ve verilerin toplandığı sistemlerdir. Bu sistemler sayesinde trafik akışı, güvenlik, çevre kirliliği, enerji yönetimi, çöp yönetimi ve daha birçok konuda veriler toplanabilmekte ve analiz edilebilmektedir. Böylece kent yöneticileri, kentlerin daha etkin yönetilmesi ve sürdürülebilir bir yapıya kavuşturulması için kararlar alabilmektedirler. Ayrıca akıllı şehirler, vatandaşların hayatını kolaylaştırmak için de kullanılabilmektedir. Örneğin çevrimiçi olarak park yeri arama, toplu taşıma saatleri ve trafik durumu hakkında bilgi sağlayabilmektedirler.

Akıllı şebekeler ise enerjinin üretildiği kaynaklardan tüketicilere kadar olan sürecin yönetiminde kullanılan sistemlerdir. Bu sistemler sayesinde enerji üretimindeki değişkenliklere uyum sağlanabilmekte, tüketicilerin enerji tüketimleri analiz edilebilmekte ve enerji kaynaklarının verimli kullanımı sağlanabilmektedir. Akıllı şebekeler, yenilenebilir enerji kaynaklarının kullanımı için de önemli bir temel taşı durumuna gelmektedir. Örneğin güneş panellerinden üretilen enerjinin depolanması ve tüketicilere yönlendirilmesi için akıllı şebeke sistemleri kullanılabilmektedir.

Ancak akıllı evler, akıllı şehirler ve akıllı şebekelerin uygulanması aşamasında bazı zorluklar da bulunmaktadır. Bu sistemlerin uyumlu ve güvenli bir şekilde çalışması için farklı cihazların birbirleriyle uyumlu olması ve standartlar oluşturulması gerekmektedir.

Verilerin toplanması, depolanması ve analiz edilmesi için uygun altyapı ve standartların oluşturulması ve bu sistemlere gerçekleştirilebilecek siber saldırılara karşı siber güvenlik önlemlerinin alınması gerekmektedir. Akıllı evler, akıllı şehirler ve akıllı şebekeler insan yaşamını kolaylaştıran, sürdürülebilir bir yapıya katkı sağlayan ve enerji tasarrufu sağlayan önemli sistemlerdir. Bu sistemlerin yaygınlaşmasıyla birlikte, toplumların ve endüstrilerin daha verimli bir şekilde yönetilmesi mümkün hale gelecektir. Ancak, bu sistemlerin uygulanması aşamasında karşılaşılacak olan zorluklarda göz önünde bulundurulmalı ve gerekli önlemler alınmalıdır.

Bu akıllanma sürecini hızlandıran en önemli etkenlerden biri de Endüstri 4.0 konseptidir. Dördüncü Sanayi Devrimi veya Endüstri 4.0 dijital, fiziksel ve biyolojik sistemlerin birleşmesi ile karakterize edilmektedir. Bu teknolojik devrim, yaşam ve çalışma şeklimizi dönüştürmekte ve küresel ekonomiyi yeniden şekillendirmektedir. Endüstri 4.0, Nesnelerin İnterneti (IoT), Yapay Zeka (Artificial Intelligence-AI) ve Robotik gibi teknolojilerdeki ilerlemeler tarafından yönlendirilmektedir.

Endüstri 4.0'ın gelişimi, ilk programlanabilir mantık denetleyicilerinin geliştirildiği geç 20. yüzyıla kadar takip edilebilir. Bu denetleyiciler, makinelerin yazılım tarafından kontrol edilmesini sağlayarak otomasyonun yolunu açmıştır. İnternetin 1990'larda geliştirilmesi, makinelerin ve süreçlerin entegrasyonunu mümkün kılarak bu süreci hızlandırmıştır. "Endüstri 4.0" terimi, Alman hükümeti tarafından 2011 yılında dördüncü sanayi devrimini tanımlamak için kullanılmıştır. Üretimde küresel bir lider olan Almanya, Endüstri 4.0'ın üretim sürecini dönüştürme ve ekonomik büyümeyi tetikleme potansiyelini tanımış, Alman hükümeti, ülkede Endüstri 4.0'ın uygulanması için bir yol haritası geliştirmek için bir çalışma grubu kurmuştur. Yol haritası, standart arayüzlerin geliştirilmesi, veri güvenliği ve gizlilik standartlarının belirlenmesi ve yeni iş modellerinin geliştirilmesi gibi birçok anahtar odak alanını belirlemiştir. O zamandan beri, Endüstri 4.0 küresel olarak ivme kazanmış ve birçok ülke gelişimine yatırım yapmaktadır. Avrupa Birliği, Endüstri 4.0 alanındaki araştırma ve yenilik için fon sağlayan Horizon 2020 programını başlatmıştır. ABD, gelişmiş üretim teknolojilerinin gelişimini hızlandırmayı amaçlayan bir kamu-özel ortaklığı olan Advanced Manufacturing Partnership (AMP) başlatmıştır.

Endüstri 4.0 dijital teknolojiler, makineler ve süreçlerin karmaşık bir etkileşimidir. Veri odaklı karar verme, otomasyon ve optimizasyonu mümkün kılmak için akıllı cihazların,

sensörlerin ve makinelerin entegrasyonunu içermektedir. Endüstri 4.0'ın bazı temel bileşenleri şunlardır:

Nesnelerin İnterneti (IoT): IoT, sensörler, yazılım ve ağ bağlantısı ile donatılmış fiziksel cihazlar, araçlar ve diğer nesnelerin ağına atıfta bulunmaktadır. Endüstri 4.0'da IoT, makinelerin birbirleriyle iletişim kurmasını, veri paylaşmasını ve bu verilere dayanarak karar vermelerini sağlamaktadır.

Yapay Zeka (AI): AI, genellikle insan zekasına ihtiyaç duyulan görevleri yerine getirebilen bilgisayar sistemlerinin geliştirilmesini içermektedir, örneğin konuşma tanıma, karar verme ve görsel algılama gibi. Endüstri 4.0'da AI, süreçleri optimize etmek, makine arızalarını öngörmek, sistemlerin siber güvenliğini sağlamak ve ürün kalitesini iyileştirmek için kullanılmaktadır.

Büyük Veri Analitiği: Büyük veri, Endüstri 4.0'da sensörler ve diğer kaynaklar tarafından oluşturulan büyük veri hacimlerine atıfta bulunmaktadır. Büyük veri analitiği, bu verileri analiz etmek, süreçleri optimize etmek, ürün kalitesini iyileştirmek ve maliyetleri azaltmak için gelişmiş algoritmalar ile araçlar kullanarak bilgiler çıkarmayı içermektedir.

Eklemeli Üretim: Eklemeli üretim, üç boyutlu nesnelerin malzemelerin üst üste konmasıyla oluşturulan bir süreçtir. Endüstri 4.0'da, eklemeli üretim özelleştirilmiş ürünler ve yedek parçaların talep üzerine üretilmesinde kullanılmakta ve bu sayede büyük envanterlere ihtiyaç azaltılmaktadır.

Arttırılmış Gerçeklik (Augmented Reality-AR) ve Sanal Gerçeklik (Virtual reality-VR): AR ve VR, dijital teknolojinin kullanımını içeren etkileşimli ve etkileyici deneyimler oluşturmak için kullanılmaktadır. Endüstri 4.0'da AR ve VR, işçileri eğitmek, üretim süreçlerini simüle etmek ve ürün tasarımlarını görselleştirmek için kullanılmaktadır.

Siber Güvenlik: Endüstri 4.0 sistemleri daha fazla bağlantılı ve veri odaklı hale geldikçe, siber güvenlik giderek daha önemli hale gelmektedir. Endüstri 4.0 bileşenleri, hassas verileri korumak ve siber saldırıları önlemek için blockchain ve güvenli iletişim protokolleri gibi gelişmiş güvenlik önlemleri içermektedir.

Endüstri 4.0 süreci üretim, sağlık, lojistik ve perakende dahil olmak üzere çeşitli endüstrileri dönüştürmektedir. Üretim endüstrisinde yüksek derecede otomatik, esnek ve verimli olan akıllı fabrikaların oluşturulmasını sağlamıştır. Dijital teknolojileri üretim süreciyle entegre ederek üreticiler, üretimi optimize edebilir, maliyetleri azaltabilir ve ürün kalitesini artırabilirler. Sağlık alanında, AI aracılığı ile hastalık verilerini analiz

ederek kişiye göre özelleştirilmiş tedavi planları hazırlayabilir ve kişiselleştirilmiş tıbbın geliştirilmesine olanak sağlayabilir. Lojistikte, gönderilerin gerçek zamanlı takibini sağlayarak teslimat rotalarını optimize edebilir, bu sayede tedarik zinciri yönetimini iyileştirebilir. Perakende sektöründe kişiselleştirilmiş öneriler ve gerçek zamanlı envanter yönetimi ile alışveriş deneyimini dönüştürebilir.

Bilgi teknolojilerinin yaygın kullanımı beraberinde bazı riskleri de getirmiştir. Özellikle siber güvenlik tehditleri, kişisel veri gizliliği ihlalleri ve internet bağımlılığı gibi sorunların dikkatli bir şekilde ele alınması oldukça önemlidir. Bu nedenle bilgi teknolojilerinin sağladığı faydaların yanı sıra olası risklerin de öngörülerek uygun tedbirlerin alınması gerekmektedir. Böylece, bilgi teknolojilerinin faydaları en üst düzeyde sağlanırken, olası riskler de en aza indirilebilir.

2.1.1. Endüstri 4.0'ın Ekonomiye Etkisi

Endüstri 4.0'ın küresel ekonomi üzerindeki etkisinin önemli olması beklenmektedir. Dünya Ekonomik Forumu'nun bir raporuna göre, Endüstri 4.0'ın 2025 yılına kadar 3,7 trilyon dolar değer yaratabileceği potansiyeli bulunmaktadır [1]. McKinsey Global Institute tarafından hazırlanan başka bir rapor ise Endüstri 4.0'ın 2025 yılına kadar küresel olarak 3,7 trilyon dolar değer yaratabileceğini tahmin etmektedir [2].

Endüstri 4.0'ın küresel ekonomi üzerindeki etkisi, üretim, sağlık, lojistik ve perakende gibi çeşitli endüstrileri dönüştürerek yayılması beklenmektedir. Üretim endüstrisinde, Endüstri 4.0, yüksek derecede otomatik, esnek ve verimli olan akıllı fabrikaların oluşturulmasını sağlamaktadır. Dijital teknolojileri üretim süreciyle entegre ederek üreticiler, üretimi optimize edebilir, maliyetleri azaltabilir ve ürün kalitesini artırabilirler. Sağlık alanında, Endüstri 4.0, AI kullanarak hastalık verilerini analiz ederek özelleştirilmiş tedavi planları geliştirerek kişiselleştirilmiş tıbbın geliştirilmesine olanak tanımaktadır. Lojistikte, Endüstri 4.0, gönderilerin gerçek zamanlı takibini sağlayarak teslimat rotalarını optimize ederek tedarik zinciri yönetimini iyileştirmektedir. Perakende sektöründe Endüstri 4.0, kişiselleştirilmiş öneriler ve gerçek zamanlı envanter yönetimi ile alışveriş deneyimini dönüştürmektedir. Endüstri 4.0, yaşam ve iş yapma şeklini dönüştürmekte ve küresel ekonomi üzerindeki etkisi oldukça yüksektir. Dijital teknolojilerin üretim sürecine entegre edilmesi, yüksek derecede otomatik, esnek ve verimli olan akıllı fabrikaların oluşturulmasını sağlamaktadır. Endüstri 4.0'ın gelişimi,

devletler, işletmeler ve akademisyenler tarafından desteklenmekte ve birçok ülke gelişimine yatırım yapmaktadır.

2.1.2. Endüstri 4.0'ın Geleceği

Endüstri 4.0, gelecekte daha da önemli hale gelecektir. İnternetin yaygınlaşması, makinelerin ve süreçlerin daha da entegrasyonu, yapay zeka ve büyük veri analitiği gibi teknolojik ilerlemelerle birlikte, Endüstri 4.0 süreci daha da gelişecektir. Endüstri 4.0'ın geleceği, daha sürdürülebilir ve çevre dostu üretim süreçleri, daha yüksek otomasyon ve daha özelleştirilmiş ürünlerin yanı sıra, daha da gelişmiş bir dijital altyapı ve siber güvenlik önlemlerinin de dahil olduğu daha geniş bir ekosistemi içermektedir. Endüstri 4.0, dijital, fiziksel ve biyolojik sistemlerin birleşmesiyle dünya ekonomisinde köklü bir dönüşüme neden olmuştur. Akıllı fabrikalar, kişiselleştirilmiş tıp, daha verimli lojistik ve kişiselleştirilmiş alışveriş deneyimleri gibi Endüstri 4.0 bileşenleri, verimlilik, kalite ve maliyet açısından birçok fayda sağlamaktadır. Ancak, Endüstri 4.0'ın işgücü piyasasını nasıl etkileyeceği gibi bazı zorluklar da mevcuttur. Bu nedenle, Endüstri 4.0'a geçişte, getirdiği verimlilik ve etkinlik gibi yararların yanında özellikle süreklilik ve sürdürülebilirlik için Endüstri 4.0'ın temel bileşenlerinden biri olan siber güvenlik boyutuna da daha fazla önem verilmesi ve yatırım yapılması gerekmektedir [3].

2.2. Nesnelerin İnterneti (IoT)

2.2.1. IoT Kavramının Ortaya Çıkışı

İnsanlık tarihi, sosyal hayatı etkileyen üç temel evreden geçmiştir: tarım toplumu, sanayi toplumu ve bilgi toplumu. Bilgi sistemleri ve ağ kavramlarının ortak kullanımıyla oluşan bilgi toplumu, hayatımızda önemli değişikliklere neden olmuştur. İnternetin ortaya çıkışıyla birlikte bankacılıktan sağlık hizmetlerine kadar pek çok alanda dijital dönüşüm yaşanmıştır.

Bilgi teknolojilerinde gerçekleşen bu gelişim sonucunda insan hayatını önemli şekilde etkileyen kavramlardan biri de nesnelerin internetidir. Son yıllarda ortaya çıkan Nesnelerin İnterneti (IoT) kavramı, yaşamımızı, çalışma şeklimizi dönüştüren bir teknoloji olarak karşımıza çıkmaktadır. IoT, sensörler, yazılımlar ve ağ bağlantısı ile donatılmış fiziksel nesnelerin veya "şeylerin" bir ağıdır. Bu nesneler birbirleriyle iletişim kurabilmekte ve veri alışverişi yapabilmektedir. IoT kavramı ilk kez 1990'ların sonlarında İngiliz teknoloji öncüsü Kevin Ashton tarafından kullanılmıştır. O zamanlar kavram

sadece lojistik ve tedarik zinciri yönetimi gibi birkaç özel alanda kullanılmıştır. Ancak, teknoloji ilerledikçe IoT'nin potansiyeli daha da artmıştır. Sonraki on yıl boyunca IoT gelişmeye ve genişlemeye başlamış ve giderek daha fazla cihaz internete bağlanmıştır. Bu da Wi-Fi ve Bluetooth gibi kablosuz ağ teknolojilerinin yaygın olarak benimsenmesi ile mümkün hale gelmiştir. Akıllı telefonlar ile diğer mobil cihazların yaygın kullanımı ve internete bağlanması da bu gelişmede önemli bir rol oynamıştır. 2010'ların başlarında IoT teknolojileri hem teknoloji endüstrisi hem de genel halk tarafından geniş çapta ilgi görmeye başlamıştır. Şirketler IoT teknolojilerinin geliştirilmesine büyük yatırımlar yapmaya başlamışlar ve yeni startuplar büyüyen pazarı kullanmak için ortaya çıkmıştır. IoT'nin potansiyel uygulamaları akıllı evler ve şehirlerden endüstriyel otomasyona ve sağlık sektörüne kadar uzanmaktadır. Bugün, IoT yaşamımızın ayrılmaz bir parçası haline gelmiştir ve milyarlarca [4] cihaz günlük olarak internete bağlanarak veri alışverişi yapmaktadır. IoT cihazları insanların sağlık durumlarını izlemek, evlerini kontrol etmek ve hatta arabaların insansız olarak yönetimi için kullanılmaktadır. Ayrıca IoT, yeni iletişim, otomasyon ve kontrol yöntemlerinin oluşturulmasına imkan sağlamaktadır.

IoT'nin insan hayatında kullanılmaya başlamasıyla beraber, yukarıda bahsedilen insan hayatına sağladığı önemli katkılarına rağmen, özellikle güvenlik ve gizlilik konusunda birçok risk ve zorluk da beraberinde ortaya çıkmıştır. IoT cihazları tarafından üretilen büyük miktarda veri genellikle hassas ve kişisel nitelikte olup, bu verilerin nasıl toplandığı, depolandığı ve kullanıldığı konusunda güvenlik endişeleri ortaya çıkmıştır. IoT teknolojisi geliştikçe, bu konuların ele alınması ve teknolojinin faydalarının tüm insanlık tarafından paylaşılması önemli olacaktır.

2.2.2. IoT Kullanım Alanları

IoT, birçok farklı uygulama ve kullanım alanı olan hızla genişleyen bir teknoloji alanıdır. IoT kullanım alanlarından biri endüstriyel otomasyondur. IoT sensörleri, performans, verimlilik ve bakım ihtiyaçları hakkında değerli veriler sağlayarak makineleri ve ekipmanları gerçek zamanlı olarak izlemek için kullanılmaktadır. Bu veriler, üretim süreçlerini optimize etmek, duruş süresini azaltmak ve genel verimliliği artırmak için kullanılmaktadır. Ayrıca, IoT teknolojisi envanter yönetimi ve kalite kontrol gibi görevlerde işlemleri otomatikleştirmek, optimize etmek ve maliyetleri azaltmak için kullanılmaktadır.

IoT'nin giderek artan kullanıldığı bir diğer alan ise önceki maddelerde de belirtilen akıllı şehirlerdir. IoT sensörleri ve cihazları, trafik akışı, hava kalitesi ve atık yönetimi gibi kentsel yaşamın çeşitli yönlerini izlemek ve yönetmek için kullanılmaktadır. Bu, kirlilik, trafik sıkışıklığı ve diğer kentsel sorunları azaltarak sakinlerin yaşam kalitesini artırmaya yardımcı olmaktadır. Ayrıca IoT teknolojisi, şehirleri daha sürdürülebilir ve çevre dostu hale getirmek, enerji tüketimini optimize etmek ve genel enerji kullanımını azaltmak için kullanılmaktadır.

Sağlık, IoT'nin giderek artan kullanıldığı bir başka alandır. IoT cihazları, hastaların hayati değerlerini izlemek, ilaç kullanımını takip etmek ve hastanın sağlık durumu hakkında gerçek zamanlı veri sağlamak için kullanılmaktadır. Bu da sağlık hizmeti sağlayıcılarının potansiyel sağlık sorunlarını erken teşhis etmelerini sağlayarak, hastalığı önlemek veya yönetmek için proaktif önlemler almalarına olanak sağlamaktadır. Ayrıca IoT teknolojisi, ilaç hatırlatıcıları ve hasta programlama gibi rutin sağlık görevlerini otomatikleştirmek için kullanıldığı taktirde sağlık çalışanlarının yükünü azaltmak için ve genel verimliliği artırmak için kullanılabilmektedir.

IoT teknolojisi, ulaşım alanında da giderek artan bir kullanım alanı bulmaktadır. IoT sensörleri, araç performansını izlemek, araçların konumunu takip etmek ve trafik koşulları hakkında gerçek zamanlı veri sağlamak için kullanılmaktadır. Bu sayede ulaşım rotalarını optimize etmeye, trafik sıkışıklığını azaltmaya ve genel verimliliği artırmaya yardımcı olmaktadır.

2.2.3. IoT’nin İnsan Hayatına Katkısı

IoT, son yılların en popüler teknolojilerinden biri haline gelmiştir. Bu teknoloji, sağlık kuruluşlarından küçük ev aletlerine, fabrikalarda kullanılan makinelerden giyilebilir teknolojilere kadar pek çok alanda mikroişlemcilerle kontrol edilen cihazları internete bağlamayı sağlamaktadır. Bu cihazlar, gerçek dünyadan veri toplamakta, bu verileri işlemekte ve bilgi işlem merkezlerine aktararak ve bazı bilgi tabanlı hizmetler sunarak, gerekli aksiyonları almaktadır.

Nesnelerin interneti teknolojisi, lojistik, ulaşım, akıllı cihazlar, akıllı tarım, akıllı sağlık gibi pek çok alanda kullanılmayı hedeflemektedir ve 2025 yılına kadar 75 milyar cihaza entegre edilmesi beklenmektedir. Bu durum, McKinsey Global Institute tarafından 11 trilyon dolarlık ekonomik büyüme potansiyeli olarak tahmin edilmiştir. Ancak, bu gelişimle birlikte güvenlik kaygıları da artmıştır.

IoT yukarıda belirtilen çeşitli alanlarda kullanılarak insan hayatına önemli katkılar sağlamaktadır. Bunların başında artan verimlilik, geliştirilmiş sağlık ve güvenlik, artırılmış konfor ve kolaylık gelmektedir. IoT sensörleri ve cihazları, endüstriyel üretimden ev otomasyonuna kadar birçok süreci izlemek ve optimize etmek için kullanılmaktadır. Gerçek zamanlı performans ve kullanım verileri sağlayarak, proaktif önlemler alınmasına olanak tanımaktadır.

2.2.4. IoT Teknolojileri ve Protokolleri

IoT kavramı beraberinde kendine özgü protokollerin de ortaya çıkmasına neden olmuştur. Çünkü IoT, cihazların birbirleriyle iletişim kurmasını ve veri alışverişi yapmasını sağlamak için çeşitli protokollere ihtiyaç duyan hızla genişleyen bir teknoloji alanıdır. Protokol, cihazlar arasında veri iletimini yöneten kurallar ve prosedürler kümesidir. Yaygın olarak kullanılan IoT protokollerinin OSI (Open Systems Interconnection) katmanlarına göre dağılımı aşağıda belirtilmiştir.

Fiziksel Katman (Physical Layer)

Zigbee

Düşük veri hızları ve düşük güç tüketimi gerektiren kablosuz ağlar için geliştirilmiş bir protokoldür. IEEE 802.15.4 standardına dayanan Zigbee, özellikle akıllı ev otomasyonu, endüstriyel kontrol sistemleri ve sağlık izleme uygulamalarında yaygın olarak kullanılmaktadır. Zigbee'nin temel avantajları arasında düşük enerji tüketimi, düşük maliyet ve güvenilir ağ yapısı bulunmaktadır. Zigbee cihazları, mesh ağ topolojisi kullanarak birbirleriyle iletişim kurabilmekte, bu da ağın kapsama alanını genişletmektedir ve tek bir cihazın arızası durumunda bile veri iletimini sürdürebilmektedir. Ancak, Zigbee'nin veri iletim hızı düşüktür ve bu nedenle yüksek bant genişliği gerektiren uygulamalar için uygun değildir. Yine de düşük güç tüketimi ve maliyeti, Zigbee'yi birçok IoT uygulaması için ideal bir seçenek haline getirmektedir.

Bluetooth Low Energy (BLE)

Kısa mesafeli veri iletimi için tasarlanmış düşük güç tüketimli bir kablosuz protokoldür. BLE, klasik Bluetooth teknolojisine göre çok daha az enerji tüketmektedir, bu da onu giyilebilir cihazlar, sağlık izleme sistemleri ve akıllı ev uygulamaları için ideal hale getirmektedir. BLE, kısa mesafelerde veri iletimi için optimize edilmiştir ve bu nedenle özellikle kişisel alan ağlarında (Personal Area Network-PAN) yaygın olarak

kullanılmaktadır. BLE'nin temel özellikleri arasında hızlı bağlantı kurulumu, düşük gecikme süreleri ve enerji verimliliği bulunmaktadır. BLE cihazları, düşük güç tüketimi sayesinde uzun pil ömrüne sahiptir ve bu da onları sürekli izleme gerektiren uygulamalar için uygun hale getirmektedir. Ancak, BLE'nin kısa menzili, geniş alanlarda veri iletimi için kısıtlayıcı olabilmektedir.

LoRa (Long Range)

Düşük veri hızlarıyla uzun mesafelerde iletişim sağlamak için tasarlanmış bir kablosuz protokoldür. LoRaWAN, LoRa protokolünü kullanan geniş alan ağları (Wide Area Network-WAN) için bir standarttır. LoRa, özellikle akıllı şehir uygulamaları, tarım, çevresel izleme ve endüstriyel IoT çözümlerinde yaygın olarak kullanılmaktadır. LoRa'nın temel avantajları arasında düşük güç tüketimi, geniş kapsama alanı ve yüksek veri güvenilirliği bulunmaktadır. LoRa cihazları, lisanssız frekans bantlarında çalışmakta ve bu da iletişim maliyetlerini düşürmektedir. LoRaWAN ağları, yıldız topolojisi kullanarak veri iletimini sağlamakta ve bu sayede büyük ölçekli dağıtımlarda etkili bir şekilde çalışabilmektedir. LoRa'nın düşük veri iletim hızı, yüksek bant genişliği gerektiren uygulamalar için sınırlayıcı olabilmektedir. Buna rağmen, geniş kapsama alanı ve enerji verimliliği, LoRa'yı birçok IoT uygulaması için uygun bir seçenek haline getirmektedir.

Veri Bağlantı Katmanı (Data Link Layer)

IEEE 802.15.4

Düşük veri hızları ve düşük güç tüketimi gerektiren Kablosuz Kişisel Alan Ağları (Wireless Personal Area Network-WPAN) için bir standarttır. Bu standart, Zigbee, 6LoWPAN ve diğer düşük güç protokollerinin temelini oluşturmaktadır. IEEE 802.15.4, kısa menzilli iletişim için optimize edilmiştir ve özellikle düşük veri oranlarıyla yüksek güvenilirlik sağlamaktadır. Standart, fiziksel ve Medya Erişim Kontrol (Media Access Control-MAC) katmanlarını kapsamakta, bu da veri iletimini ve ağ oluşturmayı sağlamaktadır. IEEE 802.15.4 cihazları, düşük güç tüketimi sayesinde uzun pil ömrüne sahiptir ve bu da onları enerji verimliliği gerektiren uygulamalar için ideal kılmaktadır. Özellikle sensör ağları, endüstriyel kontrol sistemleri ve akıllı şehirler gibi alanlarda yaygın olarak kullanılmaktadır.

WiFi

Yüksek veri hızları ve geniş kapsama alanı sağlayan kablosuz bir ağ standardıdır. IEEE 802.11 ailesine ait olan kablosuz sadakat (Wireless Fidelity-WiFi), geniş bir cihaz yelpazesi arasında veri iletimi sağlar ve ev, ofis, kamu alanları gibi birçok ortamda yaygın olarak kullanılır. WiFi, yüksek bant genişliği gerektiren uygulamalar için uygundur ve video akışı, dosya paylaşımı, internet erişimi gibi faaliyetlerde kullanılmaktadır. WiFi ağları, güçlü güvenlik protokolleri *(WiFi Korumalı Erişim 2-WiFi Protected Access 2-WPA2, WiFi Protected Access 3-WPA3 gibi)* ve geniş kapsama alanı sunmaktadır. WiFi cihazları genellikle yüksek enerji tüketimi nedeniyle batarya ömürleri sınırlıdır, bu da sürekli güç kaynağı gerektiren uygulamalar için uygun hale getirmektedir. IoT uygulamalarında, WiFi genellikle yüksek veri hızları ve güvenilir bağlantı gerektiren senaryolarda tercih edilmektedir.

Ağ Katmanı (Network Layer)

IPv6

Internet Protokol versiyon 6 (IPv6), internet üzerinden veri paketlerinin iletilmesini sağlayan bir protokoldür ve özellikle IoT cihazları için geniş bir adresleme alanı sunmaktadır. IPv6, adres alanının genişliği sayesinde, IoT cihazlarının benzersiz IP adresleri almasını sağlamakta ve her cihazın doğrudan internet üzerinden erişilebilir olmasını mümkün kılmaktadır. IPv6, gelişmiş yönlendirme ve otomatik yapılandırma özellikleri sunmakta ve ağ yönetimini kolaylaştırmaktadır. Ayrıca, güvenlik protokolleri *(IP Security-IPsec)* ve mobilite desteği ile entegre edilmiştir, bu da veri iletimini daha güvenli ve esnek hale getirmektedir. IPv6, IoT ve IIoT cihazlarının büyük ölçekli dağıtımlarında kritik bir rol oynamakta ve ağ performansı ile güvenliğini artırmaktadır.

RPL

Düşük güçlü ve kayıplı ağlar için tasarlanmış bir yönlendirme protokolüdür. Düşük Güçlü ve Kayıplı Ağlar İçin Yönlendirme Protokolü (Routing Protocol for Low-Power and Lossy Networks-RPL), özellikle kablosuz sensör ağları ve IoT cihazları gibi düşük enerji tüketimi ve yüksek veri kaybı riski olan ağlar için optimize edilmiştir. RPL, cihazlar arasında yönlendirme yolları oluşturmakta ve veri paketlerinin güvenli bir şekilde hedeflerine ulaşmasını sağlamaktadır. Protokol, ağın dinamik doğasına uyum sağlayarak, değişen ağ koşullarına göre yönlendirme yollarını sürekli olarak güncellemektedir.

RPL’nin düşük enerji tüketimi, uzun pil ömrü ve yüksek güvenilirlik sağlaması, IoT ve IIoT uygulamalarında geniş çapta kullanılmasını sağlamaktadır.

Taşıma Katmanı (Transport Layer)

TCP

Güvenilir veri iletimi sağlayan bir taşıma katmanı protokolüdür. İletim Kontrol Protokolü (Transmission Control Protocol-TCP), verilerin doğru sırayla ve eksiksiz bir şekilde iletilmesini garanti etmektedir. Bu özellik, IoT ve IIoT cihazları arasında kritik veri iletimi gerektiren uygulamalar için ideal olup, veri iletiminde hata kontrolü, akış kontrolü ve tıkanıklık kontrolü gibi mekanizmalar kullanmaktadır. Bu sayede veri iletiminde yüksek güvenilirlik sağlamaktadır. TCP’nin sağladığı bu güvenilirlik, protokolün daha fazla kaynak tüketmesine ve veri iletiminde gecikmelere neden olabilmektedir. Bu nedenle, gerçek zamanlı veri iletimi gerektiren uygulamalarda UDP gibi daha hafif protokoller tercih edilebilmektedir.

UDP

Kullanıcı Datagram Protokolü (User Datagram Protocol-UDP), hızlı ve hafif bir veri iletimi sağlayan taşıma katmanı protokolüdür. UDP, verilerin güvenilirliği yerine hız ve düşük gecikmeye odaklanmaktadır. Bu nedenle, hata kontrolü veya veri sıralaması gibi mekanizmalar içermez. UDP, özellikle ses ve video akışı gibi gerçek zamanlı uygulamalar için idealdir. IoT ve IIoT cihazlarında, düşük gecikme süreleri ve düşük kaynak tüketimi gerektiren senaryolarda yaygın olarak kullanılmaktadır. UDP’nin güvenilirlik sağlamaması nedeniyle, veri kaybı veya hatalara toleranslı olmayan uygulamalarda dikkatli kullanılmalıdır. UDP’nin basit yapısı, protokolün hızlı ve verimli bir şekilde çalışmasını sağlamaktadır.

Uygulama Katmanı

MQTT

Mesaj Kuyruklama Telemetri Aktarımı (Message Queuing Telemetry Transport-MQTT), düşük bant genişliği ve yüksek gecikme süreleri için optimize edilmiş, hafif bir mesajlaşma protokolüdür. MQTT, IoT cihazları arasında veri iletimi için yaygın olarak kullanılmaktadır ve özellikle düşük güç tüketimi ve güvenilir veri iletimi gerektiren uygulamalar için idealdir. Protokol, yayınlama/abone olma *(publish/subscribe)* modeline dayanmakta ve cihazların belirli konulara abone olarak veri almasını veya bu konulara

veri yayınlamasını sağlamaktadır. MQTT'nin basitliği ve esnekliği, protokolün akıllı ev otomasyonu, sağlık izleme sistemleri ve endüstriyel otomasyon gibi çeşitli IoT uygulamalarında yaygın olarak kullanılmasını sağlamaktadır. Protokol, güvenlik için de (Güvenli Soket Katmanı-Secure Sockets Layer-SSL / Taşıma Katmanı Güvenliği-Transport Layer Security-TLS) ile şifreleme desteği sunmaktadır.

CoAP

Kısıtlı Uygulama Protokolü (Constrained Application Protocol-CoAP), kısıtlı kaynaklara sahip cihazlar için tasarlanmış hafif bir uygulama katmanı protokolüdür. CoAP, Hiper Metin Aktarım Protokolü (Hypertext Transfer Protocol-HTTP)'ye benzer şekilde çalışmaktadır, ancak daha az bant genişliği tüketmekte ve düşük güç tüketimi sağlamaktadır. CoAP, IoT cihazlarının web hizmetlerine erişimini kolaylaştırır ve makine-makine (M2M) iletişimi için optimize edilmiştir. Protokol, UDP üzerinde çalışmakta ve veri iletiminde hızlı yanıt süreleri sağlamaktadır. CoAP'ın temel özellikleri arasında küçük mesaj boyutları, düşük gecikme süreleri ve kolay entegrasyon bulunmaktadır. Akıllı enerji yönetimi, çevresel izleme ve akıllı tarım gibi uygulamalarda yaygın olarak kullanılmaktadır.

HTTP

Hiper Metin Aktarım Protokolü (Hypertext Transfer Protocol-HTTP), internet üzerinden veri iletimi için yaygın olarak kullanılan bir uygulama katmanı protokolüdür. HTTP, web sayfalarının ve web hizmetlerinin temelini oluşturmaktadır. IoT cihazlarının web tabanlı uygulamalarla entegrasyonunu sağlar. HTTP, veri iletiminde güvenilirlik sağlar ve geniş bir cihaz yelpazesi tarafından desteklenmektedir. HTTP'nin yüksek bant genişliği ve enerji tüketimi gerektirmesi, düşük güç tüketimi gerektiren IoT cihazları için bir dezavantaj olabilmektedir. Buna rağmen, HTTP'nin yaygın kullanımı ve mevcut web altyapısıyla uyumu, protokolün IoT uygulamalarında sıkça tercih edilmesine neden olmaktadır. Güvenlik için HTTP yerine HTTPS *(güvenli-secure)* kullanılmaktadır.

SCADA (Supervisory Control and Data Acquisition - Gözetleyici Kontrol ve Veri Toplama Sistemi) Cihaz İletişim Protokolleri

MODBUS (Modicon-Bus)

MODBUS, endüstriyel otomasyon sistemlerinde veri iletimi için yaygın olarak kullanılan bir haberleşme protokolüdür. İlk olarak 1979'da Modicon (şimdi Schneider Electric) tarafından geliştirilen MODBUS, ana cihaz ve alt cihazlar arasında veri iletimini

sağlamaktadır. Protokol, basitliği ve esnekliği ile bilinir ve çeşitli endüstriyel cihazlar ile kontrol sistemleri tarafından desteklenmektedir. MODBUS, TCP/IP üzerinde (MODBUS TCP) veya seri hatlar üzerinden (MODBUS RTU) çalışabilmektedir. Veri blokları olarak iletilen bilgiler, cihazlar arasında okunabilir ve yazılabilir. MODBUS, düşük maliyeti ve yaygın desteği nedeniyle endüstriyel otomasyon sistemlerinde, SCADA sistemlerinde ve enerji yönetiminde geniş bir kullanım alanına sahiptir.

Profibus

İşlem Alanı Veri Yolu (Process Field Bus-Profibus), Siemens tarafından geliştirilen ve endüstriyel otomasyon sistemlerinde yaygın olarak kullanılan bir haberleşme protokolüdür. Profibus, endüstriyel cihazlar arasında yüksek hızlı ve güvenilir veri iletimi sağlamaktadır. Protokol, özellikle proses otomasyonu ve üretim otomasyonu için tasarlanmıştır. Profibus, iki ana varyanta sahiptir: Profibus DP *(Merkezi Olmayan Çevre Birimleri-Decentralized Peripherals)* ve Profibus PA *(Süreç Otomasyonu-Process Automation)*. Profibus DP, hızlı veri iletimi gerektiren uygulamalar için optimize edilmiştir ve genellikle üretim otomasyonunda kullanılmaktadır. Profibus PA ise patlayıcı ortamlar gibi zorlu endüstriyel koşullarda güvenli veri iletimi sağlamaktadır. Profibus güvenilirliği, yüksek veri hızları ve geniş uyumluluğu ile endüstriyel otomasyon projelerinde yaygın olarak tercih edilmektedir.

DNP3

Dağıtık Ağ Protokolü (Distributed Network Protocol-DNP3), elektrik ve su dağıtım sistemleri gibi kritik altyapıların SCADA sistemlerinde veri iletimi için kullanılan bir haberleşme protokolüdür. DNP3, uzaktan veri toplama ve kontrol için optimize edilmiştir ve özellikle güvenilirliği, esnekliği ve hata toleransı ile bilinmektedir. Protokol, uzak cihazlardan veri toplamak, alarmları yönetmek ve kontrol komutlarını iletmek için kullanılmaktadır. DNP3, hem seri iletişim hatları hem de TCP/IP ağları üzerinde çalışabilmektedir. Güvenlik özellikleri, zaman senkronizasyonu ve veri bütünlüğü sağlama kabiliyeti ile DNP3, SCADA sistemlerinde yaygın olarak kullanılan güvenilir bir iletişim protokolüdür. DNP3, özellikle enerji dağıtım sistemlerinde standart bir protokol haline gelmiştir.

Bu protokoller, OSI modelinin farklı katmanlarında çalışarak IoT, IIoT ve SCADA cihazlarının birbirleriyle ve ağlarla etkin bir şekilde iletişim kurmasını sağlamaktadır. Her bir protokolün kendine özgü avantajları ve açıklıkları bulunmaktadır.

2.3. Endüstriyel Nesnelerin İnterneti (IIoT)

2.3.1. IIoT Kavramının Ortaya Çıkışı

İleri teknoloji ürünü IoT'lerin endüstriyel süreçler ile entegrasyonu sonucunda Endüstriyel Nesnelerin İnterneti (Industrial Internet Of Things-IIoT) kavramı ortaya çıkmıştır. IIoT, sensörlerin, yazılımların ve ağ bağlantısının kullanımıyla endüstriyel ekipman ve süreçlerin izlenmesi ve kontrol edilmesini amaçlamaktadır. Aynı zamanda operasyonları optimize etmeyi ve verimliliği artırmayı hedeflemektedir. Sensörlerin ve otomasyon sistemlerinin üretim endüstrisinde kullanımının giderek yaygınlaşmaya başlaması sonucunda, 2000'li yılların başlarına IIoT kavramı ortaya çıkmıştır.

İlk çıktığı yıllarda bu sistemler, montaj hatları ve kalite kontrol sistemleri gibi üretim süreçlerinin izlenmesi ve kontrol edilmesi için kullanılmaktaydı. Ancak, sensörlerin ve ağ teknolojilerinin maliyeti azaldıkça, IIoT'nin potansiyeli daha da açık hale gelmiştir. Son on yılda IIoT gelişmiş, genişlemiş ve giderek daha fazla endüstriyel cihaz internete bağlanmaya başlamıştır. Bu süreç, Wi-Fi ve Bluetooth gibi kablosuz ağ teknolojilerinin yaygın olarak benimsenmesiyle daha da hızlanmıştır. 2010'lu yılların başlarında, IIoT teknolojileri hem teknoloji endüstrisi hem de endüstriyel sektör tarafından geniş çapta dikkat çekmeye başlamıştır. IIoT'nin potansiyel uygulamaları, endüstriyel otomasyon ve erken müdahale bakımından, tedarik zinciri yönetiminden varlık takibine kadar çok çeşitli alanlarda önemli katkılar sağlamaktadır. Halihazırda IIoT, milyarlarca cihazın günlük olarak internete bağlı olduğu ve veri alışverişi yaptığı endüstriyel süreçlerin yaygın bir parçasıdır. IIoT'nin endüstriyel süreçlere etkisi önemli olmuş, iletişim, otomasyon ve kontrol gibi yeni formların ortaya çıkmasını sağlamıştır.

