

**T.C.
BİNGÖL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**

**YENİLENEBİLİR ENERJİ TABANLI İoT-ENTGRE SCADA
SİSTEMLERİNDE VOLÜMETRİK
SİBER SALDIRILARIN DERİN ÖĞRENME İLE TESPİTİ**

YÜKSEK LİSANS TEZİ

SÜMEYYA BULUT

YENİLENEBİLİR ENERJİ SİSTEMLERİ ANABİLİM DALI

**TEZ DANIŞMANI
Dr. Öğr. Üyesi Onur POLAT**

BİNGÖL-2026

**YENİLENEBİLİR ENERJİ TABANLI İoT-ENTGRE SCADA SİSTEMLERİNDE
VOLÜMETRİK SİBER SALDIRILARIN DERİN ÖĞRENME İLE TESPİTİ**

Dr. Öğr. Üyesi Onur POLAT danışmanlığında, Sümeyya BULUT tarafından hazırlanan bu çalışma 31/07/2026 tarihinde aşağıdaki jüri tarafından Yenilenebilir Enerji Sistemleri Anabilim Dalı'nda Yüksek Lisans Tezi olarak **oybirliği** ile kabul edilmiştir.

Başkan	: Doç. Dr. Muzaffer ASLAN	İmza	:
Üye	: Dr. Öğr. Üyesi Ferdi DOĞAN	İmza	:
Üye	: Dr. Öğr. Üyesi Onur POLAT	İmza	:

Yukarıdaki sonuç;

Enstitü Yönetim Kurulunun// tarih ve/
nolu kararı ile onaylanmıştır.

Doç. Dr. Murat DENER
Enstitü Müdürü

ÖNSÖZ

Bu tez çalışması, kritik altyapı sistemlerinin temelini oluşturan SCADA ağlarının artan siber tehditlere karşı korunması ihtiyacından yola çıkılarak hazırlanmıştır. Çalışmada, SCADA sistemlerine özgü gerçekçi bir saldırı veri seti oluşturulması ve bu veri seti üzerinde etkili bir derin öğrenme tabanlı saldırı tespit yaklaşımının geliştirilmesi amaçlanmıştır.

Araştırma sürecinde, özellikle SCADA'ya özgü kapsamlı ve kamuya açık veri setlerinin sınırlı olması ile dengesiz sınıf dağılımlarının model eğitimi üzerindeki olumsuz etkileri, çalışmanın temel zorluklarını oluşturmuştur.

Buna karşın, tamamen izole bir sanal laboratuvar ortamının kurulabilmesi ve farklı saldırı senaryolarının kontrollü bir biçimde üretilmesi, çalışmanın deneysel güvenilirliğini önemli ölçüde desteklemiştir.

Tez çalışmam boyunca bilgi birikimi, rehberliği ve desteğiyle beni yönlendiren değerli danışmanım Dr. Öğr. Üyesi Onur POLAT'a en içten teşekkürlerimi sunarım.

Tez savunma jürisinde yer alarak çalışmama katkıda bulunan değerli jüri üyelerine, lisansüstü eğitimim süresince emeği geçen Bingöl Üniversitesi Fen Bilimleri Enstitüsü'nün akademik ve idari personeline teşekkür ederim.

Bu zorlu ve yoğun süreç boyunca sevgisi, sabrı ve desteğiyle her zaman yanımda olan değerli eşim Abdulsamet Bulut'a; hayatıma anlam katan, varlıklarıyla bana ilham ve güç veren canım kızlarım Eylül Ayza Bulut ve Asya Bulut'a sonsuz teşekkür ederim. Ayrıca bu süreçte bana inanan, sabır gösteren ve desteğini hiçbir zaman esirgemeyen aileme minnettarlığımı sunarım.

Sümeyya BULUT

Bingöl, 2026

İÇİNDEKİLER

ÖNSÖZ	i
İÇİNDEKİLER	ii
SİMGELER VE KISALTMALAR LİSTESİ.....	iv
ŞEKİLLER LİSTESİ	viii
TABLolar LİSTESİ	ix
ÖZET.....	x
ABSTRACT.....	xi
1. GİRİŞ	1
1.1. Siber Güvenlikte Kritik Altyapı Sistemlerinin Önemi	1
1.2. SCADA Sistemlerini Hedef Alan Siber Tehditler	2
1.3. Kritik Sistemlerde Saldırı Tespitinde Karşılaşılan Zorluklar	3
1.4. Bu Çalışmanın Amaçları ve Katkıları	5
1.5. Tez Çalışmasının Yapısı	7
2. KAYNAK ÖZETLERİ.....	8
2.1. SCADA ve Endüstriyel Kontrol Sistemlerini Hedef Alan Siber Saldırıları.....	8
2.2. Geleneksel SCADA Saldırı Tespit Yöntemleri	9
2.3. Makine Öğrenimi Tabanlı SCADA Saldırı Tespiti.....	10
2.4. Derin Öğrenme Tabanlı SCADA Güvenlik Çözümleri.....	11
2.5. Hibrit ve Çok Ölçekli Mimari Yaklaşımlar	13
2.6. Mevcut Çalışmaların Sınırlılıkları ve Araştırma Açığı	14
3. MATERYAL VE YÖNTEM.....	16
3.1. Veri Ön İşleme.....	16
3.2. Önerilen Model Mimarisi.....	16
3.3. Eğitim Stratejisi.....	24
4. BULGULAR VE TARTIŞMA.....	26
4.1. Deney Düzeni ve SCADANet Veri Setinin Toplanması	26
4.2. Trafik Oluşturma ve İletişim Akışları	30
4.3. Trafik Yakalama ve Özelliklerin Çıkarılması.....	30

4.4. Etiketleme Süreci	31
4.5. Trafik Oluşturma ve Saldırı Senaryosu Tasarımı	31
4.6. Önerilen Mimarının SCADA Odaklı Tasarımı.....	34
4.7. Karşılaştırma için Kullanılan İkinci Veri Kümesi (WUSTL-IIoT-2021)	35
4.8. Dengesiz Veri Sorununun Ele Alınması	36
4.9. Değerlendirme Ölçütleri.....	37
4.10. SCADANet Veri Kümesinde Elde Edilen Sonuçlar.....	37
4.11. WUSTL-IIoT-2021 Veri Seti Üzerinde Elde Edilen Sonuçlar	40
4.12. Ablasyon Çalışması	42
4.13. Hesaplama Karmaşıklığı ve Uygulama Olanakları	44
4.14. Karar Analizi Modeli.....	46
4.15. Gerçek Zamanlı Uygulanabilirlik	47
5. LİTERATÜRDEKİ GÜNCEL ÇALIŞMALARLA KARŞILAŞTIRMA.....	49
6. SONUÇLAR VE ÖNERİLER	52
KAYNAKLAR.....	54

SİMGELER VE KISALTMALAR LİSTESİ

ACK	: Acknowledge – TCP onay bayrağı
AE	: Autoencoder – Otomatik Kodlayıcı
AI	: Artificial Intelligence – Yapay Zekâ
APT	: Advanced Persistent Threat – Gelişmiş Kalıcı Tehdit
ARP	: Address Resolution Protocol – Adres Çözümleme Protokolü
AUC	: Area Under the Curve – Eğri Altında Kalan Alan
BN	: Batch Normalization – Toplu Normalleştirme
BPTT	: Backpropagation Through Time – Zaman İçinde Geri Yayılım
BT	: Bilgi Teknolojisi (Information Technology, IT)
CAE	: Convolutional Autoencoder – Evrişimli Otomatik Kodlayıcı
CEC	: Constant Error Carousel – Sabit Hata Karuseli
CNN	: Convolutional Neural Network – Evrişimli Sinir Ağı
Conv1D	: One-Dimensional Convolution – Tek Boyutlu Evrişim
ConvLSTM	: Convolutional LSTM – Evrişimli LSTM
CSV	: Comma-Separated Values – Virgülle Ayrılmış Değerler
CUDA	: Compute Unified Device Architecture
DCNN	: Deep Convolutional Neural Network – Derin Evrişimli Sinir Ağı
DDoS	: Distributed Denial of Service – Dağıtık Hizmet Reddi
DeepFM	: Deep Factorization Machine – Faktörizasyon Makinesi + Derin Yapay Sinir Ağı
DL	: Deep Learning – Derin Öğrenme

DNP3	: Distributed Network Protocol v3.0
DoS	: Denial of Service – Hizmet Reddi (Hizmet Engelleme)
DT	: Decision Tree – Karar Ağacı
F1	: F1 Score – F1 Skoru
FDI	: False Data Injection – Yanlış Veri Enjeksiyonu
FN	: False Negative – Yanlış Negatif
FP	: False Positive – Yanlış Pozitif
FP16	: 16-bit Floating Point – Yarı Hassasiyetli Kayan Nokta
FP32	: 32-bit Floating Point – Tek Hassasiyetli Kayan Nokta
GAN	: Generative Adversarial Network – Çekişmeli Üretici Ağ
GAP	: Global Average Pooling – Küresel Ortalama Havuzlama
GAT(GAT-AD)	: Graph Attention Network – Grafik Dikkat Ağı (Tabanlı Anomali Tespiti)
GPU	: Graphics Processing Unit – Grafik İşlem Birimi
GRU	: Gated Recurrent Unit – Geçitli Tekrarlayan Birim
HMI	: Human-Machine Interface – İnsan-Makine Arayüzü
HTTP	: HyperText Transfer Protocol
ICMP	: Internet Control Message Protocol
ICS	: Industrial Control Systems – Endüstriyel Kontrol Sistemleri
IDS	: Intrusion Detection System – Saldırı Tespit Sistemi
IIoT	: Industrial Internet of Things – Endüstriyel Nesnelerin İnterneti
IoT	: Internet of Things – Nesnelerin İnterneti
IP	: Internet Protocol – İnternet Protokolü
JA4 / JA4+ / JA4S / JA4X	: Ağ trafiği parmak izi (fingerprinting) yöntemleri
k-NN	: k-Nearest Neighbors – k-En Yakın Komşu
LSTM	: Long Short-Term Memory – Uzun Kısa Vadeli Bellek
MB	: Megabyte – Megabayt

MiTM	: Man-in-the-Middle – Ortadaki Adam Saldırısı
ML	: Machine Learning – Makine Öğrenmesi
NAT	: Network Address Translation – Ağ Adresi Çevirisi
OPC	: Open Platform Communications
OS	: Operating System – İşletim Sistemi (OS Scan)
OT	: Operational Technology – Operasyonel Teknoloji
PCA	: Principal Component Analysis – Temel Bileşen Analizi
PLC	: Programmable Logic Controller – Programlanabilir Mantık Denetleyicisi
ReLU	: Rectified Linear Unit – Düzeltilmiş Doğrusal Birim
RF	: Random Forest – Rastgele Orman
RNN	: Recurrent Neural Network – Tekrarlayan Sinir Ağı
SCADA	: Supervisory Control and Data Acquisition – Denetleyici Kontrol ve Veri Toplama
SE	: Squeeze-and-Excitation
SHAP	: SHapley Additive exPlanations
SIEM	: Security Information and Event Management – Güvenlik Bilgi ve Olay Yönetimi
SIS	: Safety Instrumented System – Güvenlik Enstrümanlı Sistem
SQL	: Structured Query Language (SQL Enjeksiyonu bağlamında)
SVDD	: Support Vector Data Description
SVM	: Support Vector Machine – Destek Vektör Makinesi
SYN	: Synchronize – TCP senkronizasyon bayrağı
TCP	: Transmission Control Protocol
TN	: True Negative – Doğru Negatif
TP	: True Positive – Doğru Pozitif
UDP	: User Datagram Protocol

VAE	: Variational Autoencoder – Varyasyonel Otomatik Kodlayıcı
VM	: Virtual Machine – Sanal Makine
XGBoost	: Extreme Gradient Boosting

ŞEKİLLER LİSTESİ

Şekil 1.1. Scada Sistem Mimarisi	2
Şekil 3.1. Önerilen Hibrit Mimari Yapısı	17
Şekil 3.2. LSTM mimarisi (Heddam vd., 2022)	22
Şekil 4.1. Veri setini elde etmek için oluşturulan sanallaştırılmış SCADA mimarisinin genel tasarımı	29
Şekil 4.2. SCADANet Veri Kümesi için 5 Katlı Birleşik Karmaşıklık Matrisi	39
Şekil 4.3. WUSTL-IIoT-2021 Veri Kümesi için 5 Katlı Birleşik Karmaşıklık Matrisi	41

TABLÖLER LİSTESİ

Tablo 2.1. SCADA ve ICS sistemlerine yönelik bazı saldırılar ve etkileri	8
Tablo 2.2. Çeşitli makine öğrenme yöntemleri ve özellik seçimleri kullanılarak yapılan çalışmalar	11
Tablo 2.3. SCADA tabanlı sistemlerde saldırı tespiti için kullanılan derin öğrenme tabanlı modellerin karşılaştırılması	12
Tablo 2.4. SCADA tabanlı sistemlerde saldırı tespiti için hibrit modellerin karşılaştırılması	13
Tablo 4.1. SCADANET veri setinin sınıf dağılımı	28
Tablo 4.2. Veri kümesini elde etmek için oluşturulan deneysel sanal laboratuvar yapısında kullanılan sanal makineler	29
Tablo 4.3. SCADANet Veri Kümesi için 5 Katlı Ortalama Performans Sonuçları.....	38
Tablo 4.4. WUSTL-IIoT-2021 Veri Kümesi için 5 Katlı Ortalama Performans Sonuçları	40
Tablo 4.5. Ablasyon çalışması sonuçları	42
Tablo 5.1. SCADA ve endüstriyel nesnelerin interneti veri kümeleri üzerinde son dönem siber saldırı tespit çalışmalarının performans karşılaştırması	51

YENİLENEBİLİR ENERJİ TABANLI İoT-ENTGRE SCADA SİSTEMLERİNDE VOLUMETRİK SİBER SALDIRILARIN DERİN ÖĞRENME İLE TESPİTİ

ÖZET

Kritik altyapı sistemlerinde kullanılan Denetleyici Kontrol ve Veri Toplama (Supervisory Control and Data Acquisition-SCADA) sistemlerine dayalı endüstriyel kontrol ağları, artan siber tehditler karşısında güvenilir, ölçeklenebilir ve genelleştirilebilir saldırı tespit mekanizmalarına ihtiyaç duymaktadır. Bununla birlikte, literatürde yaygın olarak kullanılan veri setlerinin büyük bir kısmı genel amaçlı ağ trafiğine dayanmakta ve Modbus/TCP gibi endüstriyel protokollerin döngüsel, deterministik ve süreç odaklı iletişim yapısını yeterince yansıtmamaktadır. Bu tez çalışmasında, söz konusu sınırlamayı gidermek amacıyla tamamen izole edilmiş bir sanal SCADA ortamı tasarlanmış ve SCADANet adı verilen, SCADA'ya özgü çok sınıflı bir saldırı veri seti oluşturulmuştur. Bu veri seti, meşru ağ trafiği ile birlikte üretilen 13 farklı saldırı senaryosunu içermektedir. Bu kapsamda, dönüştürülmüş trafik temsillerini analiz etmek amacıyla paralel genişletilmiş Evrişimli Sinir Ağı (Convolutional Neural Network-CNN) yapıları, Residual-SE blokları ve Uzun Kısa Vadeli Bellek (Long Short-Term Memory-LSTM) katmanlarından oluşan hibrit bir derin öğrenme mimarisi önerilmiştir. Önerilen mimari, çok ölçekli uzamsal örüntüleri etkili bir şekilde öğrenirken özellik düzeyindeki sıralı ve bağlamsal ilişkileri de modelleyerek ağ trafiğinin daha kapsamlı bir şekilde temsil edilmesini sağlamaktadır. Önerilen yaklaşımın genelleştirilebilirliğini değerlendirmek amacıyla geliştirilen model, hem SCADANet veri seti hem de literatürde yaygın olarak kullanılan WUSTL-IIoT-2021 veri seti üzerinde test edilmiştir. Deney sonuçları, önerilen mimarinin her iki veri setinde de yüksek doğruluk ve Makro F1 skoru elde ettiğini ve özellikle azınlık saldırı sınıflarında duyarlılığı önemli ölçüde artırdığını göstermektedir. Ayrıca, gerçekleştirilen ablasyon çalışması, mimaride yer alan her bir bileşenin genel performansa anlamlı ve birbirini tamamlayıcı katkılar sağladığını ortaya koymaktadır. Bulgular, önerilen derin öğrenme tabanlı yaklaşımın SCADA sistemlerine özgü trafik özelliklerini etkili bir şekilde modelleyebildiğini ve farklı veri kaynakları arasında istikrarlı bir saldırı tespit performansı sergilediğini göstermektedir. Bu bağlamda çalışma, SCADA tabanlı kritik altyapıların siber güvenliğinde saldırı tespitine yönelik literatüre önemli metodolojik ve deneysel katkılar sunmaktadır.

Anahtar Kelimeler: SCADA Güvenliği, Kritik Altyapı Sistemleri, Hibrit Derin Öğrenme, Siber Saldırı Tespiti.

DETECTION OF VOLUMETRIC CYBERATTACKS USING DEEP LEARNING IN RENEWABLE ENERGY-BASED IoT-INTEGRATED SCADA SYSTEMS

ABSTRACT

Industrial control networks based on Supervisory Control and Data Acquisition (SCADA) systems used in critical infrastructure require reliable, scalable, and generalizable intrusion detection mechanisms in the face of increasing cyber threats. However, a large proportion of the datasets commonly used in the literature are based on general-purpose network traffic and do not adequately reflect the cyclic, deterministic, and process-oriented communication characteristics of industrial protocols such as Modbus/TCP. In this thesis, a fully isolated virtual SCADA environment was designed to address this limitation, and a SCADA-specific multiclass attack dataset, named SCADANet, was developed. The dataset contains 13 distinct attack scenarios generated alongside legitimate network traffic. In this context, a hybrid deep learning architecture consisting of parallel extended Convolutional Neural Network (CNN) structures, Residual-SE blocks, and Long Short-Term Memory (LSTM) layers was proposed to analyze transformed traffic representations. The proposed architecture effectively learns multi-scale spatial patterns while also modeling feature-level sequential and contextual relationships, thereby enabling a more comprehensive representation of network traffic. To evaluate the generalizability of the proposed approach, the developed model was tested on both the SCADANet dataset and the widely used WUSTL-IIoT-2021 dataset. The experimental results demonstrate that the proposed architecture achieves high accuracy and Macro F1 scores on both datasets and significantly improves sensitivity, particularly for minority attack classes. Furthermore, the conducted ablation study demonstrates that each component of the architecture makes a meaningful and complementary contribution to the overall performance. The findings indicate that the proposed deep learning-based approach can effectively model SCADA-specific traffic characteristics and maintain consistent intrusion detection performance across different data sources. In this regard, the study provides significant methodological and experimental contributions to the literature on intrusion detection in the cybersecurity of SCADA-based critical infrastructure systems.

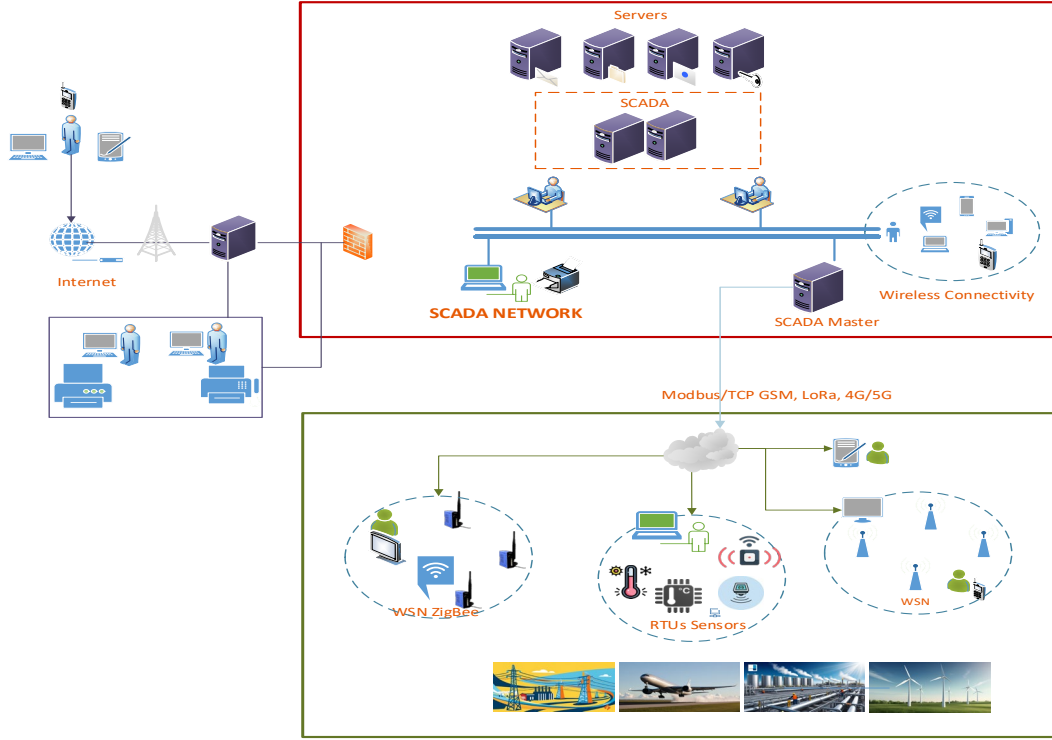
Keywords: SCADA Security; Critical Infrastructure Systems; Hybrid Deep Learning; Cyber Attack Detection.

1. GİRİŞ

1.1. Siber Güvenlikte Kritik Altyapı Sistemlerinin Önemi

Enerji, sağlık, ulaşım ve finansal hizmetler gibi kritik altyapıya sahip sistemler, yaşamın doğal akışı için hayati öneme sahiptir (bkz. Şekil 1.1). Bu tür sistemlerin büyük bir kısmı, Denetleyici Kontrol ve Veri Toplama (Supervisory Control and Data Acquisition-SCADA) ve Endüstriyel Kontrol Sistemleri (Industrial Control Systems-ICS) teknolojileri kullanılarak yönetilmektedir (Alsabbagh vd., 2023; Birnbaum vd., 2020). SCADA sistemleri, sürekli olarak operasyonel veriler üreten birbirine bağlı endüstriyel cihazlardan oluşur. Sistemleri uzaktan yönetme yeteneği, sistem içinde doğal bir siber güvenlik gereksinimi yaratır. Kritik altyapı tarafından sağlanan hizmetlerin sürekliliğini sağlamak için, sistemin dış saldırılara karşı korunması gerekir (Do vd., 2017; Paulraj vd., 2025).

Sistemdeki bir güvenlik açığı, yalnızca sistemde bir arızaya neden olmakla kalmaz. Sisteme bağlı dış faktörler de zarar görebilir (Do vd., 2017). Bu tehditlerin başında Hizmet Engelleme (DoS) saldırıları ve Gelişmiş Kalıcı Tehditler (APT) gelmektedir. Bu saldırılar oldukça sık meydana gelir ve sistemin çalışmasını yavaşlatır veya engeller (Jahan Simu ve Zaman, 2023; Lehto, 2022).



Şekil 1.1. Scada Sistem Mimarisi

1.2. SCADA Sistemlerini Hedef Alan Siber Tehditler

SCADA ve IDS sistemlerini içeren kritik altyapılar için siber güvenlik son derece önemlidir. Bu altyapıya yönelik saldırıları tespit etmek, geleneksel ortamlardaki saldırıları tespit etmekten daha karmaşık ve zordur (Le vd., 2025). Endüstriyel sistemler, Modbus/TCP, şifreleme, kimlik doğrulama ve bütünlük kontrolleri gibi yerleşik güvenlik özelliklerinden yoksundur. Bu durum, söz konusu sistemleri çeşitli saldırılara karşı savunmasız hale getirir (Mohammed vd., 2022).

