
GAZİ ÜNİVERSİTESİ
Gazi
1926

SCADA SİSTEMLERİNE YÖNELİK SİBER SALDIRILARIN TESPİTİ İÇİN YENİ BİR HİBRİT MAKİNE ÖĞRENMESİ YÖNTEMİ

Esra SÖĞÜT

DOKTORA TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

HAZİRAN 2023

ETİK BEYAN

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

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Esra SÖĞÜT

21/06/2023

SCADA SİSTEMLERİNE YÖNELİK SİBER SALDIRILARIN TESPİTİ İÇİN YENİ BİR HİBRİT MAKİNE ÖĞRENMESİ YÖNTEMİ

(Doktora Tezi)

Esra SÖĞÜT

GAZİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

Haziran 2023

ÖZET

Otomasyon ve kontrol sistemlerinin farklı sistemler ile bütünleşik şekilde çalışmaya başlaması kritik altyapı sistemlerinde büyük teknolojik gelişmelere sebep olmuştur. Kritik altyapı sistemleri farklı karakteristik özelliklere ve iletişim için farklı ağ mimarilerine sahiptir. Bu yüzden sistemlerin kontrol edilmesi ve gerekli durumlarda sistemlere etkin şekilde müdahale edilmesi gerekmektedir. Bu zorunluluklardan dolayı kapsamlı bir teknoloji olan Denetim Kontrol ve Veri Toplama (Supervision Control and Data Acquisition - SCADA) sistemleri kullanılmaya başlanmıştır. SCADA sistemleri bağlı oldukları diğer sistemleri ve var olan süreçleri takip ve kontrol etmektedir. SCADA sistemlerinde yaşanan teknolojik gelişmeler sonucunda gerçekleşebilecek veya SCADA sistem mimarisine özgü ortaya çıkabilecek siber açıklıklar güvenlik için büyük sorunlardır. Bunların fark edilmesi ve sömürülmesi ihtimalleri siber saldırılar için uygun bir zemin oluşturmaktadır. SCADA sistemleri kritik altyapılarda ve ulaşım, iletişim, sağlık ve ekonomi gibi birçok sektörde kullanıldığı için siber güvenliğin sağlanması önem arz etmektedir. Bu çalışmada gerçek bir su tesisinin küçültülmüş hali bir test yatağı ortamına aktarılmıştır. Bu test yatağında su tanklarının kontrolü ve süreçlerin izlenmesi için SCADA sistemi kullanılmıştır. Bu ortama beş farklı Dağıtık Servis Hizmet Reddi (Distrubuted Denial of Service - DDoS) saldırı senaryosu gerçekleştirilmiştir ve saldırısız normal durum senaryosu da değerlendirilmiştir. Senaryolar sonucunda elde edilen verilere Evrişimli Sinir Ağları, Uzun-Kısa Süreli Bellek, bu ikisinin hibrit kullanımı, KStar, Yerel Ağırlıklı Öğrenme, K-En Yakın Komşu, LogitBoost, AdaBoost, Naive Bayes, BayesNet, ZeroR, PART, Karar Tablosu, Karar Ağacı, Rastgele Orman ve Rastgele Ağaç makine öğrenmesi modelleri uygulanmıştır. SCADA sistemine yönelik DDoS saldırı tespiti ve DDoS saldırı türü tespiti için en iyi sonuçlar hibrit model (doğru sınıflandırma oranı %95) ve Karar Ağacı modeli (doğru sınıflandırma oranı %99) ile elde edilmiştir. Hibrit modelin başarısını desteklemek için literatürde sıklıkla kullanılan bir veri kümesi analiz edilmiştir (doğru sınıflandırma oranı %98). Elde edilen sonuçlar, SCADA sistem güvenliğinin etkili bir şekilde iyileştirebileceğini ve önerilen modellerin gerçek saha sistemleriyle uyumlu şekilde çalışabileceğini göstermiştir.

Bilim Kodu	:	92403
Anahtar Kelimeler	:	Siber güvenlik, SCADA, Modbus protokolü, makine öğrenmesi, DDoS saldırıları
Sayfa Adedi	:	107
Danışman	:	Prof. Dr. O. Ayhan ERDEM

A NEW HYBRID MACHINE LEARNING METHOD FOR DETECTION OF CYBER ATTACKS ON SCADA SYSTEMS

(Ph. D. Thesis)

