



**KRİTİK ALTYAPILARDAKİ POTANSİYEL SİBER SALDIRILARIN
TESPİTİNE YÖNELİK YAPAY ZEKA TABANLI BİR ALGORİTMA
GELİŞTİRİLMESİ**

Mehmet Akif ÖZGÜL

**YÜKSEK LİSANS TEZİ
ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ ANA BİLİM DALI**

**GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**

TEMMUZ 2025

ETİK BEYAN

Gazi Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmada;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
 - Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
 - Tez çalışmada yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
 - Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
 - Bu tezde sunduğum çalışmanın özgün olduğunu,
- bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

İmza

Mehmet Akif ÖZGÜL

08/07/2025

KRİTİK ALTYAPILARDAKİ POTANSİYEL SİBER SALDIRILARIN TESPİTİNE YÖNELİK YAPAY ZEKA TABANLI BİR ALGORİTMA GELİŞTİRİLMESİ

(Yüksek Lisans Tezi)

Mehmet Akif ÖZGÜL

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Temmuz 2025

ÖZET

Kritik altyapılarda kullanılan Denetleyici Kontrol ve Veri Toplama (Supervisory Control and Data Acquisition – SCADA) sistemleri, günümüzde giderek karmaşıklaşan ve sürekli evrilen siber tehditler karşısında savunmasız kalmakta ve bu durum, ulusal güvenliği riske atabilecek düzeyde ciddi tehditler doğurabilmektedir. Bu çalışma, SCADA sistemlerine yönelik gerçekleştirilebilecek siber saldırıların erken aşamada ve güvenilir biçimde tespitine olanak tanıyan yapay zekâ tabanlı bir yaklaşım geliştirmeyi amaçlamaktadır. Çalışma kapsamında, bir hidroelektrik santralin SCADA haberleşme mimarisinin ölçeklendirilmiş bir modeli fiziksel olarak tasarlanmış ve bu yapıya uygun bir test ortamı oluşturulmuştur. Bu test ortamına, SCADA sisteminin kontrolü ve süreçlerin izlenmesini sağlamak amacıyla, saldırısız durum senaryosuna ek olarak; veri bütünlüğünü bozmayı hedefleyen Ortadaki Adam (Man-in-the-Middle – MITM), sistem kaynaklarını tüketmeye yönelik Hizmet Engelleme (Denial of Service – DoS) ve kontrol komutlarının dışarıdan müdahaleyle değiştirilmesini amaçlayan Komut Enjeksiyonu (Command Injection) olmak üzere yerel ağ üzerinden üç farklı siber saldırı senaryosu uygulanmıştır. Sistemin çalışması için oluşturulan proses sürekli modda çalışırken siber saldırı testleri gerçekleştirilmiştir. Senaryoların uygulanması sonucunda oluşan ağ trafiği, Wireshark aracı kullanılarak kaydedilmiş; ardından veri ön işleme adımları gerçekleştirilerek, bu çalışmaya özgü olarak oluşturulmuş etiketli bir veri seti elde edilmiştir. Senaryolar sonucunda elde edilen veri seti üzerinde, K-En Yakın Komşu (K-Nearest Neighbors – KNN), Naive Bayes (NB), Karar Ağacı (Decision Tree – DT) ve Lojistik Regresyon (Logistic Regression – LR) gibi temel makine öğrenmesi algoritmalarının yanı sıra, bu yöntemlerin ikili ve üçlü hibrit kombinasyonları da uygulanmıştır. Gerçekleştirilen analizler sonucunda, Karar Ağacı ve Lojistik Regresyon algoritmalarının birleşimiyle oluşturulan hibrit model, %98,29 doğruluk oranı ve 0,998 Eğri Altındaki Alan (Area Under the Curve – AUC) değeri ile en başarılı performansı göstermiştir. Elde edilen bulgular, geliştirilen modelin yalnızca saldırıların varlığını tespit etmekle kalmayıp farklı saldırı türlerini de yüksek doğrulukla sınıflandırabildiğini ve bu yönüyle SCADA sistemlerine yönelik siber tehditlerin zamanında ve güvenilir bir şekilde belirlenmesine katkı sağlayabileceğini göstermektedir.

Bilim Kodu : 93438
Anahtar Kelimeler : SCADA, siber saldırı, siber-fiziksel sistem, siber güvenlik, yapay zekâ ve makine öğrenmesi
Sayfa Adedi : 109
Danışman : Prof. Dr. Şevki DEMİRBAŞ

DEVELOPMENT OF AN ARTIFICIAL INTELLIGENCE-BASED ALGORITHM FOR DETECTING POTENTIAL CYBER ATTACKS IN CRITICAL INFRASTRUCTURES

(M. Sc. Thesis)

Mehmet Akif ÖZGÜL

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

July 2025

ABSTRACT

Supervisory Control and Data Acquisition (SCADA) systems used in critical infrastructures are increasingly vulnerable to ever-evolving and complex cyber threats, and this situation may lead to serious threats that can endanger national security. This study aims to develop an artificial intelligence-based approach that allows for early and reliable detection of cyber attacks that may be carried out against SCADA systems. Within the scope of this study, a scaled model of a hydroelectric power plant's SCADA communication architecture was physically designed, and a suitable test environment was established for this structure. In this test environment, in order to ensure the control of the SCADA system and the monitoring of the processes, in addition to the non-attack scenario, three different cyber attack scenarios were implemented over the local network: Man-in-the-Middle (MITM), which aims to disrupt data integrity; Denial of Service (DoS), which targets the consumption of system resources; and Command Injection, which aims to modify control commands through external intervention. Cyber attack tests were carried out while the process designed for the system's operation was running in continuous mode. The network traffic generated as a result of the application of the scenarios was recorded using the Wireshark tool; then, data preprocessing steps were performed to obtain a labeled data set created specifically for this study. Basic machine learning algorithms such as K-Nearest Neighbors (KNN), Naive Bayes (NB), Decision Tree (DT) and Logistic Regression (LR), as well as binary and ternary hybrid combinations of these methods were applied on the data set obtained as a result of the scenarios. As a result of the analyses performed, the hybrid model created by combining Decision Tree and Logistic Regression algorithms showed the most successful performance with 98,29% accuracy rate and 0,998 Area Under the Curve (AUC) value. The findings show that the developed model not only detects the presence of attacks but also classifies different attack types with high accuracy and in this respect, it can contribute to the timely and reliable determination of cyber threats to SCADA systems.

Science Code : 93438
Key Words : SCADA, cyber attack, cyber-physical system, cyber security, artificial intelligence and machine learning
Page Number : 109
Supervisor : Prof. Dr. Şevki DEMİRBAŞ

TEŞEKKÜR

Lisansüstü eğitimim süresince bilgi ve tecrübesiyle akademik gelişimime katkıda bulunan, tez çalışmam boyunca özverili desteğini ve sabrını esirgemeyen değerli danışman hocam Sayın Prof. Dr. Şevki DEMİRBAŞ'a; deneysel çalışmalarımın gerçekleşmesine olanak sağlayan ve süreç boyunca teknik destekleriyle katkıda bulunan Elektrik Elektronik Mühendisi Erkan AKKÖSE ile Bilgisayar Mühendisi Fatih İZGİ'ye en içten teşekkürlerimi sunarım. Tez sürecim boyunca sabrıyla, anlayışıyla ve desteğiyle her zaman yanımda olan ve motivasyonumu korumama katkı sağlayan sevgili eşime; günlere gelmemi sağlayan ve benim için hiçbir fedakârlıktan kaçınmayan kıymetli anneme ve babama; fikir alışverişi yapmak için zaman ayıran ve katkılarıyla sürece değer katan tüm arkadaşlarıma, hocalarıma ve desteğini esirgemeyen amirlerime teşekkür etmeyi bir borç bilirim.

İÇİNDEKİLER

	Sayfa
ÖZET	iv
ABSTRACT.....	v
TEŞEKKÜR.....	vi
İÇİNDEKİLER	vii
ÇİZELGELERİN LİSTESİ.....	x
ŞEKİLLERİN LİSTESİ.....	xii
SİMGELER VE KISALTMALAR.....	xiv
1. GİRİŞ.....	1
2. LİTERATÜR TARAMASI	9
3. TEORİK ALTYAPI.....	21
3.1. SCADA Sistemleri	21
3.1.1. SCADA sistemi ana bileşenleri.....	21
3.1.2. Endüstriyel sistemlerde kullanılan SCADA iletişim protokolleri.....	22
3.2. Veri Haberleşme Teknolojileri	24
3.2.1. Ethernet	24
3.2.2. Yerel alan ağları	25
3.3. Ağ Topolojileri	25
3.3.1. Doğrusal (Bus) topoloji.....	26
3.3.2. Yıldız (Star) topoloji	26
3.3.3. Halka (Ring) topoloji	27
3.3.4. Ağaç (Tree) topoloji.....	28
3.3.5. Karmaşık (Mesh) topoloji	28
3.4. Kullanılan Haberleşme Protokolü Güvenlik Açıkları.....	29
3.5. EKS/SCADA Sistemlerine İlişkin Siber Saldırıları	30

	Sayfa
3.5.1. MITM saldırıları.....	31
3.5.2. DoS saldırıları	33
3.5.3. Komut enjeksiyonu saldırıları	35
3.6. Kullanılan Makine Öğrenmesi Tabanlı Modeller.....	36
3.6.1. KNN modeli	37
3.6.2. NB modeli	39
3.6.3. DT modeli	40
3.6.4. LR modeli.....	42
3.6.5. KNN-NB hibrit modeli.....	43
3.6.6. DT-LR hibrit modeli	43
3.6.7. KNN-NB-DT hibrit modeli.....	44
4. MATERYAL VE METOT	45
4.1. Fiziksel Test Ortamı	45
4.2. Siber Saldırı Senaryolarının Test Ortamında Uygulanması	55
4.3. Veri Kümesi Oluşturma Süreci.....	57
4.4. Siber Saldırı Tespitinde Kullanılan Makine Öğrenmesi Performans Metrikleri	59
4.5. Siber Saldırı Tespiti İçin Makine Öğrenmesi Modelleri	62
4.5.1. Analize uygun veri kümesi yapılandırması.....	63
4.5.2. Uygulanan sınıflandırma modelleri.....	66
5. SONUÇLAR VE ÖNERİLER	93
5.1. Deneysel Sonuçlar	93
5.2. Tartışma ve Sınırlılıklar.....	95
5.2.1. Tartışma.....	95
5.2.2. Sınırlılıklar	96
5.3. Sonuç	96
5.4. Öneriler	97

Sayfa

KAYNAKLAR	99
ÖZGEÇMİŞ	109



ÇİZELGELERİN LİSTESİ

Çizelge	Sayfa
Çizelge 1.1. Enerji sektörüne yönelik gerçekleşmiş büyük siber-fiziksel saldırılar.....	3
Çizelge 3.1. KNN modelinin avantajları ve dezavantajları	39
Çizelge 3.2. NB modelinin avantajları ve dezavantajları	40
Çizelge 3.3. Karar ağacı modelinin avantajları ve dezavantajları	42
Çizelge 3.4. Lojistik regresyon modelinin avantajları ve dezavantajları	43
Çizelge 4.1. Test ortamında kullanılan ekipmanlar ve açıklamaları	46
Çizelge 4.2. Ağ trafiği istatistiksel özeti ve senaryo bazlı karşılaştırma.....	56
Çizelge 4.3. Veri kümesi için belirlenen özellikler ve açıklamaları.....	57
Çizelge 4.4. Karışıklık (Confusion) matrisi.....	59
Çizelge 4.5. KNN modeli test metrikleri.....	68
Çizelge 4.6. KNN modeline ait sınıf bazlı tahmin süreleri	69
Çizelge 4.7. KNN modelinin karmaşıklık matrisi verilerine göre performansı	70
Çizelge 4.8. NB modeli test metrikleri.....	72
Çizelge 4.9. NB modeline ait sınıf bazlı tahmin süreleri	72
Çizelge 4.10. NB modelinin karmaşıklık matrisi verilerine göre performansı	73
Çizelge 4.11. DT modeli test metrikleri	76
Çizelge 4.12. DT modeline ait sınıf bazlı tahmin süreleri.....	76
Çizelge 4.13. DT modelinin karmaşıklık matrisi verilerine göre performansı.....	77
Çizelge 4.14. LR modeli test metrikleri	79
Çizelge 4.15. LR modeline ait sınıf bazlı tahmin süreleri.....	80
Çizelge 4.16. LR modelinin karmaşıklık matrisi verilerine göre performansı.....	81
Çizelge 4.17. KNN-NB hibrit modeli test metrikleri	83
Çizelge 4.18. KNN-NB hibrit modeline ait sınıf bazlı tahmin süreleri.....	83
Çizelge 4.19. KNN-NB hibrit modelinin karmaşıklık matrisi verilerine göre performansı.....	84

Çizelge	Sayfa
Çizelge 4.20. DT-LR hibrit modeli test metrikleri	86
Çizelge 4.21. DT-LR hibrit modeline ait sınıf bazlı tahmin süreleri.....	86
Çizelge 4.22. DT-LR hibrit modelinin karmaşıklık matrisi verilerine göre performansı.....	87
Çizelge 4.23. KNN-NB-DT hibrit modeli test metrikleri.....	89
Çizelge 4.24. KNN-NB-DT hibrit modeline ait sınıf bazlı tahmin süreleri	89
Çizelge 4.25. KNN-NB-DT hibrit modelinin karmaşıklık matrisi verilerine göre performansı.....	90
Çizelge 5.1. Sınıflandırma modelleri performans karşılaştırma tablosu (ortalama)	93

ŞEKİLLERİN LİSTESİ

Şekil	Sayfa
Şekil 1.1. Çalışmanın genel organizasyon şeması.....	8
Şekil 3.1. SCADA sistemi ana bileşenleri.....	22
Şekil 3.2. SCADA iletişim protokollerinin kullanım oranları	24
Şekil 3.3. Doğrusal (Bus) topoloji.....	26
Şekil 3.4. Yıldız (Star) topoloji	27
Şekil 3.5. Halka (Ring) topoloji	27
Şekil 3.6. Ağaç (Tree) topoloji.....	28
Şekil 3.7. Karmaşık (Mesh) topoloji	29
Şekil 3.8. Normal ağ trafiği ve MITM saldırısı ağ trafiği	33
Şekil 3.9. DoS saldırısı şematik gösterimi	35
Şekil 3.10. Komut enjeksiyonu saldırısının şematik gösterimi	36
Şekil 3.11. Makine öğrenmesi süreci	37
Şekil 3.12. KNN modelinin temel çalışma mantığı	39
Şekil 3.13. Karar ağacı modelinin temel çalışma mantığı örneği	41
Şekil 3.14. Lojistik regresyon modeli temel çalışma prensibi	43
Şekil 4.1. Test ortamında kullanılan ekipmanların gösterimleri	48
Şekil 4.2. TIA Portal genel arayüzü	49
Şekil 4.3. Test ortamının mimari yapısı	51
Şekil 4.4. SCADA sistemindeki komutların modellenmesine ilişkin ekran görüntüleri.....	52
Şekil 4.5. Fiziksel test ortamına ait sistemin blok diyagramı.....	53
Şekil 4.6. Deneysel çalışma yapılan tüm test ortamının görünümü	53
Şekil 4.7. Wireshark yazılımı ile kaydedilen ağ trafiğine ait paket yakalama ekranı ..	54
Şekil 4.8. ROC eğrisi örneği	62
Şekil 4.9. Veri hazırlama ve modelleme süreci.....	66

Şekil	Sayfa
Şekil 4.10. KNN modeli temel çalışma prensibi.....	67
Şekil 4.11. Komşu sayısı (k) değerine bağlı olarak doğrulama başarımının değişimi...	68
Şekil 4.12. KNN modeli karmaşıklık matrisi.....	69
Şekil 4.13. KNN modeli her sınıf için ROC eğrileri.....	70
Şekil 4.14. Naive Bayes algoritması temel çalışma prensibi	71
Şekil 4.15. Naive Bayes modeli karmaşıklık matrisi	73
Şekil 4.16. Naive Bayes modeli her sınıf için ROC eğrileri	74
Şekil 4.17. Karar ağacı öğrenme süreci.....	75
Şekil 4.18. Karar ağacı modeli karmaşıklık matrisi	76
Şekil 4.19. Karar ağacı modeli her sınıf için ROC eğrileri	78
Şekil 4.20. Lojistik regresyon temel çalışma prensibi	79
Şekil 4.21. Lojistik regresyon modeli karmaşıklık matrisi	80
Şekil 4.22. Lojistik regresyon modeli her sınıf için ROC eğrileri	82
Şekil 4.23. KNN-NB hibrit modeli karmaşıklık matrisi	83
Şekil 4.24. KNN-NB hibrit modeli her sınıf için ROC eğrileri	85
Şekil 4.25. DT-LR hibrit modeli karmaşıklık matrisi	87
Şekil 4.26. DT-LR hibrit modeli her sınıf için ROC eğrileri	88
Şekil 4.27. KNN-NB-DT hibrit modeli karmaşıklık matrisi.....	89
Şekil 4.28. KNN-NB-DT hibrit modeli her sınıf için ROC eğrileri.....	91
Şekil 5.1. DT-LR modeli için eğitim ve doğrulama metriklerinin sınıf bazlı görsel analizi	94

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler

Açıklamalar

%	Yüzde
csv	Comma-Separated Values (Virgülle Ayrılmış Değerler)
Mbps	Megabits Per Second (Saniye Başına Megabit)
ms	Milisaniye

Kısaltmalar

Açıklamalar

ACK	Acknowledgement (Alındı Bildirimi)
AGA	American Gas Association (Amerikan Gaz Birliği)
ANN	Artificial Neural Network (Yapay Sinir Ağları)
ANOVA	Analysis of Variance (Varyans Analizi)
ARP	Address Resolution Protocol (Adres Çözümleme Protokolü)
AUC	Area Under the Curve (Eğri Altındaki Alan)
BT	Bilgi Teknolojileri
CART	Classification and Regression Trees (Sınıflandırma ve Regresyon Ağaçları)
DC	Direct Current (Doğru Akım)
DDoS	Distributed Denial of Service (Dağıtık Hizmet Engelleme Saldırısı)
DHCP	Dynamic Host Configuration Protocol (Dinamik Ana Bilgisayar Yapılandırma Protokolü)
DIX	Digital/Intel/Xerox
DNP3	Distributed Network Protocol Version 3.0 (Dağıtık Ağ Protokolü Sürüm 3.0)
DNS	Domain Name System (Alan Adı Sistemi)

Kısaltmalar**Açıklamalar**

DoS	Denial of Service (Hizmet Engelleme Saldırısı)
DT	Decision Tree (Karar Ağacı)
EKS	Endüstriyel Kontrol Sistemleri
FNN	Feedforward Neural Network (İleri Beslemeli Sinir Ağı)
FPR	False Positive Rate (Yanlış Pozitif Oranı)
GNB	Gaussian Naive Bayes
HES	Hidroelektrik Santral
HMI	Human Machine Interface (İnsan Makine Arayüzü)
HMM	Hidden Markov Models (Gizli Markov Modelleri)
HNA-NN	Hierarchical Neuron Architecture based Neural Network (Hiyerarşik Nöron Mimarisi Tabanlı Sinir Ağı)
ICMP	Internet Control Message Protocol (İnternet Denetim Mesaj Protokolü)
ID3	Iterative Dichotomizer 3 (Yinelemeli İkili Ayırıcı 3)
IEEE	Institute of Electrical and Electronics Engineers (Elektrik ve Elektronik Mühendisleri Enstitüsü)
IP	Internet Protocol (İnternet Protokolü)
IWP-CSO	Intrusion Weighted Particle based Cuckoo Search Optimization (Yetkisiz Erişim Ağırlıklı Parçacık Tabanlı Guguk Kuşu Arama Optimizasyonu)
KNN	K-Nearest Neighbors (K-En Yakın Komşular)
LAN	Local Area Network (Yerel Alan Ağı)
LASSO	Least Absolute Shrinkage and Selection Operator (En Küçük Mutlak Daraltma ve Seçim Operatörü)
LR	Lojistik Regresyon (Lojistik Regresyon)
LSTM	Long Short-Term Memory (Uzun Kısa Süreli Bellek)
MAC	Media Access Control (Ortam Erişim Kontrolü)
MDB	Merkezi Denetleyici Birimi
MITM	Man in the Middle (Ortadaki Adam Saldırısı)
MSU	Mississippi State University (Mississippi Eyalet Üniversitesi)

Kısaltmalar	Açıklamalar
NB	Naive Bayes
PI	Profibus International
PLC	Programmable Logic Controller (Programlanabilir Lojik Kontrolör)
PROFINET	Process Field Network
RF	Random Forest (Rastgele Orman)
RILS	Recursively Iterated Least Squares (Yinelemeli En Küçük Kareler)
ROC	Receiver Operating Characteristic (Alıcı İşletim Karakteristik Eğrisi)
SCADA	Supervisory Control and Data Acquisition (Denetleyici Kontrol ve Veri Toplama Sistemi)
STS	Saldırı Tespit Sistemi
SVM	Support Vector Machine (Destek Vektör Makinesi)
SVMSMOTE	Support Vector Machine Synthetic Minority Over-sampling Technique (Destek Vektör Makinesi Sentetik Azınlık Aşırı Örnekleme Tekniği)
SWaT	Secure Water Testbed (Güvenli Su Test Ortamı)
SYN	Synchronize (Eşzamanlama)
TCP	Transmission Control Protocol (İletim Denetimi Protokolü)
TIA	Totally Integrated Automation (Tam Entegre Otomasyon)
TNT	Trinitrotoluene (Trinitrotoluen)
TPR	True Positive Rate (Doğru Pozitif Oranı)
UDP	User Datagram Protocol (Kullanıcı Veri Paket Protokolü)
UUB	Uzak Uç Birimleri
VPN	Virtual Private Network (Sanal Özel Ağ)
WPA	Wi-Fi Protected Access (Wi-Fi Korumalı Erişim)
WPA2	Wi-Fi Protected Access 2 (Wi-Fi Korumalı Erişim 2)
YZ	Yapay Zekâ

1. GİRİŞ

Günümüzde dijital teknolojilerin yaygınlaşması ve karmaşıklaşmasıyla birlikte siber güvenlik, bireylerin, kurumların ve devletlerin varlıklarını koruma ihtiyacını karşılamak üzere gelişen önemli bir alan haline gelmiştir. Uluslararası Telekomünikasyon Birliği, siber güvenlik kavramını, siber ortamda bulunan bilgi ve sistemlerini korumak için kullanılabilecek araçlar, politikalar, güvenlik kavramları ve önlemleri, eylemler, risk yönetimi stratejileri, eğitim, en etkili yöntemler, altyapı ve teknolojilerin kompleks bir bütünü olarak ifade etmektedir [1]. Genel olarak siber güvenlik, bilgi sistemlerinin ve sistemlerde bulunan verilerin, yasadışı erişimden, saldırılardan ve kötüye kullanımdan korunmasını amaçlamaktadır [2]. Çeşitli saldırı yöntemlerini kullanarak tespit ettikleri zafiyetleri kendi amaçları doğrultusunda kullanmak isteyen saldırganlar için özellikle kritik altyapılar hedef haline gelmiştir.

Kritik altyapılar, bir ülkenin veya kurumun varlığını ve işleyişini sürdürmesi için gerekli olan temel sistemleri ve tesisleri ifade etmektedir. Su, enerji, ulaşım, finans, iletişim ağları, gıda tedarik zincirleri, sağlık hizmetleri ve güvenlik kurumları gibi temel sistemler ve tesisler kritik altyapıları oluşturmaktadır. Kritik enerji altyapısı ise elektrik santralleri, iletim hatları, dağıtım şebekeleri, depolama tesisleri, petrol ve doğal gaz boru hatları ve diğer ilgili tesisler gibi enerjinin üretimi, iletimi, dağıtımı, tedariki ve depolanmasında kullanılan tüm sistemleri temsil etmektedir. Bu sistemler, zorlu fiziksel koşullarda uzun süreli ve kesintisiz çalışacak şekilde tasarlanmış bileşenlerden oluşmaktadır. Kritik altyapıların lokal ve uzak sahalardaki bileşenlerini izleme ve kontrol etmek için Denetleyici Kontrol ve Veri Toplama (Supervisory Control and Data Acquisition – SCADA) sistemleri kullanılmaktadır [3].

SCADA; üretim tesisi ya da fabrika gibi önemli alt yapıların herhangi birinde sistem erişimine sahip bir operatörün uzaktan ayar noktalarını değiştirebilmesine, vana veya anahtarların durumlarını değiştirebilmesine, alarm durumlarını izlemesine ve ölçüm verilerini toplamasına olanak tanıyan bir sistemdir. Otomasyon teknolojisinin perspektifine göre ise SCADA, kontrol edilmek istenen sisteme özel işlemler içeren, fiziksel çevredeki yapılarla iletişim kurabilen ve hesaplamalar gerçekleştirebilen sistemler olarak tanımlanmaktadır [3]. Örneğin, belediyelerin şebeke suyu dağıtım tesislerinde bulunan tanklardaki su seviyelerini, sıcaklığını ve boru basıncını izlemek için SCADA sistemleri kullanılmaktadır [4].

SCADA sistemleri farklı operasyonel alanlarda kullanıma bakılmaksızın temel olarak Merkezi Denetleyici Birimi (MDB), Uzak Uç Birimleri (UUB) ve haberleşme ağı olmak üzere 3 ana bileşenden oluşmaktadır [4]. Her bir bileşenin kendine özgü görevi bulunmakla birlikte hizmet edilen amaca göre bileşen sayısı ve çeşitliliği sağlanmaktadır. MDB, sistemin durumunun sürekli olarak gözlemlendiği ve herhangi bir aksaklık veya anormallik durumunda sisteme müdahale edilen yerdir. UUB, gözlemlenen sistemle ilgili verileri toplayarak bunları kaydetmekte ve gerektiğinde bu verileri MDB'ye iletmektedir. MDB, verilerin kaydedilmesi ve ilgili bileşene komut gönderilmesi gibi işlevleri de yerine getirmektedir.

Endüstriyel Kontrol Sistemlerinin (EKS) kontrol ve izleme sistemlerine yönelik gerçekleşen fiziksel ve siber saldırılar, sistemlerin yetkisiz kişilerce kontrolünün ele geçirilmesine, işleyişinin ve fonksiyonunun değiştirilmesine veya bozulmasına neden olabilecek ciddi güvenlik riskleri oluşturmaktadır [5]. Dolayısıyla, SCADA sistemlerinin güvenliğinin sağlanması kritik öneme sahiptir. SCADA sistemlerinin siber güvenliği, siber saldırılar sonucunda oluşabilecek hizmet kesintilerinin potansiyel olarak yıkıcı sonuçları ve günlük yaşamın işleyişini bozması nedeniyle diğer sistemlere göre daha dikkat çekici olmaktadır [6]. SCADA sistemlerinin kritik altyapılar için oldukça maliyetli olmasından ötürü söz konusu saldırıların neden olabileceği kesintilerin önlenmesi, hem kuruluşun hem de hizmetten yararlanan toplumun güvenliği açısından SCADA sistemlerine yönelik güvenlik tedbirlerinin alınmasını zorunlu kılmaktadır. Aslında bir nevi, kritik altyapıların güvenliğinin sağlanması SCADA sistemlerini korumaktan geçmektedir [3].

Kritik altyapılarda kullanılan SCADA sistemlerine yönelik yapılan saldırılar, siber terör faaliyetleri olarak değerlendirilebilir [4]. Kritik altyapılardan olan elektrik üretim, iletim ve dağıtım sistemlerini hedef alarak gerçekleştirilen siber saldırılar, elektrik, gaz ve ısı gibi hizmetleri etkileyerek enerji kesintilerine neden olabilmektedir. Enerji kesintilerine sebebiyet veren siber saldırılar, ülkelerde toplumsal ve ekonomik düzeni bozucu nitelikte ciddi bir kaos ortamına yol açabilmektedir. Çizelge 1.1, son zamanlarda dünya çapında enerji sektörünü hedef alan siber saldırıların bir yelpazesini sunmaktadır.

Çizelge 1.1. Enerji sektörüne yönelik gerçekleşmiş büyük siber-fiziksel saldırılar

Sıra No	Yıl	Konum	Saldırıya Uğrayan Bileşenler	Saldırı Türü	Etkisi	Referans
1	1982	Rusya	Gaz boru hattı kontrol sistemi yazılımı	Kod manipülasyonu	Gaz boru hattı kontrol yazılımına yerleştirilen mantık bombası, 3 kiloton TNT (Trinitrotoluene) eşdeğeri bir patlamaya neden oldu. Saldırı, dışarıdan herhangi bir bağlantı olmaksızın, sistem içine sızdırılan zararlı yazılım ile belirli bir koşul gerçekleştiğinde yerel ağ üzerinden tetiklendi.	[7]
2	1999	Bellingham, Amerika Birleşik Devletleri	Bir benzin boru hattının SCADA sistemi	Güvenliksiz SCADA veritabanı müdahalesi	SCADA sistem yöneticisi tarafından sisteme yapılan veri girişi sırasında oluşan yazılımsal hatalar, sistemin kontrol komutlarına yanıt vermemesine yol açtı. Dışarıdan herhangi bir saldırı olmadan, içerden gerçekleşen bu zafiyet sonucunda 237.000 galon benzin sızarak patladı; 3 kişi öldü, 8 kişi yaralandı.	[8, 9]
3	2003	Ohio, Amerika Birleşik Devletleri	Nükleer santral kontrol sistemi	Kötü amaçlı yazılım enjeksiyonu	Santral için çalışan bir danışmanın bilgisayarına bulaşan Slammer solucanı, bu bilgisayarın santralin yerel ağına olan bağlantısı üzerinden kontrol sistemine yayıldı. Parametre görüntüleme sistemi 5 saat boyunca kapandı.	[9, 10]
4	2007	Idaho Ulusal Laboratuvarı, Amerika Birleşik Devletleri	Dizel jeneratörün devre kesicisi	Yanlış veri enjeksiyonu	Jeneratör patladı.	[11]
5	2008	Türkiye	Petrol boru hattının kontrol sistemi	Yanlış veri enjeksiyonu	Petrol patlaması gerçekleşti ve 30 bin varil suya karıştı.	[9, 12]
6	2010	İran	Nükleer santral SCADA sistemi	Kötü amaçlı yazılım enjeksiyonu	USB bellek aracılığıyla yerel ağ üzerinden sisteme bulaştırılan Stuxnet solucanı, İran'daki bir uranyum zenginleştirme tesisini enfekte etti.	[13, 14]
7	2011	Macaristan (ilk tespit), Avrupa merkezli hedef	MS Windows tabanlı kontrol sistemleri	Bilgi hırsızlığı(Duqu)	Stuxnet'e benzer şekilde yerel ağ ortamında faaliyet göstermiştir. Fiziksel hasar vermemiştir. Bulaştığı sistemlerde tuş kaydı yapma, ekran görüntüsü alma ve yapılandırma dosyalarını arşivleme gibi işlevler gerçekleştirmiştir.	[15]
8	2012	Suudi Arabistan ve Katar	Aramco ve RasGas	Kötü amaçlı yazılım enjeksiyonu	Enerji üretimi ve dağıtımını etkilenmiştir.	[9]
9	2015	Ukrayna	3 dağıtım şirketinin kesicileri	Yanlış veri enjeksiyonu	Birkaç saat boyunca 225 bin müşteri hizmetsiz kaldı.	[11]
10	2016	Ukrayna	İletim trafo merkezi kontrol sistemleri	Kötü amaçlı yazılım enjeksiyonu	Gece saatlerinde güç kullanımında beşte bir azalma oldu.	[9]

Çizelge 1.1. (devam) Enerji sektörüne yönelik gerçekleşmiş büyük siber-fiziksel saldırılar

Sıra No	Yıl	Konum	Saldırıya Uğrayan Bileşenler	Saldırı Türü	Etkisi	Referans
11	2017	Suudi Arabistan Petrol Rafinerisi	Bir elektrik santralının güvenlik sistemleri	Kötü amaçlı yazılım enjeksiyonu	Tesisin acil durum kapatma sistemini harekete geçirmek için tetikledi.	[13]
12	2019	Power Utilities@ California & Wyoming, Amerika Birleşik Devletleri	İletişim ağı	Hizmet engelleme	Kısa bir süre için elektrik sisteminin işleyişi kesintiye uğradı, ancak bu bir elektrik kesintisine neden olmadı.	[9, 13]
13	2019	Kudankulam Nükleer Santrali, Tamil Nadu, Hindistan	Santraldeki sistemler	Ortadaki adam saldırısı	Etkilenen sistemler hayati iç ağdan ayrıldı ve sistemin geri kalan işlevselliği etkilenmedi.	[13]
14	2022	Ukrayna	SCADA altyapısı	Industroyer2 zararlı yazılımı ile altyapı sabotajı	İşgal öncesi ve sonrasında enerji altyapısını hedef alan saldırılarda artış tespit edildi. Kritik altyapıya yönelik operasyonel tehdit oluşturdu.	[16]

Bu tür kesintilere maruz kalan ülkelerde, kritik altyapı sistemlerinde meydana gelen aksamaların ne kadar kritik olduğu anlaşılmıştır. Ülkelerdeki kritik altyapıların siber güvenliğinin sağlanmasında milyonlarca insanın temel hizmetlere (su, elektrik, doğalgaz vb.) ulaşımının otomatik kontrolünü ve uzaktan yönetimini sağlayan SCADA sistemlerinin güvenliğinin sağlanması kritik önem taşımaktadır [3]. Bu sistemlerin güvenlik zafiyetlerinin araştırılması ve giderilmesi, kritik altyapıların siber güvenliğinin sağlanması için gerekli bir ön koşul olmakla birlikte siber saldırı tespiti ve engellenmesi, kritik altyapılardaki siber güvenlik stratejilerinin temel taşlarından biridir. Siber saldırı tespit ve engelleme sistemlerinin geliştirilmesi ülkelerin kritik altyapılarının siber tehditlere karşı direncini artırarak kritik sistemlerin sürekliliğine önemli bir katkıda bulunacaktır.

EKS veya SCADA sistemlerinin temel bileşenleri arasında veri alışverişini sağlamak için özelleştirilmiş haberleşme protokolleri kullanılmaktadır [17]. Endüstriyel otomasyon alanında yaygın olarak kullanılan protokollerden biri de Process Field Network (PROFINET) protokolüdür [18]. PROFINET protokolü, farklı protokolleri destekleyen cihazlarla aynı fiziksel ağ altyapısını paylaşarak entegrasyon ve işletim kolaylığı sağlarken yetkisiz erişim ve program tabanlı saldırılar açısından güvenlik riskleri barındırmaktadır. Haberleşme protokollerinin siber güvenlik analizi yapıldığında, bir dizi güvenlik açığının

mevcut olduğu bilinmektedir. Geniş bir kullanım alanına sahip olan PROFINET protokolüne, güvenlik açıklarından faydalanılarak siber saldırı gerçekleştirilmesi muhtemeldir [19]. PROFINET protokolündeki güvenlik açıklarının sömürülmesiyle gerçekleştirilebilecek siber saldırılar, saldırının amacına ve şiddetine bağlı olarak verilerin ele geçirilmesi, SCADA sistemlerinin kontrol edilmesi ve devre dışı bırakılması gibi farklı olumsuz sonuçlara yol açabilir. Bu nedenlerden dolayı kritik altyapılarda kullanılan PROFINET protokolünün siber güvenliğinin sağlanması ile ilgili çalışmaların yapılması, kritik altyapıların potansiyel tehditlere karşı istikrarını ve bütünlüğünü korumak açısından önem arz etmektedir.

Günümüzde kritik altyapılarda, siber savunma alanındaki süreçlerin hızı ve kullanılan veri miktarı katlanarak artmaktadır. Bu durum, salt insan gücüyle etkin bir savunma yapmayı imkânsız hale getirmektedir. Siber saldırıların karmaşıklığı ve dinamizmi arttıkça, klasik sabit algoritmalar ile yazılım geliştirmenin siber savunmada etkin bir çözüm olarak yetersiz kaldığı açıkça görülmektedir [20]. Bu bağlamda, SCADA sistemleri siber saldırı tespit çalışmalarında Yapay Zekâ (YZ) tabanlı yöntemler kullanılabilir. Potansiyel tehditleri erken aşamada tespit etmeye ve tanımlamaya yönelik çalışmalar SCADA sistemlerinin güvenliğini ve kritik altyapının korunmasını sağlamada önemli bir rol oynayarak SCADA sistemlerinin siber güvenliğine katkı sağlayabilir. Kritik altyapıların güvenliğini sağlamak için, SCADA sistemlerine yönelik farklı siber saldırıları önceden yüksek başarıyla tespit edebilecek yapay zekâ tabanlı metodolojiler geliştirmek büyük önem arz etmektedir. Bu araştırmada, siber güvenlik alanındaki çalışmalara katkıda bulunmak amacıyla bir Hidroelektrik Santral (HES) SCADA haberleşme mimarisi, donanım ve yazılım bileşenleri modellenmiştir. Modelleme aşamasında fiziksel ve siber süreçlerin işlenmesini mümkün kılan bir test ortamı oluşturulmuştur. Bu test ortamı, bir hidroelektrik santralin SCADA haberleşme mimarisinin basitleştirilmiş bir modelini sunmaktadır. Siber fiziksel ortam sunan test ortamında endüstriyel ağ anahtarları, programlanabilir lojik kontrolör (Programmable Logic Controller – PLC), dijital giriş veya dijital çıkış işlemleri gerçekleştiren unsurlar gibi tipik bir hidroelektrik santralin SCADA sistemlerinde yaygın olarak tercih edilen bileşenler kullanılmıştır. Hidroelektrik santrallerin SCADA haberleşme mimarisine benzetim yapılarak dışarıya kapalı olan halka (ring) şeklinde bir iletişim ağı oluşturulmuştur. Bu ağ oluşturulurken SCADA sistemlerinde sıklıkla kullanılan PROFINET protokolü ve kablolu bağlantılar kullanılmıştır. Literatürde, halka topolojisinin endüstriyel tesislerde, kurumsal ağlarda, ulaşım sistemlerinde ve yerel düzeydeki kritik altyapılarda uygulama alanı bulduğu

belirtilmektedir [21]. Guilherme ve arkadaşlarının çalışması, halka topolojisinin endüstriyel üretim hatlarında uygulandığını göstermekte ve bu yapı üzerinden büyük bir Profinet ağını değerlendirmektedir [22]. Bu bağlamda, test ortamında tercih edilen halka yapısı, sahadaki uygulamalara benzer ve gerçekçi bir benzetim sunmaktadır. Veri iletimi ve komutların merkezi birim ile uç birimler arasında iletilmesi sağlanmış ve sistemin çalışması fiziksel olarak gözlenmiştir. Sistemin fiziksel fonksiyonlarını aksatmak, operasyonel süreçlerine zarar vermek ve olası siber saldırılar karşısındaki tepkisini değerlendirmek amacıyla test ortamında yetkisiz komut enjeksiyonu saldırısı, ortadaki adam saldırısı ve hizmet engelleme saldırısı uygulanarak analizler gerçekleştirilmiştir. Test ortamının siber güvenliğinin sağlanabilmesi için, gerçekleştirilen saldırıların tespit edilmesi gereklidir. Bu doğrultuda, normal çalışma koşullarına ve farklı saldırı senaryolarına ait ağ trafiği izlenmiş ve kaydedilerek analiz edilmiştir. Kaydedilen ağ trafik paketlerinin analiz edilmesi ve yalnızca saldırı olup olmadığının değil, aynı zamanda saldırının türünün de belirlenebilmesi amacıyla denetimli makine öğrenmesi algoritmaları kullanılmıştır. Çalışma kapsamında normal durum senaryosu ile birlikte üç farklı siber saldırı senaryosu (MITM, DoS ve Komut Enjeksiyonu) sınıflandırılarak saldırı tespiti gerçekleştirilmiştir. Bu amaçla, yedi farklı makine öğrenmesi algoritması değerlendirilmiştir. Temel sınıflandırma yöntemleri olan K-Nearest Neighbors (KNN), Naive Bayes (NB), Decision Tree (DT) ve Lojistik Regresyon (LR) modellerine ek olarak, bu yöntemlerin ikili ve üçlü hibrit kombinasyonları (KNN-NB, DT-LR, KNN-NB-DT) kullanılarak kapsamlı bir analiz gerçekleştirilmiştir. Elde edilen sonuçlara göre, yüksek doğruluk oranlarına ulaşan modeller bu çalışma için önerilmiştir.