Flood saldırıları, yanlış komut enjeksiyonu ve DoS saldırıları gibi gelişmiş saldırı teknikleri, SCADA gibi endüstriyel sistemler için ciddi tehditler oluşturur. Flood saldırılarında saldırganlar, denetleyicinin komutları yorumlamasını engellemek veya güvenli olmayan senaryolara neden olmak için Modbus/TCP paketlerini bozarlar (Mohammed vd., 2022). Yanlış komut enjeksiyon saldırılarında ise saldırganlar, SCADA operatörünün tekrarlayan yanıtlarının arkasına saklanarak komut enjekte etmeye çalışır. Bu durum, önemli hasara yol açabilir. Geleneksel DoS saldırıları sistemdeki hizmeti kesintiye uğratmaya odaklanırken, protokole özgü DoS saldırıları iletişimi kesintiye uğratmak

amacıyla Modbus/TCP protokollerindeki güvenlik açıklarına odaklanır (H. Zhang vd., 2022).

1.3. Kritik Sistemlerde Saldırı Tespitinde Karşılaşılan Zorluklar

SCADA tabanlı sistemlerde saldırı ve anomali tespiti, gerçek zamanlı operasyonel gereklilikler, yanlış pozitiflere karşı düşük tolerans ve dengesiz trafik dağılımları nedeniyle hâlâ kritik bir sorun teşkil etmektedir. Ayrıca, endüstriyel ağ trafiğinin çok boyutlu ve heterojen yapısı, meşru iletişim akışlarının içine gizlenmiş saldırılarla birleştiğinde, gerçekçi operasyonel koşullar altında saldırıları güvenilir bir şekilde tespit etmeyi zorlaştırmaktadır (Soumya R vd., 2026; Nader vd., 2013; Sayghe, 2025; Zhu ve Sastry, 2012).

Sistemlere yönelik bu tür saldırılara karşı çeşitli tespit ve önleme stratejileri mevcuttur. Bunlara örnek olarak anomali tespit sistemleri, Saldırı Tespit Sistemleri (IDS) ve kriptografik sistemler verilebilir. Modbus/TCP işlemlerini izleyen yaklaşımlar, anomali tespiti kapsamında anormal trafiği tespit edebilir. Ayrıca DoS ve komut enjeksiyon saldırılarına da hızlı bir şekilde müdahale edebilirler (Kim ve Kang, 2018). Kriptografik sistemler, ASCON gibi şifreleme algoritmaları kullanarak Modbus/TCP iletişimlerinin uçtan uca gizlilikle gönderilmesini sağlayabilir. Öte yandan, IDS sistemleri anomali algılama tabanlı bir yaklaşım benimsemektedir (Le vd., 2025; Radoglou-Grammatikis vd., 2020). İmza tabanlı tehditlerin tespit edilebilmesi için imza tabanlı tanımlayıcılar gereklidir. Tehditleri tespit etmek için önceden tanımlanmış imzalar gereklidir. Daha önce karşılaşılmış ve belgelenmiş saldırılar tespit edilebilir. Bu saldırılar, sistemin sıfıncı gün saldırıları ve mevcut imzalarla eşleşmeyen yeni saldırı türlerine karşı etkisiz kaldığını göstermektedir. İmza tabanlı koruma, sistemin sürekli güncellenmesini gerektirir. Bu durum, gecikmeli güncelleme süreçlerinde bir güvenlik açığı yaratır ve bu tür saldırılara karşı sınırlı bir koruma sağlar (Mehrotra ve Saxena, 2018). Saldırganlar, bu bilinen saldırıları modelleyerek, sistemi etkisiz hale getirmek için küçük değişiklikler yaparak bunları atlatır (Doğan vd., 2025).

Kural tabanlı sistemler, önceden tanımlanmış kurallara göre hareket eder ve tehditlere karşı bir yaklaşım sunar. Bu, karmaşık ve gelişmiş saldırılara karşı savunmasız bir sistem yaratır.

Ayrıca, ağlar her geçen gün genişlemektedir. Bu durum, ağın ölçeklenebilirliğinde ve performansında bir düşüşe neden olmaktadır (Bajwa vd., 2025).

İstatistiksel yöntemlerde temel bir ağ davranışı söz konusudur. Ağ iyi tanımlanmış olsa bile, gelişen tehditler karşısında zorluk çeker. İstatistiksel yöntemler, gelişen tehditlere karşı genellikle düşük performans gösterir. Sonuç olarak, ağ trafiğindeki normal davranışları yanlış yorumlayabilir. Yanlış pozitif oranı artar ve yanlış negatiflere neden olabilir (Sharma ve Arora, 2025). İstatistiksel yaklaşımlar, zararsız ve kötü niyetli ağ trafiğini ayırt etmede bağlamsal anlayıştan yoksundur. Bu nedenle, yanlış sınıflandırma olasılığı daha yüksektir (Razaque vd., 2025).

Siber güvenlik sistemlerinde tehdit tespiti ve saldırı tanımlamasında kullanılan geleneksel yöntemler, artan karmaşıklık karşısında yetersiz kalmaktadır. Saldırıları tespit etmek için daha etkili yolların aranması, derin öğrenme ve yapay sinir ağı tabanlı yaklaşımlara odaklanan ve başarı gösteren çalışmalara yol açmıştır. Evrişimli Sinir Ağları (CNN), Tekrarlayan Sinir Ağları (RNN), Uzun Kısa Süreli Bellek (LSTM) ağları ve hibrit derin öğrenme (DL) modelleri, ortaya çıkan tehditlere karşı daha dayanıklı yaklaşımlar sergilemektedir. Bu modellerin uyarlanabilirliği, yüksek doğruluğu ve çeşitli veri türlerini işleme yeteneği, siber güvenlik alanına önemli katkılar sağlamaktadır. Siber güvenlik tehditlerine karşı, veri paketlerindeki kalıplar CNN mimarileri kullanılarak tespit edilebilir. Bu, ağ trafiğine uyarlanabilen bir tespit sistemi çerçevesinin oluşturulmasını sağlamıştır (Cui vd., 2018). CNN'lerin, verilerin uzamsal yapısından yararlanarak ağ trafiği modellemesini etkili bir şekilde analiz ettiği belirtilmektedir (Elsayed vd., 2024).

RNN ve LSTM gibi yöntemler, diziler halinde düzenlenmiş verileri analiz etmede oldukça etkilidir. Bunlar, ağ trafiği için yetkisiz erişim tespit sistemlerinde saldırıları tespit etmek için ideal yöntemlerdir (Al-Shurbaji vd., 2025; Kimanzi vd., 2024). Ayrıca, LSTM'lerin siber tehditleri tespit etmede iyi performans gösterdiği ve bazı durumlarda CNN'lerden daha üstün olduğu da gösterilmiştir (Markkandeyan vd., 2025; Sangeetha vd., 2024). CNN ve LSTM'lerin güçlü yönlerinin birleştirilmesi, yüksek doğruluk sağlar. Bunlar, uzamsal ve zamansal verileri işleyerek tehditleri tespit etmede daha etkilidir (Alguliyev ve Shikhaliyev, 2024).

1.4. Bu Çalışmanın Amaçları ve Katkıları

SCADA ve Saldırı Tespit Sistemi (Intrusion Detection System-IDS) tabanlı kritik altyapıya sahip ağlarda, yanlış alarm oranı düşük gerçek zamanlı sistemlere olan ihtiyaç giderek artmaktadır. Geleneksel güvenlik sistemleri, sürekli gelişen saldırılara karşı yetersiz kalmaktadır. Saldırganların saldırılarını normal trafik akışına gizlemesi ve veri kümelerindeki sınıf dengesizliği, daha etkili yöntemler araştırılması ihtiyacını daha da artırmaktadır. Derin öğrenme gibi gelişmiş yöntemler, veri dengesizliği olan sınıflarda sadece yüksek doğruluk değil, aynı zamanda yüksek duyarlılık da sağlamaktadır. Bu nedenle, geliştirilecek yeni ve etkili derin öğrenme modelleri, bu tür sistemleri korumak için son derece değerli olacaktır. Bu çalışma, SCADA'ya özgü farklı saldırı senaryolarını gerçekçi bir şekilde temsil eden bir SCADANet veri seti önermektedir. Ayrıca, saldırılarda çok ölçekli ve zaman bağımlılıklarını iyi modelleyebilen bir hibrit derin öğrenme mimarisi önerilmiştir. Bu çalışma, literatüre katkıda bulunmayı ve önemli bir boşluğu doldurmayı amaçlamaktadır. Bu çalışmanın temel dayanağı, SCADA tabanlı altyapı için güvenilir saldırı tespiti yapabilen bir hibrit derin öğrenme mimarisine ihtiyaç duyulduğudur. Bu nedenle, çok ölçekli uzamsal desenler ve özellik düzeyinde bağlamsal ilişkiler içeren SCADA'ya özgü trafik verileriyle bir veri setini birleştiren bir hibrit model yapısına sahip olmalıdır.

Bu sorunu ele almak için, ağ trafiğine yönelik eşzamanlı siber saldırı senaryolarını içeren, tamamen izole edilmiş bir sanal ortamda SCADANet adlı SCADA'ya özgü bir veri kümesi geliştirilmiştir. Dönüştürülmüş trafik temsillerinden çok ölçekli uzamsal özellikleri ve özellik düzeyinde bağlamsal ilişkileri yakalayabilen çok ölçekli bir derin öğrenme mimarisi önerilmiştir.

Birçok çalışma, tek bir karşılaştırma ölçütüyle değerlendirilen genel amaçlı saldırı tespit veri kümelerini ve modellerini kullanmaktadır. Bu çalışma, izole bir sanal ortamda SCADA'ya özgü bir veri seti oluşturarak ve önerilen modeli hem SCADANet hem de WUSTL-IIoT-2021 veri setleri üzerinde değerlendirerek bu yaklaşımlardan ayrılmaktadır. Önerilen mimari, Parallel Dilated Conv1D, Residual-SE blokları ve LSTM katmanlarını entegre ederek çok ölçekli ve özellik düzeyinde bağlamsal trafiği temsil etmesini sağlar.

Her bir bileşenin mimariye katkısı, ablasyon analizi kullanılarak ayrıntılı olarak incelenmiştir. Bu çalışmanın katkıları şu şekilde özetlenebilir:

SCADA'ya özgü SCADANet veri seti: SCADA tabanlı bir yapıya sahip, tamamen izole bir ortam içinde bir sanal ortam oluşturulmuştur. Bu ortamda, arka plan trafiğinde bulunan Modbus/TCP ve ICMP/HTTP birlikte üretilmiştir.

Saldırı senaryosu, normal ağ trafiği akışıyla eşzamanlı olarak oluşturulmuş ve bu akışın içine yerleştirilmiştir. Veri kümesi, normal trafik verilerinin yanı sıra 13 saldırıdan (SYN/ACK/UDP/ICMP/HTTP Flood, SQLi, Port Taraması, Güvenlik Açığı Taraması, İşletim Sistemi Taraması, Modbus Yanlış Veri Enjeksiyonu, Modbus Komut Kötüye Kullanımı, APT Veri Çalma ve İçeriden Gelen Tehdit (Sabotaj)) oluşan bir veri kümesinden oluşmaktadır.

Akış zenginliği: Ağdaki ham paketler için çok katmanlı özellikler çıkarılmıştır. Ağ trafiğinde özellikle düşük hacimli saldırıları ayırt edebilen JA4+ tabanlı parmak izi özellikleri elde edilmiştir.

Yeni hibrit mimari: SCADA sisteminde kısa ve uzun menzilli özellikleri çıkarmak için Paralel genişletilmiş Conv1D kullanılmıştır. Temsil gücünü artırmak için bir Residual-SE bloğu eklenmiştir. LSTM kullanarak zaman bağımlılıklarını da öğrenen bir hibrit yöntem sunulmuştur.

Dengesiz veri sınıflarına dengeli bir yaklaşım: Veri dengesizliğine rağmen, Focal Loss ve sınıf ağırlıkları kullanılarak iki aşamalı bir optimizasyon uygulanmıştır. Bu, azınlık sınıflarda duyarlılığın artmasını sağlamıştır.

Veri kümeleri arası genelleştirilebilirlik: Önerilen hibrit yöntem, hem oluşturulan veri kümesine hem de literatürde sıklıkla kullanılan WUSTL-IIoT-2021 veri kümesine uygulanmıştır (Teixeira vd., 2021). Bu, önerilen hibrit yöntemin veri kümesine bağlı olmadığını ve güçlü genelleştirme yetenekleri sergilediğini göstermektedir.

Güçlü değerlendirme ölçütleri: Çalışmada kullanılan veri kümesindeki eğitim ve test verileri, 5 katlı çapraz doğrulama yöntemi ile doğruluk, makro/ağırlıklı kesinlik, geri çağırma ve F1 ölçütleri kullanılarak değerlendirildi. Ayrıca, hatalar karışıklık matrisleri aracılığıyla ayrıntılı olarak gösterildi.

Model ablasyon çalışması: Dilated CNN, LSTM ve Res-SE modellerinin kaldırılması durumunda elde edilen sonuçlar sunulmuş ve bu sayede hibrit modelin performansı ortaya konmuştur.

1.5. Tez Çalışmasının Yapısı

Çalışmanın bu bölümü, SCADA sistemlerine, tehditlere, literatürdeki sınırlılıklara ve bu çalışmanın katkılarına genel bir giriş sunmaktadır. Bölüm II, siber saldırı tespiti ile ilgili çalışmaları ve mevcut araştırma boşluklarını gözden geçirmektedir. Bölüm III, deneysel çalışma süreçlerini açıklamaktadır. Bu bölüm, veri ön işleme adımlarını ve önerilen derin öğrenme mimarisinin ayrıntılarını sunmaktadır. Bölüm IV, deneysel kurulum, veri seti oluşturma süreci, değerlendirme ölçütleri, sonuçlar, ablasyon analizi ve model yorumlarına bilirlilik analizini sunmaktadır. Bölüm V, önerilen yapıyı literatürdeki son çalışmalarla karşılaştırmaktadır. Bölüm VI, makaleyi sonlandırmakta ve çalışmanın sınırlılıklarını ele almaktadır. Gelecekteki araştırmalar da tartışılmaktadır.

2. KAYNAK ÖZETLERİ

2.1. SCADA ve Endüstriyel Kontrol Sistemlerini Hedef Alan Siber Saldırıları

SCADA ve IDS sistemlerine yönelik saldırılar her geçen gün artmaktadır. Bu saldırılar, söz konusu sistemlerin içindeki farklı noktaları hedef almaktadır. Her saldırı türünün kendine özgü bir hedefi vardır. Keşif saldırıları, SCADA sistemi hakkında bilgi toplar ve sistemin mimari yapısını haritalandırır. Mimari yapının zayıf noktaları, ağ araçlarıyla yapılan taramalarla tespit edilir (Morris ve Gao, 2013). Komut ve ölçüm enjeksiyon saldırılarında ise sistemi manipüle etmek amacıyla komutlar gönderilir. Bu aldatıcı komutlar sistemde istenmeyen davranışlara neden olur ve fiziksel hasara ve sistem kesintilerine yol açabilir. DoS saldırıları, sistemi gereksiz veri trafiğiyle boğar. Bu, sistemde çalışan hizmetlerin kesintiye uğramasına neden olur. Bu saldırılar, protokol zayıflıklarından yararlanarak sistemi kullanılamaz hale getirmeyi amaçlar (Yang vd., 2022). Kötü amaçlı yazılım saldırıları, yetkisiz erişim sağlamaya çalışır. Erişim sağlandığında, veriler çalınır veya işlemleri kesintiye uğratmak için kullanılır (Altaieb ve Rajnai, 2023). Ele geçirme ve karartma saldırıları, sistemin kontrolünü ele geçirmeye ve sistemi tamamen kapatmaya odaklanır. Geleneksel IDS sistemleri, protokol tabanlı güvenlik açıklarından yararlanır (Wali vd., 2025). Tekrar ve parçalama saldırıları, veri paketlerini yakalamaya odaklanır. Bu paketler yeniden gönderilerek işlem kesintilerine neden olur (Mondal vd., 2025; Sayegh vd., 2013). Dünyada bu tür saldırılar çeşitli hasarlara yol açmaktadır. Bu saldırılardan bazıları Tablo 2.1'de özetlenmiştir.

Tablo 2.1. SCADA ve ICS sistemlerine yönelik bazı saldırılar ve etkileri

Saldırı İsmi	Hedef	Saldırı Merkezi	Yıl	Ülke/Bölge	Etki
Stuxnet (Langner, 2011)	SCADA/ICS	İran Natanz Tesisi	Nükleer 2010	İran	PLC/SCADA sistemlerinin manipülasyonu yoluyla santrifüjlerde fiziksel hasar ve operasyonların kesintiye uğraması.
BlackEnergy Ukraine Power Grid (Robert M. Lee vd., 2016)	(2015 SCADA/ICS Grid)	Ukrayna Şebekesi (iletim/dağıtım)	Elektrik 2015	Ukrayna	Uzak SCADA sisteminin kapatılması nedeniyle meydana gelen elektrik kesintileri (yaklaşık 230,000 kullanıcıyı etkiledi).
Triton / Trisis (Mundo, 2020)	SCADA/ICS	Orta Doğu'daki petrokimya tesisinde Triconex SIS	Orta Doğu 2017	Orta Doğu(Arabistan)	SIS lojji hedef alınarak güvenlik sistemi devre dışı bırakıldı.

Tablo 2.1. (devam) SCADA ve ICS sistemlerine yönelik bazı saldırılar ve etkileri

Havex (Backdoor.Oldrea) (Slowik, 2021)	SCADA/ICS	Avrupa enerji şirketleri	2013–2014	Avrupa (öncelikle enerji sektörü)	ICS/OPC ortamlarında keşif ve sabotaj amacıyla bilgi toplandı.
Dragonfly Bear) (Khan vd., 2023)	(Energetic SCADA/ICS)	Avrupa ve ABD enerji şirketleri	2010	Küresel (kritik altyapı/enerji)	Sisteme sızmak ve keşif yapmak amacıyla tedarik zinciri + hedefli oltalama (spearphishing) + drive-by indirme yöntemleri kullanıldı.
Fragroute ile IDS Atlasma (Verkerken vd., 2022)	IDS IDS	General IDS sistemleri	1998 / 2002	—	Paket parçalama/yeniden yazma vb. nedenlerle trafiğin IDS tarafından yanlış yorumlanması; tespiti engellenmesi.
Snort IDS Atlasma (Verkerken vd., 2022)	IDS IDS	Snort kullanan ağlar	1998+	—	Yeniden birleştirme/parçalama gibi farklılıklar nedeniyle Snort'un bazı senaryoları kaçırma riski (eğer doğru bir ön işlemci/normalleştirici yoksa).
Shamoon (Bronk ve Tikk-Ringas, 2013)	ve SCADA (dolaylı)	Saudi Aramco (BT ağı; 2012 OT entegrasyonları etkilenmiş olabilir)	2012	Suudi Arabistan	Geniş çaplı veri silici etkisi; raporlara göre yaklaşık 30,000 bilgisayar etkilendi.

Fiziksel ve operasyonel hasara yol açan SCADA ve ICS sistemlerine yönelik saldırılar Tablo 2.1’de ayrıntılı olarak verilmiştir. Bu saldırıların ülkelere ve insanlara verdiği zararın boyutu ortadadır.

2.2. Geleneksel SCADA Saldırı Tespit Yöntemleri

SCADA ve IDS sistemlerine yönelik saldırılar, sisteme önemli fiziksel ve operasyonel zararlar vermektedir. Bu saldırıları önlemek için çeşitli yöntemler ve yaklaşımlar geliştirilmiştir. Sistemlere yönelik saldırıları önleme ve tespit etme çabaları, literatürde geleneksel tespit yöntemleri, makine öğrenimi yöntemleri, derin öğrenme tabanlı yöntemler ve hibrit yöntemler olarak belgelenmiştir. Bu yöntemler arasında geleneksel saldırı tespiti, imza tabanlı saldırı tespit sistemleri, kural tabanlı yaklaşımlar ve anomali tabanlı istatistiksel modelleri içermektedir.

IDS tabanlı sistemler, önceden tanımlanmış kalıplara ve bilinen tehditlerin imzalarına dayalı olarak yetkisiz erişimi önlemek üzere tasarlanmıştır. Bu, bilinen saldırıları tespit etmek için etkili bir yöntemdir. Ancak, yeni veya bilinmeyen tehditleri tespit etmede başarılı değildir. Basit olmaları ve düşük yanlış pozitif oranına sahip olmaları nedeniyle tercih edilmektedirler (Liao vd., 2013). Tripathi ve meslektaşları tarafından yapılan bir çalışma, SCADA sistemlerinde yaygınlaşan sıfırıncı gün saldırıları ve yeni tür yetkisiz erişim tekniklerinin, geleneksel imza tabanlı tespit sistemleri tarafından tespit edilemediğini göstermiştir (Tripathi vd., 2025). Kural tabanlı tespit sistemlerinde, şüpheli faaliyetleri belirlemek için uzmanlar veya geçmiş bilgiler kullanılır. Sayghe, çalışmasında

kural tabanlı sistemlerin belirli işlemlerde başarılı olabileceğini belirtmiştir (Soumya R vd., 2026; Sayghe, 2025). Ancak Okpeseyi ve meslektaşları, kural tabanlı sistemlerin gelişen tehditlere karşı zayıf olduğunu ve bu tür sistemlerdeki kuralların sürekli güncellenmesi gerektiğini belirtmiştir (Soumya R vd., 2026).

Anomalilere dayalı istatistiksel tespit yöntemlerinde, normal davranış kalıplarından sapmalar dikkate alınır. Anormal davranışları tanımlamak için istatistiksel modeller ve sapmalar değerlendirilir. Bilinen saldırılara genel amaçlar için güvenilmez. Bu nedenle, diğer geleneksel modellere kıyasla yeni saldırılara karşı daha iyi bir saldırı tespiti sağlar. Bu yaklaşım, SCADA gibi dinamik ortamlar için biraz daha uygun görünmektedir (Awaad vd., 2024). Ahakonye ve meslektaşları, SCADA sistemlerinde istatistiksel modeller kullanarak tespit yapmanın zorlu bir süreç olduğunu, çünkü doğal akışların yanlışlıkla tehdit olarak algılanabileceğini belirtmiştir. Bu nedenle, bu yöntemlerin yanlış pozitif sonuçlar verme eğiliminde olduğunu göstermişlerdir (Ahakonye vd., 2023).

Geleneksel tespit sistemleri, sistemdeki bilinen saldırıları tespit etmenin mümkün olduğunu, ancak bu tür yöntemleri kullanarak yeni saldırı türlerini tespit etmenin zor olduğunu göstermektedir.

2.3. Makine Öğrenimi Tabanlı SCADA Saldırı Tespiti

Geleneksel yöntemlerin aksine, makine öğrenimi yöntemleri SCADA sistemlerine yönelik saldırıları tespit etmede daha başarılıdır. Çeşitli makine öğrenimi yöntemleri bir dizi avantaj sunmaktadır. Literatürde, Destek Vektör Makineleri (SVM), Karar Ağaçları (DT), Rastgele Orman, k-En Yakın Komşu (k-NN) ve XGBoost gibi SCADA sistemlerine yönelik saldırıların tespitini mümkün kılan makine öğrenimi yöntemleri yer almaktadır. Patil, çalışmasında SCADA tabanlı sistemlere yönelik saldırıların düşük bir hata oranıyla tespit edilebileceğini göstermiştir (Patil, 2020). Sukhadeo ve ark. NSL-KDD veri seti üzerinde rastgele orman ve k-KNN kullanarak saldırıları sınıflandırmıştır (Sukhadeo vd., 2024). Lee ve ark. SVM ve XGBoost yöntemlerini kullanarak SCADA sistemlerindeki saldırıları tespit etmede %95'lik bir sonuç elde etmiştir (Lee vd., 2023). Çalışmalar incelendiğinde, makine öğrenimi tabanlı tespitlerde özellik çıkarmanın performans üzerinde büyük bir etkisi olduğu görülmektedir. Çeşitli özellik çıkarma yöntemlerinin

kullanıldığı başka bir çalışmada, gereksiz alanlar ortadan kaldırılmış ve genelleştirilebilirlik artırılmıştır (Lee vd., 2023). Genel olarak, yapılan çalışmalarda elde edilen performans %90'ın üzerindedir. Makine öğrenimi yöntemlerini kullanan bazı çalışma örnekleri Tablo 2.2'de gösterilmiştir.