IIoT teknolojileri, insan hayatını kolaylaştırıcı bileşenler üzerinde yoğunlaşarak verimlilik, hız ve etkinlik gibi faktörleri öne çıkarmaktadır. Ancak, teknolojilerin açıklıklarından faydalanarak ortaya çıkan saldırılar, maliyet ve insan hayatını tehdit eden sonuçlar doğurmuştur. Bu nedenle, akıllı bina ve akıllı şehir gibi projelerin kullanımı yaygınlaşırken, güvenlik önlemleri de önem kazanmıştır.

2.3.2. IIoT Kullanım Alanları

Endüstriyel Nesnelerin İnterneti (IIoT), endüstriyel ortamlarda birçok farklı uygulama ve kullanım alanına sahiptir. IIoT kullanım alanlarının anahtar alanlarından biri endüstriyel otomasyondur. IIoT sensörleri, makineleri ve ekipmanları gerçek zamanlı olarak izlemek

için kullanılabilir, performans, verimlilik ve bakım gereksinimleri hakkında endüstriyel kurumlar için kritik veriler sağlamaktadır. Bu veri, üretim süreçlerinin optimize edilmesi, iş sürekliliğinin sağlanması ve genel üretkenliğin artırılması için kullanılmaktadır. Ayrıca IIoT teknolojisi, envanter yönetimi ve kalite kontrol gibi görevlerin otomatikleştirilmesi ile süreçlerin optimize edilerek maliyetlerin azaltılmasına yardımcı olmaktadır.

IIoT'nin artan kullanım alanlarından bir diğeri sistemsel hata ve erken arıza tespitidir. IIoT sensörleri ve cihazları, ekipmanları izleyerek bakım gereksinimlerinin ne zaman olacağını tahmin ederek, ekipman arızası meydana gelmeden önce gerçek zamanlı performans ve kullanım verileri sağlamaktadır. Bu, bakım personelinin ekipman sürekliliğini sağlayarak, proaktif önlemler almasını temin etmektedir.

Varlık takibi, IIoT'nin diğer bir kullanım alanıdır. IIoT cihazları, endüstriyel ekipman ve araçların konumlarını gerçek zamanlı olarak takip etmek için kullanılmaktadır. Bu, ekipmanların kullanılabilirliğini artırmaya, iş süreçlerini optimize etmeye ve kaynakları daha verimli bir şekilde kullanmaya yardımcı olmaktadır.

Tedarik zinciri yönetimi de IIoT teknolojisinin önemli bir kullanım alanıdır. IIoT sensörleri, nakliye ve depolama gibi tedarik zinciri işlemlerinin izlenmesi için kullanılmaktadır. Bu veriler, işletmelerin lojistik süreçlerini optimize etmelerine ve maliyetleri azaltmalarına yardımcı olmaktadır.

Son olarak, akıllı fabrikalar da IIoT'nin kullanım alanları arasındadır. Bu sayede, üretim süreçleri daha verimli hale getirilerek, iş süreçleri daha fazla otomatikleştirilmektedir. Bu, üretimdeki hatalar ile atıkları azaltarak kaliteyi artırmaya ve maliyetleri azaltmayı sağlamaktadır.

2.3.3. IIoT’nin İnsan Hayatına Etkileri

Endüstriyel Nesnelerin İnterneti (IIoT), bağlı cihazların ve sensörlerin endüstriyel ve üretim ortamlarında verimlilik, üretkenlik ve güvenliği artırmak için kullanılmasını ifade eder. IIoT, birçok şekilde insan hayatını geliştirmektedir:

İyileştirilmiş Verimlilik: IIoT, endüstriyel süreçlerin otomatikleştirilmesini ve optimize edilmesini sağlayarak önemli maliyet tasarrufları ve artan üretkenlik sağlamaktadır.

Daha Güvenli Çalışma Ortamı: IIoT sensörleri, ekipmanları izleyerek ve olası tehlikeleri tespit ederek iş güvenliğini artırır ve kazaların riskini azaltmaktadır.

Daha İyi Kalite Kontrolü: IIoT cihazları, ürün kalitesi hakkında gerçek zamanlı veri toplayarak üreticilerin sorunları tespit etmelerine ve yaygın hale gelmeden önce düzeltmelerine olanak sağlamaktadır.

Uzaktan İzleme ve Kontrol: IIoT, endüstriyel süreçlerin uzaktan izlenmesi ve kontrol edilmesini sağlayarak insan müdahalesine olan ihtiyacı azaltarak, endüstriyel ekipmanın güvenilirliğini ve çalışma süresini artırmaktadır.

Erken Müdahale: IIoT sensörleri, ekipman performansını izlemek ve bakımın ne zaman gerektiğini öngörmek için kullanılmaktadır. Bu sayede, iş sürekliliğini artırmakta ve bakım maliyetlerini azaltmaktadır.

Genel olarak IIoT, endüstriyel süreçlerin verimliliğini, güvenliğini ve üretkenliğini artırarak insan hayatı üzerinde önemli bir etkiye sahiptir. IIoT, endüstriyel sistemlerde otomatikleştirmeyi ve optimize etmeyi mümkün kılarak, maliyetleri azaltmakta ve aynı zamanda üretkenliği artırarak, işçiler ve tüketicilerin yaşam kalitesini iyileştirmektedir.

Yukarıda belirtilen endüstriyel sistemlerin işleyişine önemli katkılar sağlamasının yanında IIoT, özellikle siber güvenlik ile ilgili olarak önemli yeni tehdit yüzeyleri ve buna bağlı olarak da çeşitli risklerin ortaya çıkmasına neden olmuştur. IIoT cihazları tarafından üretilen büyük miktardaki veri sıklıkla hassas ve kurumların öz bilgisini (know-how) içermekte olup, bu verinin nasıl toplandığı, depolandığı ve kullanıldığı konusunda önemli güvenlik endişelerini ortaya çıkarmaktadır. Teknolojideki yeni iletim ortamlarının ve yöntemlerinin ortaya çıkmasına bağlı olarak IIoT'nin devam eden gelişimi ile birlikte, bu sorunların ele alınması ve teknolojinin gelişiminden endüstrinin yeterince faydalanılması açısından gerekli güvenlik testlerinin yapılması oldukça önemlidir.

IoT ve IIoT ortamlarında siber güvenlik kritik bir endişedir, çünkü bağlı cihazların ve sensörlerin yaygınlaşması siber suçlular için yeni zayıf noktalar ve saldırı vektörleri oluşturmaktadır. Hem IoT hem de IIoT ortamlarında önemli olan bazı temel siber güvenlik kavramları:

Kimlik Doğrulama ve Yetkilendirme: Kimlik doğrulama ve yetkilendirme, IoT ve IIoT ortamlarında temel güvenlik önlemleridir. Sadece yetkili cihazların veya kullanıcıların ağa, verilere veya cihazlara erişebildiğinden emin olmaya yardımcı olmaktadır. Bunun için beyaz veya siyah listeleme (white/black listing) yöntemleri kullanılabilmektedir.

Şifreleme: Şifreleme, verilerin yetkisiz kullanıcılar tarafından anlamlı hale getirilmesini engelleyen ve bu sayede sadece yetkili kullanıcılar tarafından açık hale getirilerek

kullanılmasını sağlayan bir güvenlik önlemidir. Şifreleme, verilerin şifreleme anahtarı olmadan okunamayacak şekilde olmasını sağlamaktadır.

Ağ Bölümlendirme: Ağ bölümlendirme, bir ağı daha küçük, izole edilmiş segmentlere ayırma işlemidir. Verilere sadece yetkisi ve bilmesi gereken prensibine dayanarak erişim sağlayan önemli bir güvenlik önlemidir. Aynı zamanda kötü amaçlı yazılımların veya siber saldırıların yayılmasını da önlemektedir.

Yetkisiz Erişim Algılama ve Önleme: Yetkisiz erişim algılama ve önleme sistemleri, siber tehditleri gerçek zamanlı olarak tespit etmek ve gerekli önlemlerin alınmasını sağlamak için tasarlanmıştır. Bu sistemler, imza temelli tespit, anormallik tespiti ve davranış analizi gibi çeşitli teknikler kullanarak siber saldırıları tespit etmek ve önlemek için kullanılmaktadır.

Sürekli İzleme: Sürekli izleme, ağı sürekli olarak izleyerek güvenlik tehditleri ve anormallikleri tespit etmek için kullanılan bir süreçtir. Potansiyel güvenlik tehditlerini belirlemek için günlük analizi, ağ trafiği analizi ve tehdit istihbaratı gibi güvenlik araçları ve tekniklerinin kullanılmasını içermektedir.

Yama Yönetimi: Yama yönetimi, tüm yazılım ve donanım yazılımının (firmware) en son güvenlik yamaları ve güncellemelerle güncel tutulmasını sağlamayı içermektedir. Böylece bilinen zayıf noktaların kapatılmasını sağlamaktadır.

IIoT ortamlarında, kritik altyapı ve varlıkları korumak için güvenlik duvarları, erişim kontrol sistemleri ve fiziksel güvenlik önlemleri gibi ek güvenlik önlemleri de kullanılmaktadır. IoT veya IIoT ortamının belirli ihtiyaçlarını ve gereksinimlerini dikkate alan kapsamlı bir siber güvenlik stratejisi uygulamak ve gelişen tehditlere karşı sürekli olarak güvenlik önlemlerini izlemek ve güncellemek önemlidir.

2.3.4. IIoT Protokolleri

Endüstride halihazırda yaygın olarak kullanılan MODBUS, Profibus, DNP3 protokollerine IIoT kavramı ile yeni protokoller eklenmiştir. Endüstriyel cihazlar ile IoT sensörleri arasındaki iletişim için kullanılan IIoT protokollerinden bazıları:

MQTT (Message Queuing Telemetry Transport): Bu protokol düşük bant genişliği ve yüksek gecikmeli ağlar için yaygın olarak kullanılır ve makine-makine (Machine to Machine-M2M) iletişimi için tasarlanmıştır.

CoAP (Constrained Application Protocol): CoAP, düşük güçlü cihazlar için tasarlanmış hafif bir protokoldür ve düşük gecikme gerektiren uygulamalarda kullanılmaktadır.

OPC UA (Open Platform Communications Unified Architecture): Bu protokol endüstriyel otomasyonda yaygın olarak kullanılmaktadır. Cihazlar arasında güvenli ve güvenilir iletişim sağlamaktadır.

DDS (Data Distribution Service): DDS gerçek zamanlı sistemler için yaygın olarak kullanılan bir protokoldür ve cihazlar arasında yüksek performanslı, ölçeklenebilir iletişim sağlamak için tasarlanmıştır.

AMQP (Advanced Message Queuing Protocol): AMQP güvenilir ve güvenli iletişim sağlamak için tasarlanmış bir mesajlaşma protokolüdür. Endüstriyel ve finansal uygulamalarda yaygın olarak kullanılmaktadır.

IIoT protokolü seçimi, bant genişliği, gecikme, güvenlik ve ölçeklenebilirlik gibi uygulamanın belirli gereksinimlerine bağlıdır. Farklı protokoller farklı cihaz ve uygulamalar için daha uygun olmaktadır. Bu nedenle, bir protokol seçilmeden önce sistemin gereksinimlerini ve sınırlamalarını dikkatlice değerlendirmek önemlidir.

2.4. IoT ve IIoT Sistemlerinde Kullanılan Saldırı ve Savunma Yöntemleri

IoT ve IIoT sistemleri, Hizmet Reddi (Denial of Service - DoS) saldırıları, kötü amaçlı yazılım enfeksiyonları ve veri ihlalleri gibi geniş bir yelpazede siber saldırılara karşı savunmasızdır. Bu saldırılara karşı korunmak için savunma ve saldırı stratejileri kullanılmaktadır. IoT ve IIoT sistemlerinde yaygın olarak kullanılan saldırı ve savunma yöntemleri:

Hizmet Reddi (Denial of Service - DoS) ve Dağıtık Hizmet Reddi (Distributed Denial of Service - DDoS) Saldırıları

Hizmet Reddi (DoS) ve Dağıtık Hizmet Reddi (DDoS) saldırıları, bir sistemin aşırı yüklenmesine neden olarak hizmet veremeyecek duruma getirilmesi amacıyla gerçekleştirilen saldırılardır. DoS saldırıları, tek bir kaynaktan gelen büyük miktarda trafik ile hedef sistemi meşgul ederken, DDoS saldırıları, çok sayıda farklı kaynaktan eş zamanlı olarak gönderilen trafik ile daha büyük bir etki yaratmayı hedeflemektedir. Bu saldırıların temel amacı, yetkili kullanıcıların sistem kaynaklarına erişimini engelleyerek hizmet kesintisine neden olmaktır. DDoS saldırıları, botnet adı verilen kötü amaçlı yazılımlar tarafından ele geçirilmiş çok sayıda bilgisayarın senkronize olarak hedef

sisteme trafik göndermesiyle gerçekleştirilmektedir. Bu tür saldırılar, hedef sistemin bant genişliğini, işlem gücünü veya bellek kaynaklarını tüketerek, sistemi çökertir veya yanıt veremez hale getirmektedir. Ayrıca DoS ve DDoS saldırılarının diğer bir kullanım maksadı da yetkili kullanıcının dikkatini sistem kaynaklarına yönelterek, diğer taraftan hatalı veri enjeksiyonu, veri sızıntısı gibi başka saldırıların eş zamanlı olarak gerçekleştirilmesidir.

Bu saldırılara karşı kullanılan kimi savunma mekanizmaları ise; ağ filtreleme, hız sınırlama ve yedeklilik gibi teknikler kullanılmaktadır:

Ağ Filtreleme: Gelen trafik analiz edilerek zararlı trafik paketleri tespit edilmekte ve engellemektedir. Özellikle, önceden tanımlanmış saldırı imzaları kullanılarak, DoS ve DDoS saldırılarını gerçekleştiren trafik filtrelenmektedir.

Hız Sınırlama (Rate Limiting): Belirli bir süre içinde bir kaynaktan gelen trafik miktarını sınırlandırılmaktadır. Bu sayede, anormal derecede yüksek trafik yoğunluğu tespit edildiğinde, saldırının etkisi azaltılmaktadır.

Yedeklilik (Redundancy): Sistem kaynaklarının yedekli olması, bir saldırı durumunda alternatif kaynakların devreye girmesini sağlamaktadır. Yedeklilik, yük dengeleme (load balancing) ve coğrafi dağıtımlı sunucular kullanılarak sağlanabilmektedir. Bu da sistemin yüksek trafiğe karşı dirençli olmasını sağlamakta ve hizmet kesintilerini en aza indirmektedir.

Kötü Amaçlı Yazılım ve Fidye Yazılımı Saldırıları

Kötü amaçlı yazılım ve fidye yazılımı saldırıları, cihazları ve sistemleri enfekte ederek çeşitli zararlar vermeyi amaçlamaktadır. Kötü amaçlı yazılımlar (malware), sistemlere gizlice sızarak veri çalma, veri yok etme ve sistem işleyişini bozma gibi faaliyetlerde bulunmaktadır. Fidye yazılımları (ransomware) ise, kullanıcı verilerini şifreleyerek erişilemez hale getirmekte ve bu verilerin yeniden erişilebilir olması için fidye talep etmektedir. Bu tür saldırılar, kullanıcıların verilerini ve sistem kaynaklarını kontrol altına alarak büyük ölçüde zarara neden olabilmektedir.

Bu saldırılara karşı etkili savunma mekanizmaları arasında son kullanıcı güvenlik yazılımları, yazılım (firmware) güncellemeleri ve davranışsal analiz bulunmaktadır:

Son Kullanıcı Güvenlik Yazılımları: Antimalware yazılımları, Endpoint Detection and Response (EDR) ve Extended Detection and Response (XDR) gibi araçlar, kötü amaçlı

yazılımları tespit etmekte ve engellemektedir. Bu yazılımlar, sistemdeki anormal faaliyetleri izleyerek, zararlı aktiviteleri önlemek için gerekli önlemleri almaktadır.

Yazılım Güncellemeleri: Cihazların yazılımlarını düzenli olarak güncellemek, bilinen güvenlik açıklarının kapatılmasını sağlamaktadır. Üreticiler tarafından yayınlanan güncellemeler, cihazları en son tehditlere karşı korunmasını sağlamaktadır.

Davranışsal Analiz: Sistemlerin normal işleyişini öğrenen ve anormal davranışları tespit eden yazılımlar, kötü amaçlı faaliyetleri erken aşamada belirleyebilmektedir. Bu tür yazılımlar, kullanıcı davranışlarını analiz ederek, alışılmadık aktiviteleri hızlı bir şekilde tanımlamakta ve müdahale etmektedir.

Ortadaki Adam Saldırıları (Man in the Middle - MitM)

Ortadaki adam saldırıları (MitM), iki taraf arasında iletilen verileri yakalamak ve değiştirmek amacıyla gerçekleştirilen saldırılardır. Saldırgan, iletişim hattına gizlice girerek, gönderilen ve alınan verileri izlemekte veya değiştirebilmektedir. Bu saldırılar, veri bütünlüğünü ve gizliliğini tehdit etmekte olup, özellikle hassas bilgilerin ele geçirilmesi için kullanılmaktadır.

MitM saldırılarına karşı savunma mekanizması olarak şifreleme, güvenli kimlik doğrulama ve karşılıklı kimlik doğrulama bulunmaktadır:

Şifreleme: İletilen verilerin şifrelenmesi, saldırganların bu verileri okuyamamasını sağlamaktadır. Özellikle, Transport Layer Security (TLS) ve Secure Sockets Layer (SSL) gibi protokoller, veri iletimini güvenli hale getirmektedir.

Güvenli Kimlik Doğrulama: Kimlik doğrulama yöntemleri, iletişime katılan tarafların kimliklerini doğrulamakta, güçlü parolalar, biyometrik doğrulama ve iki faktörlü kimlik doğrulama (2FA) gibi yöntemler, kimlik sahtekarlığını önlemektedir.

Karşılıklı Kimlik Doğrulama: İletişime katılan her iki tarafın da birbirlerinin kimliklerini doğrulaması, MitM saldırılarını önlemeye yardımcı olmaktadır. Bu yöntem ile her iki tarafın da güvenilir olduğunu teyit edilmektedir.

Sahte Kimlik Saldırıları

Sahte kimlik saldırıları, saldırganların meşru bir cihaz veya kullanıcı gibi davranarak sistem erişimi elde etmeye çalıştığı saldırı türüdür. Bu saldırılar, kimlik bilgilerinin ele geçirilerek veya sahte kimlikler oluşturarak gerçekleştirilmektedir. Sahte kimlik

saldırıları, sistem güvenliğini ciddi şekilde tehlikeye atmakta ve yetkisiz erişimlerin önünü açmaktadır.

Sahte kimlik saldırılarına karşı savunma mekanizmaları arasında güçlü kimlik doğrulama, erişim kontrolü ve anomali tespiti bulunmaktadır:

Güçlü Kimlik Doğrulama: Kimlik doğrulama süreçlerinde güçlü parolalar, biyometrik veriler ve iki faktörlü kimlik doğrulama (2FA) gibi yöntemler kullanılarak, sahte kimlik oluşturmanın önüne geçilmesi hedeflenmektedir.

Erişim Kontrolü: Erişim kontrol sistemleri, yalnızca yetkili kullanıcıların ve cihazların sistem kaynaklarına erişmesini sağlamaktadır. Rol tabanlı erişim kontrolü (Role Based Access Control - RBAC) ve öznitelik tabanlı erişim kontrolü (Attribute Based Access Control - ABAC) gibi yöntemler, erişim izinlerini kullanıcı yetkilerine göre düzenlemektedir.

Anomali Tespiti: Sistem davranışlarını izleyerek, normalden sapmalar tespit edilmektedir. Ayrıca anormal aktiviteler, potansiyel sahte kimlik saldırılarının erken aşamada belirlenmesine yardımcı olmaktadır.

Fiziksel Saldırılar

Fiziksel saldırılar, donanım ayarlarını değiştirmek, cihazları çalmak veya kablolara zarar vermek gibi yöntemlerle sistemlere fiziksel erişim sağlamayı hedeflemektedir. Bu saldırılar, cihazların fiziksel güvenliğini tehdit etmekte ve sistem işleyişini bozabilmektedir.

Fiziksel saldırılara karşı savunma mekanizmaları arasında kilitler, alarm sistemleri, kamera sistemleri ve hat kontrolü gibi fiziksel güvenlik önlemleri bulunmaktadır:

Kilitler: Cihazların ve donanım bileşenlerinin güvenliğini sağlamak için fiziksel kilitler (asma kilit, kapı kilidi gibi) kullanılmaktadır. Bu sayede, yetkisiz kişilerin cihazlara erişimi engellenmektedir.

Alarm Sistemleri: Fiziksel erişim denemeleri tespit edildiğinde, alarm sistemleri devreye girmekte, bu da hızlı müdahale ve saldırının önlenmesini sağlamaktadır.

Kamera Sistemleri: Güvenlik kameraları, fiziksel alanların izlenmesini sağlayarak yetkili/yetkisiz erişimleri kaydetmektedir. Bu da saldırıların tespit edilmesini ve kanıt toplanmasını kolaylaştırmaktadır.

Hat Kontrolü: Kabloların güvenliği sağlanarak, sabotaj ve müdahaleler engellenmektedir. Bu sayede ağ bağlantılarının güvenliğini artırılmaktadır.

Sosyal Mühendislik Saldırıları

Sosyal mühendislik saldırıları, sistem bileşenleri içerisindeki en zayıf halka olan insanları hassas bilgileri vermeye veya sistemi tehlikeye atabilecek eylemleri gerçekleştirmeye ikna etmeyi içeren saldırı türüdür. Saldırının temel hedefi, insan zafiyetleridir. Saldırganlar, manipülasyon ve aldatma tekniklerini kullanarak, hedeflerin güvenini kazanmakta ve gerekli bilgileri elde etmektedir.

Sosyal mühendislik saldırılarına karşı savunma mekanizmaları arasında farkındalık eğitimi, güvenlik politikaları ve sıkı erişim kontrolü bulunmaktadır:

Farkındalık Eğitimi: Bu eğitimler ile bütün personel (yöneticiler dahil), sosyal mühendislik saldırılarına karşı bilinçlendirilmekte ve bu tür saldırıları tanıma konusunda eğitilmektedir. Eğitimler ile insan zafiyetlerinin azaltılması hedeflenmektedir.

Güvenlik Politikaları: Güçlü güvenlik politikaları oluşturularak, hassas bilgilerin nasıl korunacağı belirlenmelidir. Bu politikalar ile veri erişimi düzenlenmekte ve yetkisiz erişimler engellemektedir.

Sıkı Erişim Kontrolü: Erişim kontrol mekanizmaları, yalnızca yetkili kişilerin hassas bilgilere erişimini sağlamaktadır. Bu sayede veri güvenliği artırılmakta ve sosyal mühendislik saldırılarının etkisini azaltılmaktadır.

2.4.1. IoT ve IIoT Ortamlarında Savunma Stratejileri

Teknik ve Organizasyonel Önlemler

IoT ve IIoT sistemlerinde savunma stratejileri; erişim kontrolü, şifreleme, sızma tespiti ve önleme ile sürekli izleme gibi teknik ve organizasyonel önlemlerin birleşimini içermektedir. Bu stratejiler, sistemlerin güvenliğini artırmak ve olası saldırılara karşı korunmak amacıyla uygulanmaktadır.

Erişim Kontrolü: Kimlik doğrulama ve yetkilendirme mekanizmaları kullanılarak, sadece yetkili kullanıcıların ve cihazların sistem kaynaklarına erişimi sağlanmaktadır.

Şifreleme: Verilerin şifrelenmesi, ağ üzerindeki iletim sırasında gizlilik ve bütünlüğün sağlanması için kullanılmaktadır. Şifreleme ile yetkisiz kişilerin verilere erişimi engellenmektedir.

Sızma Tespiti ve Önleme: Sistemlerde anormal aktiviteleri tespit eden ve önleyen yazılımlar kullanılarak, olası saldırılar erken aşamada belirlenmekte ve müdahale edilmektedir.

Sürekli İzleme: Sistemlerin 7/24 sürekli izlenmesi, güvenlik tehditlerinin zamanında tespit edilmesini sağlayarak, saldırılara karşı hızlı tepki verilmesine olanak sağlamaktadır.

Penetrasyon Testi ve Zafiyet Değerlendirmesi

Penetrasyon testi ve zafiyet değerlendirmesi gibi saldırgan stratejiler, potansiyel güvenlik açıklarını ve saldırı vektörlerini belirlemek, ayrıca sistemler üzerindeki savunma önlemlerinin etkinliğini test etmek amacıyla kullanılmaktadır. Bu yöntemler, sistemlerin güvenlik seviyesini değerlendirmek ve iyileştirme alanlarını belirlemek için önemlidir.

Penetrasyon Testi: Güvenlik uzmanları, sistemlere saldırı senaryoları uygulayarak, olası güvenlik açıklarını tespit etmekte ve bunları raporlamaktadır.

Zafiyet Değerlendirmesi: Sistemlerin mevcut güvenlik açıkları belirlenerek, açıkların kapatılması için gerekli önlemler alınmaktadır.

Belirtilen yöntemler, sistemlerin güvenlik seviyesini artırmak, güvenlik risklerini azaltmak ve sistemleri olası saldırılara karşı daha güvenli hale getirmek için uygulanmaktadır.

IoT ve IIoT ortamlarında güvenlik, sürekli olarak gözden geçirilmesi ve güncellenmesi gereken bir süreçtir. Yeni tehditlerin ve teknolojilerin ortaya çıkması, savunma stratejilerinin de sürekli olarak uyarlanmasını gerektirmektedir. Bu bağlamda, güvenlik politikaları ve prosedürleri düzenli olarak güncellenmeli ve bütün personel sürekli olarak eğitilmelidir. Ayrıca, teknolojik gelişmeler takip edilerek, en yeni ve etkili savunma mekanizmaları uygulanmalıdır. Bu, IoT ve IIoT sistemlerinin güvenli bir şekilde çalışmasını sağlamak için kritik öneme sahiptir.

Önerilen sistem, IoT ve IIoT sistemlerinin bir arada kullanıldığı bir ağ topolojisinde yazılımsal ve donanımsal sistemlerin güvenlik açıklarının incelenmesini, gerçekleştirilen saldırıların analizini ve daha karmaşık hale getirilmesini sağlayan yöntemlerin (şifreleme, karmaşıklaştırma vb.) araştırılmasını içermektedir. Son aşamada, bir uzman sistem modeli tasarlanarak insan müdahalesi ve saldırı tespitinde en az hata ile IoT ve IIoT sistemlerinin sürekli faal halde kalması hedeflenmektedir.

Gelişen teknoloji ile akıllı şehirler, fabrikalar, enerji santralleri ve su arıtma tesisleri gibi birçok alanda kullanılan teknolojik cihazların sayısı ve çeşitliliği artmıştır. Bu cihazlar, Endüstriyel Kontrol Sistemleri (EKS) gibi kritik altyapı sistemlerinde kullanılmaktadır ve Denetimsel Kontrol ve Veri Toplama (Supervisory Control and Data Acquisition - SCADA) sistemleri ile kontrol edilmektedir. PLC cihazları da bu sistemlerin önemli bir parçasıdır ve intranet ağlarına ve internete açık hale gelmiştir. PLC cihazları, Akıllı Fabrikalar, Akıllı Şehirler ve Kritik altyapılarda, giriş/çıkışlarından aldığı veriler doğrultusunda yüklenen programa bağlı olarak çalışan ve minimum insan etkileşimi 7/24 çalışması beklenen donanım ve yazılım bileşenlerinden oluşan cihazlar olarak tanımlanmaktadır [5, 6].

Endüstri 4.0'ın etkisiyle, PLC cihazları da dijital bağlantılar ile IoT protokollerini destekleyerek Endüstriyel Nesnelerin İnternetinde önemli bir yer edinmiştir. IoT güvenliği alanı, sürekli gelişen ve yenilikçi çözümler talep eden zorluklarla karşı karşıyadır.

Makineler arası iletişim sistemleri de gelişmektedir ve Endüstri 4.0'ın ortaya çıkmasıyla birlikte Nesnelerin İnterneti (IoT) kavramı da ortaya çıkmıştır. IoT, endüstriyel sistemler ile birlikte kullanıldığında avantajlar sağlamaktadır. Ancak, kritik altyapı sistemlerinde IoT sistemlerinin kullanımı arttıkça güvenlik endişeleri de artmıştır. IIoT cihazları ve bu sistemleri kullanılan protokoller yeni güvenlik zafiyetlerini de kritik altyapı sistemlerine eklemiştir. Bu tez çalışmasında daha sonraki bölümlerde ayrıntısı verilen IIoT sistemlerinin saldırı analizleri ve açıkların tespiti için çözüm önerileri sunulmaktadır.

3. LİTERATÜR TARAMASI

Bu bölümde, IoT ve IIoT cihazlarına yönelik siber güvenlik tehditleri ile bu tehditlerin yapay zeka (AI) algoritmaları kullanılarak tespit edilmesine yönelik çalışmalar incelenmiştir.

3.1. IoT ve IIoT Güvenlik Zorlukları ve Çözümleri

Khan ve arkadaşları [7] tarafından yapılan çalışma, IoT güvenliğine yönelik kapsamlı bir inceleme sunmuş, saldırıları, zayıf noktaları, güvenlik çözümlerini ve açık sorunları tartışırken, IoT güvenliğini artırmak için potansiyel bir çözüm olarak blockchain teknolojisinin kullanımını da araştırmıştır. Benzer şekilde, Serror ve arkadaşları Endüstriyel Nesnelerin İnterneti (IIoT)'nin karşılaştığı güvenlik zorluklarını gözden geçirmiş ve güvenli iletişim protokolleri, sızma tespiti ve önleme ile erişim kontrolü gibi potansiyel çözümleri araştırmıştır [8].

Alsheikh ve arkadaşları, veri gizliliği, güvenli iletişim ve cihaz kimlik doğrulama gibi IoT'deki siber güvenlik zorluklarını gözden geçirmiş ve şifreleme, erişim kontrolü ile sızma tespiti ve önleme gibi potansiyel çözümleri tartışmıştır [9]. Tawalbeh ve arkadaşları IoT güvenliği hakkında kapsamlı bir araştırma sunarken, güvenlik zorluklarını ve eğilimleri ile potansiyel çözümleri ele almışlardır [10]. Zhao ve arkadaşları endüstriyel IoT'de kenar veri bütünlüğü doğrulaması üzerine kapsamlı bir inceleme sunarken, güvenlik tehditleri, zorluklar ve potansiyel çözümleri gözden geçirmiştir [11]. Shen ve arkadaşları IoT veri yönetimi için blockchain tabanlı çözümleri inceleyerek, izinli blockchain ve akıllı sözleşmeler gibi son gelişmeleri gözden geçirmiştir [12].

Kumar ve arkadaşları IoT için güven yönetimi mekanizmalarını kapsamlı bir şekilde ele alırken [13], Liu ve arkadaşları IoT ağları için veri birleştirme tekniklerini inceleyerek, güvenli veri birleştirme ve gizlilik koruyucu veri birleştirme gibi alanlara odaklanmıştır [14].

3.2. Yapay Zeka ve Makine Öğrenimi Kullanımı

Wu ve arkadaşları, anomali tespiti, sızma tespiti ve önleme ile kötü amaçlı yazılım tespiti gibi IoT güvenliği için makine öğrenimi kullanımını incelemiş, yapay zekanın IoT ağlarını korumadaki kritik rolünü vurgulamıştır [15]. Nguyen ve arkadaşları IoT güvenliği için federatif öğrenmenin kullanımını, anomali tespiti, saldırı tespiti ve kötü

amaçlı yazılım tespiti dahil olmak üzere tartışırken, potansiyel zorlukları ve gelecekteki araştırma yönlerini ele almışlardır [16]. Qi ve arkadaşları Endüstri 4.0'ı güvenli hale getirmek için dinamik bir saldırı tespit sistemi önerirken, ağ üzerindeki anomalileri kullanmayı önermiştir [17]. Venkatasubramanian ve arkadaşları, IoT ve IIoT cihazları için zararlı yazılım tespit mekanizmalarını federe öğrenme modeli ve blockchain algoritmaları kullanarak inceleyen kapsamlı bir inceleme sunmuş, bu alandaki teknolojilerin kesişimini ve IoT güvenliğini vurgulamıştır [18].

Sarker, Khan, Abushark ve Alsolami, IoT sistemlerinin siber tehditlere karşı güvenliğini artırmak için makine ve derin öğrenme teknolojilerinin entegrasyonunu vurgulayarak IoT güvenliğine kapsamlı bir genel bakış sunmuşlardır. IoT güvenlik açıkları ile saldırıların gelişen durumuna uyum sağlayabilen dinamik bir güvenlik çerçevesi geliştirmede yapay zekanın önemli rolünü vurgulamışlardır. Ayrıca, çeşitli makine öğrenimi ile derin öğrenme modellerini analiz ederek, IoT cihazlarını ve ağlarını güvenli hale getirmek için akıllı, veri odaklı bir yaklaşımı savunmuşlardır [19].

3.3. Temel Bileşen Analizi (Principal Component Analysis - PCA) Kullanımı

Kablosuz Sensör Ağları (Wireless Sensor Network - WSN) ve Nesnelerin İnterneti (IoT) sistemleri, kablosuz teknolojilerin ve akıllı cihazların yaygınlaşmasıyla birlikte son yıllarda önemli gelişmeler kaydetmiştir. Ancak, bu hızlı gelişim, ağ operasyonlarını ciddi şekilde aksatabilecek Hizmet Reddi (DoS) ve Dağıtılmış Hizmet Reddi (DDoS) saldırılarıyla ilgili güvenlik endişelerini de artırmıştır. Bu saldırılar, WSN ve IoT cihazlarının sınırlı hesaplama ve depolama kapasitelerini istismar ederek, güçlü ve verimli tespit mekanizmalarına olan ihtiyacı doğurmuştur.

Son araştırmalar, anormal trafik tespitini geliştirmek amacıyla Ana Bileşen Analizi (PCA) ile derin öğrenme tekniklerinin entegrasyonuna odaklanmıştır. PCA, veriyi ortogonal bileşenler setine dönüştüren ve yüksek boyutlu veriyi indirgemek için kullanılan istatistiksel bir prosedürdür. Bu indirgeme, WSN'ler ve IoT sistemleri gibi kaynak sınırlı ortamlarda yüksek boyutlu verilerin işlenmesi için kritik öneme sahiptir. Örneğin, Shakya ve arkadaşları, PCA ile Derin Konvolüsyonel Sinir Ağı (DCNN) kombinasyonunun, WSN'lerdeki DoS trafiğinde anormallikleri belirlemedeki etkinliğini göstermiştir. Önerilen model, veri boyutunu azaltmak için PCA'yı, ardından öznitelik çıkarma ve sınıflandırma için DCNN'yi kullanarak, doğruluk ve hesaplama verimliliği açısından üstün performans elde etmiştir [20].

Benzer şekilde, Dash ve arkadaşları, IoT ortamlarında DDoS saldırılarını tespit etmek için PCA'yı çeşitli makine öğrenimi sınıflandırıcılarıyla birleştirmenin etkisini incelemiştir [21]. Çalışma, NSL-KDD veri setini kullanarak, PCA'nın Rastgele Orman, K-En Yakın Komşu ve Naïve Bayes gibi sınıflandırıcıların performansını artırmadaki etkinliğini değerlendirmiştir. Sonuçlar, PCA'nın ağ trafiği verilerinin daha sağlam bir şekilde ölçeklenmesi ve kodlanmasına katkıda bulunarak tespit doğruluğunda önemli bir iyileşme sağladığını göstermiştir. Bu yaklaşım, makine öğrenimi modellerinin IoT güvenliği için tespit yeteneklerini artırmada boyut azaltma tekniklerinin önemini vurgulamaktadır.

PCA ve derin öğrenmenin entegrasyonu, yüksek boyutluluk sorununu ele almanın yanı sıra, modelin karmaşık ağ trafiği verilerinden ilgili özellikleri öğrenme yeteneğini de artırır. Örneğin, "IoT'de DDoS Saldırı Tespitini PCA Kullanarak Geliştirme" başlıklı araştırma, öznitelik seçiminin saldırı tespit sistemlerinin performansını artırmadaki kritik rolünü vurgulamaktadır. Çalışma, PCA ile makine öğrenimi sınıflandırıcılarını birleştirmenin yüksek tespit doğruluğu, kesinlik ve hatırlama sağladığını belirlemiş ve bu yaklaşımın IoT ağlarını DDoS saldırılarına karşı güvence altına almak için güvenilir bir çözüm sunduğunu göstermiştir.

PCA ve derin öğrenme tekniklerinin sinerjisi, WSN'ler ve IoT sistemlerinin güvenliğini artırmak için umut verici bir yol sunmaktadır. Veri boyutunu etkin bir şekilde azaltarak ve öznitelik çıkarımını geliştirerek, bu hibrit modeller, ağ anomali tespitinde yüksek doğruluk ve verimlilik elde edebilmekte ve bu da onları kaynak sınırlı ortamlarda dağıtım için uygun hale getirmektedir [22, 23].

3.4. Endüstriyel Kontrol Sistemleri (EKS) ve IIoT Güvenlik İncelemeleri

IoT cihazlarının, çeşitli siber-fiziksel arayüzlerle donatılması ve uzaktan yönetilebilir olması yeni saldırı vektörleri yaratmaktadır. Bu cihazlar, farklı ve muhtemelen ayrı ağlar arasında köprü kurarak siber-fiziksel etkileşimleri genişletebilmekte veya kötüye kullanılabilmektedir. IoT'deki güvenlik sertifikası eksikliği, güvenlik açığı yüzeyini ve mevcut bağlantı yollarını artırırken, geleneksel risk değerlendirme metodolojileri bu yeni ve gelişen tehdit ortamını yakalayamamaktadır [24]. IoT sistemlerinin güvenliği, mobilite, kablosuz iletişim, gömülü kullanım, bileşenlerin çeşitliliği ve ölçeklenebilirlik olmak üzere beş ayrılmaz noktada incelenmelidir. IoT cihazları, Bluetooth, 802.11, WiMAX (Worldwide Interoperability for Microwave Access), MQTT, Zigbee gibi birçok

kablosuz bağlantı protokolü aracılığıyla internete bağlanmaktadır ve çoğunlukla tek bir işlevi bulunmaktadır. Bu nedenle, güvenlik sistemleri, veri iletimindeki protokollerin tespiti ve bilgi akışının kontrolü gibi önemli noktaları dikkate almalıdır. Bağlı cihazların sayısının artması, IoT istemcilerinin cihazlarına ait verilerin gizliliğine yeterince önem vermemesine neden olmaktadır [25-28]. IoT cihazları, uzaktan algılama, iletişim ve düşük güç tüketimi gibi benzersiz özelliklere sahip sensörlerin güç ve bant genişliği gibi sınırlı kaynaklarla bağlanabildiği cihazlar olarak tanımlanmakta olup IIoT, IoT'nin bir alt kümesidir ve IoT cihazlarının endüstriyel süreçlerde uygulanmasıdır. IIoT cihazları, EKS'deki Operasyonel Teknoloji (OT) sistemlerinin bileşenleri olan PLC'ler, Uzak Terminal Birimleri (Remote Terminal Unit - RTU), sensörler ve aktüatörler gibi cihazların bağlantısını kolaylaştıran sistemler olarak tanımlanmaktadır [29].