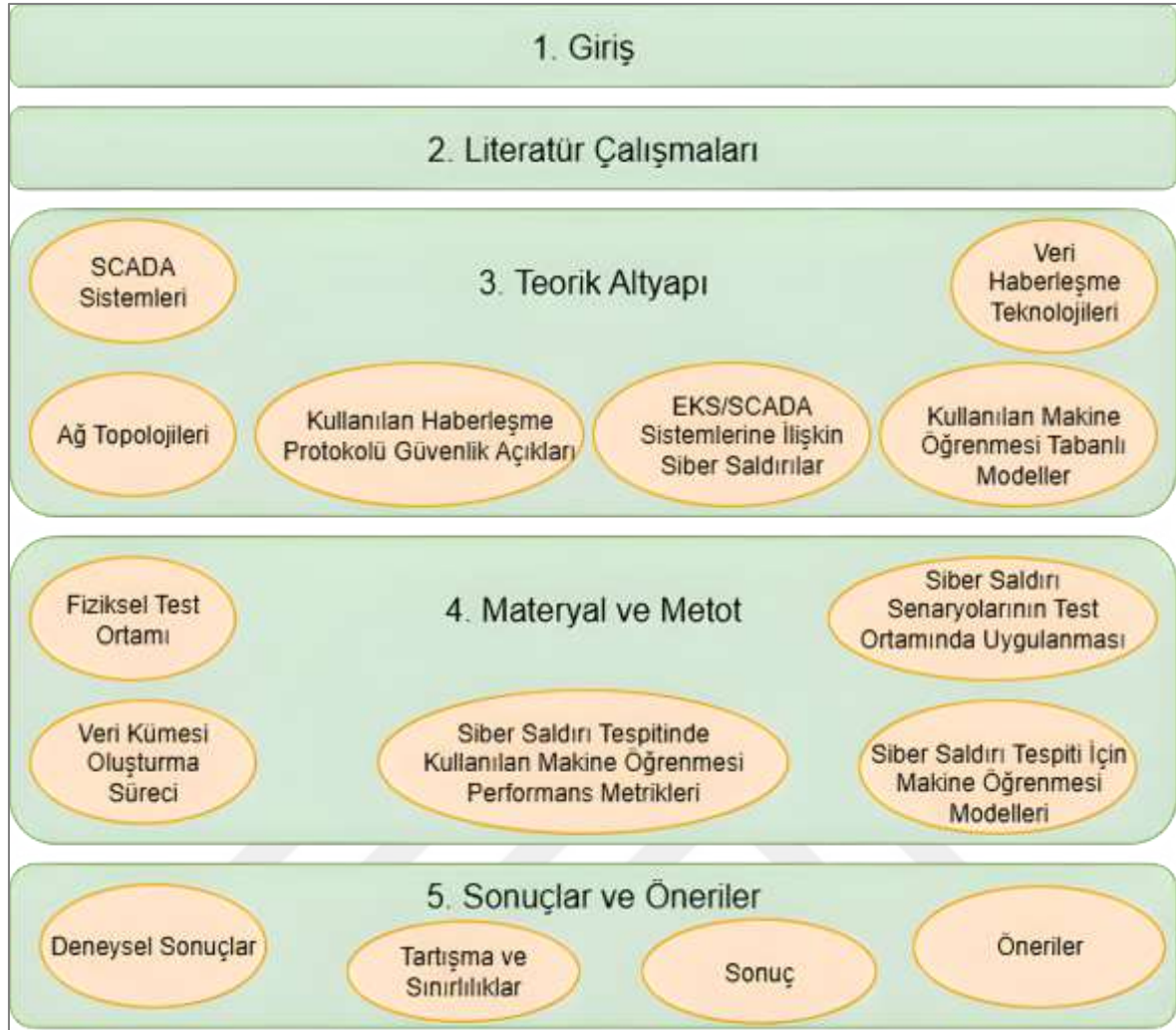
Bu çalışmada, SCADA sistemlerinin siber güvenliğini değerlendirmek amacıyla gerçekçi bir test ortamında oluşturulan özgün veri kümesi üzerinden, saldırı türlerini sınıflandırmaya yönelik uygun makine öğrenmesi modellerini belirlemek hedeflenmiştir.

Bu tez çalışmasının literatüre katkıları aşağıdaki şekilde özetlenebilir:

- Kritik altyapılarda kullanılan SCADA sistemlerinin çalışma şeklinin fiziksel olarak gösterilmesi ve siber saldırı testlerinin bu fiziksel ortamda gerçekleştirilmesi için bir test ortamı oluşturulmuştur. Literatürde bu konu ile ilgili çalışmalarda fiziksel test yatakları bulunmakla birlikte genellikle simülasyonlar üzerinde yoğunlaşmıştır. Fiziksel ortamda yapılan çalışma sayısı kısıtlıdır. Bu nedenle, kullanılan donanım, yazılım ve bileşenlerle siber fiziksel ortam hazırlanarak literatürdeki bu boşluğu gidermek amaçlanmıştır.

- Hidroelektrik santrallerin SCADA haberleşme yapısı modellenerek, PROFINET protokolüne özgü dışa kapalı halka topolojisine sahip bir test ortamı oluşturulmuştur.
- Test ortamına MITM, DoS ve Komut Enjeksiyonu saldırıları uygulanarak sistem üzerindeki etkileri anlık olarak incelenmiş, normal çalışma koşullarında ve siber saldırı altındaki durumlarda ağ trafiği verileri toplanarak analiz edilmiştir.
- Literatürde yaygın olarak kullanılan hazır veri kümelerinin aksine, bu çalışmada SCADA sistemlerine özgü, protokol ve donanım temelli özgün ve etiketli bir veri kümesi oluşturulmuştur.
- Saldırıların yalnızca tespit edilmesi değil aynı zamanda saldırı türlerinin sınıflandırılması hedeflenmiş ve bu amaçla yedi farklı makine öğrenmesi modeli (KNN, NB, DT, LR, KNN-NB, DT-LR, KNN-NB-DT) kullanılmıştır. Saldırı türlerinin sınıflandırılmasında tekil ve hibrit makine öğrenmesi modelleri karşılaştırılmış; modelleme yaklaşımlarının performansları çeşitli metrikler üzerinden değerlendirilmiştir.
- Çalışma sonucunda, SCADA sistemlerine yönelik farklı saldırı türlerinin ayırt edilmesinde kullanılabilecek etkili makine öğrenmesi yaklaşımları belirlenmiş ve bu alanda yapılacak ileri düzey çalışmalar için temel oluşturulmuştur.
- Ayrıca bu tez çalışması, siber fiziksel sistemlerin korunmasına yönelik farkındalığın artmasına ve kritik altyapıların güvenliğini tehdit eden saldırılara karşı teknik çözüm önerilerinin literatüre kazandırılmasına katkı sunmaktadır.

Bu tez beş ana bölümden oluşmaktadır. Birinci bölümde, SCADA sistemleri ve kritik altyapılar çerçevesinde siber güvenliğin önemi ele alınmış, çalışmanın amacı ve kapsamı açıklanmıştır. İkinci bölüm, saldırı türleri ve bu saldırıların SCADA sistemlerindeki etkilerine odaklanan literatür taramasını içermekte; ayrıca yapay zekâ ve makine öğrenmesi tabanlı saldırı tespitine yönelik güncel çalışmalar da ele alınmaktadır. Üçüncü bölümde, SCADA sistemlerinin teknik yapısı, haberleşme protokolleri, ağ topolojileri ve güvenlik açıkları ayrıntılı şekilde sunulmuş; ayrıca çalışmada kullanılan makine öğrenmesi algoritmaları açıklanmıştır. Dördüncü bölümde, fiziksel test ortamının kurulumu, senaryo bazlı siber saldırılar, oluşturulan veri kümesinin yapısı ve uygulanan sınıflandırma modelleri ile performans metrikleri ayrıntılı olarak aktarılmıştır. Beşinci bölümde, uygulamalar sonucunda elde edilen deneysel veriler değerlendirilmiş ve elde edilen sonuçlara göre genel çıkarımlar ile öneriler sunulmuştur. Bu tez çalışmasının genel organizasyon yapısına Şekil 1.1’de yer verilmiştir.



Şekil 1.1. Çalışmanın genel organizasyon şeması

2. LİTERATÜR TARAMASI

Bu bölümde, kritik altyapıların işletilmesinde kilit bir role sahip olan SCADA sistemlerinin önemine odaklanarak SCADA sistemlerinin güvenlik açıkları ile ilgili çalışmalar ve bu sistemlere yönelik gerçekleştirilen siber saldırılar ele alınmaktadır. Siber saldırıların tespitine yönelik yapılan araştırmaların yanı sıra yapay zekânın bu süreçteki rolü de incelenerek SCADA ağına yönelik gerçekleştirilen siber saldırıların yapay zekâ yöntemleri kullanılarak tespiti ile ilgili olarak yapılan araştırmalar değerlendirilmektedir.

İnsanların büyük kentlere göç etmesiyle birlikte, şehir nüfusları hızla artmıştır. Artan nüfusla birlikte, insanların ihtiyaç duyduğu ısı, ışık ve enerji gibi temel gereksinimler de hızla artmıştır. Bu artan taleplere cevap vermek için sunulan sistemler hantallaşmış, işletilmesi, kontrol edilmesi ve denetlenmesi zorlaşmıştır. Bu zorlukların üstesinden gelmek için SCADA sistemi geliştirilmiştir.

SCADA, 1980'lerden bu yana saha verilerinin toplanması ve sahadaki aktüatörlerin kontrol edilmesi amacıyla kullanılan temelde alarm bazlı izleme ve kontrol prensiplerini içeren bir sistemdir [23]. Zamanla, SCADA sistemlerinde kullanılan PLC'lerin tedarikçileri kendi standartlarını oluşturmuşlar, bu da farklı PLC'lerin tedarikçilerinin birbirleriyle haberleşmesini gerektirdiğinden bir sorun haline gelmiştir. Bu nedenle, 1980'lerde bazı standartlar üzerinde mutabakata varılmış, bugün çoğu tedarikçi daha fazla pazar payı elde etmek için UUB'lerini standart bir iletişim arayüzü ile donatmıştır [24]. Bu sistemler zamanla birçok kritik altyapıda kullanılmaya başlanmıştır. Bunlar arasında, enerji santralleri, su arıtma tesisleri, havayolları, demiryolları, gemi sistemleri, gaz boru hatları ve benzer kritik altyapılar bulunmaktadır. Kritik altyapıların işletilmesinde kullanılan SCADA sistemleri, akademik alanda yoğun bir araştırma konusu haline gelmiştir.

Endi ve arkadaşları, açık sistem teknolojisi ve mimarisine bağlı olarak 3 katmanlı SCADA sistem mimarisi önermişlerdir. Denetim kontrol katmanı, proses kontrol katmanı ve saha enstrüman katmanı olan ve gerçek zamanlı bir endüstriyel prosesi simüle eden eksiksiz bir 3 katmanlı model SCADA sistemi geliştirmişlerdir. Araştırmacılar tasarladıkları çok katmanlı SCADA sistem mimarisinin, geleneksel SCADA sisteminden daha fazla faydaya sahip olduğunu ve açık sistem standardına bağlı üç katmanlı SCADA sistem mimarisinin

kullanılmasının önceki nesil SCADA sistemlerinin sınırlamalarını ortadan kaldıracığını belirtmişlerdir [25].

Lahti ve arkadaşları [26], yaptıkları çalışma kapsamında farklı web tabanlı teknolojileri Otomasyon ve SCADA sistemi açısından incelemiş ve analiz etmişlerdir. Santral Otomasyonu ve SCADA sistemleri açısından web kullanıcı arayüzü teknolojisinin uygunluğunun değerlendirmesini yapmışlardır. Araştırmalarında ayrıca, enerji santrali sistem satıcıları için teknik çözümlerin temeli olarak kullanılan çeşitli web tabanlı kontrol ekranlarının son teknoloji kontrol uygulamalarını da vurgulamışlardır.

Chauhan ve arkadaşları, araştırmalarında enerji üretimi ve dağıtımı, petrol, gaz, su ve atık yönetimi gibi ülkelerin kritik altyapılarının kontrolü ve izlenmesinde kullanılan SCADA sistemlerini ele almışlardır. SCADA sistemlerinin denetleyici kontrol ve veri toplama işlevlerine odaklanmışlar, dış dünyaya bireysel mesaj veya komut gönderme yeteneği içeren sistemleri incelemişlerdir [27].

İbrahim, şehir içi ve şehirlerarası yolların aydınlatma sisteminin izlenmesi ve kontrolü için Irak-Kerkük şehrinde yapılan bir uygulama ile SCADA sistemi yazılımı geliştirmiştir. Araştırmacı, çalışmasında otomasyon ve SCADA sistemini donanım, yazılım, iletişim protokolleri ile bağlantı türleri açısından incelemiştir. Araştırmacı, yaptığı analizler neticesinde geliştirdiği SCADA yazılımında, yolların aydınlatma sistemlerindeki tüm olayların izlenmesi ve kontrolünün yanı sıra günlük verilerin izlenmesi, güvenlik yönetimi, alarm yönetimi, veri arşivi ve raporlama işlemleri gibi işlevleri de yerine getirmiştir. Sonuç olarak araştırmacı geliştirdiği SCADA yazılımının şehir içi ve şehirlerarası yolların aydınlatma sistemi kontrolünde kusursuz, senkronize ve verimli bir şekilde çalıştığını, aydınlatma direklerinden gelen bilgileri kullanıcılara başarılı bir şekilde ilettiğini ve aydınlatma sisteminin işletme maliyetlerini azalttığını belirtmiştir [28].

EKS/SCADA sistemleri sık kullanılmakla birlikte güvenlik zafiyetleri barındırmaktadır. SCADA sistemlerinde genellikle eski veya güncellenmemiş işletim sistemleri ve yazılım sürümleri kullanılmaktadır. Bunun gibi durumlar, saldırganların zayıf noktaları hedef alarak sisteme sızma ve kontrolü ele geçirme ihtimalini artırmaktadır. SCADA sistemlerinde karşılaşılan bir diğer güvenlik zafiyeti ise standart parola güvenliği uygulamalarıdır. SCADA sistemlerinde, sistem kullanıcılarının zayıf ve varsayılan olarak atanmış parolaları

kullanması yetkisiz erişimi kolaylaştırmaktadır. SCADA sistemlerinin çoğu internete bağlı cihazlarla etkileşime girebildiğinden ve günümüzde sistemlere bağlantı noktasında uzaktan erişim gibi yöntemler tercih edilebildiğinden siber saldırganlar için potansiyel bir hedef haline gelmektedir.

EKS/SCADA sistemleri günümüzde artan bilgi, iletişim ve internet teknolojisi kullanımıyla bilişim teknolojileriyle entegre bir şekilde çalışma yönünde eğilim göstermektedir. Bu eğilime bağlı olarak SCADA sistemlerinde saha cihazları ile MDB arasındaki veri alışverişini sağlamak için kullanılan haberleşme protokolleri, bilgi ve iletişim teknolojisindeki zafiyetlere maruz kalabilmektedir. Amerikan Gaz Birliği'nin American Gas Association-12 (AGA-12) standardına göre, yaklaşık 150-200 adet SCADA protokolü vardır. SCADA veya endüstriyel kontrol sistemleri içerisindeki temel bileşenler arasındaki iletişim özel olarak geliştirilmiş haberleşme protokolleri aracılığıyla gerçekleştirilmektedir. Profinet, Modbus, Distributed Network Protocol Version 3.0 (DNP3), EtherNet/IP, ControlNet, Foundation Fieldbus, Profibus en çok kullanılan haberleşme protokollerindendir [29]. 2003 yılında geliştirilen ve endüstriyel otomasyon alanında benimsenmiş bir standart haline gelmiş olan PROFINET haberleşme protokolü, özellikle Siemens sistemlerinde yaygın şekilde kullanılmaktadır [30]. Bu protokolde bulunan güvenlik açıkları, söz konusu standartları kullanan sistemlerde de yer aldığından, bu yapıları çeşitli tehditlere karşı savunmasız hâle getirmektedir. PROFINET protokolünün özelliklerinden yola çıkılarak ağdaki cihazlara erişim, ortadaki adam saldırısı, tekrarlama saldırısı, DoS gibi saldırılar gerçekleştirilebilmektedir [31]. Paul ve arkadaşları, DoS ve MITM gibi PROFINET protokolüne yönelik gerçekleştirilebilecek saldırıları çalışmalarında incelemişlerdir [32]. Bu tür çalışmaların da gösterdiği üzere, SCADA sistemlerindeki varlıklar siber tehditlere karşı savunmasız hâle gelmekte ve çeşitli saldırı riskleriyle karşı karşıya kalmaktadır. Bu saldırı türlerinin tamamı endüstriyel sistemlerin verimliliğini, güvenilirliğini ve güvenliğini tehlikeye atabilir.

SCADA sistemlerine bugüne kadar birçok siber saldırı gerçekleşmiştir. 2007, 2010 ve 2014 yıllarında farklı sürümleriyle ortaya çıkan BlackEnergy adlı zararlı yazılım, ilk olarak Distributed Denial of Service (DDoS) saldırıları için kullanılmıştır. En son sürümünde, kullanıcının klavye girişlerini izleyebilme yeteneği kazanmış ve Sanal Özel Ağ (Virtual Private Network - VPN) kimliklerine erişebilmesi sayesinde şirket içi ağlarda dolaşabilir hâle gelmiştir [33].

2013 yılında Havex Rat adlı kötü niyetli bir yazılım, endüstriyel kontrol sistemlerine yönelik bir saldırı aracı olarak rapor edilmiştir [33]. Saldırganlar, SCADA sistemlerine yönelik yazılım sağlayan web sitelerine bu zararlı yazılımı entegre etmiştir. Kullanıcılar, bu web sitelerinden yazılım indirip kurulum gerçekleştirdiğinde, sistem söz konusu zararlı yazılımla enfekte olmakta ve yazılım, yayıldığı kontrol ağı içerisinde endüstriyel protokoller ve açık portları tarayarak yayılım göstermektedir.

2017 yılında meydana gelen Dragonfly 2.0 saldırısı ile saldırganlar, enerji sektöründeki kuruluşların SCADA sistemlerini hedef alarak endüstriyel tesislerin üretim süreçlerini etkilemeye çalışmışlardır [34].

Bad Rabbit fidye yazılımı saldırısı, Rusya'daki bir petrol ve gaz şirketinin SCADA sistemlerine karşı 2020 yılında gerçekleştirilmiştir. Saldırının amacı, enerji üretim ve dağıtım sistemlerine zarar vermektir. Bad Rabbit sisteme bulaştığında kullanıcıların dosyalarına erişimini şifreleyerek engelliyordu ancak saldırı başarıyla sonuçlanmamıştır. Eğer saldırı başarılı olsaydı, şirketin enerji üretim ve dağıtımını felç ederek büyük bir enerji krizine yol açabilirdi [34].

Bu nedenle, gerekli önlemler alınmalı, sistemlerin güvenliği için siber saldırı tespit sistemleri geliştirilmelidir. Siber saldırıların sıklığı ve bu saldırılardan ekonomik olarak zarar görenlerin sayısı hakkında kesin verilere ulaşmak saldırıların gizlenmesi ve suçluların yakalanmaması gibi faktörler nedeniyle zor olmaktadır [35]. Bu bağlamda, güvenliği sağlamak için yazılım geliştirme öncelik hâline getirilmeli ve güçlü yasal düzenlemelerle desteklenmelidir.

Angin, yaptığı çalışmada askeri otonom ağ sistemlerine yönlendirilen veri bütünlüğü ihlalleri, kimlik doğrulama yanıltmaları, gizli mesaj saldırıları ve ortadaki adam saldırılarını blokzincir tabanlı bir iletişim mimarisiyle tespit etmeye ve engellemeye odaklanmıştır [36]. Çalışmanın, veri bütünlüğü ihlalleri ve kimlik doğrulama yanıltmaları saldırılarına karşı etkili koruma sağladığı tespit edilmiştir.

Süzen ve arkadaşları [37], Endüstri 4.0'ın bir parçası olan nesnelerin kablosuz iletişiminde ağa sızma, kırma ve taklit etme yeteneklerinin veri güvenliğini nasıl etkilediğini ve güvenlik için hangi yöntemlerin gerektiğini değerlendirmişlerdir. Kablosuz ağlara ve bu ağlardaki

cihazlara yapılan saldırıları içeren üç farklı senaryo ile ağ yapısının güvenliği incelenmiştir. Wi-Fi Protected Access (WPA), WEB, Wi-Fi Protected Access 2 (WPA2) gibi güvenlik önlemlerinin tek başına yetersiz olduğu ve güvenlik politikaları, gizlilik, yetkilendirme ve şifreleme sistemleri gibi unsurlarla güçlendirilmesi gerektiği vurgulanmıştır.

Çelik ve arkadaşları [38], yaptıkları araştırmada 1989 ile 2017 yılları arasındaki GPCoder, Winlock, Reveton, CryptoLocker, Cryptowall, Locky ve KeRanger, WannaCry, Petya gibi saldırıları incelemişlerdir. Bu saldırılara karşı da çözüm yöntemleri olarak ağ yapısı ve yönetilmesi, eğitim, antispam/malware, yedekleme ve veri kurtarma, yeni nesil güvenlik sistemleri, operasyonel temizleme gibi yöntemleri önermişlerdir.

Siber saldırıların tespitinde bu ve buna benzer çalışmalar yapılmış olmakla birlikte günümüzde siber saldırıların giderek karmaşık hale gelmesi saldırıların tespitini zor hale getirmiştir. Bu nedenle, geleneksel yöntemlerle saldırı tespiti yerine büyük miktarda veriyi analiz ederek anormallikleri tanımlama yeteneği bulunan yapay zekâ yöntemlerine yönelim artmıştır. Yapay zekâ, bilgisayarların veya dijital sistemlerin insan benzeri davranışlarını taklit eden ve belirli görevleri gerçekleştirebilen yetenek olarak tanımlanabilir [39]. Birçok siber saldırı anlık olarak gerçekleşir ve hızlı bir şekilde tespit edilmesi gerekmektedir. Yapay zekâ algoritmaları ile büyük veri kümeleri gerçek zamanlı olarak analiz edilebilir ve anında yanıt verilebilir. Ayrıca, yapay zekâ sistemleri insan hatalarını en aza indirirken farklı türdeki siber saldırıları tanımlama ve savunma stratejileri geliştirme konusunda esneklik sunmaktadır. Dolayısıyla, günümüzde yapay zekâ sistemleri siber güvenlikte önemli bir rol oynamaktadır ve saldırıları tespit etme ve önleme süreçlerinde temel bir araç haline gelmiştir. Literatürde siber saldırıların yapay zekâ yöntemleri ile ilgili tespitine yönelik çalışmalar mevcuttur.

Nader ve ekibi [40], kritik altyapıları ve endüstriyel süreçleri tehdit eden siber saldırılar üzerinde bir çalışma yürütmüşlerdir. Geleneksel saldırı tespit sistemlerinin, veri tabanlarında yer almayan yeni siber saldırı türlerini tanımlama ve tespit etme konusunda yetersiz kaldığı öne sürülmüştür. Çalışmalar, Fransa'daki birincil içme suyu dağıtım sistemini temsil eden Süveyş'teki bir içme suyu dağıtım tesisinden alınan gerçek bir veri kümesi üzerinde gerçekleştirilmiştir. Siber saldırıları ve izinsiz girişleri tespit etme konusunda makine öğrenme tekniklerinden tek sınıflı sınıflandırma kullanılmıştır. Araştırmacılar, bu metodun

endüstriyel süreçlere yönelik kötü niyetli siber saldırıların tespit edilmesinde önemli rol oynayacağını ifade etmişlerdir.

Kalech, kritik altyapıların SCADA güvenliğini sağlamak için zamansal örüntü tanımaya dayalı siber saldırı tespiti tekniklerinden özellikle Gizli Markov Modeli (Hidden Markov Models-HMM) ve Yapay Sinir Ağlarına (Artificial Neural Network-ANN) dayalı iki algoritma önermiştir. Araştırma, birincisi CyberGym tarafından kurulan kapsamlı bir eğitim SCADA laboratuvarından, ikincisi ise Negev Ben-Gurion Üniversitesi'nde bulunan gerçek bir SCADA sisteminden elde edilen veriler üzerinde gerçekleştirilmiştir. Elde edilen bulgulara göre, zamansal örüntü tanıma yöntemlerinin literatürde tespit edilmesi zor olarak bilinen meşru işlevleri de dahil olmak üzere siber saldırıları tespit edebildiği ifade edilmiştir [41].

Lin ve arkadaşları [42], bir endüstri kontrol sistemi test yatağı oluşturarak, su seviyesi kontrolü ve hava kirliliği kontrolü olmak üzere iki operasyonel durumu incelemişlerdir. Bu endüstriyel kontrol ağı için normal davranış kalıpları oluşturan ve böylece anormal izinsiz giriş olaylarını tespit edebilen bir Saldırı Tespit Sistemi (STS) geliştirmek için makine öğrenimi tabanlı bir şema önermişlerdir. Geliştirilen test ortamında gerçekleştirilen test sonuçlarına göre, bu yöntemin çeşitli ağ saldırılarını etkili bir şekilde tespit edebildiği belirtilmiştir.

Kravchik ve Shabtai [43], endüstriyel kontrol sistemlerine yönelik siber saldırıları tespit etmek için evrimsel sinir ağları kullanarak bir çalışma sunmuşlardır. Çalışma, gerçek dünyadaki bir endüstriyel su arıtma tesisinin küçültülmüş bir modelini temsil eden Güvenli Su Arıtma test yatağı (Secure Water testbed-SWaT) veri kümesi üzerinde gerçekleştirilmiştir. Önerilen yöntem, 31 siber saldırıyı 3 yanlış pozitif ile tespit ederek bu veri kümesi üzerinde gerçekleştirilen önceki çalışmalardan daha iyi bir performans göstermiştir. Araştırmacılar, sundukları modelin çalışma süresi ve performansı üzerinde durmuşlar ve EKS siber saldırı tespiti için büyük umut vaat ettiğini belirtmişlerdir.

Gao ve arkadaşları [44], SCADA ağları için derin öğrenme tabanlı saldırı tespit sistemini araştırdıkları bir çalışmada, saldırıları tespit etmek için İleri Beslemeli Sinir Ağı (Feedforward Neural Network – FNN) ve Uzun Kısa Süreli Bellek (Long Short-Term Memory – LSTM) algoritmalarının hangi kategorilerde daha iyi performans gösterdiğini

karşılaştırmışlardır. Araştırmacılar, FNN algoritmasının zamansal ilişkisiz saldırıları tespit etmede daha başarılı olduğunu, LSTM'nin ise zamansal ilişki olanları tespit etmede daha iyi performans gösterdiğini gözlemlemişlerdir. Ayrıca, FNN-LSTM modelinin ise zamansal ilişki düzeyine bakılmaksızın her türlü SCADA saldırısını yüksek oranda tespit ettiği belirlenmiştir.

Feng ve arkadaşları, endüstriyel kontrol sistemleri için ağ paketi içeriklerinin analizini birleştiren bir anomali algılama yöntemi önermişlerdir. Bu çalışmada, Bloom filtre paketi düzeyi anomali algılayıcısını ve LSTM ağ tabanlı zaman serisi düzeyi anomali algılayıcısını tutarlı bir şekilde birleştiren EKS'ye özgü yeni bir anomali algılama çerçevesi üzerinde durulmuştur. Araştırmacılar, bir gaz boru hattı SCADA sisteminden oluşturulan gerçek bir veri setini de inceleyerek her iki yaklaşımı birleştiren bir anomali tespit şemasının, mevcut çeşitli son teknoloji tekniklere kıyasla daha yüksek performans elde edebileceğini göstermişlerdir [45].

Potluri ve arkadaşları, endüstriyel kontrol ağları bağlamında çeşitli siber saldırıları tespit etmek için bir çözüm önermişlerdir [46]. Yaptıkları çalışmada, STS'nin geliştirilmesi için derin öğrenme tekniklerini makine öğrenmesi teknikleriyle birleştirerek tespit mekanizmasının performansını değerlendirmişlerdir. Kesinlik (precision), duyarlılık (recall) ve F-skoru gibi performans metrikleri ölçülmüştür. Hibrit mimariyle geliştirilmiş doğruluklara rağmen, en iyi performans izinsiz giriş tespitini elde etmek için sıralama tabanlı hiyerarşik ağ kullanmışlardır. Araştırmacılar, bu yaklaşımın bireysel özellik çıkarma tekniklerinin dezavantajlarını önlediğini ve mevcut teknikler arasında mümkün olan en iyi algılama doğruluğunu sağladığını vurgulamışlardır.

Wang ve arkadaşlarının yaptıkları çalışmada, akıllı şebekeler için tam ve eksik ağ bilgisi içeren senaryo tabanlı iki aşamalı seyrek siber saldırı modelleri önerilmiştir. Ardından, belirlenen siber saldırıları etkin bir şekilde tespit etmek için yenilikçi bir şekilde aralıklı durum tahminine dayalı bir savunma mekanizması geliştirilmiştir. Son olarak elektrik yükü tahmininin doğruluğunu artırmak için tipik bir derin öğrenme modeli olan yığılmış otomatik kodlayıcı tasarlanarak uygulanmıştır. Önerilen siber saldırı modellerinin ve savunma mekanizmasının etkinliği, kapsamlı testlerle gösterilmiştir [47].

Shitharth ve Winston [48], optimizasyona dayalı olarak bir SCADA ağındaki izinsiz girişleri tespit etmek ve sınıflandırmak için bir STS tasarlamışlardır. Bu çalışmada, İzinsiz Giriş Ağırlıklı Parçacık Tabanlı Guguk Kuşu Arama Optimizasyonu (Intrusion Weighted Particle based Cuckoo Search Optimization – IWP-CSO) ve Hiyerarşik Nöron Mimarisi tabanlı Sinir Ağı (Hierarchical Neuron Architecture based Neural Network – HNA-NN) teknikleri önermişlerdir. Testlerde hem mevcut hem de önerilen tekniklerin performans sonuçları değerlendirilmiştir. Yapılan analizlere göre, önerilen IWP-CSO'nun HNA-NN algoritması ile diğer tekniklere göre daha iyi sonuçlar verdiği görülmüştür.

Alhaidari ve Al-Dahasi [49], SCADA sistemlerini DDoS saldırılarına karşı korumak için üç farklı makine öğrenimi algoritması kullanarak bir çerçeve geliştirmeye çalışmışlardır. J48, NB ve Rastgele Orman (Random Forest – RF) algoritmalarını kullanmışlardır. Bu algoritmalar KDDCup'99 veri seti üzerinde eğitilmiş ve değerlendirilmiştir. Elde edilen sonuçlar, en iyi sınıflandırmanın %99,99 doğruluk oranı ile RF kullanılarak elde edildiğini, NB algoritmasının ise %97,74 ile en düşük doğruluk oranına sahip olduğunu göstermiştir.

Teixeira ve arkadaşları, su arıtma ve dağıtma sürecinde bir aşama olan bir su depolama tankının kontrol sistemini temsil eden test yatağına EKS'ye özgü 5 keşif saldırısı gerçekleştirdiler [50]. Bu saldırılar sırasında cihazlarla ilgili bilgilerin (vanalar, pompalar, sensörler) bulunduğu ağ trafiğini ele geçirdiler. Bu ağ trafiğinden oluşturdukları veri kümesine siber saldırıları tespit etmek için “Rastgele Orman, Karar Ağacı, Lojistik Regresyon, Naive Bayes ve KNN” olmak üzere beş farklı geleneksel makine öğrenimi algoritması uyguladılar. Elde ettikleri sonuçlar, makine öğrenimi modellerinin saldırıları gerçek zamanlı olarak tespit etmedeki verimliliğini göstermiştir.

Miciolino ve arkadaşları, küçük bir şehrin su sistemini taklit eden siber-fiziksel test ortamına farklı siber saldırılar gerçekleştirerek SCADA haberleşme ağının tutarlılığını ve doğruluğunu test etmişlerdir. Deneysel sonuçlar, endüstriyel kontrol sistemlerinde yaygın olarak kullanılan Modbus protokolündeki güvenlik açıklarını vurgulamıştır. Araştırmacılar, bir saldırganın sistem hakkında yeterli bilgi edinerek, kötü niyetli hedeflerine ulaşmak için aktüatörlerin komutlarını veya sensör okumalarını değiştirebileceği sonucuna varmışlardır [51].

Keliris ve arkadaşları, saldırıları gerçek zamanlı olarak tespit etmek için bir EKS'nin operasyonel davranışını dikkate alan, sürece duyarlı, denetimli bir öğrenme savunma stratejisi geliştirdiler. Yaptıkları çalışmada bir kıyaslama kimyasal süreci kullandılar ve donanım denetleyicilerinde çeşitli saldırı vektörleri kategorilerini göz önünde bulundurdular. Anormallikleri gerçek zamanlı olarak tespit etmek ve kötü niyetli davranışları ayırt etmek amacıyla eğitilmiş Destek Vektör Makinesi (Support Vector Machine – SVM) modellerini kullandılar [52].

Hindy ve arkadaşları yaptıkları çalışmada, SCADA sistemleri tarafından kontrol edilen su şebekelerinde anomali tespiti için yeni bir model geliştirmişlerdir [53]. Modbus protokolü kullanılmıştır. Model geliştirilirken LR, Gaussian Naive Bayes (GNB), SVM, KNN, DT ve RF olmak üzere altı farklı makine öğrenmesi algoritmasını kullanmışlardır. Hazır bir veri kümesi kullanılarak geliştirilen model, sabotaj, donanım hataları ve siber saldırılar gibi çeşitli anomali türlerini sınıflandırmak için tasarlanmıştır. Önerilen model, mevcut tespit sistemlerinden farklı olarak operatöre bir olayın gerçekleşme olasılığını bildirme ve saldırı etkilerini azaltmaya yönelmiştir.

Başka bir çalışmada Benisha ve Ratna, SCADA ağlarındaki siber saldırıların belirlenmesi ve sınıflandırılması için yeni bir metodoloji önermişlerdir [54]. Çalışmada kullandıkları veri kümesi, su depolama sisteminin ağ saldırılarını içermektedir. Araştırmacılar önerdikleri yaklaşımda, en uygun özelliklerin seçimi için kümeleme ve STS tabanlı Geliştirilmiş Guguuk Kuşu Arama Optimizasyon (Enhanced Cuckoo Search Optimization) algoritmasını kullanmışlar. Sınıflandırma aşamasında ise, Genetik Makine Öğrenmesi Tabanlı Sinir Ağı (Genetic Machine Learning based Neural Network) algoritmasını tercih etmişler. Yeni metodoloji ile doğruluğun en az sürede artırılması sağlanmıştır. Performans analizi sonuçları, geleneksel algoritmalara kıyasla daha iyi kümeleme, optimizasyon ve sınıflandırma sonuçları elde edildiğini göstermiştir.

Perez ve arkadaşları [55], Mississippi Eyalet Üniversitesi (Mississippi State University – MSU) tarafından sağlanan ve bir gaz boru hattı sisteminden toplanan gerçek bir veri setini kullanarak SCADA sistemlerinde izinsiz giriş tespiti için makine öğrenmesi tekniklerini uygulamış ve ağ saldırılarını tespit etmişlerdir. Çalışmalarında, SVM ve RF algoritmalarını kullanmayı tercih etmişlerdir. Elde edilen sonuçlar, RF'nin izinsiz girişleri etkili bir şekilde

tespit ettiğini ve F1 değerinin kullanılması da performansların doğru bir şekilde değerlendirilmesine olanak sağladığını göstermiştir.

Grammatikis ve arkadaşları, DNP3 protokolünü kullanan SCADA sistemleri için bir saldırı tespit ve önleme sistemi önermişlerdir [56]. Bu sistem, denetimli ve denetimsiz makine öğrenimi algılama modellerine dayanmakta olup ağ trafiğinin belirli bir DNP3 siber saldırısıyla veya anormalliğiyle ilişkilendirilip ilişkilendirilmediğini ayırt edebilmektedir. Gerçek bir trafo merkezinden elde edilen veriler kullanılmış ve önerilen sistemin etkinliği gösterilmiştir.

Söğüt ve Erdem tarafından gerçekleştirilen çalışmada, kritik altyapıların bir parçası olan gaz boru hattı kontrol sistemine ait bir veri seti kullanılmıştır. Bu çalışmada, gaz boru hattı kontrol sistemi üzerindeki Modbus protokolüne yönelik komut enjeksiyonu, keşif ve hizmet engelleme gibi kategorilerde çeşitli ataklar gerçekleştirilmiştir. Veri seti üzerinde çeşitli algoritmalar ile veri madenciliği yöntemi kullanılmıştır. Bu veri seti kullanılarak EKS veya SCADA'lara yönelik saldırı yapılan ve saldırı yapılmayan durumlar farklı niteliklere göre değerlendirilip analiz edilmiştir. Analiz sonuçlarına göre en doğru sınıflandırma oranının Random Tree algoritması ile sağlandığı görülmüştür [17].

Başka bir çalışmada Basnet ve arkadaşları, SCADA kontrollü elektrikli araç şarj istasyonunda derin sinir ağı, 1D evrişimli sinir ağı ve LSTM tekrarlayan sinir ağı olmak üzere üç farklı derin öğrenme algoritmasını kullanarak derin öğrenme tabanlı yeni fidye yazılımı algılama çerçevesi önermişlerdir [57].

Rajesh ve Satyanarayana [58], Endüstriyel Proses Kontrol Sistemleri – SCADA ağında saldırı tespiti için filtreleme ve örnekleme teknikleri ile birlikte makine öğrenimi algoritmalarını kullanmışlardır. Araştırmacılar, yaptıkları çalışmada gerçek zamanlı bir SCADA test yatağı kullanarak hem normal hem de saldırı verilerini içeren ağ trafiği ile kendi veri kümelerini oluşturmuşlardır. Veri kümesi oluşturulurken Chi-Square, Analysis of Variance (ANOVA) ve Least Absolute Shrinkage and Selection Operator (LASSO) ile Support Vector Machine Synthetic Minority Over-sampling Technique (SVMOTE) tekniklerini uygulamışlardır. Veri kümesini oluşturduktan sonra, saldırıları tespit etmek için makine öğrenimi algoritmalarından SVM, KNN, RF ve NB algoritmalarını kullanmışlardır.

Ullah ve Mahmud, SCADA ağlarında anomali tabanlı saldırı tespiti için makine öğrenmesi yaklaşımını kullanarak bir hibrit model geliştirmişlerdir. Çalışmada, Mississippi Eyalet Üniversitesi Starkville Dağıtılmış Analitik ve Güvenlik Enstitüsü'nde geliştirilen bir endüstriyel kontrol sistemi veri kümesi kullanılmıştır. Elde edilen sonuçlar, geliştirilen modelin zaman ve hesaplama karmaşıklığını azaltmada önemli bir etki sağladığını ve gelişmiş doğruluk ve tespit oranı elde ettiğini göstermiştir [59].

Literatürde SCADA ağlarına yapılan saldırılar ve bu saldırıların tespiti için kullanılan yapay zekâ algoritmaları incelenmiştir. Bu literatür taraması sonucunda, siber saldırıların tespiti amacıyla makine öğrenimi algoritmalarının diğer yöntemlere göre daha sık tercih edildiği gözlemlenmiştir. Bu tez çalışmasında, kritik altyapılar arasında yer alan enerji sektörü kapsamına giren ve PROFINET protokolünü kullanan bir hidroelektrik santralin SCADA ağı hedef alınarak gerçekleştirilebilecek potansiyel siber saldırılardan MITM, yetkisiz komut enjeksiyonu ve DoS saldırıları ele alınmakta olup siber saldırıların tespiti için yapay zekâ modelleri sunulmaktadır. Bu doğrultuda, PROFINET protokolü üzerinden gerçekleştirilen haberleşmeler temel alınarak özgün bir veri kümesi oluşturulmuş ve bu veri üzerinde çeşitli makine öğrenimi algoritmaları uygulanmıştır. Çalışmada; KNN, NB, DT, LR gibi temel algoritmaların yanı sıra KNN-NB, DT-LR ve KNN-NB-DT hibrit modelleri de değerlendirilmiştir. Bu yöntemler, SCADA sistemlerine yönelik siber saldırıların tespitine ilişkin farklı yaklaşımlar sunmakta ve mevcut çalışmaların sınırlılıklarını aşmaya yönelik alternatif çözüm önerileri sağlamaktadır. Bu tez kapsamında elde edilen saldırı tespit doğruluk oranları ve diğer metrikler, 5.1. Deneysel Sonuçlar başlığı altında sunulan tabloya yerleştirilmiştir. Böylelikle, tez kapsamında yürütülen çalışmaların çıktıları, metodolojik bir çerçevede karşılaştırılarak bütüncül bir değerlendirme yapılmıştır.



3. TEORİK ALTYAPI

Bu bölümde, SCADA sistemlerinin ana bileşenleri ve iletişim protokolleri, veri haberleşme teknolojileri ve ağ topolojileri ele alınmaktadır. Ayrıca, SCADA sistemlerine yönelik siber saldırı türleri ve yapay zekâ ile makine öğrenmesi tabanlı modeller hakkında bilgiler verilmektedir.