Tablo 2.2. Çeşitli makine öğrenme yöntemleri ve özellik seçimleri kullanılarak yapılan çalışmalar

Yöntem	Öznitelik Seçimi	Başarı Oranı	Sınıf Sayısı	Açıklama
SVM (Lee vd., 2023)	PCA	%93,5	5	Lineer SVM, SCADA verilerinde normal ve 4 saldırı sınıfı için yüksek doğrulukla çalışmıştır.
SVM (Arqane vd., 2022)	Özyinelemeli Seçimi (Recursive FS)	Öznitelik %90,2	2	Endüstriyel IDS için ikili sınıflandırma (saldırı/normal); çekirdek tabanlı SVM kullanılmıştır.
Random Forest (Patil, 2020)	Bilgi Kazancı (Information Gain)	%95,1	4	SCADA ağ trafiğinde düşük aşırı öğrenme ile yüksek performans gösterilmiştir.
Random Forest (Sukhadeo vd., 2024)	Ki-Kare (Chi-Square)	%97,3	5	NSL-KDD tabanlı IDS tasarımı; sınıf dengesizliğine karşı dayanıklılık sağlanmıştır.
k-NN (Lee vd., 2023)	Korelasyon Tabanlı Seçimi (CFS)	Öznitelik %92,4	4	PLC verilerine dayalı; en iyi sonuçlar k=5 ile elde edilmiştir.
k-NN (Gbashi vd., 2025)	Relief-F	%94,2	3	SCADA sisteminde ağırlıklı mesafe metrikleri ile daha kararlı sonuçlar elde edilmiştir.
XGBoost (Roopesh vd., 2024)	Karşılıklı Bilgi (Mutual Information)	%98,6	5	XGBoost, diğer modellere göre daha kararlı ve daha hızlı sonuçlar sunmuştur.
XGBoost (Roopesh vd., 2024)	Rastgele Öznitelik Kütmesi (RFS)	Alt %96,8	6	SCADA elektrik şebekesi ağlarındaki farklı saldırı türlerine karşı dayanıklı sonuçlar elde edilmiştir.
LightGBM (Roopesh vd., 2024)	L1 Regularization	%95,4	5	XGBoost'a kıyasla daha düşük kaynak kullanımı ile benzer doğruluk elde edilmiştir.

Makine öğrenimi yöntemleri üzerine yapılan araştırmalar, bu yöntemlerin geleneksel yöntemlere kıyasla daha yüksek performans gösterdiğini ortaya koymuştur. Araştırmalar, bu performansın en önemli nedeninin özellik seçimi olduğunu göstermektedir.

2.4. Derin Öğrenme Tabanlı SCADA Güvenlik Çözümleri

SCADA tabanlı sistemlerde daha gelişmiş saldırı tespit yöntemleri, derin öğrenme temelli yöntemlerdir. Bunlar, Evrişimli Sinir Ağı (Convolutional Neural Network -CNN), Uzun-Kısa Süreli Bellek (Long Short-Term Memory -LSTM), Otomatik Kodlayıcı ve Transformer Modelleri olarak bilinir. CNN modelleri, bu tür sistemlerde tespit amacıyla yaygın olarak kullanılmaktadır. Tek başlarına kullanıldıklarında, uzun vadeli sıralı ilişkileri veya zamansal kalıpları yakalamada sınırlılık gösterebilirler. Bununla birlikte, hesaplama verimliliği ve hızları sayesinde öne çıkmaktadırlar (Shang vd., 2024). LSTM'ler, özellikle sıra yapılı temsilleri işlemede daha iyidir. Bu, ilgili saldırıları tespit etmede daha etkili öğrenme sağlar. Bunlar, yüksek hatırlama oranları ve hesaplama kaynakları gerektirir (Gao vd., 2021). Otomatik kodlayıcılara dayalı denetimsiz yöntemlerin sınıflandırma problemlerinde iyi performans gösterdiği belirtilmektedir (Fährmann vd., 2025).

Transformatör modelleri ise uzun menzilli bağımlılıkları ve karmaşık sıralı kalıpları yakalamada oldukça iyi performans gösterir (M. Musthafa, 2025).

Derin öğrenme modellerini kullanan her algılama sisteminin, belirli özelliklere sahip veri kümelerinde daha etkili olduğu vurgulanmaktadır. Her derin öğrenme tabanlı yöntem, sistem içindeki belirli özelliklere odaklanır. Bu, her modelin kendine özgü bir yapıya sahip olduğunu göstermektedir (bkz. Tablo 2.3).

Tablo 2.3. SCADA tabanlı sistemlerde saldırı tespiti için kullanılan derin öğrenme tabanlı modellerin karşılaştırılması

Tespit Doğruluğu	Verimlilik Performansı	Zamansal-Mekansal Öznitelik Çıkarımı	Yanlış Pozitif/Negatif Oranları
Transformer modelleri, doğruluk ve genelleme açısından CNN ve RNN'lere göre daha üstün performans göstermektedir (M. Musthafa, 2025).	Transformer, düşük çıkarım için performans optimize edilmiştir.	Transformer modelleri, uzun vadeli bağımlılıkları için RNN/CNN'e göre daha iyi yakalar.	Düşük yanlış pozitif ve yanlış negatif oranları
CNN, birden fazla veri kümesinde diğer derin öğrenme (DL) modellerine göre daha üstün performans göstermektedir (Nour ve Said, 2024).	CNN için uygun verimlilik	CNN mekansal öznitelikler için etkilidir; mekanizmaları (attention) dahil edilmiştir.	Değerlendirmede yanlış pozitif oranları dikkate alınmıştır.
1D CNN ve RNN, anomali tespitinde geleneksel yapay öğrenme (ML) yöntemlerine göre daha iyi performans göstermektedir (Siegel, 2020).	1D CNN'ler, verimlilikleri uzun diziler için tercih edilmektedir.	Spatio-temporal (uzay- zaman) öznitelikleri için RNN yerine 1D CNN kullanılmıştır.	Geleneksel yöntemlere kıyasla yanlış pozitif oranlarında iyileşme sağlanmıştır.
CKAN modeli, çoklu-IDS veri kümesinde %98'in üzerinde doğruluk değerine ulaşmıştır (Abd Elaziz vd., 2024).	Daha az parametre kullanılması, verimliliğini artırmaktadır.	Blok katmanları ile CNN hesaplama öznitelik geliştirilmiştir.	Standart CNN'e göre yanlış pozitif oranlarında iyileşme elde edilmiştir.
ICS veri kümelerinde LSTM üzerinde, DCNN ise %96 doğruluk oranına ulaşmıştır (Saheed vd., 2023).	LSTM %99'un üzerinde doğruluk verimliliği artırılmıştır.	LSTM ve DCNN, zamansal ve mekansal öznitelikler için son derece etkilidir.	Düşük yanlış pozitif ve yanlış negatif oranları gözlenmiştir.
Gaz boru hatlarında SCADA tabanlı, denetimsiz (unsupervised) anomali tespiti yapılmıştır (Nazir vd., 2021).	Gerçek zamanlı işlemler için uygun verimlilik	Otomatik kodlayıcı (autoencoder), normal trafik özelliklerini başarılı şekilde yakalamaktadır.	Yanlış pozitif ve yanlış negatif oranları eşikleme (thresholding) yöntemiyle yönetilmiştir.
Transformer modelleri iyi bir performans sunmaktadır (Casajús-Setièn vd., 2023).	Hesaplama verimliliği tartışılmamıştır.	Transformer zaman serisi modellerinde üstün başarı göstermektedir.	Yanlış pozitif ve yanlış negatif oranları detaylandırılmamıştır.
Derin otomatik kodlayıcı (deep autoencoder), DDoS saldırılarını tespit ve düşük yanlış alarm oranlarıyla belirlemektedir (Ortega-Fernandez vd., 2024).	Gerçek zamanlı işlemler için uygun verimlilik	Otomatik kodlayıcı, ağ akış özelliklerini yakalamaktadır.	Düşük yanlış pozitif ve yanlış negatif oranları
LSTM tabanlı IDS, MiTM ve DoS saldırılarını 2 dakika içinde tespit etmektedir (Ramos ve Yang, 2023).	Gerçek zamanlı işlemler için uygun verimlilik	LSTM bağımlılıkları yakalamaktadır.	Düşük yanlış pozitif ve yanlış negatif oranları
DNP 3.0 ağında yapay zeka tabanlı anomali tespiti %99 doğruluğa ulaşmaktadır (Ji vd., 2024).	Ortalama verimlilik	Otomatik kodlayıcı, ağ trafiği özelliklerini yakalamaktadır.	Düşük yanlış pozitif ve yanlış negatif oranları
Dikkat tabanlı varyasyonel otomatik kodlayıcı (attention-based VAE), sWAT veri kümesindeki anomali tespitini iyileştirmektedir (Macas vd., 2023).	Ortalama verimlilik	Dikkat mekanizması, uzay- zamansal öznitelik çıkarımını geliştirmektedir.	Yanlış pozitif ve yanlış negatif oranları

Her derin öğrenme modeli, saldırı tespitiyle ilgili belirli bağlamsal özellikler ortaya koymaktadır. Bu bağlamsallık, model türüne göre değişiklik gösterebilir. Bu nedenle, her model ayrı bir tespit işlemi için daha uygun görünmektedir.

2.5. Hibrit ve Çok Ölçekli Mimari Yaklaşımlar

Derin öğrenme modelleri, farklı saldırıların kendine özgü bağlamını daha iyi kavrar. Bu durum, tek bir modelle tüm saldırı türlerini ele almanın mümkün olmadığını göstermektedir. CNN'ler zaman bağımlılıklarında zayıf olsa da, yerel ve uzamsal kalıpları ortaya çıkarmada oldukça etkilidir. LSTM'ler zaman bağımlılıklarında güçlüdür ancak gürültüye karşı hassas olabilir. Oto-kodlayıcılar temsil öğreniminde güçlüdür, ancak tek başlarına sınıflandırma için yetersizdir. Transformer modelleri uzun bağımlılıklarda iyidir, ancak büyük miktarda veri gerektirir ve bu da donanım maliyetlerini artırır. Derin öğrenme modelleri tek başına kullanıldığında zayıftır. Bu nedenle, farklı derin öğrenme modellerini birleştirerek daha iyi avantajlar sunan yeni modeller oluşturmak suretiyle daha yüksek performans elde edilebilir. Hibrit modellerle yürütülen çalışmalara ilişkin örnekler Tablo 2.4'te gösterilmiştir. Bu modeller, elde ettikleri performansla mevcut yöntemler arasında en iyi performansı sergilemektedir.

Tablo 2.4. SCADA tabanlı sistemlerde saldırı tespiti için hibrit modellerin karşılaştırılması

Algılama Doğruluğu	Verimlilik Performansı	Zamansal-Mekansal Öznitelik Çıkarımı	Yanlış Oranları	Pozitif/Negatif
ICS (Endüstriyel Kontrol Sistemleri) veri kümelerinde F1 skoru ve AUC değerlerinde iyileşme sağlanmıştır (Shang vd., 2024).	Transformer entegrasyonu (inference) verimliliği düşük	CAE + Transformer ile güçlü uzamsal-zamansal öznitelikler yakalanmıştır.	SVDD sayesinde düşük yanlış alarm oranı (<%1,88)	optimizasyonu
SCADA fidiye yazılımı (ransomware) tespitiinde yaklaşık %97 doğruluk ve %98'in üzerinde AUC elde edilmiştir (Basnet vd., 2021).	Orta düzey	CNN + LSTM ile zamansal-zamansal temsiller	Düşük yanlış alarm oranı	
ConvLSTM ile oldukça yüksek Doğruluk/F1 skoru elde edilmiştir (Eshmaei vd., 2025).	Birleştirilmiş (hibrit) yapı sayesinde pratikte verimli	ConvLSTM uzamsal+ zamansal bağımlılık	ve FP minimize edilmiştir.	
DNP3 protokolünde %99,5 doğruluk (Alsaiairi ve Ilyas, 2025)	Orta Düzey	CNN-LSTM	Düşük FP/FN	
PLC ağında Doğruluk = %95,11 ve F1 Skoru = %95,12 (Y. Zhang vd., 2024)	Yüksek maliyeti hesaplama/üretim	Çok ölçekli Transformer	CNN + FP/FN iyileştirilmiştir.	
AE-GRU modeli, bağımsız tekil yöntemlere göre daha üstün performans göstermiştir (Harrou vd., 2024).	Orta Düzey	GRU-tabanlı kodlayıcı	otomatik FP/FN iyileştirilmiştir..	
CNN-LSTM-AE modeli ile FDI saldırısı tespiti geliştirilmiştir (Mahi-Al-rashid vd., 2022).	Orta Düzey	CNN-LSTM + AE	Yanlış pozitif (FP) oranlarında önemli bir düşüş gerçekleşmiştir.	
Yarı denetimli LSTM-AE modelinin etkili olduğu görülmüştür (Muhlburger ve Wotawa, 2022).	Orta Düzey	LSTM Otokodlayıcı	FP/FN iyileştirilmiştir.	
GoogLeNet-LSTM modeli, Modbus protokolünde %97,56 doğruluk oranına ulaşmıştır (Chu vd., 2019).	Orta Düzey	CNN-LSTM	Düşük FP ve düşük kaçırma	

Hibrit yöntemler, geleneksel yöntemler, makine öğrenimi tabanlı yöntemler ve derin öğrenme modellerini bir araya getirerek daha iyi sonuçlar elde etmek amacıyla birden fazla modelin birleştirildiği yöntemlerdir. Bu yöntemler, SCADA ve IDS sistemlerinde saldırı tespiti için en yaygın olarak kullanılan yöntemler olarak kabul edilmektedir.

2.6. Mevcut Çalışmaların Sınırlılıkları ve Araştırma Açığı

Literatür incelemeleri, SCADA sistemlerine yönelik saldırıların tespitinde önemli ilerlemeler olduğunu ortaya koymuştur. Bu gelişmelere rağmen, bazı araştırma boşlukları tespit edilmiştir. Bu çalışmaların bulgularına dayanarak, mevcut sınırlamalar ve araştırma boşlukları şu şekilde özetlenebilir.

Gerçekçi ve SCADA'ya özgü veri kümesi: Literatürde SCADA sistemlerinde saldırı tespiti üzerine birçok çalışma bulunmaktadır. Çalışmalarda, genel ağ trafiğine ait NSL-KDD ve CIC-IDS2017 gibi veri kümeleri kullanılmıştır. Bu veri kümeleri, normal ağlarda bulunan düzensiz trafik akışlarına dayanmaktadır. Bu veri kümeleri, Modbus/TCP gibi endüstriyel protokolleri içeren trafikle ilişkili döngüsel ve öngörülebilir veri akışını yansıtmamaktadır. Gerçek bir SCADA ortamında, cihazlara belirli aralıklarla sorgu gönderilir. Sorgu-yanıt döngüsü uzun bir süre devam eder. Paket boyutu ve trafik genellikle düşüktür. Anormallikler genellikle paket içindeki bir komuttan veya zamanlama döngüsündeki bir kesintiden kaynaklanır. NSL-KDD ve CIC-IDS2017 gibi veri kümeleri genel ağ trafiğini yansıttığı için, komut enjeksiyonunu ve protokol tabanlı saldırı vektörlerini yansıtmaz. Bu durum, SCADA sistemlerinde saldırı tespiti için eğitim verisi olarak bu veri kümelerinin güvenilirliğini sorgulanır hale getirir. **Dengesiz Verilerle Çeşitli Saldırı Senaryolarının Birlikte Ele Alınmaması:** SCADA tabanlı sistemlerde, normal ağ trafiği saldırı trafiğinden çok daha fazladır. Bu durum, saldırı kategorileri arasında önemli bir sınıf dengesizliğine yol açar. Nadiren meydana gelen saldırı sınıflarını tespit etmek özellikle zordur. Bu durum, geliştirilen modelin çoğunluk sınıfına ait saldırılara odaklanmasına neden olur ve azınlık sınıfına ait saldırıların gözden kaçmasına yol açar. Mevcut veri kümelerinde çok sayıda saldırı sınıfına yönelik kapsamlı senaryolar sınırlıdır.

Tekli modellerin yetersizliği ve hibrit mimari modellere duyulan ihtiyaç: Derin öğrenme modelleri, bir veri kümesindeki belirli özelliklere odaklanır. Bir model bir veri kümesinde iyi performans gösterirken, başka bir derin öğrenme modeli farklı bir veri kümesinde daha etkili olabilir. CNN modelleri yerel ve uzamsal örüntülere, LSTM'ler yapılandırılmış özellik temsillerindeki sıralı veya bağlamsal ilişkilere ve otomatik kodlayıcılar ise normal davranış temsillerine odaklanır. SCADA sistemlerinde meydana gelen bir saldırı, hem paket iç yapısında anomaliler hem de trafikten türetilen öznitelikler veya sıra yapılı

temsiller arasında düzensiz ilişkiler sergileyebilir. Mevcut çalışmaların büyük bir kısmı, bunu tek bir model aracılığıyla yakalamaya çalışmaktadır. Bu çalışma, önerilen hibrit model aracılığıyla farklı özelliklere sahip saldırıların tespit edilmesini sağlayan sofistike bir model sunmaktadır.

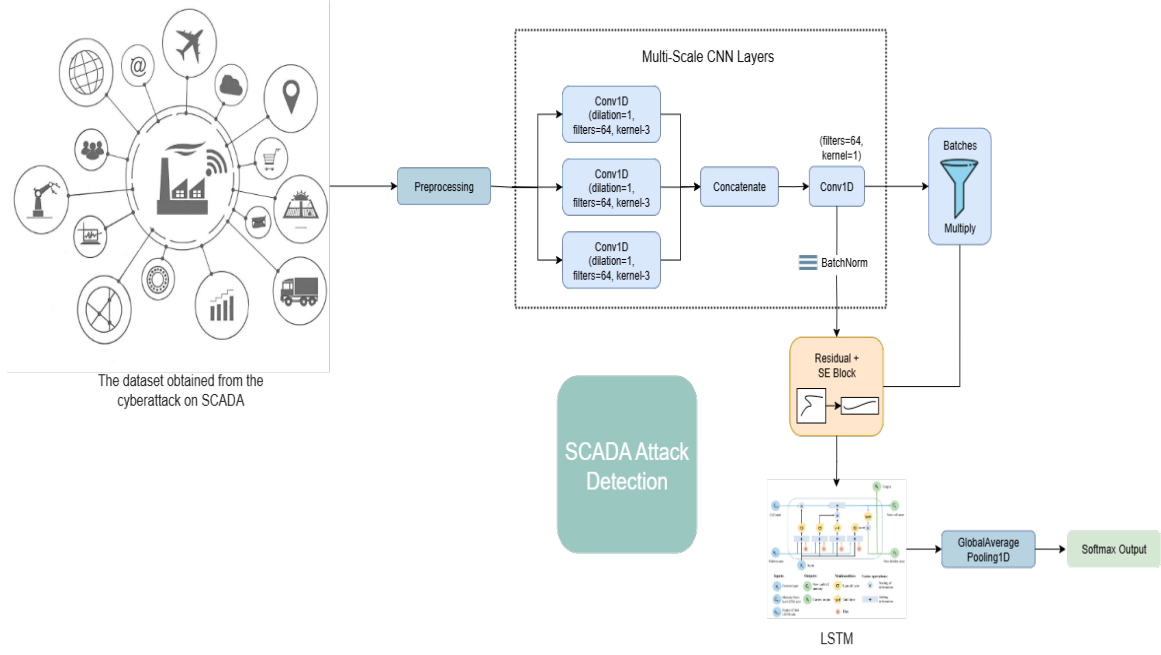
3. MATERYAL VE YÖNTEM

3.1. Veri Ön İşleme

Bu çalışmada kullanılan SCADANet veri kümesi, öncelikle eksik değerlerin doldurulması, özellik ölçeklendirme ve etiket kodlama aşamalarından geçirildi. Eksik değerler, 0 sabit değeriyle dolduruldu. Tüm sayısal özellikler, StandardScaler kullanılarak normalleştirildi. Güvenilir bir değerlendirme sağlamak ve veri kümesi bölümleri arasında veri sızıntısını önlemek amacıyla, tüm ön işleme adımları her bir çapraz doğrulama katında bağımsız olarak gerçekleştirildi. Her katmanda, tamamlayıcı ve StandardScaler yalnızca eğitim verileri üzerinde eğitildi. Öğrenilen parametreler daha sonra ilgili doğrulama ve test alt kümelerine uygulandı. Veri bölümleri arasında istenmeyen bilgi aktarımını önlemek için, eğitim ve test kümeleri ön işleme öncesinde birbirinden ayrıldı. Ek olarak, her katmanda ön işleme ve özellik çıkarımı bağımsız olarak gerçekleştirilerek, veri kümesi bölümleri arasında son derece benzer veri örneklerinin çakışması en aza indirildi. Bu süreç, farklı ölçeklere sahip değişkenlerin model üzerindeki etkisini dengeledi. Ayrıca, güvenilir bir model değerlendirmesi sağladı. Normalleştirilmiş girdi verileri daha sonra CNN tabanlı mimariyle uyumlu hale getirmek için (örnek sayısı, özellik sayısı, 1) formatına dönüştürüldü. Son olarak, çıktı etiketleri bir LabelEncoder kullanılarak kodlandı.

3.2. Önerilen Model Mimarisi

Bu çalışmada, dönüştürülmüş SCADA temsillerinde trafik kaynaklı özellikler arasındaki çok ölçekli uzamsal örüntüleri ve sıralı bağlamsal ilişkileri bir arada modellemek üzere, Paralel Dilated Conv1D, Residual-SE blokları ve LSTM katmanlarından oluşan bir hibrit derin öğrenme mimarisi önerilmiştir. Önerilen mimarinin genel akış şeması Şekil 3.1’de sunulmuştur.



Şekil 3.1. Önerilen Hibrit Mimari Yapısı

Giriş Katmanı: Modelin girişi, her örnek için $(T, 1)$ boyutunda olacak şekilde düzenlenmiştir. Burada T , zaman adımı veya özellik uzunluğunu temsil eder.

Çıkarılan SCADA trafik özellikleri ile çok katmanlı hibrit mimari tarafından işlenen giriş temsilleri arasındaki ilişki netleştirilerek, önerilen matematiksel formülasyonun yorumlanaabilirliği artırılmıştır. Protokol düzeyindeki trafik özellikleri, paket meta verileri ve JA4+ tabanlı parmak izi özellikleri, yapılandırılmış özellik temsillerine dönüştürülür. Bu özellikler daha sonra paralel genişletilmiş evrişim ve sıralı modelleme bileşenleri tarafından işlenir.