EKS'lere yönelik ilk siber saldırı 1903 yılında İtalyan radyo öncüsü Guglielmo Marconi'nin uzun mesafeli kablosuz telgraf sunumunun Mors kodu kullanılarak hacklenmesiyle gerçekleşmiştir [30]. EKS'de bileşenlerin güncellenmesine yüksek maliyet, iş gücü ve zaman ihtiyacı nedeniyle üst düzey yöneticiler tarafından çoğunlukla izin verilmemekte ve iş çerçevesine odaklanılmaktadır [31]. IIoT destekli PLC cihazlarının kullanımı akıllı fabrikalar, akıllı şehirler ve kritik altyapılarda hayatımızın bir parçası haline geldikçe, saldırganların insan hayatını etkileyen bu sistemlere verebileceği zarar daha da kritik hale gelmektedir. Mohammed ve arkadaşları Modbus protokolünü kullanarak 3 PLC sistemine hizmet reddi saldırısı gerçekleştirmiş ve saldırı tespiti için denetimli bir XGBoost algoritması önermiştir [32]. Gueye ve diğerleri IoT/IIoT cihazlarında kullanılan Modbus protokolüne yönelik siber saldırıları tespit etmek için sinir ağı tabanlı bir yöntem önermiştir. Bu yöntem, bir cihaza saldırı olup olmadığını ve meydana gelen saldırı sınıfını modellemek için gömme işlevine sahip bir NN'nin etkili bir şekilde kullanılabileceğini göstermektedir [33]. Yılmaz ve Gönen gerçek cihazlar kullanarak bir test yatağı üzerinde S7-1200 PLC cihazlarına başlat-durdur saldırısı gerçekleştirmiş ve saldırı tespiti için imza tabanlı Snort (Saldırı Tespit Sistemi-Intrusion Detection System-IDS) sistemini kullanmışlardır. Saldırı tespit sisteminin imza tabanlı yapısı nedeniyle statik olduğu görülmüştür [34].

Kelli, Radoglou-Grammatikis, Sesis, Lagkas, Fountoukidis, Kafetzakis, Giannoulakis ve Sarigiannidis, Endüstriyel Kontrol Sistemleri (EKS), Denetleyici Kontrol ve Veri Toplama (Supervisory Control and Data Acquisition-SCADA) sistemlerinde kullanılan Dağıtılmış Ağ Protokolü 3'ün (Distributed Network Protocol 3-DNP3) güvenlik

açıklarını araştırmıştır. Yaptıkları kapsamlı çalışma, DNP3'te bulunan güvenlik açıklarını ortaya çıkararak sekiz özel siber saldırı senaryosunu uygulamışlardır. Bu tehditlere karşı koymak için, siber saldırı senaryolarını içeren deneysel bir ağ akışı veri kümesi üzerinde eğitilen Derin Sinir Ağı (Deep Neural Network-DNN) tabanlı çok modelli İzinsiz Giriş Tespit Sistemi (Intrusion Detection System-IDS) geliştirmiş ve göstermişlerdir. IDS, DNP3 ve EKS/SCADA sistemleri siber saldırılarını sınıflandırmada %99,0 doğruluk oranı sağlamıştır [35]. Ayrıca, Saldırı Savunma Ağaçlarını (ADT'ler) Ortak Güvenlik Açığı Puanlama Sistemi v3.1 (CVSS) ile birleştiren yeni bir risk değerlendirme metodolojisi sunmuşlardır. Bu yöntem ile DNP3 özellikli altyapılara yönelik siber saldırı riskini ölçebilmekte ve potansiyel tehditleri belirleyerek, risk seviyesini azaltma stratejileri için bu saldırıların seviyesini değerlendirerek kritik sistemleri güvence altına almayı amaçlamışlardır [36].

Radoglou-Grammatikis ve arkadaşları, Ortadaki Adam (MitM) eylemleri yoluyla kolaylaştırılan Yanlış Veri Enjeksiyonu (False Data Injection - FDI) siber saldırılarına odaklanarak akıllı şebekedeki düşük voltajlı dağıtım sistemlerinin siber güvenlik açıklarını araştırmıştır. Çalışmalarında, biri akıllı sayaç ile Aktif Dağıtım Yönetim Sistemi (ADMS) arasındaki iletişimi, diğeri ise akıllı invertör ile ADMS arasındaki iletişimi hedef alan iki özel FDI saldırı senaryosu gerçekleştirmişlerdir. Bu saldırılar, dağıtım transformatörlerinin çalışmasını etkileyerek potansiyel olarak yıkıcı sonuçlara yol açtığını görmüşlerdir. Bu tehditlere karşı koymak için FDI tipi siber saldırıların etkili bir şekilde tespit edildiğini ve azaltıldığını gösteren ve böylece akıllı şebeke altyapısının güvenlik duruşunu artıran Yapay Zeka (AI) tabanlı bir İzinsiz Giriş Tespit Sistemi (IDS) önermişlerdir. Önerilen IDS'nin etkinliği deneysel sonuçlarla doğrulanmış ve FDI saldırılarını yüksek bir doğrulukla tespit etme ve bunlara yanıt verme kabiliyeti göstermişlerdir [37]. Gönen ve arkadaşları, M241 PLC cihazına hatalı veri enjeksiyonu ile cihaz üzerindeki verilerin değişimini başarılı olarak gerçekleştirmiş ve çözüm önerisi olarak LiFi modelini önermişlerdir [38].

3.5. Yeni Nesil Güvenlik Sistemleri ve Yaklaşımlar

Radoglou-Grammatikis ve arkadaşları tarafından yapılan bir araştırma, özellikle yüksek voltajlı elektrik güç ve enerji sistemlerinin (EPES) durum tahminini tehlikeye atan Yanlış Veri Enjeksiyon Saldırılarına (FDIA) odaklanmış, EPES'in sayısallaştırılmasının siber güvenlik açıklarını incelenmişlerdir. Araştırmaları FDIA'ları iki farklı türe ayırmaktadır: GPS Spoofing Saldırıları ve IEEE C37.118 FDIA'lar, her ikisi de yüksek voltajlı bir

IEEE 9-Bus iletim şebekesi emülasyonu içindeki Fazör Ölçüm Birimi (PMU) ölçümlerini hedef almaktadır. Yapay Zeka (AI) tabanlı Saldırı Tespit Sisteminin (IDS) uygulanması, sistemin bu siber saldırıları etkili bir şekilde tespit etme yeteneğini göstermiştir. Çalışmaları, FDIA'ların şebekenin operasyonel bütünlüğü üzerindeki önemli etkisini ortaya koymuş ve önerilen IDS'nin bu tür tehditlere karşı korumadaki etkinliğini göstermiştir [39].

Jakovljevic ve Nedeljkovic, ICS'deki iletişim bağlantılarına yapılan siber saldırıların tespiti için yarı denetimli bir CNN algoritmasına dayanan ana bilgisayar tabanlı bir IDS önermiştir. Çalışmalarında, sistemlerini tasarlamak için ilk olarak Güvenli Su Arıtma (SWaT) test yatağı verilerini kullanmışlar ve daha sonra tasarlanan IDS sistemini kullanmak için Üretim Otomasyon Laboratuvarı'ndaki Elektro-Pnömatik Konumlandırma Sisteminden (DisEPP) gerçek verilere dayanan veri setini kullanmışlardır [40]. Abdelaty ve arkadaşları SWaT ve Su Dağıtım (WADI) verilerini kullanarak aktüatörlerdeki anomalileri tespit etmek için "A Deep Learning Solution for Anomaly Detection in Industrial Control Systems (DAICS)" çerçevesini geliştirmişlerdir [41]. Charilaou ve arkadaşları, sahada kullanılan IIoT cihazları ve PLC cihazları üzerindeki operasyonel saldırıları tespit etmek için SWaT ve WADI veri kümelerini kullanarak İkili Lojistik Regresyon algoritmasını kullanan bir Operasyonel Teknoloji Saldırı Tespiti Sistemi (SOTAD) önermiştir [42]. SWaT veri kümesini kullanan diğer çalışmalar ise Sinir Ağı denetimli anomali tespit yöntemini kullanarak Endüstriyel Kontrol Sistemlerine yönelik saldırıları tespit etmeyi amaçlamaktadır [6, 43].

Mladenov ve arkadaşları, enerji sektöründeki acil siber güvenlik sorununu ele almış ve özellikle Bulgaristan'daki Leshnitsa tesisi gibi merkezi olmayan enerji şebekesinin ayrılmaz bir parçası olan küçük hidroelektrik santrallerinin güvenlik açıklarına odaklanmışlardır. Küçük ölçekli çiftçilerin güçlendirilmesi (SPEAR) konsorsiyumu bünyesinde, uygun maliyetli ve etkili siber savunma mekanizmalarına duyulan kritik ihtiyacın farkında olarak, çeşitli enerji sektörü aktörlerine yönelik kapsamlı bir güvenlik platformu geliştirilmiştir. Bu sayede, önceden güvenlik sistemleri olmayan daha küçük kuruluşlar için siber güvenlik önlemlerinin geliştirilmesini vurgulamışlardır. Leshnitsa hidroelektrik santralinde test edilen bu platform, siber saldırıların gerçek zamanlı tespiti, sinyalizasyonu ve adli analizi için tasarlanmış çok bileşenli araç setini göstermiş ve hayati öneme sahip enerji üretim tesislerinin dayanıklılığı ile operasyonel güvenliğini güçlendirmeyi amaçlamıştır [44].

Mohy-Eddie ve arkadaşları, akıllı tarım güvenlik açıklarını azaltmak için bir ağ saldırı tespit sistemi (NIDS) gerçekleştirmiş, modellerini NF-Bot-IoT ve NF-ToN-IoT veri kümelerini kullanarak değerlendirmiş ve %99,25 doğruluk elde etmiştir [45]. Sivasakthi ve arkadaşları, IoT ağları üzerindeki hibrit saldırıları tahmin etmek ve tespit etmek için HybridRobustNet (HRN) adlı öğrenme yaklaşımını önermiştir. HRN, gelişen hibrit saldırı modellerine karşı tespit doğruluğu ve esneklik elde etmek için çeşitli derin öğrenme (Deep Learning-DL) ve makine öğrenmesi (Machine Learning-ML) algoritmalarını entegre etmektedir. Çok katmanlı eş zamanlı derin takviyeli öğrenme sistemi (HRN) 0,99977 doğruluk göstermiştir [46].

Khan ve arkadaşları, İnternet Endüstriyel Kontrol Sistemleri (IICS) içindeki siber saldırıların gerçek zamanlı tespiti için derin öğrenme tabanlı bir Saldırı Tespit Sistemi (IDS) kullanarak Endüstriyel Nesnelerin İnterneti (IIoT) ağlarının korunmasını geliştirmeyi amaçlayan sağlam bir güvenlik modeli sunmuştur. Uzun Kısa Süreli Bellek (LSTM) oto kodlayıcı tasarımını kullanan modelleri, IICS ağlarındaki istilacı faaliyetleri verimli bir şekilde tanımlamayı amaçlamaktadır. Gaz Boru Hattı veri kümesi ve UNSW-NB15 veri kümesi üzerinde yapılan deneysel doğrulama, önerilen IDS'nin etkinliğini göstermiş, sırasıyla %97,95 ve %97,62 doğruluk oranlarına ulaşarak alandaki diğer önde gelen yöntemlerden daha iyi performans göstermiştir [47]. Khan ve arkadaşları, diğer araştırmalarında Endüstriyel Nesnelerin İnterneti (IIoT) ağlarındaki siber tehditlerin tespitini ve anlaşılmasını geliştirmeyi amaçlayan yenilikçi bir derin öğrenme çerçevesi önermektedir. Çerçeve, siber tehditleri etkili bir şekilde ayırt etmek ve açıklamak için konvolüsyonel ve tekrarlayan ağları entegre eden otoenkoder tabanlı bir algılama mekanizmasından yararlanmaktadır. Bu çalışma, iki aşamalı bir kayan pencere tekniği kullanarak, sadece IIoT ağlarındaki anormallik tespit yeteneklerini geliştirmekle kalmıyor, aynı zamanda çerçevenin tahminleri için açıklamalar sağlama yeteneğini vurgulayarak, tespit edilen tehditlerin altında yatan nedenlerin daha derinlemesine anlaşılmasını kolaylaştırıyor. Ampirik sonuçlar, çerçevenin çeşitli değerlendirme ölçütlerinde kötü niyetli olayları tanımlamadaki sağlamlığının altını çizmekte, çağdaş yöntemlerden önemli ölçüde daha iyi performans göstermekte ve gerçek dünya IIoT uygulamalarında pratik bir çözüm olarak potansiyelini güçlendirmektedir [48].

Chander N. ve Kumar M., endüstriyel prosedürlerin güvenliğini sağlamak için topluluk oylama tabanlı anormallik tespiti (EPOA-EVAD) yaklaşımı ile geliştirilmiş bir pelikan optimizasyon modeli geliştirmiştir. Çalışmalarında, EPOA-EVAD tekniğini kullanarak

IIoT'de anomali tespit yeteneklerini geliştirmeyi amaçlamışlardır. Önerdikleri yöntem, Sentetik Azınlık Aşırı Örnekleme Tekniği (SMOTE) ve topluluk oylama sınıflandırıcısı gibi teknikleri birleştiren bir optimizasyon modeli sağlamıştır [49]. Alkhudaydi, Krichen ve Alghamdi, bu tür saldırıları etkili bir şekilde tespit etmek için makine öğrenimi (ML) ve derin öğrenme (DL) algoritmalarından yararlanarak Nesnelerin İnterneti (IoT) üzerindeki siber güvenlik saldırılarının artan zorluğunu ele almaktadır. Çalışmaları, analiz için Bot-IoT veri kümesini kullanarak hem tek sınıflandırıcılar hem de topluluk sınıflandırıcıları ve dört derin öğrenme mimarisi dahil olmak üzere on farklı ML modelinin kapsamlı bir değerlendirmesini içermektedir. Özellikle, veri dengesizliğini gidermek için SMOTE'nin uygulanması, CatBoost ve XGBoost sınıflandırıcılarının sırasıyla %98,19 ve %98,50'lik doğruluk oranlarına ulaşmasıyla model performansını artırmışlardır. Bu araştırma, IoT ağlarındaki siber güvenlik tehditlerinin tespitini iyileştirmek için SMOTE gibi veri dengeleme stratejileriyle birlikte ML ve DL tekniklerinin potansiyelini göstermektedir [50].

3.6. Blockchain ve RPL Tabanlı Çözümler

IIoT güvenliği için potansiyel bir çözüm olarak blockchain teknolojisinin kullanımını araştıran Latif ve arkadaşları, güvenli veri paylaşımı, erişim kontrolü ve cihaz kimlik yönetimi gibi konuları ele almıştır [51]. Choo ve arkadaşları IIoT'de güvenlik ve gizlilik için blockchain teknolojisinin kullanımını araştırırken, dağıtılmış uzlaşma, değişmezlik ve merkezi olmayan yönetişim gibi blockchain tabanlı çözümlerin potansiyel zorluklarını ve fırsatlarını tartışmışlardır [52]. Yılmaz ve diğerleri ise 2021 yılındaki çalışmalarında IoT ağlarının güvenliği için transfer öğrenme kullanarak saldırı tespit algoritmalarının geliştirilmesini incelemiştir. RPL tabanlı ağlarda, transfer öğrenme geleneksel yöntemlere göre daha hızlı ve etkili sonuçlar vermiş, yeni cihazlar ve saldırı türleri için güvenlik çözümleri sunmuştur [53].

Aydogan ve arkadaşları RPL (Routing Protocol for Low-Power and Lossy Network) protokolü tabanlı IIoT sistemlerine çeşitli saldırıları simüle etmiş ve saldırı tespiti için genetik programlama tabanlı bir IDS çözümü önermiştir [54]. Doğan ve arkadaşları, RPL hedef fonksiyonlarının güvenlik açısından analizini yapmış ve farklı saldırgan türlerinin farklı etkilere yol açabileceğini göstermişlerdir [55]. Singh ve arkadaşlarının araştırmasında sel (hello flood) saldırılarını tespit etmek için çok katmanlı algılayıcı sinir ağı ve bulanık mantığı birleştiren gelişmiş bir hibrit saldırı tespit sistemi önermiştir [25]. Çakır ve arkadaşları, IoT ağlarında kullanılan RPL protokolüne yönelik sel (hello flood)

saldırılarını tespit etmek için Gated Recurrent Unit modeline dayalı bir derin öğrenme sistemi önermişlerdir [26]. Deveci ve arkadaşları, RPL'ye özgü çeşitli saldırı türlerini tespit etmek maksadıyla pareto tabanlı çok amaçlı bir yöntemin önermişlerdir. Gerçekleştirdikleri simülasyon ve değerlendirmeler, önerilen yaklaşımın hedefli saldırıları tespit etmede %90 üzerinde başarılı olduğunu göstermiştir [56]. Loulianou ve arkadaşlarının çalışması, DDoS saldırılarını, özellikle de sel türündeki saldırıları azaltmak için hibrit hafif imza tabanlı bir IDS sistemini önermiştir [27].

Yavuz ve arkadaşları, IoT ağlarında saldırı tespiti için derin öğrenme tabanlı bir makine öğrenimi yöntemini araştırmış, UNSW-NB15 ve KDDCUP99 veri setleriyle karşılaştırmalı bir simülasyon yapmışlardır [57]. Jan ve arkadaşları, IoT ağına fazla veri enjekte etmeye çalışan bir saldırganı tespit etmek için hafif denetimli makine öğrenimi tabanlı bir Destek Vektör Makinesi (SVM) önermiştir [58].

3.7. Federatif Öğrenme ve Diğer İnovatif Modeller

Khan ve arkadaşları tarafından önerilen çalışma, IoT ile güçlendirilmiş Endüstriyel Kontrol Sistemlerinin (EKS) güvenliğini artırmayı amaçlayan Federated-Simple Recurrent Units (Federated-SRU) adlı yeni bir Saldırı Tespit Sistemi (IDS) modelini geliştirmişlerdir. Bu model, hesaplama maliyetlerini azaltmak ve tekrarlayan ağlarda yaygın olarak karşılaşılan gradyan kaybolması sorununu hafifletmek için Basit Tekrarlayan Birimlerin (SRU) geliştirilmiş mimarisinden yararlanmaktadır. Federated-SRU IDS modeli, federe bir öğrenme yaklaşımı kullanarak, gizliliği koruyan bir şekilde birden fazla Endüstriyel Kontrol Sistemi (EKS) ağında veri toplamayı kolaylaştırmakta ve kapsamlı bir IDS modelinin işbirliğine dayalı olarak geliştirilmesine olanak tanımaktadır. Federated-SRU IDS modelinin etkinliği, gerçek gaz boru hattı tabanlı EKS ağ verileri üzerinde yapılan kapsamlı deneylerle doğrulanmış, gizlilik ve güvenlikten taviz vermeden izinsiz girişleri gerçek zamanlı olarak doğru bir şekilde tespit etme kabiliyeti göstermiştir. Deneysel sonuçlar, Federated-SRU modelinin mevcut son teknoloji yaklaşımları aştığını ve IoT tabanlı EKS ağlarını siber tehditlere karşı korumak için umut verici bir çözüm olduğunu göstermektedir [59].

Louati ve arkadaşları, büyük veri ağlarında daha etkili saldırı tespiti için Merkezi Olmayan Çok Ajanlı Takviye Öğrenme (MARL) tabanlı bir IDS önermektedir. Önerdikleri sistemi NSL-KDD kıyaslama veri kümesi üzerinde test etmişler ve %97,44'lük bir doğruluk oranı elde etmişlerdir [60]. Nanjappan ve arkadaşları ise, IoT

cihazlarını yetkisiz erişime ve siber saldırılara karşı güçlendirmek için Uzun Kısa Süreli Bellek (LSTM), Geçitli Güvenli Ağ (SecNet) ve Çapraz Kaos Oyun Optimizasyonu (CCGO) gibi derin öğrenme tekniklerinin birleşiminden oluşan DeepLG SecNet yaklaşımını önermişlerdir. Önerilen yöntem, BoT-IoT veri kümesinden ve NSL-KDD veri kümesinden toplanan çeşitli örnekler üzerinde %98,92 doğruluk elde etmiştir [61].

3.8. 5G Teknolojileri ve IoT Güvenliği

5G teknolojileri bağlamında Amponis ve arkadaşları, 5G çekirdek ağının güvenlik açıklarını araştırmış, özellikle yetkisiz Hizmet Reddi (DoS) saldırıları bağlamında Paket Yönlendirme Kontrol Protokolüne (PFCP) odaklanmışlardır. Çalışmalarında, saldırı tespitini zorlaştırmak için abonelerin Yeni Nesil Radyo Erişim Ağına (NG-RAN) bağlantısını etkilemeden saldırıların uygulanabilirliğini göstermiş ve yerleşik 5G tünellerini bozmayı amaçlayan bir dizi saldırıyı gerçekleştirmişlerdir. Yazarlar, bu saldırıların simüle edilmiş bir ortamda geliştirilmesi ve uygulanması yoluyla 5G çekirdeğindeki, özellikle PFCP protokolünün oturum kontrol paketlerini incelenmesiyle ilgili önemli güvenlik kusurlarını vurgulamışlardır. Bu çalışma 5G ağ istikrarı ve güvenliğine yönelik potansiyel tehditleri ortaya koymakla birlikte, güvenlik açıklarını etkili bir şekilde azaltmak için 5G mimarisi içinde gelişmiş koruyucu önlemlere ve protokollere duyulan ihtiyacı göstermiştir [62].

Khan ve arkadaşları IoT güvenliği ve gizliliğindeki son gelişmeleri inceleyerek, güvenli iletişim protokolleri, veri şifrelemesi ve kimlik doğrulama gibi konuları kapsamlı bir şekilde ele almışlardır [63]. Corallo ve arkadaşları IIoT'da siber güvenlik farkındalığını sistematik bir şekilde incelerken, veri gizliliği, erişim kontrolü ve güvenli iletişim gibi güvenlik zorluklarını ele almışlardır [64].

3.9. 6G Teknolojileri ve IoT Güvenliği

Mahmood ve arkadaşları 6G döneminde IoT güvenliğini güçlendirmek için yapay zeka/makine öğrenimi algoritmalarının kullanımını incelemiş, zorlukları ve gelecekteki araştırma yönlerini tartışmışlardır [65]. Rahman ve Hossain geliştirdikleri 6G IT-OT test yatağı üzerinde çeşitli saldırılar gerçekleştirmiş ve derin öğrenme yöntemleri kullanarak saldırıları tespit etmeye çalışmışlardır. Yaptıkları çalışmalar sonucunda BT-OT yakınsamasının 6G için getireceği yeniliklerin ve gerçekleştirilen saldırıların derin öğrenme yöntemleri ile tespit edilebileceğini belirtmişlerdir [66]. Kim ve Lee akıllı fabrikalardaki IIoT cihazlarına yapılan kötü amaçlı yazılım saldırılarına karşı koymak

için CIC-IDS-2017 veri kümesi üzerinde çeşitli derin öğrenme modelleri kullanarak bir siber saldırı tespit sistemi önermişlerdir [67]. Zhang ve diğerleri, IIoT cihazlarına yönelik siber saldırıları tespit etmek için 2014 yılında Mississippi Eyalet Üniversitesi Altyapı Koruma Merkezi tarafından hazırlanan bir veri kümesini kullanmış ve bu amaçla bir Grafik Saldırı Tespiti (GID) çerçevesi önermiştir [68].

İncelenen çalışmalar, IoT ve IIoT cihazlarının güvenliği ile mevcut zorlukları ve potansiyel çözüm yollarını ortaya koymaktadır. Bu kapsamda makine öğrenimi ve derin öğrenme yöntemlerinin çeşitli saldırı türlerini tespit etmede önemli bir rol oynayabileceği ile IoT ve IIoT güvenliğinin gelecekte daha da geliştirilmesi gerektiği vurgulanmaktadır.

Yapılan araştırmalar sonucunda literatürdeki çalışmaların özeti ile mantıksal bölümlendirilmesi Tablo 3.1.'de sunulmuştur.

Çalışma Alanı	***Yazarlar***	***Yıl***	***Güvenlik Yaklaşımı / Çözüm***
IoT ve IIoT Güvenlik Zorlukları ve Çözümleri	*Khan ve ark.*	*2018*	*Blockchain teknolojisi kullanımı [7]*
	Serror ve ark.	*2020*	*Güvenli iletişim protokolleri, sızma tespiti [8]*
	Alsheikh ve ark.	*2021*	*Şifreleme, erişim kontrolü, sızma tespiti [9]*
	Tawalbeh ve ark.	*2020*	*Güvenlik zorlukları ve eğilimleri [10]*
	Zhao ve ark.	*2005*	*Kenar veri bütünlüğü doğrulaması [11]*
	Shen ve ark.	*2022*	*Blockchain tabanlı çözümler [12]*
	Kumar ve ark.	*2022*	*Güven yönetimi mekanizmaları [13]*
	Liu ve ark.	*2022*	*Veri birleştirme teknikleri [14]*
Yapay Zeka ve Makine Öğrenimi Kullanımı	*Wu ve ark.*	*2020*	*Makine öğrenimi ile anomali tespiti [15]*
	Nguyen ve ark.	*2021*	*Federatif öğrenme ile anomali tespiti [16]*
	Qi ve ark.	*2021*	*Dinamik saldırı tespit sistemi [17]*

	Venkatasubramaniam ve ark.	*2023*	*Federe öğrenme modeli ve blockchain algoritmaları [18]*
	Sarker ve ark.	*2023*	*Makine ve derin öğrenme entegrasyonu [19]*
PCA Kullanımı	*Shakya ve ark.*	*2024*	*PCA ile Derin Konvolüsyonel Sinir Ağı [20]*
	Dash ve ark.	*2024*	*PCA ve makine öğrenimi sınıflandırıcıları [21]*
	Mengara ve ark.	*2024*	*PCA ve IoT güvenliği [22]*
	Stellos ve ark.	*2024*	*PCA ve IoT güvenliği [23]*
Endüstriyel Kontrol Sistemleri (EKS) ve IIoT Güvenlik İncelemeleri	*Kumari ve ark.*	*2021*	*IoT güvenlik sertifikaları [24]*
	Singh ve ark.	*2017*	*Veri gizliliği [25]*
	Çakır ve ark.	*2020*	*Veri gizliliği [26]*
	Ioulianou ve ark.	*2018*	*Veri gizliliği [27]*
	Raza ve ark.	*2013*	*Veri gizliliği [28]*
	Xu ve ark.	*2018*	*IIoT tanımı [29]*
	Hemsley ve ark.	*2018*	*EKS saldırıları [30]*
	Ibarra ve ark.	*2019*	*EKS zafiyetleri [31]*
	Mohammed ve ark.	*2023*	*XGBoost algoritması [32]*
	Gueye ve ark.	*2023*	*Sinir ağı tabanlı yöntem [33]*
	Yılmaz ve Gönen	*2018*	*Snort IDS sistemi [34]*
	Kelli ve ark.	*2022*	*DNN tabanlı çok modelli IDS [35]*

	Kelli ve ark.	*2022*	*DNN tabanlı çok modelli IDS [36]*
	Radoglou-Grammatikis ve ark.	*2022*	*AI tabanlı IDS [37]*
	Gönen ve ark.	*2020*	*Hatalı veri enjeksiyonu [38]*
Yeni Nesil Güvenlik Sistemleri ve Yaklaşımlar	*Radoglou-Grammatikis ve ark.*	*2023*	*Hatalı veri enjeksiyonu [39]*
	Jakovljevic ve Nedeljkovic	*2022*	*Yarı denetimli CNN algoritması [40]*
	Abdelaty ve ark.	*2021*	*EKS için derin öğrenme yöntemleri [41]*
	Charilaou ve ark.	*2022*	*İkili Lojistik Regresyon algoritması [42]*
	E.A.Boateng	*2021*	*Sinir ağı tabanlı yöntem [6]*
	E.A.Boateng ve ark.	*2022*	*Sinir ağı tabanlı yöntem [43]*
	Mladenov ve ark.	*2020*	*Güvenlik platformu geliştirilmesi [44]*
	Mohy-Eddie ve ark.	*2024*	*NIDS kullanımı [45]*
	Sivasakthi ve ark.	*2024*	*HybridRobustNet (HRN) [46]*
	Khan ve ark.	*2022*	*LSTM oto kodlayıcı tasarımı [47]*
	Khan ve ark.	*2021*	*Otoenkoder tabanlı algılama [48]*
	Chander and Kumar	*2024*	*Pelikan optimizasyon modeli [49]*
	Alkhudaydi ve ark.	*2023*	*CatBoost ve XGBoost ML modelleri [50]*
Blockchain ve RPL Tabanlı Çözümler	*Latif ve ark.*	*2021*	*Blockchain kullanımı [51]*
	Choo ve ark.	*2020*	*Blockchain tabanlı çözümler [52]*

	Yılmaz ve ark.	*2021*	*Transfer öğrenme kullanımı [53]*
	Aydogan ve ark.	*2019*	*Genetik programlama tabanlı IDS [54]*
	Doğan ve ark.	*2022*	*RPL hedef fonksiyonları [55]*
	Singh ve ark.	*2017*	*Hibrit saldırı tespit sistemi [25]*
	Çakır ve ark.	*2020*	*Gated Recurrent Unit modeli [26]*
	Deveci ve ark.	*2023*	*Pareto tabanlı çok amaçlı yöntem [56]*
	Ioulianou ve ark.	*2018*	*Hafif imza tabanlı yöntem [27]*
	Yavuz ve ark.	*2018*	*Derin öğrenme tabanlı makine öğrenimi [57]*
	Jan ve ark.	*2019*	*Hafif denetimli makine öğrenimi [58]*
Federatif Öğrenme ve Diğer İnovatif Modeller	*Khan ve ark.*	*2022*	*Federe basit tekrarlayan birim modeli [59]*
	Louati ve ark.	*2024*	*Merkezi olmayan çok ajanlı takviye öğrenme modeli [60]*
	Nanjappan ve ark.	*2024*	*DeepLG SecNet modeli [61]*
5G Teknolojileri ve IoT Güvenliği	*Amponis ve ark.*	*2022*	*PFCP odaklı güvenlik [62]*
	Khan ve ark.	*2019*	*Güvenli iletişim protokolleri [63]*
	Corallo ve ark.	*2022*	*Siber güvenlik farkındalığı [64]*
6G Teknolojileri ve IoT Güvenliği	*Mahmood ve ark.*	*2022*	*6G dönemi zorlukları [65]*
	Rahman ve Hossain	*2022*	*Derin öğrenme ile saldırı tespiti [66]*
	Kim ve Lee	*2022*	*CIC-IDS-2017 veri kümesi [67]*

	Zhang ve ark.	*2022*	*Grafik Saldırı Tespiti (GID) [68]*

Tablo 3.1. Literatürdeki Çalışmaların Mantıksal Bölümlendirilmesi

Yapılan literatür incelemesinde, IoT ve IIoT cihazlarına yönelik siber güvenlik tehditleri ile bu tehditlerin yapay zeka (AI) algoritmaları kullanılarak tespit edilmesine yönelik çalışmaların genel bir değerlendirmesi yapılmış, ayrıca IoT ve IIoT sistemlerinin güvenliği için geliştirilen çeşitli yaklaşımlar ile bu yaklaşımların etkileri ele alınmıştır. Çalışmalar, güvenlik tehditlerinin tanımlanması, savunma mekanizmalarının geliştirilmesi ve yapay zeka algoritmalarının kullanılması gibi çeşitli konuları kapsamaktadır.

IoT ve IIoT cihazlarına yönelik güvenlik tehditleri arasında hizmet reddi (DoS/DDoS) saldırıları, kötü amaçlı yazılım ve fidye yazılımı saldırıları, orta adam (MitM) saldırıları, sahte kimlik saldırıları, fiziksel saldırılar ve sosyal mühendislik saldırıları gibi birçok farklı saldırı çeşidi bulunmaktadır. Bu tehditler, sistemlerin çalışmasını kesintiye uğratmak, veri çalmak veya manipüle etmek, sistem kaynaklarını tüketmek ve kullanıcıların sistemlere erişimini engellemek amacıyla gerçekleştirilmiştir.

Bu tehditlere karşı geliştirilen savunma mekanizmaları arasında ağ filtreleme, hız sınırlama, yedeklilik, son kullanıcı güvenlik yazılımları, şifreleme, güvenli kimlik doğrulama, erişim kontrolü, anomali tespiti ve fiziksel güvenlik önlemleri bulunmaktadır. Bu mekanizmalar, sistemlerin güvenliğini artırmak ve olası saldırılara karşı koruma sağlamak için kullanılmaktadır.

Yapay zeka ve makine öğrenimi algoritmaları, IoT ve IIoT sistemlerinin güvenliğini sağlamak amacıyla yaygın olarak kullanılmaktadır. Kullanılan algoritmalar ile anomali tespiti, sızma tespiti ve önleme, kötü amaçlı yazılım tespiti gibi çeşitli güvenlik tedbirleri alınmaktadır. Yapay zeka, büyük veri setlerini analiz ederek normal ve anormal davranışları tanımlamakta ve potansiyel tehditleri erken aşamada tespit etmektedir. Bu sayede, saldırılara karşı daha hızlı ve etkili bir savunma sağlanmaktadır.

İncelenen çalışmalar arasında, IoT ve IIoT güvenliğine yönelik çeşitli yaklaşımlar ve bu yaklaşımların avantajları ve dezavantajları ele alınmaktadır. Özellikle, yapay zeka ve makine öğrenimi algoritmalarının kullanımı, bu alanda önemli katkılar sağlamaktadır. Ancak, bu teknolojilerin uygulanmasında karşılaşılan zorluklar ve sınırlamalar da göz

önünde bulundurulmalıdır. Yapay zeka tabanlı sistemlerin geliştirilmesi ve uygulanması, yüksek doğruluk ve düşük yanlış pozitif oranları elde etmek için sürekli olarak iyileştirilmelidir.

Bu nedenle çalışmada, literatürde bahsedilen çalışmalardan farklı olarak yapay zeka tabanlı uzman sistemlerin karar ağaçlarıyla oluşturulan kuralların IoT ve IIoT sistemlerinde saldırı tespiti ve önleme süreçlerine entegrasyonunun sağlandığı hibrit bir yapıya odaklanılmıştır. Literatürde mevcut olan çalışmalar genellikle belirli bir saldırı türüne odaklanırken, bu çalışmada farklı saldırı senaryoları için genel bir yöntem önerilmiştir. Ayrıca, Snort gibi yaygın olarak kullanılan kural tabanlı IPS/IDS sistemleriyle entegrasyon, saldırıların hızlı bir şekilde tespit edilmesini ve müdahale edilmesini sağlamaktadır. Bu yaklaşım, sistemlerin güvenilirliğini artırmak ve gelecekteki güvenlik tehditlerine karşı daha esnek ve genişletilebilir çözümler sunmak amacıyla tasarlanmıştır.

4. DENEYSEL SİSTEM GELİŞTİRİLMESİ VE SALDIRI ANALİZ ÇALIŞMALARI

Endüstri 4.0 ve bunun bileşenleri olan özellikle IoT, IIoT, artırılmış gerçeklik gibi bilgi teknolojilerinin en önemli bileşenlerinden biri de siber güvenlik boyutudur. Büyük kurum/kuruluşlar başta olmak üzere tüm sektörel yapıdaki kuruluşların insanların hizmetine sunacakları sistemlerle etkinlik, verimlilik, sürat gibi kar marjı yüksek ve talebi artıracak bileşenlere öncelik verilmesi doğaldır. Bilgi çağına yön veren önemli iki kavram olan IoT ve IIoT sistemlerinin güvenliğidir.

Endüstriyel kontrol sistemleri ve IIoT cihazlarına yönelik siber saldırıların tespit edilmesinde etkili bir mekanizma gerekmektedir. Bu mekanizma için yapay zeka tabanlı uzman sistem kullanılması tezin kapsamını oluşturmaktadır. Bu şekilde saldırıların tespiti ve etkisiz hale getirilmesi endüstriyel kontrol sistemleri ve IIoT cihazlarına yönelik siber saldırılara karşı koruma sağlayacaktır.

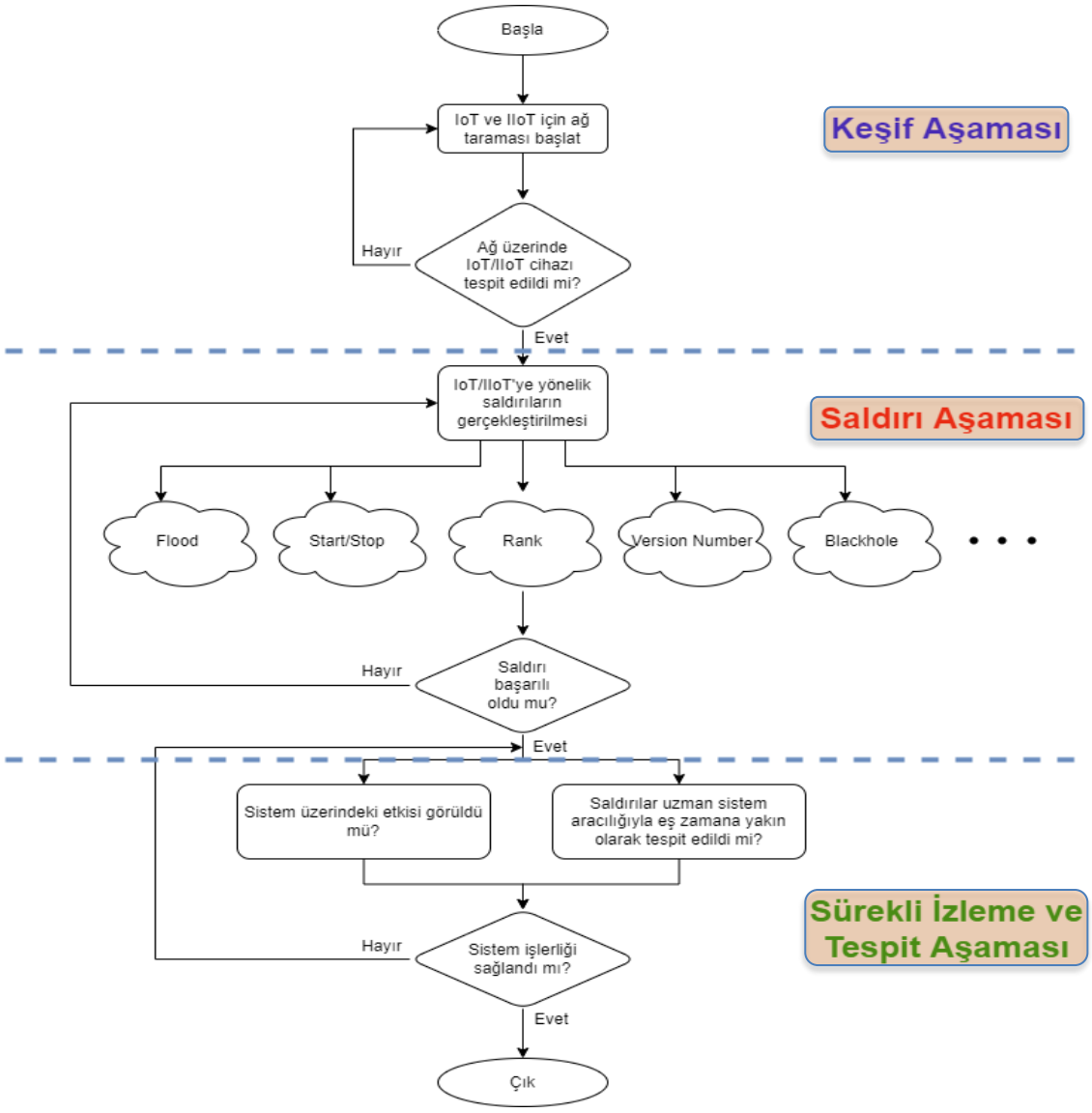
Önerilen uzman sistem modeli, endüstriyel kontrol sistemleri ve IoT/IIoT cihazlarına yönelik siber saldırıların tespiti için etkili bir mekanizmanın oluşturulması için önemli bir yaklaşım olacağı önerilmektedir.