3.1. SCADA Sistemleri

SCADA sistemleri, endüstriyel süreçlerin güvenli ve etkin bir şekilde yönetilmesi, ayrıca operasyonel verimliliğin artırılması amacıyla kullanılan sistemlerdir. SCADA sistemleri ile endüstriyel süreçlerin kontrolü ve izlenmesi sağlanmaktadır. SCADA sistemleri, süreçleri gerçek zamanlı izleme ve hızlı müdahale imkânı sunarak verimliliği artırma, arıza ve bakım maliyetlerini azaltma gibi avantajlar sağlar. Ancak, bu sistemler siber saldırılara karşı savunmasız olabilmekte ve bu da özellikle kritik altyapıların zarar görmesine neden olabilmektedir. Bu sistemlerin siber güvenlik tehditlerine karşı korunması ve güncellenmesi önem arz etmektedir. SCADA sistemlerinin ana bileşenleri ve bu sistemlerde kullanılan protokoller siber güvenlik açısından dikkat edilmesi gereken önemli unsurlardır.

3.1.1. SCADA sistemi ana bileşenleri

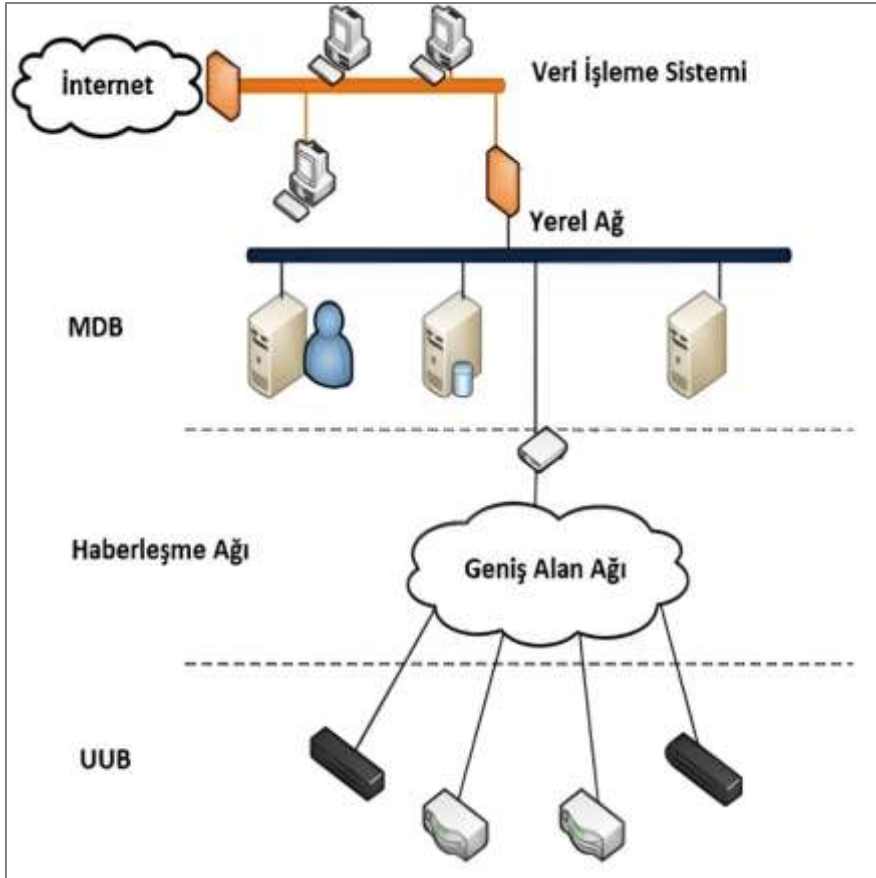
SCADA sistemleri MDB, UUB'ler ve haberleşme ağı olmak üzere ana unsurlardan oluşmaktadır. Bu unsurlara veri işleme sistemi de (İşletme Bilgi Teknolojileri – BT ağı) eklenebilir.

MDB, merkezi bir kontrol ve yönetim noktasıdır. Sahadaki tüm uç birimlerin kontrol edildiği, gözlemlendiği, ölçüm verilerinin toplandığı ve depolandığı merkezi birimdir. Ana kumanda ve izleme merkezi olarak da tanımlanabilir. Sistemdeki tüm cihazların birbirleriyle bağlantı kurmasını ve veri iletişimini sağlamaktadır. MDB, sistemin en kritik birimidir. Bu birimde meydana gelebilecek bir siber saldırı, tüm ağı etkileyebilecek bir güce sahiptir [60].

UUB'ler, sahada izlenmesi ve kontrol edilmesi gereken süreçlerin yönetilmesi için kullanılan, belirli ve tanımlı görevleri yerine getirmek için tasarlanmış uç nokta cihazlardır. Sahadan topladıkları verileri analiz ederek bu verileri MDB'ye aktarırlar. Aynı şekilde,

MDB'den gelen komutları sahadaki cihazlara iletirler, böylece sahadaki operasyonların etkin bir şekilde kontrol edilmesini sağlarlar [60]. PLC'ler bu bölümde yer almaktadır.

Haberleşme ağları, sistemin tüm bileşenleri arasında iletişim kurulması amacıyla kullanılan SCADA sistemlerinin mimarisine özel olarak tasarlanmış iletişim protokollerini içermektedir. Bu unsurlar, Şekil 3.1'de gösterilmektedir.



Şekil 3.1. SCADA sistemi ana bileşenleri [29]

3.1.2. Endüstriyel sistemlerde kullanılan SCADA iletişim protokolleri

Endüstriyel uygulamaların SCADA sistemlerinde MDB ve UUB'ler arasındaki iletişimi sağlamak amacıyla kullanılan protokoller arasında Modbus, EtherNet/IP, DNP3 ve Profinet gibi protokoller yer almaktadır [60, 61].

Modbus protokolü, 1979 yılında Modicon firması tarafından geliştirilmiş endüstriyel otomasyon sistemlerindeki cihazlar arasındaki veri iletişimi için kullanılan bir haberleşme protokolüdür. Modbus protokolü, çeşitli fiziksel katmanlarda işlev görebilen farklı

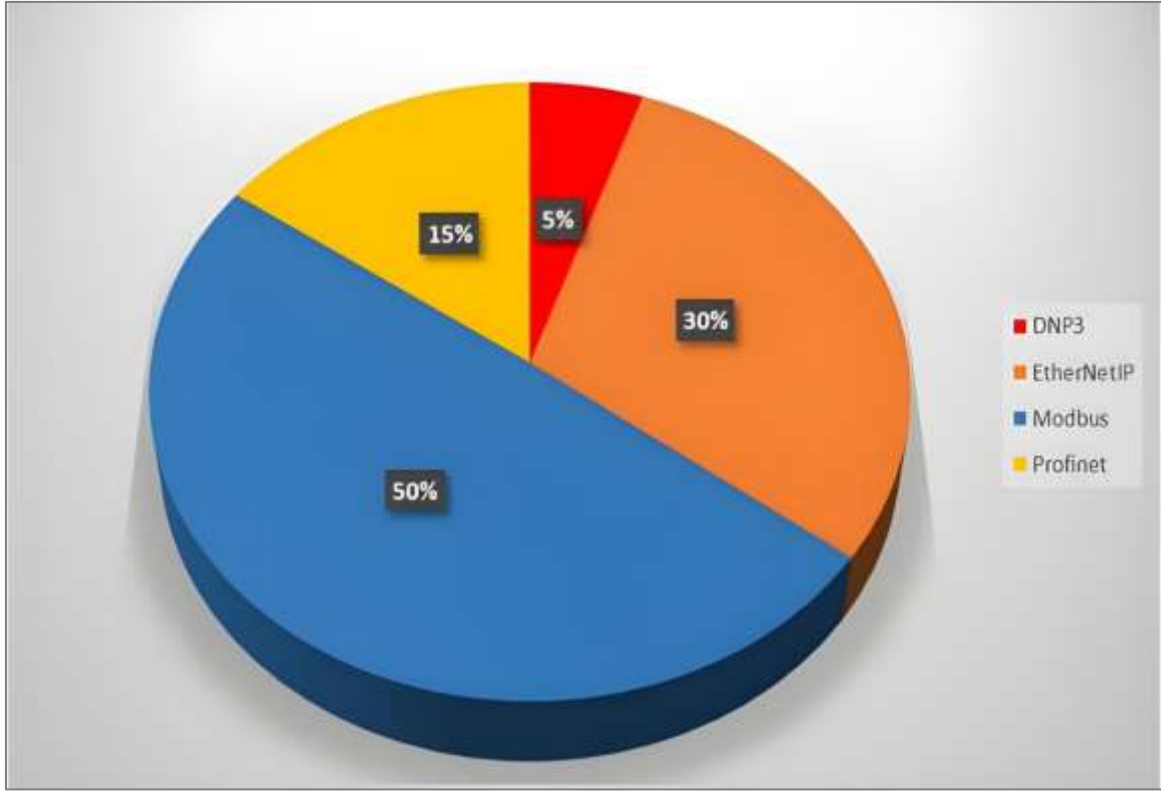
versiyonlara sahiptir. Bu versiyonlardan ikisi, Modbus'un seri iletişim hatları üzerinden çalışan türü Modbus Seri ile Ethernet tabanlı Modbus Transmission Control Protocol (TCP)'dür [60]. Modbus protokolü çerçevesinde, istekler belirlenen uzak uç birimlerine gönderilir ve bu cihazlardan geri dönüş mesajları alınır. Bu protokolde varsayılan olarak 502 numaralı port kullanılmaktadır.

EtherNet/IP (Internet Protocol) protokolü, ilk olarak 2001 yılında piyasaya sunulmuş olup günümüzde üretim otomasyonu için en gelişmiş, olgun ve kapsamlı endüstriyel Ethernet çözümü olarak kabul edilmektedir. Bu protokol, açık teknolojilerin ve internetin avantajlarını kullanmak isteyen kullanıcılar arasında hızlı bir şekilde yaygınlaşmıştır. EtherNet/IP, IEEE (Institute of Electrical and Electronics Engineers) 802.3 standardı ve TCP/IP protokol paketini temel alarak ortak endüstriyel protokolü uygular [62].

DNP3 protokolü, ABD ve dünya çapında elektrik enerjisi sektöründe geniş kullanım alanına sahip, en yaygın ve tanınmış EKS protokollerinden biri olarak bilinmektedir. DNP3, başlangıçta diğer geleneksel SCADA protokollerinde olduğu gibi seri iletişim için tasarlanmıştır. Birçok diğer protokol gibi DNP3 protokolü, mesajlarının taşınması için TCP/IP kullanılmasına olanak tanıyacak şekilde modernize edilmiştir. DNP3 protokolü, uzun mesajların parçalanmasını ve yeniden birleştirilmesini sağlayan sahte bir taşıma katmanına sahiptir. Bu özellik, bir mesajın DNP3 veri bağlantı katmanı üzerinden iletilmesi için çok büyük olması durumunda gerekli olmaktadır [63].

Profinet protokolü, Ethernet tabanlı gerçek zamanlı veri iletişimini destekleyen endüstriyel bir ağ standartıdır ve bu amaçla hizmet tanımları ve protokol mekanizmaları sunmaktadır [64].

Profinet protokolü, Profibus International (PI) tarafından yönetilir ve merkezi bir istasyon ile merkezi olmayan cihazlara dayalı bir sağlayıcı/tüketici iletişim modeli kullanır. Bu modelde, sağlayıcı cihazı işlem verilerini tüketici cihazına iletir. Bu protokolün yapısında cihazlar, denetleyici, saha cihazı ve süpervizör olmak üzere sınıflandırılırlar. Veri alışverişi denetleyici tarafından kontrol edilir. Saha cihazı döngüsel işlem verilerini sağlamaktadır. Mühendislik istasyonu veya İnsan Makine Arayüzü (Human Machine Interface-HMI) ise süpervizörü temsil etmektedir [18]. Bahsedilen SCADA iletişim protokollerinin kullanım oranları Şekil 3.2' de sunulmaktadır [5].



Şekil 3.2. SCADA iletişim protokollerinin kullanım oranları [5]

SCADA sistemlerinde yaygın olarak kullanılan protokollerden biri de Profinet protokolüdür. Profinet protokolündeki zafiyetlerin sömürülmesiyle sistemlere çeşitli siber saldırılar gerçekleştirilebilmektedir [65]. Bu tür saldırılara karşı SCADA sistemlerinin korunması için Profinet protokolüne özgü saldırı tespit modellerinin geliştirilmesi bu sistemlerin güvenliği açısından önem arz etmektedir.

3.2. Veri Haberleşme Teknolojileri

Günümüzde Ethernet ve Local Area Network (LAN) gibi veri haberleşme teknolojileri, endüstriyel otomasyonda bulunan kontrol sistemlerinde geniş bir kullanım alanı bulmaktadır.

3.2.1. Ethernet

Ethernet, yaklaşık 30 yıllık bir geçmişe sahip olan bir fiziksel katman yerel alan ağı teknolojisidir. 1973 yılında Xerox firması tarafından bilgisayar iş istasyonları ile yazıcılar arasında bağlantı kurmak amacıyla tasarlanmıştır. 1975 yılında Xerox, bu teknoloji için

"hata algılamalı çok noktalı veri haberleşme sistemi" adı altında patent başvurusunda bulunmuş ve 1976'da "Ethernet: yerel bilgisayar ağları için düzenlenmiş paket anahtarlama" başlıklı ilk bildiriye yayımlamıştır. 1980 yılında 10 Mbps veri hızına sahip Ethernet, "Digital/Intel/Xerox" (DIX) adı altında standart hale getirilmiştir [66].

Ethernet, cihazlar arasındaki iletişimi kolaylaştırmak için kullanılan bir ağ teknolojisidir ve hem kablolu hem de kablosuz ağlarda yaygın olarak bulunur. Genellikle bilgisayarlar arasında veri iletimini sağlamak için fiziksel bir ortam kullanır ve veri yolu tabanlı bir ağ teknolojisi olarak işlev görür. Ethernet, en yaygın kullanılan LAN teknolojisi türüdür [67].

3.2.2. Yerel alan ağları

Yerel alan ağları, kısaca "LAN" olarak bilinmektedir. Bu ağlar, sınırlı bir coğrafi bölgede bulunan bilgisayarları birbirine bağlayan ağ türleridir. LAN, genellikle dar bir alanı kapsayan ve iş istasyonları, kişisel bilgisayarlar, yazıcılar ve sunucular gibi cihazları birbirine bağlayan veri ağlarıdır [68]. LAN'larda temel özellik, sistemlerin aynı ortamda veya birbirlerine yakın mesafede olmasıdır.

LAN'ı oluşturan bileşenlerin birbirleriyle farklı şekillerde bağlantı biçimleri, topoloji terimiyle tanımlanmaktadır. Son yıllarda Ethernet, yerel ağlarda baskın bir protokol haline gelmiş ve 10/100/1000 Mbps hızlarında veri iletimi sağlayabilir hale gelmiştir. Yerel ağlar, çeşitli alanlarda ve farklı amaçlarla kullanılmaktadır. Günümüzde ofisler, üniversiteler, fabrikalar, hastaneler, laboratuvarlar, satış ve dağıtım bölümleri gibi pek çok farklı ortamda yerel ağlar kullanılmaktadır [69].

3.3. Ağ Topolojileri

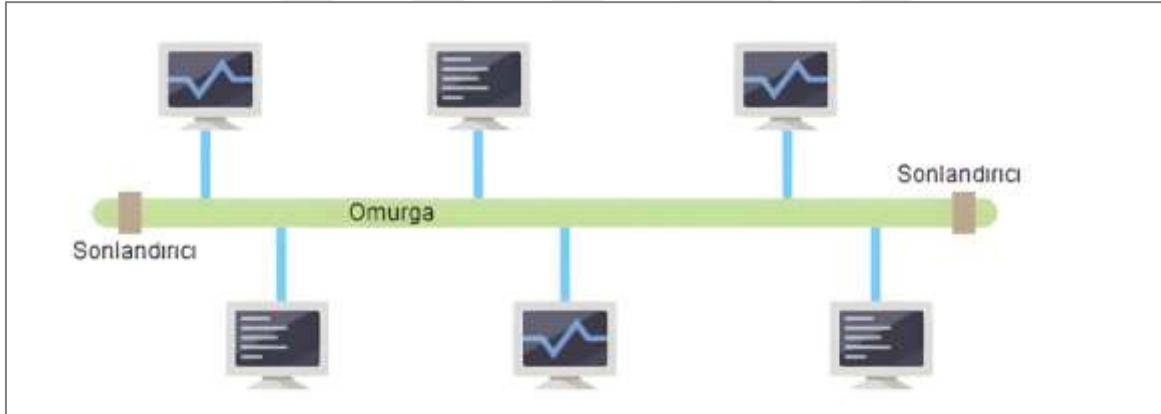
Bilgisayar ağlarının birbirine doğrudan nasıl entegre edildiğini belirleyen bir yapıdır [70]. Ağ topolojisi, ağ içerisindeki bilgisayarların ve ağ cihazlarının birbirine nasıl bağlandığını tanımlar. Yerel ağlarda sıkça kullanılan topolojiler şunlardır:

- Doğrusal (Bus) Topoloji
- Yıldız (Star) Topoloji
- Halka (Ring) Topoloji

- Ağaç (Tree) Topoloji
- Karmaşık (Mesh) Topoloji

3.3.1. Doğrusal (Bus) topoloji

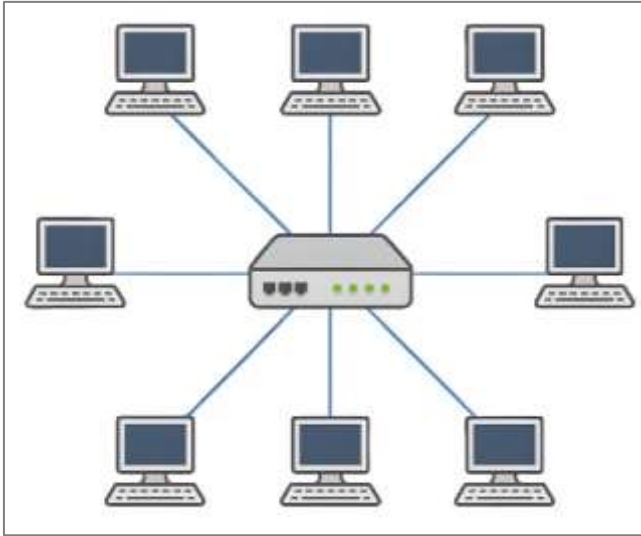
Doğrusal (Bus) topolojisinde, ağdaki tüm bilgisayarlar ortak bir kabloya (genellikle omurga olarak da adlandırılır) bağlanır [68]. Sınırlı sayıda bağlantının yer aldığı ve bilgisayarların aynı hat üzerinden veri aldığı bir topolojidir. Bir cihazdan diğerine veri gönderilmek istendiğinde, veri doğru cihaza ulaşmadan önce tüm cihazları ağ boyunca dolaşır. Bu nedenle, verimli olmayan bir yapıdır. Kurulumu basit ve maliyeti düşük olduğundan karmaşık olmayan çözümler için uygun olabilir, çünkü switch veya hub gerektirmez. Ancak, arıza tespiti zor olduğundan ve bağlantı kurulacak bilgisayar sayısının sınırlı olması nedeniyle dezavantajlıdır [71]. Doğrusal (Bus) topolojisinin genel bağlantı yapısı Şekil 3.3.'te şematik olarak gösterilmektedir.



Şekil 3.3. Doğrusal (Bus) topoloji [72]

3.3.2. Yıldız (Star) topoloji

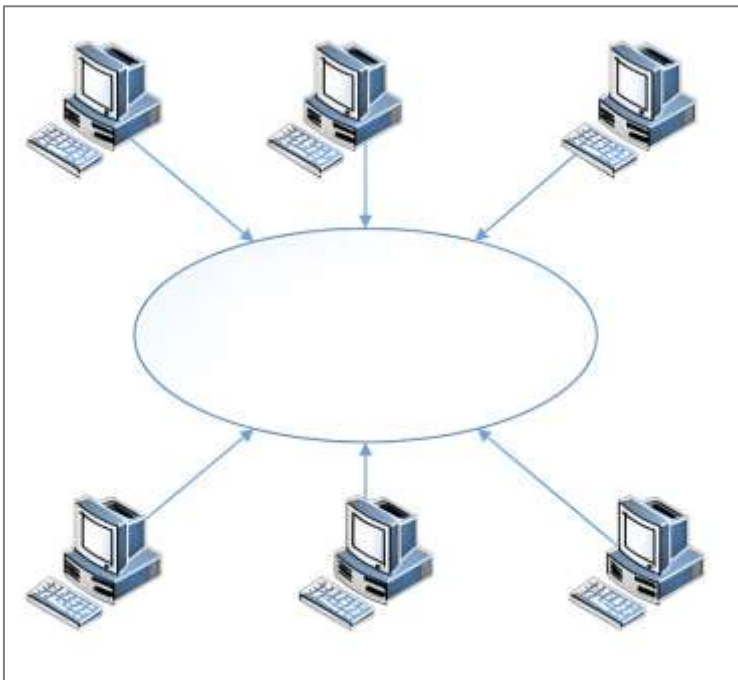
Yıldız topolojisinde, tüm cihazlar merkezi bir cihaza (örneğin, bir switch veya hub) bağlanır. Bu merkezi cihaz, ağdaki bir bilgisayardan gelen sinyali alır ve onu hedef bilgisayara iletir [68]. Yıldız (Star) topolojinin temel bağlantı yapısı Şekil 3.4'te sunulmaktadır.



Şekil 3.4. Yıldız (Star) topoloji

3.3.3. Halka (Ring) topoloji

Ring topolojisi bilgisayarlar, dairesel bir düzen içinde birbirlerine bağlanır. Bu topolojide, bilgisayarlar bir kablo üzerinde halka şeklinde yerleştirilir ve bu düzen "Ring topoloji" olarak adlandırılır. Bu yapının Bus topolojisinden farkı, kullanılan kablonun iki ucunun birbirine bağlanmış olmasıdır; yani herhangi bir sonlandırma işlemi yapılmaz [69]. Halka (Ring) topolojisine ait bağlantı yapısı Şekil 3.5'te yer almaktadır.

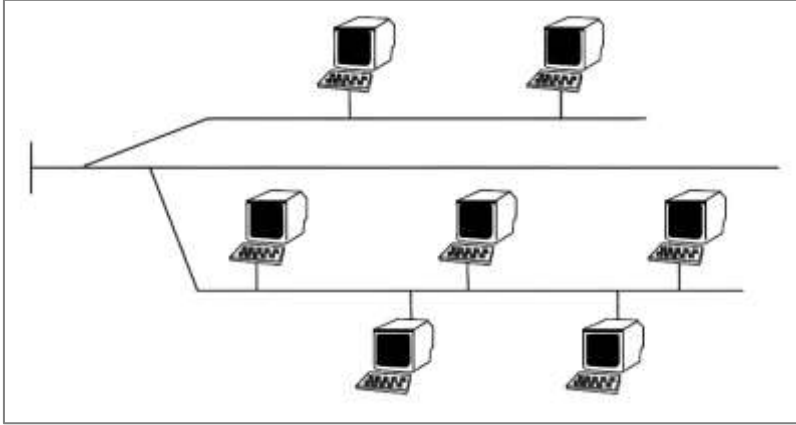


Şekil 3.5. Halka (Ring) topoloji

Ring topolojisi, gerçek dünya uygulamalarında kullanılan düzenli ağ yapılarından biridir [73]. Literatürde, bu topolojinin yaygın şekilde kullanıldığı belirtilmektedir [74]. Ayrıca, ring topolojisinin kritik altyapılarda da yer aldığı görülmektedir. Örneğin, Romanya'daki bir elektrik trafo merkezine ilişkin vaka çalışmasında, bu yapının tercih edildiği ifade edilmektedir [75].

3.3.4. Ağaç (Tree) topoloji

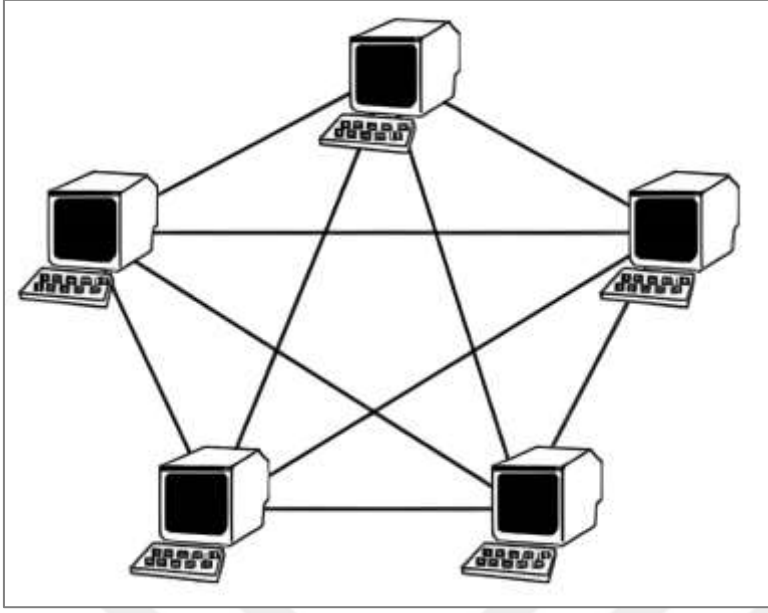
Ağaç topolojisi, bus topolojisinin dallanarak genişlemiş halidir. Bu topoloji, birbirine bağlı ve alt alta sıralanmış düğümlerden oluşmaktadır [68]. Ağaç (Tree) topolojinin bağlantı şeması Şekil 3.6'da gösterilmektedir.



Şekil 3.6. Ağaç (Tree) topoloji

3.3.5. Karmaşık (Mesh) topoloji

Karmaşık (Mesh) topolojisi, ağdaki tüm düğümlerin birbirine doğrudan bağlandığı bir topoloji türüdür. Bu yapı, aynı zamanda karmaşık topoloji olarak da bilinmektedir. Karmaşık (Mesh) topolojinin bağlantı yapısı Şekil 3.7'de şematik olarak sunulmaktadır [69].



Şekil 3.7. Karmaşık (Mesh) topoloji [69]

3.4. Kullanılan Haberleşme Protokolü Güvenlik Açıkları

İlk nesil SCADA sistemleri, yalnızca kapalı ağ yapıları içerisinde faaliyet gösterecek şekilde geliştirilmiş ve bu nedenle tasarım aşamasında siber güvenlik tehditlerine karşı herhangi bir koruma mekanizması entegre edilmemiştir [4]. Yerleşik siber güvenlik mekanizmalarının bulunmaması, SCADA sistemlerinde ciddi güvenlik zaafiyetlerinin oluşmasına zemin hazırlamaktadır. SCADA sistemleri, saldırganlar tarafından ağ üzerinden yetkisiz erişim sağlandığında manipülasyona açık hale gelir. Bu durum, haberleşme altyapısının güvenliğini son derece kritik kılmaktadır.

Tez kapsamında kullanılan PROFINET protokolü, Profibus & Profinet International ve Siemens iş birliğiyle geliştirilen, endüstriyel otomasyon sistemlerinde veri toplama ve kontrol işlemlerini gerçekleştirmek amacıyla tasarlanmış, Ethernet tabanlı ve açık mimariye sahip bir haberleşme protokolüdür. Fiziksel iletim ortamı olarak Ethernet'i kullanan PROFINET, TCP/IP ve diğer Bilgi Teknolojileri (BT) standartlarıyla uyumlu şekilde çalışmaktadır. Bu yönüyle, geleneksel PROFIBUS mimarisinin Ethernet ve IP protokol desteğiyle evrilmiş bir versiyonu olarak değerlendirilebilir [76].

Gerçek zamanlı iletişimi destekleyen bir Ethernet tabanlı protokol olan PROFINET, Ethernet altyapısının taşıdığı güvenlik risklerine karşı hassasiyet göstermektedir [77].

Akerberg ve Bjorkman tarafından yapılan çalışmada, PROFINET protokolüne yönelik bir ortadaki adam saldırısının gerçekleştirilebildiği gösterilmiştir [78].

Dünya genelinde kabul gören standartlar ve güvenlik rehberleri yayımlayan Ulusal Standartlar ve Teknoloji Enstitüsü (NIST - National Institute of Standards and Technology) veritabanında, PROFINET protokolüne ilişkin hizmet reddi (DoS), komut enjeksiyonu ve diğer saldırı türlerine yönelik tespit edilmiş güvenlik açıklarına yer verildiği görülmektedir [79]. Örneğin, 2024 yılında PROFINET protokolünde tespit edilen bir güvenlik açığının, saldırganların cihazın yanıt verememesine neden olacak şekilde hizmet reddi (DoS) saldırısı gerçekleştirmesine olanak tanıdığı ve bu zafiyetin CVE-2024-48989 kimliğiyle güvenlik veritabanına kaydedildiği belirtilmiştir [79]. Özellikle Address Resolution Protocol (ARP) spoofing, yetkisiz erişim, DoS ve replay saldırıları gibi tehditler, sistemin işleyişini bozabilir veya kontrolün ele geçirilmesine neden olabilir. Ayrıca trafik dinleme ve komut enjeksiyonu gibi saldırılarla veri bütünlüğü ve operasyonel güvenlik riske atılmaktadır. Bu tür zafiyetler, PROFINET protokolünün güvenli konfigürasyonlarla ve çok katmanlı savunma yöntemleriyle korunmasını gerekli kılmaktadır.

PROFINET protokolünün kötüye kullanımını engellemek amacıyla, ağ trafiğinin denetlenmesi kritik öneme sahiptir. Bu doğrultuda, güvenlik duvarları ve EKS uyumlu saldırı önleme sistemleri, yalnızca yetkili alanlardan gelen PROFINET trafiğine izin verecek şekilde konfigüre edilmelidir [76]. PROFINET tabanlı sistemlerde çok katmanlı güvenlik önlemleri uygulanması kritik öneme sahiptir.

3.5. EKS/SCADA Sistemlerine İlişkin Siber Saldırıları

SCADA sistemlerinin konuşlandırıldığı endüstriyel ortamlarda, siber güvenlik zafiyetlerinin keşfi, mevcut zafiyetlerin sürekliliği, belirlenen zafiyetlerin kötü niyetli aktörler tarafından istismarı, sistem bütünlüğünün ihlali veya operasyonel sürekliliğin sekteye uğratılması gibi senaryolar günümüzün gerçekçi tehdit vektörleri arasında yer almaktadır.

Sistemlerin uzaktan kontrol altına alınması veya enerji kesintileri nedeniyle ortaya çıkan operasyonel aksaklıklar, olası senaryolar arasında yer almaktadır. Özellikle elektrik üretim tesislerinin siber saldırılara maruz kalması sonucunda, geniş çaplı elektrik kesintileri veya kentsel alanların aydınlatma yetersizliği gibi durumlar ortaya çıkabilir [4].

Kritik altyapılara yapılmış çeşitli siber saldırı örnekleri bulunmaktadır. Örneğin, 5 Şubat 2021'de gerçekleşen Oldsmar Saldırısı, TeamViewer kullanılarak bir tesis operatörünün konsoluna erişilmesiyle yapılmıştır. Saldırgan, tesisin HMI aracılığıyla suyun sodyum hidroksit içeriğini toksik seviyelere çıkarmaya çalışmış, ancak operatörün müdahalesiyle saldırı 3-5 dakika içinde durdurulmuştur. Sodyum hidroksit, suyun asidik seviyesini düzenlemek için kullanılan ve yüksek dozda maruz kalındığında sağlık sorunlarına yol açabilen bir madde olup, saldırırganın konumu belirsizdir. Bu olay, kritik altyapılara yönelik en önemli siber saldırılardan biri olarak değerlendirilmektedir [80].

SCADA sistemleri, hem kısmi hem de tamamlayıcı düzeyde siber saldırılara maruz kalabilir. Bu tür saldırılar, yalnızca SCADA sistemlerinin işleyişini değil aynı zamanda bu sistemlerle entegre olan diğer altyapıları da olumsuz etkileyebilir. Günümüzde, SCADA sistemlerindeki güvenlik açıkları kullanılarak gerçekleştirilen saldırılar, toplumsal düzeni bozma, günlük yaşamı aksatma veya halk sağlığını tehdit etme potansiyeline sahiptir. Bu nedenle, SCADA sistemlerinin siber güvenliğinin sağlanması, hem ekonomik hem de sosyal açıdan kritik bir gereklilik haline gelmiştir.

3.5.1. MITM saldırıları

MITM saldırıları, iki uç cihaz (örneğin bir HMI ve PLC) arasındaki haberleşmeye gizlice müdahale eden ve bu sayede verilerin izinsiz olarak ele geçirilmesini veya değiştirilmesini mümkün kılan siber saldırı türleridir. Saldırgan, istemci ve sunucu arasındaki veri alışverişinde araya girerek, tarafların haberi olmadan paketleri dinleyebilir, manipüle edebilir veya yönlendirebilir. Özellikle SCADA ve diğer endüstriyel kontrol sistemlerinde, bu tür saldırılar süreç güvenliğini ve operasyonel sürekliliği doğrudan tehdit eder. Ağ iletişimini hedef alan tekniklerle gerçekleştirilen MITM saldırıları arasında ARP sahtekârlığı, Domain Name System (DNS) sahtekârlığı ve Dynamic Host Configuration Protocol (DHCP) aldatma gibi yöntemler yer almaktadır [81].

ARP spoofing saldırısı

MITM saldırıları çeşitli tekniklerle gerçekleştirilebilmekle birlikte, yerel ağlar üzerinde en sık kullanılan yöntemlerden biri ARP Spoofing tekniğidir. Adres Çözümleme Protokolü (Address Resolution Protocol-ARP), IP adreslerini ilgili fiziksel ağ adresleri (Media Access

Control-MAC) ile ilişkilendiren, bağlantı durumunu izlemeyen (stateless) bir iletişim protokolüdür. Anahtarlanmış yerel alan ağlarında, her cihaz kendi ARP önbelleğinde IP ve MAC adres çiftlerini içeren geçici bir tabloyu tutarak yönlendirme işlemlerini gerçekleştirir [82]. Ancak ARP kimlik doğrulama veya paket denetimi gibi kontroller içermediğinden, saldırganlar bu zafiyetten yararlanarak ağ trafiğini manipüle edebilir.

DNS sahtekârlığı saldırısı

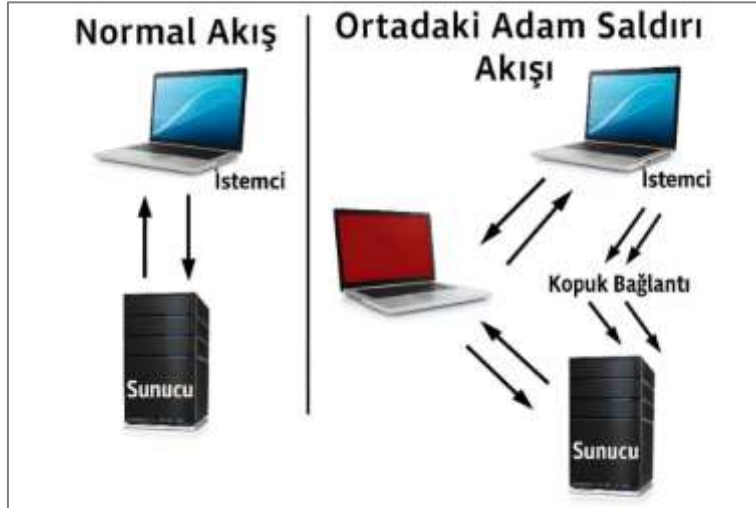
DNS, kullanıcıların erişmek istediği alan adlarını, bilgisayar sistemlerinin iletişim kurmak için kullandığı sayısal IP adreslerine çeviren temel bir ağ hizmetidir. DNS sahtekârlığı, DNS'in bütünlüğünü ve güvenilirliğini tehdit eden ciddi bir siber güvenlik ihlalidir. DNS sahtekârlığı saldırılarında, kötü niyetli aktörler, DNS protokolünün çözümleme aşamasında ortaya çıkan güvenlik açıklarını kullanarak, istemcilerin meşru adresler yerine sahte IP adreslerine yönlendirilmesini amaçlamaktadır [83]. Bu bağlamda, insan ile makine arasındaki iletişimin temelini oluşturan bu dönüştürme süreci, sahip olduğu yapısal önemi nedeniyle siber tehdit aktörlerinin hedeflerinden biri hâline gelebilir.

DHCP aldatma

Bir DHCP istemcisi, ağda IP adresi almak amacıyla yayın yoluyla bir keşif mesajı gönderdiğinde, bu mesaj yalnızca meşru DHCP sunucuları tarafından değil, aynı zamanda kötü niyetli aktörler tarafından da algılanabilir. Eğer ağda bulunan sahte bir DHCP sunucusu, istemciye yetkili DHCP sunucusundan daha hızlı yanıt verirse ya da meşru sunucunun IP havuzu tükenmişse, istemcinin yapılandırma bilgileri bu sahte sunucudan alınabilir. Bu durumda saldırgan, istemci cihaza istediği IP adresi, alt ağ maskesi, ağ geçidi ve DNS bilgilerini ileterek cihazın ağ yapılandırmasını kendi kontrolü altına alır. İstemci, aldığı bu yanıtla göre yapılandırma ayarlarını otomatik olarak günceller [84].

Şekil 3.8'de, istemci ve sunucu arasında gerçekleşen doğrudan veri akışı (Normal Akış) ile siber saldırı sırasında oluşan müdahaleye uğramış veri trafiği (Ortak Adam Saldırı Akışı) karşılaştırılması gösterilmektedir [85]. Normal ağ iletişiminde veri, istemci ile sunucu arasında doğrudan ve çift yönlü olarak iletilirken; MITM saldırısı senaryosunda, bu iletişim trafiği saldırganın aracılığıyla yönlendirilir. Bu durum, saldırganın hem istemciden gelen hem de sunucudan iletilen veriyi gözlemleme, değiştirme veya engelleme yetisine sahip

olmasına neden olur. Böylece, iletişimin gizliliği, bütünlüğü ve güvenilirliği ciddi şekilde zedelenmiş olur.



Şekil 3.8. Normal ağ trafiği ve MITM saldırısı ağ trafiği [85]

3.5.2. DoS saldırıları

Bilişim sistemlerinde en sık karşılaşılan saldırı türlerinin başında DoS ve DDoS saldırıları yer almaktadır. DoS saldırısı, temel olarak bir sunucunun, meşru kullanıcıların hizmet taleplerine yanıt veremez duruma getirilmesini amaçlayan bir saldırı türüdür. Bu tür saldırılarda, hedef sistemin işlem gücü aşırı taleple meşgul edilerek sistem kaynaklarının tükenmesi sağlanır ve böylece sistem, herhangi bir yetkisiz erişim olmadan hizmet dışı bırakılır. Eğer bu saldırı, birden fazla cihaz aracılığıyla eşzamanlı olarak gerçekleştirilirse, bu durum DDoS saldırısı olarak adlandırılır [86].

Yerel ağda kablolu Ethernet altyapısı üzerinden gerçekleştirilebilen birçok DoS saldırısı arasında User Datagram Protocol (UDP) Flooding, Internet Control Message Protocol (ICMP) Flooding ve TCP SYN Flood gibi saldırı yöntemleri bulunmaktadır.

UDP flooding saldırıları

UDP Flooding saldırısı, saldırganın hedef sisteme çok sayıda rastgele sahte UDP paketi göndererek, sistemin kaynaklarını ve/veya ağ bant genişliğini tüketmesini amaçlayan bir DoS saldırısıdır. Bu saldırılar sonucunda, işlemci ve ağ kaynaklarının aşırı kullanımına neden olarak sistemin yanıt veremez hâle gelmesine yol açabilir [4].

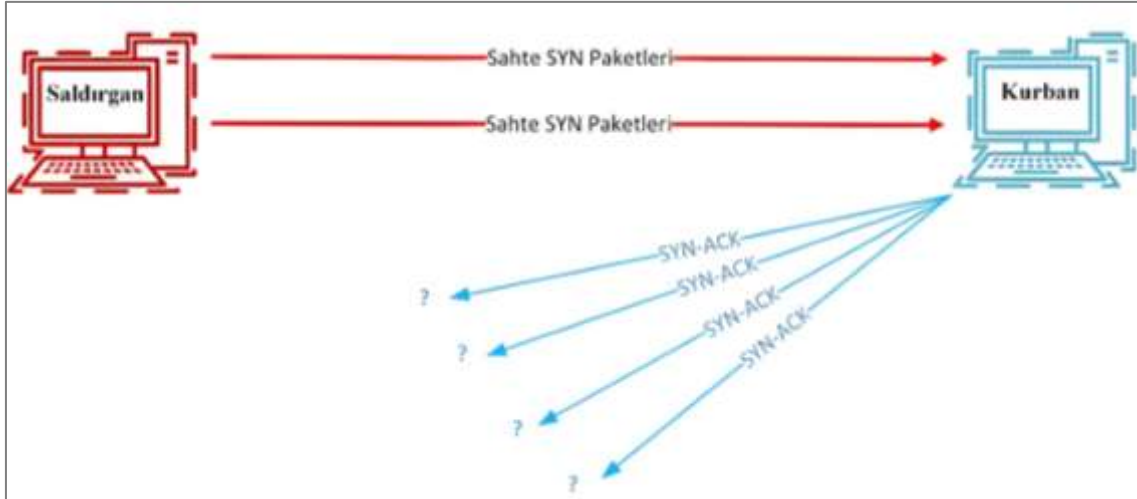
ICMP flooding saldırıları

ICMP Flooding saldırısı, saldırganın kısa süre içerisinde hedef sisteme yoğun miktarda ping paketi göndererek, sistemin işlem gücünü ve ağ bant genişliğini tüketmesini amaçlayan bir DoS saldırı türüdür. Bu saldırı sonucunda hedef sistem, gelen isteklere cevap vermekte zorlanır veya tamamen erişilemez duruma gelir [4].