Esra SÖĞÜT

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

June 2023

ABSTRACT

The integrated operation of automation and control systems with different systems has led to major technological developments in critical infrastructure systems. Critical infrastructure systems have different characteristics and have different network architectures for communication. Therefore, it is necessary to control the systems and effectively intervene in the systems when necessary. Due to these requirements, comprehensive technology, Supervision Control and Data Acquisition (SCADA) systems have started to be used. SCADA systems monitor and control other systems and existing processes to which they are connected. Cyber vulnerabilities that may occur as a result of technological developments in SCADA systems or that may be specific to the SCADA system architecture are major problems for security. The possibility of their detection and exploitation creates a suitable ground for cyber attacks. Since SCADA systems are used in many sectors and critical infrastructures such as transport, communication, health and economy, it is important to ensure cyber security. In this study, a scaled-down version of a real water plant is transferred to a testbed environment. In this testbed, a SCADA system was used to control the water tanks and monitor the processes. Five distinct Distributed Denial of Service (DDoS) attack scenarios were performed on this environment and a normal case scenario without attack was also evaluated. Convolutional Neural Networks, Long Short Term Memory, hybrid use of these two, KStar, Local Weighted Learning, K-Nearest Neighbor, LogitBoost, AdaBoost, Naive Bayes, BayesNet, ZeroR, PART, Decision Table, Decision Tree, Random Forest and Random Tree machine learning models were applied to the data obtained as a result of the scenarios. The best results for DDoS attack detection and DDoS attack type detection for SCADA system were obtained with the hybrid model (accuracy rate 95%) and the Decision Tree model (accuracy rate 99%). To support the success of the hybrid model, a data set frequently used in the literature was analyzed (accuracy rate 98%). The obtained results showed that SCADA system security can be improved effectively and the proposed models can work in harmony with real field systems.

Science Code	:	92403
Key Words	:	Cyber security, SCADA, Modbus protocol, machine learning, DDoS attacks
Page Number	:	107
Supervisor	:	Prof. Dr. O. Ayhan ERDEM

TEŞEKKÜR

Lisansüstü eğitimim süresince çalışmalarımda önderlik eden ve desteklerini esirgemeyen danışman hocam Prof. Dr. O. Ayhan ERDEM'e, tez çalışmalarım boyunca desteklerini esirgemeyen tez izleme üyeleri Doç. Dr. Hüseyin POLAT ve Doç. Dr. Mustafa SERT hocalarıma, çalışmalarım sırasında beni sürekli yüreklendiren Gazi Üniversitesi Teknoloji Fakültesi Bilgisayar Mühendisliği Bölümü Öğretim üyelerine, fikir alışverişi yapmak için zaman ayıran ve bana katkılar sunan arkadaşlarıma, tez savunması sırasında yanımda olan arkadaşlarıma, test işlemleri sırasında destek veren Bilgisayar Yüksek Mühendisi Merve GÜLLÜ'ye ve takıldığım konularda farklı çözümler öneren Bilgisayar Yüksek Mühendisi Çağla AKSOY'a en derin teşekkürlerimi sunarım. Eğitim hayatım boyunca maddi manevi desteklerini hep yanımda hissettiğim sevgili anneme, babama ve ağabeyime sonsuz teşekkür ederim.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

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

Simgeler	Açıklamalar
cm	Santimetre
csv	Comma-Separated Values
dB	Desibel
gb	Gigabayt
gHz	Gigahertz
m	Metre
Mbps	Megabits Per Second
mHz	Megahertz
mm	Milimetre
ms	Milisaniye
sn	Saniye
tb	Terabayt
v	Volt

Kısaltmalar	Açıklamalar
AB	AdaBoost
ACK	Acknowledgement
ADAM	Adaptive Moment Estimation
ADSL	Asymmetric Digital Subscriber Line
ANN-SOM	Artificial Neural Networks based Self-Organized Map
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
BN	BayesNet
CNN	Convolutional Neural Networks
DC	Direct Current
DDoS	Distrubuted Denial of Service

Kısaltmalar	Açıklamalar
DN	Doğru Negatif
DNP3	Distributed Network Protocol Version 3.0
DoS	Denial of Service
DP	Doğru Pozitif
DS	Decision Stump
DSL	Digital Subscriber Line
DT	Decision Tree
DTa	Decision Table
FNN	Feedforward Neural Network
HNA-NN	Hierarchical Neuron Architecture based Neural Network
HT	Hoeffding Tree
GNB	Gaussian Naive Bayes
HMM	Hidden Markov Models
ICMP	Internet Control Message Protocol
IEC	International Electrotechnical Commission
IEEE	The Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IWP-CSO	Intrusion Weighted Particle based Cuckoo Search Optimization
İMA	İnsan Makine Ara Yüzü
KNN	K-Nearest Neighbors
KS	KStar
LB	LogitBoost
LR	Logistic Regression
LSTM	Long-Short Term Memory
LWL	Locally Weighted Learning
MDB	Merkezi Denetleyici Birimi
MITM	Man in the Middle
NB	Naive Bayes
NN	Neural Networks
OCSVM	One-Class Support Vector Machine

Kısaltmalar	Açıklamalar
OSI	Open Systems Interconnection
PLC	Programmable Logic Controller
ReLU	Rectified Lineer Unit
RF	Random Forest
ROC	Receiver Operating Characteristic
RT	Random Tree
SCADA	Supervisory Control and Data Acquisition
SSD	Solid State Disk
STS	Saldırı Tespit Sistemi
SVM	Support Vector Machines
SYN	Synchronize
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
UUB	Uzak Uç Birimleri
YN	Yanlış Negatif
YP	Yanlış Pozitif