Paralel Genişletilmiş Evrişim Katmanları: Evrişimli Sinir Ağları, ağ trafiği analizi, anomali tespiti ve DDoS saldırı sınıflandırması için siber güvenlik alanında sıklıkla kullanılan derin öğrenme mimarileridir (Alam vd., 2020). CNN'ler, $X \in \mathbb{R}^{H \times W \times C}$ giriş tensörü üzerindeki uzamsal korelasyonları korur ve yerel örüntüleri çıkarır. Bir konvolüsyon işlemi, Denklem 3.1'de gösterildiği gibi $k \in \mathbb{R}^{n \times n \times C}$ çekirdek filtresi kullanılarak tanımlanır.

$$Y(i, j) = \sum_{m=1}^n \sum_{n=1}^n X(i + m, j + n) \cdot k(m, n) \quad (3.1)$$

Denklem 3.1'de, $Y(i, j)$ özellik haritasını, $(i + m, j + n)$ ise girdi tensöründeki yerel pikselleri temsil eder; $k(m, n)$ ise bu piksellerle çarpılan öğrenilebilir ağırlıkları temsil eder. Bu klasik

yapı, sınırlı alıcı alanı nedeniyle yalnızca kısa menzilli bağımlılıkları öğrenebilir. Yüksek boyutlu ağ trafik akışlarında bu durum, uzun menzilli bağımlılıkları yakalamayı zorlaştırır. Bu sınırlamayı aşmak için genişletilmiş evrişim mekanizması kullanılır. Bu yaklaşımda, genişletme oranı d ile çekirdek elemanları arasına boşluklar eklenir. Böylece, parametre sayısı sabit tutulurken etkili alıcı alan genişletilir. Tek boyutlu genişletilmiş evrişim işlemi, Denklem 3.2'de gösterildiği gibi matematiksel olarak ifade edilir.

$$(F^{(d)} * k)t = \sum_{\tau} k_{\tau} \cdot F_{t-d\tau} \quad (3.2)$$

Denklem 3.2'de F , giriş sinyali (trafik akışı sinyali vb.), k çekirdek ağırlığını, d genişleme oranını ve τ ise çekirdeğin konum indeksini temsil eder.

Bu durumda, etkin alıcı alanı R_{eff} Denklem 3.3'te olduğu gibi ifade edilir.

$$R_{\text{eff}} = [(n - 1)d + 1]^2 \quad (3.3)$$

Bu artış, modelin aynı sayıda parametreyle daha geniş bağlamsal bilgileri yakalamasını sağlar. Bu sayede hem yerel (ince ölçekli) hem de küresel özelliklerin aynı anda öğrenilmesi mümkün hale gelir (Chauhan ve Kumar, 2025).

Verimli Uzamsal Piramit modülünde, çok ölçekli özellik çıkarma, farklı genişleme oranlarına sahip konvolüsyon dallarının paralel olarak çalıştırılmasıyla gerçekleştirilir. Genişleme oranı $d_k = 2^{k-1}$ olarak tanımlanırsa, etkin alıcı alan Denklem 3.4'te gösterildiği gibi genişler.

$$R_{\text{ESP}} = [(n - 1)2^{K-1} + 1]^2 \quad (3.4)$$

Verimli Uzamsal Piramit modülünün parametre sayısı Denklem 3.5'te belirtildiği gibi ifade edilir.

$$P_{\text{ESP}} = \frac{1}{K} (NM + n^2 N^2) \quad (3.5)$$

Bu, klasik CNN mimarilerine kıyasla daha az parametreyle daha geniş bir uzamsal bağlamın öğrenilmesini sağlar.

Bu yapının genelleştirilmiş biçimi, Paralel Genişletilmiş Evrişimli Sinir Ağı mimarisi olarak adlandırılır. Bu mimari, farklı genişletme oranlarına (d_i) sahip birden fazla evrişimli katmanı eşzamanlı olarak çalıştırır. Her genişletme oranı için özellik çıkarma süreci, Denklem 3.6'da ifade edildiği gibidir.

$$D_c^{(i)} = \sigma(F^{d_i} * X) \quad (3.6)$$

Denklem 3.6, ReLU veya Swish gibi doğrusal olmayan aktivasyon fonksiyonlarını temsil eden σ 'yı ifade eder. Elde edilen çok ölçekli özellik haritaları daha sonra Küresel Ortalama Havuzlama katmanında birleştirilir. Küresel Ortalama Havuzlama katmanı, Denklem 3.7'de gösterildiği gibi ifade edilir.

$$y_c = \frac{1}{H \times W} \sum_{i=1}^H \sum_{j=1}^W D_c^{(L)}(i, j) \quad (3.7)$$

Denklem 3.7'deki her adım, her kanalın ortalama aktivasyon değerini çıkarır. Bu, aynı zamanda modelin genelleme yeteneğini artırır ve aşırı uyum riskini azaltır. Siber saldırı tespitinde, düşük genişleme oranları yerel paket istatistiklerini ve kısa menzilli korelasyonları öğrenir. Öte yandan, yüksek genişleme oranları ise ağ trafiği içindeki küresel anomalileri ve uzun menzilli ilişkileri yakalar. Böylece model, geniş bir etkin alıcı alanı R_{eff} ile bağlamsal farkındalık geliştirir. Bu, DDoS saldırıları gibi çok ölçekli kalıpları tespit etmede yüksek doğruluk ve genelleme performansı sağlar.

Bu çalışmada geliştirilen modelin uygulama aşamasında, girdi üç paralel Conv1D katmanına gönderildi. Bu katmanlarda aynı filtre boyutu (3) kullanılırken, farklı genişleme oranları uygulandı. Böylece mimari, kısa ve uzun vadeli bağımlılıkları aynı anda öğrenebildi. Her dal 64 filtre ve bir ReLU aktivasyon fonksiyonu kullandı. Paralel dallardan elde edilen çıktılar birleştirilerek (T,192) boyutunda bir tensör oluşturuldu. Bu yapı, modelin büyük ölçekli özellik çıkarma kapasitesini artırarak siber saldırı tespit performansını güçlendirdi (Qi vd., 2025).

Toplu Normalleştirme ve 1×1 Konvolüsyon: Toplu Normalleştirme (BN), derin sinir ağlarında eğitim sürecini hızlandırırken aynı zamanda ağın kararlılığını artırmak için yaygın olarak kullanılan bir normalleştirme tekniğidir. Temel olarak, bu teknik, eğitim sırasında katmanlar arasındaki aktivasyon dağılımındaki sürekli değişimden kaynaklanan iç kovaryans kaymasını azaltmayı amaçlar. Bu yöntem, her mini partideki aktivasyonları normalize ederek, bunları ortalama sıfır ve varyans bir olacak şekilde dönüştürür. Ardından, modelin öğrenebileceği ölçek (γ) ve önyargı (β) parametrelerini kullanarak bunları yeniden şekillendirir (Hussen vd., 2023). Matematiksel olarak, bu süreç Denklem 3.8'de ifade edilir.

$$\mu = \frac{1}{m} \sum_{i=1}^m x_i, \quad \sigma^2 = \frac{1}{m} \sum_{i=1}^m (x_i - \mu)^2 \quad (3.8)$$

Burada, $\mu = \frac{1}{m} \sum_{i=1}^m x_i$ ifadesi, mini yığın(mini-batch) içindeki verilerin ortalamasını hesaplar. $\sigma^2 = \frac{1}{m} \sum_{i=1}^m (x_i - \mu)^2$ ifadesi ise mini yığın verilerinin varyansını hesaplar. Ardından, Denklem 3.9'da belirtilen normalleştirme işlemi uygulanır. Bu işlem, ortalamanın sıfır ve varyansın bir olması için verileri normalleştirir.

$$\sigma^2 = \frac{1}{m} \sum_{i=1}^m (x_i - \mu)^2 \quad (3.9)$$

Çıktı, son denklem 3.10'da belirtilen yeniden ölçeklendirme ve kaydırma işlemiyle elde edilir.

$$y_i = \gamma \hat{x}_i + \beta, \quad \gamma \in \mathbb{R} \text{ and } \beta \in \mathbb{R} \quad (3.10)$$

Burada (Denklem 3.10), ϵ sayısal kararlılığı sağlayan küçük bir sabittir. Eğitim aşamasında istatistikler minibatch'ler üzerinde hesaplanırken, test aşamasında ise tüm eğitim kümesinden elde edilen hareketli ortalama ve varyans kullanılır. Toplu normalleştirme (Batch Normalisation), daha yüksek öğrenme hızlarıyla eğitimi mümkün kılar ve gradyanların patlamasını veya yok olmasını önler. Ayrıca, düzenleyici görevi görerek aşırı uyum riskini azaltır. Bu çalışma kapsamında geliştirilen modelde, birleştirme işleminden sonra elde edilen yüksek boyutlu özellik haritası, Toplu Normalleştirme kullanılarak normalleştirilmiştir. Ardından, parametre sayısını azaltmak ve boyutları dengelemek için 1×1 Conv1D katmanı (64 filtre, ReLU aktivasyonu) kullanılmıştır (J. Bjorck vd., 2018).

Residual-SE Bloğu: Derin sinir ağlarında katman sayısı arttıkça, gradyan azalması ve öğrenme zorlukları gözlemlenir. Bu sorunu aşmak için kullanılan Residual Bloğu, doğrudan amaç fonksiyonu yerine girdi ile hedef arasındaki farkı öğrenir (Kumar, 2025). Yapı, Denklem 3.11'de gösterildiği gibi matematiksel olarak tanımlanır:

$$y = \mathcal{F}(x, W) + x \quad (3.11)$$

Denklem 3.11, artık bloğun temel ilkesini göstermektedir. Girdi x , W parametreleri kullanılarak dönüştürülmüş hali $\mathcal{F}(x, W)$ ile birleştirilir. Böylelikle ağ, hedefi doğrudan değil, giriş ile hedef arasındaki farkı öğrenir. Bu çalışmada kullanılan artık bloğu aşağıdaki işlemlerden oluşmaktadır:

$$\mathcal{F}(x) = \text{Conv1D}_{3 \times 3} \rightarrow \text{Swish} \rightarrow \text{BN} \rightarrow \text{Conv1D}_{1 \times 1} \quad (3.12)$$

Denklem 3.12, fonksiyonun nasıl hesaplandığını belirtmektedir. 3x3 konvolüsyon, Swish aktivasyonu ve Toplu Normalleştirme adımlarından geçtikten sonra, 1x1 konvolüsyon uygulanır. Amaç, girdi özelliklerini dönüştürmek ve daha anlamlı temsiller elde etmektir. Kısayol dönüşümü:

$$x' = \text{Conv1D}_{1 \times 1}(x) \quad (3.13)$$

Bu ifade (Denklem 3.13) kısayol dönüşümünü tanımlar. Giriş verileri, boyut eşleşmesi sağlamak için 1x1 konvolüsyon kullanılarak dönüştürülür, böylece $\mathcal{F}(x)$ 'e eklenebilir.

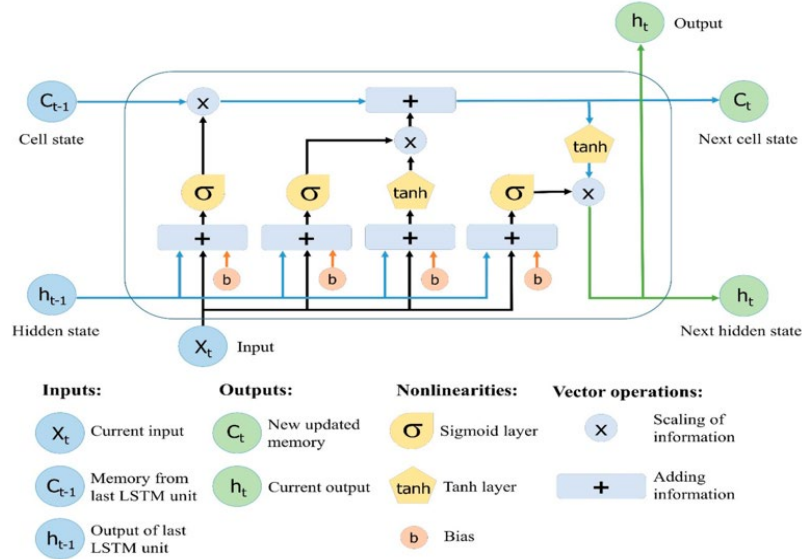
$$y = \text{Swish}(\mathcal{F}(x) + x') \quad (3.14)$$

Nihai çıktı, Denklem 3.14'te belirtilen formül kullanılarak elde edilir. Artık fonksiyonu ve kısayol çıktısı toplandıktan sonra, bunlar Swish aktivasyon fonksiyonundan geçirilir. Bu yapı, doğrusal ve doğrusal olmayan bileşenleri birleştirerek çok katmanlı temsillerin etkili bir şekilde öğrenilmesini ve derin mimarilerin verimli bir şekilde eğitilmesini sağlar.

LSTM Katmanı: Uzun-Kısa Süreli Bellek (LSTM), 1997 yılında Hochreiter ve Schmidhuber tarafından önerilen ve geleneksel Tekrarlayan Sinir Ağlarının (RNN) uzun vadeli bağımlılıkları öğrenirken karşılaştığı gradyan kaybolması/patlama sorularını

çözmek üzere özel olarak geliştirilmiş bir yapıdır. LSTM'nin en temel özelliği, bilgi akışını düzenleyen geçit mekanizmaları aracılığıyla geçmiş verilerden elde edilen bilgileri uzun süreler boyunca muhafaza etme yeteneğidir (Kang vd., 2019). Bu çalışmada, LSTM katmanı ham paket düzeyindeki zaman serilerini veya sürekli trafik akışlarını doğrudan modellemek için kullanılmamıştır. Bunun yerine, her bir SCADA trafik örneği, ağ trafiğinden çıkarılan ve tek boyutlu bir özellik dizisi haline getirilen sıralı bir sayısal özellik vektörü olarak temsil edilmiştir. Bu nedenle, LSTM bileşeni, paket akışlarındaki doğrudan zamansal bağımlılıklar yerine, trafikten türetilen öznitelikler arasındaki sıralı ve bağlamsal ilişkileri öğrenmek için kullanılmıştır. Bir LSTM hücresi aşağıdaki öğeleri içerir (bkz. Şekil 3.2).

Hücre durumu (C_t): Uzun vadeli bilgilerin aktarılmasında kullanılan ana yol. Gizli durum (h_t): Mevcut çıktıyı temsil eden kısa vadeli bilgiler. Unutma kapısı (f_t): Bellekten hangi bilgilerin silineceğini belirler. Giriş kapısı (i_t): Gelen verilerin hangi kısımlarının belleğe yazılacağını kontrol eder. Çıkış kapısı (o_t): Bellekteki bilgilerin ne kadarının dışarı aktarılacağını düzenler. Hücre adayı ($\tilde{C}_t$): Eklenebilecek yeni bilgiler için bir aday oluşturur.



Şekil 3.2. LSTM mimarisi (Heddam vd., 2022)

LSTM'nin güncelleme süreci aşağıdaki denklemlerle tanımlanır:

$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f)$: Bu ifade unutma kapısını tanımlar. Ayrıca önceki bilgilerin ne kadarının saklanacağını belirler. $i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i)$: Bu, giriş kapısıdır. Yeni bilginin belleğe girme hızını düzenler. $\tilde{C}_t = \tanh(W_C \cdot [h_{t-1}, x_t] + b_C)$: Aday bellek. Ekleme için uygun yeni bilgiler üretir. $C_t = f_t \odot C_{t-1} + i_t \odot \tilde{C}_t$: Güncellenmiş hücre durumu, eski bilgilerin uygun kısmı ile yeni bilgilerin birleşimini temsil eder. $O_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o)$: Çıkış kapısı. Hücre bilgisinin hangi kısmının çıktı olacağını seçer $h_t = o_t \odot \tanh(C_t)$: Gizli durum, nihai çıktıyı oluşturan bilgiyi temsil eder.

Burada, σ sigmoid fonksiyonunu, $\tanh$ hiperbolik tanjant fonksiyonunu ve $\odot$ eleman bazlı çarpımı ifade eder. Bu yapı, LSTM'nin gerektiğinde bilgileri güncellemesini ve gerektiğinde uzun süreler boyunca saklamasını sağlar. LSTM'nin başarısındaki kilit faktörlerden biri, hata sinyalinin zaman içinde kayıpsız bir şekilde taşınmasını sağlayan Sabit Hata Karuseli (Constant Error Carousel -CEC) adlı mekanizmadır. Bu, modelin uzun dizilerde bile geçmiş bilgilere erişmesini sağlar. Eğitim süreci genellikle Zaman İçinde Geri Yayılım (Backpropagation Through Time -BPTT) algoritması kullanılarak gerçekleştirilir. Zamanla, farklı LSTM türleri geliştirilmiştir. Temel (vanilya) LSTM yalnızca giriş, unutma ve çıkış kapılarından oluşur. Peephole LSTM, bellek durumunu geçitlere doğrudan bağlayarak ek bilgi aktarımı sağlar. Bidirectional LSTM, verileri hem ileri hem de geri yönde işlerken, Stacked LSTM, birden fazla katmanı üst üste istifleyerek daha karmaşık bağımlılıkları öğrenebilir. LSTM, doğal dil işleme, konuşma tanıma, zaman serisi tahmini, sağlık verileri analizi ve ağ güvenliği gibi birçok alanda yaygın olarak kullanılmaktadır. Uzun vadeli ilişkileri öğrenme yeteneği sayesinde, dizi tabanlı problemler için vazgeçilmez bir derin öğrenme modeli haline gelmiştir (Laghrissi vd., 2021).

Bu çalışma kapsamında geliştirilen modelde, Residual-SE bloğundan elde edilen çıktılar, dönüştürülmüş SCADA trafik temsilindeki özellik düzeyindeki sıralı ve bağlamsal bağımlılıkları modellemek üzere 128 birimli bir LSTM katmanına (return_sequences=True) beslendi. Bu, CNN tabanlı özellik çıkarmanın yanı sıra trafikten türetilen özellikler arasındaki ilişkilerin de yakalanmasını sağladı.

Havuzlama ve Tam Bağlantılı Katmanlar: LSTM katmanının çıktısı, Global Average Pooling (GAP) kullanılarak özetlendi ve sabit uzunlukta bir vektöre dönüştürüldü. Bu vektör, 128 nöronlu ve ReLU aktivasyonlu yoğun bir katmana beslendi ve aşırı uyumlanmayı azaltmak için Dropout (oran=0,3) uygulandı.

Çıkış Katmanı: Son katman C nöron içerir; burada C , veri kümesindeki hedef sınıfların toplam sayısını belirtir. SCADANet veri kümesinde $C = 14$ olup, bir normal trafik sınıfını ve on üç saldırı sınıfını temsil eder. Her nöron bir sınıfa karşılık gelir ve Softmax aktivasyon fonksiyonu, çıkış logitlerini sınıf olasılıklarına dönüştürür. Bu nedenle, çıktı vektörü $p = [p_1, p_2, \dots, p_C]$ olarak tanımlanır; burada p_i , girdi örneğinin i 'inci sınıfa ait olma olasılığını gösterir ve $\sum_{i=1}^C p_i = 1$ 'dir. En yüksek olasılığa sahip sınıf, nihai tahmin edilen etiket olarak seçilir.

3.3. Eğitim Stratejisi

Bu çalışma kapsamında önerilen modelin eğitimi, 0,001 başlangıç öğrenme hızına sahip Adam optimizasyon algoritması kullanılarak gerçekleştirilmiştir. Veri kümesi dengesiz saldırı sınıfları içerdiğinden, nihai model standart kategorik çapraz entropi yerine çok sınıflı focal loss fonksiyonu kullanılarak eğitilmiştir. Focal Loss (Odak Kayıp), çapraz entropi formülasyonundan türetilmiştir ve optimizasyon sırasında kolayca sınıflandırılabilen örneklerin katkısını azaltırken, sınıflandırılması zor ve azınlık sınıfına ait örneklerin etkisini artırır. Bu çalışmada, odak kayıp parametreleri $\gamma = 2,0$ ve $\alpha = 0,25$ olarak ayarlandı.

Odak kaybına ek olarak, sınıf dengesizliğinin olumsuz etkisini daha da azaltmak için sınıf ağırlıkları kullanıldı. Bu ağırlıklar, yalnızca her katın eğitim verilerine dayalı olarak hesaplandı ve her sınıftaki örnek sayısı ile ters orantılı olarak tanımlandı. Bu nedenle, nadir saldırı sınıfları, model eğitimi sırasında toplam kayba daha güçlü bir şekilde katkıda bulundu.

Eğitim aşamasında, aşırı öğrenmeyi önlemek, genelleme yeteneğini geliştirmek ve öğrenme sürecini istikrara kavuşturmak amacıyla çeşitli düzenleme ve optimizasyon stratejileri kullanıldı. Doğrulama kaybı (Validation Loss) izlenerek erken

durdurma(EarlyStopping) yöntemi uygulandı. Arka arkaya 15 döngü boyunca herhangi bir iyileşme gözlemlenmezse, eğitim süreci otomatik olarak sonlandırıldı ve en iyi model ağırlıkları geri yüklendi. Ayrıca, öğrenme hızını uyarlanabilir bir şekilde ayarlamak için ReduceLROnPlateau yöntemi kullanıldı. Doğrulama kaybında 7 ardışık döngü boyunca iyileşme görülmezse, öğrenme hızı yarı yarıya azaltıldı. Son olarak, en düşük doğrulama kaybına karşılık gelen model ağırlıklarını kaydetmek için kontrol noktası (ModelCheckpoint) kullanıldı.

Odak kaybı, sınıf ağırlıklandırması, erken durdurma, uyarlanabilir öğrenme hızı azaltma ve kontrol noktası oluşturma'nın bir arada kullanılması, aşırı uyum riskini azaltırken daha istikrarlı ve sınıf dengeli bir eğitim süreci sağladı.

4. BULGULAR VE TARTIŞMA

Bu bölümde, önerilen modelin iki farklı veri kümesi üzerinde yapılan deneysel değerlendirmeler, kullanılan çapraz doğrulama stratejisi, dengesiz veri sorunu için yapılan optimizasyonlar, performans ölçütleri ve ablasyon analizleri ayrıntılı olarak sunulmaktadır. Deneyler, yöntemin genelleştirilebilirliğini, bileşenlerinin katkılarını ve sınıf dengesizliği koşullarındaki sağlamlığını kapsamlı bir şekilde ortaya koymayı amaçlamaktadır.

4.1. Deney Düzeni ve SCADANet Veri Setinin Toplanması

Bu deneysel çalışmada kullanılan SCADANet veri kümesi, tamamen izole edilmiş bir sanal SCADA laboratuvar ortamında oluşturulmuştur. Deneysel çalışmanın sonunda elde edilen veri kümesi, toplam 486.714 adet etiketlenmiş ağ paketinden oluşmaktadır. Veri kümesi, normal trafiğin yanı sıra 13 farklı saldırı senaryosundan elde edilen paketleri içermekte olup, toplam 14 trafik sınıfını kapsamaktadır. Veri seti, 6.403 farklı kaynak IP adresi, 123 hedef IP adresi ve 165 farklı ağ protokolü içermektedir. Trafik yaklaşık %83'ü saldırı paketlerinden, %17'si ise normal trafik paketlerinden oluşmaktadır. Ayrıca, veri setinde sınıf dengesizliği gözlemlenmektedir. Bu durum, yeterince temsil edilmeyen saldırı sınıflarının doğru bir şekilde öğrenilmesini sağlamak için uygun eğitim stratejilerinin kullanılmasını gerektirmektedir.

TCP SYN Flood, TCP ACK Flood, UDP Flood, ICMP Flood, HTTP Flood, SQL Injection, Port Scan, Vulnerability Scan ve Operating System Scan gibi klasik ağ saldırılarının yanı sıra, veri seti Modbus False Data Injection (FDI), Modbus Command Abuse, APT Data Exfiltration ve Insider Threat gibi SCADA'ya özgü saldırıları da içermektedir. Bu saldırılar, keşif faaliyetleri, kaynak tüketimi, hizmet istismarı, güvenlik açığı taraması, protokol manipülasyonu, gizli veri sızdırma ve içeriden sabotaj dahil olmak üzere endüstriyel kontrol sistemlerinde karşılaşılan çeşitli tehdit kategorilerini temsil etmek üzere deneysel bir çalışmanın parçası olarak tasarlanmıştır.