TCP SYN flood saldırıları

SYN Flood saldırısı, TCP protokolünün üç yönlü el sıkışma (three-way handshake) mekanizmasını hedef alan ve en yaygın görülen DoS saldırılarından biridir. Bu saldırıda, saldırgan hedef sistemlere yüksek sayıda TCP SYN paketi gönderir ve her bir SYN paketi karşılığında hedef sistem SYN-ACK yanıtı üretir. Ancak saldırgan bağlantıyı tamamlamak için gerekli olan ACK paketini göndermez. Bu durum, hedef sistemin her bağlantı için bellekte kaynak ayırmasına ve bağlantıyı yarı açık (half-open) durumda tutmasına neden olur. Yeterli sayıda yarı açık bağlantı oluştuğunda, sistemin bellek ve işlem gücü tükenerek meşru bağlantılara hizmet veremez hâle gelir [4].

Şekil 3.9’da DoS saldırısının şematik gösterimi bulunmaktadır [4]. Şemada görüldüğü üzere saldırgan, hedef sisteme çok sayıda sahte Synchronize (SYN) paketi göndererek bağlantı taleplerinde bulunmaktadır. Hedef sistem, her bir SYN isteğine karşılık olarak SYN-ACK (Acknowledgement) yanıtı üretmekte ve bağlantının tamamlanmasını beklemektedir. Ancak saldırgan bu süreci kasıtlı olarak tamamlamadığından, hedef sistemde çok sayıda yarı açık bağlantı oluşmakta ve kaynaklar hızla tükenmektedir. Bu durum, sistemin ağ trafiğini yönetmede zorlanmasına, altyapı performansının ciddi şekilde bozulmasına ve hizmetlerin geçici veya kalıcı olarak devre dışı kalmasına neden olmaktadır.



Şekil 3.9. DoS saldırısı şematik gösterimi [4]

3.5.3. Komut enjeksiyonu saldırıları

Komut enjeksiyonu, saldırganın bir uygulamanın kullanıcı giriş verisini yeterince filtrelemediği durumlarda, girdiye zararlı sistem komutları enjekte ederek hedef sistemde komut çalıştırmasını sağlamasına olanak tanıyan bir güvenlik açığıdır. Saldırgan bu açıklardan yararlanarak sistemde yetkisiz işlemler gerçekleştirebilir, verilere erişebilir veya hizmet aksamasına neden olabilir [87].

Şekil 3.10'da bir komut enjeksiyonu saldırısının temel işleyiş akışı sunulmaktadır [88]. Saldırgan, sistemin kullanıcı girdisi aldığı bir alana meşru veriyle birlikte zararlı bir kabuk (shell) komutu enjekte eder. Uygulama bu girdiyi yeterli doğrulama veya filtreleme gerçekleştirmeksizin sunucuya ilettiğinde, söz konusu zararlı komut sistem düzeyinde çalıştırılır (Komutun Yürütülmesi). Bunun sonucunda, sistem komutunun çıktısı ve saldırganın ilettiği kötü amaçlı komutlar saldırgana geri döner. Bu durum, sistemin gizliliğini, bütünlüğünü ve güvenliğini ihlal ederek, saldırgana yetkisiz erişim olanağı sağlar.

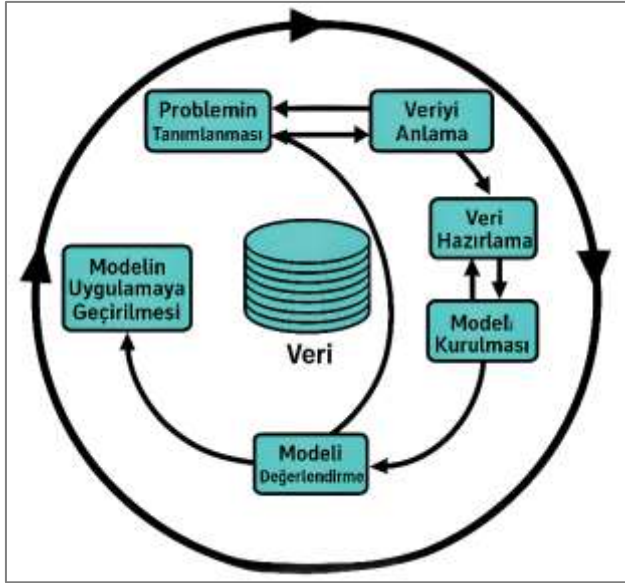


Şekil 3.10. Komut enjeksiyonu saldırısının şematik gösterimi [88]

3.6. Kullanılan Makine Öğrenmesi Tabanlı Modeller

Literatür incelendiğinde, SCADA sistemlerine yönelik saldırıların tespitinde makine öğrenmesi tabanlı yöntemlerin yaygın olarak kullanıldığı görülmektedir. Bu çalışmada, SCADA sistemi kullanılan bir test yatağı ortamında gerçekleştirilen DoS, MITM ve Komut Enjeksiyonu gibi saldırıların tespiti ve ilgili saldırı türlerinin sınıflandırılması amacıyla makine öğrenmesi tabanlı modeller kullanılmıştır.

Makine öğrenmesi süreci, problemin tanımlanması, veriyi anlama, veri hazırlama, modelin kurulması, modeli değerlendirme ve modelin uygulamaya geçirilmesi olmak üzere altı aşamadan oluşmaktadır. Bu süreç Şekil 3.11’de şematik olarak sunulmaktadır [89].



Şekil 3.11. Makine öğrenmesi süreci

Makine öğrenmesi, genellikle örneklerden öğrenmeye dayanan bir yaklaşım olup; denetimli öğrenme (sınıflandırma ve öngörü), denetimsiz öğrenme (kümeleme), yarı-denetimli öğrenme ve pekiştirmeli öğrenme olmak üzere dört temel yönteme ayrılmaktadır [90]. Bu çalışmada kullanılan veriler, üç saldırı senaryosu ve bir normal durum senaryosunu içeren etiketli bir yapıya sahip olduğundan, denetimli öğrenme yöntemi kullanılmıştır.

Literatürde yaygın olarak kullanılan KNN, NB, DT, LR algoritmaları, öncelikle tekil olarak incelenmiş, daha sonra ise birlikte kullanılarak hibrit yaklaşımlar geliştirilmiş ve bu modeller üzerinde çeşitli testler uygulanmıştır. Geliştirilen tüm modeller performans metrikleri doğrultusunda karşılaştırılmış ve elde edilen sonuçlar Çizelge 5.1’de sunulmuştur.

Bu bölümde, kullanılan makine öğrenmesi modellerine ilişkin açıklamalara yer verilmiştir.

3.6.1. KNN modeli

Thomas M. Cover ve Peter E. Hart tarafından geliştirilen K-NN algoritması, veri noktalarını en benzer komşu örneklerle dayanarak sınıflandıran bir denetimli öğrenme yöntemidir. K-NN algoritması, genellikle ANN ve SVM gibi daha karmaşık sınıflandırma yöntemleriyle karşılaştırmalarda referans olarak kullanılan, sağlam ve güvenilir bir sınıflandırma algoritmasıdır [91].

KNN algoritmasında komşuluk ilişkilerini belirlemek amacıyla farklı mesafe ölçütleri kullanılabilir. Bu ölçütler arasında genellikle Öklidyen kullanılmakla birlikte Manhattan, Minkowski ve Hamming mesafeleri de kullanılabilen diğer ölçütlerdir. Öklidyen mesafe, çok boyutlu öznitelik uzayında iki veri noktası arasındaki düz çizgi (doğrusal) uzaklığı hesaplayarak benzerlik ölçümü sağlar ve KNN algoritmasında en sık tercih edilen yöntemlerden biridir. Manhattan mesafesi, veri noktaları arasındaki uzaklığı; her bir karşılık gelen öznitelik arasındaki mutlak farkların toplamı şeklinde hesaplar. Minkowski mesafesi, Öklidyen ve Manhattan mesafelerinin genelleştirilmiş formudur ve mesafe hesaplamalarında farklı boyutlara duyarlılığı kontrol etmeye olanak tanıyan bir parametre içerir. Hamming mesafesi ise ikili (binary) özniteliklerden oluşan veri kümelerinde veya ikili vektörlerin karşılaştırılmasında kullanılır; iki vektör arasında farklılık gösteren pozisyonların sayısını temel alır [92].

Öklidyen uzaklık;

$$d(P, Q) = \sqrt{\left\{ \sum_{i=1}^n (p_i - q_i)^2 \right\}} \quad (3.1)$$

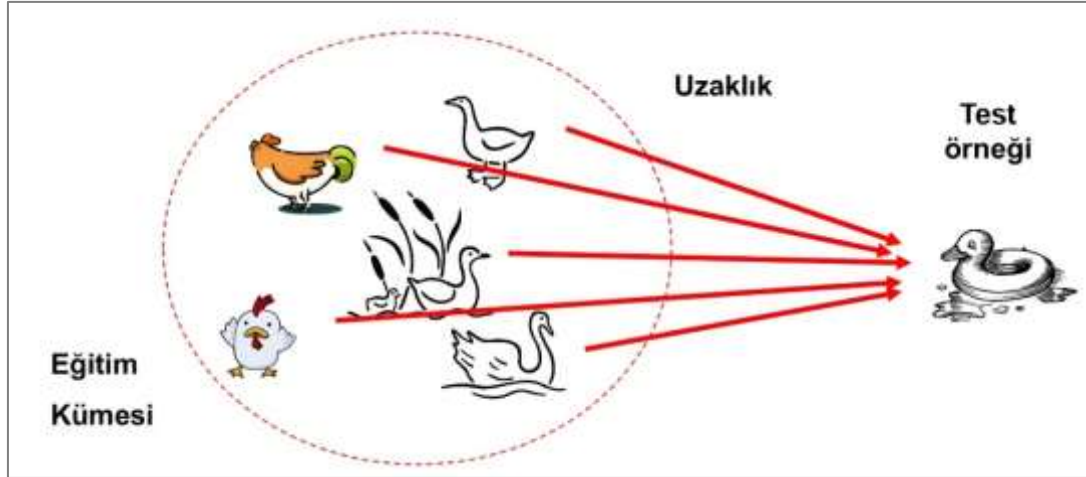
Manhattan uzaklık;

$$d(P, Q) = \sqrt{\left\{ \sum_{i=1}^n |p_i - q_i| \right\}} \quad (3.2)$$

Minkowski uzaklık;

$$d_{r(P,Q)} = \left(\sum_{i=1}^n |p_i - q_i|^r \right)^{\frac{1}{r}} \quad (3.3)$$

Şekil 3.12'de, KNN modelinin temel sınıflandırma süreci görselleştirilmiştir. Test örneği, eğitim kümesindeki her bir örnekle olan uzaklığına göre değerlendirilir. En yakın k komşu belirlenerek bu komşular arasında en sık karşılaşılan sınıfa test örneği atanır. Bu yaklaşım, özellikle sınıf dağılımının belirgin olduğu veri kümelerinde etkili sonuçlar verir. Şekilde test örneği ördek olarak temsil edilmekte olup, en yakın komşularının büyük kısmı aynı sınıfa ait olduğunda doğru sınıflandırma gerçekleştirilir.



Şekil 3.12. KNN modelinin temel çalışma mantığı [93]

Çizelge 3.1. KNN modelinin avantajları ve dezavantajları [91]

Avantajlar	Dezavantajlar
KNN algoritması, kavranması ve uygulanması açısından oldukça basit ve sezgiseldir.	Tüm örneklerin bellekte saklanması gerektiğinden yüksek hafıza gereksinimi doğar.
Diğer denetimli öğrenme algoritmalarının aksine, KNN algoritması klasik anlamda bir model eğitimi gerçekleştirmez. Bunun yerine, eğitim verileri yalnızca referans olarak saklanır ve sınıflandırma süreci test sırasında gerçekleştirilir.	Dengesiz sınıf dağılımına sahip veri kümelerinde sınıflandırma performansı düşebilir.
Hem sınıflandırma hem de regresyon problemlerinde uygulanabilirlik göstermektedir.	Yüksek boyutlu veri kümelerinde işlem maliyeti artar; algoritmanın verimliliği azalır.
Hafıza tabanlı yapısı sayesinde yeni verilerle kolayca güncellenebilir.	Yeni bir örneğin sınıflandırılması, tüm veri kümesine olan uzaklıkların hesaplanmasını gerektirdiğinden zaman açısından maliyetlidir.
Gerçek zamanlı uygulamalarda, giriş verisindeki değişimlere hızlı yanıt verebilir.	Eksik veri değerleriyle doğrudan başa çıkma yeteneğine sahip değildir.
Çok sınıflı sınıflandırma problemlerine kolaylıkla uyarlanabilir.	Modelin başarımı; komşu sayısı (k), uzaklık metriği ve öznitelik sayısı gibi hiperparametrelere duyarlıdır.
Kullanıcıya farklı uzaklık ölçütleri seçme esnekliği sunar.	Uzaklık temelli karar verdiği için aykırı değerlere karşı oldukça hassastır.

3.6.2. NB modeli

Naive Bayes sınıflandırıcısı, Bayes teoremine dayanan ve sınıflar ile öznitelikler arasındaki ilişkileri olasılık temelli modelleyen denetimli bir öğrenme algoritmasıdır. Adını, 1702–1761 yılları arasında yaşamış matematikçi Thomas Bayes’ten alır ve ilk olarak 1973’te sınıflandırma problemlerinde kullanılmış, 1992’de yaygın olarak tanımlanmıştır. En temel varsayımı, tüm özniteliklerin birbirinden bağımsız olduğu ve sınıfa eşit derecede katkı sağladığıdır. Bu varsayım genellikle gerçek dünyada tam olarak sağlanmasa da, algoritma birçok uygulamada beklenenden iyi performans sergileyebilir. Özellikle metin

sınıflandırma, e-posta filtreleme ve tıbbi teşhis gibi alanlarda başarıyla kullanılmaktadır. Hızlı, basit ve etkili yapısı sayesinde sık tercih edilen bir yöntemdir [91].

Naive Bayes sınıflandırıcıları arasında en yaygın olarak kullanılan Multinomial, Bernoulli ve Gaussian gibi çeşitli Bayes sınıflandırıcıları, özelliklerin birbirinden bağımsız olduğu varsayımı altında, farklı uygulama alanlarında kullanılmaktadır [94, 95].

Genel Bayes Teoremi,

$$P(A | B) = [P(B | A) \cdot P(A)] / P(B) \quad (3.4)$$

Gaussian Naive Bayes,

$$P(x_j | c_i) = (1 / \sqrt{(2\pi\sigma_{ji}^2)}) \times \exp(-((x_j - \mu_{ji})^2 / (2\sigma_{ji}^2))) \quad (3.5)$$

Çizelge 3.2. NB modelinin avantajları ve dezavantajları [91, 96-98]

Avantajlar	Dezavantajlar
Hesaplaması hızlıdır ve büyük veri kümelerinde etkili çalışır.	Özellikler arası bağımsızlık varsayımı gerçek verilerde çoğu zaman geçerli değildir.
Uygulaması ve kodlaması oldukça kolaydır.	Özellikler arası güçlü ilişki varsa performans ciddi şekilde düşebilir.
Eğitim süresi kısadır, yeni verilere kolayca uygulanabilir.	Sürekli verilerde dağılım varsayımı (örneğin Gaussian) her zaman uygun olmayabilir.
Az sayıda veriye rağmen sınıflandırma başarısı gösterebilir.	Özellikle düşük sayıda örnek içeren sınıflarda kesinlik ve F1-Score gibi metriklerde dengesizlik görülebilir.
Yorumlanabilirliği yüksektir (olasılık temelli karar verir).	Veri ön işleme (örneğin varyansı sıfır olan sütunların çıkarılması) gerekebilir.

3.6.3. DT modeli

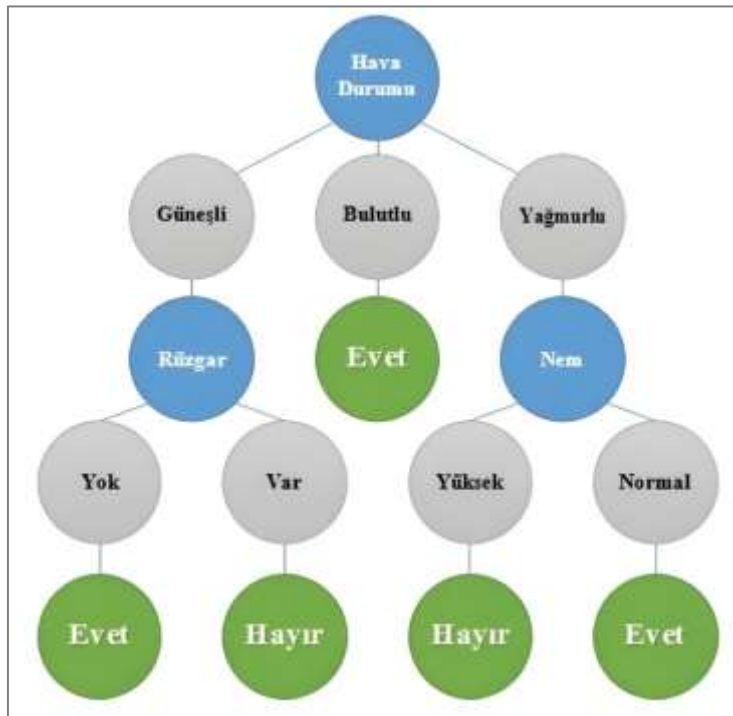
Karar ağaçları, hem sınıflandırma hem de regresyon problemleri için kullanılan, denetimli ve parametrik olmayan bir makine öğrenmesi algoritmasıdır. If-then-else şeklindeki karar kurallarını eğitim verileri üzerinden öğrenerek ağaç yapısında modeller. Hem sayısal hem de kategorik verilerle çalışabilir. Yorumlanabilirliği yüksek olduğundan sık tercih edilir [97]. Karar ağaçlarında sınıflandırma yöntemleri, yalnızca kategorik verilerle çalışan Iterative Dichotomizer 3 (ID3) (Quinlan, 1986) ve hem kategorik hem sayısal verileri işleyebilen C4.5 (Quinlan, 1993) gibi entropiye dayalı algoritmalar ile Gini indeksi veya Twoing algoritmasını kullanan, hem sınıflandırma hem de regresyon görevlerine uygun

Classification and Regression Trees (CART) algoritması olmak üzere iki temel grupta incelenmektedir.

Gini kriteri

Gini algoritması, CART yapısında kullanılan bir bölme kriteridir. Bu yöntemde her karar düğümü, ağacı iki alt dala ayıracak şekilde yapılandırılır. Hangi özelliğe göre ve hangi eşik değeriyle bölme yapılacağı, Gini indeksi hesaplanarak belirlenir. Gini indeksi, veri kümesindeki sınıf dağılımının homojenliğini ölçer; değerlerin eşit olması, sınıfların benzer oranda dağıldığını gösterir. Eğer bir değişken çok sayıda kategori içeriyorsa, ikili bölme şartı nedeniyle benzer kategoriler bir araya getirilerek gruplanır [99].

Hava durumu değişkenlerine bağlı olarak bir etkinliğin yapılıp yapılmayacağına ilişkin karar sürecini gösteren karar ağacı modeli temel çalışma mantığı örneği Şekil 3.13'te sunulmaktadır. Ağaç yapısı, “Hava Durumu” özelliği ile başlamakta ve sırasıyla “Rüzgâr” ve “Nem” gibi alt değişkenlerle ikili dallara ayrılmaktadır. Örneğin, hava durumu güneşli ise karar, rüzgârın varlığına göre şekillenmekte; rüzgâr yoksa “Evet”, varsa “Hayır” sonucu üretilmektedir. Bu yapı, karar ağaçlarının if-then-else kurallarına dayalı olarak nasıl çalıştığını ve yorumlanabilirliğinin yüksek olduğunu göstermektedir.



Şekil 3.13. Karar ağacı modelinin temel çalışma mantığı örneği

Çizelge 3.3. Karar ağacı modelinin avantajları ve dezavantajları [100]

Avantajlar	Dezavantajlar
Karar ağaçları açıklayıcıdır ve profesyonel olmayan kullanıcılar tarafından kolayca anlaşılabilir.	Küçük veri değişiklikleri, ağaç yapısında büyük değişimlere neden olabilir, bu da modelin kararlılığını azaltır.
Hem sayısal hem de kategorik verilerle çalışabilir ve eksik ya da hatalı verilerle başa çıkabilir.	Aşırı öğrenme (overfitting) eğilimi yüksektir, bu nedenle budama gibi önlemler alınması gerekebilir.
Parametrik olmayan bir yöntemdir; veri dağılımı veya sınıf yapısı hakkında herhangi bir varsayımda bulunmaz.	Karmaşık öznitelik etkileşimleri içeren veri kümelerinde performansı düşebilir.
Sınıflandırma maliyeti yüksek olan uygulamalarda, yalnızca karar yolundaki özniteliklerin değerlendirilmesi nedeniyle daha verimli çalışabilir.	Bazı algoritmalar (örneğin ID3, C4.5) yalnızca ayrık hedef değişkenler ile çalışabildiğinden sınırlayıcı olabilir.

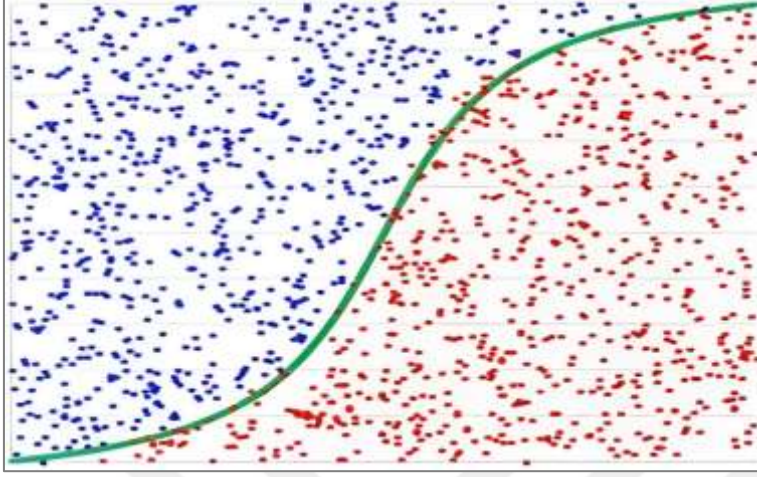
3.6.4. LR modeli

Lojistik regresyon, diskriminatif (ayrıştırıcı) model tabanlı bir sınıflandırma yöntemidir ve bağımlı değişkenin sınıflarından birinin gerçekleşme olasılığını tahmin etmeye yönelik bir analiz tekniğidir. Model, bağımsız değişkenlerin sürekli ya da kesikli olmasına ilişkin herhangi bir kısıtlamaya sahip değildir. Lojistik regresyon, bağımsız değişkenleri girdi olarak alır ve çıktı olarak 0 ile 1 arasında yorumlanabilir olasılık değerleri üretir. Bu bağlamda, genellikle 1 başarılı/pozitif, 0 ise başarısız/negatif durumu temsil eder. Modelin amacı, veriye en uygun lojistik fonksiyonu tanımlayarak regresyon katsayılarını optimize etmektir [91]. Lojistik regresyon modellerinde katsayı tahmini için başlıca yöntemler; en büyük olabilirlik (maximum likelihood), yeniden ağırlıklandırılmış iteratif en küçük kareler (Recursively Iterated Least Squares-RILS) ve dereceli iniş (gradient descent) algoritmalarıdır. Bu yöntemler, modelin veriye en uygun şekilde öğrenmesini sağlamak amacıyla katsayıları iteratif olarak optimize eder.

Genel olarak, en çok olabilirlik yöntemi, gözlemlenen veri kümesinin mevcut model altında gerçekleşme olasılığını en yüksek düzeye çıkaran parametre (katsayı) değerlerini tahmin etmeyi amaçlar.

Şekil 3.14'teki görsel, lojistik regresyonun iki sınıfı birbirinden ayırmak için kullandığı karar sınırını göstermektedir. Mavi ve kırmızı noktalar farklı sınıflara ait verileri temsil ederken, aradaki yeşil eğri modelin öğrenmiş olduğu karar sınırını göstermektedir. Bu eğri, lojistik fonksiyonun olasılık çıktısı üzerinden sınıflandırma yaptığı bölgeyi tanımlamaktadır. Her ne kadar bu görsel ikili sınıflandırmayı yansıtsa da, çok sınıflı problemler için "bir sınıfa karşı diğerleri

(one-vs-rest)" veya "birbirine karşı ikili sınıflar (one-vs-one)" stratejileri ile birden fazla lojistik regresyon modeli oluşturularak benzer ayrımlar yapılmaktadır.



Şekil 3.14. Lojistik regresyon modeli temel çalışma prensibi

Çizelge 3.4. Lojistik regresyon modelinin avantajları ve dezavantajları [101]

Avantajlar	Dezavantajlar
Veri kümesi doğrusal olarak ayrılabilir olduğunda yüksek performans gösterir.	Bağımlı ve bağımsız değişkenler arasında doğrusal ilişki varsayımı vardır.
Aşırı uyuma daha az eğilimlidir; yüksek boyutlu verilerde düzenleme ile iyileştirilebilir.	Gözlem sayısı, değişken sayısından azsa aşırı uyuma neden olabilir.
Katsayıların büyüklüğü ve işareti üzerinden değişkenlerin etkisi yorumlanabilir.	Yalnızca ayırık (categorical) çıktılar için uygundur; sürekli değişkenleri tahmin edemez.
Uygulaması ve yorumlanması kolaydır; hesaplama açısından verimlidir.	

3.6.5. KNN-NB hibrit modeli

KNN ve NB modelleri birlikte kullanılarak hibrit bir model elde edilmektedir. Bu model, hem mesafe tabanlı hem de olasılık temelli yaklaşımların avantajlarını bir araya getirerek, sınıflar arasında daha dengeli ve doğru bir sınıflandırma performansı sağlamayı amaçlamaktadır.

3.6.6. DT-LR hibrit modeli

DT ve LR modelleri birlikte kullanılarak hibrit bir model elde edilmektedir. Karar ağacı ve lojistik regresyon algoritmalarının birleşimiyle oluşturulan bu hibrit model, karar ağacının

veri ayrıştırma gücünü lojistik regresyonun doğrusal sınıflandırma yeteneğiyle birleştirerek yüksek doğruluk ve güçlü genelleme performansı hedeflemektedir.

3.6.7. KNN-NB-DT hibrit modeli

KNN, NB ve DT modelleri birlikte kullanılarak hibrit bir model elde edilmektedir. KNN, Naive Bayes ve Karar Ağacı algoritmalarının birleştirilmesiyle oluşturulan bu üçlü hibrit model, her bir algoritmanın farklı güçlü yönlerinden faydalanarak sınıflar arası ayırt ediciliği artırmayı ve genel sınıflandırma performansını iyileştirmeyi amaçlamaktadır.



4. MATERİYAL VE METOT

Bu bölümde, oluşturulan test ortamı ayrıntılı olarak açıklanmıştır. Test ortamına yönelik uygulanan saldırılar, belirlenen senaryolar çerçevesinde ele alınmıştır. Ayrıca, test ortamından elde edilen veri seti ile bu veri setinde yer alan öznitelikler hakkında kapsamlı bilgiler verilmiştir. Veri setinin analizinde kullanılacak metriklerin kavramsal çerçevesi de bu kısımda ele alınmaktadır.

4.1. Fiziksel Test Ortamı

Test ortamı, gerçek bir tesisin veya fabrikanın endüstriyel kontrol sistemlerini birebir kopyalamadan, mümkün olduğunca aslına uygun bir şekilde modelleyen bir benzetimdir [102]. Bu bölümde, oluşturulan test ortamının yapısal tasarımı, mimarisi ve işlevsel süreçleri detaylı bir şekilde açıklanmaktadır. Test ortamının kurulumu ve kullanımı, gerçek siber saldırıların gerçekleştirilmesi ve saldırı sonuçlarının gözlenmesi için uygun bir ortam sağlar. Bu kapsamda oluşturulan test ortamları, siber tehditlerin sistemler üzerindeki etkisini değerlendirmeye, güvenlik açıklarını belirlemeye ve bu açıkları gidermeye yönelik çözümler üretmeye imkân tanımaktadır. Gerçek dünyadaki saldırı senaryolarını kontrollü bir ortamda simüle ederek, saldırı tespit mekanizmalarının etkinliği ölçülebilir ve yeni savunma stratejileri geliştirilebilir. Bu tür ortamlar, akademik araştırmalara önemli katkılar sunarak, teorik bilginin pratik uygulamalarla desteklenmesine ve siber güvenlik alanında yenilikçi çözümlerin üretilmesine olanak sağlamaktadır.

Siber güvenlik alanındaki çalışmalara katkıda bulunmak amacıyla bu çalışmada, bir hidroelektrik santralin SCADA haberleşme mimarisini simüle eden bir test ortamı oluşturulmuştur. Test ortamı, iki katmanlı bir SCADA haberleşme ağı mimarisine sahip olacak şekilde tasarlanmıştır. Bu ortamda, endüstriyel sistemlerde yaygın olarak kullanılan Profinet haberleşmesi kullanılmakta olup santralin işleyişini temsilen çeşitli işlemler gerçekleştirilmektedir. Bu test ortamı, gerçek bir hidroelektrik santralin SCADA haberleşme mimarisinin sadeleştirilmiş bir benzetimini temsil etmektedir. Hidroelektrik santralin operasyonel durumu, SCADA sistemi aracılığıyla kontrol edilip izlenmektedir.

Test ortamında kullanılan ekipmanlar, tipik bir hidroelektrik santralin SCADA sistemlerinde sıklıkla kullanılan bileşenlerden seçilmiştir. Bu ekipmanlara, UUB'lere, MDB'ye ve siber

saldırı bölümlerinde kullanılan tüm donanım ve yazılımlara ait detaylı bilgiler Çizelge 4.1’de verilmiştir.

Çizelge 4.1. Test ortamında kullanılan ekipmanlar ve açıklamaları

Sıra No	Ekipmanlar ve Yazılımlar	Açıklamalar (Kullanım Amacı)
1	Endüstriyel ağ anahtarları (HirschmannRS30)	SCADA ağında ring topoloji oluşturulması ve ekipmanlar arasında veri iletiminin sağlanması
2	SIMATIC S7-1200 PLC. CPU 1212C AC/DC/RLY	Ekipmanların kontrolü ve otomasyonu
3	Gentek HT-2 sıcaklık-nem transmitteri	Uzak uç birimi-6 (PLC I0.1 girişi ve PLC Q0.5 çıkışı)
4	MDB (Laptop) Windosw 10. 11th Gen Intel(R) Core(TM) i7 2.80 GHz. 16,0 GB RAM. 64 Bit. 237 GB Harddisk. Hp Dizüstü Bilgisayar	Uzak uç birimlerinin izlenmesi ve kontrolü
5	220VAC/24VDC güç kaynağı NL1050D-24	Gerekli voltaj seviyelerinin elde edilmesi
6	(AC) 6 amperlik tek kutuplu sigorta	Aşırı yük ve kısa devre koruması
7	Ray klemens	Düzenli kurulum işlemleri
8	Cat6 kablo	Bağlantıları oluşturmak
9	Uzak uç birimi-1 (PLC Q0.0 çıkışı)	Baraj kapağı açılırken tepki verir: Yeşil led aktif
10	Uzak uç birimi-2 (PLC Q0.1 çıkışı)	Baraj kapağı kapanırken tepki verir: Yeşil led aktif
11	Uzak uç birimi-3 (PLC Q0.2 çıkışı)	İkaz kesicisi kapatılınca tepki verir: Yeşil led aktif
12	Uzak uç birimi-4 (PLC Q0.3 çıkışı)	İkaz kesicisi açılınca tepki verir: Yeşil led aktif
13	Uzak uç birimi-5 (PLC Q0.4 çıkışı)	Soğutma suyu pompası çalıştığında: Yeşil led aktif Soğutma suyu pompası durduğunda: Yeşil led pasif
14	Wireshark	Ağ trafik paketleri işlemleri
15	Saldırgan (Laptop sanal makine)	Ağ taranması ve siber saldırıların uygulanması İşletim sistemi: Kali Linux Saldırı gerçekleştirme araçları: Nmap, Netdiscover, Hping3
16	MS Excel	Ağ trafik paketlerinin saklanması ve düzenlenmesi
17	MATLAB	Saldırı tespiti ve saldırı tür tespiti yapan modellerin hazırlanması

Çizelge 4.1’de, fiziksel test ortamında kullanılan komponentler, donanım elemanları, yazılımlar ve bilgisayarlar ile bu ekipmanlar üzerinde kullanılan yazılımlar ve gerçekleştirilen fonksiyonlar belirtilmiştir. Fiziksel test ortamında kullanılan ekipmanlara ilişkin görseller, Şekil 4.1’de sunulmaktadır.

Şekil 4.1’de gösterilen Hirschmann BRS30 model endüstriyel ağ anahtarları, zorlu çevresel koşullara karşı yüksek dayanıklılık sağlayacak şekilde tasarlanmıştır. Bu cihazlar, aşırı sıcaklık değişimlerine, düşük sıcaklıklara ve titreşimli çalışma ortamlarına karşı direnç göstererek endüstriyel veri iletişim sistemlerinde güvenilir bir performans sergilemektedir. Yönetilebilirlik özelliği sayesinde ağ yönetimini optimize etme imkânı sunan bu anahtarlar, 12/24/48V DC besleme gerilimi ile çalışmakta olup, -40 ile +70 °C arasındaki geniş sıcaklık aralığında stabil bir şekilde faaliyet göstermektedir [103]. Bu tez kapsamında, Hirschmann

BRS30 endüstriyel ağ anahtarı, tipik bir hidroelektrik santralde SCADA haberleşme mimarisinde yaygın olarak kullanılan ring topolojisinin oluşturulmasında kullanılmaktadır. Ayrıca, sistemdeki veri iletişimi endüstriyel ağ anahtarları aracılığıyla sağlanmaktadır.

Test ortamında yer alan bileşenlerin uygun voltaj seviyelerinde çalışmasını sağlamak amacıyla konvertör güç kaynağı kullanılmıştır. Ayrıca, sistemde oluşabilecek aşırı akım veya kısa devre durumlarına karşı bileşenleri korumak için test düzeneğine sigorta entegre edilmiştir.

SIMATIC S7-1200 PLC, ekipmanların kontrolünü ve otomasyonunu sağlamak amacıyla giriş sinyallerini işlemek ve uygun çıkış sinyalleri üretmek için kullanılmaktadır. PLC'ler, endüstriyel süreçlerin gereksinimlerine göre kolaylıkla uyarlanabilen ve yeniden programlanabilen yapıları sayesinde yüksek düzeyde esneklik sunmaktadır.

Test ortamında kullanılan sıcaklık-nem transmitteri, hidroelektrik santralde belirli bölgelere entegre edilen ve otomasyon sistemleriyle uyumlu çalışan sıcaklık-nem ölçüm cihazlarını simüle etmektedir. Bu sayede, tesis operatörleri farklı sistemlerin çalışma koşulları durumunu izleyebilmekte ve gerektiğinde müdahale edebilmektedir. Bu çalışmada, sıcaklık-nem transmitteri belirlenen eşik değerin üzerine çıktığında, santral sistem odasındaki klimanın devreye girmesi şeklinde bir modelleme yapılmıştır.

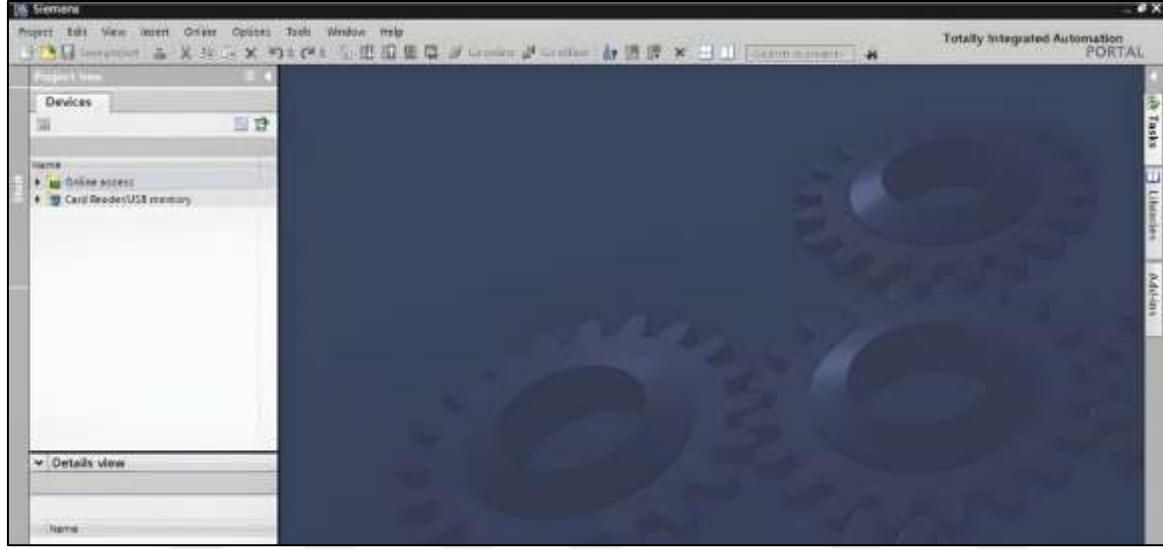


Şekil 4.1. Test ortamında kullanılan ekipmanların gösterimleri

Test ortamında yer alan Siemens S7-1200 PLC'yi programlamak için TIA (Totally Integrated Automation) Portal yazılımı kullanılmıştır. Bu çalışmada, Profinet protokolünü kullanan bir hidroelektrik santralin SCADA sisteminde yer alan komutlardan belirli örnekler seçilerek, TIA Portal yazılımında sanal HMI ile fiziksel PLC arasındaki veri iletişimi

modellenmiş ve operasyonel süreçleri temsil edecek şekilde görselleştirilmiş, böylece operatör komutlarının PLC'ye aktarılması ve sistemin yönetilmesi sağlanmıştır.

Profinet protokolüyle çalışan bir hidroelektrik santralinin SCADA sistemindeki komutların, sanal HMI ve fiziksel PLC kullanılarak gerçekleştirildiği ve görselleştirildiği TIA Portal genel arayüzü Şekil 4.2'de gösterilmektedir.



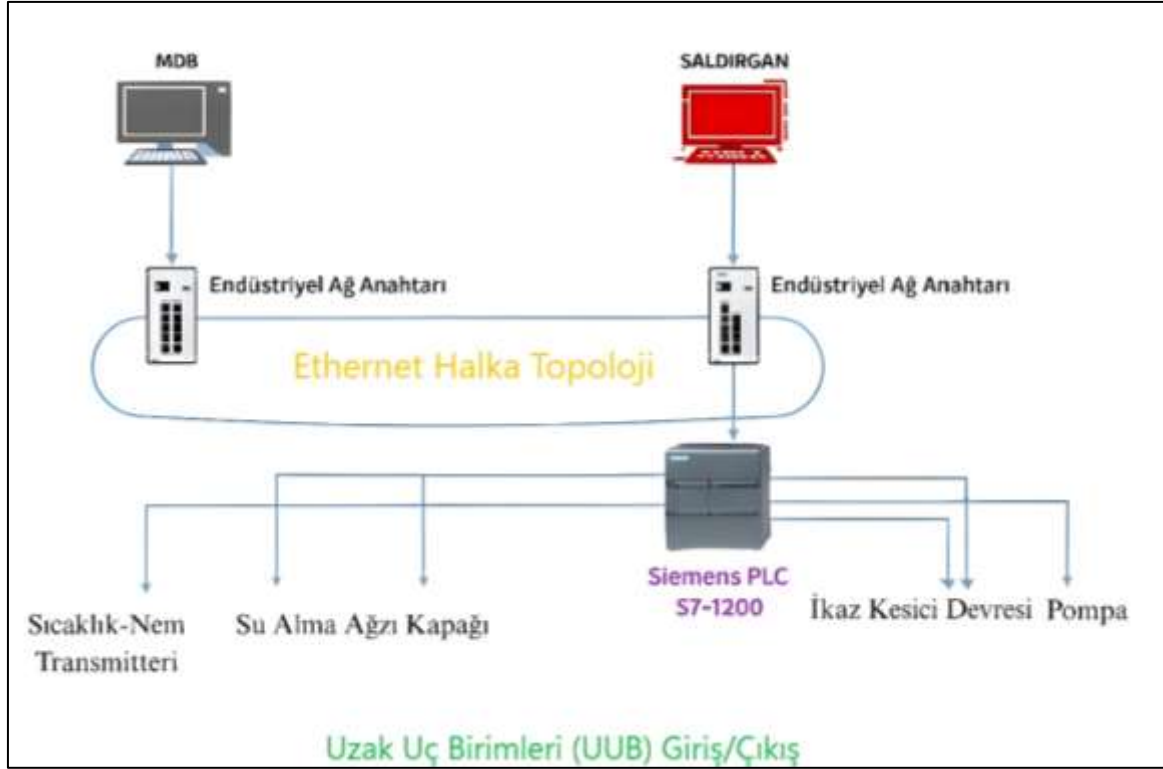
Şekil 4.2. TIA Portal genel arayüzü

Bu tez çalışmasında, Şekil 4.1'de belirtilen bileşenler kullanılarak bir test ortamı oluşturulmuş ve bir hidroelektrik santralin SCADA haberleşme mimarisi simüle edilerek ring topolojisi uygulanmıştır. Çalışma kapsamında, iki endüstriyel ağ anahtarı ile bir yerel alan ağı yapılandırılmış ve sistemdeki tüm bileşenler arasında kesintisiz iletişim sağlamak amacıyla statik IP adresleri tahsis edilmiştir.