1. GİRİŞ

Dünya genelinde iletişim ağı hızla genişlemekte ve ülkeler arasındaki mesafeler internet aracılığıyla kolaylıkla aşılmaktadır. Artık birçok işlem aracıya gerek kalmadan kesintisiz şekilde gerçekleştirilmektedir. Kullanılan, işlenen ve kaydedilen veri niteliği ve niceliği de giderek değişmektedir. Hem teknoloji hem de veri yönünden yaşanan gelişmeler kötü niyetli kişilerin faaliyetlerini gerçekleştirebileceği daha çok alan ve daha çok yöntem üretilmesine sebep olmuştur. Kötü niyetli saldırganlar tarafından kamu kurumları, telekom operatörleri, şirketler ve özellikle kritik altyapılar gibi ortamlar cazip hedefler haline gelmiştir.

Su, petrol, doğal gaz gibi kaynakların veya hidroelektrik, güneş, nükleer gibi santrallerdeki enerjinin üretiminin ve iletiminin yapıldığı tesisler kritik altyapıları oluşturmaktadır. Buna ek olarak uzay, uydu, hava, deniz veya tren ulaşım sistemleri de kritik altyapı sistemlerine dâhildir. Bu sistemler küçük bir alana veya geniş alanlara yayılarak çalışmaktadır. Kritik altyapılardaki süreçleri ve olayları bir merkez üzerinden izleyen, kontrol eden ve gerektiğinde süreçlere ve olaylara müdahale eden sistemler bulunmaktadır. Bunlardan biri Merkezi Denetim ve Veri Toplama (Supervisory Control and Data Acquisition - SCADA) Sistemleridir. Örneğin, belediyelerin şebeke suyu dağıtım tesislerinde yer alan tanklardaki su seviyeleri, boru basıncı ve sıcaklığı izlemek için SCADA sistemleri kullanılır.

SCADA sistemleri temel olarak üç ana bileşene sahiptir. Bu bileşenler Merkezi Denetleyici Birimi (MDB - Master Terminal Unit), Uzak Uç Birimleri (UUB - Remote Terminal Unit) ve haberleşme ağıdır. Her bileşenin ayrı görevi vardır. MDB dışındaki bileşen sayısı ve çeşitliliği hizmet edilen amaca göre değişmektedir. UUB'lerden veri alınarak MDB'ye iletilir, İnsan Makine Ara Yüzü (İMA – Human Machine Interface) üzerinde görüntüleme ve takip yapılır. Ayrıca verilerin kaydedilmesi ve ilgili bileşene komut gönderilmesi de sağlanır. Gerekli durumlarda da MDB tüm sisteme müdahale edebilir.

Siber güvenlik alanında her sene yayınlanan raporlara ve araştırmalara göre, içeriden meydana gelebilecek ve dışarıdan gerçekleştirilecek saldırılara karşı her zaman hazırlıklı olunmalıdır [1]. Siber dünyada SCADA güvenliğinin sağlanması da önemli bir konudur. SCADA sistemlerine yönelik gerçekleştirilen siber saldırılar, kritik altyapı sistemleri için son derece tehlikeli kabul edilmektedir ve bu saldırılar ele alınıp incelenmelidir [2]. SCADA sistemlerinin sahip olduğu mimari yapısından dolayı yeni ve gelişmiş teknolojilerle

bütünleşme konusu tam olarak çözülememiştir. Ayrıca internet kullanımı, dış ağlara erişim yapılması ve uzaktan kontrol özelliklerinin kullanımı da giderek artmaktadır. Bunun gibi durumlar geleneksel SCADA sistemlerinin işlevselliğini arttırmaktadır fakat beraberinde birçok güvenlik açıklığını da getirmektedir.

Bu sistemlere yönelik gerçekleşebilecek saldırıların hem ulusal hem uluslararası anlamda büyük zararlar verebileceği tahmin edilmektedir. Bu gibi durumların gelişerek devam etmesi beraberinde siber terör gibi yeni bir sorunu da getirmektedir. Siber terör kesin sınırları olan, belirli ve herkesçe bilinen bir tanıma sahip değildir. Terör eylemlerinin siber savaş alanında gerçekleştirilmesi veya siber ortamın terör eylemleri için gösterim yeri halini alması olarak tanımlanabilir. Meydana gelen siber terör faaliyetlerinin etkileri tüm ülkeleri alarma geçirecek ve vatandaşları da tedirgin edecek duruma getirmiştir.