Gerçek dünyadaki endüstriyel ağ davranışını yansıtmak amacıyla, saldırılar Modbus/TCP, UDP, ICMP ve HTTP gibi çeşitli protokol yapıları kullanılarak normal trafik akışlarının içine yerleştirildi. Sonuç olarak, veri kümesi hem SCADA sistemlerinin normal çalışma davranışını hem de çok sınıflı saldırı modellerini kapsayan zengin ve gerçekçi bir araştırma ortamı sunmaktadır. Özellikle, veri setine SCADA protokolü manipülasyon senaryolarının dahil edilmesi, veri setinin yalnızca geleneksel ağ saldırılarını değil, aynı zamanda endüstriyel iletişim protokollerini hedef alan siber-fiziksel tehditleri de temsil etmesini sağlar.

Bu çalışma için oluşturulan deneysel ortam, Windows işletim sisteminde çalışan VMware Workstation Pro kullanılarak yapılandırılmıştır. Şekil 4.1'de gösterildiği gibi, bu tamamen izole edilmiş sanal laboratuvar ortamı, yedi sanal makineden (VM) oluşan çok düğümlü bir SCADA topolojisi olarak tasarlanmıştır. Topoloji, saldırgan sistemleri, hedef sunucuları, Modbus/TCP tabanlı saha cihazlarını, SCADA/HMI ana kontrol sistemlerini ve tüm ağ trafiğini pasif olarak izleyen bir izleme düğümünü içerir.

Tüm sanal makineler, NAT tabanlı bir ağ üzerinden birbirine bağlanacak şekilde yapılandırılmış ve tek bir yayın etki alanı oluşturmuştur. Ağ trafiğini yakalamak üzere yapılandırılan Ubuntu tabanlı sniffer sanal makinesi, sanal anahtarda pasif modda çalıştırılmış ve ortamda üretilen tüm paketleri kaydetmiştir. Tüm ağ trafiği, Wireshark ve TShark araçları kullanılarak “.pcapng” formatında kaydedildi ve ardından çok katmanlı ağ özellikleri çıkarıldı. Çıkarılan özellikler arasında kaynak/hedef IP adresleri, bağlantı noktası bilgileri, TCP bayrakları, paket uzunlukları, oturum bilgileri, zaman damgaları ve JA4/JA4S/JA4X tabanlı davranışsal trafik parmak izi özellikleri yer almaktadır.

Veri etiketleme süreci, saldırı komut dosyalarındaki zaman damgalarının ağ trafiği zaman damgalarıyla senkronize edilmesi yoluyla gerçekleştirildi. Bu, saldırı başlangıç ve bitiş aralıklarının kesin olarak belirlenmesini sağladı ve yanlış etiketleme olasılığını azalttı. Ayrıca, ön işleme aşamasında gereksiz ARP yayın paketleri ve yinelenen kayıtlar filtrelendi.

SCADANet veri kümesi, gerçek endüstriyel kontrol sistemlerinde gözlemlenen doğal trafik dengesizliğini korumak üzere tasarlanmıştır. Flood tabanlı saldırılar daha yüksek

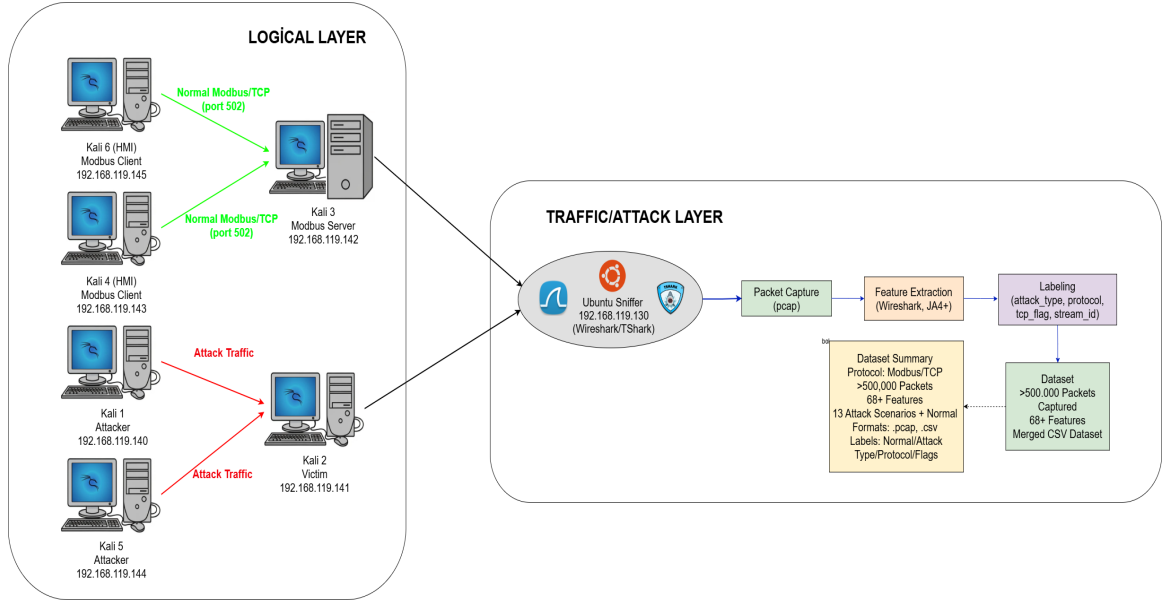
trafik hacmine sahipken, keşif ve SCADA'ya özgü saldırılar daha düşük yoğunluklarda gerçekleşir. Veri kümesinin sınıf dağılımları Tablo 4.1'de sunulmuştur.

Çalışmanın tekrarlanabilirliğini desteklemek için sanal ağ mimarisi, trafik oluşturma süreçleri, saldırı senaryoları, trafik toplama mekanizmaları ve ön işleme adımları ayrıntılı olarak açıklanmıştır. Ayrıca, SCADANet veri seti Kaggle platformu aracılığıyla araştırmacıların kullanımına sunulmuştur. İlgili analiz kodunun da makalenin kabul edilmesinin ardından kamuya açık olarak paylaşılması planlanmaktadır.

Tablo 4.1. SCADANET veri setinin sınıf dağılımı

Trafik Kategorisi	Saldırı Türü	Örnek Sayısı	Yüzde (%)
Normal Trafik	Meşru SCADA İletişimi	82,741	17,00
Flooding (Dağıtık/Yoğunluk) Saldırısı	TCP-SYN Flood	58,214	11,96
Flooding Saldırısı	TCP-ACK Flood	41,325	8,49
Flooding Saldırısı	UDP Flood	52,884	10,86
Flooding Saldırısı	ICMP Flood	44,632	9,17
Flooding Saldırısı	HTTP Flood	36,911	7,58
Web Saldırısı	SQL Enjeksiyonu (SQL Injection)	18,406	3,78
Keşif Saldırısı	Port Tarama	29,154	5,99
Keşif Saldırısı	Zafiyet Tarama	21,486	4,41
Keşif Saldırısı	İşletim Sistemi Tarama	17,632	3,62
SCADA-Özgü Saldırı	Modbus Yanlış Veri Enjeksiyonu	24,870	5,11
SCADA-Özgü Saldırı	Modbus Komut İstimarı	18,995	3,90
Gelişmiş Sürekli Tehdit	APT Veri Sızdırma	22,411	4,60
İç Tehdit	Sabotaj Faaliyeti	17,053	3,50
Toplam		486,714	100

Tablo 4.1’de gösterildiği gibi, SCADANet veri kümesi, endüstriyel kontrol sistemlerinde sıklıkla gözlemlenen doğal trafik düzensizliklerini korumak üzere tasarlanmıştır. Flood tabanlı saldırılar daha yüksek paket yoğunluğu sergilerken, keşif amaçlı saldırılar ve SCADA’ya özgü saldırılar trafik akışı içinde daha düşük yoğunluklarda gerçekleşmektedir. Bu yaklaşım, veri kümesinin gerçekçiliğini artırmaktadır. Ayrıca, gerçekçi SCADA trafik koşulları altında saldırı tespit modellerinin daha güvenilir bir şekilde değerlendirilmesine katkıda bulunmaktadır.



Şekil 4.1. Veri setini elde etmek için oluşturulan sanallaştırılmış SCADA mimarisinin genel tasarımı

Tablo 4.2. Veri kümesini elde etmek için oluşturulan deneysel sanal laboratuvar yapısında kullanılan sanal makineler

Sanal Makineler	Rol	Görev Tanımı	IP Adresi
Ubuntu VM	Dinleyici (Sniffer)	Wireshark ve Tshark kullanarak ağ üzerindeki tüm trafiği pasif olarak yakalamak üzere yapılandırılmıştır.	192.168.119.130
Kali VM 1	Saldırgan	Kötü niyetli faaliyetleri simüle etmek amacıyla saldırı betikleri (scriptleri) çalıştırmıştır.	192.168.119.140
Kali VM 2	Kurban	Bir web sunucusuna ev sahipliği yapmış ve saldırıların ana hedefi olarak işlev görmüştür.	192.168.119.141
Kali VM 3	Modbus Sunucusu	Bir Modbus/TCP sunucusu çalıştırarak bir SCADA saha cihazını simüle etmiştir.	192.168.119.142
Kali VM 4	Modbus İstemcisi	Meşru Modbus trafiği üreten bir SCADA/HMI ana (master) sistemini temsil etmiştir.	192.168.119.143
Kali VM 5	Saldırgan	Farklı kötü niyetli trafik senaryoları oluşturmak için ek saldırı betikleri çalıştırmıştır.	192.168.119.144
Kali VM 6	Modbus İstemcisi	Standart Modbus iletişimi üreten ikinci bir SCADA/HMI ana sistemi olarak görev yapmıştır.	192.168.119.145

Sanal laboratuvar ortamında kullanılan sanal makinelerin rolleri ve görev tanımları Tablo 4.2'de özetlenmiştir.

4.2. Trafik Oluşturma ve İletişim Akışları

Simüle edilmiş ortamda iki temel iletişim akışı tanımlanmıştır. İlk akış, Kali 3 üzerinde çalışan Modbus/TCP sunucusu ile Kali 4 ve Kali 6 üzerindeki Modbus istemcileri arasında kurulan meşru endüstriyel iletişimidir. Bu yapı, gerçek saha ortamlarında gözlemlenen periyodik sorgu-yanıt döngülerini taklit edecek şekilde yapılandırılmıştır. Modbus istemcileri, belirli zaman aralıklarında tutma kaydı, giriş kaydı ve bobin okuma/yazma işlemleri gerçekleştirerek deterministik SCADA trafiği oluşturmuştur.

İkinci akış ise saldırı trafiğidir. Kali 1 ve Kali 5 üzerinde bulunan saldırgan düğümler, Kali 2 üzerinde çalışan hedef sistemi hedef alan çeşitli saldırı senaryoları gerçekleştirmiştir. Tüm bu trafik, normal Modbus iletişimini kesintiye uğratmadan eşzamanlı olarak üretilmiş ve serpiştirilmiştir. Bu yaklaşım, saldırı trafiğinin normal endüstriyel akışa gömülü olduğu gerçekçi trafik modellerinin elde edilmesini sağlamıştır.

Normal trafik oluşturma sırasında, sadece Modbus/TCP iletişimi değil, aynı zamanda endüstriyel ağlarda yaygın olarak gözlemlenen ICMP tabanlı kullanılabilirlik kontrolleri ve HTTP tabanlı hizmet istekleri de arka plan trafiği olarak sisteme dahil edilmiştir. Böylece, ortaya çıkan veri kümesi, tek bir protokole dayalı sentetik bir yapıdan ziyade, çok hizmetli ve heterojen bir SCADA ağını temsil etmektedir.

4.3. Trafik Yakalama ve Özelliklerin Çıkarılması

Ağ trafiği yakalama işlemi, Ubuntu sanal makinesinde çalışan TShark aracı kullanılarak pasif bir şekilde gerçekleştirilmiştir. Her senaryo için ayrı pcapng dosyaları oluşturulmuş ve analiz aşamasında 2. Katman gürültü trafiği (ARP paketleri gibi) filtrelenmiştir.

Yakalanan ham paketler Wireshark ve TShark kullanılarak ayrıştırılmış; çerçeve, IP, TCP/UDP/ICMP ve uygulama katmanlarına ait öznitelikler ayrıntılı olarak çıkarılmıştır. Ek olarak, JA4+ mekanizması kullanılarak oturum ve akış düzeylerinde kriptografik ve davranışsal parmak izi özellikleri elde edilmiştir.

DeneySEL çalışmadan elde edilen SCADANet veri seti, SCADA ağ iletişimlerinin heterojen yapısını temsil etmek amacıyla hem düşük seviyeli paket meta verilerini hem de protokol

bilgisine dayalı trafik özelliklerini içerecek şekilde tasarlanmıştır. Zaman damgaları, protokol tanımlayıcıları, paket uzunlukları, TCP bayrakları, sıra ile ilgili bilgiler ve JA4+ tabanlı trafik parmak izi özellikleri gibi çerçeve düzeyindeki özellikler çıkarılmıştır. Ek olarak, veri seti IP katmanında, TCP/UDP/ICMP katmanında ve uygulama katmanında bulunan öznitelikleri de içermektedir. Ön işlemin ardından, veri seti hem sayısal hem de kategorik trafik özniteliklerini kapsayan yüksek boyutlu özellik temsillerini içerecek şekilde oluşturulmuştur. Boyutluluk ve hesaplama yükünü azaltmak için, ön işleme aşamasında yüksek kardinaliteye ve düşük bilgi içeriğine sahip alanlar kaldırılmıştır. Bununla birlikte, özellik seçimi ve kodlama süreçleri sayesinde trafiğin ayırt edici özellikleri korunmuştur. Geliştirilen bu ön işleme stratejisi, derin öğrenme tabanlı siber saldırı tespiti için uygundur. Sonuç olarak, bu strateji kompakt ve hesaplama açısından verimli özellik temsillerinin oluşturulmasını sağlamıştır.

Bu özellikler, özellikle düşük hacimli ve gizli SCADA saldırılarının tespitinde ayırt edici bilgiler sunmaktadır.

4.4. Etiketleme Süreci

Veri etiketleme süreci, yalnızca bağlantı noktası veya protokol tabanlı sezgisel kurallara dayanmamaktadır. Bunun yerine, saldırı senaryolarını başlatan komut dosyalarının günlük kayıtları ile paket zaman damgaları senkronize edilerek saldırıların başlangıç ve bitiş zamanları kesin olarak belirlenmiştir. Bu yaklaşım, sınıf etiketlerinin doğruluğunu artırmış ve veri setinin çok sınıflı saldırı tespit çalışmalarında güvenilir bir şekilde kullanılabilmesini sağlamıştır.

Sonuç olarak, her paket “normal trafik” veya ilgili saldırı sınıfı olarak etiketlenmiş ve analiz aşamasında kullanılmak üzere CSV formatında yapılandırılmıştır.

4.5. Trafik Oluşturma ve Saldırı Senaryosu Tasarımı

Endüstriyel ortamlarda saldırı tespit mekanizmalarının dayanıklılığını değerlendirmek amacıyla, hem geleneksel bilgi teknolojilerini hedef alan tehditleri hem de endüstriyel kontrol altyapılarını etkileyebilecek saldırıları temsil eden bir siber saldırı senaryosu tasarlanmıştır. Saldırı modelleme süreci, normal endüstriyel iletişim trafiği ile kötü niyetli

faaliyetlerin eşzamanlı olarak üretildiği kontrollü bir sanal SCADA ortamında gerçekleştirilmiştir.

Deneysel çalışmada, SCADA sistemindeki trafik oluşturma süreci iki aşamada gerçekleştirildi. İlk aşamada, normal çalışma koşullarını temsil eden zararsız trafik oluşturuldu ve referans verisi olarak kaydedildi. Bu aşamada, gerçekçi endüstriyel iletişim davranışını yansıtmak için SCADA istemci ve sunucu düğümleri arasında sürekli Modbus/TCP iletişimi oluşturuldu. Bu iletişim, SCADA tabanlı izleme ve kontrol sistemleri ile sahadaki Programlanabilir Mantık Denetleyicileri (Programmable Logic Controllers-PLCs) arasındaki kontrol ve veri alışverişini temsil etmektedir. Ayrıca, endüstriyel ağ ortamlarında yaygın olarak bulunan yardımcı hizmetleri taklit etmek için arka planda ICMP ve HTTP trafiği oluşturulmuştur.

İkinci aşamada, arka planda normal trafik devam ederken çeşitli siber saldırı senaryoları uygulanmıştır. Bu yaklaşım, kötü niyetli faaliyetlerin meşru SCADA iletişim trafiğine gömüldüğü karma trafik ortamlarının oluşturulmasını sağlamıştır. Sonuç olarak, endüstriyel süreçlerin devam ettiği gerçek operasyonel ortamlarda ortaya çıkabilecek saldırı koşulları daha gerçekçi bir şekilde modellenmiştir. Tüm ağ trafiği pasif olarak yakalanmış ve daha sonra analiz ve etiketleme amacıyla kaydedilmiştir.

Uygulanan saldırı senaryoları arasında TCP-SYN Flood, TCP-ACK Flood, UDP Flood, ICMP Flood, HTTP Flood, SQL Injection, Port Scan, Vulnerability Scan ve OS Scan saldırıları yer almaktadır. Bu saldırılar, keşif faaliyetleri, kaynak tüketimi ve uygulama katmanı istismarı gibi farklı tehdit kategorilerini temsil etmek üzere seçilmiştir. Özellikle Port Tarama, Güvenlik Açığı Taraması ve İşletim Sistemi Taraması saldırıları, endüstriyel ağ altyapısı içindeki açık hizmetleri, sistem yapılandırmalarını ve potansiyel güvenlik açıklarını belirlemeyi amaçlayan keşif faaliyetlerini temsil etmektedir. Buna karşılık, TCP-SYN Flood, TCP-ACK Flood, UDP Flood, ICMP Flood ve HTTP Flood saldırıları, ağ bant genişliğini veya sistem kaynaklarını tüketerek kritik SCADA hizmetlerinin kullanılabilirliğini bozmayı amaçlayan Hizmet Engelleme Saldırısı (Denial of Service-DoS) koşullarını simüle etmektedir. SQL Enjeksiyon saldırısı ise, modern sistemlerle entegre web tabanlı yönetim arayüzlerini hedef alan uygulama katmanı istismarını modellemektedir.

Öte yandan, SQL Enjeksiyon saldırısı, modern SCADA izleme sistemleriyle entegre edilmiş web tabanlı yönetim arayüzlerini hedef alan uygulama katmanı istismarlarını simüle etmektedir.

Bu geleneksel Bilgi Teknolojileri (BT) tabanlı tehditlerin yanı sıra, endüstriyel kontrol sistemlerini hedef alan SCADA'ya özgü saldırı senaryoları da deneysel ortama dahil edilmiştir. Bu saldırılar arasında Modbus Yanlış Veri Enjeksiyonu (False Data Injection-FDI), Modbus Komut Kötüye Kullanımı, Advanced Persistent Threat (APT) Veri Çalma ve İçeriden Gelen Tehdit (Sabotaj) yer almaktadır. Modbus Yanlış Veri Enjeksiyonu (FDI) saldırısı, endüstriyel cihazlar ile SCADA sistemleri arasında iletilen proses verilerinin manipülasyonunu simüle ederek, hatalı operasyonel kararlara yol açabilecek durumları temsil eder. Modbus Komut Kötüye Kullanımı saldırısı ise, Modbus protokolü aracılığıyla saha cihazlarına yetkisiz kontrol komutlarının gönderilmesini ifade eder. APT Veri Sızdırma senaryosu, hassas operasyonel verilerin endüstriyel ağ dışına gizli ve uzun süreli olarak sızdırılmasını modellemektedir. İçeriden Gelen Tehdit (Sabotaj) senaryosu ise, sistem operasyonlarını kesintiye uğratmak veya kontrol süreçlerini manipüle etmek amacıyla kötü niyetli davranışlarda bulunan yetkili bir kullanıcıyı temsil etmektedir.

Her saldırı senaryosu, saldırı türüne bağlı olarak 5 ila 20 dakika arasında değişen sürelerde gerçekleştirildi. Keşif saldırıları, gerçekçi tarama davranışını taklit etmek için aralıklarla kısa süreli patlamalar halinde gerçekleştirilirken, sel(flood) tabanlı saldırılar, sürekli anormal trafik modelleri oluşturmak için daha uzun süreler boyunca yürütülmüştür. Öte yandan, SCADA'ya özgü saldırılar, endüstriyel iletişim kanallarıyla doğrudan etkileşime girilerek gerçekleştirilmiş; Bu sayede Modbus tabanlı kontrol trafiğinde meydana gelebilecek anormal komut kalıpları ve veri manipülasyonlarının gözlemlenmesi mümkün olmuştur.

Deneysel çalışmanın bir parçası olarak oluşturulan veri seti, bir normal trafik sınıfı ve on üç farklı saldırı sınıfından oluşan toplam on dört trafik kategorisini içermektedir. Geleneksel ağ saldırılarını aynı endüstriyel iletişim ortamındaki SCADA'ya özgü tehdit senaryolarıyla birleştiren veri seti, endüstriyel kontrol ağları için geliştirilen makine öğrenimi ve derin öğrenme tabanlı saldırı tespit sistemlerini değerlendirmek için kapsamlı bir test ortamı sunmaktadır.

4.6. Önerilen Mimarinin SCADA Odaklı Tasarımı

Bu çalışmada önerilen derin öğrenme tabanlı çok katmanlı mimari, genel ağ saldırı tespit problemlerine uygulanabilir. Ayrıca, bu çalışmada kullanılan deney ortamı ve trafik modelleme yaklaşımı, SCADA sistemlerinin operasyonel özelliklerini yansıtacak şekilde özel olarak tasarlanmıştır. Çalışmada kullanılan veri kümesi, sanal bir ortamda İnsan-Makine Arayüzü (Human-Machine Interface-HMI) sistemleri ile saha cihazları arasındaki iletişimi temsil eden Modbus/TCP tabanlı bir SCADA mimarisinin modellenmesiyle oluşturulmuştur. Bu yapı, endüstriyel izleme ve kontrol süreçlerinde yaygın olarak gözlemlenen deterministik sorgu-yanıt iletişim döngülerini yeniden üretmektedir. Bu iletişim yapısı, geleneksel kurumsal ağ trafiğinden önemli ölçüde farklıdır.

Veri seti, normal meşru operasyonel trafiğin yanı sıra hem geleneksel ağ saldırılarını hem de SCADA sistemlerine özgü tehdit senaryolarını içermektedir. Bu bağlamda, model sadece Modbus Yanlış Veri Enjeksiyonu ve Modbus Komut Kötüye Kullanımı gibi protokol düzeyindeki saldırıları değil, aynı zamanda APT tabanlı veri sızdırma ve içeriden gelen tehditler (sabotaj) gibi daha karmaşık saldırı senaryolarını da içermektedir. Bu tür saldırılar, endüstriyel iletişim süreçlerini ve kontrol komutlarını doğrudan hedef alır ve kritik altyapı sistemlerinde ortaya çıkabilecek gerçekçi siber-fiziksel tehditleri temsil eder. Ayrıca, deney ortamı, saldırı trafiğinin normal Modbus iletişimi ile eşzamanlı olarak üretildiği karma trafik koşullarını yansıtacak şekilde yapılandırılmıştır. Bu, önerilen tespit yaklaşımının gerçekçi çalışma koşulları altında hem normal endüstriyel iletişim davranışını hem de saldırılardan kaynaklanan anormal davranışları öğrenmesini sağlar.