IoT ve IIoT sistemlerinin bir arada olduğu ağ topolojilerindeki yazılımsal ve donanımsal sistemlerin güvenlik zafiyetlerinin incelenmesi, bu zafiyetlere yönelik saldırıların analiz edilmesi ve bir uzman sistem modeli oluşturulması tezde amaçlanmaktadır. Bu çalışmanın aşamaları Şekil 4.1.'de gösterilmektedir. Her aşama, gelecekte ortaya çıkabilecek yeni IoT ve IIoT sistemlerine yönelik tehditler için de uygulanabilir olması düşünülmüştür.

Sistemin ilk aşamasında, IoT ve IIoT sistemlerinin bir arada olduğu ağ topolojilerinde sistemlerin güvenlik zafiyetleri incelenmiştir. Bu zafiyetlerin üzerinde gerçekleştirilen saldırılar incelenerek, IIoT sistemlerine yönelik saldırıların etkisi tartışılmıştır. İkinci aşamada, bu saldırıların tespiti için gerekli olan nitelikler *(feature)* belirlenmiş ve örnek bir uzman sistem modeli oluşturulmuştur. Üçüncü aşamada ise, IoT ve IIoT sistemleri için potansiyel saldırılardan en az hasarla kurtularak sistemin sürekli faal halde tutulabilmesi için bir uzman sistem modeli önerilmiştir.

Sistemlere saldırı bağlamında, IIoT sistemlerine yönelik ortadaki adam, hizmet reddi ve başlat-durdur saldırıları gerçekleştirilerek, sistem üzerindeki etkileri incelenmiştir.

Deneysel olarak, IoT cihazlarında yaygın olarak kullanılan MQTT protokolüne ortadaki adam, kaba kuvvet *(bruteforce)*, hizmet reddi ve hatalı veri girişi saldırıları gerçekleştirilerek paket toplama işlemleri çalışmaları yapılmıştır. MQTT Broker üzerine IIoT cihazlarının veri gönderip alması açık kaynak kodlu Node-RED uygulaması kullanılarak sağlanmıştır. Bu deneysel çalışmaların sonucunda, uzman sistem modeli tasarımı için gerekli olabilecek özellikler belirlenmiş ve IIoT sistemlerine yönelik saldırıların tespiti için bir uzman sistem modeli tasarlanmıştır.



Şekil 4.1. IoT ve IIoT Sistemler için Güvenlik Analizi Aşamaları

Geliştirilen örnek sistemin tasarım ve uygulanma kriterleri, IoT ve IIoT teknolojilerinin güvenlik açıklarını gerçekçi ve kapsamlı bir şekilde analiz edebilmek amacıyla belirlenmiştir. İlk olarak, sistemin donanım ve yazılım bileşenleri, endüstriyel kontrol sistemlerinde yaygın olarak kullanılan teknolojileri içerecek biçimde seçilmiştir. Bu da

araştırmanın bulgularının gerçek dünya uygulamalarıyla uyumlu olmasını sağlamıştır. Özellikle, sensörler, ağ protokolleri ve veri işleme birimleri, güncel IIoT altyapılarında sıklıkla karşılaşılan bileşenleri temsil edecek şekilde seçilmiştir.

Bir diğer yaklaşım ise, sistemin tasarımında, farklı saldırı türlerinin etkilerini değerlendirebilmek için çok katmanlı bir güvenlik mimarisi oluşturulmuştur. Bu mimari, dağıtık hizmet reddi (DDoS), ortadaki adam (MitM) ve kaba kuvvet (*bruteforce*) gibi çeşitli saldırı senaryolarını benzetimi (*simulation*) yapılabilecek biçimde yapılandırılmıştır. Bu yaklaşım ile sistemin farklı güvenlik tehditlerine karşı nasıl tepki verdiğini ve savunma mekanizmalarının etkinliğinin ölçmesi mümkün olacaktır.

Sistemin yazılım bileşenleri ise Yapay Zeka alanında, Temel Bileşen Analizi (PCA) ve Derin Öğrenme Modelleri (Deep Learning) gibi gelişmiş veri analizi tekniklerini kullanımından da yararlanılması düşünülerek tasarlanmıştır. Anomali tespiti ve saldırı algılama gibi kritik güvenlik işlevlerinin etkinliğini arttırması konularında bu tekniklerden karşılaştırma sağlamak amacıyla değerlendirilmiştir. Makine öğrenimi ve yapay zeka algoritmalarının entegrasyonu ile sistemin adaptif ve proaktif bir güvenlik yaklaşımı sergilemesi amacı ile ayrıca irdelenmektedir.

Deneysel çalışmaların bir diğer önemli sayılan kriteri, gerçek dünya koşullarını yansıtan test ortamlarının deneysel ölçekte oluşturulmasıdır. Bu bağlamda, IoT ve IIoT cihazlarının gerçek zamanlı veri toplama, analiz ve karar verme süreçleri benzetimlerine olanak sağlanmıştır. Bu biçimde gerçek çalışma ortamındaki performans ve zaafların anlaşılması ve giderilmesine yönelik olmaktadır.

Son olarak, sistemin genel tasarım ve uygulama kriterleri, genişletilebilirlik ve ölçeklenebilirlik prensiplerine dayanmıştır. Bu, gelecekteki çalışmalar için yeni teknolojiler ve saldırı türleri ile entegrasyonun kolayca gerçekleştirilebilmesini sağlamıştır. Böylece, araştırmanın bulguları, sadece mevcut güvenlik tehditlerine karşı değil, aynı zamanda gelecekte ortaya çıkabilecek potansiyel yeni tehditlere karşı da geçerli ve uygulamaya yönelik olması amaçlanmaktadır. Özetle verilen tüm bu tanımlar, çalışmanın güvenilir ve geçerli sonuçlar üretebilmesi ile IoT ve IIoT sistemlerinin güvenliğini artırmaya yönelik stratejiler geliştirilmesini mümkün hale getirmiştir.

4.1. Örnek Sistem Tasarımı

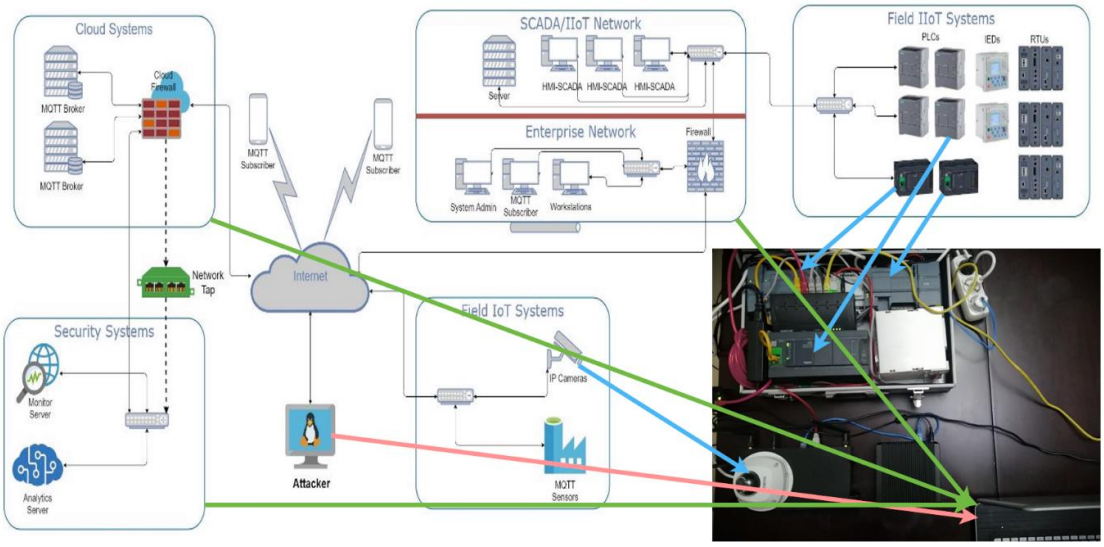
Tez Çalışmasında Endüstriyel Kontrol Sistemlerinin (EKS) önemli bir bileşeni olan PLC’lere yönelik saldırı ve tespit aşamalarını gerçekleştirmek amacıyla bir örnek

donanım ve yazılım altyapısı tasarlanıp gerçekleştirilmiştir. Bu tasarım ile, sahadaki uzaktan kontrol edilen cihazları ve sensörleri, insan-makine etkileşimi arayüzlerini ve bulut üzerinden yönetim sağlayan IIoT cihazlarını içeren üç ana bölümden oluşmaktadır. Her bölüm, farklı güvenlik tehditlerine karşı özel olarak tasarlanmış ve çeşitli siber saldırı senaryoları ile test edilmiştir. Yapılan analizler, sistemin genişletilebilirlik ve ölçeklenebilirlik ilkeleri doğrultusunda gelecekteki güvenlik tehditlerine karşı da etkili çözümler sunmasını hedeflemiştir. Bu sayede, EKS ve IIoT sistemlerinde güvenlik açıklarının tespiti ve önlenmesine yönelik stratejiler yönelik çalışmalar gerçekleştirilmiştir.

Şekil 4.2.'de, tasarlanan ve gerçekleştirilen altyapının ilke şeması verilmiştir. Sınama altyapısı, üç temel alt bölümden oluşmaktadır. İlk bölüm, EKS'nin kontrol cihazları ve sensörleri olan uzaktan kontrol edilen saha donanımlarını içermektedir. Bu donanımlar RTU, PLC ve IIoT donanımları bulundurmaktadır. İkinci bölüm, saha donanımlarının yönetimi ve işleyişinden sorumlu olan insan makine etkileşimi arayüzlerini (Human Machine Interface - HMI) içermektedir. Bu iki bölüm sıradan kapalı bir intranet aracılığıyla birbirleriyle bağlanmıştır. Bunun yanı sıra, cihazların ekonomik değerleri, erken arıza tespiti ve müdahale, verimlilik gibi nedenlerle farklı IIoT cihazları da bu ağa test için bağlanabilmektedir. Ayrıca söz konusu bu cihazlar bulut üzerinde bulunan yönetim birimlerine internet üzerinden bağlanabilmektedirler. Farklı güvenlik önlemlerine sahip ağlara bağlanmaları nedeniyle, her bir birim için kendine özgü güvenlik zafiyetleri ve tehditlere de sahip olmaktadır.

MQTT Broker bulut mimarisi, sanallaştırma platformu üzerinde Ubuntu 22.04 LTS işletim sistemi ile gerçeklenmiştir. Yapay Zeka ve Analiz yazılımları için ise Quad Core Intel Core i7-7700HQ işlemci, 32 GB RAM ve 4GB NVIDIA GeForce GTX 1050 ekran kartına sahip bilgisayarda Windows 2011 işletim sistemi ile kullanılmıştır.

Analiz ve incelemelerde paketlerin aynalanması *(mirroring)* gerçekleştirilmiştir. Bu biçimde endüstriyel kontrol sistemlerinin en önemli güvenlik bileşeni olan sürekliliğe zarar verilmemesi sağlanmıştır.



Şekil 4.2. Örnek Sistem Tasarımı

Şekil 4.3.'te gösterilen analiz, saldırı ve tespit aşamaları kullanılarak bir saldırı tespit modeli oluşturulmuştur. Bu model yapay zeka tabanlı uzman sistem analiz yöntemi kullanılarak değerlendirilmiştir. Model oluşturma sürecinde ilk aşamada, ağ üzerinde bir PLC cihazının olup olmadığını tespit etmek için öncelikle ağ taraması yapılmıştır. Ağ taraması için açık kaynaklı *"nmap"* aracı kullanılmıştır. Bu sayede, ağ üzerinde bulunan PLC cihazları marka, model ve sürüm numaraları ile birlikte tespit edilmiştir. Bu bilgiler müteakip aşamada açıklıkların ve söz konusu açıklıklara yönelik saldırı vektörlerinin bulunmasında önemli rol oynamaktadır.

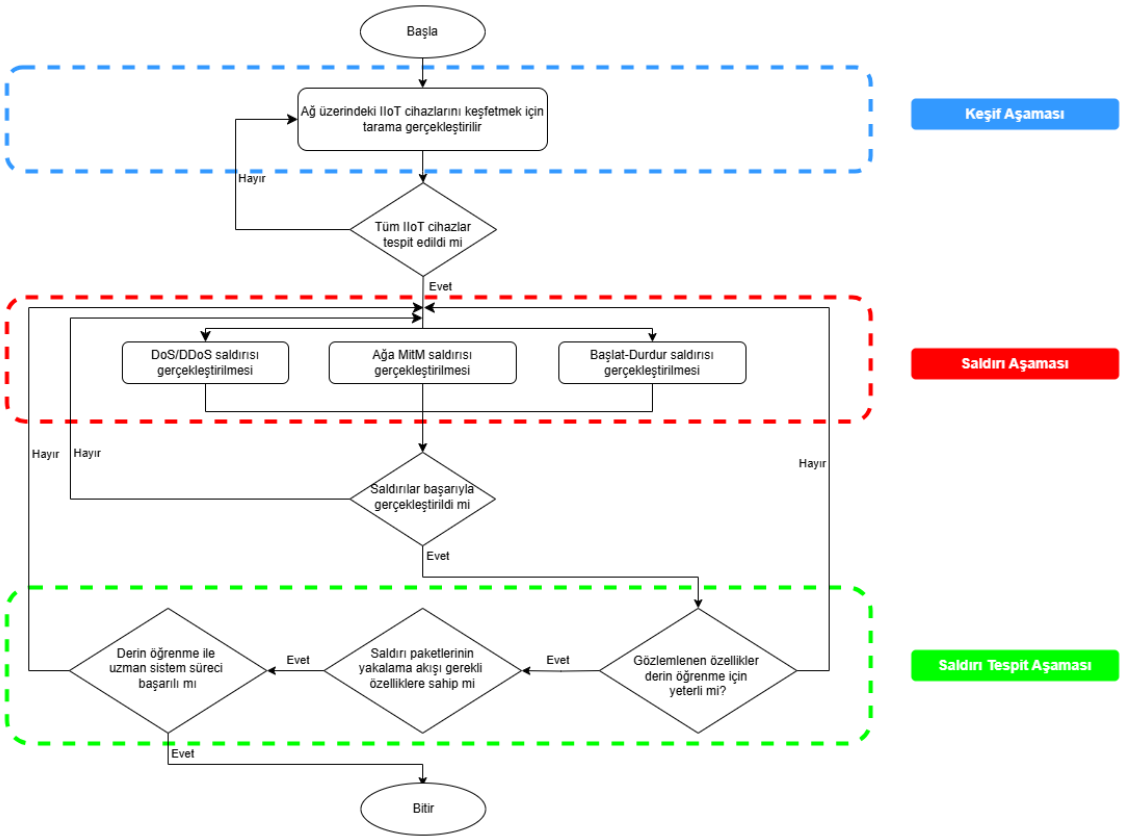
İkinci aşamada, tespit edilen PLC cihazlarına ilişkin bilgilerin doğruluğunu test etmek için ağ trafiği dinlenmiştir. Bu kapsamda, ortadaki adam saldırısı gerçekleştirilmiştir. Bu saldırı türü, ağdaki verileri dinleyerek ağ üzerindeki cihazları ve verileri ele geçirmek için kullanılmaktadır. Saldırı yaklaşımının gerçekleştirilmesinde, günümüzdeki saldırganların uyguladıkları yaklaşımlara benzer davranışlar planlanmıştır. Planlanan senaryo gereği ağ üzerindeki PLC cihazları doğrulandıktan sonra, gerçekleştirilen saldırılar ile ağ yöneticilerinin ve siber güvenlik personelinin dikkatini dağıtmak için DDoS saldırısı gerçekleştirerek ağın yasal kullanıcılara hizmet vermesi engellenmiş ve hedef saldırı olan başlat-durdur saldırısı için de perdeleme saldırısı olarak kullanılmıştır.

Ardından, saldırı analizlerinin asıl hedefi olan kritik altyapıların önemli bir bileşeni olan S7-1200 PLC cihazına başlat-durdur saldırısı gerçekleştirerek sistem istem dışı olarak kapatılıp-açılmıştır. PLC cihazları, endüstriyel nesnelerin interneti (IIoT) cihazlarından gelen sensör verilerini merkeze aktarmak veya motor sistemlerinin yönetimini yapmak

için kullanılan cihazlardır. Bu cihazlar, akıllı fabrikalar, akıllı şehirler ve kritik altyapılar gibi birçok alanda yaygın olarak kullanılmaktadır. Bu nedenle söz konusu cihazların başlatılması ve durdurulması aşamaları oldukça kritiktir. Örneğin, bir baraj kapağının açılması gereken noktada açılamaması ya da açılmaması gereken noktada istenilen seviyeden çok daha fazla miktarda açık kalması insan hayatı da dahil olmak üzere önemli sonuçlara neden olabilmektedir.

Gerçekleştirilen saldırılardan DDoS ve başlat-durdur saldırılarının etkileri sistem üzerinde açıkça görülebilir olduğu için ağ yöneticileri ve siber güvenlik personeli tarafından nispeten kolaylıkla tespit edilebilmektedir. Ancak, ortadaki adam saldırısı, ağda iz bırakmadığı için tespit edilmesi daha zor olmaktadır. Bu nedenle çalışmanın saldırı tespit çalışmaları kısmında her bir saldırı özel olarak tek tek incelenmiştir.

Tezin bu kesiminde tez içinde önem verilen, gerçekleştirilen saldırı ve tespitler aktarılmaktadır.



Şekil 4.3. Akış Şeması

4.1.1. Önerilen İzinsiz Giriş Tespit Çözümünün Mimari Tasarımı

Önerilen uzman sistem analiz yöntemi üç ana bileşenden oluşmaktadır: Veri toplama, Veri işleme ve Veri görselleştirme.

Veri toplama işleminde; bir ağ bağlantı cihazı, orijinal veri paketlerini etkilemeden verilerin yansıtılmış bir kopyasını oluşturmaktadır. Ağ dinleme cihazı ise bu yansıtılmış kopya üzerinden IoT ve IIoT cihazları tarafından oluşturulan trafik verilerini toplamakta, toplanan trafik bilgisini veri işleme bileşeninin konuşlandırıldığı bir bilgisayara göndermektedir.

Veri işleme, yapay zeka tabanlı uzman sistemin uygulandığı önerilen analiz yönteminin temel bileşenidir. Veri işleme bileşeni, toplanan ağ trafik verilerini almakta, verileri analiz etmek ve herhangi bir saldırıyı tespit etmek için belirlenen saldırı tespit modellerini kullanarak gerekli analizleri gerçekleştirmektedir. Veri işleme bileşeni dört alt bileşenden oluşmaktadır: Paket filtreleme, Öznitelik çıkarma, Sınıflandırma ve Uyarı oluşturma.

Paket filtreleme, ağ trafiği verilerinden alakasız veya gereksiz paketlerin filtrelenmesi işlemidir. Örneğin, IIoT cihazları ile PLC'ler arasındaki veya PLC'ler ile HMI arasındaki iletişimle ilgili olmayan paketler atılmaktadır. Paket filtreleme ile verilerin boyutu azaltılmakta ve sonraki analiz adımları hızlandırılmaktadır.

Öznitelik çıkarma, ağın normal veya anormal davranışını karakterize etmek için kullanılacak filtrelenmiş paketlerden ilgili öznitelikleri çıkarma işlemidir. Öznitelikler, kullanılan protokole ve uygulamaya bağlı olarak paket başlıklarından veya yüklerinden belirlenmektedir.

Sınıflandırma, ağ trafiği verilerini normal veya saldırı kategorilerine sınıflandırmak için yapay zeka tabanlı uzman sistemin uygulanma sürecidir. Uzman sistem, ağ taraması, MitM, DDoS ve başlat-durdur saldırıları gibi farklı saldırı türlerinin kalıplarını ve imzalarını tanımlamak için yapay zeka tabanlı bir yaklaşım kullanmakta ayrıca, geçmiş veya etiketli verilerden öğrenmek, doğruluğunu artırmak için makine öğrenimi tekniklerini de kullanmaktadır. Sınıflandırma işlemi, saldırıların varlığını veya yokluğunu ve saldırı türünü gösteren ikili veya çok sınıflı bir çıktı üretmektedir.

Uyarı oluşturma, sınıflandırma sürecinin çıktısına dayalı olarak uyarı oluşturma sürecidir. Uyarılar kural tabanlı uzman sistem kullanılarak zaman damgası, kaynak ve hedef IP adresleri, bağlantı noktaları, protokol, saldırı türü ve saldırının önem düzeyi gibi bilgileri

içermektedir. Ayrıca, oluşturulan uyarılar saklanmakta ve sistem yöneticileri tarafından aksiyon alınmak için veri görselleştirme bileşenine gönderilmektedir.

Veri görselleştirme, uyarıları ve ağ trafiği verilerini siber güvenlik personeline veya sistem yöneticilerine grafiksel ve etkileşimli bir şekilde sunma sürecidir. Veri görselleştirme, uyarıları ve ağ trafiği verilerini siber güvenlik personeli ve/veya sistem yöneticileri tarafından sezgisel ve anlaşılması kolay bir şekilde görüntülemek için grafiksel ve etkileşimli bir şekilde göstermek için gösterge tabloları, çizelgeler, grafikler, haritalar veya tablolar kullanılmaktadır. Ayrıca, veri görselleştirme, kullanıcıların verileri keşfetmesine ve ayrıntılara inmesine olanak tanımak için filtreleme, arama, sıralama ve yakınlaştırma işlevleri de sağlayabilmektedir. Veri görselleştirme, kullanıcıların ağ durumunu izlemelerine, saldırı kaynaklarını ve hedeflerini belirlemelerine, saldırıların etkisini değerlendirmelerine ve saldırıları azaltmak için uygun önlemleri almalarına yardımcı olmaktadır.

4.2. IoT ve IIoT Sistemlerine Saldırı Aşamaları

IoT ve IIoT sistemlerine yönelik gerçekleştirilen saldırıların aşamaları ve bu saldırıların sistemler üzerindeki etkileri detaylı bir şekilde incelenmiştir. IoT cihazlarının yaygınlaşmasıyla birlikte, bu cihazların güvenliğini tehdit eden çeşitli saldırılar, hem günlük hayatın parçası olan cihazlar hem de endüstriyel uygulamalar için büyük önem arz etmektedir. İlk olarak, IoT sistemlerine yönelik saldırılar ele alınmış, sel *(hello flood)* saldırıları ve MQTT protokolüne yönelik kaba kuvvet *(bruteforce)* saldırıları gibi yöntemlerle hedef cihazların zafiyetleri ortaya konulmuştur. Bu aşamada elde edilen veriler kullanılarak, saldırıların ağ trafiği, güç tüketimi ve cihaz performansı üzerindeki etkileri detaylı analizlerle incelenmiştir.

Benzer şekilde, IIoT sistemlerine yönelik saldırılar da ağ taraması ve ortadaki adam (MitM) saldırıları ile başlamış, ardından dağıtık hizmet reddi (DDoS) ve başlat-durdur saldırıları gibi daha sofistike saldırılar gerçekleştirilmiştir. Bu saldırıların tespiti ve etkilerinin minimize edilmesi amacıyla yapay zeka tabanlı uzman sistemler kullanılarak, güvenlik önlemlerinin etkinliği değerlendirilmiştir. Her iki sistem türü için gerçekleştirilen saldırıların ağ trafiği ve cihaz performansı üzerindeki etkileri detaylı analizlerle ortaya konulmuştur.

Bu kapsamlı analizler, IoT ve IIoT cihazlarının güvenliğinin sağlanmasında kritik adımların belirlenmesine ve uygun savunma stratejilerinin geliştirilmesine katkı

sağlamaktadır. IoT ve IIoT teknolojilerinin güvenli bir şekilde kullanılabilmesi için gerçekleştirilen bu çalışmalar, güvenlik açıklarının tespit edilmesi ve bu açıkların giderilmesi yönünde önemli bilgiler sunmaktadır.

4.2.1. IoT Cihazlarına Yönelik Gerçekleştirilen Saldırıların Analizi

Son yıllarda Nesnelerin İnterneti (IoT) teknolojisi, çeşitli alanlarda (örneğin sağlık kurumları, küçük ev aletleri ve fabrikalar gibi) mikroişlemciler kullanarak cihazların kontrol mekanizmalarını iyileştirmek için yaygın olarak benimsenmiştir. Bu teknoloji, gerçek dünyadan veri toplayan akıllı cihazlar üzerine kurulmuştur. Bu cihazlar, aldıkları verileri işleyerek ve ileterek bilgi temelli hizmetler üretmekte ve gerekli işlemleri gerçekleştirmektedir [69].

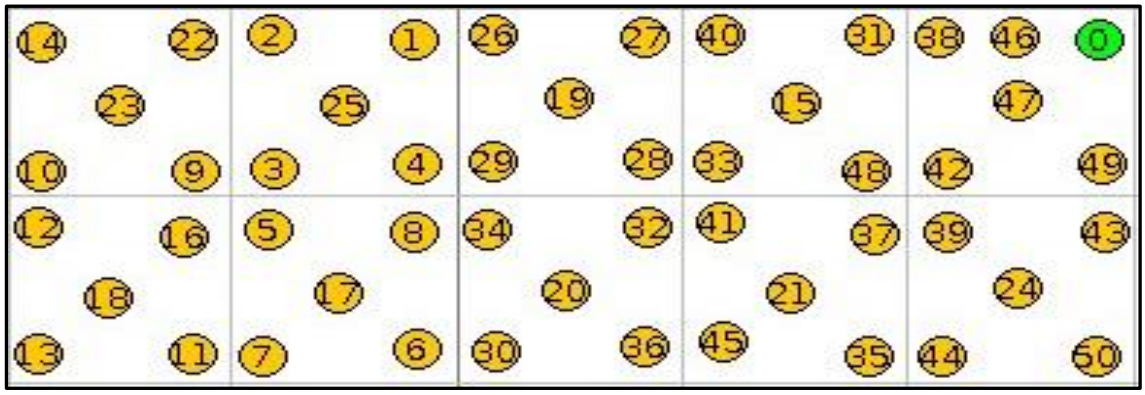
IoT teknolojisinin popüler hale gelmesiyle birlikte, bu teknolojinin birçok alanda kullanılması öngörülmektedir. Lojistik, ulaşım, giyilebilir teknoloji, akıllı cihazlar, akıllı tarım, akıllı sağlık gibi birçok sektörde kullanılması beklenen IoT, 2025 yılına kadar 75 milyar farklı cihaza entegre edilmesi planlanmaktadır [70]. McKinsey Global Institute, IoT'nin 2025 yılına kadar ekonomik olarak 11 trilyon dolar değerine ulaşacağını ve bunun büyük bir kısmının iş ve endüstriyel uygulamalarda gerçekleşeceğini tahmin etmektedir [71, 72]. Ancak, IoT sektörünün hızlı büyümesiyle birlikte, sistemin güvenliği de önemli bir konu haline gelmiştir. Bu hızlı büyüyen sektörde güvenlik analizine maalesef yeterince önem verilmemektedir. IoT cihazları, günlük işlerimizi kolaylaştırsa da yüksek güvenlik açıklarına sahip olmaktadır. Mevcut yetersiz güvenlik önlemleri, insanların IoT sistemlerinden yeterince faydalanmalarını engellemekte ve IoT cihazlarının özellikle kaynak ve güç tüketimi sınırlamaları, saldırganların hedefi haline gelmektedir.

Saldırı analizlerinin bu bölümünde, akıllı fabrika modeli kullanılarak ısı, nem, basınç gibi IoT cihazlarının ve bir saldırgan cihazının merkezi düğüm *(mote)* ve uzak düğümler kullanarak temsil edilmesiyle IoT sistemlerine yönelik saldırı analizleri yapılmıştır. Gerçekleştirilen saldırının sistem üzerindeki etkisi, güç tüketimi ve paket analizi yoluyla çeşitli araçlar kullanılarak incelenmiştir. Ayrıca, çalışmanın uzman sistem bölümünde belirtildiği üzere trafik kayıtlarının analizi sonucunda, saldırgan düğüm, K-means algoritması kullanarak başarılı bir şekilde tespit edilmiştir.

4.2.1.1. 6LoWPAN Protokolü Sel (Flood) Saldırısı

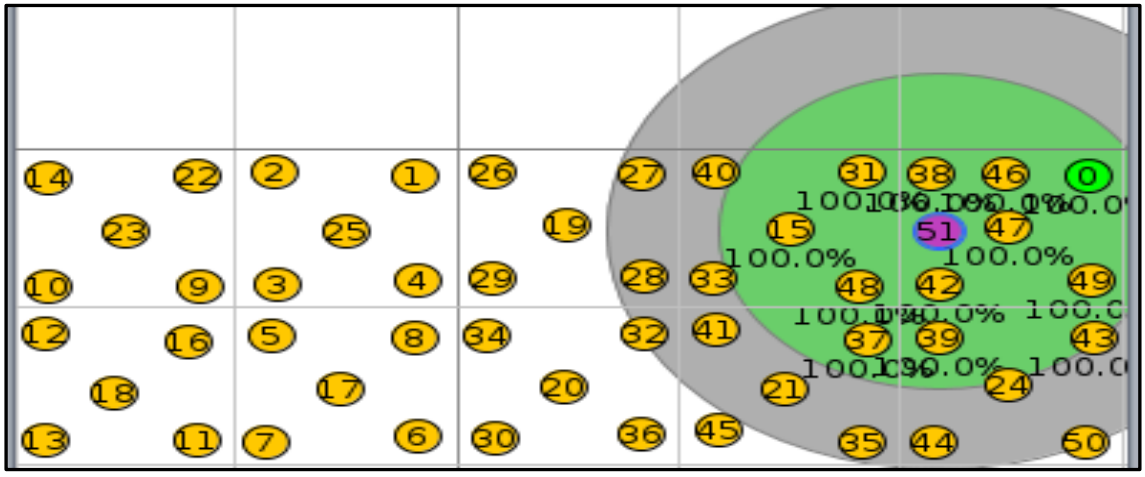
IoT'ye yönelik gerçekleştirilen ilk saldırı analizinde önemli saldırılardan biri olan sel *(flood)* saldırısının sistem üzerindeki etkisi incelenmiştir. Çalışmada, merhaba sel *(hello flood)* saldırısı Contiki işletim sistemi üzerinde Cooja simülatörü ve Foren6 6LoWPAN ağ analiz aracı kullanılarak simüle edilmiştir. Analiz kapsamında ilk olarak, Contiki simülatörü ile bir ağ modeli oluşturulmuştur. Modelde bir merkezi düğüm, 50 standart düğüm ve bir saldırgan düğüm yer almaktadır. Nesnelerin İnternetinin büyük bir bölümü, sensörlerle donatılmış kablosuz alıcı-vericilerden oluşan düğümlerle sağlanmaktadır. Bu düğümlere "mote *(remote control)*" denilmekte ve genellikle her fiziksel sensör cihazında bulunmaktadır. Standart düğümler, dış ağlarla iletişim kurmak için merkezi düğümü kullanmaktadır. Saldırgan düğümün amacı, ağa sürekli olarak merhaba *(hello)* paketleri göndererek standart ve merkezi düğümlerin batarya tüketimini arttırmaktır. Bu trafiğin sonucunda, diğer düğümler saldırgan düğümlerden gelen paketlere yanıt vermeye çalışarak, görevlerini yerine getiremez hale gelmektedir.

Şekil 4.4.'te saldırganın bulunmadığı IoT ağına ilişkin saldırganın bulunmadığı topoloji görülmektedir. Bu ağ, referans model ağı olarak nitelendirilmiştir. Referans model ağın paketlerinin yakalanmasıyla saldırganın bulunduğu ağ paketlerinin sistem üzerine etkisi mukayese edilmesi yoluyla görülebilmektedir.



Şekil 4.4. Referans Ağ Topolojisi

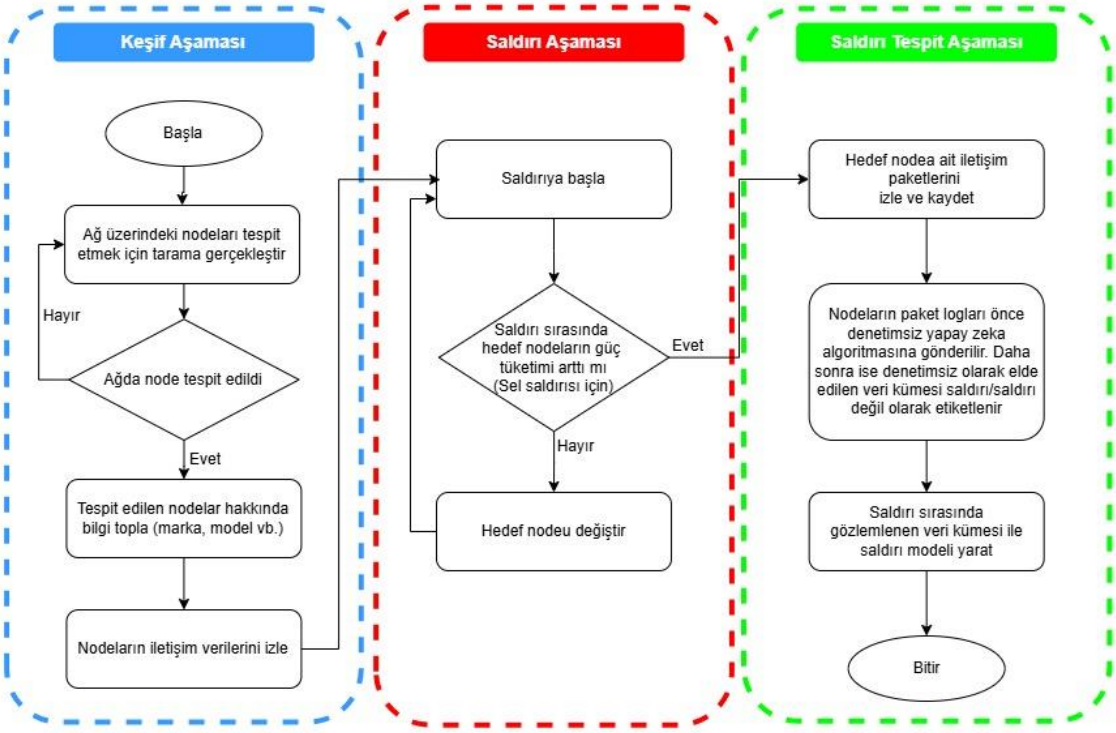
Şekil 4.5.'te yer alan yeşil düğüm, merkezi düğümü temsil etmekte, sarı düğümler standart düğümleri, mor düğüm ise saldırgan düğümü temsil etmektedir. Saldırı sırasında, saldırgan düğüm merkezi düğümün iletim kapasitesi içerisinde bulunarak diğer düğümlere merhaba *(hello)* paketleri gönderir. Diğer düğümler, gönderilen merhaba paketlerine yanıt vererek, paketin kaynak düğüme geri dönmesini sağlamaktadır. Bu şekilde saldırı başarılı bir şekilde gerçekleştirilmektedir.



Şekil 4.5. Saldırganlı Ağ Topolojisi

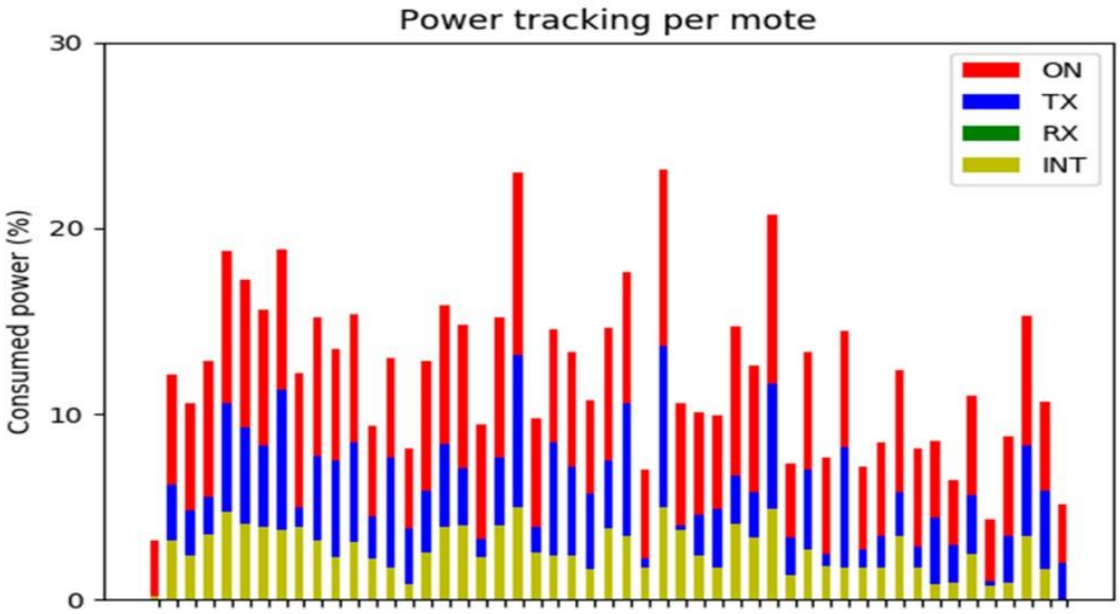
Ağ topolojisindeki bütün sensör cihazları, iletişim için birbirlerine paket göndermektedir. Simülasyon sırasında gerçekleştirilen senaryoda, düğümler arasındaki iletişim Wireshark aracılığıyla izlenmiş, kaydedilmiş ve incelenmiştir. Bu yöntemle saldırının sistem üzerindeki etkisi sürekli olarak izlenmiştir.

Şekil 4.6.'da yer alan akış diyagramı incelendiğinde, merhaba sel *(hello flood)* saldırısının üç aşamadan oluştuğu görülmektedir. İlk olarak, cihazlara ait bilgiler toplanmıştır. Bu aşamada, ağ taraması yapılarak ağda yer alan düğümler tespit edilmiştir. Düğümler tespit edildikten sonra cihazlara ait bilgiler toplanmış ve ağ trafiği analiz edilmiştir; böylece merkezi düğüm belirlenmiştir. İkinci aşamada ise merhaba sel saldırısı başlatılmış ve saldırgan düğüm ağ üzerinde bulunan diğer düğümlere sürekli olarak merhaba paketleri göndermiştir. Müteakip olarak, gönderilen paketlerin yoğunluğu nedeniyle, diğer düğümlerin iletişim süreleri ve batarya tüketim durumları izlenmiştir. Son aşamada, saldırının tespit edilmesine odaklanılmıştır. Bu aşamada, aynalanan ağ trafiği kaydedilmiş, bir yandan ağ adli analiz aracı ile incelenirken diğer yandan da makine öğrenimi algoritmasına aktarılarak saldırının tespitine odaklanılmıştır.