Kritik altyapılar, ülkede yaşayan insanların hayatlarını daha iyi koşullarda idame ettirmeleri için büyük önem taşımaktadır. Bu yapıların işleyişlerinde yaşanacak sorunlar sadece ilgili alanı veya bölgeyi değil ülkenin tümünü etkileyecek düzeyde olabilir. Kurumlarda veya kritik altyapılarda kullanılan SCADA sistemlerine yönelik gerçekleştirilen saldırılar, siber terör saldırıları olarak değerlendirilebilir. Bu saldırılar sistemleri yavaşlatmakta, sistemlere zarar vermekte veya sistemlerin tamamen durmasına sebep olabilmektedir. Örneğin elektrik üretim, iletim ve dağıtım tesislerinin işlevsiz hale getirilmesi bir ülkede büyük bir kargaşaya neden olabilir ve elektrikle çalışan diğer sistemleri de doğrudan etkileyebilir. Bu şekilde elektrik kesintisi sorunları yaşanmış ve bunlara maruz kalan ülkelerde kesintinin ne kadar önemli olduğu anlaşılmıştır. Bunun gibi kritik altyapılara yapılacak siber terör saldırılarının ekonomik, güvenlik veya sağlık açısından ne kadar tehlikeli sonuçlar doğuracağı anlaşılmıştır. Kritik altyapılarda bulunan SCADA sistemlerine yönelik gerçekleşebilecek siber saldırıların sonuçları tahminlerin veya yazılan raporların çok ötesinde olabilir. Sonuç olarak SCADA sistemlerinin siber güvenliğinin sağlanması zorunlu hale gelmiştir. Bu sistemlerde kullanılan teknolojilerin, haberleşme protokollerinin, ağ yapısının ve bileşenlerin siber güvenliğinin sağlanması önem arz etmektedir. Saldırı tespiti ve engellenmesi gibi güvenlik sistemlerinin geliştirilmesi ülkelerin kritik altyapılarının devamlılığına çok büyük katkı sunacaktır.

SCADA sistemlerinde kullanılan haberleşme protokollerinin güvenliği ele alındığında birçok açıklığın olduğu bilinmektedir. En çok kullanılan protokollerden biri olan Modbus

protokolünün özelliklerinden yola çıkılarak gerçekleştirilen ve gerçekleştirilmesi muhtemel saldırı çeşitleri bulunmaktadır. Modbus protokolünün sahip olduğu güvenlik açıklıklarından faydalanılarak SCADA sistemlerinin işleyişine zarar verilebilir veya sistemdeki veriler üzerinde değişiklikler yapılabilir. Hatta sistem tamamen çalışamaz hale getirilebilir. Bu sebeplerden dolayı Modbus protokolünün güvenlik açıklıklarının değerlendirilip siber güvenliğin sağlanmasına yönelik çalışmalar yapılması ulusal ve uluslararası alanda önem arz etmektedir.

Saldırı tespit çalışmalarında kullanılan makine öğrenmesi veya yapay zekâ algoritmalarını içeren modeller SCADA sistemlerine de uygulanabilir. Saldırı olup olmadığına yönelik veya saldırı türünü belirlemeye yönelik çalışmalar SCADA sistemlerinin siber güvenliğine katkı sunabilir. Farklı türlerde siber saldırılar bulunmaktadır ve Dağıtık Servis Hizmet Reddi (Distrubuted Denial of Service - DDoS) saldırıları diğer saldırılara göre daha sık görülmektedir. Özellikle DDoS saldırılarının SCADA sistemleri için ele alınması, siber güvenlik alanında önemli bir konudur. Farklı algoritmaların kullanıldığı modeller birbirinden farklı yapılara sahip oldukları için yapılan analiz sonuçları da çeşitlilik göstermektedir. Örneğin bir model bir veri kümesi üzerinde yüksek performans sağlarken, başka bir veri kümesi üzerinde düşük performans gösterebilir. Bir veri kümesi üzerinde bir model yüksek başarıya sahipken, başka bir model başarılı sonuçlar vermeyebilir. Bu sebeplerden dolayı belirli bir veri kümesi için yüksek performans sağlayan bir model geliştirmek önem arz etmektedir.

Bu çalışmada, kritik altyapılarda kullanılan bir SCADA sisteminin donanım ve yazılım içerecek şekilde modellenmesi amaçlanmıştır. Bunun için fiziksel ve siber süreçlerin işlenmesini sağlayan bir test yatağı hazırlanmıştır. Siber fiziksel sistem ortamı sunan bu test yatağında su depolama tankları, giriş yapan veya ölçme yapan elemanlar (algılayıcılar), iş yapan veya çıkış yapan elemanlar (aktüatörler) gibi bileşenler kullanılmıştır. SCADA sistemlerinde sıklıkla kullanılan Modbus Aktarım Denetimi Protokolü (Transmission Control Protocol - TCP) ve kablolu/kablosuz bağlantılar kullanılarak dışarıya kapalı olan bir iletişim ağı oluşturulmuştur. Uç birimler ile merkezi birim arasında veri ve komut gönderimi sağlanmış ve test yatağındaki işleyiş fiziksel olarak canlı gözlemlenmiştir. Fiziksel işleyişi bozmak, SCADA sisteminin süreçlerine zarar vermek ve saldırılar karşısında sistemin tepkisini ölçmek amaçlarıyla test yatağına yönelik çeşitli DDoS saldırıları uygulanmış ve testler gerçekleştirilmiştir. Test yatağının siber güvenliğinin sağlanması için saldırı tespitinin