Gerçek sahada bulunan açma, kapama, motor ve pompa gibi sinyaller, Siemens TIA Portal yazılımı kullanılarak programlanmış ve Siemens S7-1200 PLC'nin dijital giriş ve çıkış kanallarında LED göstergeleri aracılığıyla görselleştirilmiştir.

Test ortamında siber saldırı gerçekleştirmek amacıyla, harici bir bilgisayar kullanılmaksızın, MDB üzerinde sanallaştırma yazılımı VMware Workstation aracılığıyla Kali Linux işletim sistemi kurulmuş ve bu sanal makine saldırgan bilgisayar olarak yapılandırılarak saldırılar bu sistem üzerinden gerçekleştirilmiştir.

Belirtilen ekipmanlar ve yazılımlar kullanılarak oluşturulan test ortamının mimari yapısının genel görünümü Şekil 4.3'te gösterilmektedir. Şekil 4.3'te gösterilen mimaride, UUB'ler kapsamında bir hidroelektrik santralindeki ekipmanlar, PLC üzerindeki LED'ler kullanılarak temsili olarak modellenmiştir. Bu amaçla, UUB'ler için PLC üzerinde 6 adet dijital çıkış ve 1 adet dijital giriş kanalı kullanılmıştır. Test ortamında kullanılan 6 adet dijital çıkış ve 1 adet dijital giriş, hidroelektrik santral SCADA sistemindeki komutlardan örnekleme yöntemiyle seçilerek modellenmiştir. Bu kapsamda, 2 adet dijital çıkış su alma ağzı kapağının açılması ve kapatılması, 2 adet dijital çıkış ikaz kesici devresinin devreye alınması ve devreden çıkarılması, 1 adet dijital çıkış soğutma suyu pompasının çalıştırılması ve durdurulması amacıyla kullanılmıştır. Ayrıca, 1 adet dijital giriş ve 1 adet dijital çıkış, sıcaklık-nem transmitteri tarafından belirlenen eşik değerin aşılması durumunda sistem odasındaki klimayı otomatik olarak açıp kapatacak şekilde yapılandırılmıştır. Modelleme kapsamında kullanılan UUB'lerden su alma ağzı kapağı, gölde biriken suyun elektrik enerjisi üretimi amacıyla geçtiği ilk kısım olup, suyun türbinlere kontrollü bir şekilde iletilmesini sağlamaktadır. İkaz kesici devresi, jeneratörün uyarım sistemini yöneten kritik bir bileşen olup, ikaz sisteminde üretilen Direct Current (DC) gerilimin jeneratör rotor sargılarına iletilmesini sağlar. Böylece, jeneratörün manyetik alanı oluşturularak enerji üretimi sürdürülebilir hale getirilir. Soğutma suyu pompası, jeneratör, yataklar ve diğer ekipmanların aşırı ısınmasını önlemek için devreye alınarak, sistemdeki sıcaklık dengesinin korunmasını sağlar. Bu süreçte, soğutma suyu çıkış suyundan veya belirli bir su kaynağından çekilerek filtrelendir ve sisteme iletilir.



Şekil 4.3. Test ortamının mimari yapısı

Söz konusu sistemler, gerçek sahadaki işleyişlerine benzer şekilde test ortamında modellenmiş ve sistem bileşenleri arasındaki veri akışı detaylı olarak analiz edilmiştir. Bunun yanı sıra, test ortamında haberleşmenin sağlanması için hidroelektrik santrallerde ve Siemens PLC'lerin iletişimde yaygın olarak kullanılan Profinet protokolü kullanılmıştır. Bu yapı sayesinde, UUB'lerden elde edilen veriler MDB'ye aktarılmış ve süreçlerin izlenmesi sağlanmıştır. Aynı zamanda, MDB üzerinden UUB'lere komutlar iletilerek, sistemin kontrol edilebilirliği test edilmiştir. Bu sayede, hidroelektrik santral operasyonlarında kullanılan haberleşme yöntemleri test ortamında başarıyla simüle edilerek, sistemin çalışma şekli kapsamlı bir şekilde incelenmiştir. Şekil 4.4'te, UUB'lerin çalışmaları sırasında meydana gelen olayların, TIA Portal yazılımı kullanılarak SCADA sistemindeki komutların sanal HMI arayüzü ile fiziksel PLC arasındaki veri iletişimi üzerinden modellenmesine ait program ekran görüntüleri sunulmuştur.

Şekil 4.4'te sunulan yapıda, sanal HMI üzerinden verilen komutlar, fiziksel PLC ile Profinet protokolü aracılığıyla haberleşerek sistemdeki donanım bileşenlerini (su alma ağız kapak motoru, ikaz kesici devresi, soğutma suyu pompası vb.) kontrol etmektedir. Hidroelektrik santral prototipine ait dört farklı kontrol arayüzü (ana sayfa, su alma ağız kapak kontrolü,

ıkaz kesici devresi kontrolü ve soğutma suyu pompası kontrolü) ekranlarda gösterilmektedir. Bu arayüzler, gerçek zamanlı veri akışı ve kontrol mekanizmasının modellenmesini sağlamaktadır.

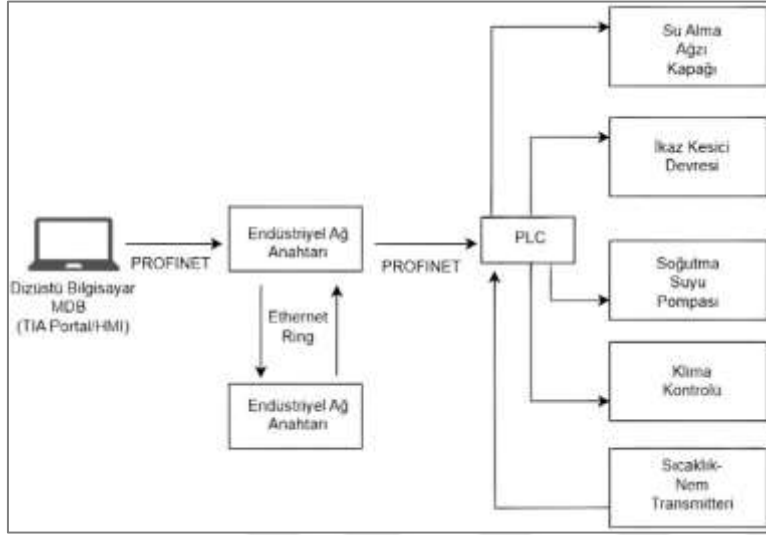
Ortamdaki haberleşme için Profinet protokolü kullanılmıştır. Sanal HMI arayüzü üzerinden verilen komutlar fiziksel PLC'ye iletilmiş ve PLC üzerindeki çıkış modülleri aracılığıyla sistem bileşenleri kontrol edilmiştir. Aynı zamanda fiziksel PLC'den alınan geri bildirimler de sanal HMI ekranında görsel olarak izlenebilmiştir. Gerçekleştirilen bu yapı sayesinde hem komut gönderimi hem de durum izleme işlemleri eşzamanlı olarak gerçekleştirilmiştir. Profinet protokolünün yapısı gereği, veri iletimi hızlı ve deterministik bir şekilde sağlanmakta olup, sensör ve aktüatör verileri doğrudan PLC belleğinde saklanmakta ve işlenmektedir. Çalışmada bu yapı, hidroelektrik santral prototipine ait bileşenlerin test ortamında modellenmesinde başarıyla kullanılmıştır.



Şekil 4.4. SCADA sistemindeki komutların modellenmesine ilişkin ekran görüntüleri

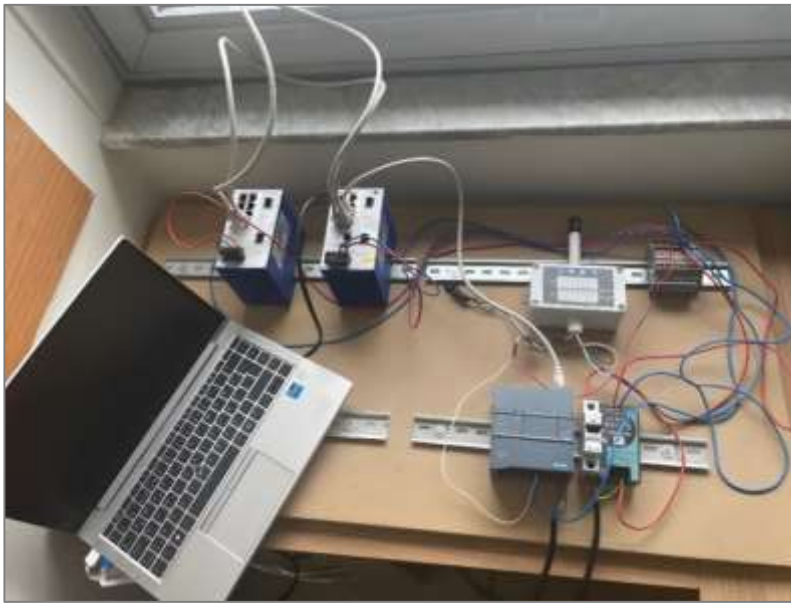
Test ortamında, yerel ağ üzerinde saldırgan bir cihaz kullanılarak tarama işlemleri gerçekleştirilmiş ve fiziksel PLC'ye yönelik çeşitli siber saldırı senaryoları uygulanmıştır. Bu senaryolar kapsamında, fiziksel sistemin ve kontrol edilen süreçlerin çalışma durumu izlenmiş; bazı saldırı türlerinde ise sanal HMI arayüzü üzerinden kullanıcı etkileşimi engellenmiş ve sistemle etkileşim kurmak mümkün olmamıştır. Öte yandan, ağ trafiğinde

oluşan anormal veri akışları ile dijital çıkışlardaki beklenmedik tepkiler analiz edilerek sistemin saldırılara karşı verdiği tepkiler detaylı bir şekilde değerlendirilmiştir. Şekil 4.5’ te fiziksel test ortamına ait sistemin blok diyagramı yer almaktadır.



Şekil 4.5. Fiziksel test ortamına ait sistemin blok diyagramı

Fiziksel test ortamının kurulumu tamamlandıktan sonra elde edilen sistem yerleşimi ve bileşen görünümü Şekil 4.6’da yer almaktadır. Bu test ortamı, deneysel çalışmaların gerçekleştirildiği donanım altyapısını yansıtmakta ve uygulama sürecinin somut yapısını göstermektedir.



Şekil 4.6. Deneysel çalışma yapılan tüm test ortamının görünümü

Sistemde herhangi bir saldırı durumu olup olmadığı, ağ trafiği analiz edilerek ana bilgisayarda kontrol edilmiştir. Saldırı senaryoları, aynı bilgisayar üzerinde sanal makine olarak yapılandırılan ve Kali Linux işletim sistemi yüklü saldırgan ortam aracılığıyla gerçekleştirilmiştir. Bu ortam kullanılarak, öncelikle yerel ağ içerisinde IP adresleri, port numaraları, işletim sistemi türleri ve kullanılan protokoller gibi bilgileri tespit etmeye yönelik tarama işlemleri uygulanmıştır. Gerçekleştirilen çalışmada, hedef olarak seçilen fiziksel PLC'ye yönelik üç farklı siber saldırı türü uygulanmıştır. Bu saldırılar; MITM kategorisinde yer alan ARP Spoofing, DoS saldırı türlerinden TCP SYN Flood ve komut enjeksiyonu saldırısı olmak üzere üç farklı saldırı gerçekleştirilmiştir. Her bir saldırı senaryosu için ağ trafiği, Wireshark yazılımı aracılığıyla ayrı ayrı izlenmiş ve ilgili paketler kaydedilmiştir. Ayrıca, karşılaştırma yapılabilmesi amacıyla herhangi bir saldırının bulunmadığı normal çalışma durumuna ait ağ trafiği de benzer şekilde izlenerek kayıt altına alınmıştır. Wireshark aracılığıyla gerçekleştirilen ağ trafiği izleme sürecine ilişkin örnek bir görüntü Şekil 4.7'de yer almaktadır.

No.	Time	Source IP	Destination IP	Protocol	Length	Source Port	Destination Port	Source MAC Address	Destination MAC Address	Sequence Number (seq)
1099	279.284000	192.168.1.40	192.168.1.50	COTP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1018	279.284000	192.168.1.50	192.168.1.50	TCP	132	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1011	279.284000	192.168.1.50	192.168.1.40	TCP	94	63924	102	TPLink_47:e4:a2	SiemensIndus_a2:65:28	95494943
1012	279.284000	192.168.1.50	192.168.1.40	COTP	62	63924	102	TPLink_47:e4:a2	SiemensIndus_a2:65:28	95494943
1013	279.284000	192.168.1.50	192.168.1.40	TCP	86	63924	102	TPLink_47:e4:a2	SiemensIndus_a2:65:28	95494943
1014	279.284000	192.168.1.50	192.168.1.40	TCP	81	63924	102	TPLink_47:e4:a2	SiemensIndus_a2:65:28	95494943
1015	279.284000	192.168.1.50	192.168.1.50	TCP	80	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1016	279.284000	192.168.1.50	192.168.1.50	TCP	80	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1017	279.284000	192.168.1.50	192.168.1.50	COTP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1018	279.284000	192.168.1.50	192.168.1.50	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1019	279.284000	192.168.1.50	192.168.1.40	TCP	94	63924	102	TPLink_47:e4:a2	SiemensIndus_a2:65:28	107820397
1020	279.284000	192.168.1.50	192.168.1.40	COTP	62	63924	102	TPLink_47:e4:a2	SiemensIndus_a2:65:28	107820397
1021	279.284000	192.168.1.50	192.168.1.40	TCP	86	63924	102	TPLink_47:e4:a2	SiemensIndus_a2:65:28	107820397
1022	279.284000	192.168.1.50	192.168.1.40	TCP	81	63924	102	TPLink_47:e4:a2	SiemensIndus_a2:65:28	107820397
1023	279.284000	192.168.1.50	192.168.1.40	COTP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1024	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1025	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1026	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1027	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1028	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1029	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1030	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1031	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1032	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1033	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1034	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1035	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1036	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1037	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1038	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1039	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1040	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1041	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1042	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1043	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1044	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1045	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1046	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1047	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1048	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1049	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1050	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1051	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1052	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1053	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1054	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1055	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1056	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1057	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1058	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1059	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1060	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1061	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1062	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1063	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1064	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1065	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1066	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1067	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1068	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1069	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1070	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1071	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1072	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1073	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1074	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1075	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1076	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1077	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1078	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1079	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1080	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1081	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1082	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1083	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1084	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1085	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1086	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993
1087	279.284000	192.168.1.50	192.168.1.40	TCP	122	302	63924	SiemensIndus_a2:65:28	TPLink_47:e4:a2	21993

gerçekleştirilmiştir. Ayrıca, modellerin sonuçlarını destekleyici görsel çıktılar elde edilmiştir.

4.2. Siber Saldırı Senaryolarının Test Ortamında Uygulanması

Bu bölümde, oluşturulan test ortamının normal çalışma durumu ile bu ortama yönelik gerçekleştirilen siber saldırı senaryoları ele alınmaktadır. SCADA sistemlerinin güvenliğini tehdit eden yaygın saldırı türleri analiz edilmiş ve test ortamına uygulanmıştır. Bu kapsamda, PLC ve HMI arasındaki haberleşmeyi kesmeyi hedef alan saldırıların yanı sıra, belirli UUB'leri hedef alan noktasal saldırılar da gerçekleştirilmiştir.

Gerçekleştirilen saldırılarla, sistemin bütünlüğü ve kararlılığı üzerindeki etkiler gözlemlenmiş; saldırı öncesi ve sonrası ağ trafiği Wireshark yazılımı ile detaylı olarak kaydedilmiştir. Uygulanan senaryolar aşağıdaki şekilde özetlenmiştir:

Normal durum senaryosu

Sistemin olağan koşullar altında, herhangi bir dış müdahale olmaksızın çalıştığı referans senaryodur.

ARP spoofing saldırı senaryosu

Ağ üzerindeki cihazların MAC-IP eşleşmelerini manipüle ederek saldırganın kendisini iletişim trafiğinin arasına yerleştirmesi (Man-in-the-Middle) amaçlanmıştır.

Yetkisiz komut enjeksiyonu senaryosu

Sisteme ait olmayan bir cihazın sahte HMI gibi davranarak PLC'ye doğrudan komut göndermesi sağlanmış ve kontrol yetkisinin ele geçirilmesi hedeflenmiştir.

SYN flood saldırı senaryosu

Hedef sistemin kaynaklarını tüketerek hizmet dışı bırakılmasına yönelik olarak, yarım açık TCP bağlantılarının yoğun şekilde gönderildiği bir DoS saldırısı gerçekleştirilmiştir.

Gerçekleştirilen bu saldırı senaryoları sonucunda sistem davranışları, paket boyutları, zamanlama farklılıkları ve bağlantı yoğunluğu gibi ağ parametreleri analiz edilmiş; bu veriler etiketlenerek makine öğrenmesi tabanlı anomali tespit sistemlerinde kullanılabilir hâle getirilmiştir.

Saldırgan tarafından, hedef cihazları tespit etmek amacıyla Netdiscover ve nmap gibi hem pasif hem de aktif tarama araçları kullanılmış; Hping3 aracıyla da saldırı senaryolarında kullanılmak üzere özel paketler oluşturulmuştur. Elde edilen bilgiler doğrultusunda, hedef cihazlara yönelik bilgi toplama işlemleri gerçekleştirilmiş ve bu veriler sonraki saldırı aşamalarının planlanmasında kullanılmıştır. Bu verilere dayanarak saldırı işlemleri gerçekleştirilmiş ve her bir saldırı senaryosu ortalama 4 dakika boyunca uygulanmıştır. Bu sürenin belirlenmesindeki amaç, sistem üzerindeki etkilerin gözlemlenebilmesini sağlamakla birlikte, saldırı trafiğine ait daha geniş ve kapsamlı bir veri seti oluşturmaktır. Bu sayede, makine öğrenmesi modellerinin daha sağlıklı eğitilebilmesi için gerekli olan veri çeşitliliği sağlanmıştır. Gerçekleştirilen saldırılar sonrasında sistem işleyişi, bazı durumlarda toparlanamamış ve normal çalışma düzenine geri dönememiştir. Bu durum, SCADA sistemlerinin ne kadar hassas yapıda olduğunu ve saldırıların sistem üzerindeki etkilerinin sadece geçici değil, kalıcı arızalara yol açabileceğini ortaya koymaktadır. Bu nedenle, bu tür saldırıların etkilerinin detaylı şekilde izlenmesi ve analiz edilmesi, güvenlik açıklarının belirlenmesi ve önlemler alınması açısından kritik öneme sahiptir.

Saldırı ve normal durum senaryolarının uygulanması sırasında kaydedilen ağ trafiğine ait istatistiksel veriler Çizelge 4.2'de sunulmuştur. Ağ üzerinden yakalanan paketler, oluşturulan veri kümelerindeki kayıtları temsil etmektedir.

Çizelge 4.2. Ağ trafiği istatistiksel özeti ve senaryo bazlı karşılaştırma

Senaryo	Toplam Paket Sayısı	Ortalama Paket Boyutu (bayt)	Toplam Paket Boyutu (bayt)	Senaryo Süresi (s)
Normal durum	27804	82,0	2278889	1448,525
ARP spoofing saldırısı	36128	93,0	3353449	351,076
TCP SYN Flood saldırısı	57472	60,03	3449884	210,0
Yetkisiz komut enjeksiyonu	30492	101,0	3065780	304,495

Çizelge 4.2 incelendiğinde, saldırı ve normal durum senaryolarına ait ağ trafiği parametreleri karşılaştırmalı olarak değerlendirilmiştir. Toplam paket sayısı bakımından en yoğun trafik, 57472 paket ile TCP SYN Flood saldırısına aittir. Bunu sırasıyla ARP Spoofing, komut enjeksiyonu ve normal durum senaryoları takip etmektedir. Toplam paket boyutu açısından, saldırı senaryoları genel olarak normal trafiğe göre daha fazla veri üretmiş, bu da sistem kaynakları üzerinde baskı oluşturan bir etki yaratmıştır. Ortalama paket boyutlarına bakıldığında, bazı saldırı türlerinde daha kısa ve hafif paketlerle sistemin zorlandığı, bazı saldırılarda ise daha büyük boyutlu paketlerle doğrudan müdahalelerin gerçekleştirildiği anlaşılmaktadır. Özellikle komut enjeksiyonu saldırı türü, yoğunluk ve hacim anlamında yüksek veri üretimi ile dikkat çekmektedir. TCP SYN Flood senaryosu ise 60,03 bayt ile en düşük ortalama paket boyutuna sahiptir. Bu durum, TCP SYN Flood saldırılarının kısa ve yoğun paketlerle gerçekleştirildiğini göstermektedir. Senaryo süreleri değerlendirildiğinde ise saldırıların, daha kısa zaman dilimlerinde uygulanmasına rağmen, oluşturdukları ağ trafiği hacminin dikkat çekici düzeyde olduğu gözlemlenmiştir.

4.3. Veri Kümesi Oluşturma Süreci

Bu bölümde, test ortamında gerçekleştirilen her bir senaryo sonucunda elde edilen ağ trafiği verileri kullanılarak oluşturulan toplam veri kümesi hakkında bilgi sunulmaktadır. Her senaryo için ağ trafiği, Wireshark aracılığıyla ayrı ayrı kaydedilmiş ve analiz edilmiştir. Elde edilen kayıtlar, tek bir veri kümesi altında birleştirilerek bütünsel bir yapı oluşturulmuştur. Veri kümesinde kullanılacak özniteliklerin belirlenmesi sürecinde, literatürde yaygın olarak tercih edilen ve endüstriyel haberleşme protokollerinden biri olan Profinet protokolüne özgü nitelikler incelenmiştir [104]. Bu çalışma kapsamında oluşturulan veri kümesi için uygun bulunan toplam 39 öznitelik belirlenmiş olup, bu özniteliklerin tanımları ve açıklamaları Çizelge 4.3'te sunulmuştur.

Çizelge 4.3. Veri kümesi için belirlenen özellikler ve açıklamaları

Sıra No	Öznitelik Adı	Açıklama
1	No	Pakete ait sıra numarası
2	Time	Pakete ait zaman damgası
3	SourceIP	IP Gönderen cihazın IP adresi
4	DestinationIP	IP Hedef cihazın IP adresi
5	Protocol	İletişimde kullanılan protokol
6	Length	Paketin bayt cinsinden uzunluğu
7	Source Port	Kaynak port numarası
8	Destination Port	Hedef cihazın port numarası

Çizelge 4.3. (devam) Veri kümesi için belirlenen özellikler ve açıklamaları

Sıra No	Öznitelik Adı	Açıklama
9	Source MAC Address	Kaynak MAC adresi
10	Destination MAC Address	Hedef cihazın MAC adresi
11	Sequence Number (raw)	Veri akışı sırasındaki sıra numarası
12	Acknowledgment number (raw)	Alımı onaylanan son bayta karşılık gelen sıra numarası
13	Time since first frame in this TCP stream	TCP akışının başlangıcından itibaren geçen zaman
14	Time since previous frame in this TCP stream	TCP bağlantısında önceki paketten itibaren geçen zaman aralığı
15	Frame length on the wire	Fiziksel ortamda taşınan çerçevenin uzunluğu
16	Time delta from previous captured frame	Önceki paketten itibaren geçen zaman aralığı
17	Protocols in frame	Paketteki protokol zinciri
18	Profinet Real Time FrameID	Gerçek zamanlı Profinet çerçeve kimliği
19	Profinet DCP ServiceID	DCP Profinet cihaz yapılandırması hizmet kimliği
20	Profinet DCP ServiceType	DCP Profinet hizmet tipi (sorgu/yanıt)
21	Profinet DCP Xid	Profinet DCP İletişim eşlemesi için kullanılan değişken
22	ResponseDelay	İletişimdeki gecikme süresi
23	Profinet DCPDataLength	Profinet DCP veri alanının uzunluğu
24	IG Bit	İletişim kontrol biti
25	DeviceVendorValue	Cihazın üretici bilgisi
26	Device Name (Name of Station)	Cihaza atanan istasyon adı
27	Device Role Details	Cihazın ağ üzerindeki işlevi
28	Device Instance Low High	Cihaza ait örnekleme değeri
29	Subnet Mask	IP alt ağ maskesi
30	Standard Gateway	IP Varsayılan ağ geçidi
31	Destination reference	İletişimde hedef referans
32	ROSCTR	Protokolün işlem kontrol kodu
33	Protocol Data Unit Reference	Veri birimi tanımlayıcısı
34	Community ID	Haberleşme oturum kimliği
35	Item count	İletilen veri ögesi sayısı
36	Byte Address (PLC)	PLC hafızasında erişilen bayt adresi
37	Bit Address (PLC)	PLC içerisindeki bit adresi
38	Info	Paket hakkında genel açıklayıcı bilgi
39	Attack_Type_Label	Veri kümesindeki her örneğe karşılık gelen saldırı türünü veya normal durumu temsil eden etiket bilgisi (4 adet senaryo)

Bu çalışma kapsamında, 38 öznitelik ve bir adet etiket sütunundan (Attack_Type_Label) oluşan, toplamda 171786 örnek içeren yeni ve kapsamlı bir veri kümesi oluşturulmuştur. Veri kümesinin hazırlanması sürecinde, gerçek zamanlı bir SCADA test ortamında farklı siber saldırı senaryoları uygulanmış ve sistemin tepkileri doğrudan gözlemlenmiştir. Saldırıları, sistemsel anormalliklere neden olmuş ve bu durum, veri setine etiketleme sürecinde doğrudan katkı sağlamıştır. Oluşturulan bu veri kümesi, hem saldırı tespitine

yönelik sınıflandırma problemleri için hem de farklı makine öğrenmesi yöntemlerinin eğitilip test edilmesi için uygun yapıdadır. Ayrıca, veri kümesi sadece saldırı olup olmadığını değil aynı zamanda gerçekleştirilen saldırının türünü de (örneğin: ARP spoofing, TCP SYN flood, yetkisiz komut enjeksiyonu vb.) belirlemeye imkân tanımaktadır. Bu yönüyle literatürdeki siber güvenlik ile SCADA sistemleri alanındaki mevcut çalışmalara katkı sunmaktadır.

4.4. Siber Saldırı Tespitinde Kullanılan Makine Öğrenmesi Performans Metrikleri

Makine öğrenmesinin temel amacı, mevcut eğitim veri kümesini kullanarak genelleme yeteneğine sahip bir model geliştirmektir. Ancak her makine öğrenmesi modeli, her veri kümesi üzerinde aynı başarıyı göstermeyebilir. Bazı modeller, belirli veri kümelerinde yüksek doğruluk elde ederken aynı modeller farklı veri kümelerinde zayıf sonuçlar verebilir. Ayrıca, aynı veri kümesi üzerinde çalışan farklı modellerin performansları da birbirinden önemli ölçüde farklılık gösterebilir. Bu nedenle, belirli bir veri kümesi üzerinde en iyi performansı sergileyen modeli belirlemek kritik bir adımdır. Bu amaca ulaşmak için önerilen modellerin performanslarının karşılaştırılması yaygın bir yaklaşımdır. Bu karşılaştırmaların sağlıklı bir şekilde yapılabilmesi için, model değerlendirme yöntemlerinin ve performans ölçütlerinin doğru şekilde belirlenmesi ve uygulanması gerekir. Bu doğrultuda, veri kümesi; eğitim, doğrulama ve test olmak üzere üçe ayrılarak model performanslarının değerlendirilmesinde literatürde yaygın olarak kullanılan metriklerden faydalanılmaktadır [4].

Model performansının değerlendirilmesinde yaygın olarak kullanılan yöntemlerden biri karışıklık (confusion) matrisidir. Bu matris, modelin gerçek etiketlerle yaptığı tahminlerin karşılaştırılmasıyla oluşturulmakta ve sınıflandırma doğruluğunun yanı sıra hata türlerinin de analizine imkân tanımaktadır. İki sınıflı bir veri kümesi için örnek karışıklık matrisi Çizelge 4.4'te gösterilmektedir.

Çizelge 4.4. Karışıklık (Confusion) matris

	Gerçek Pozitif (Sınıf 1)	Gerçek Negatif (Sınıf 2)
Tahmin Pozitif (Sınıf 1)	Doğru Pozitif (DP)	Yanlış Pozitif (YP)
Tahmin Negatif (Sınıf 2)	Yanlış Negatif (YN)	Doğru Negatif (DN)

Doğru pozitif (DP)

Gerçek sınıf pozitif (Sınıf 1) ve modelin tahmini de pozitif (Sınıf 1) olan örnek sayısıdır. Model, doğru tahminde bulunmuştur.

Yanlış pozitif (YP)

Gerçek sınıf negatif (Sınıf 2) olduğu hâlde model tarafından yanlışlıkla pozitif (Sınıf 1) olarak tahmin edilen örnek sayısıdır.

Yanlış negatif (YN)

Gerçek sınıf pozitif (Sınıf 1) olduğu hâlde modelin tahmini negatif (Sınıf 2) olan örnek sayısıdır. Model, bu örnekleri gözden kaçırmıştır.

Doğru negatif (DN)

Gerçek sınıf negatif (Sınıf 2) ve modelin tahmini de negatif (Sınıf 2) olan örnek sayısıdır. Model, doğru şekilde sınıflandırmıştır.

Makine öğrenmesi modellerinin performansını değerlendirmek amacıyla çeşitli metrikler kullanılmaktadır. Bu metrikler, modelin doğruluğunu, hata oranlarını ve genelleme kapasitesini nicel olarak analiz etmeye olanak sağlar. Literatürde en yaygın şekilde kullanılan performans ölçütleri arasında doğruluk (Accuracy), duyarlılık (Sensitivity/Recall), özgüllük (Specificity), kesinlik (Precision), F1 skoru (F1 Score) ile Receiver Operating Characteristic (ROC) eğrisi ve altında kalan alan (Area Under the Curve - AUC) yer almaktadır [97]. Bu metrikler, genellikle test veri kümesi üzerinde uygulanarak modelin tahmin başarısı ve genel sınıflandırma performansı hakkında kapsamlı bilgi sunar.

Doğruluk (Accuracy), bir sınıflandırma modelinin hem pozitif hem de negatif sınıflara ait örnekleri doğru tahmin etme oranını ifade eder. Bu metrik, modelin doğru sınıflandırdığı örnek sayısının toplam örnek sayısına oranı olarak hesaplanır.

$$\text{Doğruluk (Accuracy)} = (\text{DP} + \text{DN}) / (\text{DP} + \text{YP} + \text{DN} + \text{YN}) \quad (4.1)$$

Duyarlılık (Sensitivity veya Recall), sınıflandırma modelinin pozitif sınıfa ait örnekleri doğru bir şekilde tahmin etme yeteneğini ölçen bir başarı metriğidir. Gerçek pozitif örnekler içerisinde, modelin doğru biçimde pozitif olarak sınıflandırdığı örneklerin oranı olarak ifade edilir. Başka bir ifadeyle, modelin pozitif sınıfı ne ölçüde doğru öngörebildiğini göstermektedir.

$$\text{Duyarlılık (Recall)} = \text{DP} / (\text{DP} + \text{YN}) \quad (4.2)$$

Özgüllük (Specificity), sınıflandırma modelinin negatif sınıfa ait örnekleri doğru şekilde tahmin etme başarısını ölçen bir performans ölçütüdür. Gerçek negatif örnekler içerisinde modelin doğru şekilde negatif olarak sınıflandırdığı örneklerin oranını ifade eder. Başka bir ifadeyle, modelin negatif sınıfı ne ölçüde doğru tanıyabildiğini gösterir.

$$\text{Özgüllük (Specificity)} = \text{DN} / (\text{DN} + \text{YP}) \quad (4.3)$$

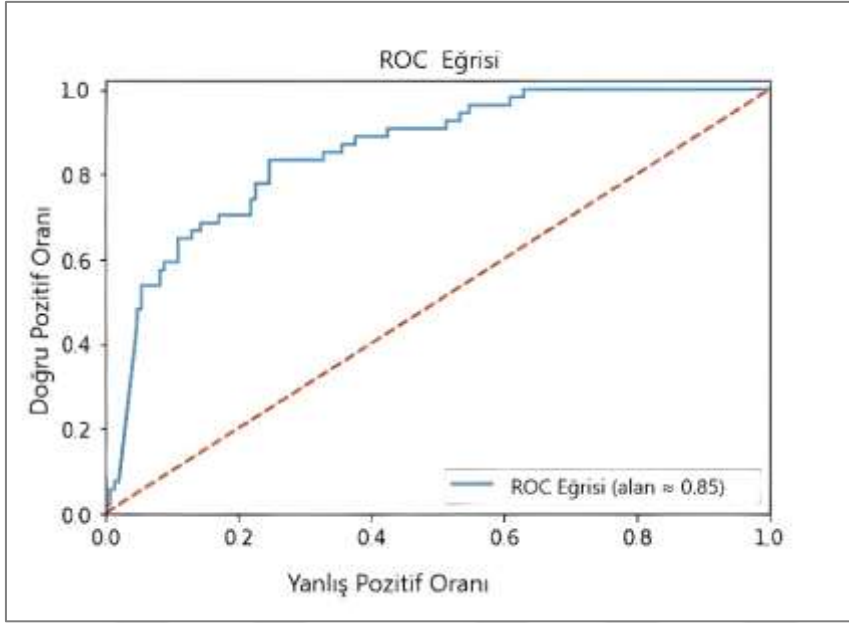
Kesinlik (Precision), modelin pozitif olarak sınıflandırdığı örnekler içinde, gerçekten pozitif olanların oranını ifade eder. Yani, modelin pozitif sınıfı tahmin ederken ne kadar isabetli olduğunu gösterir.

$$\text{Kesinlik (Precision)} = \text{DP} / (\text{DP} + \text{YP}) \quad (4.4)$$

F1 skoru (F1 Score), bir sınıflandırma modelinin kesinlik (precision) ve duyarlılık (recall) metriklerinin harmonik ortalaması olarak tanımlanır. F1 skoru, duyarlılık ve kesinlik metrikleri arasında bir denge kurarak modelin genel başarımını optimize etmeyi amaçlar.

$$\text{F1 Skoru} = 2 \times (\text{Kesinlik} \times \text{Duyarlılık}) / (\text{Kesinlik} + \text{Duyarlılık}) \quad (4.5)$$

ROC eğrisi, sınıflandırma modellerinin performansını değerlendirmede kullanılan önemli bir grafiksel araçtır. Şekil 4.8’de yatay ekseninde yanlış pozitif oranı (False Positive Rate - FPR), dikey ekseninde ise doğru pozitif oranı (True Positive Rate - TPR) yer almaktadır.



Şekil 4.8. ROC eğrisi örneği

AUC, modelin sınıflar arasında ne kadar başarılı ayırım yapabildiğini gösterir. Modelin öngörü etkinliği, aşağıda verilen AUC'ye ilişkin değer aralıkları dikkate alınarak değerlendirilmektedir [105].

- $AUC = 0,5 \rightarrow$ Model, sınıflar arasında ayırım yapma yetisine sahip değildir.
- $0,5 < AUC < 0,7 \rightarrow$ Modelin öngörü performansı zayıftır.
- $0,7 \leq AUC < 0,8 \rightarrow$ Model kabul edilebilir bir sınıflandırma başarısına sahiptir.
- $0,8 \leq AUC < 0,9 \rightarrow$ Modelin sınıflar arası ayırımı mükemmel düzeydedir.
- $0,9 \leq AUC \leq 1 \rightarrow$ Model üstün bir sınıflandırma yeteneğine sahiptir.

Bu tez kapsamında, sınıflandırma modellerinin başarılarını değerlendirmek amacıyla doğruluk, kesinlik, duyarlılık, özgüllük, F1 skoru ve ROC-AUC olmak üzere yaygın olarak kullanılan performans metriklerinden yararlanılmıştır.

4.5. Siber Saldırı Tespiti İçin Makine Öğrenmesi Modelleri

Bu çalışmada, fiziksel bir SCADA test ortamında oluşturulan veri kümesi üzerinde saldırı tespiti amaçlanmaktadır. Bu kapsamda, farklı makine öğrenmesi algoritmaları hazırlanarak üçe bölünmüş (eğitim, doğrulama ve test) veri seti üzerinde uygulanmaktadır. Elde edilen sonuçlar; doğruluk, duyarlılık, özgüllük, kesinlik, F1 skoru ve ROC-AUC gibi performans

metrikleriyle değerlendirilerek karşılaştırılmaktadır. Geliştirilen modellerin daha yüksek başarı sağlaması için veri ön işleme adımları gerçekleştirilmekte ve deneysel analizler yürütülmektedir. Çalışma kapsamında, SCADA sisteminin siber güvenliğini artırmaya yönelik bir test ortamı kurgulanarak özgün bir veri seti oluşturularak farklı yaklaşım sunulmaktadır.

4.5.1. Analize uygun veri kümesi yapılandırması

Bu bölümde, analiz sürecine uygun veri kümesi yapısının oluşturulması ve bu veri kümesine en uygun makine öğrenmesi modellerinin tasarlanmasına yönelik adımlar ele alınmaktadır. Şekil 4.9, bu bölümde açıklanan sürecin özet bir akışını sunmaktadır.

Veri kümesinin analiz ve modelleme için elverişli hâle getirilmesi amacıyla çeşitli ön işleme teknikleri uygulanmıştır. Literatürde, bir veri serisinin güvenilir biçimde tamamlanabilmesi için en az %70 oranında eksiksiz olması gerektiği, %30'un üzerinde eksik veriye sahip sütunların ise istatistiksel özellikleri yeterli düzeyde yansıtamayacağı kabul edilmektedir [106]. Bu doğrultuda, ön işleme sürecinin ilk adımında, yüksek oranda eksik değer içeren öznitelikler (örneğin: Byte Address (PLC), Profinet DCP ServiceID, StandardGateway vb.), veri kalitesini artırmak amacıyla veri setinden çıkarılmıştır. Ayrıca, bu yaklaşım, eksik verilerle başa çıkmada en temel ve en basit yöntemlerden biri olup yaygın olarak uygulanmaktadır [107, 108]. Ardından, veri setinde yinelenen kayıtlar tespit edilerek tekrarlı (duplicate) satırlar silinmiştir. Bu işlem, veri bütünlüğünü sağlamak ve modelin aynı örneklerden etkilenerek yanlış öğrenmesini önlemek amacıyla gerçekleştirilmiştir. Tekrarlanan kayıtların varlığı; sistem performansının yavaşlaması, veri kalitesinin düşmesi, veri depolama alanının israf edilmesi ve yüksek işletim maliyetleri gibi sorunlara yol açmakta, bu nedenle veri ön işleme sürecinde kayıt tekilleştirme yöntemiyle tekrar eden kayıtların silinmesi kritik bir adım olarak uygulanmaktadır [109]. Bu süreç, yalnızca tek bir kopyanın korunması ve diğer tekrar eden kayıtların silinmesi yoluyla gerçekleştirilmekte olup, bu sayede veri daha temiz, tutarlı ve analiz için uygun hâle getirilmektedir [110].