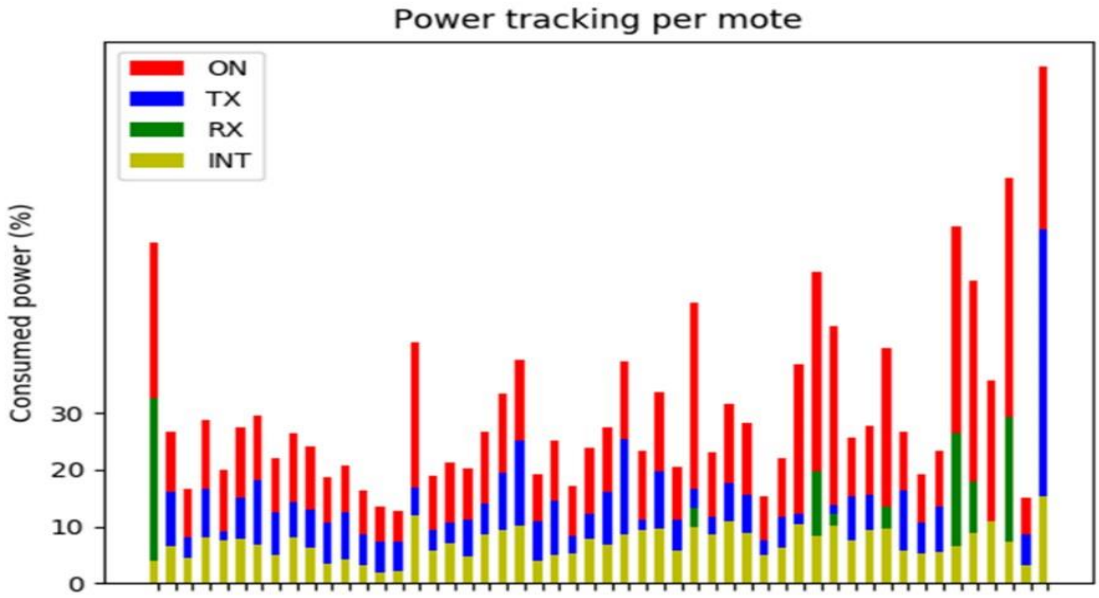


Şekil 4.6. IoT Merhaba Sel *(Hello Flood)* Saldırısı Akış Diyagramı

Bu bölümde, Şekil 4.7.'de gösterilen referans değerleri, saldırı gerçekleştirilen Şekil 4.8.'deki değerler ile karşılaştırılmıştır. Bu nedenle, IoT cihazları üzerindeki saldırının etkileri incelenmiştir. Şekil 4.7. ve Şekil 4.8. karşılaştırıldığında, ON değerleri cihaz düğümlerinin çalışırken tükettikleri güç miktarını göstermektedir. INT değerleri ise düğümlerin iletişim yoğunluğunu temsil eden karışma değerleridir. Şekil 4.7.'de, cihaz düğümleri çalışırken güç tüketimleri yaklaşık %20 olurken karışma değerlerinin %5 civarında olduğu görülmektedir. Şekil 4.8.'de ise, cihaz düğümleri açıkken güç tüketiminin yaklaşık %40 - %50 arasında olduğu gözlenmiştir. Ayrıca, saldırgan düğüme yakın düğümlerde karışma değerlerinde bir artış olduğu belirlenmiştir. Bu şekilde, IoT cihazları üzerinde saldırının etkileri değerlendirilmiştir.



Şekil 4.7. Referans Güç Tüketim Grafiği

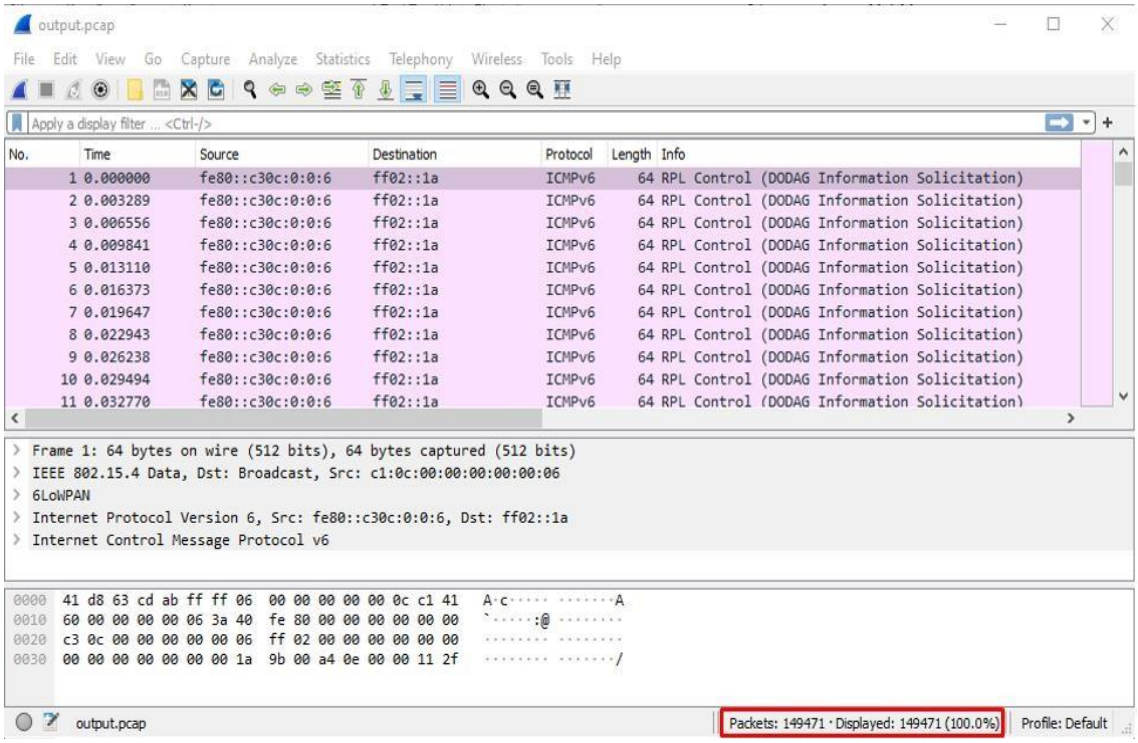


Şekil 4.8. Saldırganlı Güç Tüketim Grafiği

Test ortamı, Hedef Odaklı Yönlendirilmemiş Akrilik Grafik (Destination Oriented Directed Acyclic Graph-DODAG) ağı üzerinde gerçekleştirilmiştir. DODAG yapısında, ağ iletişimi kök düğümde sona erdirilmelidir. Aksi taktirde, kök düğümün gecikmiş iletişimi bu ağda önemli kayıplara yol açabilmektedir [73].

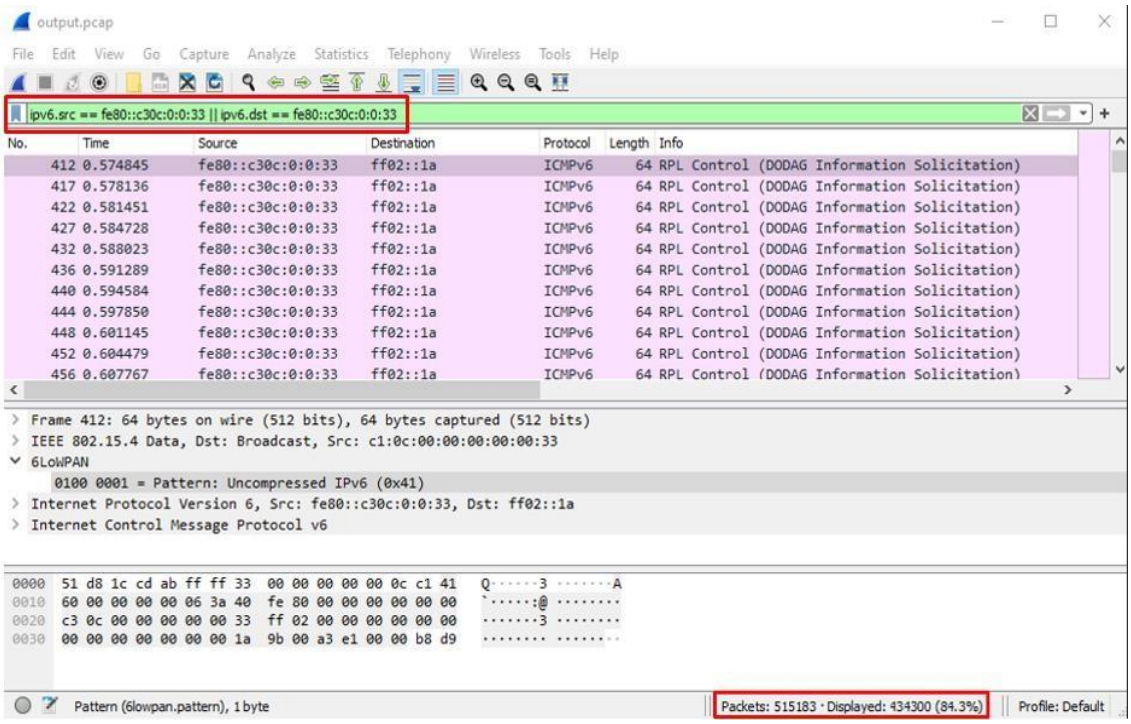
Wireshark'ta DODAG ağındaki *"pcap"* kayıtları incelendiğinde, Şekil 4.7. ve Şekil 4.8.'deki grafiksel açıklamaların desteklendiği görülmüştür. Şekil 4.9., saldırgan düğümün DODAG ağı içinde olmadığı zaman dilimini gösterirken, Şekil 4.10. saldırgan

düğümün ağa merhaba sel *(hello flood)* saldırısı gerçekleştirdiği senaryoyu göstermektedir.



Şekil 4.9. Referans Yakalanan Ağ Paketleri

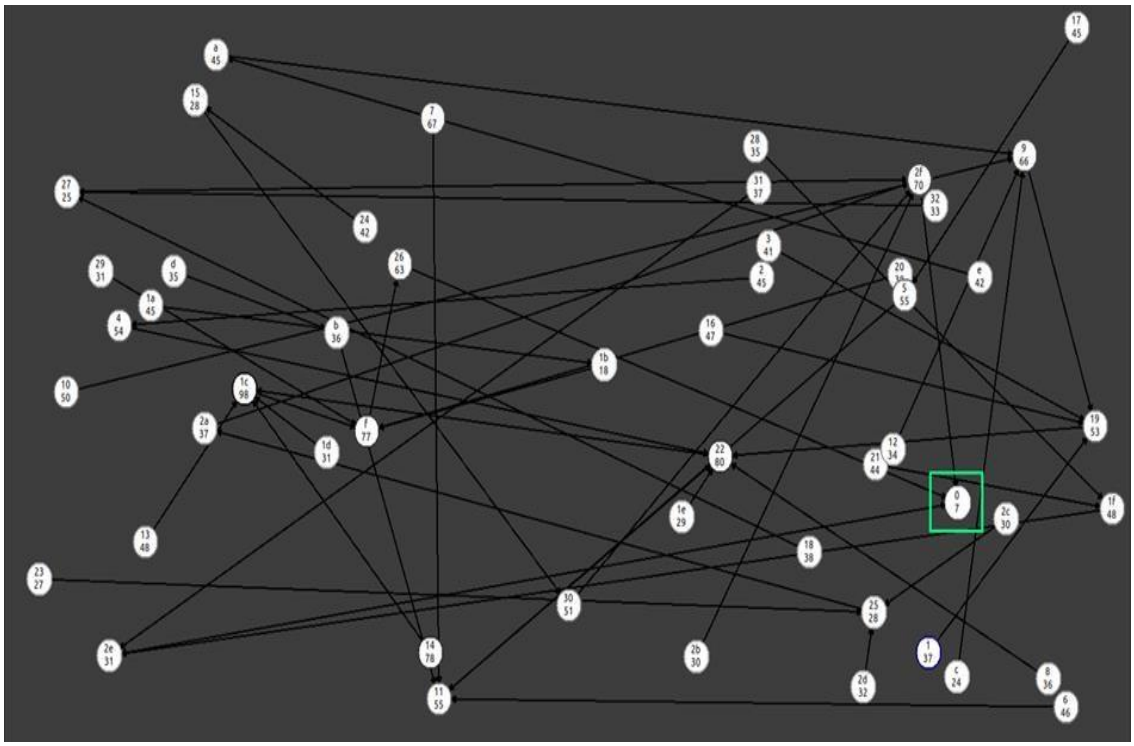
Wireshark ile analiz edilen paketler Şekil 4.9. ve Şekil 4.10.'da gösterilmiştir. Şekil 4.9. ve Şekil 4.10. karşılaştırıldığında, aynı zamanda meydana gelen iletişim trafiğinin referans ağda 149471 paket iken saldırı senaryosunda 515813 paket olduğu görülmüştür. Ayrıca, saldırı senaryosunda gözlenen paketlerin %84,3'ü saldırgan düğüm tarafından gönderilen ve alınan paketlere ait olduğu görülmektedir. Bu veriler, IoT ağlarında güç tüketiminin kritik öneme sahip olduğunu ve sel saldırısının etkilerini göstermektedir.



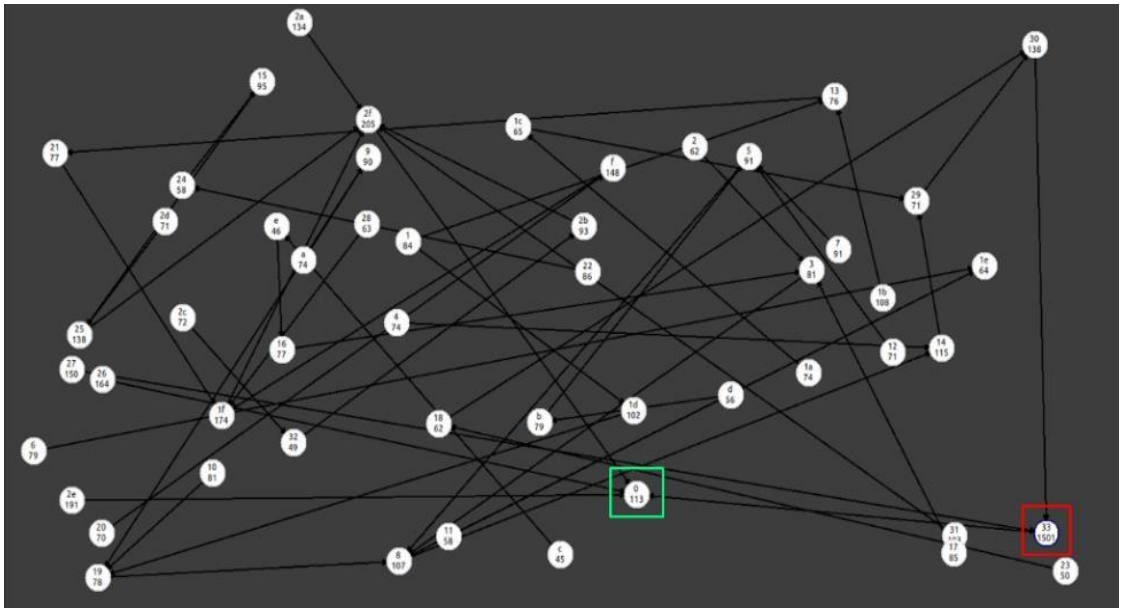
Şekil 4.10. Saldırganlı Yakalanan Ağ Paketleri

Sel saldırısının sistem üzerindeki etki analizi değerlendirildiğinde, saldırgan düğümün ağa dahil edilmesiyle birlikte tüm trafiğin bozulduğu görülmüştür. Kablosuz sensör ağlarında (Wireless Sensor Network-WSN), güç tüketimi ve sistem akışı, diğer sistemlerden farklılık gösterebilmektedir. Örneğin, veri merkezlerindeki sunucular, sabit bir sıcaklıkta bulundurulmalıdır. Kablosuz sensör ağları, sıcaklık belirli bir eşiğin altına veya üstüne çıktığında devreye girmekte ve önceden belirlenmiş sıcaklık düzeylerine ulaşmak için soğutma veya ısıtma sistemlerini aktive etmektedir. Bu çalıştırma işlemi sonucunda, veri merkezi otomatik olarak istenen sıcaklık seviyesine getirilmektedir. Ancak, bu kablosuz sensör ağına giren ve/veya ele geçirilen bir saldırgan düğüm, veri merkezini yangın gibi felaket riskiyle karşı karşıya bırakabilmektedir. Bu durum, sistemde kök düğümün iletişimini geciktirerek ısıtma/soğutma sisteminin tetiklenmesini de geciktirebilmektedir.

Analizin ikinci aşamasında, referans ve saldırı senaryolarının ağ trafiği, 6LoWPAN ağların da adli analiz yapabilen açık kaynak kodlu Foren6 IoT ağ analiz aracı [74] ile incelenmiştir. Foren6 uygulaması, IoT ağlarında gerçek zamanlı veya sonradan analiz ve paket incelemesi yapabilen bir ağ adli analizi yazılımdır. Analiz sonuçları, Şekil 4.11. ve Şekil 4.12.'de gösterilmektedir.



Şekil 4.11. Referans Ağ Paketlerinin Analizi



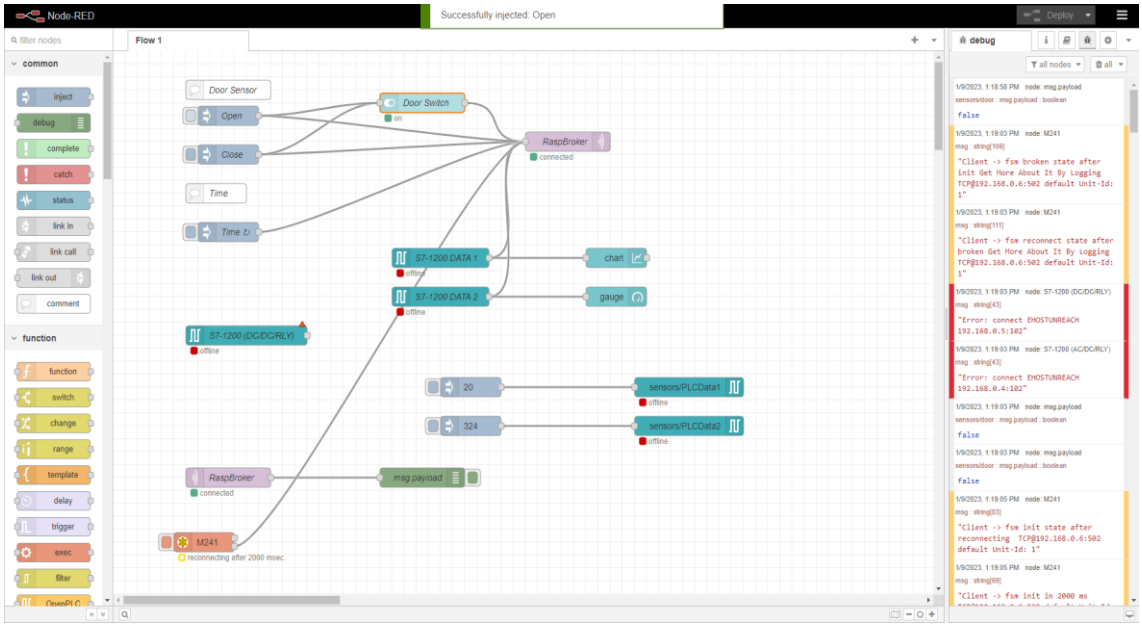
Şekil 4.12. Saldırganlı Ağ Paketlerinin Analizi

Saldırganın bulunduğu ağda, saldırgan düğüm 1501 paket gönderirken, tüm düğümlerle haberleşme halinde olması gereken kök düğüm ise yalnızca 113 paket gönderebilmiştir. Ayrıca, referans model olan saldırganın bulunmadığı ağda kontrol ve veri paketlerinin toplam sayısı 2015 iken, saldırganın bulunduğu ağ trafiği incelendiğinde, paketlerin toplam sayısının 5956'ya yükseldiği görülmüştür.

4.2.1.2. MQTT Protokolü Saldırıları

IoT saldırı analizlerinin ikinci kısmında, IoT cihazlarında yaygın olarak kullanılan MQTT protokolüne yönelik saldırılar gerçekleştirilmiştir ve bu saldırılara ait veriler ağ üzerinden toplanarak analiz edilmiştir. MQTT saldırılarının ilk aşamasında, Şekil 4.13.'te görülen Node-RED uygulaması kullanılarak, IoT ve IIoT sistemleri bir arada çalıştırılmış ve MQTT Broker'a gönderilen ve gelen paketlerin yönetilebildiği ve IIoT cihazı olan PLC'lerin veri tablosu üzerinde değişiklik yapılabildiği teyit edilmiştir. MQTT Broker, sistem üzerinde bulut (*on-premise*) tabanlı olarak tasarlanmış ve kullanıcı adı ve parola koruması ile yetkisiz erişimler kısıtlanmıştır. Bu şekilde, MQTT protokolünün kullanımı ile ilgili olası saldırıları öngörmek için saldırı verileri analiz edilmiştir. Bu veriler, ağ üzerinden toplanarak, saldırganların kullanabileceği çeşitli araçlar ve tekniklerle ilgili bilgileri içermektedir. Analiz edilen veriler, saldırıları tespit etmek ve önlemek için oldukça faydalı bilgiler sağlamaktadır.

Analizler kapsamında, MQTT protokolü kullanılarak yapılabilecek saldırılara karşı önlem almak amacıyla, saldırıları verilerinin analizi yapılmış ve saldırılara karşı bir savunma stratejisi belirlenmesi önerilmiştir.

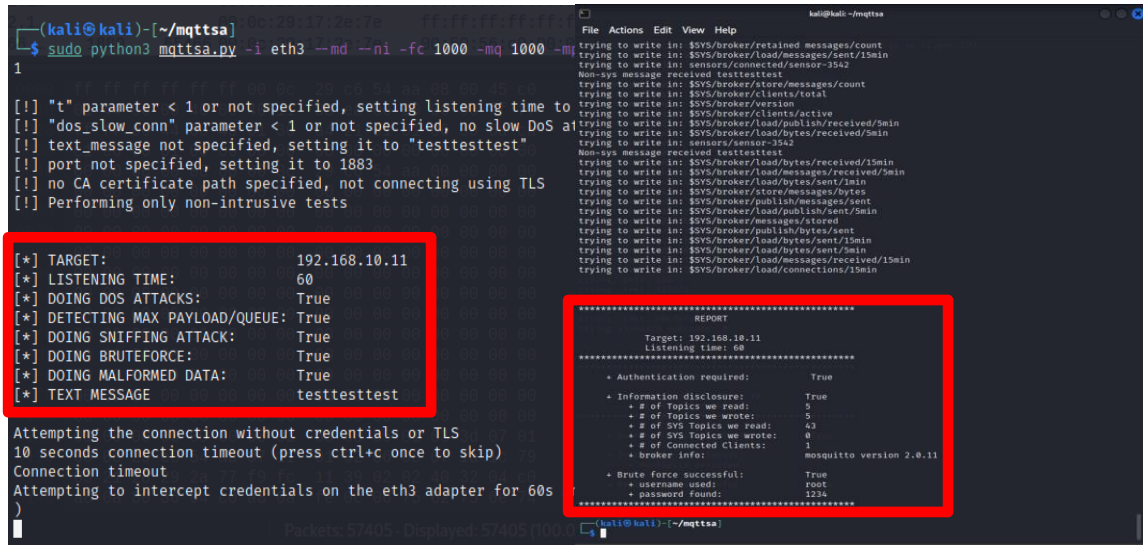


Şekil 4.13. Node-RED Uygulaması

MQTT saldırı analizinin ikinci aşamasında, MQTT Protokolüne yönelik gerçekleştirilebilecek saldırılar belirlenmiştir. Bu saldırılar; kaba kuvvet *(bruteforce)* parola saldırısı, hizmet reddi saldırısı, veri sızdırma ve hatalı veri enjeksiyonu olarak

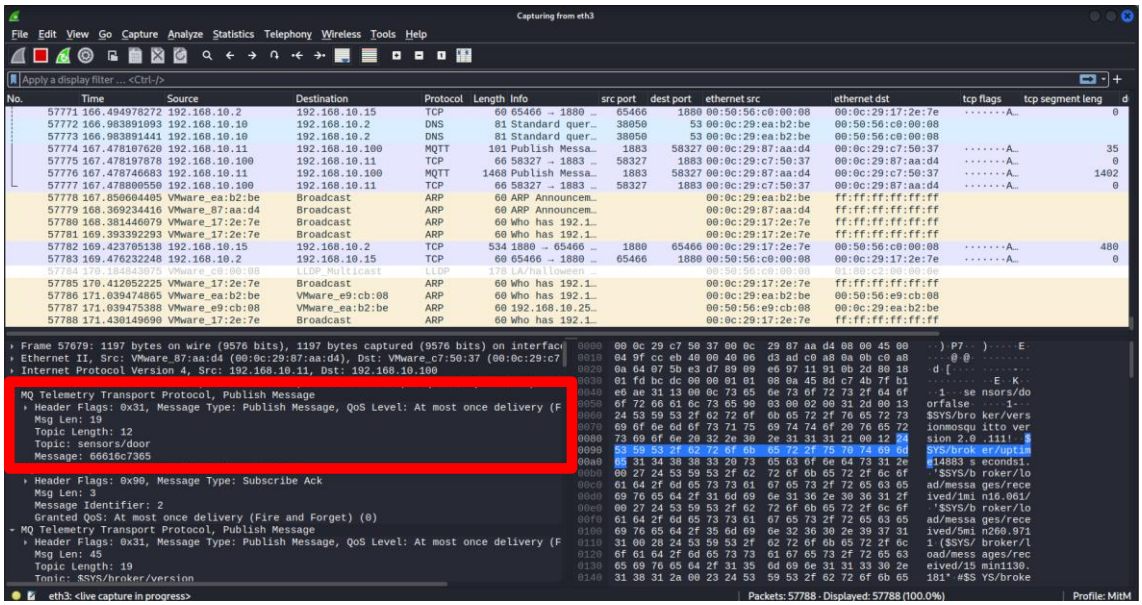
sıralanmıştır. Saldırılar MQTT Broker'ına yönelik olarak gerçekleştirilmiş ve ağ üzerinde saldırılara ait paketler toplanarak analiz edilmek üzere incelenmiştir.

Kaba kuvvet saldırısı esnasında saldırganlar, zayıf parolaları tahmin ederek, sisteme yetkisiz erişim sağlamaya çalışabilmektedir. Kaba kuvvet saldırısı gerçekleştirilirken, öncelikle saldırı yapılacak sistem tespit edilmiş ve sözlük dosyası hazırlanmıştır. Ardından, hazırlanan sözlük dosyası kullanılarak saldırı gerçekleştirilmiştir. Saldırı sonucu elde edilen veriler Şekil 4.14.'te görülmektedir. Bunun yanı sıra, veri sızıntısı saldırısı da denenmiştir ve Şekil 4.13.'te görülen kapı durumuna ait veri, Şekil 4.15.'te görüldüğü gibi ağ üzerinden okunabilmiştir.



Şekil 4.14. MQTT Broker Kaba Kuvvet ve Veri Sızıntısı Saldırısı

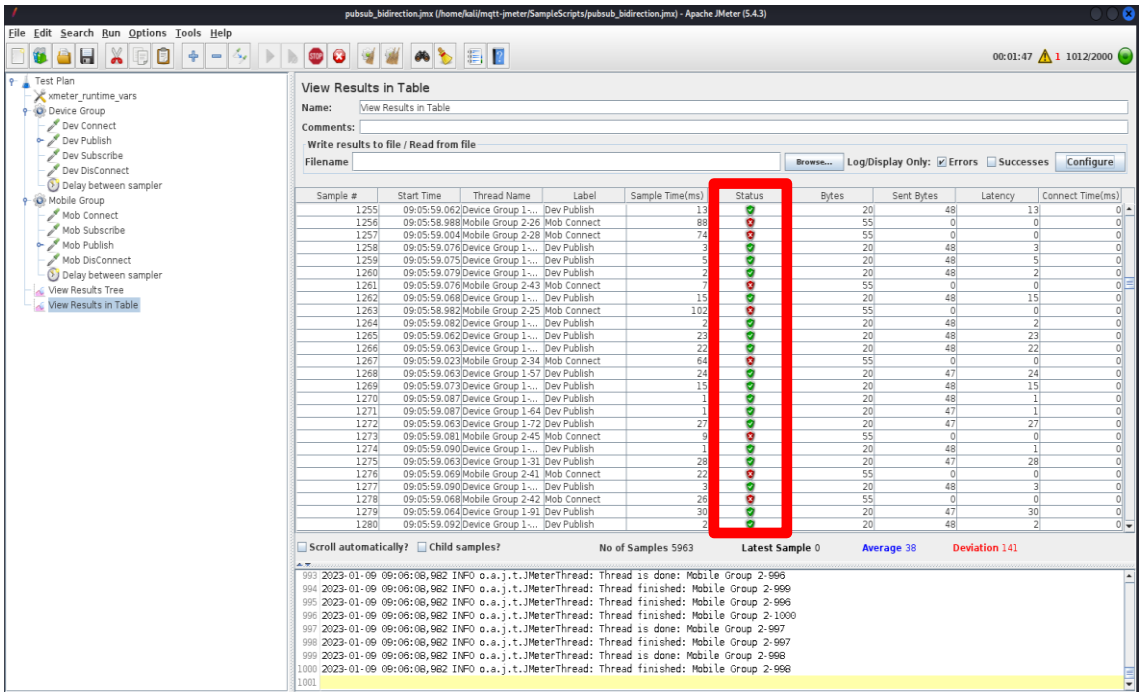
Bu durum, MQTT protokolüne yönelik gerçekleştirilebilecek veri sızıntısı saldırılarının varlığını göstermektedir. Saldırganlar, MQTT Broker'a yetkisiz erişim sağlayarak, cihazların verilerini çalmaya veya okumaya çalışabilmektedir. Bu nedenle, kullanıcı adı ve parola koruması gibi güvenlik önlemleri alınarak, MQTT Broker'ın güvenliği artırılmalıdır. Ayrıca, cihazların veri iletişimi güvenli hale getirilmeli ve saldırılara karşı korunaklı hale getirilmelidir.



Şekil 4.15. MQTT Broker Veri Sızıntısı

MQTT Broker sunucusuna yönelik Şekil 4.16.'da görülen JMeter yük/stress testi aracı kullanılarak kaba kuvvet saldırısı gerçekleştirilmiştir. Bu saldırı sonucunda, elde edilen kullanıcı adı ve parola bilgileri kullanılarak 1000 kullanıcı cihaz ve 1000 adet mobil cihazdan veri yükleme ve kayıt işlemleri gerçekleştirilmiştir. Kaydedilen cihaz sayısının yüksek olmamasına rağmen, MQTT Broker'ın bazı kayıtlara cevap veremediği ve kullanıcı sayısının artırılarak sistemin hizmet dışı bırakılabildiği Şekil 4.16.'da görülmektedir.

Bu durum, MQTT Broker'ın kısıtlı kaynaklara sahip olması nedeniyle yüksek kullanıcı trafiği altında hizmet dışı kalabileceğini göstermektedir. Bu nedenle, MQTT Broker'ın performansını artırmak için gereken önlemler alınmalıdır. Örneğin, kaynak kullanımını optimize etmek, yüksek kullanıcı trafiği altında stabil çalışmasını sağlamak, veri iletişiminde hızlı ve güvenli bağlantılar sağlamak gibi önlemler alınmalıdır. Ayrıca, saldırılara karşı korunmak için güvenlik duvarı gibi yazılımsal ve donanımsal güvenlik sistemleri de kullanılmalıdır.



Şekil 4.16. MQTT Brokera Yönelik Yük Testi ile Hizmet Dışı Bırakma Saldırısı

MQTT protokolüne yönelik saldırılar gerçekleştirilerek, saldırılara ait ağ paketleri toplanmıştır. Bu paketler, müteakip aşamada belirtilen uzman sistem modeli oluşturmak amacıyla kullanılmıştır. Bu model, saldırıları tespit etmek ve önlemek için kullanılmaktadır. Bu saldırıların gerçekleştirilmesi, MQTT protokolünün güvenliği hakkında farkındalık yaratmış ve kullanıcıları bu tür saldırılara karşı korunmaya teşvik etmiştir. Ayrıca, MQTT Broker'ın güvenliği artırmak ve performansını optimize etmek için gereken önlemler belirlenmiştir.

MQTT Broker'a gerçekleştirilen saldırılara ve saldırıların gerçekleşme durumuna ait karşılaştırması Tablo 4.1.'de görülmektedir.

Saldırı Tipleri	MQTT Broker (Korumasız)	MQTT Broker (Parola Korumalı)		MQTT Broker (TLS ve Parola Korumalı)
		Parolası Kırılamayan	Parolası Kırılan	
Kaba Kuvvet Saldırısı	--	✓		X
Bilgi İfşası	✓	X	✓	X

Hizmet Dışı Bırakma (DoS)/Sürekli Paket Gönderme	✓	X	✓	X
Hizmet Dışı Bırakma (Slowite-SlowDoS)/ Fasılalı Paket Gönderme	✓	X	✓	X
Hizmet Dışı Bırakma (DoS)/Büyük Paket Gönderme	✓	X	✓	X
Yanlış Veri Enjeksiyonu (FDI)	✓	X	✓	X

Tablo 4.1. MQTT Saldırı Gerçekleşme Durumu Kıyas Tablosu

MQTT sistemine gerçekleştirilebilecek saldırılar için veri iletişim hattının güvenliğinin alınması ile birlikte kullanılacak parolaların güçlü ve karmaşık yapıda seçilmesinin önemi Tablo 4.1.'de görülmektedir.

4.2.2. IIoT Cihazlarına Yönelik Gerçekleştirilen Saldırıların Analizi

Bu bölümde, örnek sistem üzerinde gerçekleştirilen saldırıların aşamaları ele alınmıştır. İlk olarak, ağ üzerindeki PLC cihazlarının tespiti için ağ taraması yapılmıştır. Tespit edilen cihazların doğruluğunu test etmek için ortadaki adam saldırısı gerçekleştirilmiş, PLC cihazları hakkında temel bilgiler alındıktan sonra, siber güvenlik personelinin dikkatini dağıtmak için perdeleme saldırısı olarak dağıtık hizmet reddi saldırısı aşamasına geçilmiştir. Son aşamada ise, çalışmanın hedef saldırısı olan başlat-durdur saldırısı gerçekleştirilmiştir. Bu saldırıların analizlerinde öncelikle gerçekleştirilen saldırıların sistem üzerindeki etkileri incelenmiştir. Saldırıların tespiti aşamasında ise yapay zeka tabanlı uzman sistemler kullanılmıştır.

4.2.2.1. IIoT Protokollerine Yönelik Saldırılar

Saldırı analizinin ilk aşamasında, ağda bulunan IIoT sistemlerini tespit etmek için *"nmap"* ağ tarama aracı kullanılmıştır. Bu tarama sonucunda, ağda bulunan IIoT cihazları Şekil 4.16.'da gösterildiği şekilde tespit edilmiştir. Ağ taramasının sonucunda, hedef alınacak PLC cihazlarının IP adresleri ve diğer bilgileri belirlenmiştir. Bu bilgiler, saldırıların daha etkili bir şekilde gerçekleştirilmesi için kullanılmıştır. Bu aşama, saldırıların hedefleri ile ilgili önemli bilgilerin elde edilmesi açısından oldukça önemlidir.

Sistemlere ait bilgilerin tespit edilmesi ve toplanması, saldırıların başarılı bir şekilde gerçekleştirilebilmesi için temel bir adımdır. Şekil 4.17. incelendiğinde PLC cihazının Siemens marka ve S7-1200 modeli olduğu, ayrıca modül ve temel donanım bilgileri ile versiyon bilgisinin açık bir şekilde elde edildiği görülmektedir.

```
Nmap scan report for 192.168.0.4
Host is up (0.0036s latency).
Not shown: 32 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
102/tcp open  iso-tsap Siemens S7 PLC
| s7-info:
|   Module: 6ES7 214-1BE30-0XB0
|   Basic Hardware: 6ES7 214-1BE30-0XB0
|_  Version: 2.2.0
Service Info: Device: specialized

Nmap scan report for 192.168.0.5
Host is up (0.0036s latency).
Not shown: 32 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
102/tcp open  iso-tsap Siemens S7 PLC
| s7-info:
|   Module: 6ES7 214-1HE30-0XB0
|   Basic Hardware: 6ES7 214-1HE30-0XB0
|_  Version: 2.2.0
Service Info: Device: specialized

Nmap scan report for 192.168.0.6
Host is up (0.0019s latency).
Not shown: 31 closed tcp ports (conn-refused)
PORT    STATE SERVICE VERSION
80/tcp  open  http    Wind River Web Server 4.8
|_http-server-header: WindRiver-WebServer/4.8
|_http-title: Site doesn't have a title (text/html).
502/tcp open  modbus  Modbus TCP

Nmap scan report for 192.168.0.7
Host is up (0.0016s latency).
Not shown: 31 closed tcp ports (conn-refused)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Hikvision IP camera httpd
|_http-title: index
|_http-server-header: App-webs/
| http-methods:
|_  Potentially risky methods: TRACE PUT DELETE
|_http-favicon: Hikvision DVR
443/tcp open  ssl/http Hikvision IP camera httpd
| ssl-cert: Subject: commonName=192.168.1.64/stateOrProvinceName=ZJ/countryName=CN
| Not valid before: 2015-09-09T01:31:16
|_Not valid after:  2018-09-08T01:31:16
|_http-server-header: App-webs/
|_ssl-date: 2023-01-01T14:02:12+00:00; +3h01m03s from scanner time.
|_http-favicon: Hikvision DVR
Service Info: Device: webcam
```

Şekil 4.17. Nmap ile Ağ Taraması

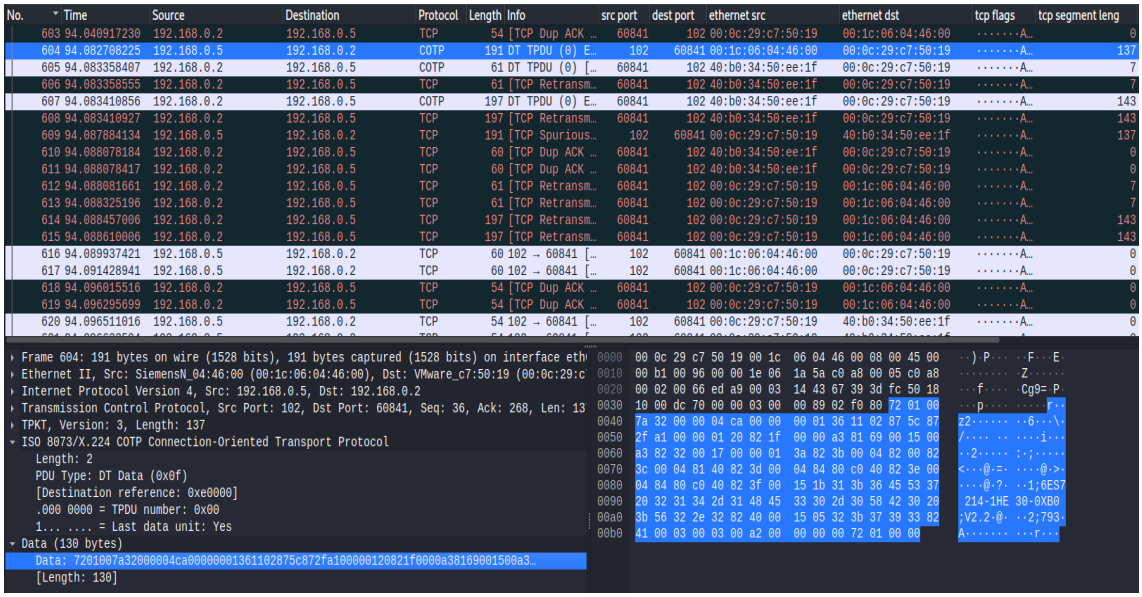
Ortadaki Adam Saldırısı (MitM)

PLC cihazlarına gerçekleştirilen saldırıların ikinci aşamasında, pasif bir saldırı türü olan ortadaki adam saldırısı (Man in the Middle - MitM) gerçekleştirilmiştir. Bu saldırı, ağ yöneticileri tarafından hedefli olarak araştırılmadığı takdirde tespiti zor bir saldırı olmaktadır. MitM saldırısı, kötü niyetli saldırganın iletişim kuran iki sistem arasına girerek iletişimi dinlediği, taklit ettiği ve aradaki bilgilere ulaştığı bir saldırı olarak

gerçekleştirilmektedir. Bu saldırı sayesinde, ağ üzerindeki hedef cihazların iletişim bilgileri kayıt altına alınabilmekte, aynı ağ paketleri kullanılarak istem dışı olarak benzer aktivasyonlar *(tekrar-replay saldırısı)* gerçekleştirilebilmekte ya da ağ paketlerinin içeriği değiştirilerek *(yanlış veri enjeksiyonu-false data injection saldırısı)* sistemlere farklı işlemler yaptırılabilmektedir.