yapılması zorunludur. Bunun için saldırısız normal duruma ve saldırılı durumlara ait üretilen ağ trafikleri dinlenmiş ve kaydedilmiştir. Kaydedilen ağ trafik paketlerinin analiz edilmesi ve saldırı olup olmadığının anlaşılması için makine öğrenmesi algoritmaları kullanılmıştır. Saldırı tespiti yapılmasının yanı sıra saldırı türünün belirlenmesi için de bu algoritmalar üzerinde çalışılmıştır. Evrişimli Sinir Ağları (Convolutional Neural Networks - CNN), Uzun-Kısa Süreli Bellek (Long-Short Term Memory - LSTM), CNN-LSTM hibrit, KStar (KS), Yerel Ağırlıklı Öğrenme (Locally Weighted Learning - LWL), K-En Yakın Komşu (K-Nearest Neighbors - KNN), LogitBoost (LB), AdaBoost (AB), Naive Bayes (NB), BayesNet (BN), ZeroR, PART, Karar Tablosu (Decision Table – DTa), Karar Ağacı (Decision Tree – DT), Rastgele Orman (Random Forest – RF) ve Rastgele Ağaç (Random Tree – RT) olmak üzere 16 adet makine öğrenmesi algoritması kullanılarak yüksek başarı oranı elde eden modeller bu çalışma için önerilmiştir. Elde edilen sonuçlar, CNN-LSTM hibrit modeli (%95) ve DT modeli (%99) ile SCADA sistemine yönelik DDoS saldırı tespiti ve DDoS saldırı türü tespiti için yüksek doğruluk oranlarına ulaşıldığını göstermiştir. SCADA sistemlerinin siber fiziksel sistem güvenliğinin sağlanmasına yönelik farklı bir bakış açısı sunmak ve saldırı türü belirlenmesi için uygun modeller hazırlamak amaçlanmıştır.

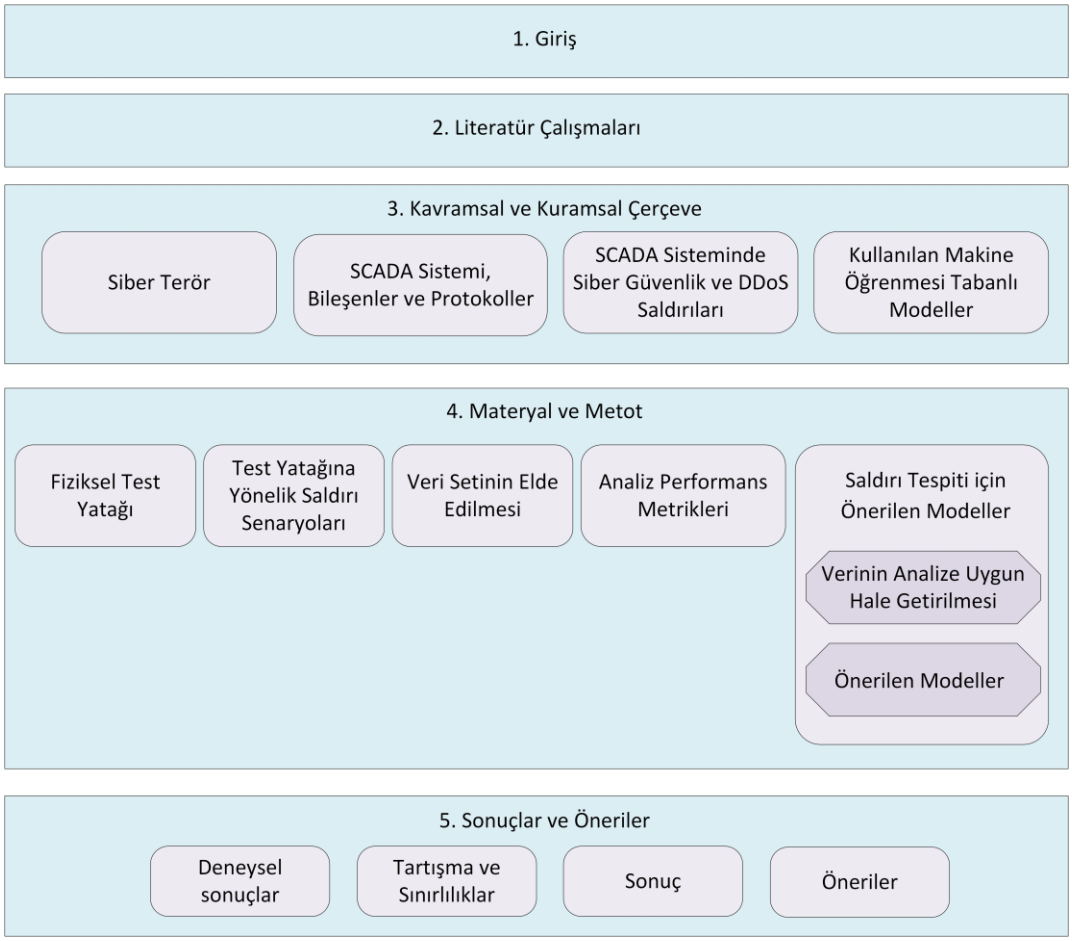
Bu tez çalışmasının başlıca katkıları aşağıdaki gibidir:

- SCADA sisteminin ve işleyişlerin canlı olarak gösterilmesi için fiziksel bir test yatağı ortamı hazırlanmıştır. Kullanılan bileşenler, yazılımlar, donanımlar ve teknolojiler ile literatürdeki çalışmaları zenginleştirmek amaçlanmıştır.
- SCADA sisteminin yer aldığı test yatağına yönelik 5 farklı DDoS saldırısı gerçekleştirilmiş ve saldırıların etkileri canlı olarak gözlenmiştir. Saldırısız durumda ve her bir saldırı anında ağ akış verileri toplanmıştır.
- Literatürde genellikle hazır veri kümeleri üzerinde çalışılmıştır. Bu çalışmada farklı DDoS saldırılarının bulunduğu ve saldırısız durumun da olduğu yeni bir veri kümesi hazırlanmıştır. Bu veri kümesi Modbus TCP protokolü kullanılan test yatağına özgüdür.
- Saldırı tespiti ve saldırı türü belirlenmesi için makine öğrenmesi tabanlı CNN ve LSTM algoritmaları ayrı ayrı modeller olarak kullanılmıştır. Buna ek olarak CNN ve LSTM algoritmaları birlikte değerlendirilerek hibrit bir model şeklinde kullanılmıştır. İncelediğimiz literatürdeki çalışmalarda bu şekilde ayrı ayrı ve hibrit kullanımlar az

sayıda görülmüştür. Hibrit model kullanımı ile tek tek modellerin kullanılmasından daha yüksek bir başarı oranı elde edilmiştir.

- Bu 3 modele ek olarak, 13 adet makine öğrenmesi algoritması ile analizler de yapılmış ve en yüksek başarı oranı DT modeli ile elde edilmiştir.
- Hibrit modelin yeterliliğini ve güvenirliğini değerlendirmek için literatürde yaygın olarak kullanılan bir veri kümesi seçilmiş ve test edilmiştir. Elde edilen sonuçlara göre literatürdeki çalışmanın sonuçlarından daha yüksek bir doğruluk oranına ulaşılmıştır.
- SCADA sistemlerinde veya bu sistemlerin kullanıldığı kurumlarda meydana gelebilecek siber saldırılara karşı tespit işlemleri için önerilerde bulunulmuştur. Bu tür önerilerin ele alınması ve kullanılması hem sistemlerin daha iyi korunmasını sağlayacak hem de veri kaybını en aza indirecektir.
- Ayrıca çalışmanın siber terör kapsamında olması personellerin, görevli olan operatörlerin de bilinçlenmesini ve dikkatli davranmasını sağlayacaktır. Gelecekte bu sistemlere karşı olabilecek saldırılar için tahminlerde bulunularak sistem yöneticileri ve kullanıcıları için farkındalık oluşturulması sağlanacaktır.

Bu tez çalışması beş bölüm halinde yapılandırılmıştır. Birinci bölümde kritik altyapılar, SCADA sistemleri, siber terör ve saldırılardan bahsedilmiştir. Bu tez çalışmasının önemi ve kapsamı açıklanmıştır. İkinci bölümde kendi oluşturdukları veri kümelerini, hazır veri kümelerini veya kendi hazırladıkları test yataklarını kullanarak saldırı tespiti yapan çalışmalar incelenmiştir. Üçüncü bölümde SCADA sistemleri, bu sistemlerin siber güvenliği, bu sistemlere yönelik siber saldırılar ve çalışmada kullanılan makine öğrenmesi tabanlı modeller ele alınmıştır. Hazırlanan test yatağı, gerçekleştirilen saldırı senaryoları, elde edilen veri kümesi, başarı metrikleri ve önerilen saldırı tespit modelleri dördüncü bölümde anlatılmıştır. Sonraki bölümde yapılan testlerin sonuçları hakkında, elde edilen analizler hakkında bilgi verilmiş ve çalışmanın sonuçları özetlenmiştir. Tez çalışmasının organizasyon şemasına Şekil 1.1'de yer verilmiştir.



Şekil 1.1. Çalışmanın organizasyon şeması

2. LİTERATÜR ÇALIŞMALARI

SCADA sistemlerine yönelik gerçekleşen siber saldırılar ve bu saldırıların tespit edilmesi konularında yapılmış çalışmalar literatürde bulunmaktadır. Bunlar arasından test yatağı kullanarak kendi veri kümelerini üreten veya hazır veri kümelerini kullanan çalışmalar ele alınmıştır. İlgili çalışmalara bu bölümde yer verilmektedir.