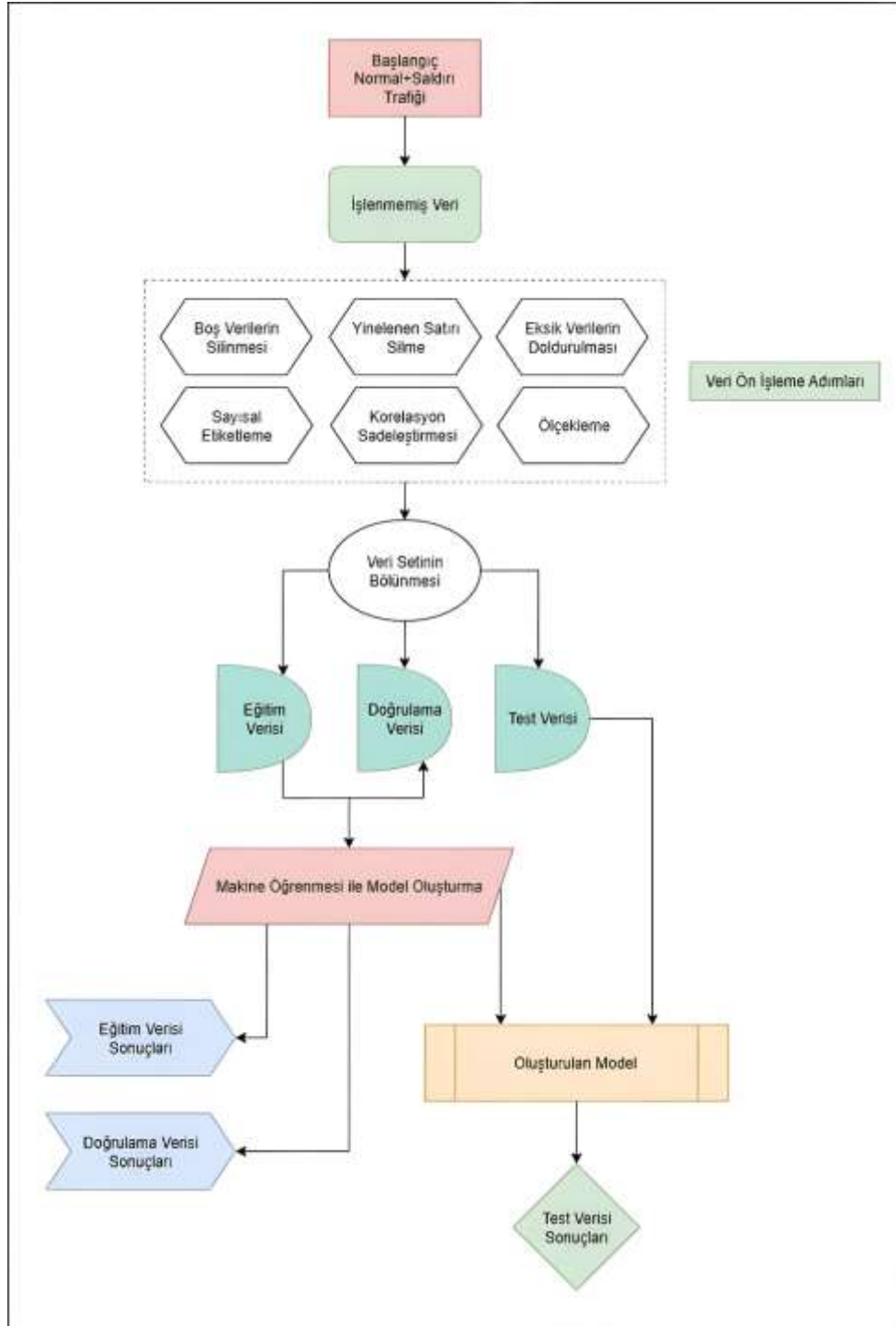
Eksik veri oranı %5'in altında olduğunda, ortalama, medyan veya mod gibi temel atama yöntemlerinin, verinin yapısını büyük ölçüde bozmadığı ve eksik bilginin etkisini azalttığı için etkili stratejiler arasında yer aldığı belirtilmektedir [111]. Bu çerçevede, üçüncü adımda yaklaşık %3 oranında eksik veri içeren ancak korunması gereken öznitelikler (Source Port,

Destination Port ve Sequence Number vb.) belirlenmiş; bu özniteliklerde uç değerlerin bulunması nedeniyle eksik değerler, dağılımın merkezini daha doğru yansıtan medyan yöntemiyle doldurulmuştur. Aykırı değerlere daha az duyarlı olması nedeniyle medyan, bu tür durumlar için literatürde kullanışlı bir istatistiksel ölçüt olarak değerlendirilmektedir [112]. Daha sonra, makine öğrenmesi algoritmalarının kategorik verileri doğrudan işleyememesi nedeniyle, modelin giriş verilerini anlamlandırabilmesi açısından kritik bir adım olan etiket verilerinin sayısal forma dönüştürülmesi işlemi 'Sayısal Etiketleme' yöntemiyle gerçekleştirilmiştir. Çünkü, yapay zekâ algoritmalarının sayısal verilerle çalışması gerektiğinden, nicel olmayan ancak anlamlı bilgi içeren kategorik verilerin modele dâhil edilebilmesi için sayısal türe dönüştürülmesi gerekmektedir [113]. Ardından, yüksek korelasyon içeren değişkenler arasındaki bilgi fazlalığını (redundancy) ortadan kaldırmak amacıyla korelasyon sadeleştirme işlemi uygulanmıştır. Günümüzde, değişkenler arasındaki ilişkiyi ölçmek amacıyla kullanılan Pearson korelasyon katsayısı ve Spearman sıralama korelasyonu katsayısı gibi doğrusal yöntemler, sayısal verilerde sıkça tercih edilen başlıca korelasyon hesaplama teknikleridir [114]. Son olarak, makine öğrenmesi algoritmalarının daha etkili çalışabilmesi amacıyla özelliklerin aynı ölçekte ifade edilmesini sağlayan ölçeklendirme işlemi Min-Max yöntemiyle gerçekleştirilmiştir. Min-Max ölçekleyici, makine öğrenmesi topluluğu tarafından yaygın olarak kullanılan, iyi bilinen ve temsil gücü yüksek bir ölçekleme tekniği olarak kabul edilmektedir. Veri kümesi ölçeklemesi, makine öğrenmesi süreçlerinde, değişkenlerin farklı ölçeklerde değişmesini önlemek ve tüm özelliklerin aynı aralıkta değişkenlik göstermesini sağlamak amacıyla uygulanan, sınıflandırma modellerinin performansını artırdığı bilinen kritik bir ön işleme adımıdır [115]. Tüm bu ön işleme adımlarının tamamlanmasının ardından, veri kümesi 26 öznitelik ve 116043 satır örnek içerecek şekilde yeniden yapılandırılmıştır.

Uygulanan veri ön işleme adımları sonucunda elde edilen temizlenmiş veri seti, makine öğrenmesi sürecine dahil edilmek üzere eğitim, doğrulama ve test alt kümelerine ayrılmıştır. Bu kapsamda, veri kümesinin bir bölümü modelin eğitimi için, daha önce kullanılmamış bir bölümü ise modelin genel başarımını objektif olarak değerlendirmek amacıyla test sürecinde kullanılmıştır. Ayrıca, hiperparametre optimizasyonu ve modelin doğruluğunu artırmak amacıyla, eğitim ve test verilerinden bağımsız bir doğrulama veri kümesi de oluşturulmuştur. Bu doğrultuda, literatürde yaygın olarak benimsenen bir yaklaşım doğrultusunda veri seti %70 eğitim, %15 doğrulama ve %15 test oranlarında üç alt kümeye ayrılmıştır [116]. Model karşılaştırmalarında tutarlılığı sağlamak amacıyla, bu bölünme oranları tüm algoritmalar için

sabit tutulmuştur. Eğitim ve doğrulama verileri sırasıyla modelin öğrenme sürecinde ve hiperparametrelerin en uygun şekilde belirlenmesinde kullanılmıştır. Son aşamada, modeller test veri kümesi üzerinde değerlendirilmiş ve her bir alt kümeye ait performans metrikleri ayrı ayrı analiz edilerek genel doğrulama süreci tamamlanmıştır.

Modellerin eğitimi için toplam 116043 satırdan oluşan veri kümesi, her üç alt kümede de tüm saldırı türleri ve normal trafiğin temsil edilmesine dikkat edilerek, sınıf çeşitliliği gözetilerek üçe ayrılmıştır. Tüm veri kümelerinde, her bir saldırı türü ve normal durum örneklerinin temsil edilmesine özen gösterilmiş; böylece sınıf temsiliyeti korunarak veri dağılımında çeşitlilik sağlanmıştır. Bu kapsamda, %70'lik bölümü oluşturan 81276 satır eğitim amacıyla, %15'lik kısmı olan 17360 satır doğrulama (validation) amacıyla, kalan 17407 satır ise modelin nihai performansını değerlendirmek üzere test amacıyla kullanılmıştır.



Şekil 4.9. Veri hazırlama ve modelleme süreci

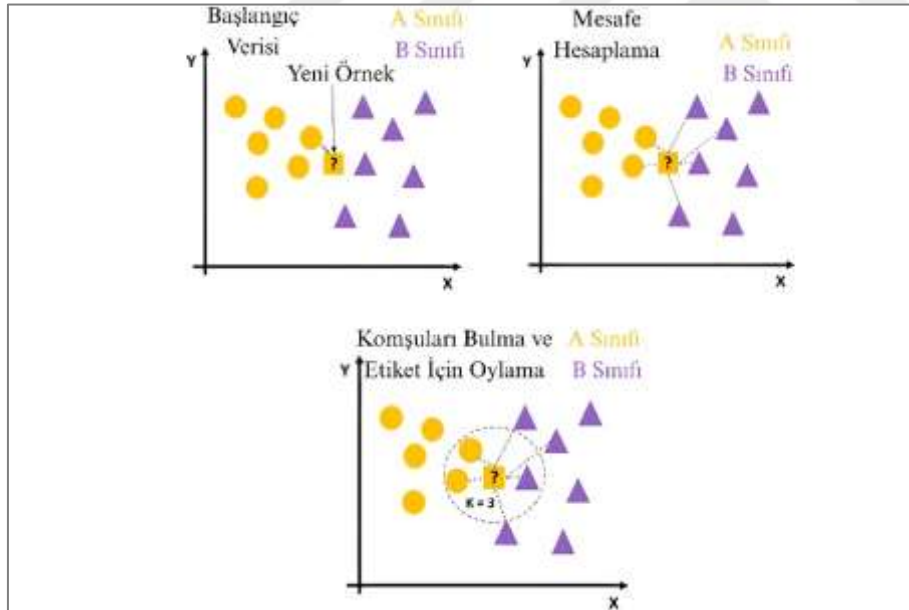
4.5.2. Uygulanan sınıflandırma modelleri

Bu çalışmada, makine öğrenmesi tabanlı sınıflandırma algoritmalarından KNN, NB, DT, LR algoritmaları ve bu algoritmaların kombinasyonları kullanılarak oluşturulan hibrit modellerin saldırı tespit performansları analiz edilmiştir. Modellerin başarımı, belirlenen

değerlendirme metrikleri doğrultusunda incelenmiştir. Bu bölümde, kullanılan sınıflandırma modellerine, modellerin temel mimarisine ve parametrelerine ilişkin bilgilere yer verilmiştir.

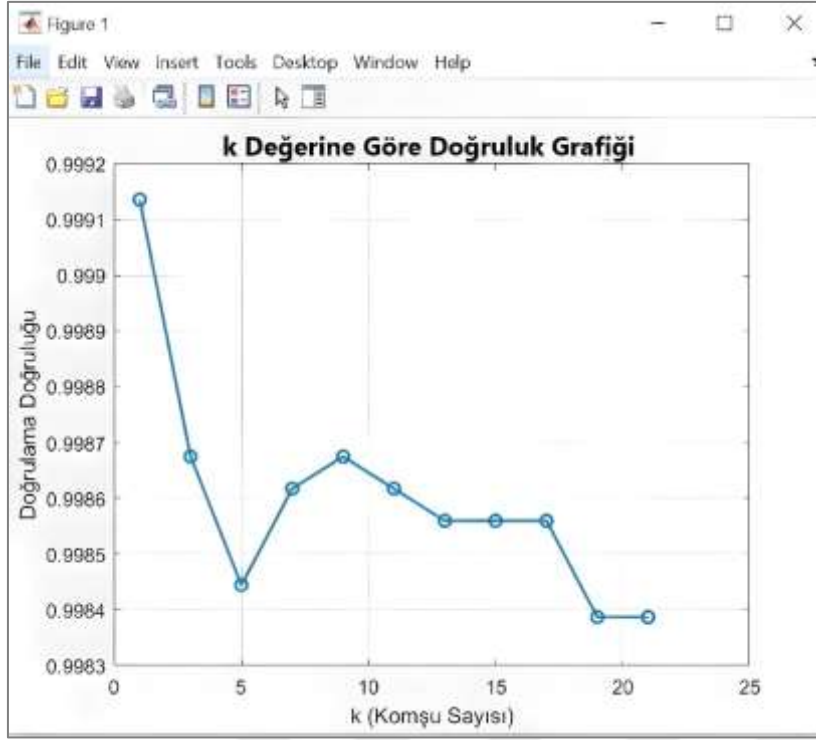
KNN modeli

Hem sınıflandırma hem de regresyon problemlerinde kullanılan, denetimli ve parametrik olmayan bir öğrenme yöntemidir. Bu algoritma, yeni bir örneği sınıflandırmak veya tahmin etmek için eğitim veri kümesindeki en yakın “k” komşuya dayanır. Sınıflandırmada, komşuların oy çokluğuna göre sınıf atanırken; regresyonda, komşuların ortalama değerine göre tahmin yapılır [117]. Şekil 4.10’da KNN modeli temel çalışma prensibi gösterilmektedir. Yeni bir örnek veri noktası, eğitim veri kümesindeki tüm örneklerle arasındaki mesafeye göre değerlendirilir. Ardından, en yakın “k” komşu seçilir ve bu komşuların sınıf etiketlerine göre çoğunluk oylaması yapılır. Elde edilen sonuç, yeni verinin hangi sınıfa ait olacağını belirler.



Şekil 4.10. KNN modeli temel çalışma prensibi [118]

Şekil 4.11’de, farklı k (komşu sayısı) değerlerine göre veri kümesine uygulanan KNN algoritmasının doğrulama başarımındaki değişim görülmektedir. Doğrulama doğruluğu, k = 1 değerinde en yüksek seviyeye ulaşmış; k değeri arttıkça doğrulukta genel olarak azalan bir eğilim gözlemlenmiştir. Bu durum, daha düşük komşu sayılarında modelin örneklerle daha duyarlı davrandığını, ancak k değeri arttıkça sınıflar arası ayırım gücünün azaldığını göstermektedir.



Şekil 4.11. Komşu sayısı (k) değerine bağlı olarak doğrulama başarımının değişimi

Çizelge 4.5'te sunulan KNN algoritmasının test verisi performans metrikleri incelendiğinde, modelin genel olarak yüksek sınıflandırma başarısı gösterdiği görülmektedir. Normal durum (Sınıf 0), TCP SYN Flood (Sınıf 2) ve komut enjeksiyonu (Sınıf 3) için tüm metriklerde elde edilen yüksek değerler, bu sınıfların başarıyla ayrıştırıldığını ortaya koymaktadır. Buna karşılık, ARP spoofing (Sınıf 1) için F1 skoru değerinin 0,896 olması, modelin bu sınıfta görece daha düşük bir performans sergilediğini göstermektedir. Bu durum, genellikle bu sınıfa ait örnek sayısının azlığıyla ilişkilendirilmektedir. Genel olarak, modelin saldırı tespitinde güçlü ve dengeli bir performans sunduğu söylenebilir.

Çizelge 4.5. KNN modeli test metrikleri

Senaryolar	Doğruluk	Kesinlik	Duyarlılık	Özgüllük	F1 Skoru
Normal durum	1	1	1	1	1
ARP spoofing saldırısı	0,90323	0,88889	0,90323	0,9996	0,896
TCP SYN flood saldırısı	1	0,99977	1	0,99977	0,99988
Komut enjeksiyonu saldırısı	0,99803	0,99869	0,99803	0,99953	0,99836

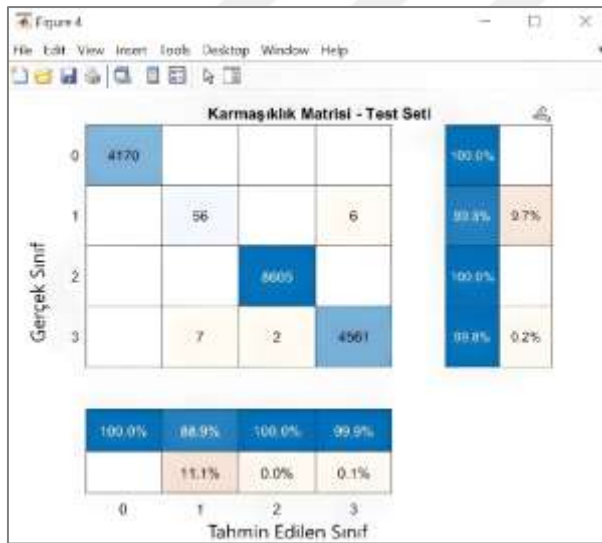
Çizelge 4.6'da KNN modeline ait sınıf bazlı tahmin süreleri yer almaktadır. Çizelge 4.6 incelendiğinde, KNN modelinin farklı saldırı türlerine yönelik tahmin sürelerinin senaryoya

göre değişiklik gösterdiği görülmektedir. TCP SYN flood ve komut enjeksiyonu saldırıları, modelin daha uzun sürede tahmin gerçekleştirdiği senaryolardır. Bu durum, ilgili saldırı türlerinin örüntü yapısının sınıflandırma sürecinde daha fazla işlem yükü oluşturduğunu göstermektedir.

Çizelge 4.6. KNN modeline ait sınıf bazlı tahmin süreleri

Senaryolar	Tahmin Süreleri (ms)
Normal durum	2440,2113
ARP spoofing saldırısı	81,7410
TCP SYN flood saldırısı	5057,8583
Komut enjeksiyonu saldırısı	2777,9689

Şekil 4.12’de KNN modelinin karmaşıklık matrisi yer almaktadır. Karmaşıklık matrisinde sağ kenarda yer alan çubuklar her bir gerçek sınıfın doğru sınıflanma oranlarını, alt kısımda yer alan çubuklar ise tahmin edilen sınıfların doğruluk oranlarını göstermektedir.



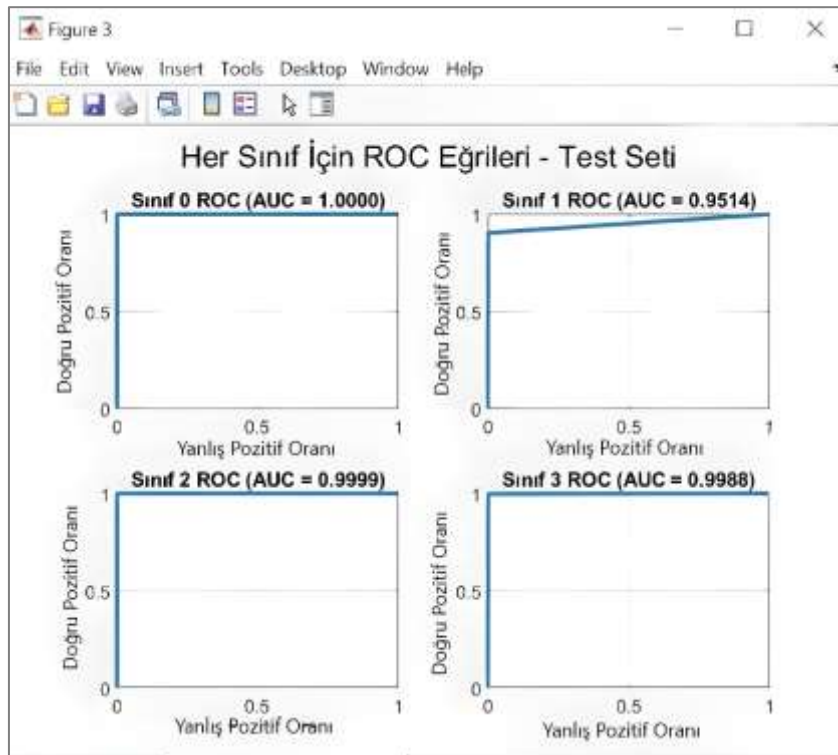
Şekil 4.12. KNN modeli karmaşıklık matrisi

KNN modelinin karmaşıklık matrisi verilerine göre performansı Çizelge 4.7’de yorumlanmıştır. Modelin test veri kümesindeki genel performansı oldukça yüksektir. Sadece Sınıf 1 (ARP spoofing) için görece düşük bir başarı oranı gözlemlenmiş olup, bu sapma tolere edilebilir düzeydedir. Elde edilen sonuçlar, modelin aşırı öğrenme (overfitting) eğilimi göstermediğini ve genelleme yeteneğinin güçlü olduğunu ortaya koymaktadır.

Çizelge 4.7. KNN modelinin karmaşıklık matrisi verilerine göre performansı

Senaryolar	Doğru Sınıflanan Örnek	Toplam Örnek Sayısı	Doğruluk (%)	Yanlış Sınıflama Bilgisi
Normal durum	4170	4170	100	-
ARP spoofing saldırısı	56	62	90,3	6 örnek komut enjeksiyonu saldırısı olarak sınıflandırılmış
TCP SYN flood saldırısı	8605	8605	100	-
Komut enjeksiyonu saldırısı	4561	4570	99,8	7 örnek ARP spoofing saldırısı olarak sınıflandırılmış, 2 örnek TCP SYN Flood saldırısı olarak sınıflandırılmış

Şekil 4.13’de, her bir sınıfa ait ROC eğrileri ve karşılık gelen AUC değerleri verilmiştir. Tüm sınıflar için $AUC > 0,9$ olup modelin sınıflar arasında yüksek düzeyde ayırt edicilik yeteneğine sahip olduğunu göstermektedir. KNN algoritması, bu çalışmada kullanılan veri kümesi üzerinde yüksek sınıflandırma başarısı göstermiştir. Eğitim, doğrulama ve test aşamalarında tutarlı sonuçlar elde edilmiş; aşırı öğrenme belirtileri gözlenmemiştir. ROC-AUC değerleri ve karmaşıklık matrisi, modelin genel başarımını desteklemektedir.

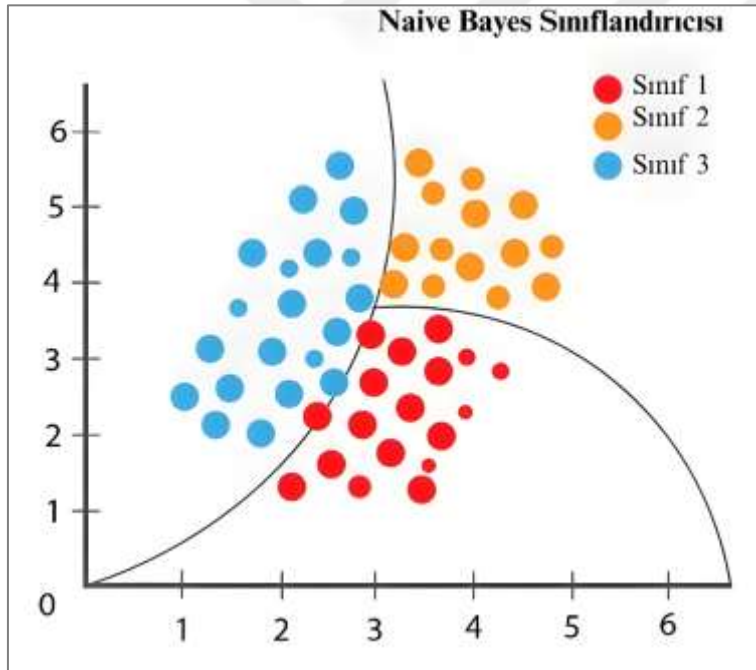


Şekil 4.13. KNN modeli her sınıf için ROC eğrileri

NB modeli

Naive Bayes sınıflandırıcıları, temelini Bayes teoreminden alan ve olasılıksal yaklaşıma dayanan sınıflandırma algoritmalarıdır. Bu yöntem, veri kümesindeki özelliklerin sıklıklarını ve değer kombinasyonlarını dikkate alarak çeşitli olasılıkları hesaplar. Her bir sınıf için gözlemlerin gerçekleşme olasılığı değerlendirilir ve en yüksek olasılığa sahip sınıfa ait olduğu varsayılarak sınıflandırma işlemi gerçekleştirilir [119].

Şekil 4.14'te her sınıfa ait veri noktalarının kümелendiği görülmekte olup eğrisel karar sınırları, ilgili bölgedeki sınıflardan hangisinin olasılık açısından baskın olduğunu göstermektedir. Örneğin, şeklin sağ alt bölgesinde kırmızı sınıfa ait örneklerin yoğunluğu daha fazladır. Bu nedenle, Naive Bayes sınıflandırıcısı bu bölgeye düşen yeni bir örneği, olasılığı en yüksek sınıf olan “Sınıf 1” olarak sınıflandıracaktır.



Şekil 4.14. Naive Bayes algoritması temel çalışma prensibi

Çizelge 4.8’de sunulan Naive Bayes algoritmasının genel performansı incelendiğinde, Sınıf 2 (TCP SYN flood) için tüm metriklerde %99’un üzerinde yüksek başarı elde edilmiştir. Bu durum, modelin bu saldırı türünü güvenilir şekilde tanıyabildiğini göstermektedir. Sınıf 3’te (komut enjeksiyonu) benzer şekilde dengeli ve güçlü bir performans göstermiştir. Doğruluk, kesinlik, duyarlılık ve F1 skoru arasındaki uyum, modelin bu sınıfı hem doğru tanıma hem

de yanlış sınıflamaları önleme konusunda etkili olduğunu göstermektedir. Sınıf 0 (normal durum) için metriklerin dengeli ancak diğer sınıflara kıyasla bir miktar daha düşük olması, bu sınıfın ayrımının nispeten daha zor olduğunu göstermektedir. Öte yandan, Sınıf 1 (ARP spoofing) için duyarlılık yüksek olsa da kesinliğin belirgin şekilde düşük kalması, modelin bu sınıfa ait olmayan örnekleri de yanlışlıkla bu sınıfa atama eğiliminde olduğunu göstermektedir. Bu durum, veri setinde sınıf dengesizliği ve sınıf 1'e ait örneklerin sayısının az olması gibi faktörlerden kaynaklanmaktadır. Tüm sınıflar için özgüllük değerlerinin yüksek olması, modelin yanlış pozitif oranlarını düşük tuttuğunu ve genelleme yeteneğinin güçlü olduğunu göstermektedir. Genel olarak değerlendirildiğinde, modelin çoğu sınıf üzerinde başarılı bir performans sergilediği ve sadece bazı sınıflar için diğerlerine kıyasla başarı oranının düşük kaldığı söylenebilir.

Çizelge 4.8. NB modeli test metrikleri

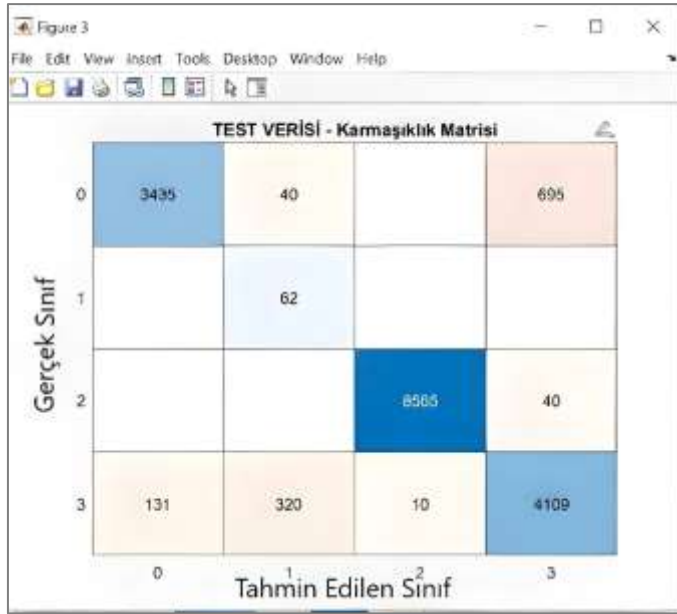
Senaryolar	Doğruluk	Kesinlik	Duyarlılık	Özgüllük	F1 Skoru
Normal durum	0,82374	0,96326	0,82374	0,9901	0,88806
ARP spoofing saldırısı	1	0,14692	1	0,97924	0,2562
TCP SYN flood saldırısı	0,99535	0,99883	0,99535	0,99886	0,99709
Komut enjeksiyonu saldırısı	0,89912	0,84827	0,89912	0,94274	0,87296

Çizelge 4.9'da, Naive Bayes modelinin sınıf bazlı tahmin süreleri verilmiştir. Sonuçlar, modelin tüm senaryolarda oldukça düşük sürelerde tahmin gerçekleştirdiğini göstermektedir. Bu durum, Naive Bayes'in işlem yükü açısından son derece verimli bir yapıya sahip olduğunu ortaya koymakta ve gerçek zamanlı sistemlerde kullanım potansiyelini desteklemektedir.

Çizelge 4.9. NB modeline ait sınıf bazlı tahmin süreleri

Senaryolar	Tahmin Süreleri (ms)
Normal durum	19,8424
ARP spoofing saldırısı	3,1637
TCP SYN flood saldırısı	5,2354
Komut enjeksiyonu saldırısı	4,5778

Şekil 4.15'te Naive Bayes modelinin karmaşıklık matrisi yer almaktadır.



Şekil 4.15. Naive Bayes modeli karmaşıklık matrisi

Naive Bayes modelinin karmaşıklık matrisi verilerine göre performans değerlendirmesi Çizelge 4.10'da sunulmuştur.

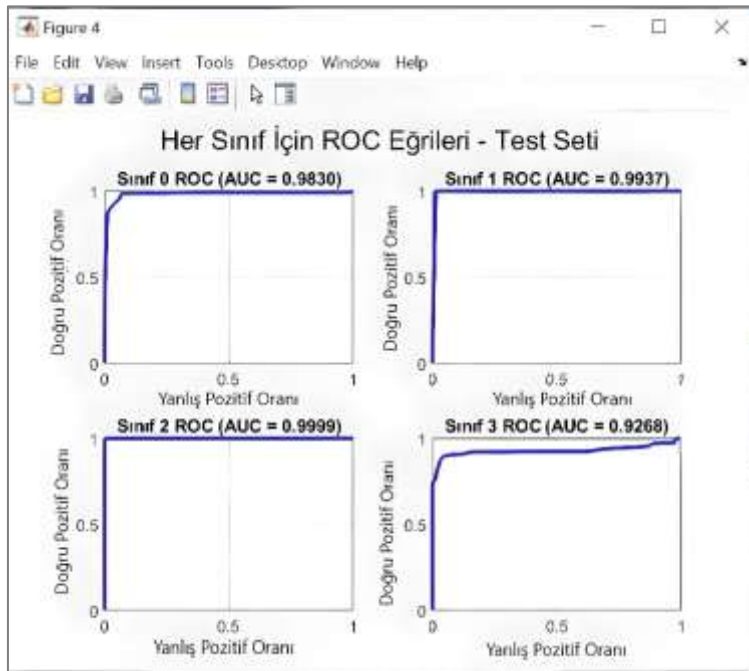
Çizelge 4.10. NB modelinin karmaşıklık matrisi verilerine göre performansı

Senaryolar	Doğru Sınıflanan Örnek	Toplam Örnek Sayısı	Doğruluk (%)	Yanlış Sınıflama Bilgisi
Normal durum	3435	4170	82,3	695 örnek komut enjeksiyonu saldırısı olarak sınıflandırılmış, 40 örnek ARP spoofing saldırısı olarak sınıflandırılmış
ARP spoofing saldırısı	62	62	100	-
TCP SYN flood saldırısı	8565	8605	99,5	40 örnek komut enjeksiyonu saldırısı olarak sınıflandırılmış
Komut enjeksiyonu saldırısı	4109	4570	89,9	131 örnek normal durum olarak sınıflandırılmış, 320 örnek ARP spoofing saldırısı olarak sınıflandırılmış ve 10 örnek TCP SYN flood saldırısı olarak sınıflandırılmış

Modelin bazı sınıflarda oldukça yüksek doğruluk sağladığı, özellikle belirgin özelliklere sahip saldırı türlerinde sınıflandırma performansının tatmin edici olduğu görülmektedir. Bununla birlikte, bazı sınıflar arasında gözlemlenen yanlış sınıflandırmalar, modelin belirli

sınıfları ayırmada zorlandığını göstermektedir. Genel olarak model, belirli sınıflarda güçlü performans sergilese de, tüm sınıflar arasında tutarlı bir ayırt edicilik sunamayabileceğini ortaya koymaktadır.

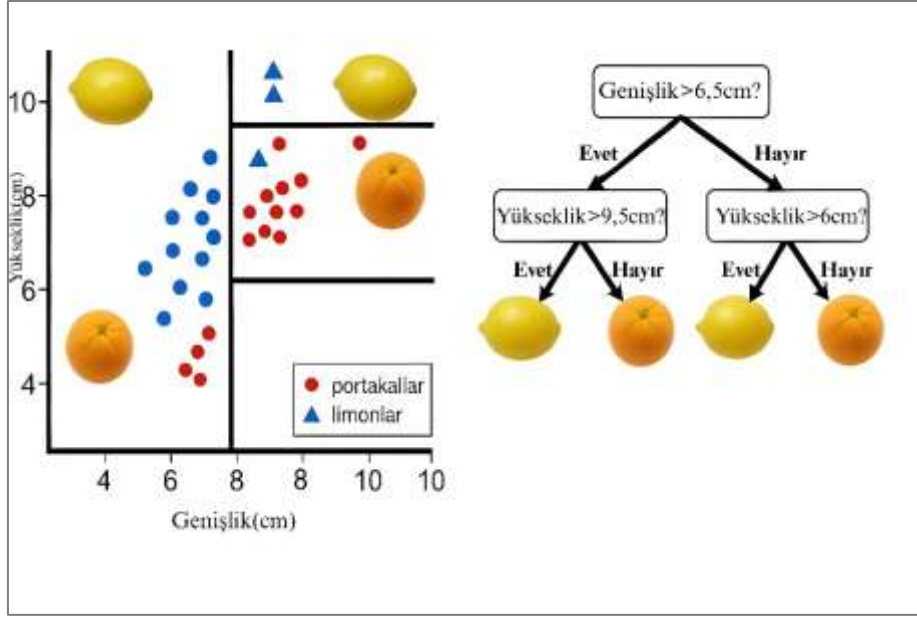
Şekil 4.16'da, her bir sınıfa ait ROC eğrileri ve karşılık gelen AUC değerleri verilmiştir. Tüm sınıflarda $AUC > 0,92$ olarak elde edilmiş ve özellikle bazı sınıflarda 0,99'un üzerinde değerler gözlemlenmiştir. ROC-AUC değerleri ve sınıf bazlı doğruluk oranları birlikte değerlendirildiğinde, Naive Bayes algoritmasının genel başarımının tatmin edici düzeyde olduğu görülmektedir. Naive Bayes modelinin eğitim, doğrulama ve test kümelerinde gösterdiği benzer performans, metriklerde ciddi bir bozulma olmaması ve ROC-AUC değerlerinin tutarlılığı dikkate alındığında, modelde aşırı öğrenme (overfitting) belirtisi bulunmamaktadır. Ancak, Naive Bayes modeli, basit ve hızlı bir yöntem olmasına karşın, karmaşık ilişkiler içeren bu veri seti için yeterli sınıflandırma performansı sunmamıştır. Özellikle ARP spoofing (Sınıf 1) için elde edilen düşük kesinlik değeri, modelin bu tür saldırıları sağlıklı şekilde ayırt edemediğini göstermektedir. Bu sınıfa ait örneklerin başka sınıflarla karıştırılması, Naive Bayes'in özellik bağımsızlığı varsayımının bu veri setinde sınırlayıcı bir faktör olduğunu ortaya koymuştur.



Şekil 4.16. Naive Bayes modeli her sınıf için ROC eğrileri

DT modeli

Karar ağacı, kök düğüm olarak adlandırılan başlangıç noktasından itibaren dallanarak ilerleyen ve değişkenler arasında hiyerarşik bir ilişki kuran ağaç yapısında bir modeldir [120]. Şekil 4.17’de görüldüğü üzere bir karar ağacı basitçe bir soru sorar ve cevaba göre (“Evet”/“Hayır”) ağacı alt ağaçlara böler.



Şekil 4.17. Karar ağacı öğrenme süreci [121]

DT modeline ait test metrikleri Çizelge 4.11’de yer almaktadır. Test verisi metrikleri incelendiğinde, modelin genel olarak yüksek doğruluk ve sınıf bazlı tutarlılık sergilediği görülmektedir. Sınıf 0 (Normal durum) ve Sınıf 2 (TCP SYN flood) için tüm metriklerde maksimuma yakın değerlere ulaşılmış, bu durum modelin bu sınıfları iyi biçimde tanımlayabildiğini göstermektedir. Sınıf 3 (Komut enjeksiyonu) için de doğruluk, kesinlik ve duyarlılık açısından yüksek ve dengeli bir performans gözlemlenmiştir. Öte yandan, Sınıf 1 (ARP spoofing) için metrikler görece daha düşük düzeydedir; bu durum, modelin bu sınıfı ayırt etmede diğer sınıflara kıyasla daha az belirginlik ortaya koyduğunu göstermektedir. Genel olarak model, çoğu sınıf üzerinde istikrarlı ve başarılı bir sınıflandırma performansı sergilemiştir.

Çizelge 4.11. DT modeli test metrikleri

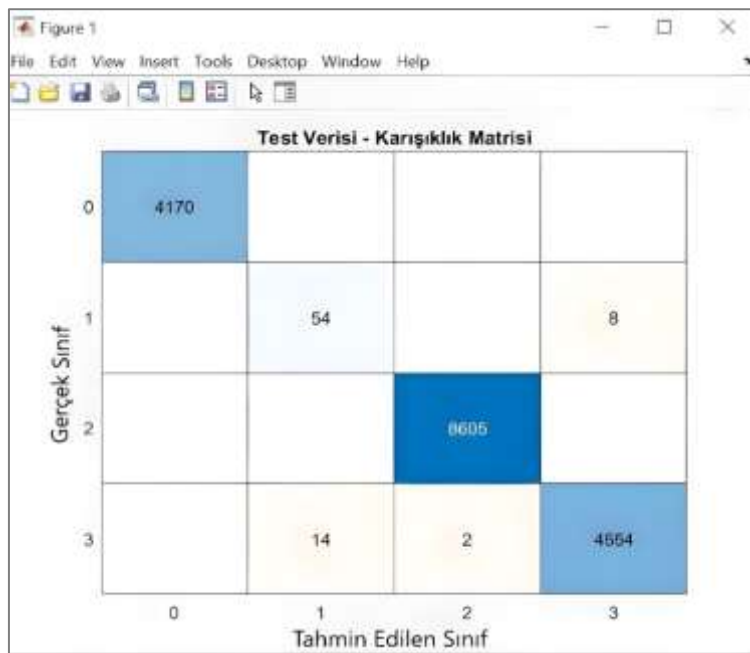
Senaryolar	Doğruluk	Kesinlik	Duyarlılık	Özgüllük	F1 Skoru
Normal durum	1	1	1	1	1
ARP spoofing saldırısı	0,87097	0,79412	0,87097	0,99919	0,83077
TCP SYN flood saldırısı	1	0,99977	1	0,99977	0,99988
Komut enjeksiyonu saldırısı	0,9965	0,99825	0,9965	0,99938	0,99737

Çizelge 4.12 incelendiğinde, karar ağacı modelinin normal duruma ait tahmin süresinin diğer sınıflara kıyasla daha yüksek olduğu görülmektedir. Buna karşılık, saldırı senaryolarına ait sınıflar daha kısa sürede tahmin edilmiştir. Bu da karar ağacının bu sınıfları daha belirgin ayırt edici özellikler üzerinden hızlı bir şekilde sınıflandırabildiğini ortaya koymaktadır.

Çizelge 4.12. DT modeline ait sınıf bazlı tahmin süreleri

Senaryolar	Tahmin Süreleri (ms)
Normal durum	25,8685
ARP spoofing saldırısı	2,7556
TCP SYN flood saldırısı	3,1041
Komut enjeksiyonu saldırısı	2,3997

Şekil 4.18’de karar ağacı modelinin karmaşıklık matrisi yer almaktadır.