Ağ taraması sırasında elde edilen PLC'lere ilişkin IP bilgileri kullanılarak, ortadaki adam saldırısı gerçekleştirilmiştir. Bu sayede, saldırı yapılan cihazların zafiyetleri ve bu zafiyetlerin sömürülmesine yönelik tehditler belirlenmiştir. Bu bilgiler, PLC cihazlarının güvenliği için önemli bir rol oynamaktadır.

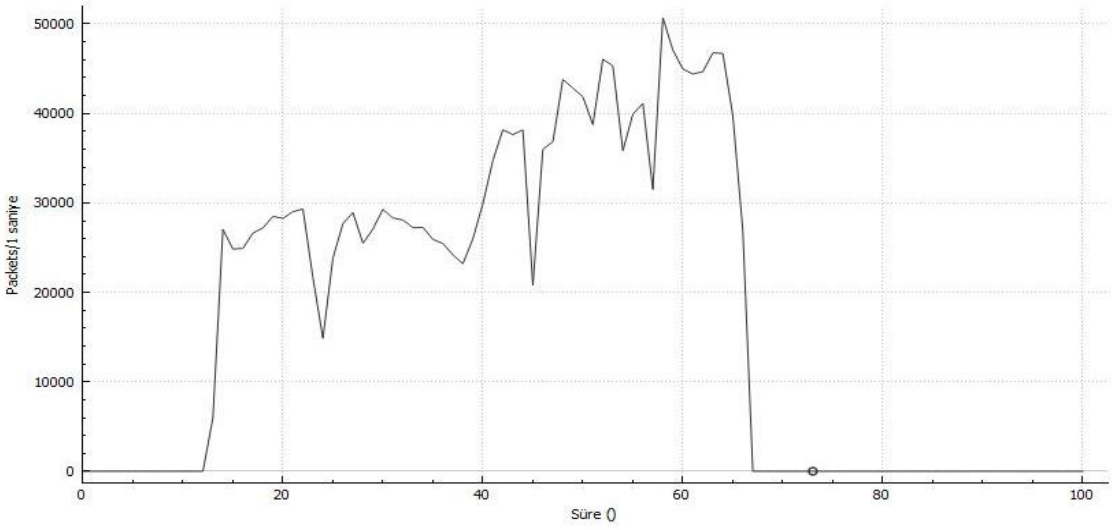
Saldırı analizinde, MitM saldırısı ile sistemler doğrulanmış ve bir tekrar saldırısı türü olan başlat-durdur saldırısı için gerekli olan yasal ağ paketleri toplanmıştır. Ortadaki adam saldırısı, saldırının gerçekleştirileceği sistemleri doğrulamak ve bir tekrar saldırısı türü olan başlat-durdur saldırısı için gerekli olan yasal ağ paketlerini toplamak amacıyla gerçekleştirilmiştir. Ortadaki adam saldırısı sırasında, PLC cihazlarına yönelik adres çözümleme protokolü (Address Resolution Protocol - ARP) zehirlenmesi gerçekleştirilerek Şekil 4.18.'de görülen önemli bilgiler elde edilmiştir. Bu bilgiler sayesinde, saldırı yapılan cihazların zafiyetleri ve bu zafiyetlerin sömürülmesine yönelik tehditler belirlenmiştir.



Şekil 4.18. MitM Saldırısı ile Yakalanan Veriler

Hizmet Reddi Saldırısı (DoS)

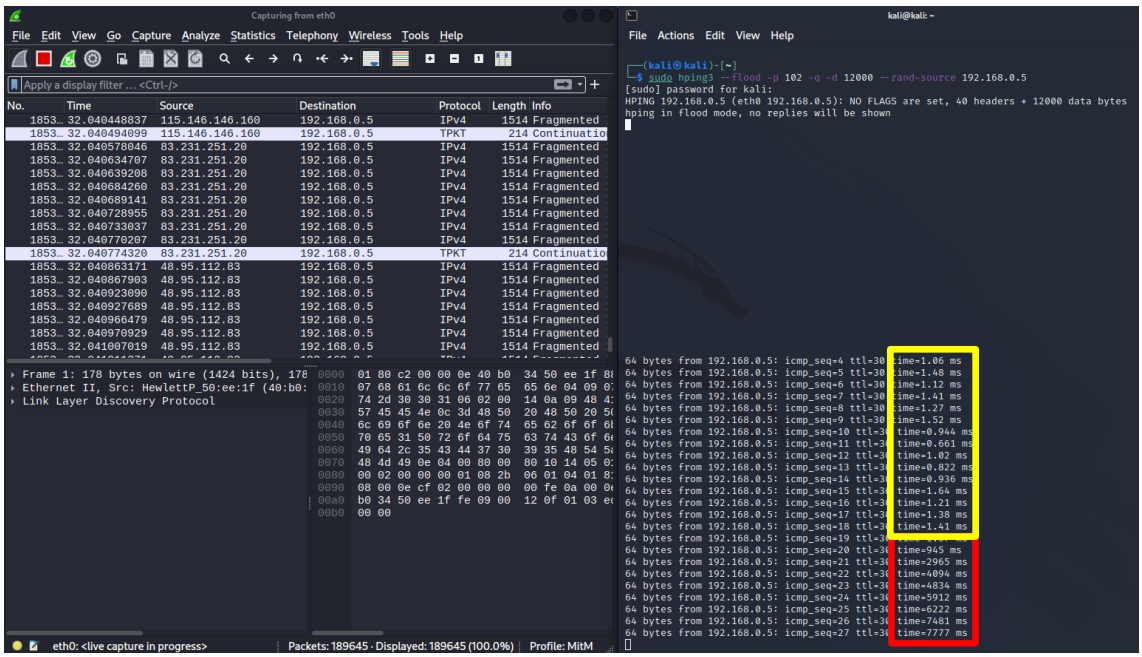
Saldırıların üçüncü aşamasında, akıllı fabrikalar, akıllı şehirler ve kritik altyapılar gibi alanlarda kullanılan S7-1200 PLC cihazına Dağıtık Hizmet Reddi (DDoS) saldırısı gerçekleştirilmiştir. DDoS saldırısı ağ, bilgisayar sistemlerinin bant genişliği, bellek ve disk alanı gibi donanım kaynaklarının kaldırabileceğinden daha fazla yük oluşturarak, sistemin yetkili kullanıcılar tarafından kullanılamaz hale getirmeyi amaçlamaktadır. Saldırının etkisini belirlemek için saldırı öncesi ve sonrasında paket erişim süreleri ve ağ paketi sayıları karşılaştırılmıştır. Hedef sistemin *"ping"* paketlerine cevap verme süresi saldırı öncesi 1ms (milisaniye) civarında iken, DDoS saldırısı sonrasında bu süre 100ms'nin üzerine çıkmıştır. Saldırıya yönelik toplanan paketlerin zaman içindeki dağılımları Şekil 4.19.'da görülmektedir. Bu saldırı, başlat-durdur saldırısına perdeleme saldırısı olarak hedef saldırının gizlenmesi amacıyla kullanılmıştır. Bu sayede, başlat-durdur saldırısının gerçekleştirilmesinden önce, ağ yöneticileri ve siber güvenlik personelinin dikkatinin dağıtılması sağlanmıştır.



Şekil 4.19. Dağıtık Hizmet Reddi Saldırısı Ağ Paket Sayıları

Sisteme yönelik gerçekleştirilen Dağıtık Hizmet Reddi saldırısı sırasında, açık kaynaklı paket çözümleyici Wireshark ile sistemde oluşan paketler analiz edilmek üzere kaydedilmiştir. Saldırı esnasında oluşan ve kaydedilen paketler, detaylı analiz edilmiştir. Wireshark ağ analizörü ve *"ping"* sürelerine ilişkin veriler Şekil 4.20.'de gösterilmiştir. Wireshark ağ analizöründe paketler incelendiğinde, DDoS saldırısı esnasında oldukça yüksek miktarda paketin tahsis edilmeyen ağ adreslerinden *(BOGON Network)* PLC cihazlarına yönlendirildiği görülmektedir. Bunun sonucunda tamamlanmayan ağ

paketleri PLC'lerin yasal kullanıcılar olan sistem yöneticilerine (özellikle HMI) cevap veremediği görülmüştür.



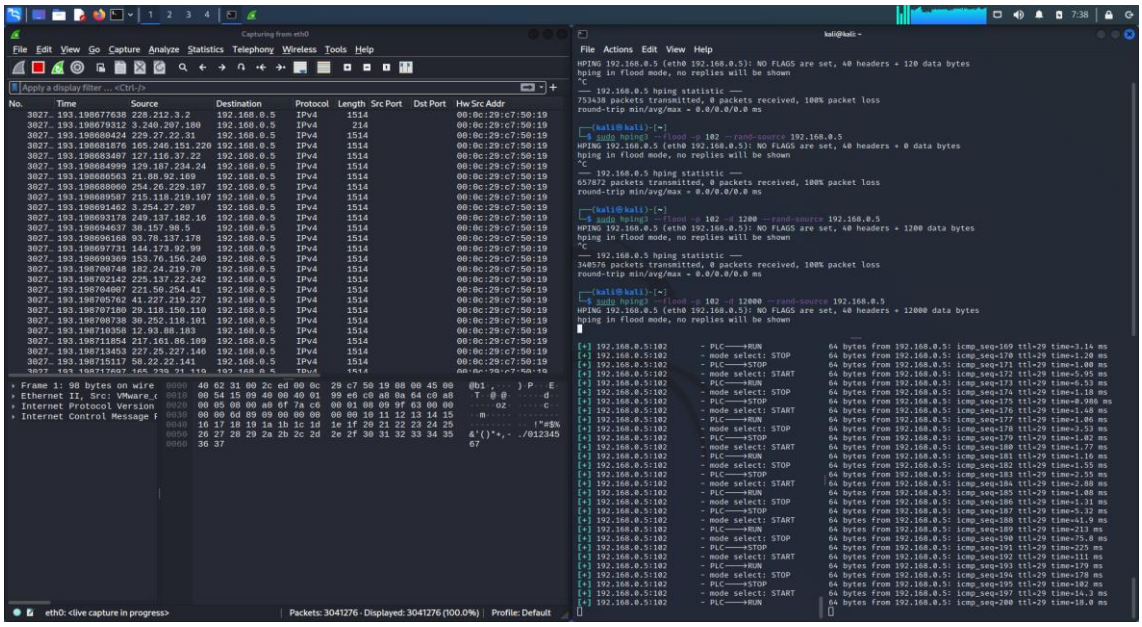
Şekil 4.20. Dağıtık Hizmet Reddi Saldırısı Sırasında Ağ Trafiği

Dağıtık Hizmet Reddi saldırısının sistem üzerindeki etkisi incelendiğinde, saldırının başarıyla gerçekleştirildiği gözlemlenmiştir. DDoS saldırısı başarıyla devam ettiği esnada çalışmanın hedef saldırısı olan başlat-durdur saldırısı da PLC cihazına aynı anda gerçekleştirilmiştir.

Başlat-Durdur Saldırısı

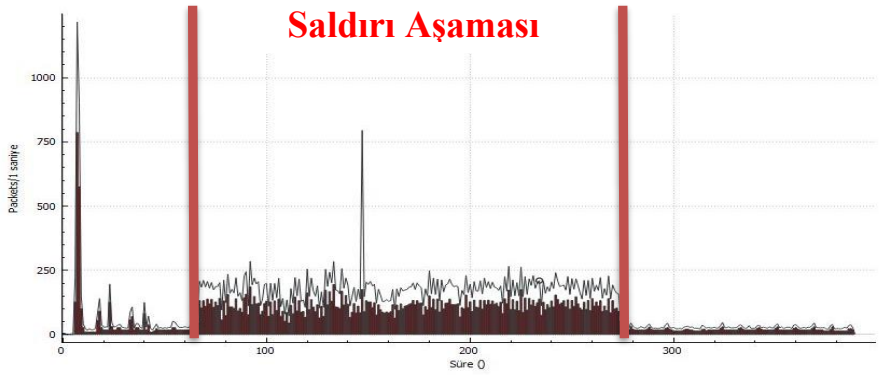
Başlat-Durdur saldırısı, tekrar saldırısı tipinde bir saldırı olarak gerçekleştirilmektedir. Bu saldırı ile saldırgan tarafından ortadaki adam saldırısı kullanılarak ağ üzerinden toplanan paketlerin analiz edilmesi sonucu tekrar edilmesi ile istenen işleve (PLC cihazlarının başlatılması ve durdurulması) yönelik paketlerin PLC cihazına yeniden istenilen sayıda gönderilmesiyle gerçekleştirilmektedir. Gerçekleştirilen saldırıda, PLC cihazına yasal olarak gönderilen başlat ve durdur komutları ağ üzerinden toplanarak, bu paketlerdeki koruma bitlerin yeniden düzenlenmesi ile saldırı gerçekleştirilmiştir. Saldırı sırasında HMI operatörü saldırının gerçekleştiğini fark etmesine rağmen müdahale edememiştir. Bunun nedeni saldırının istenilen miktarda (100 olarak belirlenmiştir) tekrar ile gerçekleştirilmiş olmasıdır. Bu sayede, belirlenen döngü tamamlanıncaya kadar HMI arayüzünden kontrol ele alınamamıştır. Şekil 4.21.'de görüldüğü üzere sağ taraftaki ekrandan PLC cihazına ilişkin IP adresine DDoS ve başlat-durdur saldırıları aynı anda

gerçekleştirilmiştir. Soldaki ekrandaki (Wireshark) ağ paketleri incelendiğinde ise DDoS paketlerinin çok fazla sayıda olması nedeniyle başlat-durdur saldırısına ilişkin paketler görülememektedir. Bu durum ağın sürekli olarak izlenmesi halinde bile perdeleme saldırısı olan DDoS saldırısı sayesinde PLC cihazının komut edildiği HMI arayüzü haricinde başlat-durdur saldırısının tespitinin zor olduğunu göstermektedir.

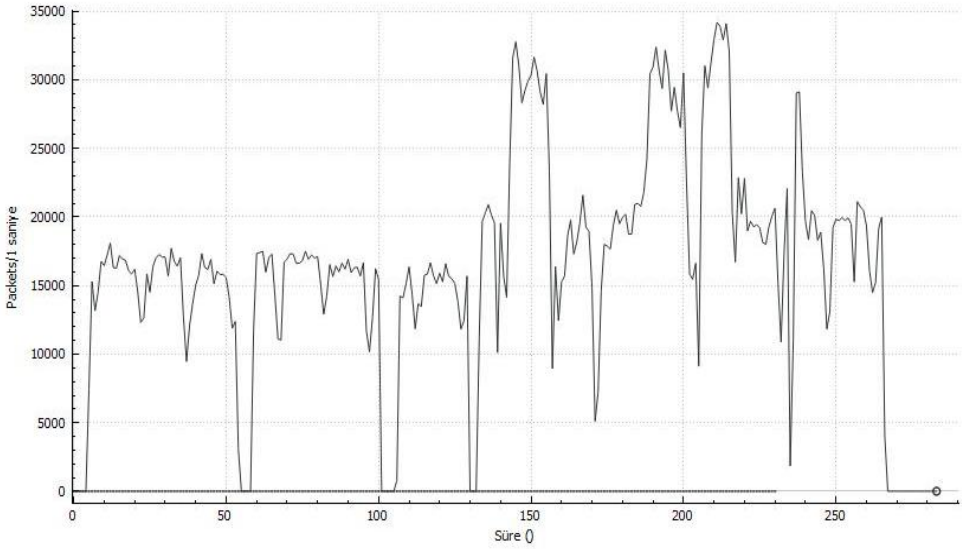


Şekil 4.21. Dağıtık Hizmet Reddi Saldırısı Sırasında Ağ Trafiği ile Başlat-Durdur Saldırısının Birlikte Gerçekleştirilmesi

Ayrıca, perdeleme saldırısının başlat-durdur saldırısına olan katkısını incelemek amacıyla DDoS saldırısı yapılmadan sadece başlat-durdur saldırısı da gerçekleştirilmiştir. Sadece başlat-durdur saldırısı gerçekleştirildiği durumda sisteme olan etkisi Şekil 4.22.'de görülürken, dağıtık hizmet reddi saldırısı perdesi altında başlat-durdur saldırısı gerçekleştirildiği duruma ilişkin sistem üzerindeki etkisi Şekil 4.23.'te gözlemlenmiştir.



Şekil 4.22. Başlat-Durdur Saldırısı



Şekil 4.23. DDoS Perdelemesinde Başlat-Durdur Saldırısı

Şekil 4.23. incelendiğinde, saldırı sırasında anlık olarak DDoS saldırısından kaynaklı saldırı paketlerinin gönderiminde kesintiler olduğu gözlemlenmiştir. Bu, sistemin DDoS saldırısı nedeniyle duraklamasından kaynaklanmaktadır. Ancak başlat-durdur saldırısı sırasında herhangi bir kesinti yaşanmamıştır.

5. UZMAN SİSTEM TEMELLİ SALDIRI TESPİT ÇALIŞMASI

Çalışmanın bu bölümünde, saldırı analizleri kapsamında gerçekleştirilen saldırıların uzman sistem aracılığıyla tespitine odaklanılmıştır. Bu kapsamda, Wireshark açık kaynak ağ trafiği analiz yazılımı ile bütün saldırılara ait ağ trafiği kayıt altına alınmıştır. Bu veriler, saldırının bulunmadığı referans ağ paketlerinin de yapay zeka tabanlı uzman sisteme eklenmesiyle saldırılara ait özelliklerin tespitinde oldukça faydalı olmuştur. Gerçekleştirilen analizler, yapay zeka tabanlı uzman sistemlerin IoT ve IIoT sistemlerine yönelik saldırı tespiti için kullanılabileceğini göstermektedir.

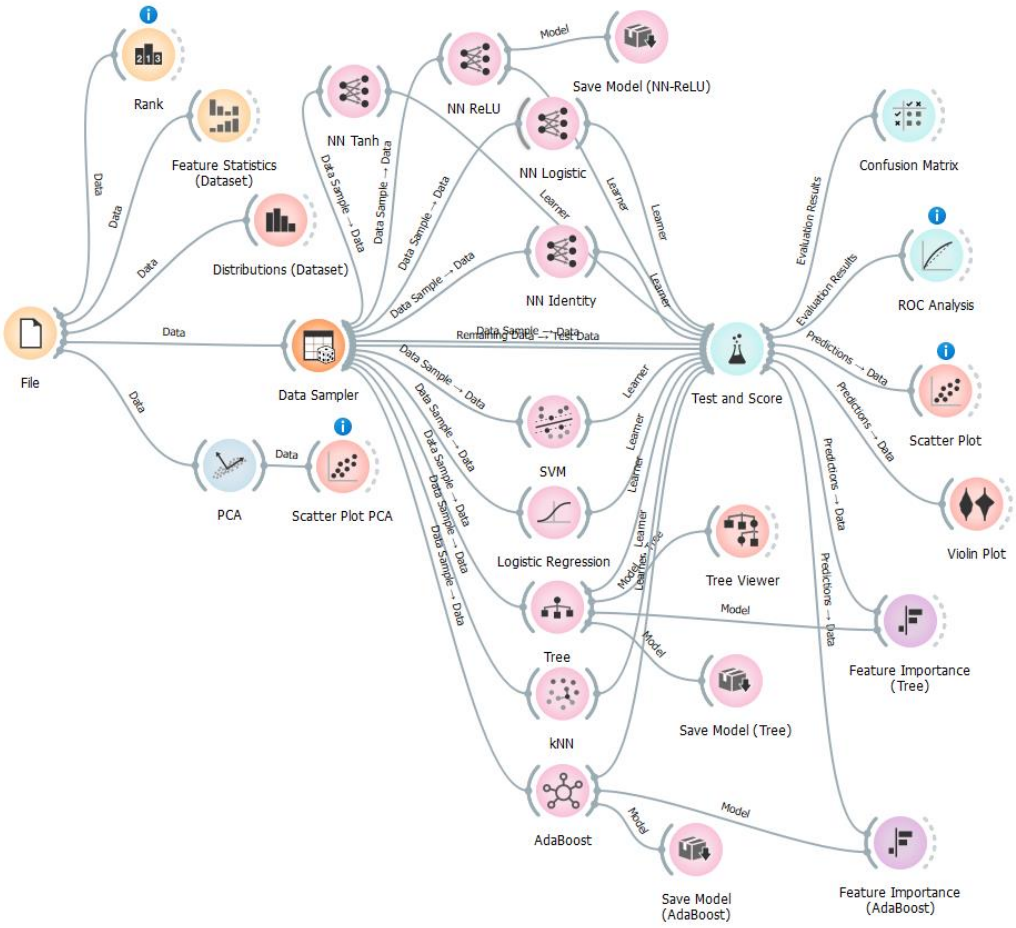
Yapay zeka teknolojisi, saldırıları tespit etmek için çok daha hızlı ve doğru bir şekilde çalışmakta ve bu nedenle siber güvenlik alanında önemli bir rol oynamaktadır. Çalışmada bütüncül bir siber güvenlik yaklaşımıyla hareket edildiğinden, yapay zeka tarafından belirlenen saldırı tespit modelleri kural tabanlı uzman sisteme aktarılarak, sürekli izleme ile birlikte kullanılmıştır. Saldırı tespiti analizlerinin müteakip kısımlarında öncelikle IIoT'ye yönelik saldırı tespitleri, sonrasında ise IoT'ye yönelik saldırı tespitleri ele alınmıştır.

5.1. IIoT 'ye Yönelik Saldırıların Yapay Zeka Tabanlı Uzman Sistem Aracılığıyla Tespiti

Bu kısımda, IIoT'ye yönelik gerçekleştirilen DDoS, MitM ve Başlat-Durdur saldırılarının uzman sistem aracılığıyla tespiti ele alınmıştır. Bu amaçla öncelikle perdeleme saldırısı olarak gerçekleştirilen DDoS ile aynı zamanda gerçekleştirilen Başlat-Durdur saldırılarına ilişkin aynalama tekniği ile toplanan veriler çeşitli yapay zeka modellerine aktarılmıştır.

Şekil 5.1. incelendiğinde, 3 ayrı katman yapısı belirlenmiş ve saldırı analizleri bu yapıya göre incelenmiştir. Toplanan veriler üzerinde öncelikle veri temizleme işlemi gerçekleştirilmiş, daha sonra uygulamaya yüklenerek öncelikle veri dağılımı ve saldırı olup olmadığı, saldırı ise paketin hangi tür saldırı olduğuna yönelik özelliklerin belirlenmesi ve son olarak da veri örneklerinin alınması uzman sistemin ilk aşamasını oluşturmuştur. İkinci aşamada, yüklenen veri karşılaştırma yapılabilmesi maksadıyla çeşitli yapay zeka modellerine aktarılmıştır. Yapılan inceleme sonucunda PCA algoritmasının çok hızlı sonuç verdiği gözlemlenmiş ancak algoritmanın sadece DDoS saldırılarını doğru bir şekilde tespit edebildiği gözlemlenmiştir. Aynı veri %70'i eğitim, %30'u ise doğrulama veri seti olacak yapıda bölümlendirilerek Şekil 5.1.'de görülen

çeşitli geleneksel ve makine öğrenmesi modellerine girdi olarak verilmiştir. Yapay zeka tabanlı uzman sistem bu işlemi 10-*fold* olarak gerçekleştirdikten sonra, Şekil 5.2.'de yer alan karşılaştırma tablosu elde edilmiştir. Üçüncü aşamada ise çeşitli araçlar üzerinden analiz sonuçları kullanıcılara yönelik olarak görselleştirilmiştir. Son aşamada ise belirlenen modele ait veri yapısı kural haline getirilerek kural tabanlı uzman sisteme aktarılmıştır.



Şekil 5.1. Yapay Zeka Saldırı Tespit Sistemi Model Araştırması İlke Şeması

Uzman sistem modelinde, geleneksel yapay zeka algoritmaları ve makine öğrenmesi algoritmaları çeşitli açılardan karşılaştırılmıştır. Temel bileşen analizi (PCA) yöntemi kullanılarak veriseti incelenmiş, modelin DDoS saldırılarını başarılı bir şekilde tespit ettiği ancak, diğer saldırı türlerini DDoS saldırısı gibi tespit edemediği gözlemlenmiştir. Ayrıca, Tablo 5.1.'de yer alan sonuçlar, farklı algoritmaların doğruluğu *(Classification Accuracy-CA)*, hassasiyeti *(precision)*, özyineleme *(recall)* ve F1 değeri gibi önemli değerler açısından mukayese edilmiştir. Uzman sistemlerde genellikle mukayese edilen

söz konusu dört değer ile birlikte, çalışmanın odak noktası olan siber saldırıların en kısa sürede tespiti değerlendirildiğinde veri setinin eğitilme zamanı (*train time*) ve özellikle saldırı veya saldırı değil sonucuna ulaşılma süresi (*cevap zamanı-response time*) algoritmalarının başarısında dikkate alınan diğer parametreler olarak belirlenmiştir. Karşılaştırılan sonuçlar içerisinde her ne kadar makine öğrenmesi modeli (Neural Network) %99,3 ile en yüksek doğruluk değerine sahip olsa da sistemin IoT ve IIoT gibi gerçek zamanlı sistemlerde kullanılacağı, doğruluk, hassasiyet, F1 değeri, özyineleme gibi değerlerdeki farkın çok az oluşu göz önüne alındığında, hızı ve kullanım kolaylığı sağlaması sebebiyle Tree modeli uzman sistem olarak seçilmiştir.

Model	**Cevap Zamanı (s)**	**Doğruluk**	**F1**	**Hassasiyet**	**Özyineleme**
Tree	0.011	0.952	0.951	0.951	0.952
AdaBoost	0.155	0.987	0.987	0.987	0.987
Logistic Regression	0.171	0.773	0.739	0.761	0.773
NN Tanh	0.280	0.993	0.993	0.993	0.993
NN Logistic	0.316	0.954	0.940	0.926	0.954
NN ReLU	0.322	0.993	0.993	0.993	0.993
NN Identity	0.483	0.993	0.993	0.993	0.993
SVM	5.118	0.804	0.799	0.797	0.804
kNN	9.157	0.797	0.783	0.787	0.797

Tablo 5.1. DDoS Perdelemesinde Başlat-Durdur Saldırısı için Yapay Zeka Modelleri Performans Ölçütleri

Bu tabloda, uzman sistem modelinde saldırı tespiti ve önleme konusunda hız, doğruluk ve hassasiyet sağlanmış olacaktır. Önerilen uzman sistem modeli gelecekte çıkacak

saldırıların tespitinde, benzer sistemlerin tasarımında ve uygulanmasında kullanılarak, daha etkili çözümlerin geliştirilmesine katkı sağlayabilecektir.

5.1.1. Veri Özniteliklerinin Belirlenmesi

Veri temizleme işlemini yapıldıktan sonra yapay zeka tabanlı uzman sistem modelinin belirlenebilmesi için modellerde kullanılacak özniteliklerin tespit edilmiştir. Öznitelikler belirlenirken uygulama üzerinde temizlenmiş çeşitli öznitelik çıkartma yöntemleri kullanılarak analiz edilmiştir. Öznitelik çıkartma işleminde veri seti içerisindeki kolonlar çeşitli istatistiki modeller kullanılarak incelenmiştir. İnceleme sonucu Şekil 5.2.'de görülmektedir.

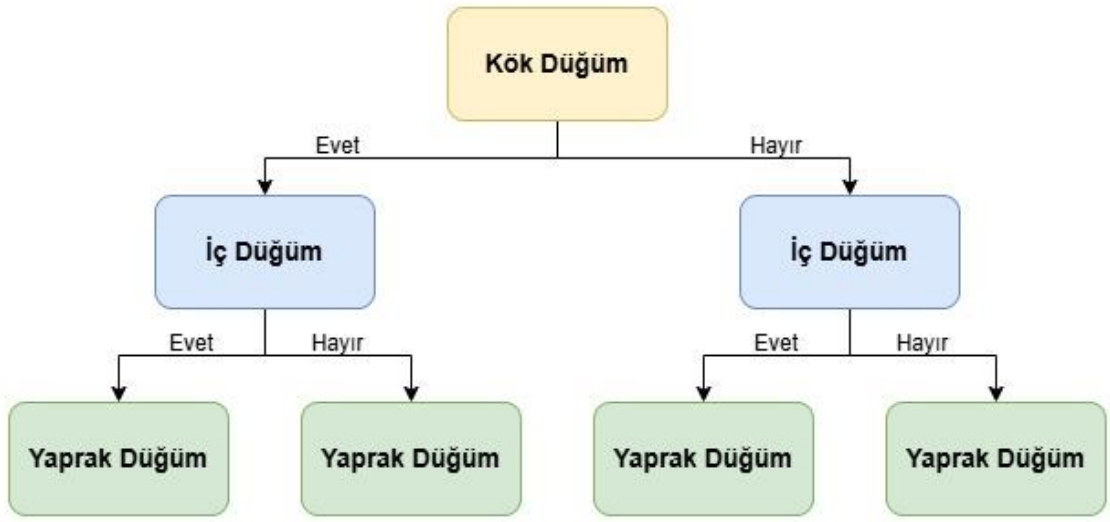
		#	Info. gain	Gain ratio	Gini	ReliefF	FCBF
1	C Protocol	2	0.332	0.522	0.165	0.017	0.666
2	N TTL		0.272	0.269	0.117	0.123	0.000
3	N Delta time		0.102	0.051	0.051	0.011	0.072
4	N RTT		0.202	0.228	0.050	0.091	0.273
5	N Seq num		0.078	0.039	0.027	0.030	0.000
6	N Frame len		0.062	0.031	0.020	0.026	0.000
7	N TCP len		0.033	0.020	0.008	0.026	0.000
8	N IP len		0.033	0.020	0.008	0.026	0.000
9	N Time		0.011	0.006	0.001	0.033	0.000
10	C Cotp type	3	0.000	0.019	0.000	-0.000	0.000
11	N Cotp len		0.000	0.021	0.000	0.230	0.001
12	C Cotp class	1	0.000	0.000	0.000	-0.000	NA
13	C Cotp param code	2	0.000	0.000	0.000	-0.000	NA
14	C Cotp param len	2	0.000	0.000	0.000	-0.000	NA
15	N Cotp tpdu size		0.000	0.000	0.000	0.000	NA
16	C Cotp src tsap	1	0.000	0.000	0.000	-0.000	NA
17	C Cotp dst tsap	1	0.000	0.000	0.000	-0.000	NA
18	N Cotp src tsap byte		0.000	0.000	0.000	0.000	NA
19	C Cotp dst tsap byte	1	0.000	0.000	0.000	-0.000	NA
20	C Ethertype	1	0.000	0.000	0.000	0.000	0.000

Şekil 5.2. Öznitelik Analizi

Şekil 5.2. incelendiğinde MitM saldırılarının tespitinde normal şartlarda kullanılan kaynağa ait donanım adresi, Başlat-Durdur saldırısının tespitinde kullanılan protokol tipi, ayrıca DDoS saldırısında kullanılan TTL verisi gibi kolonların farklı öznitelik tespit algoritmalarında öncelikli olarak belirlendiği görülmektedir.

5.1.2. Karar Ağacı Öğrenme Modeli

Karar ağacı öğrenme modeli, makine öğrenmesi ve veri madenciliği alanında yaygın olarak kullanılan gözetimli bir makine öğrenmesi modeli olup hem sınıflandırma hem de regresyon problemlerinde kullanılabilmektedir. Bu model, veri setindeki bağımlı ve bağımsız değişkenler arasındaki ilişkileri belirlemek amacıyla hiyerarşik bir yapı kullanmaktadır. Karar ağacı, kök düğüm, iç düğümler ve yaprak düğümlerinden oluşmaktadır. Kök düğüm, karar ağacının başladığı nokta olup, tüm veri setini içermektedir. İç düğümler, veri setinin belirli bir özelliğe göre bölündüğü noktaları temsil ederken, yaprak düğümler ise nihai kararları veya sınıflandırmaları içermektedir. Karar ağacı modeline ait genel betimleme Şekil 5.3.'te görülmektedir.



Şekil 5.3. Karar Ağacı Modeli

Karar ağacı, veriyi belirli özelliklere göre bölerek, her bölünmede bilgi kazancını maksimize etmek temel prensibi ile çalışmaktadır. Bilgi kazancı, genellikle "Gini katsayısı", "bilgi kazancı" veya "varyans azalması" gibi metriklerle ölçülmektedir. Gini katsayısı ve bilgi kazancı, özellikle sınıflandırma problemlerinde kullanılırken, varyans azalması regresyon problemleri için kullanılmaktadır.

Karar ağacı oluşturulurken ilk olarak, veri seti en iyi şekilde nasıl bölünebileceğine karar vermek için bir ölçüt (örneğin, Gini safsızlığı veya bilgi kazancı) belirlenmektedir. Bu

ölçüt, veri setindeki heterojenliği veya bilgi kazancını maksimuma çıkaracak şekilde bölünmeleri belirlemektedir. Her bölünme, veri setini alt kümelere ayırmakta ve bu süreç, belirli bir durma kriterine (örneğin, maksimum ağaç derinliği veya minimum yaprak düğüm boyutu) ulaşılana kadar tekrarlanmaktadır.

Sınıflandırma problemlerinde, yaprak düğümler genellikle veri noktalarının sınıflarını gösterirken, regresyon problemlerinde yaprak düğümler genellikle sürekli değerleri göstermektedir. Karar ağaçlarının en büyük avantajlarından biri, sonuçlarının kolayca yorumlanabilir olması ve diğer modellere göre yapısı gereği çok daha hızlı çalışmasıdır [75]. Ağaç yapısı, kararların hangi özelliklere dayanarak alındığını açıkça göstermekte ve bu da modelin şeffaflığını ve hızını artırmaktadır.

Bununla birlikte, karar ağaçlarının bazı dezavantajları da bulunmaktadır. Özellikle, veri setinin düzgün dağılmadığı durumlarda aşırı öğrenme (overfitting) gerçekleşebilmektedir. Bu sorunu hafifletmek için budama teknikleri (pruning) kullanılmaktadır, bu da gereksiz dalları keserek ağacın basitleştirilmesini ve sistemin daha sağlıklı ve hızlı çalışmasını sağlamaktadır.

Gini Katsayısı

Gini katsayısı, karar ağaçları ve diğer makine öğrenme algoritmalarında yaygın olarak kullanılan bir ölçüm olup, veri kümesinin saflığını veya karışıklığını değerlendirmek için kullanılmaktadır. Özellikle sınıflandırma problemlerinde kullanılmakta ve bir düğümdeki örneklerin homojenliğini belirlemek amacıyla hesaplanmaktadır.

Gini katsayısının hesaplanması aşağıda belirtilmiştir:

$$\text{Gini} = 1 - \sum_{i=1}^{n} p_i^2$$

Burada:

- p_i : "i" sınıfın olasılığıdır ("i" sınıfın örneklerinin toplam örnekler içindeki oranını göstermektedir).
- n : Sınıf sayısını göstermektedir.

Gini katsayısı 0 ile 0.5 arasında değer almaktadır. Gini katsayısının düşük olması, düğümdeki örneklerin homojen olduğunu, yani aynı sınıfa ait olduklarını göstermektedir. Gini katsayısının 0 olması ise tüm örneklerin tek bir sınıfa ait olduğu anlamına gelmekte ve bu durum tamamen saf bir düğümü göstermektedir. Gini katsayısının 0.5 olması ise

düğümdeki örneklerin iki sınıf arasında eşit olarak dağıldığını ve maksimum karışıklığı sağladığını göstermektedir.

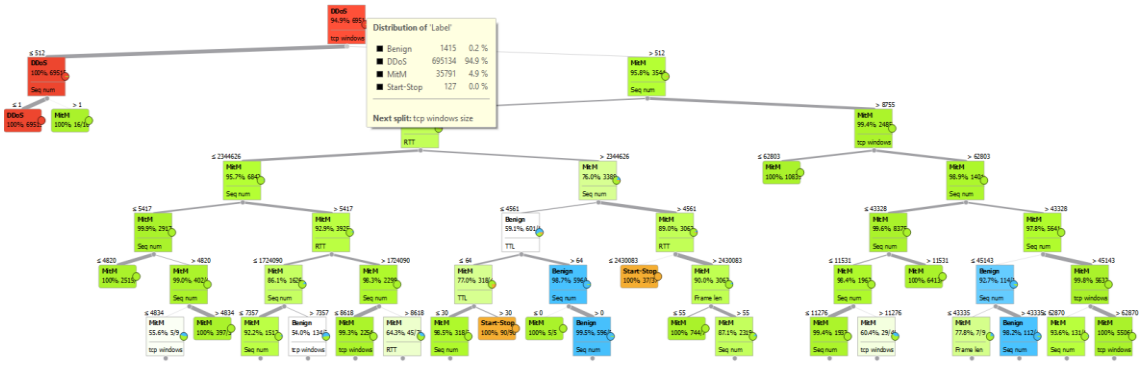
Bir karar ağacında, her bölünme için Gini katsayısı hesaplanmakta ve toplam Gini katsayısındaki azalma (veya bilgi kazancı) en yüksek olan bölünme seçilmektedir. Bu da ağacın her adımında veri setini olabildiğince saf alt kümelere ayırmayı amaçlamaktadır.

Karar ağacı öğrenme modeli hem teorik hem de pratik açıdan güçlü ve esnek bir algoritmadır. Ancak, modelin performansını ve genelleme yeteneğini artırmak için dikkatli bir şekilde yapılandırılması ve gerektiğinde budama teknikleri gibi yöntemlerle optimize edilmesi gerekmektedir.

Çalışmanın 5.2. ve 5.3. bölümlerinde, karar ağacı öğrenme modeline ait sonuçlar detaylı bir şekilde açıklanmıştır. Karar ağacı makine öğrenmesi modeli kullanılarak veriler işlenmiş ve karar ağacı modeli kaydedilerek çıkan sonuçlar kural haline dönüştürülmüştür. Bu sayede, uzman sistem modeli ile veri analizi gerçekleştirilmiştir.