Nader ve arkadaşları, endüstriyel kontrol sistemlerinin ve kritik altyapıların güvenliği üzerine bir çalışma yapmıştır. Veri tabanlarında bulunmayan veya yeni oluşturulan saldırıları, geleneksel saldırı tespit sistemlerinin tespit edemediği vurgulanmıştır. Fransa'daki bir su dağıtım sisteminden alınan veriler çalışmada kullanılmış ve saldırı tespiti için makine öğrenmesi algoritmaları önerilmiştir [3].

Bilgi ve iletişim teknolojilerinde yaşanan gelişmelere odaklanan Yang ve arkadaşları, SCADA sistemlerinde karmaşıklığın ve güvenlik açıklıklarının giderek arttığını vurgulamıştır. İnternetle ve farklı sistemlerle bütünleşmiş olan yeni nesil SCADA sistemleri için yeni güvenlik önlemlerinin alınması gerektiği belirtilmiştir. Bu yüzden çalışmada çok özellikli bir Saldırı Tespit Sistemi (STS) önerilmiştir. Geliştirilen STS davranış tabanlı ve çok katmanlı bir çerçeveye sahiptir. SCADA sistemlerinin siber güvenliğini sağlamak, veri bütünlüğünü korumak ve normal verilerin riske atılmamasını sağlamak için bir güvenlik çözümü önerilmiştir [4].

SCADA sistemleri, binlerce cihazdan oluşan büyük sistemlerle bütünleştiğinde daha savunmasız hale gelmektedir. Almalawi ve arkadaşları, bu sistemlere yönelik gerçekleşecek saldırıların tespiti için iki yaklaşım önermiştir. Birincisi sistemdeki verilerin tutarlı ve tutarsız olmasının belirlenmesidir. İkinci yaklaşım ise belirlenmiş durumlardan yakınlık algılama kurallarının çıkarılmasıdır. Çalışmada hazır bir veri kümesi ve benzetimler sonucu hazırlanan iki veri kümesi kullanılmıştır. KNN tabanlı STS'nin önemli doğruluk değeri gösterdiği belirtilmiştir [5].

Kalech, zamansal örüntü tanımaya dayalı teknikleri SCADA sistemlerinde siber saldırıların tespiti için önermiştir. Bu yöntemler, SCADA bileşenleri tarafından ağ üzerinden aktarılan verilerdeki ve komutların yanlış kullanılmasındaki anormallikleri tespit etmek için kullanılmıştır. Çalışmada Gizli Markov Modeli (Hidden Markov Models - HMM) ve Yapay

Sinir Ağları tabanlı Kendini Düzenleyen Harita (Artificial Neural Networks based Self-Organized Map – ANN-SOM) dayalı iki algoritma önerilmiştir. Elde edilen sonuçlarda, siber saldırıları tespit etmede kolaylık sağlandığı belirtilmiştir [6].

SCADA sistemlerine yönelik gerçekleştirilen zamansal olarak ilişkili ve ilişkisiz saldırılar, Gao ve arkadaşları tarafından ele alınmıştır. Bu saldırıları tespit etmek için derin öğrenmeye dayalı İleri Beslemeli Sinir Ağı (Feedforward Neural Network - FNN) ve LSTM algoritmaları kullanılmıştır. FNN, zamansal olarak ilişkisiz saldırıları tespit etmede iyi bir performans göstermiştir. LSTM ise zamansal olarak ilişkili saldırılarda iyi bir tespit mekanizmasına sahiptir. FNN - LSTM modeli ise zamansal alaka düzeyine bakılmaksızın iki türlü siber saldırıyı tespit etmede de başarı göstermiştir [7].

SCADA sistemlerine yapılan izinsiz girişler engellenememektedir ve farklı saldırı vektörlerine karşı savunma mekanizmaları yetersizdir. Bu yüzden Maglaras ve arkadaşları, SCADA sistemlerinin siber güvenliğinin sağlanmasına yönelik bir çalışma yapmıştır. Buna göre, siber saldırılara karşı ağ trafiğini okuyan, trafiği kaynağa göre bölen ve Tek-Sınıflı Destek Vektör Makinesi (One-Class Support Vector Machine - OCSVM) modelleri kümesi oluşturan bütünleşmiş bir saldırı tespit mekanizması önermişlerdir [8].

Gao ve arkadaşları, SCADA sistemlerine yönelik saldırıları tespit etmeyi amaçlayan iki model önermişlerdir. Bu modeller çoktan çoğa ve çoktan bire mimarilerine sahiptir. Modeller LSTM algoritmasını kullanır. Her iki STS de zamansal olarak ilişkisiz saldırıları tespit etmede başarılı performans sergilemiştir [9].