Şekil 4.18. Karar ağacı modeli karmaşıklık matrisi

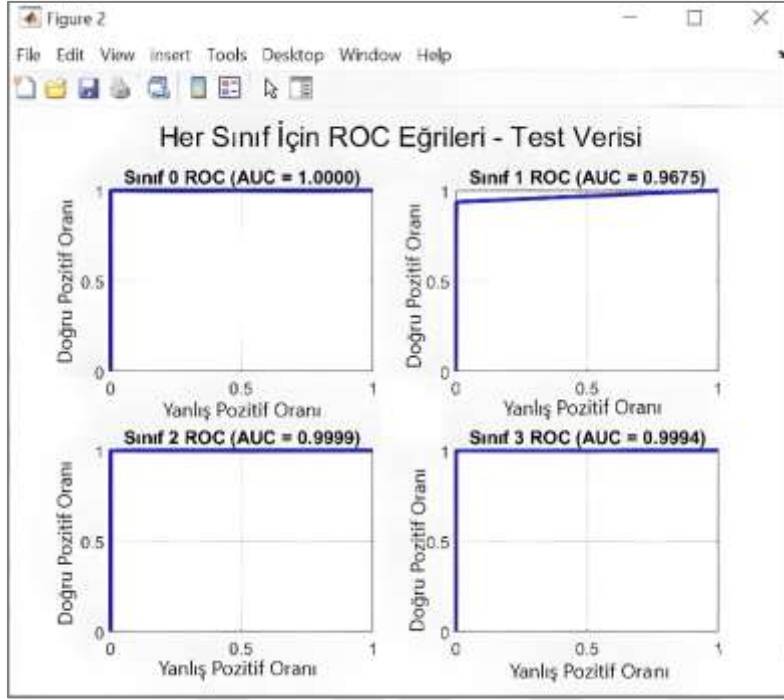
Karar ağacı modelinin karmaşıklık matrisi verilerine göre performansı Çizelge 4.13'te yorumlanmıştır.

Çizelge 4.13. DT modelinin karmaşıklık matrisi verilerine göre performansı

Senaryolar	Doğru Sınıflanan Örnek	Toplam Örnek Sayısı	Doğruluk (%)	Yanlış Sınıflama Bilgisi
Normal durum	4170	4170	100	-
ARP spoofing saldırısı	54	62	87,1	8 örnek komut enjeksiyonu saldırısı olarak sınıflandırılmış
TCP SYN flood saldırısı	8605	8605	100	-
Komut enjeksiyonu saldırısı	4554	4570	99,6	14 örnek ARP spoofing saldırısı olarak sınıflandırılmış, 2 örnek TCP SYN flood saldırısı olarak sınıflandırılmış

DT modeli, genel olarak yüksek sınıflandırma başarısı göstermiştir. Normal trafik ve TCP SYN flood saldırıları doğru şekilde sınıflandırılmıştır. Ancak ARP spoofing ve komut enjeksiyonu saldırıları arasında sınırlı düzeyde sınıflandırma hataları gözlemlenmiştir. Bu durum, modelin bazı saldırı türlerini ayırt etmede sınırlı bir ayırım gücüne sahip olabileceğini göstermektedir. Eğitim, doğrulama ve test verileri üzerinde benzer düzeyde yüksek performans sergilemesi ise, modelin aşırı öğrenme (overfitting) eğilimi göstermediğini ortaya koymaktadır.

Şekil 4.19'daki test verisine ait ROC eğrileri doğrultusunda elde edilen AUC değerleri, karar ağacı modelinin sınıflar arasında üstün düzeyde bir sınıflandırma yeteneğine sahip olduğunu göstermektedir. Tüm sınıflarda $AUC > 0,96$ olması, modelin yüksek duyarlılık ve özgüllükle çalıştığını, dolayısıyla pozitif ve negatif örnekleri başarılı şekilde ayırt edebildiğini ortaya koymaktadır. AUC değeri 0,9 ile 1,0 arasında olan modellerin sınıflar arası ayrımı güçlü biçimde gerçekleştirdiği dikkate alındığında, karar ağacı modeli bu test seti üzerinde genel olarak güçlü ve güvenilir bir performans sergilemiştir.

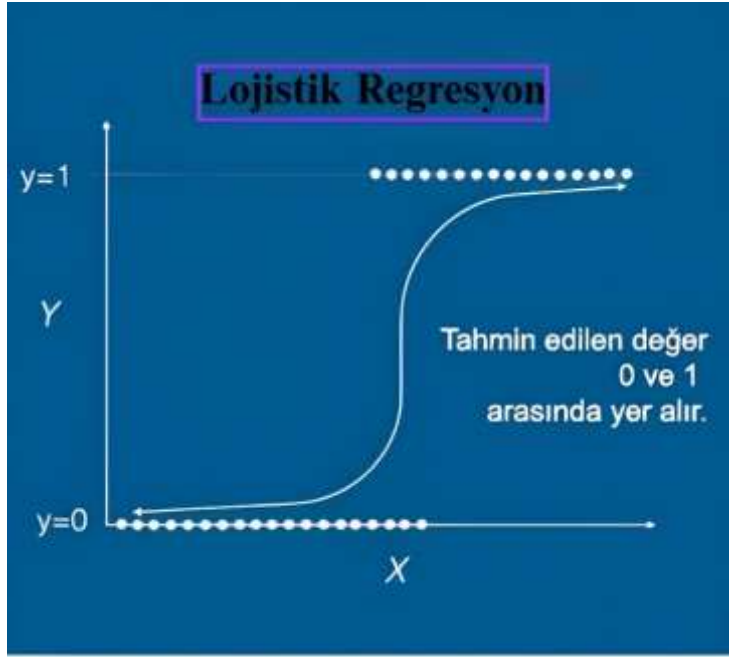


Şekil 4.19. Karar ağacı modeli her sınıf için ROC eğrileri

LR modeli

Lojistik regresyon modellerinde tahmin için yaygın olarak en çok olabilirlik yöntemi kullanılmaktadır. Bu yöntem, gözlemlenen verilerin gerçekleşme olasılığını en üst düzeye çıkaran parametre değerlerini belirlemeyi amaçlar. Bunun için ilgili olabilirlik fonksiyonu tanımlanır ve parametreler, bu fonksiyonu maksimum yapan değerler olarak tahmin edilir [122].

Şekil 4.20, lojistik regresyon modelinin sınıflandırma sürecini tanımlayan sigmoid (S-eğrisi) fonksiyonunu göstermektedir. Lojistik regresyon modeli, girdilere karşılık gelen çıktıların 0 ile 1 arasında bir değer almasını sağlayarak, gözlemin belirli bir sınıfa ait olma olasılığını tahmin eder. Modelin tahmin ettiği değerler 0'a yaklaştıkça sınıf 0, 1'e yaklaştıkça sınıf 1 olarak yorumlanır.



Şekil 4.20. Lojistik regresyon temel çalışma prensibi

Çizelge 4.14’ te sunulan test verisi üzerinde elde edilen performans metrikleri, modelin genel olarak yüksek doğruluk ve sınıf bazlı dengeli bir performans sergilediği görülmektedir. Sınıf 0 (Normal durum) ve Sınıf 2 (TCP SYN flood) için tüm metriklerde oldukça yüksek değerler elde edilmiş, bu sınıfların başarıyla tanımlandığı anlaşılmıştır. Sınıf 3 (Komut enjeksiyonu) için de doğruluk, kesinlik ve duyarlılık değerleri tutarlıdır. Ancak Sınıf 1 (ARP spoofing) için kesinlik ve F1 skoru görece daha düşüktür. Bu durum, modelin bu sınıfı diğerlerinden ayırt etmede nispeten zorlandığını göstermektedir. Genel olarak model, test verisi üzerinde güçlü ve tutarlı bir sınıflandırma performansı sunmuştur.

Çizelge 4.14. LR modeli test metrikleri

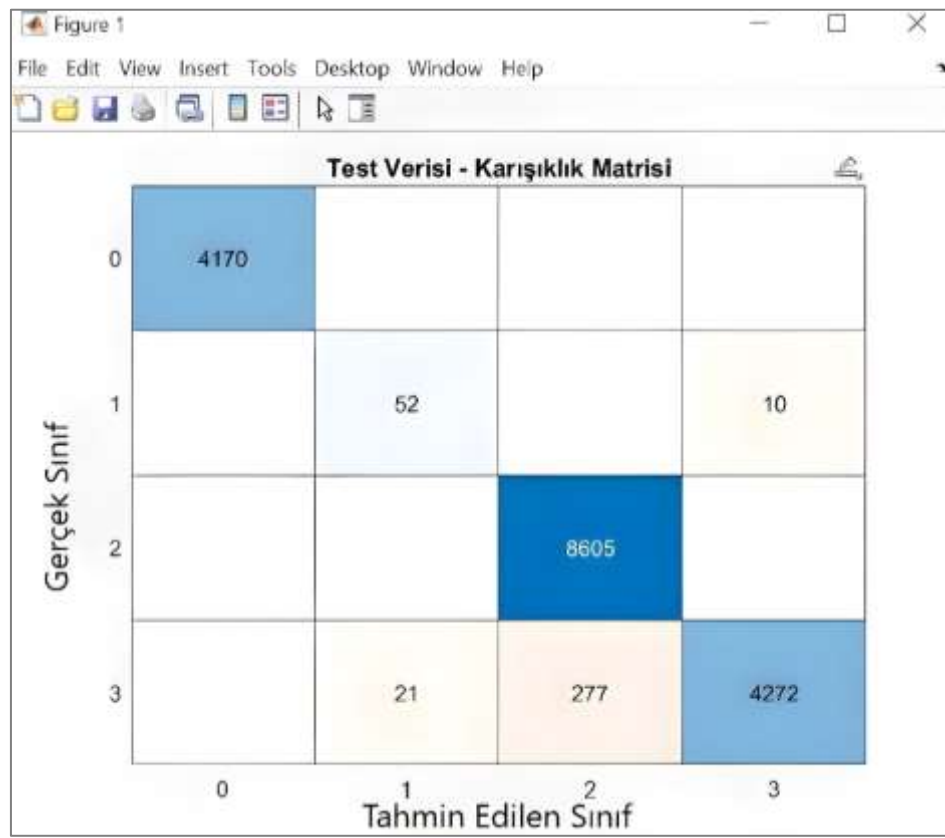
Senaryolar	Doğruluk	Kesinlik	Duyarlılık	Özgüllük	F1 Skoru
Normal durum	1	1	1	1	1
ARP spoofing saldırısı	0,83871	0,71233	0,83871	0,99879	0,77037
TCP SYN flood saldırısı	1	0,96881	1	0,96853	0,98416
Komut enjeksiyonu saldırısı	0,93479	0,99766	0,93479	0,99922	0,96521

Çizelge 4.15’te LR modeline ait sınıf bazlı tahmin süreleri verilmiştir. Tahmin süresi, saldırı türüne göre değişiklik göstermektedir. En kısa tahmin süresi komut enjeksiyonu saldırısına ait olup, diğer sınıflarda daha uzun süreler gözlemlenmiştir.

Çizelge 4.15. LR modeline ait sınıf bazlı tahmin süreleri

Senaryolar	Tahmin Süreleri (ms)
Normal durum	48,2015
ARP spoofing saldırısı	27,6650
TCP SYN flood saldırısı	7,3001
Komut enjeksiyonu saldırısı	6,2642

Şekil 4.21’de lojistik regresyon modelinin karmaşıklık matrisi yer almaktadır.



Şekil 4.21. Lojistik regresyon modeli karmaşıklık matrisi

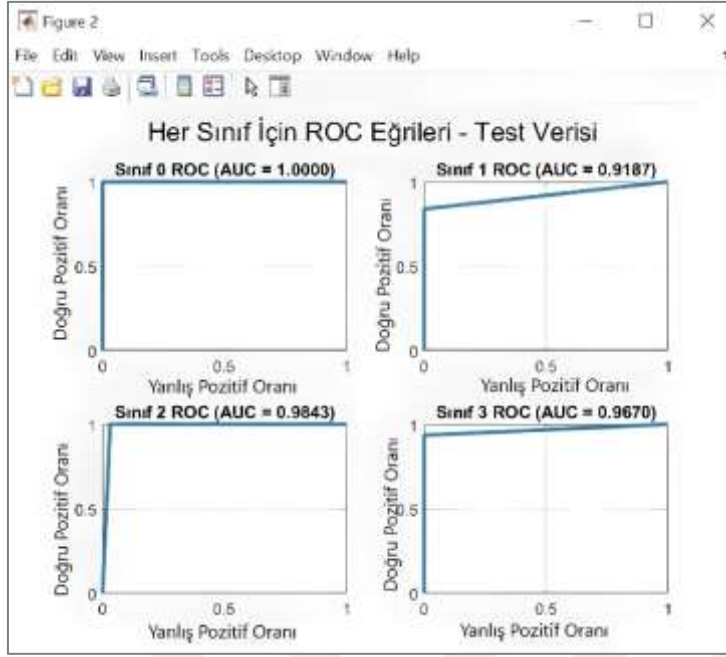
Lojistik Regresyon modelinin karmaşıklık matrisi verilerine göre performansı Çizelge 4.16’da yorumlanmıştır.

Çizelge 4.16. LR modelinin karmaşıklık matrisi verilerine göre performansı

Senaryolar	Doğru Sınıflanan Örnek	Toplam Örnek Sayısı	Doğruluk (%)	Yanlış Sınıflama Bilgisi
Normal durum	4170	4170	100	-
ARP spoofing saldırısı	52	62	83,9	10 örnek komut enjeksiyonu saldırısı olarak sınıflandırılmış
TCP SYN flood saldırısı	8605	8605	100	-
Komut enjeksiyonu saldırısı	4272	4570	93,5	21 örnek ARP spoofing saldırısı olarak sınıflandırılmış, 277 örnek TCP SYN flood saldırısı olarak sınıflandırılmış

Karışıklık matrisi ve sınıf bazlı doğruluk sonuçları incelendiğinde, lojistik regresyon algoritmasının çoğu sınıfı yüksek doğrulukla sınıflandırabildiği görülmektedir. Model, özellikle bazı trafik türlerinde tüm örnekleri hatasız şekilde doğru sınıfa atayarak güçlü bir ayırt edicilik performansı sergilemiştir. Bununla birlikte, belirli sınıflar arasında gözlemlenen sınırlı sayıdaki karışıklıklar, modelin bazı durumlarda ayırım yapmakta zorlandığını göstermektedir. Genel olarak değerlendirildiğinde, modelin test verisi üzerindeki başarımı, dengeli ve güvenilir bir sınıflandırma yapabildiğini ortaya koymaktadır.

Şekil 4.22' de yer alan ROC eğrileri incelendiğinde, modelin tüm sınıflar için yüksek ayırt edicilik performansı sergilediği görülmektedir. AUC değerlerinin 0,9 ile 1,0 aralığında yer alması, modelin üstün sınıflandırma yeteneğine sahip olduğunu ortaya koymaktadır. Eğrilerin sol üst köşeye yakın konumlanması, modelin hem yüksek doğru pozitif oranına hem de düşük yanlış pozitif oranına ulaştığını göstermektedir. Bu ROC eğrileri, lojistik regresyon modelinin özellikle Normal durum ve DoS saldırılarını son derece doğru biçimde ayırt ettiğini, buna karşın MITM ve komut enjeksiyonu gibi bazı saldırı türleri arasında sınırlı da olsa karışma yaşanabileceğini ortaya koymaktadır. Genel olarak değerlendirildiğinde, modelin çok sınıflı yapılarda dengeli ve genellenebilir sonuçlar sunduğu söylenebilir.



Şekil 4.22. Lojistik regresyon modeli her sınıf için ROC eğrileri

KNN-NB hibrit modeli

Naive Bayes ve K-En Yakın Komşu algoritmalarının hibrit biçimde birleştirilmesi, Naive Bayes'in yüksek hız ve genelleme kabiliyetleri ile KNN algoritmasının örnek tabanlı, güçlü yerel sınıflandırma yeteneklerini bir araya getirerek dengeli ve tamamlayıcı bir sınıflandırma yaklaşımı sunmaktadır. NB ve KNN algoritmaları, sırasıyla düşük varyansa ve yüksek varyansa sahip olmaları nedeniyle birbirini tamamlayıcı özellikler göstermektedir. Literatürde, NB ve KNN algoritmalarının hibrit kullanımında en yaygın olarak tercih edilen yöntemler oylama (voting) ve yığılma (stacking) tabanlı yaklaşımlardır [123]. Bu çalışmada, her iki algoritmanın birlikte çalıştığı bir hibrit sınıflandırma modeli tasarlanmış ve elde edilen tahmin sonuçları oylama tabanlı birleştirme yöntemiyle bütünleştirilmiştir.

Çizelge 4.17'de KNN-NB hibrit modeli test metrikleri sunulmaktadır. Test verisi üzerinde elde edilen sınıf bazlı metrikler, modelin Normal durum (Sınıf 0) ve TCP SYN flood (Sınıf 2) saldırılarını yüksek başarıyla ayırt edebildiğini göstermektedir. Bu sınıflar için doğruluk, duyarlılık ve F1 skoru değerleri 0,99'un üzerindedir. Komut enjeksiyonu (Sınıf 3) için de kesinlik = 1,00 ve F1 skoru = 0,96 ile güçlü bir sınıflandırma performansı elde edilmiştir. Buna karşın, ARP spoofing (Sınıf 1) için modelin başarımı oldukça düşüktür; doğruluk ve duyarlılık $\approx 0,08$, kesinlik $\approx 0,04$ seviyelerindedir. Bu durum, modelin düşük örnek sayısına sahip sınıflarda ayırım yapmada zorlandığını göstermektedir. Genel olarak model, yaygın

saldırı türlerinde yüksek sınıflandırma başarısı gösterirken; veri dengesizliği, nadir saldırıların doğru şekilde tespit edilmesini zorlaştırmaktadır.

Çizelge 4.17. KNN-NB hibrit modeli test metrikleri

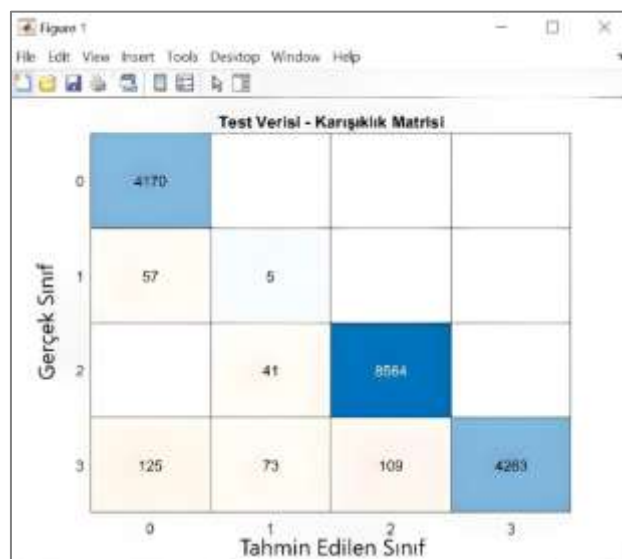
Senaryolar	Doğruluk	Kesinlik	Duyarlılık	Özgüllük	F1 Skoru
Normal durum	1	0,95818	1	0,98625	0,97864
ARP spoofing saldırısı	0,08065	0,04202	0,08065	0,99343	0,05525
TCP SYN flood saldırısı	0,99524	0,98743	0,99524	0,98762	0,99132
Komut enjeksiyonu saldırısı	0,93282	1	0,93282	1	0,96524

Çizelge 4.18’de KNN-NB hibrit modeline ait sınıf bazlı tahmin süreleri yer almaktadır. KNN-NB hibrit modeline ait sınıf bazlı tahmin süreleri incelendiğinde, TCP SYN flood saldırısına ait tahmin süresinin diğer sınıflara kıyasla oldukça yüksek olduğu görülmektedir. En kısa tahmin süresi ise ARP spoofing saldırısı senaryosunda elde edilmiştir.

Çizelge 4.18. KNN-NB hibrit modeline ait sınıf bazlı tahmin süreleri

Senaryolar	Tahmin Süreleri (ms)
Normal durum	94920,7837
ARP spoofing saldırısı	1553,9240
TCP SYN flood saldırısı	205070,6389
Komut enjeksiyonu saldırısı	104379,4106

Şekil 4.23’te KNN-NB hibrit modelinin karmaşıklık matrisi yer almaktadır.



Şekil 4.23. KNN-NB hibrit modeli karmaşıklık matrisi

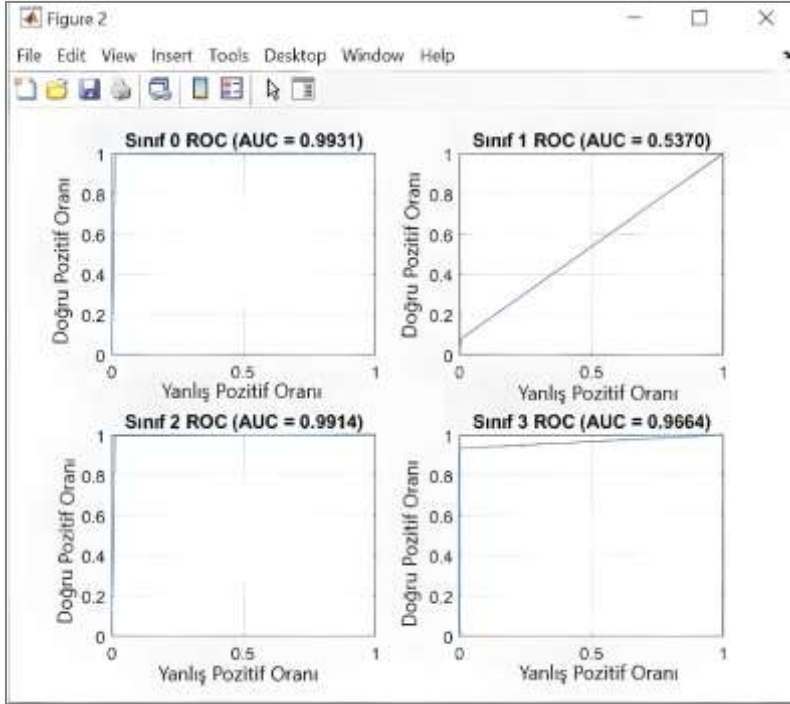
KNN-NB hibrit modelinin karmaşıklık matrisi verilerine göre performansı Çizelge 4.19’da sunulmaktadır.

Çizelge 4.19. KNN-NB hibrit modelinin karmaşıklık matrisi verilerine göre performansı

Senaryolar	Doğru Sınıflanan Örnek	Toplam Örnek Sayısı	Doğruluk (%)	Yanlış Sınıflama Bilgisi
Normal durum	4170	4170	100	-
ARP spoofing saldırısı	5	62	8,1	57 örnek normal durum olarak sınıflandırılmış
TCP SYN flood saldırısı	8564	8605	99,5	41 örnek ARP spoofing saldırısı olarak sınıflandırılmış
Komut enjeksiyonu saldırısı	4263	4570	93,3	125 örnek normal durum olarak sınıflandırılmış, 73 örnek ARP spoofing saldırısı olarak sınıflandırılmış ve 109 örnek TCP SYN flood saldırısı olarak sınıflandırılmış

Bu hibrit modelde, normal durum ve belirgin saldırı türleri doğru sınıflandırılırken, örnek sayısı az olan saldırılarda karışıklıklar oluşmuştur. Bu durum, modelin güçlü yönlerinin yanı sıra dengesiz veri dağılımına karşı hassasiyetini de ortaya koymaktadır.

Şekil 4.24 incelendiğinde, hibrit model, Normal durum (Sınıf 0), TCP SYN flood (Sınıf 2) ve komut enjeksiyonu (Sınıf 3) için 0,9’un üzerinde AUC değerleri ile üstün sınıflandırma yeteneği göstermektedir. Buna karşın, ARP spoofing (Sınıf 1) için elde edilen AUC = 0,537 değeri, modelin bu saldırı türü üzerinde ayırım yapma yetisinin zayıf olduğunu ve sınıflandırma performansının yetersiz kaldığını göstermektedir. Modelin sınıf dengesizliği içeren veri kümelerinde performansının düştüğü gözlemlenmiştir. Özellikle düşük örnek sayısına sahip saldırı türlerinde, sınıflar arası ayırım gücü zayıflamış ve bu durum sınıflandırma doğruluğunu olumsuz etkilemiştir.



Şekil 4.24. KNN-NB hibrit modeli her sınıf için ROC eğrileri

DT-LR hibrit modeli

Bu hibrit modelde, sınıflar arası dengesizliğin ve karmaşık örüntülerin bulunduğu veri seti için DT ve LR algoritmaları stacking tabanlı bir hibrit model olarak birleştirilmiştir. Karar ağacı, veriyi kurallara göre bölerek sınıf ayrımını güçlü şekilde yaparken; lojistik regresyon, bu ayrılmış yapılar üzerinde daha hassas ve genelleyici sınıflandırmalar gerçekleştirmektedir. Bu hibrit yapı sayesinde, zayıf sınıfların tanınma oranının artırılması, aşırı öğrenme riskinin azaltılması ve modelin genelleme performansının iyileştirilmesi amaçlanmıştır.

Çizelge 4.20’ de DT-LR hibrit modeline ait test metrikleri yer almaktadır. Modelin test verisi üzerindeki performansı, sınıflar arasında genel olarak dengeli ve güvenilir bir sonuç ortaya koymaktadır. Kesinlik değerlerinin yüksek olması, modelin pozitif sınıflara ait örnekleri doğru şekilde tanımladığını; yani pozitif olarak tahmin edilen örneklerin büyük çoğunluğunun gerçekten pozitif olduğunu göstermektedir. Benzer şekilde, duyarlılık değerlerinin yüksekliği ise modelin pozitif örnekleri gözden kaçırmadan doğru biçimde tespit ettiğini; yani gerçek pozitif örnekleri yanlışlıkla negatif olarak sınıflandırma oranının düşük olduğunu ortaya koymaktadır. Öte yandan, yüksek özgüllük değerleri modelin negatif sınıfları da doğru tanımlayabildiğini göstermekte; bu da yanlış alarm üretme olasılığının

düşük olduğunu ifade etmektedir. Bu metriklerin birlikte değerlendirilmesi, modelin overfitting eğiliminden uzak, genellenebilir bir performans sergilediğini göstermektedir. Genel olarak model, farklı saldırı türlerini başarılı şekilde ayırt edebilme yeteneğiyle öne çıkmaktadır.

Çizelge 4.20. DT-LR hibrit modeli test metrikleri

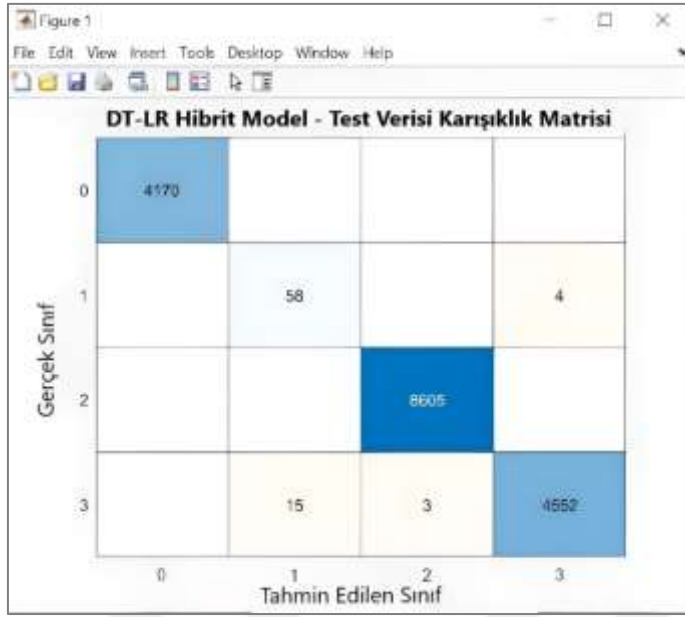
Senaryolar	Doğruluk	Kesinlik	Duyarlılık	Özgüllük	F1 Skoru
Normal durum	1	1	1	1	1
ARP spoofing saldırısı	0,93548	0,79452	0,93548	0,99914	0,85926
TCP SYN flood saldırısı	1	0,99965	1	0,99966	0,99983
Komut enjeksiyonu saldırısı	0,99606	0,99912	0,99606	0,99969	0,99759

Çizelge 4.21’de DT-LR hibrit modeline ait sınıf bazlı tahmin süreleri bulunmaktadır. DT-LR hibrit modelinin sınıf bazlı tahmin sürelerinin saldırı türlerine göre farklılık gösterdiği görülmektedir. Modelin tüm sınıflar için hızlı ve tutarlı sonuçlar üretmesi, gerçek zamanlı uygulamalar açısından önemli bir avantajdır. Özellikle saldırı senaryolarında daha kısa sürede tepki verebilmesi, modelin etkinliğini göstermektedir.

Çizelge 4.21. DT-LR hibrit modeline ait sınıf bazlı tahmin süreleri

Senaryolar	Tahmin Süreleri (ms)
Normal durum	17,8306
ARP spoofing saldırısı	13,5879
TCP SYN flood saldırısı	9,2299
Komut enjeksiyonu saldırısı	6,1357

Şekil 4.25’te DT-LR hibrit modelinin karmaşıklık matrisi yer almaktadır.



Şekil 4.25. DT-LR hibrit modeli karmaşıklık matrisi

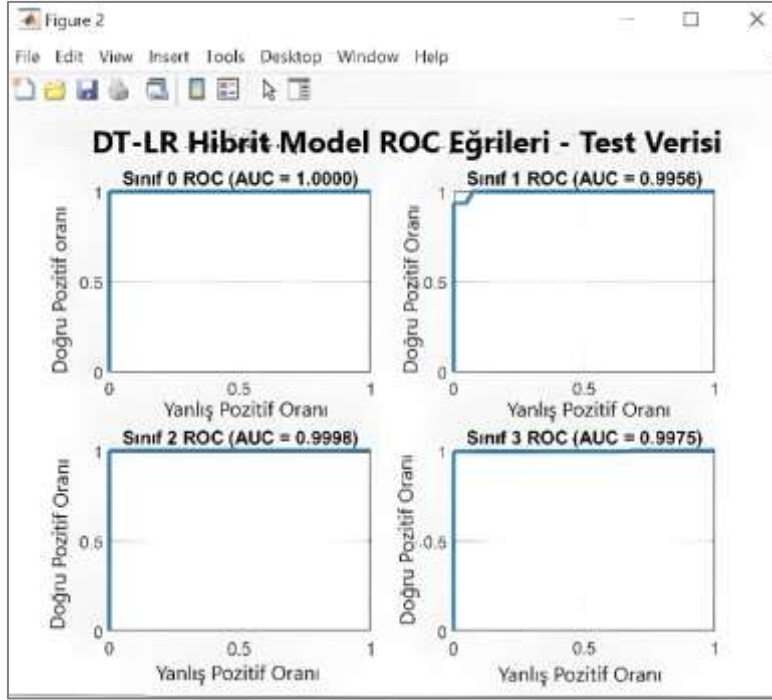
DT-LR hibrit modelinin karmaşıklık matrisi verilerine göre performansı Çizelge 4.22’de sunulmaktadır.

Çizelge 4.22. DT-LR hibrit modelinin karmaşıklık matrisi verilerine göre performansı

Senaryolar	Doğru Sınıflanan Örnek	Toplam Örnek Sayısı	Doğruluk (%)	Yanlış Sınıflama Bilgisi
Normal durum	4170	4170	100	-
ARP spoofing saldırısı	58	62	93,55	4 örnek komut enjeksiyonu saldırısı olarak sınıflandırılmış
TCP SYN flood saldırısı	8605	8605	100	-
Komut enjeksiyonu saldırısı	4552	4570	99,6	15 örnek normal durum olarak sınıflandırılmış, 3 örnek ARP spoofing saldırısı olarak sınıflandırılmış

Modelde, normal durum ve TCP SYN flood saldırıları yüksek doğrulukla sınıflandırılırken, ARP spoofing sınıfında sınırlı bir karışıklık oluşmuştur.

Şekil 4.26’da yer alan modelin ROC eğrileri incelendiğinde, tüm sınıflar için AUC değerlerinin 0,99’un üzerinde olduğu görülmüştür. Bu durum, AUC değeri aralıklarına göre değerlendirildiğinde, modelin üstün bir sınıflandırma yeteneğine sahip olduğunu göstermektedir. Sonuç olarak, DT-LR hibrit modeli, çok sınıflı veri yapısında yüksek ayırt edicilik gücü ve güvenilir performans sergilemiştir.



Şekil 4.26. DT-LR hibrit modeli her sınıf için ROC eğrileri

KNN- NB- DT hibrit modeli

Bu çalışmada kullanılan KNN-NB-DT hibrit modeli, algoritmaların birbirini tamamlayıcı yapılarından yararlanmaktadır. DT veriyi sınıflara ayırarak ön analiz yaparken, NB genel olasılıkları tahmin eder; KNN ise örnek temelli yerel kararlar verir. Bu kombinasyon sayesinde, hem genel eğilimlerin hem de ayrıntılı örüntülerin yakalanarak sınıflandırma performansının artırılması amaçlanmaktadır.

Çizelge 4.23'te sunulan test metrikleri, hibrit modelin genel olarak yüksek doğrulukta ve dengeli bir sınıflandırma performansı göstermektedir. Normal durum, TCP SYN flood ve komut enjeksiyonu sınıflarında tüm metriklerde güçlü sonuçlar elde edilmiştir. Bu durum, modelin hem doğru pozitifleri başarılı şekilde tespit edebildiğini hem de yanlış sınıflamaları minimumda tuttuğunu ortaya koymaktadır. ARP spoofing sınıfında duyarlılık ve kesinlik değerleri nispeten daha düşük kalmış olsa da, genel metrik düzeyi modelin farklı saldırı türlerini ayırt etmede etkili olduğunu göstermektedir. Bu bağlamda, KNN-NB-DT hibrit modeli, kritik altyapılarda normal ve anormal ağ trafiğini güvenilir biçimde sınıflandırabilecek potansiyele sahiptir.

Çizelge 4.23. KNN-NB-DT hibrit modeli test metrikleri

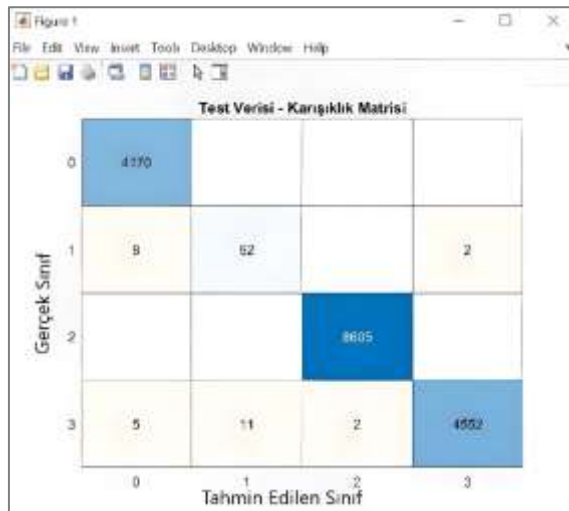
Senaryolar	Doğruluk	Kesinlik	Duyarlılık	Özgüllük	F1 Skoru
Normal durum	1	0,99689	1	0,99902	0,99844
ARP spoofing saldırısı	0,83871	0,8254	0,83871	0,99937	0,832
TCP SYN flood saldırısı	1	0,99977	1	0,99977	0,99988
Komut enjeksiyonu saldırısı	0,99606	0,99956	0,99606	0,99984	0,99781

Çizelge 4.24'te KNN-NB-DT hibrit modeline ait sınıf bazlı tahmin süreleri yer almaktadır. Sınıf bazlı tahmin süreleri incelendiğinde, modelin özellikle bazı senaryolarda uzun tahmin süreleri ürettiği görülmektedir. Bu durum, modelin gerçek zamanlı uygulamalarda kullanımını kısıtlayabilecek bir faktör olarak değerlendirilebilir.

Çizelge 4.24. KNN-NB-DT hibrit modeline ait sınıf bazlı tahmin süreleri

Senaryolar	Tahmin Süreleri (ms)
Normal durum	124683,3534
ARP spoofing saldırısı	2181,6256
TCP SYN flood saldırısı	268205,7086
Komut enjeksiyonu saldırısı	133869,8400

Şekil 4.27'de KNN-NB-DT hibrit modeline ait karmaşıklık matrisi sunulmaktadır.



Şekil 4.27. KNN-NB-DT hibrit modeli karmaşıklık matrisi

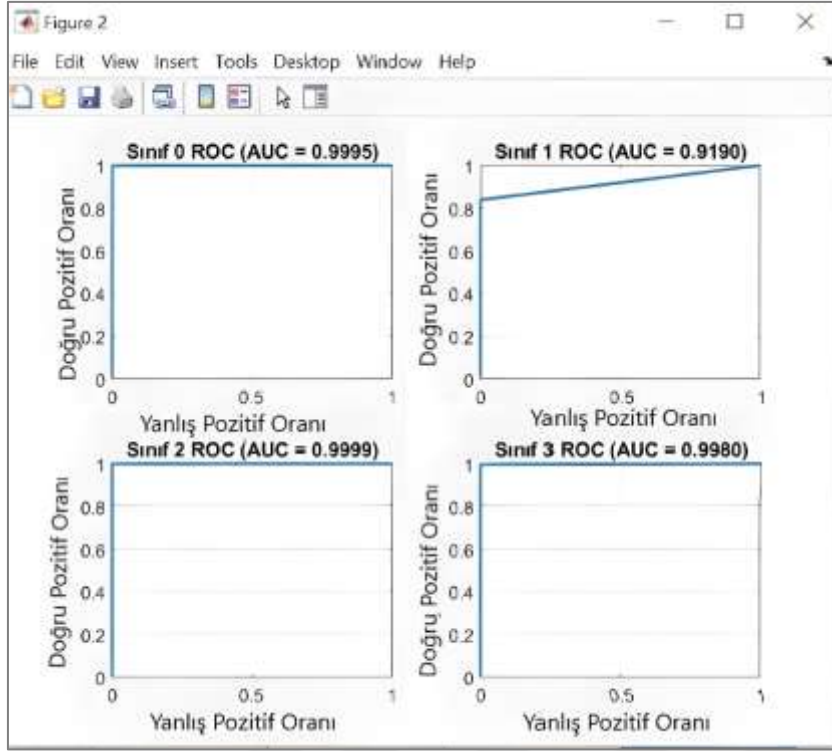
Modelin karmaşıklık matrisine ilişkin performans verileri Çizelge 4.25'te ayrıntılı olarak gösterilmektedir.

Çizelge 4.25. KNN-NB-DT hibrit modelinin karmaşıklık matrisi verilerine göre performansı

Senaryolar	Doğru Sınıflanan Örnek	Toplam Örnek Sayısı	Doğruluk (%)	Yanlış Sınıflama Bilgisi
Normal durum	4170	4170	100	-
ARP spoofing saldırısı	52	62	83,9	8 örnek normal durum olarak sınıflandırılmış, 2 örnek komut enjeksiyonu saldırısı olarak sınıflandırılmış
TCP SYN flood saldırısı	8605	8605	100	-
Komut enjeksiyonu saldırısı	4552	4570	99,6	5 örnek normal durum olarak sınıflandırılmış, 11 örnek ARP spoofing saldırısı olarak sınıflandırılmış ve 2 örnek TCP SYN flood saldırısı olarak sınıflandırılmış

Model, Normal durum ile TCP SYN flood saldırılarını hatasız sınıflandırmış, komut enjeksiyonu için yüksek doğruluk sağlamıştır. En düşük başarı ARP spoofing sınıfında gözlemlenmiş, bazı örnekler farklı sınıflarla karıştırılmıştır. ARP spoofing (Sınıf 1) sınıfındaki görece düşük doğruluk oranı, modelin bu saldırı türünü ayırt etmede zorlandığını göstermektedir. Bu durum, sınıf örneklerinin azlığına bağlı olarak oluşan dengesiz veri dağılımından kaynaklanmakta olup, modelin bu sınıfa ait temsili öğrenmesini sınırlamıştır.

Şekil 4.28’de yer alan ROC eğrilerine göre elde edilen AUC değerleri, tüm sınıflar için oldukça yüksektir. Özellikle Sınıf 0 (Normal durum), Sınıf 2 (TCP SYN flood) ve Sınıf 3 (Komut enjeksiyonu) için AUC değerleri 0,99 seviyesindedir ve bu durum, modelin bu sınıfları ayırt etme konusunda üstün sınıflandırma yeteneğine sahip olduğunu göstermektedir. Sınıf 1 (ARP spoofing) için AUC değeri ise 0,9190 olup, bu da mükemmel yakın bir ayırım gücü sergilediğini göstermektedir. Genel olarak tüm sınıflar için modelin sınıflar arası ayırımı başarıyla gerçekleştirdiği değerlendirilmektedir.



Şekil 4.28. KNN-NB-DT hibrit modeli her sınıf için ROC eğrileri



5. SONUÇLAR VE ÖNERİLER

Bu bölümde, önerilen makine öğrenmesi modellerine ait analiz sonuçları detaylı olarak incelenmektedir. Modellerin performansları; doğruluk, kesinlik, duyarlılık, özgüllük, F1 skoru, ROC AUC, tahmin süreleri gibi ölçütler çerçevesinde değerlendirilmiş ve modellerin sınıflandırma başarıları karşılaştırmalı olarak analiz edilmiştir.

5.1. Deneysel Sonuçlar

Çalışmada, KNN, NB, DT ve LR gibi temel makine öğrenmesi algoritmalarının yanı sıra, bu modellerin birleşimiyle oluşturulan üç farklı hibrit yapı (KNN-NB, DT-LR, KNN-NB-DT) ile sınıflandırma analizleri gerçekleştirilmiştir. Her bir modelin ayrı ayrı performansı değerlendirilmiş ve ardından hibrit yapıların saldırı tespitinde sağladığı katkı analiz edilmiştir. Söz konusu analizler sırasında, sistemin çalışması için oluşturulan proses sürekli modda çalışırken siber saldırı testleri gerçekleştirilmiştir. Bu sayede hem bireysel modellerin hem de bütünleşik yapıların başarımları düzeyleri kapsamlı şekilde incelenmiştir. Elde edilen analiz sonuçları Çizelge 5.1’de sunulmuştur.