Sonuç olarak, bu çalışmanın katkısı yalnızca çok bileşenli derin öğrenme mimarisiyle sınırlı değildir. Çalışma, SCADA odaklı trafik oluşturma ortamını ve protokol farkındalıklı saldırı modelleme yaklaşımını birleştiren entegre bir saldırı algılama çerçevesi sunması açısından da önemlidir. Bu yaklaşım, endüstriyel kontrol ağları içinde hem genel ağ saldırılarının hem de SCADA'ya özgü anormalliklerin ve tehditlerin algılanmasını sağlar. Ayrıca, SCADA ağlarında saldırı tespiti, paket düzeyinde anomalileri tanımlamakla sınırlı değildir. Endüstriyel kontrol sistemlerinde, ağ trafiği fiziksel süreçlerin izlenmesi ve kontrolüyle doğrudan bağlantılıdır. Sonuç olarak, saldırılar genellikle sadece ağ davranışını değil, aynı zamanda operasyonel kontrol akışını da etkileyen siber-fiziksel anomaliler

şeklinde gerçekleşir. Bu çalışmada kullanılan trafik modelleme yaklaşımı ve deneysel senaryolar, ağ iletişimi ile kontrol süreçleri arasındaki bu ilişkiyi korumak üzere tasarlanmıştır. Sonuç olarak, önerilen mimari sadece genel bilgisayar ağı tabanlı saldırıları değil, aynı zamanda endüstriyel kontrol süreçlerini etkileyebilecek davranışsal anormallikleri de öğrenme yeteneğine sahiptir. Bu sayede önerilen yaklaşım, SCADA sistemleri gibi kritik altyapı ortamlarında ortaya çıkabilecek karmaşık saldırı davranışlarının tespitine katkıda bulunabilmektedir.

4.7. Karşılaştırma için Kullanılan İkinci Veri Kümesi (WUSTL-IIoT-2021)

Bu çalışmada karşılaştırma amacıyla WUSTL-IIoT-2021 veri kümesi de kullanılmıştır. Bu veri kümesi, endüstriyel IoT tabanlı SCADA sistemlerinden gelen ağ trafiğini temsil etmek üzere izole ve sanallaştırılmış bir laboratuvar ortamında oluşturulmuştur. Normal çalışma senaryolarının yanı sıra, saldırı senaryoları da kontrollü bir şekilde oluşturulmuş ve arka plan trafiği korunmuştur.

Veri kümesi, yaklaşık 1,2 milyon ağ akışı kaydı ve 44 ağ/akış tabanlı öznitelik içermektedir. Kayıtlar beş sınıfa ayrılmıştır: normal, Arka Kapı, Komut Enjeksiyonu, Hizmet Reddi ve Keşif. SCADA sistemlerine özgü Komut Enjeksiyonu ve Arka Kapı saldırılarının açık tanımı, veri kümesini endüstriyel siber güvenlik çalışmaları için önemli bir referans haline getirmektedir. Ayrıca, veri setinde gözlemlenen sınıf dengesizliği, nadir saldırıları tespit etmek ve model sağlamlığını değerlendirmek için gerçekçi bir test ortamı sağlar. Bu çalışmada, hem dahili olarak oluşturulan bir veri seti hem de literatürde yaygın olarak kullanılan bir harici veri seti üzerinde modelin performansını değerlendirmek için iki farklı veri seti kullanılmıştır:

- SCADANet Veri Seti: Çalışma kapsamında toplanan, farklı sınıflardan örnekler içeren orijinal bir veri seti.
- WUSTL-IIoT-2021 (Teixeira vd., 2021): Literatürde sıklıkla kullanılan, yüksek sınıf çeşitliliğine ve daha heterojen bir yapıya sahip bir veri seti.

Her iki veri kümesinde de, tüm örnekler yöntemler bölümünde açıklandığı üzere standart ön işleme adımlarından (ölçeklendirme, etiket kodlama, yeniden şekillendirme vb.) geçirildi.

Modelin güvenilir ve istatistiksel olarak anlamlı bir şekilde değerlendirilmesini sağlamak için, tüm deneylerde 5 katlı çapraz doğrulama yöntemi kullanılmıştır. Buna göre, veri kümesi sınıf dağılımını koruyarak beş eşit alt bölüme ayrılmıştır; her deney döngüsünde, bu alt bölümlerden biri test kümesi olarak belirlenirken, kalan dördü eğitim için kullanılmıştır. Tüm katmanlar tamamlandıktan sonra, her bir katmandan elde edilen performans değerleri birleştirildi ve metriklerin aritmetik ortalaması ve standart sapması hesaplanarak nihai sonuçlar rapor edildi. Bu yaklaşım, farklı veri alt kümeleri arasında modelin kararlılığını, genelleştirilebilirliğini ve istatistiksel güvenilirliğini sağlamayı amaçlamaktadır.

Model, tüm deneylerde aynı hiperparametreler, aynı eğitim stratejisi ve aynı veri bölme protokolü kullanılarak eğitildi, böylece modeller arasında tutarlı bir karşılaştırma temeli sağlandı.

4.8. Dengesiz Veri Sorununun Ele Alınması

Veri kümelerindeki sınıflar arasında önemli bir dengesizlik olması nedeniyle, azınlık sınıfların temsil edilebilirliğini artırmak ve modelin bu sınıflara karşı duyarlılığını geliştirmek amacıyla iki aşamalı bir kayıp optimizasyon stratejisi uygulandı. Bu bağlamda, öncelikle Focal Loss kullanılarak sık karşılaşılan sınıflara ait kolay örneklerin kayıp fonksiyonu üzerindeki etkisi azaltıldı; böylece modelin daha zor örnekler ve azınlık sınıflara odaklanması sağlandı. Ek olarak, her sınıfın eğitim sürecine katkısını dengelemek için sınıf ağırlıkları tanımlandı; bu ağırlıklar, ilgili sınıftaki örnek sayısının tersi ile orantılı olarak belirlendi, böylece nadir sınıfların toplam kayıp üzerindeki etkisi artırıldı. Bu iki yönlü yaklaşım, dengesiz veri sorunundan kaynaklanan önyargıları azalttı ve özellikle örneklem büyüklüğü düşük sınıflar için modelin öğrenme kapasitesini önemli ölçüde güçlendirdi.

Dengesiz veri sorununa yönelik bu iki aşamalı yaklaşım, özellikle küçük örneklem boyutlarına sahip sınıflar için hem geri çağırma hem de F1 puanında önemli iyileştirmeler sağladı.

4.9. Değerlendirme Ölçütleri

Modelin performansı, yalnızca doğruluk temelinde değil, sınıf dengesizliğinin etkilerini daha doğru bir şekilde yansıtmak amacıyla Denklem 4.1– 4.4’de belirtilen ölçütler kullanılarak da değerlendirildi.

$$\text{Doğruluk(Accuracy)} = (TP + TN) / (TP + TN + FP + FN) \quad (4.1)$$

$$\text{Kesinlik(Precision)} = TP / (TP + FP) \quad (4.2)$$

$$\text{Duyarlılık(Recall)} = TP / (TP + FN) \quad (4.3)$$

$$\text{F1 – Skoru(F1 – Score)} = (2 \times \text{Kesinlik} \times \text{Duyarlılık}) / (\text{Kesinlik} + \text{Duyarlılık}) \quad (4.4)$$

Bu metriklerde TP, doğru pozitifleri; TN, doğru negatifleri; FP, yanlış pozitifleri; FN ise yanlış negatifleri temsil eder. Bu dört temel terim, Doğruluk, Hassasiyet(Precision), Geri Çağırma(Recall), F1 puanı ve Karmaşıklık Matrisi(Confusion Matrix) hesaplamalarının temelini oluşturur. Bu metrikler hem sınıf bazında hem de ortalama (makro/ağırlıklı) olarak hesaplanmıştır; katlamalar genelinde metriklerin ortalama ve standart sapma değerleri tablolarda sunulmuştur. Sınıflar arasındaki karışıklığı ayrıntılı olarak göstermek için karışıklık matrisleri şekillerde sunulmuştur.

4.10. SCADANet Veri Kümesinde Elde Edilen Sonuçlar

Deneysel çalışmalardan elde edilen SCADANet veri seti üzerinde gerçekleştirilen beş katlı çapraz doğrulama deneyleri, önerilen modelin hem yüksek genelleme performansına hem de sınıflar arası ayrımı etkin bir şekilde gerçekleştirebilen güçlü bir temsil kapasitesine sahip olduğunu göstermektedir. Çok ölçekli özellik çıkarımı sağlayan genişletilmiş CNN yapılarının entegre kullanımı, kanal düzeyinde dikkat mekanizmaları ve dönüştürülmüş SCADA trafik temsilindeki özellik düzeyinde sıralı ve bağlamsal ilişkileri modelleyen

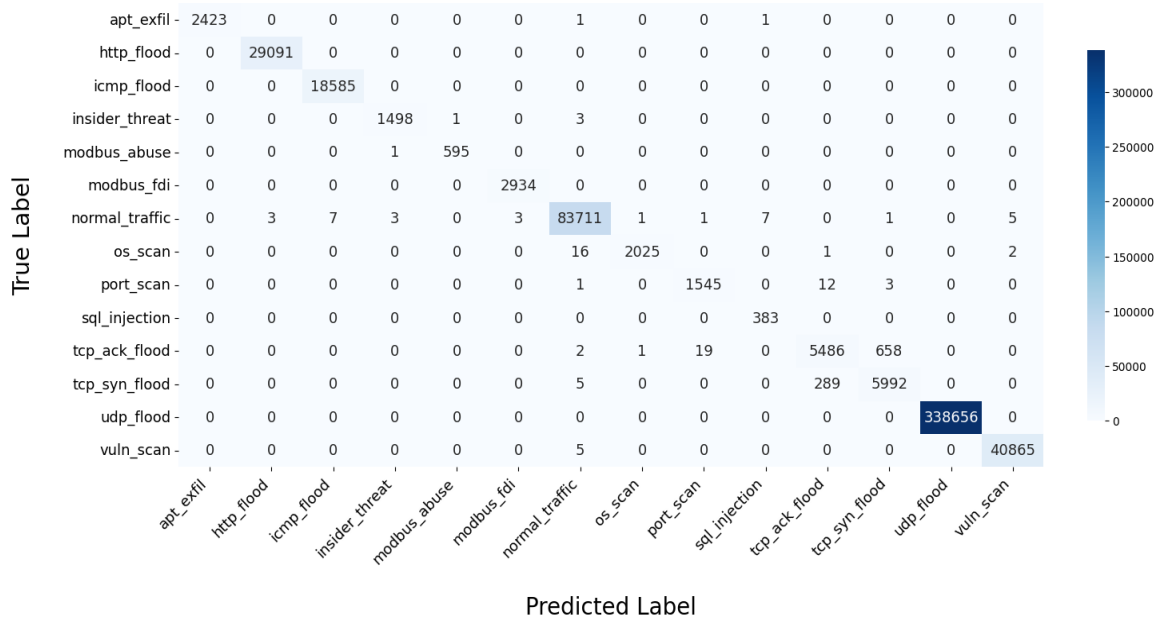
LSTM katmanları, veri setinde gözlemlenen belirgin sınıf dengesizliğine rağmen modelin istikrarlı ve tutarlı bir performans sergilemesini sağlamıştır. Modelin SCADANet veri seti üzerindeki 5 katlı ortalama performans ölçütleri Tablo 4.3'te sunulmuştur.

Tablo 4.3. SCADANet Veri Kümesi için 5 Katlı Ortalama Performans Sonuçları

Metrik	Değer
Ortalama Doğruluk	99,80
Makro Hassasiyet	98,63
Makro Geri Çağırma	98,70
Makro F1-Skoru	97,65

Tablo 4.3'te görüldüğü üzere, önerilen model %99,80 ortalama doğruluk değerine ulaşmış olup bu sonuç, beş katlı çapraz doğrulama boyunca oldukça kararlı ve tutarlı bir sınıflandırma başarımı sergilendiğine işaret etmektedir. Yüksek makro ortalamalı metrikler, modelin yalnızca çoğunluk sınıflarına odaklanmadığını, görece daha düşük örnek sayısına sahip sınıflardaki örüntüleri de etkili biçimde öğrenebildiğini göstermektedir. Özellikle %98,70'lik Makro Duyarlılık (Macro Recall) değeri, modelin azınlık sınıflarına ait örneklerin büyük bir bölümünü başarıyla yakaladığını ortaya koymakta ve nadir görülen saldırı kategorilerine yönelik güçlü duyarlılığın vurgulamaktadır. Bunun yanı sıra, %98,63'lük Makro Kesinlik (Macro Precision) değeri, modelin farklı saldırı sınıfları genelinde düşük bir yanlış pozitif oranını koruduğunu ve dolayısıyla normal trafik ile çok sayıda saldırı türü arasında güvenilir bir ayırım sağladığını göstermektedir. Kesinlik ve duyarlılığı dengeleyen %97,65'lik Makro F1 skoru ise modelin tüm sınıflar genelinde güçlü ve dengeli bir sınıflandırma başarımı elde ettiğini doğrulamaktadır. Genel olarak bu sonuçlar, önerilen mimarinin SCADANet veri kümesinin temelindeki dağılımı etkili biçimde temsil edebildiğini; çok sınıflı ve orta düzeyde dengesiz trafik koşulları altında yüksek sınıflandırma doğruluğunu ve dengeli başarımı koruyabildiğini ortaya koymaktadır.

Beş katın tüm test sonuçlarının birleştirilmesiyle elde edilen karmaşıklık matrisi Şekil 4.2'de gösterilmiştir. Bu matris, modelin sınıflar arasındaki karışıklık düzeylerinin ayrıntılı bir şekilde incelenmesine olanak tanır ve özellikle sınıf dengesizliğinin yoğun olduğu durumlarda hataların sınıflar arasında nasıl dağıldığını açıkça gösterir.



Şekil 4.2. SCADANet Veri Kümesi için 5 Katlı Birleşik Karmaşıklık Matrisi

Şekil 4.2’de sunulan 5 katlı birleştirilmiş karmaşıklık matrisi, modelin sınıfa dayalı karar verme davranışını ve hataların sınıflar arasında hangi noktalarda yoğunlaştığını açıkça göstermektedir. Matris incelendiğinde, özellikle örneklem büyüklüğü yüksek sınıflarda köşegen üzerindeki değerlerin baskın olduğu ve köşegen dışı hataların çok sınırlı olduğu gözlemlenmektedir; bu durum, modelin bu sınıflarla ilişkili ayırt edici kalıpları güçlü bir şekilde öğrendiğini göstermektedir. Azınlık sınıflardaki düşük yanlış negatif (False Negative-FN) değerleri, dengesiz veri sorununu çözmek için kullanılan Focal Loss + sınıf ağırlıkları stratejisinin istenen etkiyi sağladığını ve modelin kritik örnekleri gözden kaçırma eğilimini azalttığını göstermektedir. Öte yandan, sınıf karışıklıklarının rastgele dağılmadığı, aksine birbirlerine yapısal olarak yakın sayılabilecek belirli sınıf çiftleri arasında kümелendiği gözlemlenmektedir (örneğin, bazı sınıflarda komşu sınıflara kaymalar). Bu bulgu, modelin genel olarak karar sınırlarını net bir şekilde öğrendiğini, ancak benzer sınıflar arasında sınırlı örtüşme olan kalıpların hatalara neden olabileceğini göstermektedir. Genel olarak, Şekil 4.2, modelin çoğunluk sınıflarında yüksek doğrulukla performans gösterirken azınlık sınıflarında da duyarlılığını koruduğunu ve dengeli bir hata profili sergilediğini doğrulamaktadır.

4.11. WUSTL-IIoT-2021 Veri Seti Üzerinde Elde Edilen Sonuçlar

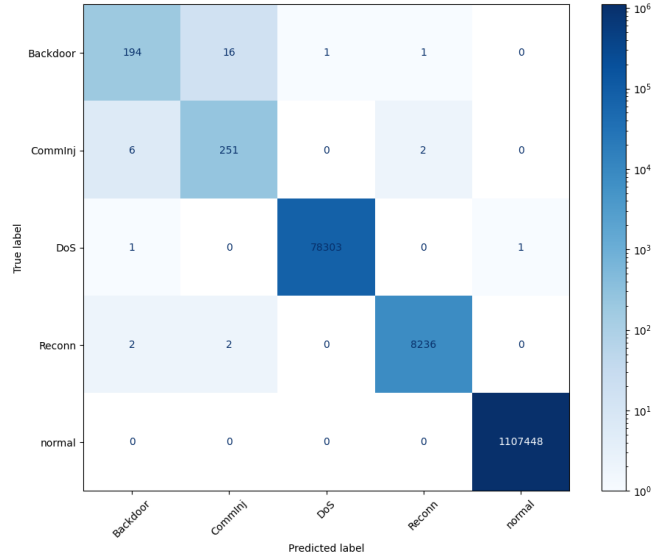
WUSTL-IIoT-2021 veri kümesi üzerinde gerçekleştirilen beş katlı çapraz doğrulama deneyleri, önerilen modelin farklı veri dağılımlarında yüksek istikrar sergilediğini ve güçlü genelleme yeteneklerine sahip olduğunu göstermektedir. WUSTL-IIoT-2021 veri setinin sınıf dağılımı, birincil veri setine kıyasla daha heterojen bir yapı sergilese de, modelin öğrenme kapasitesinin ve dengesiz veri sorununu ele almak için uygulanan stratejilerin bu veri setinde de etkili olduğu gözlemlenmiştir. Modelin WUSTL-IIoT-2021 veri seti üzerindeki 5 katlı ortalama performans ölçütleri Tablo 4.4'te sunulmuştur.

Tablo 4.4. WUSTL-IIoT-2021 Veri Kümesi için 5 Katlı Ortalama Performans Sonuçları

Metrik	Değer (%)
Ortalama Doğruluk	99,9973
Ortalama Makro Hassasiyet	97,79
Ortalama Makro Geri Çağırma	97,68
Ortalama Makro F1-Skoru	97,70
Ortalama Ağırlıklandırılmış Hassasiyet	99,9973
Ortalama Ağırlıklandırılmış Geri Çağırma	99,9973
Ortalama Ağırlıklandırılmış F1-Skor	99,9973

Tablo 4.4'te sunulan sonuçlar, önerilen modelin yalnızca veri setinin çoğunluk sınıflarında değil, aynı zamanda daha küçük örneklem büyüklüğüne sahip sınıflarda da yüksek ve dengeli bir performans sergilediğini göstermektedir. Makro ortalama Hassasiyet, Geri Çağırma ve F1 puanı değerlerinin %97'nin üzerinde olması, tüm sınıfların eşit katkı sağladığı bir değerlendirme ortamında bile modelin güçlü bir ayırt etme kapasitesine sahip olduğunu ortaya koymaktadır. Buna karşılık, tüm ağırlıklı ortalama metriklerin %99,9973 seviyesinde olması, modelin çoğunluk sınıfının dağılımını neredeyse kusursuz bir şekilde temsil edebildiğini ve genel sınıflandırma doğruluğunun olağanüstü yüksek olduğunu göstermektedir.

Tüm katların test sonuçlarının birleştirilmesiyle elde edilen karmaşıklık matrisi Şekil 4.3'te sunulmuştur. Bu matris, modelin sınıflar arasındaki karışıklık düzeylerinin ayrıntılı bir şekilde incelenmesine olanak tanır.



Şekil 4.3. WUSTL-IIoT-2021 Veri Kümesi için 5 Katlı Birleşik Karmaşıklık Matrisi

Şekil 4.3'te sunulan karmaşıklık matrisi incelendiğinde, modelin hem küçük hem de büyük örneklem sınıflarında son derece yüksek bir doğrulukla çalıştığı açıkça görülmektedir. Özellikle çoğunluk sınıfında, 1,1 milyondan fazla örneğin neredeyse tamamının doğru bir şekilde sınıflandırılmış olması, modelin yüksek temsil gücünü ve ayırt edici kapasitesini ortaya koymaktadır. Orta büyüklükteki sınıflarda ise hata oranları ihmal edilebilir düzeyde kalmakta ve yalnızca sınırlı sayıda yanlış pozitif veya yanlış negatif gözlemlenmektedir. Örneklem büyüklüğü daha düşük olan sınıflarda bile, yanlış negatif değerler minimum seviyede kalmaktadır; bu da modelin kritik sınıfları gözden kaçırmadığını ve yüksek duyarlılık sunduğunu göstermektedir. Genel olarak, son derece düşük yanlış sınıflandırma seviyesi, sınıflar arasındaki karar sınırlarının net ve tutarlı bir şekilde öğrenildiğini teyit etmektedir.

Bu bulgular bir arada değerlendirildiğinde, WUSTL-IIoT-2021 veri setinde elde edilen sonuçlar, önerilen modelin yalnızca eğitim sürecinde kullanılan veri setine değil, aynı zamanda farklı dağılımlara sahip harici veri setlerine de yüksek düzeyde genelleştirilebilirlik sunduğunu açıkça göstermektedir. Yüksek makro ortalama metrikler, azınlık sınıflarının güçlü bir şekilde temsil edildiğini gösterirken, ağırlıklı ortalama metriklerde elde edilen neredeyse kusursuz sonuçlar, modelin genel sınıflandırma istikrarını ve güvenilirliğini teyit etmektedir. Karmaşıklık matrisindeki düşük hata oranları göz önüne alındığında, önerilen yaklaşımın farklı veri kaynakları için ölçeklenebilir, güvenilir ve istikrarlı bir sınıflandırma çözümü sunduğu söylenebilir.

4.12. Ablasyon Çalışması

Önerilen mimarideki temel bileşenlerin sınıflandırma performansına katkısını nicel olarak ortaya koymak amacıyla, ablasyon çalışması yalnızca bu çalışma kapsamında geliştirilen orijinal SCADANet üzerinde gerçekleştirilmiştir. Bu bağlamda, model mimarisi belirli bileşenler devre dışı bırakılarak sistematik olarak yeniden eğitilmiş ve her bir yapılandırmanın performansı karşılaştırmalı olarak analiz edilmiştir. Böylelikle, her bir modülün çok ölçekli uzamsal temsile ve özellik düzeyinde sıralı/bağlamsal ilişki modellemesine katkısı ayrı ayrı değerlendirilebilmiştir.

Ablasyon çalışmasında değerlendirilen model konfigürasyonları aşağıda listelenmiştir:

- Tüm bileşenleri içeren önerilen model (ALL modeli),
- Residual ve SE blokları kaldırılmış model (Res-SE Bloğu Olmadan),
- LSTM tabanlı özellik düzeyinde sıralı modelleme bileşeni kaldırılmış model (LSTM Olmadan),
- Çok ölçekli özellik çıkarımı sağlayan genişletilmiş CNN yapısı kaldırılmış model (Genişletilmiş CNN Olmadan). Elde edilen performans sonuçları Tablo 4.5'te sunulmuştur.

Tablo 4.5. Ablasyon çalışması sonuçları

Model Konfigurasyonu	Doğruluk	Hassasiyet	Geri Çağırma	F1-Skoru
Tüm Modeller	99,80	98,63	98,70	98,65
Res-SE Blok Kullanılmadan	99,74	98,31	98,34	98,30
Dilated CNN Kullanılmadan	99,67	97,75	97,94	97,84
LSTM Kullanılmadan	99,59	97,29	97,38	97,33

Tablo 4.5'te sunulan ablasyon sonuçları, tüm mimari bileşenlerin aktif olduğu ALL model yapılandırmasının tüm performans ölçütleri açısından en yüksek değerlere ulaştığını açıkça göstermektedir. Model, %99,80 doğruluk, %98,63 kesinlik, %98,70 geri çağırma ve %98,65 F1 puanı elde ederek entegre mimarinin etkinliğini teyit etmektedir. Bu bulgu, bileşenler arasındaki etkileşimi dikkate alan önerilen mimarinin bütünsel tasarımının, sınıflandırma performansına anlamlı ve tutarlı katkılar sağladığını göstermektedir.