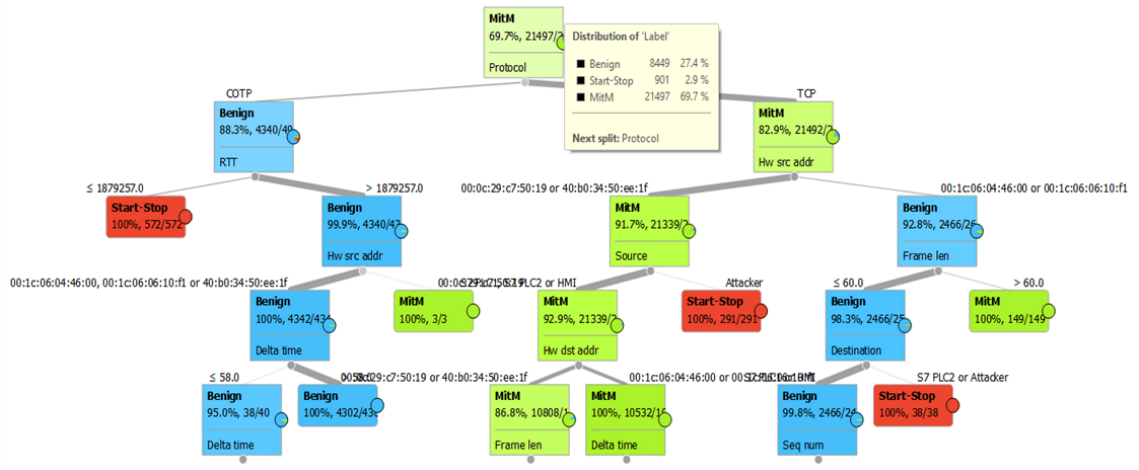
5.2. Modelin Oluşturulması ve Eğitilmesi

Çalışmanın aktif saldırılardan birisi olan başlat-durdur saldırısının tespiti, uzman sistem karar ağacı modeli kullanılarak gerçekleştirilmiş ve DDoS saldırısı perdelemesi sırasında gerçekleştirilen başlat-durdur paketlerinin tespit edilmesi için çalışılmıştır. Veriler gerçek sistemler kullanılarak toplanmış ve beyaz liste *(white list)* veri setine dönüştürülmüştür. Oluşturulan veri seti eğitim için %70, doğrulama için %30 olarak ayrılmıştır. Modeller çalıştırıldıktan sonra cevap zamanı *(Response Time)* en hızlı model olan "Karar Ağacı" uzman sistem olarak belirlenmiştir. Uzman sistem modeline ait ağaç yapısı Şekil 5.4. ve Şekil 5.5.'de, karmaşıklık matrisi *(Confusion Matrix)* ise Şekil 5.6.'da gösterilmiştir.



Şekil 5.4. DDoS Gizlemesinde Başlat-Durdur Saldırısı Karar Ağacı Modeli

Şekil 5.4.'te saldırılarının tespiti için kullanılan karar ağacı modelinde, MAC adresi (*hardware address*) bulunan bir dalların yer almasının en önemli sebebi, bu tür saldırıların belirlenmesinde MAC adreslerinin kritik bir rol oynamasıdır. MitM saldırılarında saldırgan, ağ trafiğini kendi üzerinden yönlendirerek iki taraf arasındaki iletişimi dinlemekte veya değiştirmektedir. Bu işlem genellikle ARP zehirlenmesi (*ARP Poisoning*) yöntemi ile gerçekleştirilmektedir. Karar ağacı modeli, ağdaki anormal MAC adresi davranışlarını izleyerek bu tür sahtecilikleri tespit etmektedir. Örneğin, aynı MAC adresinin birden fazla IP adresiyle ilişkilendirilmesi veya bir cihazın MAC adresinin aniden değişmesi gibi durumlar, olası bir MitM saldırısının göstergesi olabilmektedir. Bu nedenle, karar ağacı modelinde MAC adresi içeren dallar, ağ güvenliğini sağlamak için hayati öneme sahiptir ve saldırı tespiti süreçlerinin etkinliğini artırmaktadır. Ayrıca, MAC adresleri üzerinden yapılan analizler, saldırganın kimliğinin belirlenmesine ve saldırının kaynağının tespit edilmesine yardımcı olmakta, bu da saldırıya karşı alınacak önlemlerin hızla uygulanmasını sağlamaktadır. Kural tabanlı sistemlerde MitM saldırılarının tespiti ile yanlış-pozitif (*false-positive*) oranlarının düşürülmesi ve sistem kaynaklarının etkin kullanılabilmesi maksadıyla ARP zehirlenmesi yapılabilecek kritik sistemlerin (*Sunucu, Yönlendirme Cihazı-Router, Anahtarlama Cihazı-Switch gibi*) MAC adreslerinin tanımlanması önem taşımaktadır. Ancak, yapılan çalışmada önerilen uzman sistemin performansının da genelleştirilebilmesi için uzman sistem modelinde kuralların oluşturulması aşamasında Şekil 5.5.'te gösterilen MAC, IP ve port numaralarının temizlendiği karar ağacı modeli kullanılmıştır.



Şekil 5.5. IIoT için Genelleştirilmiş Karar Ağacı Modeli

Şekil 5.6.'da yer alan matris incelendiğinde, Başlat-Durdur saldırısına ait tüm paketlerin doğru bir şekilde tespit edilebildiği, diğer bir ifadeyle yanlış-pozitif (*false-positive*) değerinin bulunmadığı görülmüştür.

Yapay zeka tabanlı uzman sistem tarafından aşağıdaki bilgiler değerlendirilmiştir:

- Gerçekten saldırı paketi olarak tanımlanan paketler.

- Saldırı paketi olarak yanlış sınıflandırılan yasal ağ paketleri (saldırı olmayan).

- Saldırı paketi olmadığı halde saldırı paketi olarak yanlış sınıflandırılan paketler.

- MitM saldırı paketleri olarak yanlış sınıflandırılan başlat-durdur saldırı paketleri.

- MitM saldırı paketlerinin başlat-durdur saldırı paketleri olarak yanlış sınıflandırılanlar.

Karmaşıklık matrisi, uzman sistemin başarısını değerlendirmek için çok önemlidir, çünkü gerçekten saldırı paketi olan ve sistem tarafından doğru şekilde tanımlanan paketlere odaklanmamızı sağlamaktadır. Dolayısıyla, sistemin bildirdiği başarı oranındaki hata seviyesi bu matris üzerinden görülmektedir. Bu kapsamda karmaşıklık matrisi değerlendirildiğinde, Şekil 5.6.'daki gerçek saldırı paketlerine kıyasla yanlış-pozitif ve yanlış-negatif (*false-negative*) sayısının oldukça düşük olduğu görülmektedir.

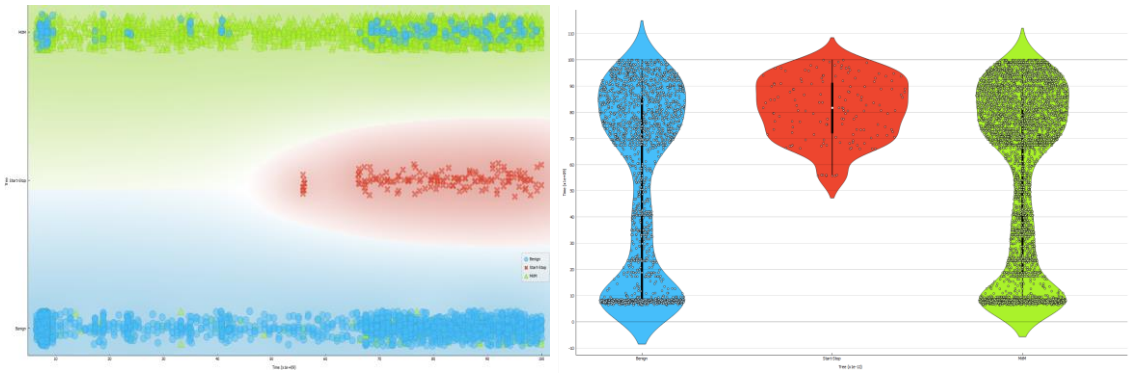
Karışıklık matrisinde karar ağacı modeli 941 paketi aslında normal ağ paketi (Benign) olmasına rağmen MitM saldırı paketi olarak, 550 paketi ise MitM saldırı paketi olmasına rağmen normal ağ paketi olarak etiketlemiştir.

		Predicted			
		Benign	**Start-Stop**	**MitM**	**∑**
Actual	**Benign**	7508	0	941	**8449**
	Start-Stop	2	898	1	**901**
	MitM	550	0	20947	**21497**
	∑	**8060**	**898**	**21889**	**30847**

Şekil 5.6. Karmaşıklık Matrisi (Confusion Matrix)

Karar ağacı modelinin zaman-başarı grafiği Şekil 5.7.'de görülmekte olup, sonuçlar incelendiğinde yasal paketlerin MitM saldırıları ile ele geçirildiği ve daha sonra PLC cihazlarına başlat-durdur saldırıları yapıldığı ve modelin bunları yüksek başarı oranı ile

tahmin edebildiği görülmektedir. Şekil 5.7.'de sol taraftaki görüntü incelendiğinde yasal olarak gönderilen paketlerin (HMI, PLC'ler tarafından gönderilen ve alınan) oluşturduğu trafik ve saldırgan tarafından üretilen trafik ile ilgili saldırlar görülmektedir. Sağ taraftaki görüntüde ise mavi renkli yasal ağ paketleri, kırmızı renkli başlat-durdur saldırı paketleri ve saldırgan tarafından başlatılan ortadaki adam saldırısına ilişkin yeşil renkli saldırı paketleri uzman sistem tarafından zaman çizelgesi üzerinde gösterilmektedir. Ayrıca, bu paketlere ilişkin kaynak IP adresi, port numarası, paket boyutu vb. detaylı bilgiler görülebilmektedir. Sonuç olarak, ağın ağ/sistem uzmanları veya siber güvenlik uzmanları tarafından sürekli olarak izlenmesi ve uzman sistemden yararlanılması, saldırıların erken tespit edilmesini ve önleyici tedbirlerin uygulanmasını sağlamaktadır.



Şekil 5.7. Karar Ağacı Modeli Sonuçları

Uzman sistemin performansını değerlendirmek için, karmaşıklık matrisine dayalı olarak doğruluk, doğru pozitif oranı (TPR), yanlış pozitif oranı (FPR) ve F1 değeri gibi çeşitli ölçütler ile birlikte cevap zamanı değerlendirilmiştir.

5.2.1. Ortadaki Adam Saldırısı (MitM)

İkinci aşamada gerçekleştirilen ortadaki adam saldırısının tespiti, endüstriyel kontrol sistemleri ile IoT ve IIoT cihazlarının güvenliği için oldukça önemlidir.

Saldırıların tespit edilmesi için örnek uzman sistem kullanılmıştır. Bu sistemler, saldırıya özgü özellikleri belirleyerek, saldırıyı tespit edebilmektedirler. Başlat-Durdur saldırısının tespiti için yapay zeka tabanlı bir uzman sistem kullanılmıştır. Bu sistem, PLC'lere yönelik tekrarlı açma-kapama işlemlerini algılayarak, saldırıyı tespit etmiştir.

Ortadaki adam ve hizmet reddi saldırılarının tespiti için de uzman sistemler kullanılmıştır. Bu sistemler, ağ trafiği analizi yaparak, saldırıya özgü özellikleri belirlemekte ve saldırıyı tespit etmektedir. Bu sayede, saldırıların tespiti ve önlenmesi mümkün hale gelmektedir.

Önerilen uzman sistem modelinin, özellikle gizleme saldırısı yapılan bir ağda gerçek HMI paket yapısına çok benzer ağ paketi kullanarak başlat-durdur saldırısını yüksek doğrulukla ve çok hızlı olarak tespit etmesi odak noktasıdır.

Uzman sistem sayesinde, saldırı istenilen eşik değerinin üzerinde başarı oranı ile tespit edilebilmiştir. Bu sayede, endüstriyel kontrol sistemleri (EKS) ve IIoT cihazlarına yapılan başlat-durdur saldırıları gibi tehditlerin tespiti için etkili bir mekanizma sağlanmıştır.

Ortadaki adam saldırısı kapsamında elde edilen saldırı paketleri, sisteme benzer saldırının yapılması durumunda tespit edilmesi için uzman sisteme aktarılmıştır. Uzman sistemin saldırıları tespiti için çalıştırılmasından sonra, Tablo 5.2.'de yer alan performans ölçütleri elde edilmiştir. Tablo 5.2.'de yer alan sonuçlar, farklı algoritmaların doğruluğu, hassasiyeti *(precision),* özyinelemeli hassasiyet *(recall)* ve F1 değeri ve cevap zamanı gibi önemli değerler açısından mukayese edilmiştir. Karşılaştırılan sonuçlar içerisinde %85,2 doğruluk ve 0,032s ile en yüksek cevap zamanı değerine sahip olan karar ağacı algoritması, F1 değeri, hassasiyet ve özyinelemeli hassasiyet gibi diğer önemli değerler de göz önünde bulundurularak ortadaki adam saldırısının tespitinde uzman sistem olarak seçilmiştir.

Model	**Cevap Zamanı (s)**	**Doğruluk**	**F1**	**Hassasiyet**	**Özyineleme**
Tree	0.032	0.852	0.853	0.864	0.852
AdaBoost	3.476	0.918	0.918	0.919	0.918
Logistic Regression	0.091	0.603	0.552	0.595	0.603
NN Tanh	0.403	0.912	0.912	0.912	0.912
NN Logistic	0.425	0.873	0.873	0.873	0.873
NN ReLU	0.333	0.906	0.906	0.906	0.906
NN Identity	0.528	0.658	0.636	0.659	0.658
SVM	15.381	0.412	0.363	0.440	0.412

kNN	261.386	0.912	0.913	0.913	0.912

Tablo 5.2. MitM Saldırısı için Yapay Zeka Modelleri Performans Ölçütleri

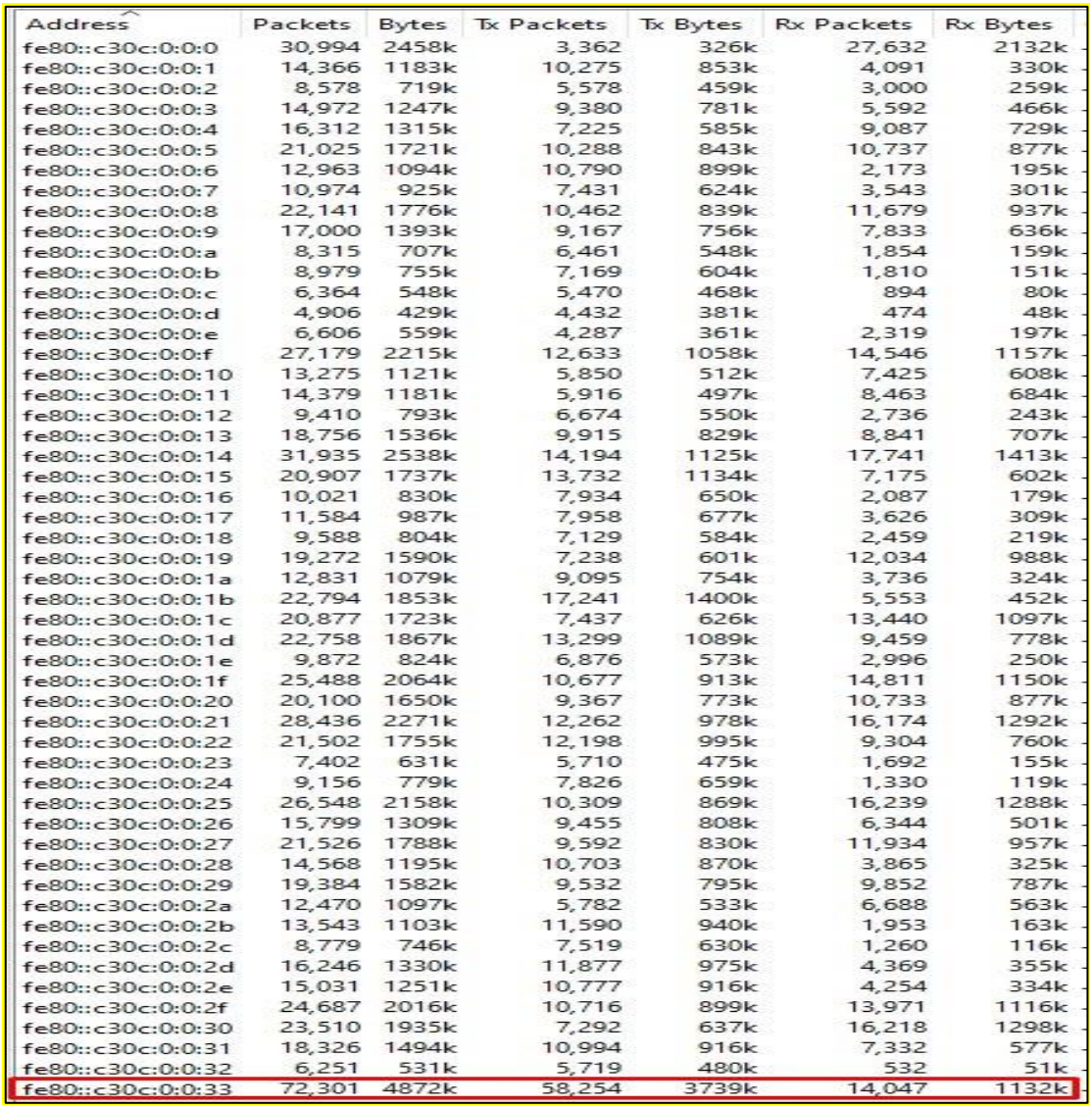
Tablo 5.2.'de, önerilen uzman sistemin sadece ortadaki adam saldırısının tespiti için kullanıldığı zaman karar ağacı modelinin bütün çalışılan saldırı senaryolarının (*DDoS, Başlat-Durdur, MitM*) bulunduğu duruma göre daha yavaş ve daha düşük doğrulukla tespit edebildiği görülmüştür.

5.3. IoT 'ye Yönelik Saldırıların Yapay Zeka Modelleri Aracılığıyla Tespiti

5.3.1. Sel (Flood) Saldırısı

Analiz senaryoları kapsamında gerçekleştirilen mevcut saldırılardan IoT sistemlerinin etkilenmesini önlemek veya saldırıyı en az zararla ortadan kaldırmak için saldırıların tespiti mümkün olan en kısa sürede yapılmalıdır. Bu kapsamda, ağ saldırılarını tespit etmek amacıyla makine öğrenmesi kullanılması önerilmiştir.

Bu analiz yöntemiyle, saldırgan düğümün bulunmadığı bir ağ üzerindeki trafik, referans veri kümesi olarak kaydedilen *"pcap"* dosyası aracılığıyla incelenmiştir. Makine öğrenmesi algoritmaları hedef sistemin normal trafiğini, saldırganın müdahalesi olmadan öğrenmektedir. Saldırgan, ağ trafiğini sürekli olarak manipüle etmek için düzenli aralıklarla merhaba *(hello)* paketleri göndermektedir. Ağdaki cihazlar tarafından gönderilen paketlerin belirli bir süre boyunca izlenip kaydedilmesi sonucunda, hangi cihazın saldırgan olduğu tespit edilebilmiştir. Bu duruma ilişkin olarak, saldırgan düğümün ve diğer düğümlerin ağ trafiğinde gönderdiği paket ve veri bilgileri Şekil 5.8.'de gösterilmiştir.



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
fe80::c30c:0:0:0	30,994	2458k	3,362	326k	27,632	2132k
fe80::c30c:0:0:1	14,366	1183k	10,275	853k	4,091	330k
fe80::c30c:0:0:2	8,578	719k	5,578	459k	3,000	259k
fe80::c30c:0:0:3	14,972	1247k	9,380	781k	5,592	466k
fe80::c30c:0:0:4	16,312	1315k	7,225	585k	9,087	729k
fe80::c30c:0:0:5	21,025	1721k	10,288	843k	10,737	877k
fe80::c30c:0:0:6	12,963	1094k	10,790	899k	2,173	195k
fe80::c30c:0:0:7	10,974	925k	7,431	624k	3,543	301k
fe80::c30c:0:0:8	22,141	1776k	10,462	839k	11,679	937k
fe80::c30c:0:0:9	17,000	1393k	9,167	756k	7,833	636k
fe80::c30c:0:0:a	8,315	707k	6,461	548k	1,854	159k
fe80::c30c:0:0:b	8,979	755k	7,169	604k	1,810	151k
fe80::c30c:0:0:c	6,364	548k	5,470	468k	894	80k
fe80::c30c:0:0:d	4,906	429k	4,432	381k	474	48k
fe80::c30c:0:0:e	6,606	559k	4,287	361k	2,319	197k
fe80::c30c:0:0:f	27,179	2215k	12,633	1058k	14,546	1157k
fe80::c30c:0:0:10	13,275	1121k	5,850	512k	7,425	608k
fe80::c30c:0:0:11	14,379	1181k	5,916	497k	8,463	684k
fe80::c30c:0:0:12	9,410	793k	6,674	550k	2,736	243k
fe80::c30c:0:0:13	18,756	1536k	9,915	829k	8,841	707k
fe80::c30c:0:0:14	31,935	2538k	14,194	1125k	17,741	1413k
fe80::c30c:0:0:15	20,907	1737k	13,732	1134k	7,175	602k
fe80::c30c:0:0:16	10,021	830k	7,934	650k	2,087	179k
fe80::c30c:0:0:17	11,584	987k	7,958	677k	3,626	309k
fe80::c30c:0:0:18	9,588	804k	7,129	584k	2,459	219k
fe80::c30c:0:0:19	19,272	1590k	7,238	601k	12,034	988k
fe80::c30c:0:0:1a	12,831	1079k	9,095	754k	3,736	324k
fe80::c30c:0:0:1b	22,794	1853k	17,241	1400k	5,553	452k
fe80::c30c:0:0:1c	20,877	1723k	7,437	626k	13,440	1097k
fe80::c30c:0:0:1d	22,758	1867k	13,299	1089k	9,459	778k
fe80::c30c:0:0:1e	9,872	824k	6,876	573k	2,996	250k
fe80::c30c:0:0:1f	25,488	2064k	10,677	913k	14,811	1150k
fe80::c30c:0:0:20	20,100	1650k	9,367	773k	10,733	877k
fe80::c30c:0:0:21	28,436	2271k	12,262	978k	16,174	1292k
fe80::c30c:0:0:22	21,502	1755k	12,198	995k	9,304	760k
fe80::c30c:0:0:23	7,402	631k	5,710	475k	1,692	155k
fe80::c30c:0:0:24	9,156	779k	7,826	659k	1,330	119k
fe80::c30c:0:0:25	26,548	2158k	10,309	869k	16,239	1288k
fe80::c30c:0:0:26	15,799	1309k	9,455	808k	6,344	501k
fe80::c30c:0:0:27	21,526	1788k	9,592	830k	11,934	957k
fe80::c30c:0:0:28	14,568	1195k	10,703	870k	3,865	325k
fe80::c30c:0:0:29	19,384	1582k	9,532	795k	9,852	787k
fe80::c30c:0:0:2a	12,470	1097k	5,782	533k	6,688	563k
fe80::c30c:0:0:2b	13,543	1103k	11,590	940k	1,953	163k
fe80::c30c:0:0:2c	8,779	746k	7,519	630k	1,260	116k
fe80::c30c:0:0:2d	16,246	1330k	11,877	975k	4,369	355k
fe80::c30c:0:0:2e	15,031	1251k	10,777	916k	4,254	334k
fe80::c30c:0:0:2f	24,687	2016k	10,716	899k	13,971	1116k
fe80::c30c:0:0:30	23,510	1935k	7,292	637k	16,218	1298k
fe80::c30c:0:0:31	18,326	1494k	10,994	916k	7,332	577k
fe80::c30c:0:0:32	6,251	531k	5,719	480k	532	51k
fe80::c30c:0:0:33	72,301	4872k	58,254	3739k	14,047	1132k

Şekil 5.8. Ağ Trafik Analizi

Şekil 5.8.'de belirtilen üzere, fe80::c30c:0:0:33 IPv6 adresine sahip düğüm, diğer düğümlere kıyasla önemli ölçüde daha fazla paket trafiği üretmiştir. Normal bir DODAG ağ yapısında, en yoğun paket trafiği genellikle kök düğümden (en fazla üst/alt ilişkisine sahip olan düğüm) ya da en uzak düğümden kaynaklanmakta ve trafikte sürekli bir artış gözlenmektedir. Ancak saldırı senaryosunda, saldırgan düğüm en uzak düğüme kıyasla yaklaşık iki kat daha fazla paket göndermiş ve trafik artışlarında belirgin bir düzensizlik tespit edilmiştir.

Makine öğrenmesi analizi, aykırı değerleri tespit etmek için kullanılmıştır. Bu da saldırganın büyük miktarda merhaba *(hello)* paketi göndermesiyle gerçekleştirilmiş olup, saldırının içeriden veya dışarıdan olması fark etmemektedir. Bu durumda, düğümler arasındaki standart iletişim bozulmuş ve aykırı bir durum oluşmuştur. Bu durum

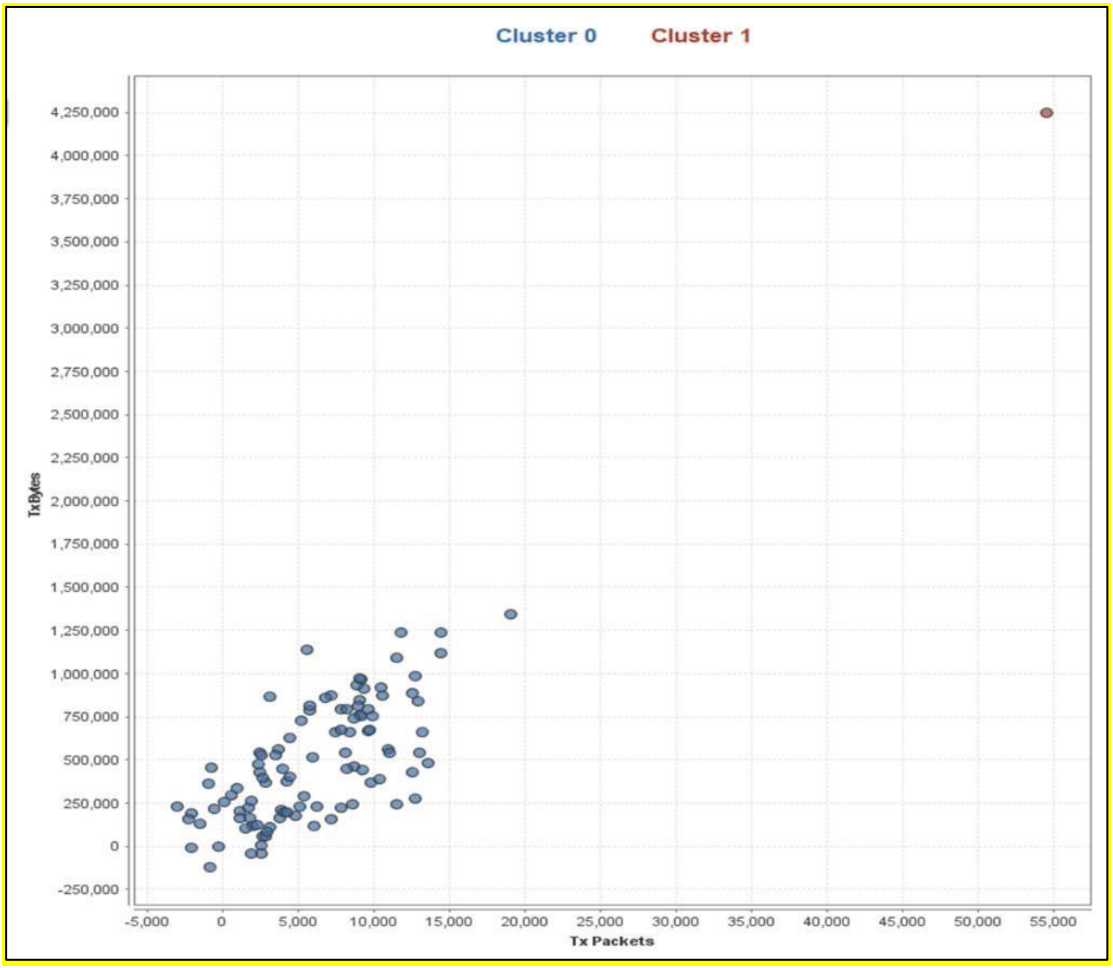
saldırganın erken tespit edilmesini, sistemden izole edilmesini veya güvenlik sistemleri tarafından bloke edilmesini sağlamıştır. Sel saldırısında, K-Means algoritması aykırı *(outlier)* özellikleri dikkate alarak kullanılmıştır çünkü saldırgan, ağ trafiğinin ortalama değerlerinden önemli ölçüde sapmaktadır. K-Means algoritması, büyük verisetlerinde anomalileri hızlı ve etkili bir şekilde belirleyebilmekte ayrıca, kümeleme yöntemleri arasında geniş bir bilinirliğe ve kullanıma sahiptir. Literatürde, K-Means algoritmasının çeşitli modifikasyonları önerilmiştir. Gözetimsiz öğrenme kapsamında yer alsa da, K-Means algoritması ve modifikasyonları, başlangıçta belirlenen küme sayısına duyarlı olarak çalışmaktadır ve bu yüzden tam anlamıyla gözetimsiz bir yöntem değildir [76]. K-Means algoritması, N veri noktasını I boyutlu uzayda K küme içerisine yerleştirmek üzere tasarlanmıştır.

K-Means algoritması, her kümenin vektörlerle tanımlanmış ortalaması olan m(k) adı verilen bir vektör ile parametrelenmektedir. Veri noktaları x(n) ile ifade edilmekte, burada n'in üst simgesi veri noktalarının sayısını göstermektedir. Her x vektörü I bileşene sahip olmakta, ayrıca başlangıçta verilen küme seti m1(1),...,mn(1) ile başlamakta ve temel adımları arasında değişim göstermektedir.

Atama adımı: Her gözlemi, en yakın olan öklidyen ortalamaya sahip kümeye atamamız gerekmektedir. Her x_p, kesin olarak bir S(t) kümesine atanmakta ve birden fazla küme bu atamayı alabilmektedir.

Güncelleme adımı: Her kümeye atanmış gözlemlerin ortalamalarını (merkezlerini) yeniden hesaplamamız gerekmektedir.

Bu algoritma hazırlama işlemi, kümelere atamalar sabit oluncaya kadar devam etmektedir. Algoritmanın optimum bir çözüm bulma garantisi bulunmamaktadır. Genellikle, nesneleri mesafeye dayalı olarak en yakın kümeye atama şeklinde çalışmakta ve öklid dışında kullanılan bir mesafe fonksiyonu, algoritmanın yakınsamasını engelleyebilmektedir. Diğer mesafe ölçütlerini kullanmak amacıyla, küresel K-Means ve K-medoids gibi çeşitli K-Means modifikasyonları önerilmiştir [77]. K-Means algoritması kullanılarak, ağ trafiğindeki anormal düğüm (saldırgan düğüm) Şekil 5.9.'da gösterildiği gibi tespit edilmiştir.



Şekil 5.9. K-Means Algoritması ile Sel Saldırısı Tespiti

Şekil 5.9.'daki şekil incelendiğinde, K-Means algoritması kullanılarak yapılan sel saldırısı tespitinde oluşturulan iki farklı kümenin grafiğini görülmektedir. Bu kümelerden biri, normal ağ trafiği düğümlerine *(Küme 0)* ait veri trafiğini temsil ederken, diğeri saldırgan düğüme *(Küme 1)* ait ağ trafiğini temsil etmektedir. Aşırı ağ trafiği anomalisi nedeniyle, bu kümelerin plot ekseninin zıt noktalarında konumlandığı görülmektedir [73]. Sel saldırıları genellikle ağ trafiğinde belirgin anomaliler yaratmaktadır; bu anomaliler, gönderilen paket sayısında ve veri miktarında olağan dışı artışlar olarak gözlemlenmektedir. K-means algoritması, bu tür anomalileri belirleyerek, olağan trafik ile anormal trafik arasında ayrım yapabilmektedir. K-Means kullanarak, olağan dışı yüksek sayıda paket gönderimi ve veri transferi yapan bir grup tespit edilirse, bu grup potansiyel saldırgan olarak tanımlanabilir.

Şekil 5.9.'da, aykırı durumundaki tek bir nokta, saldırganın varlığını işaret etmektedir. Bu nokta, diğer tüm veri noktalarından belirgin şekilde farklı bir konumda bulunmakta, yüksek miktarda paket ve veri transferi yaparak diğer gruplardan ayrılmaktadır. Bu tür

aykırı noktalar, ağ trafiğinde normalden sapmaların göstergesi olduğu için kural tabanlı uzman sistemlerde de doğrudan kullanılabilmektedir. Bu kapsamda, anormal trafik modellerini otomatik olarak tespit edecek ve ağ yöneticilerini uyaracak kurallar oluşturulmuştur. Örneğin, belirli bir eşik değerinin üzerindeki trafik miktarı ve paket sayısı gözlemlendiğinde, ilgili kural devreye girmekte ve bu trafiği potansiyel bir saldırı olarak işaretlemektedir. Bu sayede, ağ güvenliği proaktif olarak sağlanabilmekte ve saldırılara hızlı bir şekilde müdahale edilebilmektedir.

Araştırmanın algoritması şu şekilde özetlenebilir:

```
Girdi: IoT Veri Seti
Çıktı: Saldırı veya Yasal İletim
Veri setinin özelliklerini yükle
[derece, ağırlıklar]=relief(özellikler, hedef); // Özellik
dereceleri ve ortalama değerleri hesaplamak için relief
uygula
for i = 1 to 7 do
     özellikler_aykırı(:,i) = özellikler(:,derece(i));
     //Aykırı özellikleri seç
end for
accmean = 0; // Doğruluk değerini tanımla
while veri(i)=aykırı(i) do
     saldırı=saldırı+1
     acc = 0;
     for i = 1 to L do // L veri seti boyutudur
          if aykırı(i) = flagedattack(i) then
               acc = acc + 1;
          end if
     end for
     accmean = accmean + acc/L;
end while
```

5.3.2. MQTT ’ye Yönelik Saldırıların Uzman Sistem ile Analizi

Bu kısımda, IoT ve IIoT’de kullanılan MQTT Protokolüne yönelik gerçekleştirilen kaba kuvvet, hizmet reddi (*DoS, Flood, Slowite*) ve bozuk paket (*malformed*) saldırılarının uzman sistem aracılığıyla tespiti ele alınmıştır. Bu amaçla öncelikle kaba kuvvet saldırısı gerçekleştirilerek MQTT Broker’a yasal kullanıcı girişi elde edilmiş, müteakip olarak hizmet reddi ve bozuk paket saldırıları sistem üzerinde denenmiştir. Saldırılara ilişkin elde edilen paketler toplanarak paketler makine öğrenmesi algoritmalarına aynalama tekniği ile aktarılmıştır.

Tablo 5.3. incelendiğinde, MQTT protokolüne yönelik gerçekleştirilen saldırı analizleri kapsamında elde edilen veriler, uygulamaya yüklendiğinde öncelikle veri dağılımı ve

saldırı olup olmadığı, saldırı ise paketin hangi tür saldırı olduğuna yönelik olarak uzman sistemin çalıştırılması hedeflenmiştir. Saldırı paketlerine yönelik oluşturulan veri setinin %70'i Tablo 5.3.'te görülen çeşitli algoritmalara eğitim amacıyla, kalan %30'u ise doğrulama için girdi olarak verilmiştir. Uzman sistemin saldırıları tespiti için çalıştırılmasından sonra, Tablo 5.3.'te yer alan karşılaştırma tablosu elde edilmiştir. Üçüncü aşamada ise çeşitli araçlar üzerinden analiz sonuçları kullanıcılara yönelik olarak görselleştirilerek, son aşamada karar ağacı modeli ile elde edilen sonuçlar kural haline dönüştürülerek uzman sisteme aktarılmıştır.

Model	**Cevap Zamanı (s)**	**Doğruluk**	**F1**	**Hassasiyet**	**Özyineleme**
Tree	0.032	0.922	0.918	0.920	0.922
AdaBoost	6.498	0.927	0.925	0.928	0.927
Logistic Regression	0.609	0.825	0.813	0.856	0.825
NN Tanh	0.892	0.824	0.812	0.852	0.824
NN Logistic	0.912	0.829	0.819	0.854	0.829
NN ReLU	0.852	0.823	0.812	0.844	0.823
NN Identity	1.044	0.829	0.820	0.856	0.829
SVM	296.788	0.442	0.548	0.829	0.442
kNN	88.982	0.924	0.922	0.923	0.924

Tablo 5.3. MQTT Saldırıları için Yapay Zeka Modelleri Performans Ölçütleri

Tablo 5.3.'te yer alan sonuçlar, farklı algoritmaların cevap süresi, doğruluğu, hassasiyeti *(precision),* özyinelemeli hassasiyet *(recall)* ve F1 değeri ve cevap zamanı gibi önemli değerler açısından mukayese edilmiştir. Karşılaştırılan sonuçlar içerisinde 0.032ms'lik cevap süresi ve %92,2'lik yüksek doğruluk değerine sahip olan karar ağacı modeli, F1 değeri, hassasiyet ve özyinelemeli hassasiyet gibi diğer önemli değerler de göz önünde bulundurularak uzman sistem olarak seçilmiştir.

Bu şekilde, uzman sistem modelinde karar ağacı modelinin kullanılması, saldırı tespiti ve önleme konusunda daha yüksek hız, doğruluk ve hassasiyet sağlamıştır.

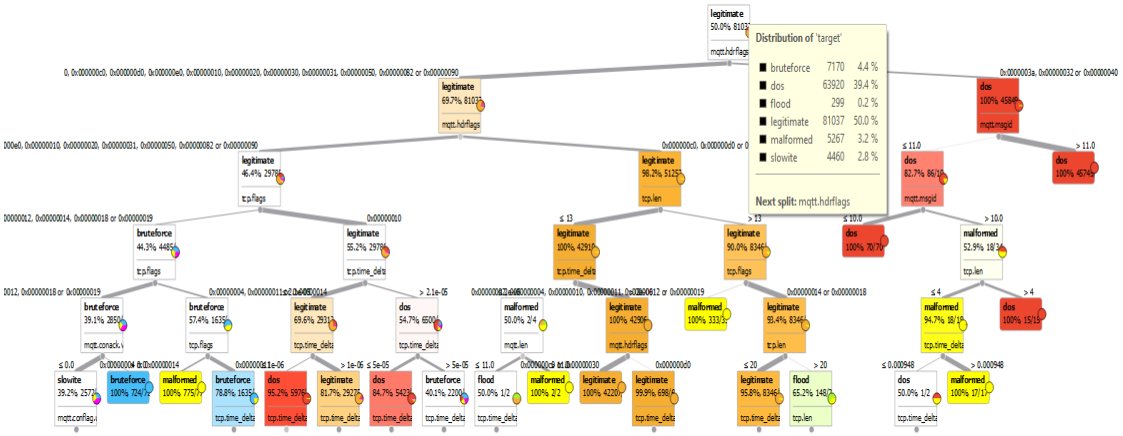
5.3.2.1. Modelin Oluşturulması ve Eğitilmesi

IIoT'ye yönelik saldırı tespit analizlerinin ikinci aşamasında IIoT'de kullanılan MQTT protokolüne yönelik gerçekleştirilen saldırıların uzman sistem aracılığıyla tespitinde en hızlı ve başarılı modelin karar ağacı olması nedeniyle, uzman sistemde karar ağacı algoritmasıyla devam edilmiştir. Veriler gerçek sistemler kullanılarak toplanmış ve beyaz liste *(white list)* veri setine dönüştürülmüştür. Oluşturulan veri seti eğitim için %70, doğrulama için %30 olarak ayrılmıştır. Karar ağacı uzman sistem modeline ait karmaşıklık matrisi *(Confusion Matrix)* Şekil 5.10.'da gösterilmiştir. Şekil 5.10.'da yer alan matris incelendiğinde, saldırı sınıflandırmasının yüksek doğrulukla tespit edilebildiği diğer bir ifadeyle yanlış-pozitif *(false-positive)* değerinin düşük olduğu görülmüştür.