Çizelge 5.1. Sınıflandırma modelleri performans karşılaştırma tablosu (ortalama)

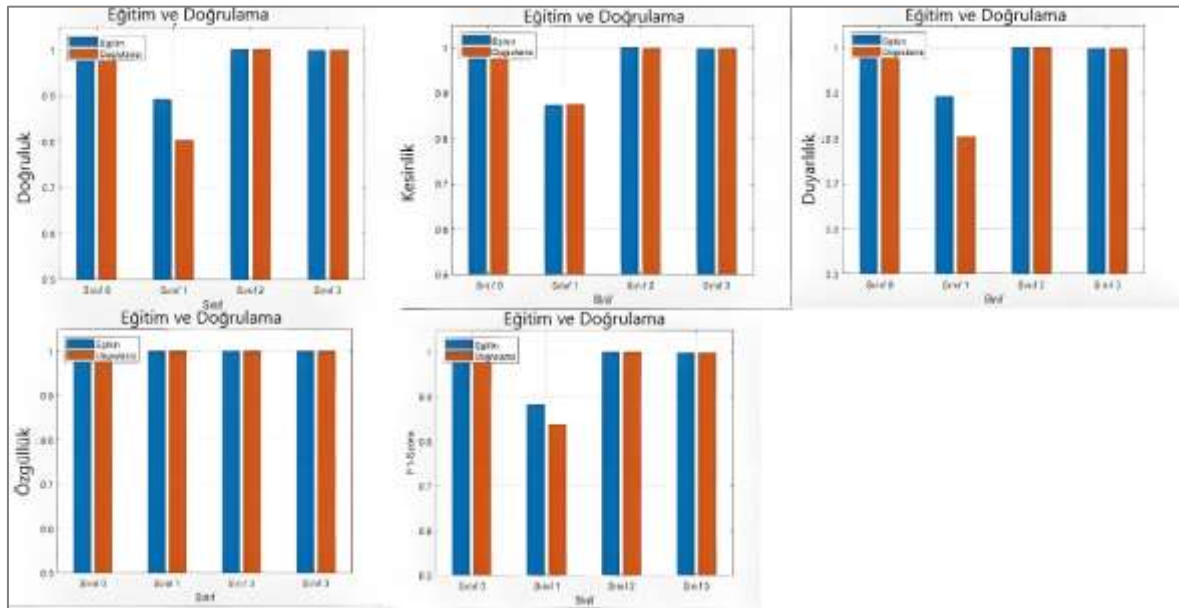
Model	Doğruluk (%)	Kesinlik	Duyarlılık	F1 Skoru	Özgüllük	AUC	Tahmin Süreleri (ms)
KNN	97,53	0,97184	0,97531	0,97356	0,99972	0,98752	2589,44
NB	92,96	0,73932	0,92955	0,75358	0,97774	0,97585	8,20482
DT	96,69	0,94804	0,96687	0,957	0,99959	0,9917	8,53197
LR	94,34	0,9197	0,94337	0,92993	0,99164	0,9675	22,3577
KNN-NB hibrit	75,22	0,74691	0,75218	0,74761	0,99183	0,87198	101481,1
DT-LR hibrit	98,29	0,94832	0,98289	0,96417	0,99962	0,99823	11,6990
KNN-NB-DT hibrit	95,87	0,95541	0,95869	0,95703	0,9995	0,9791	132235,1

Çizelge 5.1’de, kullanılan temel ve hibrit sınıflandırma modelleri farklı performans metrikleri açısından değerlendirilmiş; doğruluk (accuracy), kesinlik, duyarlılık, özgüllük, F1 skoru, ROC-AUC değerleri ve tahmin süreleri üzerinden kapsamlı bir karşılaştırma yapılmıştır. Bu değerlendirmede, özellikle Karar Ağacı ile Lojistik Regresyon (DT-LR) hibrit modeli, genel olarak en yüksek başarıyı gösteren model olmuştur. Bu model, %98,29

doğruluk oranı ile tüm modeller arasında en yüksek başarıyı elde etmiş; aynı zamanda %96,41 F1 skoru ve %99,8 AUC değeri ile hem dengesiz sınıf yapısında hem de çok sınıflı senaryolarda istikrarlı bir performans sergilemiştir.

Ayrıca, DT-LR modelinin yalnızca genel doğruluk açısından değil, saldırı sınıflarına özgü metriklerde de yüksek ve dengeli değerler üretmesi, bu modeli kritik altyapılarda saldırı tespiti amacıyla kullanılabilecek güvenilir bir yöntem haline getirmektedir. Bu yönüyle hem dengesiz veri setlerine karşı dayanıklılığını hem de çok yönlü etkinliğini ortaya koymuştur. Buna ek olarak, modele ait ortalama tahmin süresinin düşük olması, DT-LR hibrit yapısının sadece yüksek doğruluk değil, aynı zamanda zaman açısından da verimli bir çözüm sunduğunu göstermektedir.

Şekil 5.1’ de DT-LR modeli için eğitim ve doğrulama metriklerinin sınıf bazlı görsel analizi yer almaktadır. Eğitim ve doğrulama veri kümeleri üzerinden hesaplanan doğruluk, kesinlik, duyarlılık, özgüllük ve F1 skoru değerleri karşılaştırıldığında, her sınıf için metriklerin oldukça benzer olduğu ve doğrulama başarısının eğitim başarısını büyük oranda takip ettiği görülmektedir. Bu durum, DT-LR hibrit modelinin aşırı öğrenme (overfitting) problemi göstermediğini ve genelleme yeteneğinin yüksek olduğunu ortaya koymaktadır. Modelin etkinliği grafiksel analizlerle de doğrulanmıştır.



Şekil 5.1. DT-LR modeli için eğitim ve doğrulama metriklerinin sınıf bazlı görsel analizi

5.2. Tartışma ve Sınırlılıklar

5.2.1. Tartışma

SCADA sistemlerine yönelik siber tehditler, genellikle dış saldırılar ve iç saldırılar olmak üzere iki ana başlık altında sınıflandırılmaktadır. Dış saldırılar, genellikle internete açık sistemlere yönelik olarak dış ağlar üzerinden gerçekleştirilen siber saldırıları ifade eder.

Çalışmamızın odak noktası ise, kritik altyapılarda kullanılan SCADA sistemlerine yerel ağ üzerinden gerçekleştirilen saldırılardır. Bu tercihin temel nedeni, özellikle internete doğrudan bağlı olmayan veya dış ağlarla bağlantısı son derece kısıtlı olan kritik altyapılarda, saldırıların büyük ölçüde sistemlere fiziksel erişimi olan tehdit aktörleri üzerinden yapılan siber saldırılar (DoS, MITM ve komut enjeksiyonu gibi) ya da taşınabilir medya (örneğin USB bellekler) aracılığıyla bulaşan kötü amaçlı yazılımlar üzerinden gerçekleştirilmesidir. Bu tür senaryolara en bilinen örnekler arasında, Stuxnet, Duqu ve Flame gibi zararlı yazılımlar yer almaktadır. Bu yazılımlar, dış ağ bağlantısı olmayan sistemlere bile taşınabilir ortamlar yoluyla sızarak ciddi tahribatlara neden olmuştur [13-15].

İç saldırıların tespiti, dış saldırılara kıyasla daha zordur çünkü saldırgan çoğunlukla yetkili bir kullanıcı kılığına girmekte veya fiziksel erişim avantajı ile sistemlere zarar verebilmektedir. Bu sebeple, çalışmada özellikle yerel ağ trafiği izlenerek ve anormal davranışların tespiti üzerine yoğunlaşmıştır. Bu tür saldırıların erken tespiti, fiziksel zararların ve hizmet kesintilerinin önüne geçmek açısından kritik önem taşımaktadır. Bu bağlamda, çalışmanın katkılarından biri, dışarıdan gelen tehditlerin ötesinde, çoğu zaman göz ardı edilen ancak etkisi çok yüksek olan iç tehditlere odaklanarak kritik altyapıların gerçekçi bir tehdit modeli üzerinden analiz edilmesidir.

Bu çalışmada, PROFINET protokolü üzerinden analiz yapılmış olmakla birlikte, önerilen yaklaşımın farklı endüstriyel protokollere uygulanabilirliği de değerlendirilebilir. Her protokolün paket yapısı, güvenlik özellikleri ve veri iletim mekanizmaları farklılık göstermektedir. Bu nedenle modelin doğrudan uygulanması mümkün olmayabilir. Ancak, ilgili protokole ait uygun veri setlerinin elde edilmesiyle, benzer analiz yaklaşımları, gerekli protokol uyarlamaları ile geliştirilebilir. Ayrıca, çalışmada kritik altyapılarda, endüstriyel tesislerde uygulama alanı bulan halka topoloji tercih edilmiştir. Bu çalışmada

gerçekleştirilen saldırılar yerel ağ üzerinden uygulandığı için, kullanılan topolojiden bağımsız olarak birçok durumda başarıyla gerçekleştirilebilir. Bununla birlikte, ağ topolojisi; saldırının yayılım şekli, etkilediği düğüm sayısı ve tespit edilme süresi gibi faktörleri etkileyebilir. Bu nedenle farklı topolojilerde aynı saldırıların etkisi değişebilir.

5.2.2. Sınırlılıklar

Bu çalışma, PROFINET protokolü temel alınarak gerçekleştirilmiştir. Farklı endüstriyel protokoller için doğrudan genellenabilirliği sınırlıdır; bu protokollerde uygulanabilmesi için ayrı veri toplama ve analiz süreçleri gerekmektedir.

Ayrıca çalışmada, SCADA sistemlerine yönelik siber saldırılardan üç tür (DoS, MITM ve Komut Enjeksiyonu) ele alınmıştır. Bu saldırı türleri, PROFINET protokolü üzerinde uygulanabilir olmaları nedeniyle tercih edilmiştir. Diğer saldırı türleri kapsam dışı bırakılmıştır. Bu nedenle modelin farklı saldırı türleri üzerindeki etkinliği ayrıca değerlendirilmelidir.

5.3. Sonuç

Kritik altyapıların güvenli ve kesintisiz bir şekilde işletilebilmesi, büyük ölçüde SCADA sistemlerinin kararlı ve sürdürülebilir çalışmasına bağlıdır. Bu sistemlere yönelik gerçekleştirilen siber saldırılar, denetim ve izleme işlevlerinde aksamalara yol açarak ciddi operasyonel kesintilere ve ekonomik kayıplara neden olabilmektedir. Çalışma kapsamında gerçekleştirilen farklı saldırı senaryoları, SCADA sistemlerinin bu tür tehditlere karşı ne derece hassas olduğunu ortaya koymuştur. Önerilen tespit yöntemleri sayesinde, saldırıların erken evrede belirlenmesi mümkün olmakta ve olası sistemsel aksaklıkların önüne geçilerek altyapı güvenliğinin güçlendirilmesi hedeflenmektedir.

Bu çalışmada, SCADA sistemine benzer şekilde yapılandırılan bir test ortamı üzerinde çeşitli siber saldırı senaryoları uygulanmış; saldırı anları ile normal çalışma durumlarına ait ağ trafiği verileri sistematik biçimde kaydedilmiştir. Elde edilen veriler, gerekli ön işleme adımlarından geçirilerek analiz için uygun hale getirilmiştir. Oluşturulan veri kümesi üzerinde yedi farklı makine öğrenmesi algoritmasının performansları karşılaştırılmıştır. Yapılan değerlendirmeler sonucunda, Karar Ağacı (DT) ve Lojistik Regresyon (LR)

algoritmalarının birleşimiyle oluşturulan DT-LR hibrit modeli, %98,29 doğruluk oranı ile en yüksek başarıyı göstermiştir. Bu sonuç, önerilen yöntemin SCADA sistemlerine yönelik siber saldırıların tespitinde etkili ve güvenilir bir yaklaşım sunduğunu ortaya koymaktadır.

5.4. Öneriler

Siber güvenlik tehditlerinin endüstriyel kontrol sistemleri üzerindeki etkisi her geçen gün artmakta olup, bu nedenle SCADA sistemlerine yönelik saldırı tespit ve önleme yöntemlerinin geliştirilmesi büyük önem taşımaktadır. Bu doğrultuda yapılan bu çalışma, ileride gerçekleştirilecek araştırmalara yol gösterici niteliktedir. Gelecek çalışmalarda SCADA test ortamının daha kapsamlı ve çok protokollü hâle getirilmesi önerilmektedir. Mevcut çalışmada yalnızca Profinet protokolü kullanılmış olsa da, DNP3, Modbus TCP gibi farklı endüstriyel protokollerin ortama entegre edilmesiyle saldırı tespit sistemlerinin farklı iletişim yapılarına karşı performansı değerlendirilebilir. Ayrıca test ortamına analog sinyallerin de dahil edilmesiyle, sıcaklık, basınç ve seviye gibi sürekli değişen fiziksel büyüklükler üzerinden gerçekleştirilecek saldırı ve anomali tespitine yönelik çalışmalar daha kapsamlı biçimde yürütülebilecektir. İlerleyen çalışmalarda dijital verilerin yanında, analog veriler ile birlikte zamanlayıcılar (timer), sayıcılar (counter) gibi kontrol elemanlarının da kullanılması, saldırı tespit sistemlerinin daha kapsamlı hale gelmesini sağlayacaktır. Saldırı çeşitliliğinin artırılması da bir diğer önemli gelişim alanıdır. Bu tez kapsamında DoS, MITM ve komut enjeksiyonu saldırıları gerçekleştirilmiştir; ancak ilerleyen çalışmalarda farklı saldırı senaryolarının da eklenmesiyle daha geniş kapsamlı bir güvenlik değerlendirmesi mümkün olacaktır. Son olarak, bu çalışmada kullanılan makine öğrenmesi algoritmalarına ek olarak, derin öğrenme yaklaşımları, yapay sinir ağları ve hibrit model yapılarla tespit sistemlerinin çeşitlendirilmesi hedeflenebilir. Geliştirilecek olan daha kapsamlı test ortamına farklı protokoller, saldırı senaryoları ve tespit modelleri uygulanarak literatürdeki çalışmalardan daha yüksek performans elde edilmesi ve SCADA sistemlerinin güvenliğine özgün katkılar sunulması gelecekteki hedeflerdendir.



KAYNAKLAR

1. Von Solms, R., Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102.
2. Srinivas, J., Das, A. K., Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, 92, 178-188.
3. Sağıroğlu, Ş. (2021). *Siber güvenlik ve savunma kitap serisi – Siber güvenlik ontolojisi, tehditler ve çözümler*. (Birinci Baskı). Ankara: Nobel Akademik Yayıncılık.
4. Söğüt, E. (2023). *Scada Sistemlerine Yönelik Siber Saldırıların Tespiti İçin Yeni Bir Hibrit Makine Öğrenmesi Yöntemi*. Doktora Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.
5. Irmak, E., Erkek, İ. (2018). Endüstriyel kontrol sistemleri ve scada uygulamalarının siber güvenliği: Modbus TCP protokolü örneği. *Gazi University Journal of Science Part C: Design and Technology*, 6(1), 1-16.
6. Maglaras, L.A., Kim, K.H., Janicke, H., Ferrag, M.A., Rallis, S., Fragkou, P., Maglaras, A., Cruz, T. J. (2018). Cyber security of critical infrastructures. *ICT Express*, 4(1), 42-45.
7. Gürkaş-Aydin, Z., Gürtürk, U. (2022). *Cyber threats and critical infrastructures in the era of cyber terrorism*. The International Conference on Artificial Intelligence and Applied Mathematics in Engineering, La Rochelle, 274-287.
8. İnternet : Supervisory Control and Data Acquisition (SCADA) in Liquid Pipelines. (2005). URL: <https://www.nts.gov/safety/safety-studies/Documents/SS0502.pdf>. Son Erişim Tarihi : 22.07.2025.
9. Yohanandhan, R.V., Elevarasan, R.M., Pugazhendhi, R., Premkumar, M., Mihet-Popa, L., Terzija, V. (2022). A holistic review on Cyber-Physical Power System (CPPS) testbeds for secure and sustainable electric power grid – Part I: Background on CPPS and necessity of CPPS testbeds. *International Journal of Electrical Power & Energy Systems*, 136, 107718.
10. İnternet : An Effect-Centric Approach to Assessing the Risks of Cyber Attacks Against the Digital Instrumentation and Control Systems at Nuclear Power Plants. (2020). URL: https://cissm.umd.edu/sites/default/files/2020-02/Risks%20of%20Cyber%20Attacks_DICS%20at%20NPPs.pdf. Son Erişim Tarihi : 22.07.2025.
11. Musleh, A.S., Chen, G., Dong, Z.Y. (2019). A survey on the detection algorithms for false data injection attacks in smart grids. *IEEE Transactions on Smart Grid*, 11(3), 2218-2234.
12. Wadhawan, Y., AlMajali, A., Neuman, C. (2018). A comprehensive analysis of smart grid systems against cyber-physical attacks. *Electronics*, 7(10), 249.

13. Yohanandhan, R.V., Elavarasan, R.M., Manoharan, P., Mihet-Popa, L. (2020). Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications. *IEEE Access*, 8, 151019-151064.
14. İnternet: Stuxnet. (2017). URL: <https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/200661/Cyber-Reports-2017-04.pdf>. Son Erişim Tarihi : 22.07.2025.
15. Bencsath, B., Pek, G., Buttyan, L., Felegyhazi, M. (2012). The cousins of stuxnet: Duqu, flame, and gauss. *Future Internet*, 4(4), 971-1003.
16. Kozak, P., Klaban, I. Slajs, T. (2023). *Industroyer cyber-attacks on Ukraine's critical infrastructure*. International Conference on Military Technologies (ICMT), Brno, 1-6.
17. Söğüt, E. ve Erdem, O.A. (2020). Endüstriyel kontrol sistemlerine (SCADA) yönelik siber terör saldırı analizi. *Politeknik Dergisi*, 23(2), 557-566.
18. Dias, A.L., Sestito, G.S., Turcato, A.C., Brandao, D. (2018). *Panorama, challenges and opportunities in PROFINET protocol research*. 13th IEEE International Conference on Industry Applications (INDUSCON), Sao Paulo, 186-193.
19. Imanto, T., Adriansyah, A. (2020). *Performance analysis of PROFINET network in PLC-based automation system*. 2nd International Conference on Broadband Communications, Wireless Sensors and Powering (BCWSP), Yogyakarta, 47-52.
20. Şeker, E. (2020). Yapay zekâ tekniklerinin/uygulamalarının siber savunmada kullanımı. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 6(2), 108-115.
21. El Berkaoui, A., Bahsine, S., Oukennou, A., Nouh, F.A., Rzine, B. (2023). *Distribution network topology planning and optimization: A brief review*. E3S Web of Conferences, Fez, 469, 00054.
22. Sestito, G. S., Turcato, A. C., Dias, A.L., Rocha, M.S., Brandao, D., Torres, R. V. (2016). *Case of study of a Profinet network using ring topology*. IEEE International Symposium on Consumer Electronics (ISCE), Sao Paulo, 91-96.
23. Karaçor, M., Keleş, K. (2007). *Otomasyon sistemlerinin bileşenleri*. VI. Otomasyon Sempozyumu, Samsun.
24. Dransfeld, S. (2007). *Measurement and Supervision in Automated Production*. Thesis for the Degree of Doktor Ingenior, Norwegian University of Science and Technology Faculty of Engineering Science & Technology, Trondheim.
25. Endi, M., Elhalwagy, Y. (2010). *Three-layer PLC/SCADA system architecture in process automation and data monitoring*. The 2nd International Conference on Computer and Automation Engineering (ICCAE), Singapore, 774-779.
26. Lahti, J.P., Shamsuzzoha, A., Kankaanpää, T. (2011). *Web-based technologies in power plant automation and SCADA systems: A review and evaluation*. IEEE International Conference on Control System, Computing and Engineering, Penang, 279-284.

27. Chauhan, R.K., Dewal, M., Chauhan, K. (2010). Intelligent SCADA system. *International Journal on Power System Optimization and Control*, 2(1), 143-149.
28. İbrahim, M.H. (2022). SCADA sistemi: Şehir içi ve şehirlerarası yolların aydınlatma sisteminin kontrolü ve otomasyonu. *Çukurova Üniversitesi Mühendislik Fakültesi Dergisi*, 37(3), 653-662.
29. Söğüt, E., Erdem, O. (2020). Cyber terror attack analysis for industrial control systems (SCADA). *Journal Of Polytechnic-Politeknik Dergisi*, 23, 557-566.
30. Aydın, S.A.M.A. (2022). *Siber güvenlik ve savunma kitap serisi 6: Siber güvenlik ontolojisi, tehditler ve çözümler*. (Birinci Baskı). Ankara: Nobel Akademik Yayıncılık, 137.
31. Niemann, K.H. (2019). *IT security extensions for PROFINET*. IEEE 17th International Conference on Industrial Informatics (INDIN), Helsinki, 407-412.
32. Paul, A., Schuster, F., König, H. (2013). *Towards the protection of industrial control systems—conclusions of a vulnerability analysis of profinet IO*. International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Berlin, 160-176.
33. Yağci, M.Y. (2020). *SCADA Sistemler İçin Güvenli Model Oluşturulması*. Yüksek Lisans Tezi, İstanbul Üniversitesi-Cerrahpaşa Lisansüstü Eğitim Enstitüsü, İstanbul.
34. Yağmur, E. (2023). *SCADA Sistemlerinde Dağıtık Hizmet Disi Bırakma Saldırıların Derin Öğrenme ve Makine Öğrenmesi Yöntemleri İle Tespiti*. Yüksek Lisans Tezi, Konya Teknik Üniversitesi Lisansüstü Eğitim Enstitüsü, Konya.
35. Hatipoğlu, C., Tunacan T. (2021). Türkiye’de siber saldırı ve tespit yöntemleri: Bir literatür taraması. *Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi*, 8(1), 430-445.
36. Angin, P. (2020). Blockchain-based data security in military autonomous systems. *Avrupa Bilim ve Teknoloji Dergisi*, Özel Sayı, 362-368.
37. Süzen, A.A., Şimşek M.A., Gürfidan, R., Kayaalp, K. (2019). Endüstri 4.0’da nesnelerin kablosuz etki alanlarına yapılan saldırı metodolojisi. *Nevşehir Bilim ve Teknoloji Dergisi*, 8, 143-151.
38. Çelik, S., Çeliktas B. (2018). Güncel siber güvenlik tehditleri: Fidyeye yazılımlar. *CyberPolitik Journal*, 3(5), 105-132.
39. Mıjwıl, M.M., Sadıkoğlu E., Cengiz E., Candan H. (2022). Siber güvenlikte yapay zekânın rolü ve önemi: Bir derleme. *Veri Bilimi*, 5(2), 97-105.
40. Nader, P., Honeine P., Beausero P. (2016). *Detection of cyberattacks in a water distribution system using machine learning techniques*. Sixth International Conference on Digital Information Processing and Communications (ICDIPC), Beirut, 25-30.
41. Kalech, M. (2019). Cyber-attack detection in SCADA systems using temporal pattern recognition techniques. *Computers & Security*, 84, 225-238.

42. Lin, C.T., Wu S.L., Lee, M.L. (2017). *Cyber attack and defense on industry control systems*. IEEE Conference on Dependable and Secure Computing, Taipei, 524-526.
43. Kravchik, M., Shabtai, A. (2018). *Detecting cyber attacks in industrial control systems using convolutional neural networks*. In Proceedings of the 2018 Workshop on Cyber Physical Systems Security and Privacy, Toronto, 72-83.
44. Gao, J. (2020). Omni SCADA intrusion detection using deep learning algorithms. *IEEE Internet of Things Journal*, 8(2), 951-961.
45. Feng, C., Li, T., Chana, D. (2017). *Multi-level anomaly detection in industrial control systems via package signatures and LSTM networks*. 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Denver, 261-272.
46. Potluri, S., Henry, N.F., Diedrich, C. (2017). *Evaluation of hybrid deep learning techniques for ensuring security in networked control systems*. 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Limassol, 1-8.
47. Wang, H., Ruan, J., Wang, G., Zhou, B., Liu, Y., Fu, X., Peng, J. (2018). Deep learning-based interval state estimation of AC smart grids against sparse cyber attacks. *IEEE Transactions on Industrial Informatics*, 14(11), 4766-4778.
48. Shitharth, S. (2017). An enhanced optimization based algorithm for intrusion detection in SCADA network. *Computers & Security*, 70, 16-26.
49. Alhaidari, F.A., Al-Dahasi, E.M. (2019). *New approach to determine DDoS attack patterns on SCADA system using machine learning*. International Conference on Computer and Information Sciences (ICCIS), Sakaka, 1-6.
50. Teixeira, M.A., Salman T., Zolanvari M., Jain R., Meskin N. (2018). SCADA system testbed for cybersecurity research using machine learning approach. *Future Internet*, 10(8), 76.
51. Miciolino, E.E., Bernieri, G., Pascucci F., Setola R. (2015). *Communications network analysis in a SCADA system testbed under cyber-attacks*. 23rd Telecommunications Forum Telfor (TELFOR), Belgrade, 341-344.
52. Keliris, A., Salehghaffari, H., Cairl, B., Krishnamurthy, P., Maniatakos, M., Khorrami, F. (2016). *Machine learning-based defense against process-aware attacks on industrial control systems*. IEEE International Test Conference (ITC), Fort Worth, 1-10.
53. Hindy, H., Brosset D., Bayne, E., Seeam, A., Bellekens, X. (2018). *Improving SIEM for critical SCADA water infrastructures using machine learning*. 2nd International Workshop on Security and Privacy Requirements Engineering, Barcelona, 3-19.
54. R.B. Benisha, D.S.R.R. (2020). Detection of Intrusion using Enhanced Machine Learning Model in SCADA Wireless Network. *International Journal of Future Generation Communication and Networking*, 13(1), 85-98.

55. Perez, R.L., Adamsky F., Soua R., Engel T. (2018). *Machine learning for reliable network attack detection in SCADA systems*. 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (Trustcom/Bigdata), New York, 633-638.
56. Radoglou-Grammatikis, P., Sarigiannidis, P., Efstathopoulos, G., Karypidis, P.A., Sarigiannidis, A. (2020). *DIDEROT: An intrusion detection and prevention system for DNP3-based SCADA systems*. Proceedings of the 15th International Conference on Availability, Reliability and Security, Dublin, 1-8.
57. Basnet, M., Poudyal, S., Ali, M.H., Dasgupta, D. (2021). *Ransomware detection using deep learning in the SCADA system of electric vehicle charging station*. IEEE PES Innovative Smart Grid Technologies Conference-Latin America (ISGT Latin America), Lima, 1-5.
58. Rajesh, L., Satyanarayana, P. (2022). Evaluation of machine learning algorithms for detection of malicious traffic in scada network. *Journal of Electrical Engineering & Technology*, 17(2), 913-928.
59. Ullah, I., Mahmoud, Q.H. (2017). *A hybrid model for anomaly-based intrusion detection in SCADA networks*. IEEE International Conference on Big Data (Big Data), Boston, 2160-2167.
60. Özbilen, A. (2012). *TCP/IP Tabanlı Dağıtık Endüstriyel Denetim Sistemlerinde Güvenlik ve Çözüm Önerileri*. Doktora Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.
61. Erkek, İ. (2018). *Modbus Temelli Scada Sistemlerinin Siber Güvenliği İçin Yeni Bir Yaklaşım*. Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.
62. Yu, W., Wang, Y., Song, L. (2019). A Two Stage Intrusion Detection System For Industrial Control Networks Based On Ethernet/IP. *Electronics*, 8(12), 1545.
63. Nivethan, J., Papa, M. (2016). *A Linux-based firewall for the DNP3 protocol*. IEEE Symposium On Technologies For Homeland Security (HST), Waltham, 1-5.
64. Yang, M., Li, G. (2014). *Analysis of PROFINET IO communication protocol*. 2014 Fourth International Conference on Instrumentation and Measurement, Computer, Communication and Control, Harbin, 945-949.
65. Akpınar, K.O. (2019). *Ethercat Tabanlı Bir SCADA Sisteminde Kural ve Makine Öğrenmesine Dayalı Saldırı ve Anomali Tespiti*. Doktora Tezi, Sakarya Üniversitesi Fen Bilimleri Enstitüsü, Sakarya.
66. Güven, B., Uzun, T. (2007). *Kontrol sistemlerinde kullanılan veri haberleşmesi teknolojileri*. 1. Haberleşme Teknolojileri Ve Uygulamaları Sempozyumu, İstanbul.
67. İnternet : Vodafone. Ethernet Nedir? (2023). URL: <https://www.vodafone.com.tr/ev-internet/blog/ethernet-nedir>. Son Erişim Tarihi: 03.08.2024.

68. Saraç, E., Avcı, M. (2007). *Bir yerel alan ağı tasarımı ve simulasyonu*. III. İletişim Teknolojileri Ulusal Sempozyumu, Adana.
69. Taşkın, C. (2009). *Ağ Teknolojileri Ve Telekomünikasyon Kitabı* (4.Baskı). İstanbul: Pusula Yayınevi.
70. İnternet : Gökalp, Ö.M. (2021). Bilgisayar Ağları Ve Adli Bilişim. URL : https://www.researchgate.net/profile/Oemer-Goekalp/publication/352771729_BILGISAYAR_AGLARI_VE_ADLI_BILISIM/links/60d78ddc458515d6f8b013f8/BILGISAYAR-AGLARI-VE-ADLI-BILISIM.pdf. Son Erişim Tarihi: 22.07.2025.
71. Gangal, V. (2015). *Kablosuz Algılayıcı Ağlarda Karınca Koloni Algoritmali Rotalama İle Enerji Etkin Rotalamanın İncelenmesi*. Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsü, Trabzon.
72. İnternet: TeknologWeb. (2015). Ağ Topolojileri Nedir? URL: <https://www.teknologweb.com/ag-topolojileri-nedir>. Son Erişim Tarihi: 05.08.2024
73. Dong, C., Xiong, X., Xue, Q., Zhang, Z., Niu, K., Zhang, P. (2024). A survey on the network models applied in the industrial network optimization. *Science China Information Sciences*, 67(2), 121301.
74. Jiang, R.J. (2015). *A review of Network Topology*. 4th International Conference on Computer, Mechatronics, Control and Electronic Engineering, Hangzhou, 1167-1170.
75. Toma, C.I., Popescu M., Constantinescu M.D., Popa I.C. (2022). Application of electrical substation, ring topology versus star topology. *Ann. Univ. Craiova Electr. Eng. Ser.* 46(46), 63-68.
76. Yüksel, A. (2020). *Endüstriyel Kontrol Sistemlerine Yönelik Siber Saldırıları*. Tezsiz Yüksek Lisans Dönem Projesi, Ahmet Yesevi Üniversitesi Fen Bilimleri Enstitüsü, Türkistan.
77. Meshram, A., Karch, M., Haas, C., Beyerer, J. (2022). *Poet: A self-learning framework for profinet industrial operations behaviour*. International Conference on Testbeds and Research Infrastructures, Melbourne, 3-19.
78. Akerberg, J., Bjorkman M. (2009). *Exploring security in PROFINET IO*. 2009 33rd Annual IEEE International Computer Software and Applications Conference, Seattle, 406-412.
79. İnternet: Laboratory, I.T. National Vulnerability Database. URL: https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=profinet&search_type=all&isCpeNameSearch=false. Son Erişim Tarihi : 22.07.2025.
80. Hemanth, D.J., Yiğit, T., Kose, U., Guvenc, U. (2022). Engineering Cyber-Physical Systems and Critical Infrastructures 7. 4th International Conference on Artificial Intelligence and Applied Mathematics in Engineering: ICAIAME. Cham: Springer Nature Switzerland AG, 738.

81. Acar, S., Zoray, M. (2021). *Ortadaki adam saldırısının teknik yönden incelenmesi*. VII. Uluslararası TURKCESS Eğitim ve Sosyal Bilimler Kongresi, Girne, 278.
82. Datta, A.V.S.V., Koushik, P.V., Thanmayee, N. R., Ruby, D. (2022). A survey on man in the middle attack - ARP spoofing. *IOSR Journal of Computer Engineering*, 24(6), 9-20.
83. Kukutla, T.R. (2024). A deep dive into dns spoofing and security measures. *Next-Gen Tech Insights Magazine*.1(1), 1-6.
84. TBD Bilişim, (2018). 35. *Ulusal Bilişim Kurultayı Bildiriler Kitabı*. Ankara: Türkiye Bilişim Derneği.
85. Pingle, B., Mairaj, A., Javaid, A.Y. (2018). *Real-world man-in-the-middle (MITM) attack implementation using open source tools for instructional use*. IEEE International Conference On Electro/Information Technology (EIT), Rochester, 0192-0197.
86. Özocak, G. (2012). DDoS saldırısı ve failin cezai sorumluluğu. *Bilişim*, 28, 23.
87. Tuğal, İ., Almaz, C., Sevi, M. (2021). Üniversitelerdeki siber güvenlik sorunları ve farkındalık eğitimleri. *Bilişim Teknolojileri Dergisi*, 14(3), 229-238.
88. İnternet: Indusface. What is Command Injection? URL: <https://www.indusface.com/learning/what-is-command-injection/>. Son Erişim Tarihi: 27.03.2025
89. Njiru, N.M. (2015). *Clustering and visualizing the status of child health in Kenya: A data mining approach*. PhD Thesis, School Of Computing And Informatics, University of Nairobi, Nairobi.
90. Öztemel, E. (2003). *Yapay sinir ağları kitabı* (Birinci baskı). İstanbul: Papatya Yayıncılık.
91. Harrington, P. (2012). *Machine learning in action book*. Shelter Island: Manning Publications Company.
92. Karakaya, A. (2024). *Meme Kanseri Tahmininde Makine Öğrenmesi Algoritmaları ve Automl*. Yüksek Lisans Tezi, Pamukkale Üniversitesi Fen Bilimleri Enstitüsü, Denizli.
93. İnternet : Tan, S., Karpatne, Kumar. (2021). Data Mining Classification: Alternative Techniques. URL: https://www-users.cse.umn.edu/~kumar001/dmbook/slides/chap4_knn.pdf. Son Erişim Tarihi: 22.07.2025.
94. Ige, T., Kiekintveld, C. (2023). *Performance comparison and implementation of bayesian variants for network intrusion detection*. IEEE International Conference on Artificial Intelligence, Blockchain, and Internet of Things (AIBThings), Mount Pleasant, 1-5.
95. Singh, G., Kumar, B., Gaur, L., Tyagi, A. (2019). *Comparison between multinomial and Bernoulli naïve Bayes for text classification*. International Conference on Automation, Computational and Technology Management (ICACTM), London, 593-596.

96. Akbulut, S. (2006). *Veri Madenciliği Teknikleri İle Bir Kozmetik Markanın Ayrılan Müşteri Analizi ve Müşteri Segmentasyonu*. Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.
97. Marsland, S. (2011). *Chapman and Hall/CRC Machine Learning & Pattern Recognition Series Machine learning: an algorithmic perspective book*. (Second Edition). Boca Raton: Taylor & Francis Group, LLC.
98. Gollapudi, S. (2016). *Practical machine learning book*. Birmingham: Packt Publishing.
99. Adak, M.F., Yurtay N. (2013). Gini algoritmasını kullanarak karar ağacı oluşturmayı sağlayan bir yazılımın geliştirilmesi. *Bilişim Teknolojileri Dergisi*, 6(3), 1-6.
100. Maimon, O.Z., Rokach L. (2014). *Data mining with decision trees: theory and applications book*. (Second Edition). Singapore: World Scientific Publishing.
101. İnternet : Jain, A. (2020). Advantages and Disadvantages of Logistic Regression in Machine Learning. URL: https://medium.com/@akshayjain_757396/advantages-and-disadvantages-of-logistic-regression-in-machine-learning-a6a247e42b20. Son Erişim Tarihi: 06.04.2025.
102. Candell, R., Zimmerman, T., Stouffer K. (2015). An industrial control system cybersecurity performance testbed. *NIST Report*, Gaithersburg, 1-49.
103. İnternet : Solutions, D. Ağ (Network) Sistemleri > DIN Raya Takılabilen Endüstriyel Ethernet Switch. URL: <https://www.dacelsolutions.com/urun-detay/rs30-serisi-open-rail-gigabit-endustriyel-ethernet-switch-8-24-ports-/1408>. Son Erişim Tarihi: 08.05.2024.
104. Sestito, G.S., Turcato, A.C., Dias, A.L., Rocha, M.S., Silva, M.M., Ferrari, P., Brandao, D. (2017). A method for anomalies detection in real-time ethernet data traffic applied to PROFINET. *IEEE Transactions on Industrial Informatics*, 14(5), 2171-2180.
105. White, N., Parsons, R., Collins, G., Barnett, A. (2023). Evidence of questionable research practices in clinical prediction models. *BMC medicine*, 21(1), 339.
106. Barca, E., Guagliardi, I., Caloiero, T. (2024). A methodological approach for filling the gap in extreme daily temperature data: an application in the Calabria region (Southern Italy). *Theoretical and Applied Climatology*, 155(8), 7447-7461.
107. Emmanuel, T., Maupong, T., Mpoeleng, D., Semong T., Mphago, B., Tabona O. (2021). A survey on missing data in machine learning. *Journal of Big data*, 8(1), 140.
108. Boros, K., Kmetty, Z. (2024). Identifying missing data handling methods with text mining. *International Journal of Data Science and Analytics*, 18, 1-13.
109. Selvi, P. (2017). An analysis on removal of duplicate records using different types of data mining techniques: A survey. *International Journal of Computer Science Mobile Computing*. 6, 38-42.
110. Tamilselvi, J.J., Gifta C.B. (2011). Handling duplicate data in data warehouse for data mining. *International Journal of Computer Applications*, 15(4), 7-15.

111. İnternet : Ağaçdoğrayan, E. (2021). Missing Data Imputation ve Temel Çözümler. URL: <https://ecemagacdograyan.medium.com/missing-data-imputation-ve-temel-%C3%A7%C3%B6z%C3%BCmler-7822d6b8f653>. Son Erişim Tarihi: 01.04.2025.
112. Kwak, S.K., Kim,J.H. (2017). Statistical data preparation: management of missing values and outliers. *Korean journal of anesthesiology*, 70(4), 407.
113. Bolikulov, F., Nasimov R., Rashidov A., Akhmedov F., Young-lm, C. (2024). Effective methods of categorical data encoding for artificial intelligence algorithms. *Mathematics*, 12(16), 2553.
114. Lyu, Y., Feng,Y., Sakurai, K. (2023). A survey on feature selection techniques based on filtering methods for cyber attack detection. *Information*, 14(3), 191.
115. De Amorim, L.B., Cavalcanti, G.D., Cruz, R.M. (2023). The choice of scaling technique matters for classification performance. *Applied Soft Computing*, 133, 109924.
116. Titiz, F. (2023). *Kauçuk Bileşiklerinin Mekanik Özelliklerinin Yapay Zekâ Teknikleri İle Tahmin Edilmesi ve Karşılaştırmalı Analizi*. Yüksek Lisans Tezi, Sakarya Üniversitesi Fen Bilimleri Enstitüsü, Sakarya.
117. Keleş, M.B., Keleş, A. (2020). Makine öğrenmesi yöntemleri ile uçuş fiyatlarının tahmini. *Euroasia Journal of Mathematics, Engineering, Natural & Medical Sciences*, 7(11), 72-78.
118. Zhu, L., Spachos, P., Pensini, E., Plataniotis, K.N. (2021). Deep learning and machine vision for food processing: A survey. *Current Research in Food Science*, 4, 233-249.
119. Tuncel, F., Mumcu, B., Tanberk, S. (2021). *A chatbot for preliminary patient guidance system*. 29th Signal Processing and Communications Applications Conference (SIU), İstanbul, 1-4.
120. Aytekin, Ç., Sütcü, C.S., Özfidan, U. (2018). Karar ağacı algoritması ile metin sınıflandırma: müşteri yorumları örneği. *Journal of International Social Research*, 11(55), 782-792.
121. Bishop, C.M., Nasrabadi, N.M. (2006). *Pattern recognition and machine learning book*. (First Edition). New York: Springer, 738.
122. Ocakoğlu, G. (2006). *Lojistik Regresyon Analizi ve Yapay Sinir Ağları Tekniklerinin Sınıflama Özelliklerinin Karşılaştırılması ve Bir Uygulama*. Yüksek Lisans Tezi, Bursa Uludağ Üniversitesi Sağlık Bilimleri Enstitüsü, Bursa.
123. Ahuja, R., Sharma, S.C., (2021). Stacking and voting ensemble methods fusion to evaluate instructor performance in higher education. *International Journal of Information Technology*, 13, 1721-1731.





Gazili olmak ayrıcalıktır