Ablasyon çalışması kapsamında farklı mimari bileşenleri devre dışı bırakılarak elde edilen bulgular şu şekilde özetlenmiştir:

- Residual ve SE blokları kaldırıldığında, tüm performans metriklerinde bir düşüş gözlemlenmiştir; model %99,74 doğruluk, %98,31 kesinlik, %98,34 geri çağırma ve %98,30 F1 skoru elde etmiştir. Bu, derin ağ mimarilerinde ayırt edici özellikleri vurgulamak ve bilgi akışını korumak için kanal düzeyindeki dikkat mekanizmalarının kritik rolünü açıkça göstermektedir. Bu bileşenlerin devre dışı bırakılması, modelin ayırt edici temsil kapasitesini sınırlamış ve sınıflar arası karar sınırlarının daha zayıf öğrenilmesine neden olmuştur.

- LSTM katmanının kaldırılması, test edilen yapılandırmalar arasında en belirgin düşüşe neden olmuş ve performansı %99,59 doğruluk, %97,29 kesinlik, %97,38 geri çağırma ve %97,33 F1 puanı seviyesine indirmiştir. Bu bulgu, LSTM yapısının, dönüştürülmüş SCADA trafik temsiliinde özellik düzeyindeki sıralı ve bağlamsal ilişkilerin etkili bir şekilde modellenmesine önemli bir katkı sağladığını göstermektedir. Trafikten türetilen öznitelikler arasında sıralı bağlamsal bilgilerin modele aktarılamaması, özellikle azınlık sınıflara ait örneklerin yakalama oranını düşürerek, yanlış negatiflerin artmasına yol açmıştır.

- Dilated CNN mimarisi kaldırıldığında, model performansı %99,67 doğruluk, %97,75 kesinlik, %97,94 geri çağırma ve %97,84 F1 skoru seviyesine düşmektedir. Bu, modelin çok ölçekli uzamsal kalıpları temsil etme yeteneğinin önemli ölçüde zayıfladığını göstermektedir. Daha geniş bir alıcı alan sağlayan bu mimari olmadan, model farklı ölçeklerde ortaya çıkan karmaşık yapıları ayırt etme konusunda daha az yetenekli hale gelmiştir.

Genel olarak, ablasyon çalışması, her bir mimari bileşenin nihai model performansına olumlu katkı sağladığını açıkça göstermektedir. Çok ölçekli uzamsal özellik çıkarma (Dilated CNN), kanal bazlı dikkat mekanizmaları (SE blokları) ve özellik düzeyinde sıralı/baglamsal ilişki modellemesi (LSTM) kombinasyonu, modelin farklı saldırı sınıfları arasında dengeli bir algılama yeteneğini korurken yüksek doğruluk (%99,80) ve güçlü makro düzeyde sınıflandırma performansı (F1 puanı: %98,65) elde etmesini sağlar.

Elde edilen genel doğruluk değerleri oldukça yüksek olsa da, ablasyon analizi, modelin performansının önemsiz sınıf ayrılabilirliği veya veri kümesi önyargısından

kaynaklanmadığını gösteren ek kanıtlar sunmaktadır. Kilit mimari bileşenler kaldırıldığında gözlemlenen tutarlı ve sistematik performans düşüşü, sınıflandırma başarısının büyük ölçüde çok ölçekli uzamsal modelleme, kanal düzeyinde dikkat mekanizmaları ve özellik düzeyinde sıralı/bağlamsal ilişki öğrenmesine bağlı olduğunu göstermektedir. Ayrıca, tüm sonuçlar tek bir eğitim-test bölünmesi yerine 5 kat çapraz doğrulama ortalamalarıdır; bu da olumlu bölünme etkilerinin olasılığını azaltır. Farklı trafik özelliklerine sahip WUSTL-IIoT-2021 veri seti üzerinde yapılan ek doğrulama, bildirilen performansın kontrollü deneysel ortamlara özgü yapay ayrılabilirlikten ziyade gerçek temsil öğrenimini yansıttığı fikrini daha da desteklemektedir. Bununla birlikte, modeli tam olarak işleyen endüstriyel ortamlarda doğrulamanın gelecekteki araştırmalar için önemli bir yön olduğunu kabul ediyoruz.

4.13. Hesaplama Karmaşıklığı ve Uygulama Olanakları

Önerilen hibrit mimari, üç adet paralel genişletilmiş tek boyutlu evrişimli (Conv1D) dalı, Squeeze-and-Excitation (SE) kanal dikkat mekanizmasıyla geliştirilmiş bir Residual bloğu ve tek katmanlı bir Uzun Kısa Vadeli Bellek (LSTM) birimini bir araya getirir. Endüstriyel siber güvenlik uygulamalarında donanım kısıtlamaları söz konusu olabileceğinden, hesaplama ayak izi ve uygulama fizibilitesinin analiz edilmesi büyük önem taşımaktadır. L , giriş dizisi uzunluğunu (yani, tek boyutlu bir dizi olarak temsil edilen sayısal trafik özelliklerinin sayısını) temsil etsin. Çekirdek boyutu K , giriş kanalı boyutu C_{in} ve çıkış kanalı boyutu C_{out} olan bir Conv1D katmanı için, eğitilebilir parametrelerin sayısı şöyledir:

$$P_{Conv1D} = K \cdot C_{in} \cdot C_{out} + C_{out} \quad (4.5)$$

burada ikinci terim, önyargı parametrelerine karşılık gelir. Uygulanan modelde, her trafik örneği tek kanallı bir özellik dizisi olarak modellenmiş olduğundan $C_{in} = 1$ 'dir.

Çok ölçekli uzamsal kalıpları yakalamak için üç paralel genişletilmiş Conv1D katmanı (çekirdek boyutu $K=3$, $C_{out}=64$) kullanılır. Genişletme, parametre sayısını artırmadan alıcı alanı genişletir. Çıktıları birleştirilir ve 1×1 Conv1D katmanı kullanılarak 64 kanala geri yansıtılır; bu, temsil kapasitesini korurken boyutlulukları verimli bir şekilde azaltır.

Residual-SE bloğu, 64 giriş ve çıkış kanalına sahip iki Conv1D katmanı içerir. Gömülü SE mekanizması, $r = 8$ azaltma oranına sahip bir darboğaz yapısı(bottleneck structure) kullanarak kanal bazında yeniden kalibrasyon gerçekleştirir. Bu dikkat modülü, özellik seçiciliğini artırsa da, evrişimli bileşenlere göre yalnızca sınırlı sayıda ek parametre getirir. LSTM katmanı için, D 'yi giriş özellik boyutunu (burada $D=64$) ve H 'yi gizli birim sayısını (burada $H=128$) temsil etsin. LSTM parametrelerinin toplam sayısı şöyledir:

$$P_{LSTM} = 4(DH + H^2 + H) \quad (4.6)$$

Bu, LSTM mimarisinin dört iç geçit mekanizmasını yansıtır.

Ampirik model incelemesi, tam mimarinin toplam 156.818 parametre (156.178'i eğitilebilir) içerdiğini ve bunun tek hassasiyetli kayan nokta gösteriminde (FP32) yaklaşık 0,60 MB, yarı hassasiyetli gösterimde (FP16) ise 0,30 MB bellek kullanımına karşılık geldiğini göstermektedir. Bu değerler, önerilen mimarinin ağ saldırı tespitinde kullanılan birçok çağdaş derin öğrenme modeline kıyasla hafif olduğunu göstermektedir.

Hesaplama açısından, evrişimli katmanlar yaklaşık olarak $O(L \cdot K \cdot C_{in} \cdot C_{out})$ ile ölçeklenirken, LSTM katmanı $O(L \cdot H^2)$ ile ölçeklenir. Orta büyüklükteki çekirdek boyutları, sınırlı kanal boyutları ve tek katmanlı özellik düzeyinde sıralı/bağlamsal modelleme göz önüne alındığında, genel hesaplama talepleri kontrol altında kalmaktadır. Pratik dağıtım senaryolarında, SCADA saldırı tespit mekanizmaları genellikle denetim izleme düğümlerinde, endüstriyel uç ağ geçitlerinde veya trafik toplama ve denetiminin gerçekleştiği özel saldırı tespit sistemlerinde konumlandırılır. Önerilen mimarinin hafif parametre ölçeği ve mütevazı bellek ayak izi, bu tür dağıtım katmanları için uygulanabilirliği desteklemektedir. Daha fazla kaynak azaltımı gerektiren senaryolar için, hesaplama yükünü daha da en aza indirmek amacıyla yapılandırılmış budama, niceleme, karışık hassasiyetli çıkarım veya bilgi damıtma gibi model optimizasyon stratejileri uygulanabilir. Genel olarak, bu mimari endüstriyel izleme altyapıları içinde temsil kapasitesi ile dağıtım pratikliği arasında dengeli bir denge sağlamaktadır.

Bu bağlamda, gerçek SCADA ortamlarında kullanılan saldırı tespit sistemleri, kontrolörler ile saha cihazları arasındaki deterministik iletişim döngüleri nedeniyle düşük gecikmeli ve

gerçek zamanlı izleme gereksinimlerini karşılamalıdır. Literatür taraması, özellikle operasyonel kesintileri önlemek için hızlı çıkarımın gerekli olduğu durumlarda, hesaplama açısından hafif ve verimli makine öğrenimi veya derin öğrenme modellerinin endüstriyel ortamlarda dağıtım için daha uygun olduğunu göstermektedir. Bu tür modeller, uç ağ geçitlerinde veya daha üst düzey izleme düğümlerinde etkili bir şekilde çalışabilir. Ayrıca literatür, AI tabanlı saldırı tespit sistemlerinin endüstriyel izleme platformları veya SIEM altyapıları ile entegre edilmesinin, SCADA gibi kritik altyapılarda durumsal farkındalığı artırarak tehditlerin daha erken tespit edilmesine katkıda bulunduğunu vurgulamaktadır. Bu nedenle, önerilen modelin düşük hesaplama yükü ve ölçeklenebilir mimarisi, SCADA izleme altyapıları içinde gerçek zamanlı ağ trafiği analizini desteklemek için son derece uygundur. Ayrıca, önerilen model, endüstriyel siber güvenlik sistemlerini daha dayanıklı hale getirmeye katkıda bulunma potansiyeline sahiptir.

4.14. Karar Analizi Modeli

Açıklanabilirlik, operatörlerin güven, olay analizi ve uyumluluk odaklı raporlama için şeffaf bir mantık akışına ihtiyaç duyduğu SCADA tabanlı kritik altyapı bağlamlarında hayati öneme sahiptir. Bu nedenle, tahmine dayalı performans değerlendirmesinin yanı sıra, modelin kararlarına özellik düzeyinde yapılan katkıları nicel olarak belirlemek amacıyla SHAP tabanlı bir sonradan açıklanabilirlik analizi gerçekleştirdik.

Özellikle, SHAP (SHapley Additive exPlanations), eğitilmiş model çıktıları üzerinde özellik atıf puanlarını hesaplamak için kullanılmıştır. Genel önem profili, analiz edilen örnekler ve sınıflar genelinde ortalama mutlak SHAP değerlerinin toplanmasıyla elde edilmiştir. Sonuçlar, modelin tahminlerinin ağırlıklı olarak protokol düzeyindeki özellikler ve ağ trafiğindeki paket düzeyindeki yapısal özellikler tarafından yönlendirildiğini göstermektedir.

En etkili değişkenler arasında, Udp_length en yüksek atıf değerini gösterirken, onu frame_len, Tcp_stream, Tcp_src_port ve Time izlemektedir. Bu özellikler, modelin normal ve kötü niyetli trafiği ayırt ederken paket boyutu özelliklerine ve oturum düzeyindeki TCP davranışına büyük ölçüde dayandığını göstermektedir. Ayrıca, Tcp_len, Tcp_seq, Tcp_window_size ve Tcp_ack gibi taşıma katmanı göstergeleri de modelin karar verme

sürecine önemli ölçüde katkıda bulunmaktadır. Ayrıca, `Icmp_type`, `Udp_srcport` ve `Udp_dstport` gibi protokole özgü özellikler önemli açıklayıcı değişkenler arasında yer almakta olup, bu durum modelin farklı iletişim protokolleriyle ilişkili kendine özgü kalıpları yakaladığını göstermektedir. `Frame_time_delta` gibi zamansal özellikler de açıklama profiline katkıda bulunmakta ve modelin trafik zamanlama davranışlarıyla ilgili anomalileri tespit edebildiğini göstermektedir.

Bu atıf kalıpları, kötü niyetli faaliyetlerin sıklıkla anormal paket boyutu dağılımları, olağandışı aktarım katmanları davranışları ve düzensiz oturum dinamikleri yoluyla ortaya çıktığı endüstriyel ağ trafiğindeki saldırı kaynaklı sapmalarla tutarlıdır. Genel olarak, SHAP analizi, önerilen mimarinin sahte korelasyonlara dayanmak yerine alanla ilgili trafik özelliklerini yakaladığına dair yorumlanabilir kanıtlar sunmaktadır.

4.15. Gerçek Zamanlı Uygulanabilirlik

SCADA tabanlı kritik altyapı sistemlerinde gerçek zamanlı çalışabilirlik hayati bir gerekliliktir. Bu nedenle, bu çalışmada önerilen mimari yalnızca sınıflandırma performansı açısından değerlendirilmemiştir. Aynı zamanda hesaplama verimliliği ve uygulama uygulanabilirliği açısından da değerlendirilmiştir. Literatür taraması, düşük gecikme süresine ve makul hesaplama maliyetlerine sahip hafif derin öğrenme modellerinin endüstriyel ortamlar için daha uygun olduğunu vurgulamaktadır. Özellikle, CNN'lere ve LSTM'lere dayalı hibrit mimarilerin, yüksek parametrelili Transformer tabanlı modellere göre avantajlar sunduğu belirtilmektedir.

Bu çalışmada önerilen mimari, paralel genişletilmiş Conv1D katmanları, Residual-SE blokları ve LSTM bileşenlerinden oluşmaktadır. Mimari tasarım süreci sırasında, çok ölçekli özellik çıkarma kapasitesi korunmuştur. Ek olarak, amaç hesaplama karmaşıklığını dengelemektir. Bu amaçla, Batch Normalization, 1×1 Conv1D ve Global Average Pooling katmanları kullanılarak parametre artışı sınırlandırılmıştır. Eğitim süreci, CUDA ile hızlandırılmış GPU'lar kullanılarak gerçekleştirilmiştir.

SCADANet ve WUSTL-IIoT-2021 veri kümelerinden elde edilen deneysel çalışmanın sonuçları, önerilen yaklaşımın yüksek doğruluk ve dengeli sınıflandırma performansı

sunduğunu açıkça göstermektedir. Özellikle, yüksek Makro Geri Çağırma ve Makro F1 puanı değerleri, modelin düşük yoğunluklu saldırı sınıflarında bile etkili sonuçlar üretebileceğini göstermektedir. Buna ek olarak, paralel genişletilmiş CNN mimarisinin hem kısa hem de uzun vadeli trafik modellerini aynı anda modelleme yeteneği, gerçek zamanlı SCADA saldırı tespitinde önemli bir avantaj sağlar.

Ayrıca, gerçek endüstriyel ortamlarda ortaya çıkabilecek donanım kısıtlamaları, ağ gecikmeleri ve heterojen saha cihazları gibi operasyonel faktörlerin sistem performansını etkileyebileceği değerlendirilmektedir. Bu nedenle, önerilen yaklaşımın çeşitli donanım koşulları altında, özellikle uç ağ geçitlerinde ve gerçek zamanlı SCADA izleme altyapılarında test edilmesi, önemli bir araştırma alanı olarak kabul edilmektedir.

5. LİTERATÜRDEKİ GÜNCEL ÇALIŞMALARLA KARŞILAŞTIRMA

Tablo 5.1, endüstriyel kontrol sistemlerinde saldırı tespit çalışmalarına yönelik literatürde en sık kullanılan veri kümelerini listelemektedir. Tablo ayrıca, bu veri kümeleri kullanılarak yürütülen son dönem çalışmaları ile bu çalışmalarda uygulanan makine öğrenimi yaklaşımlarını da göstermektedir. Literatürdeki en son çalışmaların incelenmesi, SWAT veri setinde GAN(Generative Adversarial Network)-LSTM(Long Short-Term Memory) kullanılarak %87 doğruluk, WADI veri setinde GAT tabanlı bir yöntem kullanılarak %86,69 hassasiyet ve BATADAL ile MSU veri setlerinde sırasıyla %96,93 ve %96,6 doğruluk değerleri elde edildiğini ortaya koymaktadır. Random Forest (RF) ve Support Vector Machine (SVM) yöntemleri, Modbus tabanlı CIC-Modbus veri setinde yaklaşık %95 doğruluk elde ederken, IIoT veri setleri üzerinde yürütülen çalışmalar, Edge-IIoTset için %98 ve WUSTL-IIoT-2021 için %98,72 doğruluk değerleri vermiştir. Ancak, bu çalışmaların çoğu, sınırlı saldırı türlerine sahip veri setleri üzerinde değerlendirilmiş veya yalnızca genel ağ saldırılarına odaklanmıştır.

Bu deneysel çalışmada kullanılan SCADANet veri seti, literatürdeki bu sınırlamaları gidermek üzere tasarlanmış daha kapsamlı bir yapı sunmaktadır. Veri seti, saldırgan sistemleri, Modbus sunucuları, SCADA/HMI istemcileri ve ağ trafiğini izleyen bir dinleyici düğümünden oluşan izole bir sanal SCADA ortamında oluşturulmuştur. Önerilen bu mimari sayesinde, Modbus istemci-sunucu iletişimi gerçek endüstriyel ortamlara benzer bir şekilde devam ederken, saldırılar aynı ağ trafiği içinde gerçekleştirilmektedir. Sonuç olarak, saldırı trafiği, normal endüstriyel iletişimden izole edilmiş sentetik bir yapı yerine, gerçekçi bir trafik akışı içinde elde edilmiştir.

SCADANet veri setinin bir diğer önemli özelliği ise saldırıların çeşitliliğidir. TCP SYN Flood, UDP Flood, ICMP Flood, HTTP Flood, SQL Injection ve Port Scan gibi yaygın ağ saldırılarının yanı sıra, veri seti Modbus False Data Injection, Modbus Command Abuse, APT Data Exfiltration ve Insider Threat gibi SCADA sistemlerine özgü tehditleri de içermektedir. Bu, veri setinin hem ağ düzeyinde hem de kontrol protokolü düzeyinde

meydana gelen saldırıları temsil etmesini sağlar. Bu bakımdan SCADANet veri kümesi, literatürde halihazırda yaygın olarak kullanılan birçok veri kümesinden de ayrılır.

Ayrıca, veri kümesinde çok katmanlı ağ protokollerinden türetilen ayrıntılı paket özellikleri kullanılmıştır ve paket zaman damgalarının saldırı komut dosyalarının günlükleriyle eşleştirilmesi yoluyla yüksek doğrulukta etiketleme sağlanmıştır. Bu yaklaşım, veri kümesinin güvenilirliğini artırır ve çok sınıflı saldırı tespit çalışmalarına uygun bir veri yapısı sunar.

Literatürdeki birçok çalışma, tek bir makine öğrenimi veya derin öğrenme modeline dayanmaktadır. Buna karşın, bu çalışmada önerilen Çok Bileşenli Derin Öğrenme Yaklaşımı, ağ trafiğinin farklı özellik temsilcilerini bir arada öğrenebilen çok bileşenli bir mimari olarak tasarlanmıştır. Önerilen model, birden fazla derin öğrenme bileşeninin iş birliği içinde çalışmasını kolaylaştırarak ağ trafiğindeki hem zamansal hem de davranışsal kalıpların eşzamanlı analizini mümkün kılmaktadır. Bu yaklaşım, özellikle farklı özelliklere sahip saldırı türlerini birbirinden ayırt etmede önemli bir avantaj sunmaktadır. Tablo 5.1'de gösterilen %86 ile %98 aralığındaki sonuçlar göz önüne alındığında, önerilen modelin SCADANet veri setinde elde ettiği performans, daha çeşitli saldırı türleri ve daha karmaşık bir trafik yapısı içeren bir veri seti üzerinde değerlendirildiği düşünüldüğünde önemli bir sonuçtur.

Sonuç olarak, SCADANet veri setinin yüksek saldırı çeşitliliği, gerçekçi ağ trafiği yapısı ve ayrıntılı etiketleme yaklaşımı, literatürdeki veri setlerine kıyasla daha kapsamlı bir test ortamı sunmaktadır. Bu veri seti kullanılarak geliştirilen çok bileşenli derin öğrenme modeli, kritik altyapıda kullanılan SCADA sistemlerinde farklı türdeki siber saldırıları tespit etme açısından literatüre önemli bir katkı sağlamaktadır.

Tablo 5.1. SCADA ve endüstriyel nesnelerin interneti veri kümeleri üzerinde son dönem siber saldırı tespit çalışmalarının performans karşılaştırması

Çalışma/Yıl	Veri Seti	Protokol/Trafik Çeşitleri:	Saldırı Çeşitleri	Sınıflar	Sonuç (%)	Algoritma
(Siddique vd., 2025)/2025	SWAT	Bir su arıtma tesisinden gelen ağ trafiği ve fiziksel proses verileri.	Ağ saldırıları ve süreç kesintilerini içeren siber ve fiziksel saldırılar.	Yeniden Oynatma(Replay), DoS, Komut Enjeksiyonu(Command Injection)	Doğruluk 87 %	GAN-LSTM
(Latif-Martínez vd., 2025)/2025	WADI	SWAT veri setine benzer şekilde su dağıtım sistemlerinden elde edilen veriler.	Siber-fiziksel saldırılar.	Normal and Anomali.	Hassasiyet 86,69%	Graph Attention Network(Grafik Dikkat Ağı) Tabanlı Anomali Tespiti (GAT-AD)
(Lachure ve Doriya, 2025)/2025	BATADAL	Tipik olarak su dağıtım sistemlerini içerir.	Simüle edilmiş siber-fiziksel saldırılar.	Veri Bütünlüğü - Erişilebilirlik Odaklı Saldırıları	Doğruluk 96,93%	Toplu(Ensemble Stacking) Makine Öğrenimi (ESML)
(Naeem vd., 2025)/2024	MSU	Endüstriyel kontrol sistemi verileri, Modbus/TCP protokolü.	Çeşitli siber-fiziksel saldırılar.	Normal and Attack Scenarios.	Doğruluk 96,6%	CNN Tabanlı Topluluk Öğrenmesi (Ensemble Learning)
(B. V. Vasilica vd., 2025)/2025	CIC Modbus	Modbus protokol trafiği.	Modbus haberleşmesini hedef alan ağ tabanlı saldırılar.	Fuzzing, DoS, Replay, Modbus Command Injection	Doğruluk 95%	Rastgele Orman (RF) ve Destek Vektör Makinesi (SVM)
(Bilal vd., 2026)/2025	Edge IIOTset	Endüstriyel Nesnelerin İnterneti (IoT) verileri.	IoT-spesifik siber saldırılar	DoS, Data Injection	Doğruluk 98%	Transformer + FedNova
(Zakariah vd., 2025)/2025	WUSTL-IIoT-2021	Endüstriyel IoT cihazlarından elde edilen ağ trafiği.	IoT iletişimini hedef alan çoklu siber saldırılar.	DoS, DDoS, Keşif, Enjeksiyon	Doğruluk 98,72%	Faktörizasyon Makinesi + Derin Yapay Sinir Ağı (DeepFM)
Our Study	SCADANet	Modbus/TCP protokolü kullanan sanal bir SCADA ortamından üretilen ağ trafiği.	Ağ ve kontrol süreçlerini hedef alan siber ve SCADA'ya özgü saldırılar.	TCP-SYN Saldırısı, TCP-ACK Saldırısı, UDP Saldırısı, ICMP Saldırısı, HTTP Saldırısı, SQL Enjeksiyonu, Bağlantı Noktası Taraması, Güvenlik Açığı Taraması, İşletim Sistemi Taraması, Modbus Sahte Veri Enjeksiyonu, Modbus Komut Kötüye Kullanımı, APT Veri Çalma, İçeriden Gelen Tehdit.	Doğruluk 99,80%	Çok Bileşenli Derin Öğrenme Yaklaşımı

6. SONUÇLAR VE ÖNERİLER

Bu deneysel çalışma, SCADA tabanlı kritik altyapı ağlarını hedef alan siber saldırıları tespit etmeyi amaçlamaktadır. Bu amaçla, siber saldırıları etkin bir şekilde tespit etmek üzere paralel genişletilmiş CNN katmanları, Residual-SE blokları ve LSTM bileşenlerini bir araya getiren çok katmanlı bir hibrit derin öğrenme mimarisi önerilmiştir. Önerilen mimari, dönüştürülmüş SCADA trafiği temsilleri içinde çok ölçekli uzamsal kalıpları ve özellik düzeyinde sıralı/bağlamsal ilişkileri eşzamanlı olarak modellemek üzere tasarlanmıştır. Ek olarak, SCADANet veri seti, meşru endüstriyel iletişimlerin ve çok sınıflı saldırı senaryolarının eşzamanlı olarak üretildiği, tamamen izole edilmiş bir sanal SCADA ortamı içinde literatüre sunulmuştur.