		Predicted						
		bruteforce	**dos**	**flood**	**legitimate**	**malformed**	**slowite**	**Σ**
Actual	**bruteforce**	5902	734	1	8	488	37	**7170**
	dos	501	58671	0	4493	92	163	**63920**
	flood	0	41	148	106	2	2	**299**
	legitimate	0	1055	2	79969	9	2	**81037**
	malformed	1653	489	2	49	2983	91	**5267**
	slowite	685	380	0	618	95	2682	**4460**
	Σ	**8741**	**61370**	**153**	**85243**	**3669**	**2977**	**162153**

Şekil 5.10. Karmaşıklık Matrisi (Confusion Matrix)

Karar ağacı modeli ağaç yapısı Şekil 5.11.'de gösterilmiştir.



Şekil 5.11. MQTT Karar Ağacı Modeli

Bu ağaç yapısında, MQTT protokolüne yönelik çeşitli saldırı türleri modellemiştir. Ayrıca, modelin saldırıları tespit etme yeteneğini ve saldırı türlerini belirlemede verilecek tepkileri değerlendirmek için kullanılmıştır. Bu sayede ağ trafiğinin sürekli izlenmesinin saldırı tespitindeki önemi ele alınmıştır. Kritik altyapıların haberleşme kontrolünde oldukça önemli rol oynayan IIoT sistemlerinin güvenliği ve sürekliliğinin sağlanması açısından oldukça önemlidir. Şekil 5.11. incelendiğinde, yasal paketlerle aynı anda saldırgan tarafından IIoT'de kullanılan MQTT protokolüne yönelik gerçekleştirilen saldırıların karar ağacı üzerinde kökten yaprağa doğru ilgili yolun izlenmesi durumunda 0.032ms'de ve %92,2 doğrulukla tespit edilebildiği ayrıca, saldırıya ait sınıfın da tespit edilebildiği görülmüştür.

5.4. Yapay Zeka ve Makine Öğrenimi ile Entegrasyon

Yapay zeka ve makine öğrenimi, kural tabanlı network sistemlerinin daha dinamik ve etkili olmasını sağlamaktadır. Bu entegrasyon, sistemin zamanla değişen tehditlere karşı daha güvenli olmasını ve yeni tehditleri algılayabilmesini mümkün kılmaktadır.

Çalışmada, Karar ağacı modelleri, gerçek veri setleri üzerinde eğitilerek saldırı tespitinde yüksek doğruluk oranlarına ulaşmıştır. Karar ağacı modellerinin karmaşık veri yapılarını basit ve anlaşılabilir hale indirgeyebilme özelliği, IoT ve IIoT sistemlerindeki anormalliklerin başarılı ve hızlı bir şekilde tespit edilmesini sağlamaktadır. Bu nedenle, karar ağacı modelleri, IoT ve IIoT güvenlik sistemlerinde önemli bir rol oynamakta ve yapay zeka ile entegre edilerek güvenlik tehditlerine karşı etkili bir çözüm sunmaktadır.

Bu bağlamda, yapay zekanın karar ağaçlarına entegrasyonu, sistemlerin sadece mevcut tehditlere karşı değil, aynı zamanda gelecekte ortaya çıkabilecek yeni tehditlere karşı da

proaktif olarak hazırlıklı olmasını sağlamaktadır. Bu entegrasyon, güvenlik sistemlerinin esnekliğini artırarak, sürekli değişen siber tehdit ortamında daha güvenilir ve dayanıklı bir koruma sağlamaktadır.

Kural tabanlı uzman sistemler, belirli bir alanda uzman bilgisine dayalı olarak oluşturulan kural setinin oluşturulmasıyla çalışmaktadır. Bu sistemler, belirli bir durum veya olay gerçekleştiğinde, önceden tanımlanmış kuralları uygulayarak uygun eylemleri gerçekleştirmektedir. Önerilen kural tabanlı sistem, karar ağacı yapay zeka modeli ile oluşturulan ağaç yapısının verilerinin kural haline getirilmesi ile oluşturulmuştur. IoT ve IIoT sistemlerine yönelik olası saldırı senaryolarını için karar ağacındaki kural yapısı kullanılarak, ağ trafiğindeki anormallikler tespit edilmiştir.

5.5. Kural Tabanlı Uzman Sistemin Oluşturulması

Belirlenen yapay zeka modelleri sonucunda oluşan çıktıların kural tabanlı sisteme aktarımı ile önerilen uzman sistem modelinin IoT ve IIoT güvenliğinde kullanımı ile önerilen uzman sistem modeli kullanılarak IoT ve IIoT sistemlerine yönelik saldırılara karşı geliştirilen savunma stratejileri incelenmiştir.

5.5.1. Kural Tabanlı Yapay Zeka Sistemlerinin IoT ve IIoT Güvenliğinde Kullanımı

Kural tabanlı uzman sistem oluşturmak için açık kaynak kodlu Snort IDS yazılımı seçilmiştir. Yapay zeka tabanlı uzman sistem üzerinde kullanımına karar verilen karar ağaçları incelenmiş ve karar ağacındaki dalların her biri belirli koşullar altında çalışan kurallara dönüştürülmüştür. Her bir düğüm, belirli bir özelliğe (örneğin "TTL", "Protokol", "RTT" vb.) ve belirli bir koşula (örneğin "<= 64", "> 58" vb.) bağlı olarak kural oluşturmak için kullanılmıştır.

Kural tabanlı sistem olarak belirlenen uygulamada kurallar aşağıdaki formattaki şekilde yazılmaktadır:

alert (Alarm) <Protokol> <Kaynak IP> <Kaynak Port> -> <Hedef IP> <Hedef Port> (msg:"<Mesaj>"; priority (Kritiklik Seviyesi):<1-5>; sid:<ID Numarası>; rev:1;)

IoT saldırılarına karşı kural tabanlı uzman sistemde kullanılmak üzere karar ağacı kullanılarak oluşturulan örnek kurallar aşağıda verilmiştir:

- alert icmp6 any any -> any any (msg:"ICMPv6 Sel Saldırısı Tespit Edildi"; flow:to_server, established; threshold:type both, track by_src, count 1000, seconds 30; classtype:attempted-dos; priority:3; sid:1000001; rev:1;)

- alert tcp any any -> any any (msg:"Kaba Kuvvet Saldırısı Tespit Edildi"; flow:established; content:"loginattempt"; classtype:attempted-admin; priority:1; sid:1000002; rev:1;)
- alert tcp any any -> any any (msg:"Kaba Kuvvet Saldırısı Tespit Edildi"; flow:established; content:"loginattempt"; threshold:type threshold, track by_src, count 1, seconds 3600; classtype:attempted-admin; priority:2; sid:1000003; rev:1;)
- alert tcp any any -> any any (msg:"Kaba Saldırısı Tespit Edildi"; flow:established; content:"loginattempt"; threshold:type threshold, track by_src, count 1, seconds 3600; classtype:attempted-admin; priority:3; sid:1000004; rev:1;)
- alert tcp any any -> any any (msg:" Bozuk Paket Tespit Edildi"; flow:established; content:"malformed"; threshold:type threshold, track by_src, count 1, seconds 3600; classtype:bad-unknown; priority:3; sid:1000005; rev:1;)
- alert tcp any any -> any any (msg:"Sel Saldırısı Tespit Edildi"; flow:established; content:"flood"; threshold:type threshold, track by_src, count 1, seconds 3600; classtype:attempted-dos; priority:3; sid:1000006; rev:1;)

IIoT saldırılarına karşı kural tabanlı uzman sistemde kullanılmak üzere karar ağacı kullanılarak oluşturulan örnek kurallar aşağıda verilmiştir:

- alert cotp any any -> any any (msg:"PLC Başlat Durdur Saldırısı"; cotp.rtt > 1879257.0; priority:1; sid:1000006; rev:1;)
- alert cotp any any -> any any (msg:"PLC Başlat Durdur Saldırısı"; cotp.deltatime > 58.0; priority:1; sid:1000007; rev:1;)
- alert tcp any any -> any any (msg:"MitM Saldırısı"; ip.ttl <= 64; ip.len > 74; priority:2; sid:1000008; rev:1;)
- alert tcp any any -> any any (msg:"MitM Saldırısı"; ip.ttl <= 64; ip.len <= 0; cotp.rtt <= 54; cotp.deltatime <= 54; priority:2; sid:1000009; rev:1;)
- alert tcp any any -> any any (msg:"MitM Saldırısı Tespit Edildi"; ip.ttl > 64; ip.len > 64; cotp.deltatime <= 54; priority:2; sid:1000010; rev:1;)

Bu kurallar, ağaç yapısındaki bazı düğüm verileri kullanılarak oluşturulmuştur. Her bir düğüm için daha fazla ayrıntı eklenebilmekte ve dallanma mantığı genişletilebilmektedir.

Tam karar ağacını tümüyle kural tabanlı hale dönüştürmek için her bir düğüm ve alt düğüme ait benzer kurallar yazılmalıdır. Bu kuralların, karar ağacındaki her bir dallanma noktasına karşılık gelmesi gerekmektedir.
Ayrıca, daha karmaşık ağaç yapıları için bu kuralların kapsamının genişletilmesi ve daha detaylı kurallar yazılması gerekmektedir. Bu süreç, her bir karar düğümünü ayrıntılı olarak incelemeyi ve buna göre kuralları tanımlamayı gerektirmektedir.

IoT ve IIoT sistemlerine yönelik olarak gerçekleştirilen saldırılar kapsamında yapay zeka tabanlı uzman sistem sonucunda oraya çıkan karar ağaçlarının kural tabanlı uzman sisteme aktarılabilmesi için hazırlanan pseudo kodu aşağıda verilmiştir.

```
Girdi: Yapay Zeka Modeli (Karar Ağacı)
Çıktı: Kural Tabanlı Uzman Sistem Kuralı
function snort_kuralı_oluştur(düğüm, durum):
    if düğüm is a yaprak:
        kural = snort_kuralı_yarat(durum, düğüm.class)
        kuralı_dosyaya_yaz(kural)
    else:
        for each alt in düğüm.alt:
            yeni_durum = durum + düğüm.durum
            snort_kuralı_oluştur(alt, yeni_durum)
```

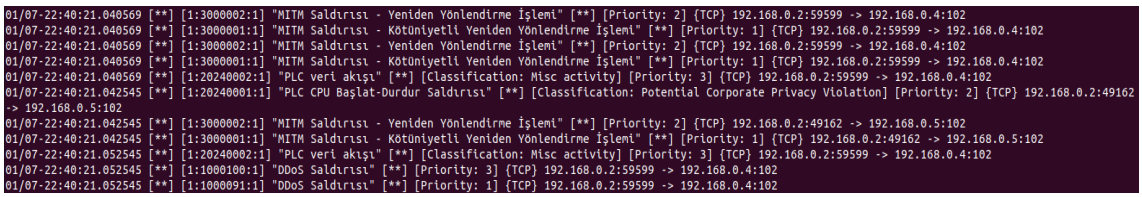
Bazı diğer yapay zeka modelleri için oluşturulan pseudo kodu aşağıda verilmiştir.

```
Girdi: Yapay Zeka Modelleri (Neural Network, Random Forest,
Adaboost, K-Means gibi)
Çıktı: Kural Tabanlı Uzman Sistem Kuralı
# Modeli dosyadan yükle
     model = model_yukle()
# Kaydedilen ağ trafiği verilerini dosyadan yükle
     trafik_verisi = trafik_verisi_yukle()
# Tahminler
     tahminler  =  model.predict(trafik_verisi)     #Modeli
Kullanarak Tahminler Yap
# Snort Kuralları Listesini Başlat
     snort_rules = []
     sid = 1000000
# Tahminleri Kullanarak Snort Kuralları Oluştur
     for tahmin in tahminler:
          if model is Neural Network:
               if tahmin > eşik:  #Saldırı olasılığı belirli
bir eşik değerinin üzerindeyse
                    rule  =  f"alert  ip  any  any  ->  any  any
(msg:\"Saldırı  olasılığı  -  Neural  Network\";  sid:{sid;
rev:1;)"
                    snort_rules.append(rule)
                    sid += 1
```

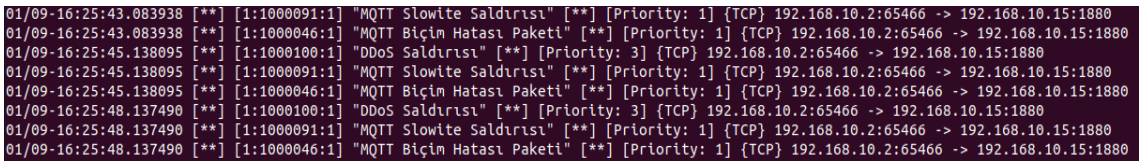
```
        if model is Random Forest:
            for tree in model:
                tree_rules
=agaci_snort_kuralina_donustur(tree)
                snort_rules.extend(tree_rules)
        if model is AdaBoost:
            for weak_classifier in model:

weak_rules=weak_classifier_snort_kuralina_
                    donustur(weak_classifier)
                snort_rules.extend(weak_rules)
        if model is K-Means:
            if tahmin == 'saldiri':    #Saldırı olarak
sınıflandırılmışsa
                rule = f"alert ipv6 any any -> any any
(msg:\"Saldırı olasılığı - K-Means\"; sid:{sid}; rev:1;)"
                snort_rules.append(rule)
                sid += 1
# Snort kurallarını dosyaya yaz (isteğe bağlı)
    snort_kurallari_dosyaya_yaz(snort_rules)
```

Yapay zeka tabanlı uzman sistem tarafından yaratılan karar ağaçlarının incelenmesi sonucunda oluşturan kurallar, saldırı sırasında toplanan ağ paketleri kullanılarak Snort yazılımı üzerinde kural tabanlı olarak uygulanmıştır. Yapılan testlerinin sonuçları Şekil 5.12. ve Şekil 5.13.'te gösterilmiştir.



Şekil 5.12. Kural Tabanlı Sistem ile IoT Saldırısı Tespiti



Şekil 5.13. Kural Tabanlı Sistem ile IIoT Saldırısı Tespiti

Uygulanan bu yöntem, saldırı tespiti ve önlenmesinde etkili bir yaklaşım sunmaktadır. Karar ağaçları, saldırı sırasında toplanan verilerden elde edilen desenleri tanımlayarak saldırıları en hızlı şekilde tespit etmek için kullanılmıştır. Şekil 5.12. ve Şekil 5.13.'te görüldüğü üzere, kural tabanlı Snort sistemine entegre edilen kuralların performansı ve etkinliği açıkça görülmektedir.

Yapay zeka tabanlı karar ağacı modeliyle oluşturulan kural tabanlı uzman sistemlerin, IoT ve IIoT sistemlerinin güvenliği alanında önemli bir araç olduğu görülmektedir. Bu sistemler, kompleks saldırı modellerini tanımlama ve anlama yetenekleriyle bilinen saldırı türlerini başarıyla sınıflandırabilmektedir. Ayrıca, yapay zeka tabanlı uzman sistem modellerinin Snort gibi kural tabanlı IPS (Saldırı Önleme Sistemi- Intrusion Prevention System)/IDS (Saldırı Tespit Sistemi-Intrusion Detection System) sistemleriyle entegrasyonları ile saldırıların hızlı bir şekilde tespit ve müdahale edilebilmesini sağlamaktadır. Geliştirilen analiz yöntemi sayesinde, gelecekte ortaya çıkabilecek yeni saldırı vektörleri için de IoT ve IIoT güvenliği alanında yeni modellerin oluşturularak sisteme eklenebilmesi sağlanmıştır.

6. SONUÇLAR VE ÖNERİLER

IoT ve IIoT teknolojileri modern endüstriyel süreçlerin temel bileşenleri haline gelmiştir. Bu teknolojilerin sunduğu avantajlar; verimlilik, otomasyon ve operasyonel maliyetlerin azaltılması gibi birçok fayda sağlamaktadır. Bununla birlikte bu sistemlerin yaygın kullanımı, sistemlerin güvenliği konusunda da ciddi bir endişe kaynağı olmaktadır.

Bu kapsamda literatürde IoT ve IIoT sistemlerinin güvenliği ile ilgili önemli eksiklikler bulunmaktadır. Bu eksikliklerin başında, bu sistemlere yönelik tehditlerin geniş bir yelpazede incelenmemesi ve savunma stratejilerinin yetersiz kalması gelmektedir. Mevcut çalışmalar genellikle belirli saldırı türlerine odaklanmakta ve bu saldırılara karşı geliştirilen savunma mekanizmaları ile sınırlı kalmaktadır. Bu durumda, IoT ve IIoT sistemlerinin güvenliğini sağlamada da çeşitli yetersizlikler oluşturmaktadır.

Bu tez çalışması, IoT ve IIoT sistemlerinin güvenlik açıklarını incelemek ve bu açıkların giderilmesine yönelik bir uzman sistem modeli geliştirmek üzerine odaklanmıştır. Çalışmada öncelikle IoT ve IIoT sistemlerinin ağ topolojilerindeki güvenlik zafiyetleri detaylı bir şekilde incelenmiştir. Analizler kapsamında, çeşitli saldırı senaryoları üzerinden incelemeler yapılmış ve IIoT sistemlerine yönelik potansiyel tehditlerin doğasını anlamak amacıyla derinlemesine bir bakış sunulmuştur.

Bu çalışma, siber güvenlik uzmanı olmayan personelin IoT ve IIoT teknolojilerine yönelik siber tehditleri anlamalarını sağlamakta ayrıca, bu tehditleri tespit etmeye yönelik yardımcı örnek uzman sistem tasarımı önermektedir. Önerilen uzman sistemin karmaşık güvenlik protokollerini sadeleştirilmiş şekilde sunması, personelin hızlı ve etkili bir şekilde tehditleri tespit edebilmesini sağlama amacındadır. Özellikle, siber güvenlik konusunda yeterli uzmanlığı ve deneyimi olmayan kişilerin, karmaşık güvenlik protokollerini ve saldırı türlerini anlamaları genellikle zor olduğundan, uzman sistem ile bu boşluğun doldurulması hedeflenmiştir. Çeşitli saldırı türlerini ve anomalileri yüksek doğrulukla tespit edebilmek için yapay zeka ve makine öğrenimi tekniklerinin performansları araştırılmıştır. Çalışmada önerilen karar ağacı modeli ile siber güvenlik konusunda yeterli uzmanlığı ve deneyimi olmayan kişilerin bile minimum eğitimle sistemdeki tehditleri tanımlayabilecek ve kurallar geliştirmesine olanak sağlayabilecek bir model önerisinde bulunulmuştur.

Siber tehditlere karşı geliştirilebilecek savunma mekanizmaları ile stratejiler derinlemesine incelenmiş ve uzman sistemlerin kullanımıyla geliştirilen bir saldırı tespit

yönteminin uygulanabilirliği ve etkinliği ele alınmıştır. Siber tehditlerin tespiti için gerekli olan öznitelikler (features) yapay zeka modellerinden yararlanılarak belirlenmiş ve bir uzman sistem modeli tasarımında kullanılmıştır. Modelin doğruluğu ve performansı, çeşitli simülasyonlar ve deneysel çalışmalar yoluyla değerlendirilmiş ve yorumlanmıştır.

Çalışma önemli bulgular sağlamasına rağmen, bazı sınırlamaları vardır. İlk olarak, çalışmada kullanılan veri setleri saldırganlar tarafından yaygın olarak kullanılan belirli sayıda saldırı türünü kapsamaktadır. Bu nedenle, daha büyük ve daha çeşitli veri setleri kullanılması ile geliştirilen yöntemlerin farklı IoT ve IIoT platformlarında da test edilmesi sonuçların genelleştirilebilirliğini artıracaktır. Örneğin, çalışma boyunca kullanılan veri setleri belirli bir IoT platformuna özgü olup, diğer platformlarda benzer sonuçların elde edilip edilemeyeceği incelenememiştir. Önerilen uzman sistem modelinin IoT ve IIoT sistemlerinin güvenliğini artırmak için nasıl kullanılabileceğinin belirlenmesi ve sistemin sürekli olarak güncellenmesi gerekliliği bulunmaktadır. Modelin her yeni saldırı oluştuğunda yeniden eğitilmesi bu çalışmada sınır oluşturmuştur.

Sistem, yapay zeka öğrenme modelleri kullanarak veri boyutu öznitelik vektörünü azaltmakta ve saldırı tespit süreçlerini iyileştirmektedir. Çalışmada sunulan sayısal analizler, geliştirilen uzman sistem tabanlı saldırı tespit yönteminin, IoT ve IIoT sistemlerine yönelik saldırıları %95 gibi yüksek bir oranda başarıyla tespit edebildiğini ortaya koymuştur. Yapay zeka tekniklerinin kullanımı ile geleneksel yöntemlere göre daha hızlı ve etkili saldırı tespit süreçleri sağlamaktadır. Karar Ağacı modelleri kullanılarak yapılan saldırı tespitinde 0.011ms gibi tepki süresine ulaşıldığı çalışma şartlarındaki verilerle görülmüştür.

Sistem, sürekli izleme ve saldırı tespitini birleştiren yapay zeka tabanlı bir uzman sistemdir. Bu sistem, belirlenen özelliklerin saldırı tespitindeki etkisini değerlendirerek, hızlı ve yüksek doğruluk oranına sahip bir “saldırı tespit modeli” oluşturmuştur. Bu sayede, IoT ve IIoT ağ trafiğine yönelik yaygın saldırılar (MitM, DDoS ve Başlat-Durdur saldırıları, vb.) etkili bir şekilde tespit edilebilmiştir.

Endüstriyel Kontrol Sistemleri ve IoT teknolojilerinin güvenli entegrasyonu, bilgi toplumunun sürdürülebilirliği ve güvenliği için önem taşımaktadır. Önerilen sistem, endüstriyel kontrol sistemlerinde kullanılan gerçek cihazlar üzerinde değerlendirilmiş ve yüksek bir saldırı tespit başarı oranı göstermiştir. Bu durum, sistemin gerçek dünya

uygulamalarıyla uyumlu olduğunu ve endüstriyel ortamlarda etkili bir şekilde kullanılabileceğini göstermektedir.

Sonuç olarak bu tez çalışması, IoT ve IIoT sistemlerinin güvenliğine yönelik mevcut tehditler ile bu tehditlere karşı alınabilecek önlemleri kapsamlı bir şekilde ele almakta ve uzman sistem tabanlı saldırı tespit yöntemlerinin potansiyel etkinliğini göstermektedir. Geliştirilen metodolojinin hızı ve yüksek başarı oranları, yapay zeka ve makine öğrenmesi tekniklerinin IoT ve IIoT güvenliğinde önemli bir role sahip olacağını göstermektedir. Ayrıca bu yöntemler, insan müdahalesine olan ihtiyacı azaltmakta ve sistem güvenliğini artırmaktadır. Elde edilen bulgular doğrultusunda, bu tez çalışması gelecekteki araştırmalar için sağlam bir temel oluşturmakta, IoT ve IIoT sistemlerinin güvenlik açıklarının anlaşılması ile güvenliğini artırmaya yönelik yenilikçi çözümlerin geliştirilmesine katkıda bulunmakta ve geliştirilen uzman sistem modelinin önemini vurgulamaktadır. Bu model, saldırı tespit süreçlerini otomatikleştirme ve saldırılara hızlı bir şekilde yanıt verme ile endüstriyel uygulamalarda güvenlik standartlarının yükseltilmesi ve gelecekteki güvenlik tehditlerine karşı daha hazırlıklı olunmasını sağlayacağı görülmektedir.

7. KAYNAKLAR

[1] H. Leurent and E. d. Boer. "The Next Economic Growth Engine Scaling Fourth Industrial Revolution Technologies in Production." https://www3.weforum.org/docs/WEF_Technology_and_Innovation_The_Next_Economic_Growth_Engine.pdf (accessed 06.04.2024.

[2] M. G. Institute. "What are Industry 4.0, the Fourth Industrial Revolution, and 4IR?" https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-industry-4-0-the-fourth-industrial-revolution-and-4ir (accessed 06.04.2024.

[3] E. N. YILMAZ, S. GÖNEN, S. Şanoğlu, G. KARACAYILMAZ, and Ö. Özbirinci, "Endüstri 4.0'ın gelişim sürecinde unutulan bileşen: Siber güvenlik," *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, vol. 9, no. 4, pp. 1142-1158, 2021.

[4] U. Cisco, "Cisco annual internet report (2018–2023) white paper," *Cisco: San Jose, CA, USA*, vol. 10, no. 1, pp. 1-35, 2020.

[5] E. López-Morales *et al.*, "Honeyplc: A next-generation honeypot for industrial control systems," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020, pp. 279-291.

[6] E. A. Boateng, "Anomaly detection for industrial control systems based on neural networks with one-class objective function," *Proceedings of Student Research and Creative Inquiry Day*, vol. 5, 2021.

[7] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future generation computer systems*, vol. 82, pp. 395-411, 2018.

[8] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, "Challenges and opportunities in securing the industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 2985-2996, 2020.

[9] M. Alsheikh, L. Konieczny, M. Prater, G. Smith, and S. Uludag, "The state of IoT security: Unequivocal appeal to cybercriminals, onerous to defenders," *IEEE Consumer Electronics Magazine*, vol. 11, no. 3, pp. 59-68, 2021.

[10] L. a. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT Privacy and security: Challenges and solutions," *Applied Sciences*, vol. 10, no. 12, p. 4102, 2020.

[11] F. Zhao, X. Koutsoukos, H. Haussecker, J. Reich, and P. Cheung, "Monitoring and fault diagnosis of hybrid systems," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 35, no. 6, pp. 1225-1240, 2005.

[12] X. S. Shen *et al.*, "Blockchain for transparent data management toward 6G," *Engineering*, vol. 8, pp. 74-85, 2022.

[13] A. Kumar, R. Saha, M. Conti, G. Kumar, W. J. Buchanan, and T. H. Kim, "A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions," *Journal of Network and Computer Applications*, vol. 204, p. 103414, 2022.

[14] X. Liu *et al.*, "Secure data aggregation aided by privacy preserving in Internet of Things," *Wireless Communications and Mobile Computing*, vol. 2022, 2022.

[15] H. Wu, H. Han, X. Wang, and S. Sun, "Research on artificial intelligence enhancing internet of things security: A survey," *Ieee Access*, vol. 8, pp. 153826-153848, 2020.

[16] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. V. Poor, "Federated learning for internet of things: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1622-1658, 2021.

[17] L. Qi, Y. Yang, X. Zhou, W. Rafique, and J. Ma, "Fast anomaly identification based on multiaspect data streams for intelligent intrusion detection toward secure

industry 4.0," *IEEE Transactions on Industrial Informatics,* vol. 18, no. 9, pp. 6503-6511, 2021.
[18] M. Venkatasubramanian, A. H. Lashkari, and S. Hakak, "Iot malware analysis using federated learning: A comprehensive survey," *IEEE Access,* vol. 11, pp. 5004-5018, 2023.
[19] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions," *Mobile Networks and Applications,* vol. 28, no. 1, pp. 296-312, 2023.
[20] V. Shakya, J. Choudhary, and D. P. Singh, "Principal Component Analysis and Deep Learning-Based Traffic Anomaly Detection in WSN," in *2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, 2024: IEEE, pp. 1-6.
[21] S. K. Dash *et al.*, "Enhancing DDoS attack detection in IoT using PCA," *Egyptian Informatics Journal,* vol. 25, p. 100450, 2024.
[22] A. G. M. Mengara, Y. Yoo, and V. C. Leung, "IoTSecUT: Uncertainty-Based Hybrid Deep Learning Approach for Superior IoT Security Amidst Evolving Cyber Threats," *IEEE Internet of Things Journal,* 2024.
[23] P. Kumari and A. K. Jain, "Timely detection of DDoS attacks in IoT with dimensionality reduction," *Cluster Computing,* pp. 1-19, 2024.
[24] I. Stellios, P. Kotzanikolaou, and C. Grigoriadis, "Assessing IoT enabled cyber-physical attack paths against critical systems," *Computers & Security,* vol. 107, p. 102316, 2021.
[25] R. Singh, J. Singh, and R. Singh, "Fuzzy based advanced hybrid intrusion detection system to detect malicious nodes in wireless sensor networks," *Wireless Communications and Mobile Computing,* vol. 2017, 2017.
[26] S. Cakir, S. Toklu, and N. Yalcin, "RPL attack detection and prevention in the Internet of Things networks using a GRU based deep learning," *IEEE Access,* vol. 8, pp. 183678-183689, 2020.
[27] P. Ioulianou, V. Vasilakis, I. Moscholios, and M. Logothetis, "A signature-based intrusion detection system for the internet of things," *Information and Communication Technology Form,* 2018.
[28] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad hoc networks,* vol. 11, no. 8, pp. 2661-2674, 2013.
[29] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A survey on industrial Internet of Things: A cyber-physical systems perspective," *Ieee access,* vol. 6, pp. 78238-78259, 2018.
[30] K. E. Hemsley and E. Fisher, "History of industrial control system cyber incidents," Idaho National Lab.(INL), Idaho Falls, ID (United States), 2018.
[31] J. Ibarra, U. J. Butt, A. Do, H. Jahankhani, and A. Jamal, "Ransomware impact to SCADA systems and its scope to critical infrastructure," in *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, 2019: IEEE, pp. 1-12.
[32] A. S. Mohammed, E. Anthi, O. Rana, N. Saxena, and P. Burnap, "Detection and mitigation of field flooding attacks on oil and gas critical infrastructure communication," *Computers & Security,* vol. 124, p. 103007, 2023.
[33] T. Gueye, Y. Wang, M. Rehman, R. T. Mushtaq, and S. Zahoor, "A novel method to detect cyber-attacks in IoT/IIoT devices on the modbus protocol using deep learning," *Cluster Computing,* vol. 26, no. 5, pp. 2947-2973, 2023.

[34] E. N. Yılmaz and S. Gönen, "Attack detection/prevention system against cyber attack in industrial control systems," *Computers & Security,* vol. 77, pp. 94-105, 2018.
[35] V. Kelli *et al.*, "Attacking and defending DNP3 ICS/SCADA systems," in *2022 18th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2022: IEEE, pp. 183-190.
[36] V. Kelli, P. Radoglou-Grammatikis, T. Lagkas, E. K. Markakis, and P. Sarigiannidis, "Risk analysis of DNP3 attacks," in *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*, 2022: IEEE, pp. 351-356.
[37] P. Radoglou-Grammatikis *et al.*, "False data injection attacks against low voltage distribution systems," in *GLOBECOM 2022-2022 IEEE Global Communications Conference*, 2022: IEEE, pp. 1856-1861.
[38] S. Gönen, H. H. Sayan, E. N. Yılmaz, F. Üstünsoy, and G. Karacayılmaz, "False data injection attacks and the insider threat in smart systems," *Computers & Security,* vol. 97, p. 101955, 2020.
[39] P. Radoglou-Grammatikis *et al.*, "False Data Injection Attacks Against High Voltage Transmission Systems," in *2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)*, 2023: IEEE, pp. 324-329.
[40] D. Nedeljkovic and Z. Jakovljevic, "CNN based method for the development of cyber-attacks detection algorithms in industrial control systems," *Computers & Security,* vol. 114, p. 102585, 2022.
[41] M. Abdelaty, R. Doriguzzi-Corin, and D. Siracusa, "DAICS: A deep learning solution for anomaly detection in industrial control systems," *IEEE Transactions on Emerging Topics in Computing,* vol. 10, no. 2, pp. 1117-1129, 2021.
[42] C. Charilaou, C. I. Ioannou, and V. Vassiliou, "System for operational technology attack detection in industrial IoT," in *2022 20th Mediterranean Communication and Computer Networking Conference (MedComNet)*, 2022: IEEE, pp. 84-93.
[43] E. A. Boateng, J. Bruce, and D. A. Talbert, "Anomaly detection for a water treatment system based on one-class neural network," *IEEE access,* vol. 10, pp. 115179-115191, 2022.
[44] V. Mladenov, V. Chobanov, P. Sarigiannidis, P. I. Radoglou-Grammatikis, A. Hristov, and P. Zlatev, "Defense against cyber-attacks on the Hydro Power Plant connected in parallel with Energy System," in *2020 12th Electrical Engineering Faculty Conference (BulEF)*, 2020: IEEE, pp. 1-6.
[45] M. Mohy-eddine, A. Guezzaz, S. Benkirane, and M. Azrour, "Malicious detection model with artificial neural network in IoT-based smart farming security," *Cluster Computing,* pp. 1-16, 2024.
[46] D. A. Sivasakthi, A. Sathiyaraj, and R. Devendiran, "HybridRobustNet: enhancing detection of hybrid attacks in IoT networks through advanced learning approach," *Cluster Computing,* pp. 1-15, 2024.
[47] I. A. Khan, M. Keshk, D. Pi, N. Khan, Y. Hussain, and H. Soliman, "Enhancing IIoT networks protection: A robust security model for attack detection in Internet Industrial Control Systems," *Ad Hoc Networks,* vol. 134, p. 102930, 2022.
[48] I. A. Khan, N. Moustafa, D. Pi, K. M. Sallam, A. Y. Zomaya, and B. Li, "A new explainable deep learning framework for cyber threat discovery in industrial IoT networks," *IEEE Internet of Things Journal,* vol. 9, no. 13, pp. 11604-11613, 2021.

[49] N. Chander and M. Upendra Kumar, "Enhanced pelican optimization algorithm with ensemble-based anomaly detection in industrial internet of things environment," *Cluster Computing*, pp. 1-19, 2024.
[50] O. A. Alkhudaydi, M. Krichen, and A. D. Alghamdi, "A deep learning methodology for predicting cybersecurity attacks on the internet of things," *Information*, vol. 14, no. 10, p. 550, 2023.
[51] S. Latif, Z. Idrees, J. Ahmad, L. Zheng, and Z. Zou, "A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things," *Journal of Industrial Information Integration*, vol. 21, p. 100190, 2021.
[52] K.-K. R. Choo, Z. Yan, and W. Meng, "Blockchain in industrial IoT applications: Security and privacy advances, challenges and opportunities," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4119-4121, 2020.
[53] S. Yılmaz, E. Aydogan, and S. Sen, "A transfer learning approach for securing resource-constrained iot devices," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 4405-4418, 2021.
[54] E. Aydogan, S. Yilmaz, S. Sen, I. Butun, S. Forsström, and M. Gidlund, "A central intrusion detection system for rpl-based industrial internet of things," in *2019 15th IEEE International Workshop on Factory Communication Systems (WFCS)*, 2019: IEEE, pp. 1-5.
[55] C. Dogan, S. Yilmaz, and S. Sen, "Analysis of RPL Objective Functions with Security Perspective," in *SENSORNETS*, 2022, pp. 71-80.
[56] A. Deveci, S. Yilmaz, and S. Sen, "Evolving lightweight intrusion detection systems for RPL-based Internet of Things," in *International Conference on the Applications of Evolutionary Computation (Part of EvoStar)*, 2023: Springer, pp. 177-193.
[57] F. Y. Yavuz, D. Ünal, and E. Gül, "Deep learning for detection of routing attacks in the internet of things," *International Journal of Computational Intelligence Systems*, vol. 12, no. 1, pp. 39-58, 2018.
[58] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, "Toward a lightweight intrusion detection system for the internet of things," *IEEE access*, vol. 7, pp. 42450-42471, 2019.
[59] I. A. Khan, D. Pi, M. Z. Abbas, U. Zia, Y. Hussain, and H. Soliman, "Federated-SRUs: A federated simple recurrent units-based IDS for accurate detection of cyber attacks against IoT-augmented industrial control systems," *IEEE Internet of Things Journal*, 2022.
[60] F. Louati, F. B. Ktata, and I. Amous, "Big-IDS: a decentralized multi agent reinforcement learning approach for distributed intrusion detection in big data networks," *Cluster Computing*, pp. 1-19, 2024.
[61] M. Nanjappan, K. Pradeep, G. Natesan, A. Samydurai, and G. Premalatha, "DeepLG SecNet: utilizing deep LSTM and GRU with secure network for enhanced intrusion detection in IoT environments," *Cluster Computing*, pp. 1-13, 2024.
[62] G. Amponis *et al.*, "Threatening the 5G core via PFCP DoS attacks: the case of blocking UAV communications," *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, no. 1, p. 124, 2022.
[63] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196-248, 2019.

[64] A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, "Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review," *Computers in Industry*, vol. 137, p. 103614, 2022.
[65] M. R. Mahmood, M. A. Matin, P. Sarigiannidis, and S. K. Goudos, "A comprehensive review on artificial intelligence/machine learning algorithms for empowering the future IoT toward 6G era," *IEEE Access*, vol. 10, pp. 87535-87562, 2022.
[66] M. A. Rahman and M. S. Hossain, "A deep learning assisted software defined security architecture for 6G wireless networks: IIoT perspective," *IEEE Wireless Communications*, vol. 29, no. 2, pp. 52-59, 2022.
[67] H.-m. Kim and K.-h. Lee, "IIoT malware detection using edge computing and deep learning for cybersecurity in smart factories," *Applied Sciences*, vol. 12, no. 15, p. 7679, 2022.
[68] Y. Zhang, C. Yang, K. Huang, and Y. Li, "Intrusion detection of industrial internet-of-things based on reconstructed graph neural networks," *IEEE Transactions on network science and engineering*, 2022.
[69] J. J. Emontsbotz *et al.*, "The Application of 5G Networks on Construction Sites and in Underground Mines: Successful Outcomes from Field Trials," in *2024 19th Wireless On-Demand Network Systems and Services Conference (WONS)*, 2024: IEEE, pp. 105-112.
[70] N. T. Y. Huan and Z. A. Zukarnain, "A Survey on Addressing IoT Security Issues by Embedding Blockchain Technology Solutions: Review, Attacks, Current Trends, and Applications," *IEEE Access*, 2024.
[71] V. Kumar, *The Economic Value of Digital Disruption: A Holistic Assessment for CXOs*. Springer Nature, 2023.
[72] M. Patel, J. Shangkuan, and C. Thomas, "What's new with the Internet of Things," *McKinsey & Company*, pp. 1-8, 2017.
[73] S. Gönen *et al.*, "A novel approach to prevention of hello flood attack in iot using machine learning algorithm," *El-Cezeri*, vol. 9, no. 4, pp. 1529-1541, 2022.
[74] S. Dawans and L. Deru, "Demo Abstract: Foren 6 a RPL/6LoWPAN Diagnosis Tool," *EWSN 2014: Posters and Demos*, p. 45, 2014.
[75] E. Akkaş, L. Akin, H. E. Çubukçu, and H. Artuner, "Application of Decision Tree Algorithm for classification and identification of natural minerals using SEM–EDS," *Computers & Geosciences*, vol. 80, pp. 38-48, 2015.
[76] D. J. MacKay, *Information theory, inference and learning algorithms*. Cambridge university press, 2003.
[77] K. P. Sinaga and M.-S. Yang, "Unsupervised K-means clustering algorithm," *IEEE access*, vol. 8, pp. 80716-80727, 2020.

EKLER

EK 1 - Tezden Türetilmiş Yayınlar

Karacayılmaz, G., and Artuner, H., “A novel approach detection for IIoT attacks via artificial intelligence”. Cluster Computing, 1-19, 2024