Önerilen çok katmanlı derin öğrenme mimarisi, hem geliştirilen SCADANet veri seti hem de literatürde yer alan köklü WUSTL-IIoT-2021 veri seti üzerinde değerlendirilmiştir. Deney sonuçları, önerilen derin öğrenme mimarisinin her iki veri setinde de yüksek doğruluk, makro F1 puanı ve geri çağırma değerlerine ulaştığını göstermektedir. Özellikle, az sayıda örneği olan saldırı sınıflarında elde edilen yüksek performans, odak kaybı ve sınıf ağırlıklandırma stratejilerinin dengesiz veri koşulları altında modelin duyarlılığını artırdığını göstermektedir. Ayrıca, yürütülen ablasyon çalışması, önerilen hibrit derin öğrenme mimarisinin her bir bileşeninin genel sınıflandırma performansına önemli bir katkı sağladığını da göstermektedir.

Bu çalışmada elde edilen bulgular, çok ölçekli evrişimli özellik çıkarma, kanal düzeyinde dikkat mekanizmaları ve özellik düzeyinde sıralı modelleme bileşenlerinin bir arada kullanılmasının, karmaşık SCADA trafik davranışının etkili bir şekilde temsil edilmesini sağladığını göstermektedir. Farklı veri kümeleri üzerinde yapılan değerlendirmeler, önerilen modelin belirli bir veri dağılımına bağlı olmadığını açıkça ortaya koymaktadır. Deney sonuçları, geliştirilen derin öğrenme mimarisinin çeşitli endüstriyel trafik yapıları genelinde tutarlı bir saldırı tespit performansı sergilediğini göstermiştir.

Ancak, alışmanın bazı sınırlamaları bulunmaktadır. SCADANet veri seti, deneysel tekrarlanabilirlięi ve sistematik deęerlendirmeyi saęlamak iin kontroll bir sanal SCADA ortamında oluřturulmuřtur. Ancak, bu tr kontroll ortamlar, gerek endstriyel sistemlerin operasyonel karmařıklıęını tam olarak yansıtamaz. zellikle, donanım eřitlilięi, sre dzeyinde deęiřkenlik, eski cihaz davranıřları ve dinamik aę kořulları bu baęlamda sınırlı kalmaktadır. Veri kmesi ok eřitli saldırıları kapsamaktadır. Ancak, ok ařamalı koordineli saldırılar, uzun vadeli gizli tehditler ve geliřmiř siber-fiziksel maniplasyon senaryoları yeterince temsil edilmemektedir.

Gelecekteki akademik arařtırmalar, deney ortamının gerekilięini artırmayı hedeflemektedir. Veri setine daha karmařık saldırı senaryoları dahil edilecektir. Ayrıca, nerilen ok katmanlı derin ęrenme mimarisi, yarı operasyonel ve gerek endstriyel ortamlarda doęrulanacaktır. Bunun yanı sıra, dřk gecikmeli ve leklenebilir u aę geidi tabanlı daęıtım stratejileri zerine arařtırmalar planlanmaktadır. Bu planlanan geliřmelerin, geliřmiř siber-fiziksel tehditlere karřı dayanıklılıęı artırması beklenmektedir. Ayrıca, planlanan gncellemelerin kritik altyapı sistemleri iin daęıtılabilir ve gvenilir AI tabanlı saldırı tespit mekanizmalarının geliřtirilmesine katkıda bulunacaęı ngrlmektedir.

KAYNAKLAR

Abd Elaziz, M., Ahmed Fares, I. and Aseeri, A. O. (2024). CKAN: Convolutional Kolmogorov-Arnold Networks Model for Intrusion Detection in IoT Environment. *IEEE Access*, 12, 134837–134851.

Ahakonye, L. A. C., Nwakanma, C. I., Lee, J. M. and Kim, D. S. (2023). SCADA intrusion detection scheme exploiting the fusion of modified decision tree and Chi-square feature selection. *Internet of Things*, 21, 100676.

Alam, M., Abid, F., Guangpei, C. and Yunrong, L. V. (2020). Social media sentiment analysis through parallel dilated convolutional neural network for smart city applications. *Computer Communications*, 154, 129–137.

Alguliyev, R. and Shikhaliyev, R. (2024). Network cybersecurity incidents multiclassification based on deep learning. *Problems of Information Technology*, 15, 16–23.

Al-Shurbaji, T., et al., (2025). Deep Learning-Based Intrusion Detection System for Detecting IoT Botnet Attacks: A Review. *IEEE Access*, 13, 11792–11822.

Alsabbagh, W., Amogbonjaye, S., Urrego, D. and Langendörfer, P. (2023). A Stealthy False Command Injection Attack on Modbus based SCADA Systems. *Proceedings of the IEEE Consumer Communications and Networking Conference (CCNC)*, 2023-January.

Alsaiani, A. and Ilyas, M. (2025). A Hybrid CNN-LSTM Deep Learning Model for Intrusion Detection in Smart Grid. *SSRN Electronic Journal*.

Altaleb, H. and Rajnai, Z. (2023). Malware Attacks on SCADA Systems: Assessing Risks and Strengthening Cybersecurity Measures. *SISY 2023 - IEEE 21st International Symposium on Intelligent Systems and Informatics*, 625–629.

Arqane, A., Boutkhoul, O., Boukhriss, H. and El Moutaouakkil, A. (2022). Intrusion Detection System using Ensemble Learning Approaches: A Systematic Literature Review. *International Journal of Online and Biomedical Engineering (iJOE)*, 18(13).

Awaad, A. M., Ali Alheeti, K. M. and Najem, A. K. A. H. (2024). Anomaly-Based IDS (Intrusion Detection System) for Cyber-Physical Systems. *Mesopotamian Journal of Big Data*, 2024, 230–240.

Bajwa, A., Al Razee Tonoy, A., Rana, S. and Ahmed, I. (2024). Cybersecurity in Industrial Control Systems: A Systematic Literature Review on AI-Based Threat Detection for SCADA and IoT Networks. *Journal of Cybersecurity*, 1–15.

Barik, K., Misra, S., Konar, K., Fernandez-Sanz, L. and Koyuncu, M. (2022). Cybersecurity Deep: Approaches, Attacks Dataset, and Comparative Study. *Applied Artificial Intelligence*, 36(1).

Basnet, M., Poudyal, S., Ali, M. H. and Dasgupta, D. (2021). Ransomware detection using deep learning in the SCADA system of electric vehicle charging station. *2021 IEEE PES Innovative Smart Grid Technologies Conference - Latin America (ISGT Latin America 2021)*.

Bilal, M. A., et al., (2026). Dataset-centric evaluation of federated intrusion detection models in IoT networks. *Scientific Reports*, 16(1), 2683.

Birnbaum, Z., et al., (2020). Cyber-Resilient SCADA Systems via Secure State Restoration. *IFIP Advances in Information and Communication Technology*, 596, 183–207.

Bjorck, N., Gomes, C. P., Selman, B. and Weinberger, K. Q. (2018). Understanding Batch Normalization. *Advances in Neural Information Processing Systems*, 31.

Bronk, C. and Tikk-Ringas, E. (2013). The Cyber Attack on Saudi Aramco. *Survival*, 55, 81–96.

Casajús-Setién, J., Bielza, C. and Larrañaga, P. (2023). Anomaly-Based Intrusion Detection in IIoT Networks Using Transformer Models. *Proceedings of the 2023 IEEE International Conference on Cyber Security and Resilience (CSR 2023)*, 72–77.

Chauhan, V. K. and Kumar, A. (2025). Cascaded capsule twin attentional dilated convolutional network for malicious URL detection. *Expert Systems with Applications*, 262, 125507.

Chu, A., Lai, Y. and Liu, J. (2019). Industrial Control Intrusion Detection Approach Based on Multiclassification GoogLeNet-LSTM Model. *Security and Communication Networks*, 2019, 6757685.

Cui, J., Long, J., Min, E., Liu, Q. and Li, Q. (2018). Comparative Study of CNN and RNN for Deep Learning Based Intrusion Detection System. *International Conference on Communication, Computing & Security*, 11067 LNCS, 159–170.

Do, V. L., Fillatre, L., Nikiforov, I. and Willett, P. (2017). Security of SCADA systems against cyber-physical attacks. *IEEE Aerospace and Electronic Systems Magazine*, 32, 28–45.

Doğan, F., Polat, O. and Yardimci, F. (2025). A new method for detecting beaconing attacks in IoT-based SCADA systems. *International Journal of Information Security*, 24(6), 244.

Elsayed, S., Mohamed, K. and Madkour, M. A. (2024). A Comparative Study of Using Deep Learning Algorithms in Network Intrusion Detection. *IEEE Access*, 12, 58851–58870.

Eshmawi, A. A., Aldrees, A. and Alharthi, R. (2025). Smart framework for industrial IoT and cloud computing network intrusion detection using a ConvLSTM-based deep learning model. *Frontiers in Computer Science*, 7, 1622382.

Fährmann, D., Ihlefeld, M., Kuijper, A. and Damer, N. (2025). Resource-Efficient Anomaly Detection in Industrial Control Systems With Quantized Recurrent Variational Autoencoder. *IET Collaborative Intelligent Manufacturing*, 7, e70032.

Gao, J., et al., (2021). Omni SCADA Intrusion Detection Using Deep Learning Algorithms. *IEEE Internet of Things Journal*, 8, 951–961.

Gbabo, E. Y., Kingsley Okenwa, O. and Chima, E. (2023). Developing Intrusion Detection Integration Models for SCADA-Controlled Electricity Infrastructure. *International Journal of Scientific Research in Science and Technology (IJSRST)*.

Gbashi, S. M., Adedeji, P. A., Olatunji, O. O. and Madushele, N. (2025). Optimal feature selection for a weighted k-nearest neighbors for compound fault classification in wind turbine gearbox. *Results in Engineering*, 25, 103791.

Harrou, F., Bouyeddou, B., Dairi, A. and Sun, Y. (2024). Exploiting Autoencoder-Based Anomaly Detection to Enhance Cybersecurity in Power Grids. *Future Internet*, 16, 184.

Heddami, S., et al., (2022). A long short-term memory deep learning approach for river water temperature prediction. *Current Trends and Advances in Computer-Aided Intelligent Environmental Data Engineering*, 243–270.

Hussen, N., Elghamrawy, S. M., Salem, M. and El-Desouky, A. I. (2023). A Fully Streaming Big Data Framework for Cyber Security Based on Optimized Deep Learning Algorithm. *IEEE Access*, 11, 65675–65688.

IEEE Xplore. (2014). *Intrusion detection in SCADA systems using one-class classification*. Erişim adresi: <https://ieeexplore.ieee.org/abstract/document/6811620>

Jahan Simu, S. and Zaman, F. I. (2023). Advanced Cybersecurity Strategies for Protecting Critical Infrastructure: Strengthening the Backbone of National Security. *International Journal of Scientific Research and Management (IJSRM)*, 11, 999–1016.

JCBI. (2020). *View of Dragonfly Cyber Threats: A Case Study of Malware Attacks Targeting Power Grids*. Journal of Cybersecurity and Information. Erişim adresi: <https://jcbi.org/index.php/Main/article/view/137/82>

Ji, I., Jeon, S. and Seo, J. T. (2024). AE-LSTM Based Anomaly Detection System for Communication Over DNP 3.0. *Lecture Notes in Computer Science*, 14402 LNCS, 91–104.

Kang, J., Jang, S., Li, S., Jeong, Y. S. and Sung, Y. (2019). Long short-term memory-based Malware classification method for information security. *Computers & Electrical Engineering*, 77, 366–375.

Kim, B. K. and Kang, Y. (2018). Abnormal Traffic Detection Mechanism for Protecting IIoT Environments. *9th International Conference on Information and Communication Technology Convergence (ICTC 2018)*, 943–945.

Kimanzi, R., Kimanga, P., Cherori, D. and Gikunda, P. K. (2024). Deep Learning Algorithms Used in Intrusion Detection Systems -- A Review. *arXiv preprint*, arXiv:2402.17020. Erişim adresi: <https://arxiv.org/pdf/2402.17020>

Kumar, A. (2025). HybridNet: Advancing Deepfake Detection Through Residual, SE, and Depthwise Convolutions. *IEEE Access*.

Lachure, J. and Doriya, R. (2025). ESML: A Hyperparameter-Tuned Stacking Machine Learning Approach for Anomaly Attack Detection in Water Distribution Systems. *SN Computer Science*, 6, 505.

Laghrissi, F. E., Douzi, S., Douzi, K. and Hssina, B. (2021). Intrusion detection systems using long short-term memory (LSTM). *Journal of Big Data*, 8(1), 65.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9, 49–51.

Latif-Martínez, H., Suárez-Varela, J., Cabellos-Aparicio, A. and Barlet-Ros, P. (2025). GAT-AD: Graph Attention Networks for contextual anomaly detection in network monitoring. *Computers & Industrial Engineering*, 200, 110830.

Le, X., Li, J., Zhao, Y. and Fan, Z. (2025). A Security-Enhanced Scheme for ModBus TCP Protocol Based on Lightweight Cryptographic Algorithm. *Electronics*, 14, 3674.

Lee, J. H., Shin, J. and Seo, J. T. (2023). Solar Power Plant Network Packet-Based Anomaly Detection System for Cybersecurity. *Computers, Materials & Continua*, 77, 757.

Lehto, M. (2022). Cyber-Attacks Against Critical Infrastructure. *Computational Methods in Applied Sciences*, 56, 3–42.

Liao, H. J., Richard Lin, C. H., Lin, Y. C. and Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36, 16–24.

Macas, M., Wu, C. and Fuertes, W. (2024). An Attention-Based Deep Generative Model for Anomaly Detection in Industrial Control Systems. *International Conference on Web Information Systems and Technologies (WEBIST)*, 566–577.

Mahi-Al-rashid, A., Hossain, F., Anwar, A. and Azam, S. (2022). False Data Injection Attack Detection in Smart Grid Using Energy Consumption Forecasting. *Energies*, 15, 4877.

Markkandeyan, S., et al., (2025). Novel hybrid deep learning based cyber security threat detection model with optimization algorithm. *Cyber Security and Applications*, 3, 100075.

McAfee. (2017). *Triton Malware Spearheads Latest Attacks on Industrial Systems*. McAfee Blog. Erişim adresi: <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/triton-malware-spearheads-latest-generation-of-attacks-on-industrial-systems/>

Mehrotra, L. and Saxena, P. S. (2018). An Assessment Report on: Statistics-Based and Signature-Based Intrusion Detection Techniques. *Advances in Intelligent Systems and Computing*, 625, 321–327.

Mohammed, A. S., Saxena, N. and Rana, O. (2022). Wheels on the Modbus - Attacking ModbusTCP Communications. *WiSec '22: Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 22, 288–289.

Mondal, S., Prudhvi, B., Khare, P. and Bharata Reddy, M. J. (2025). Real-time analysis of cyber attacks in SCADA based power system. *Australian Journal of Electrical and Electronics Engineering*.

Morris, T. H. and Gao, W. (2013). Industrial Control System Cyber Attacks. *1st International Symposium on ICS & SCADA Cyber Security Research (ICSCSR 2013)*.

Muhlburger, H. and Wotawa, F. (2022). A Passive Testing Approach using a Semi-Supervised Intrusion Detection Model for SCADA Network Traffic. *Proceedings of 4th IEEE International Conference on Artificial Intelligence Testing (AITest 2022)*, 42–47.

Musthafa, M. (2025). Real-Time Intrusion Detection Leveraging Deep Learning: A Comparative Analysis of CNN, RNN, and Transformer Architectures. *International Journal of Advanced Engineering, Management and Science (IJAEMS)*, 11, 2454–1311.

Naeem, H., Ullah, F. and Srivastava, G. (2025). Classification of intrusion cyber-attacks in smart power grids using deep ensemble learning with metaheuristic-based optimization. *Expert Systems*, 42, e13556.

Nazir, S., Patel, S. and Patel, D. (2021). Autoencoder Based Anomaly Detection for SCADA Networks. *International Journal of Artificial Intelligence and Machine Learning (IJAIML)*, 11, 83–99.

NERC. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case*. Technical Report, North American Electric Reliability Corporation.

Nour, S. M. and Said, S. A. (2024). Deep Learning Performance Evaluation Model for Enhancing Network Intrusion Detection Systems. *NILES 2024 - 6th Novel Intelligent and Leading Emerging Sciences Conference*, 61–65.

Ortega-Fernandez, I., Sestelo, M., Burguillo, J. C. and Piñón-Blanco, C. (2023). Network intrusion detection system for DDoS attacks in ICS using deep autoencoders. *Wireless Networks*, 30(6), 5059–5059.

Patil, S. B. (2022). *Network Intrusion Detection System using Ensemble Learning*. (Yayımlanmamış Yüksek Lisans Tezi). Academic Cyber Security.

Paulraj, J., Raghuraman, B., Gopalakrishnan, N. and Otoum, Y. (2025). Autonomous AI-based Cybersecurity Framework for Critical Infrastructure: Real-Time Threat Mitigation. *2025 IEEE/ACIS 29th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, 925–931.

Qi, G., Mao, J., Huang, K., You, Z. and Lin, J. (2025). Multi-Head Attention Enhanced Parallel Dilated Convolution and Residual Learning for Network Traffic Anomaly Detection. *Computers, Materials & Continua*, 82, 2159.

Radoglou-Grammatikis, P., et al., (2020). Implementation and detection of Modbus cyberattacks. *2020 9th International Conference on Modern Circuits and Systems Technologies (MOCASST)*.

Ramos, L. S. and Yang, Z. (2023). LSTM-Based Detection of OT Cyber-Attacks for an Offshore HVAC-Cooling Process. *2023 IEEE 6th International Conference on Electronic Information and Communication Technology (ICEICT 2023)*, 943–948.

Razaque, A., et al., (2025). Review of malicious code detection in data mining applications: challenges, algorithms, and future direction. *Cluster Computing*, 28, 206.

Roopesh, Albert, B., Manuel, A. S. and Hemram, S. (2024). Developing an ML Model for Detecting the Cyber Attacks in Electric Vehicles. *2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC-ROBINS 2024)*, 776–781.

Saheed, Y. K., Misra, S. and Chockalingam, S. (2023). Autoencoder via DCNN and LSTM Models for Intrusion Detection in Industrial Control Systems of Critical Infrastructures. *Proceedings of 2023 IEEE/ACM 4th International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS 2023)*, 9–16.

Sangeetha, K., Kala, A., Femi, P. S. and Priya, S. B. (2024). A Comparative Analysis of Deep Learning Based Techniques for Cyber Security. *2024 1st International Conference on Software, Systems and Information Technology (SSITCON 2024)*.

Sayegh, N., Chehab, A., Elhajj, I. H. and Kayssi, A. (2013). Internal security attacks on SCADA systems. *2013 3rd International Conference on Communications and Information Technology (ICCIT 2013)*, 22–27.

Sayghe, A. (2025). Digital Twin-Driven Intrusion Detection for Industrial SCADA: A Cyber-Physical Case Study. *Sensors*, 25, 4963.

Shang, W., et al., (2024). An Efficient Anomaly Detection Method for Industrial Control Systems: Deep Convolutional Autoencoding Transformer Network. *International Journal of Intelligent Systems*, 2024, 5459452.

Sharma, N. and Arora, B. (2025). Machine Learning and Deep Learning Models for Anomaly Intrusion Detection in Networks: A Systematic Review. *SN Computer Science*, 6(7), 832.

Siddique, M. S., et al., (2025). An intelligent intrusion detection system for cyber-physical systems using GAN-LSTM networks. *Franklin Open*, 11, 100281.

Siegel, B. (2020). Industrial Anomaly Detection: A Comparison of Unsupervised Neural Network Architectures. *IEEE Sensors Letters*, 4.

Slowik, J. (2020). *The Baffling Berserk Bear: A Decade's Activity Targeting Critical Infrastructure*. Virus Bulletin. Erişim adresi: www.virusbulletin.com

Sukhadeo, B. S., et al., (2023). MLIDS: A Machine Learning-Based Intrusion Detection System Using the NSLKDD Data. *International Journal of Intelligent Systems and Applications in Engineering*, 12, 167–179.

Tripathi, A., Upadhyay, P. and Goel, P. K. (2024). Industrial Control Systems (ICS) Security: AI-Based Threat Detection and Prevention. *IGI Global*, 149–172.

Vasilica, B. V., Anton, F. D., Pietraru, R., Anton, S. O. and Chiriac, B. N. (2025). Enhancing Security in Smart Robot Digital Twins Through Intrusion Detection Systems. *Applied Sciences*, 15.

Verkerken, M., D'hooge, L., Wauters, T., Volckaert, B. and De Turck, F. (2021). Towards Model Generalization for Intrusion Detection: Unsupervised Machine Learning Techniques. *Journal of Network and Systems Management*, 30(1), 12.

Wali, S., Farrukh, Y. A., Khan, I. and Hamilton, J. A. (2025). Covert penetrations: Analyzing and defending SCADA systems from stealth and Hijacking attacks. *Computers & Security*, 156, 104449.

WUSTL. (2021). *WUSTL-IIOT-2021 Dataset for IIoT Cybersecurity Research*. Washington University in St. Louis. Erişim adresi: <https://www.cse.wustl.edu/~jain/iiot2/index.html>

Yang, Y. S., et al., (2022). Securing SCADA Energy Management System under DDoS Attacks Using Token Verification Approach. *Applied Sciences*, 12, 530.

Zakariah, M., Amin, S. U., Alrayes, F. S., Helal, M. and Khan, Z. I. (2025). SCADA intrusion detection using deep factorization machines. *Scientific Reports*, 15(1), 39753.

Zhang, H., Min, Y., Liu, S., Tong, H. and Li, Y. (2022). MODLSTM: A Method to Recognize DoS Attacks on Modbus/TCP. *Conference Proceedings of the IEEE International Performance, Computing, and Communications Conference*, 2022-November, 319–324.

Zhang, Y., Zhang, L. and Zheng, X. (2024). Enhanced Intrusion Detection for ICS Using MS1DCNN and Transformer to Tackle Data Imbalance. *Sensors*, 24, 7883.

Zhu, B. and Sastry, S. (2012). Intrusion Detection and Resilient Control for SCADA Systems. *Cyber Security and Scada Systems*, IGI Global, 352–383.

Zolanvari, M., Teixeira, M. A., Gupta, L., Khan, K. M. and Jain, R. (2019). Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things. *IEEE Internet of Things Journal*, 6, 6822–6834.