SCADA sistemlere izinsiz girişleri tespit etmek için yapılan birçok çalışma bulunmaktadır. Shitharth ve Winston izinsiz girişleri optimizasyona dayalı olarak sınıflandıran bir STS geliştirmiştir. Bu kapsamda ilk olarak İzinsiz Giriş Ağırlıklı Parçacık tabanlı Guguk Kuşu Arama Optimizasyon algoritmasını (Intrusion Weighted Particle based Cuckoo Search Optimization – IWP-CSO) ve ikinci olarak Hiyerarşik Nöron Mimarisi tabanlı Sinir Ağı algoritmasını (Hierarchical Neuron Architecture based Neural Network – HNA-NN) önermişlerdir. İlk optimizasyon algoritması ile en iyi öznitelikler seçilmiş ve ikinci algoritma ile ağdaki izinsiz girişler sınıflandırılmıştır [10-11].

Sayegh ve arkadaşları yerel ağ üzerinde deney ortamı hazırlamışlar ve SCADA haberleşme protokollerini kullanmışlardır. Bu ortama uyguladıkları Yeniden Yönlendirme (Replay), Servis Hizmet Reddi (Denial of Service - DoS) ve Şifreleme saldırıları sonucunda siber güvenliğin tam olarak sağlanamadığını dile getirmişlerdir. Kullanılan protokollerin ve bileşenlerin zafiyetlere sahip olduğunu ve bunların siber güvenlik sorunlarına sebep olduğunu vurgulamışlardır [12].

Koutsandria ve arkadaşları, Matlab/Simulink kullanarak siber fiziksel Programlanabilir Mantıksal Denetleyici (Programmable Logic Controller - PLC) benzetim ortamı oluşturmuştur. Burada gerçek ağ trafiği kullanmışlardır. Bu ortama yönelik siber saldırılar uygulanmış ve ağ trafiği analiz edilmiştir. Saldırı tespitinin yapılması için STS güvenlik kuralları kullanılmıştır [13].

Mississippi State Üniversitesi SCADA Güvenliği Laboratuvarı'nda çalışmalar yapan Morris ve arkadaşları, SCADA sistemlerinde sıklıkla kullanılan iletişim protokollerinin güvenlik zafiyetleri üzerinde durmuştur. Saldırıları, zafiyetleri ve saldırıların etkilerini incelemişlerdir. Sinir Ağı metotları kullanarak güvenlik mekanizması geliştirmişler. Bu sayede saldırıları tespit etmeyi ve zararları en aza indirmeyi amaçlamışlardır [14].

Hahn, endüstriyel kontrol sistemlerinin kullanıldığı güç sistemleri için benzetim yapmıştır. Bu benzetim ortamına yönelik gerçekleşen siber saldırıların analiz ve tespiti üzerinde çalışmıştır [15]. Başka bir çalışmada ise arkadaşlarıyla birlikte, siber fiziksel ortamı gösteren bir deney ortamı kullanmıştır. Bu ortamda fiziksel sistem bileşenleri bulunmakta ve aralarında iletişim kurulmaktadır. Ortama yönelik farklı DoS ve Zararlı Kesici Özellikli (Malicious Breaker) saldırılar uygulanmış ve bu saldırıların sonuçları incelenmiştir [16].

Şebeke içi üretim ve dağıtım bileşenlerinin yer aldığı büyük çaplı Ulusal SCADA Deney Düzeneği projesi üzerinde çalışmalar yapılmıştır. Buna göre kritik altyapıların önemli güvenlik zafiyetlerinin olduğu belirlenmiş ve konuyla ilgili değerlendirmeler yapılmıştır [17]. Başka bir proje olan Illinois Üniversitesi Gerçek Zaman Kapsamlı Ağ Benzetim Ortamında, fiziksel bileşenler de kullanılarak Sanal Güç Sistemi Deney Düzeneği tasarlanmıştır. Bu ortamla bütünleşik çalışacak şekilde PowerWorld güç sistemi benzetim aracı da kullanılmıştır [18].

Farklı bir proje olan Avrupa CRUTIAL projesinde farklı deney ortamları bulunmaktadır. Bu ortamların birinde merkezi ve alt sistemlerin haberleşme sistemine yönelik gerçekleşen DoS saldıuları ele alınmıştır. Diğer ortamda ise akıllı elektronik cihazlar kullanılmış ve Matlab/Simulink ortamında haberleşmeleri sağlanmıştır. Bu proje dağıtık enerji kaynağı uygulamalarındaki zafiyetlerin tespiti için değerlendirilmiştir [19,20].

Arizona Üniversitesi'nde SCADA sistemlerinin güvenlik analizi için bir test yatağı hazırlanmıştır. Burada, anormal hareketliliklere odaklanan STS için araştırmalar yapılmış ve bununla ilgili benzetimler gerçekleştirilmiştir [21].

Dublin Üniversitesi'nde gerçekleştirilen çalışmada siber saldırıları yakalamak ve meydana gelebilecek fiziksel etkileri analiz etmek amaçlanmıştır. Bunun için DIgSILENT güç sistemi benzetim aracı kullanılmış ve deney ortamı oluşturulmuştur [22].

Royal Melbourne Teknoloji Enstitüsü'nde kullanılan SCADASim deney ortamı, siber saldırıya maruz kalan sistem ağının performansını değerlendirmektedir. Bu ortamda SCADA sistemlerinde sıklıkla tercih edilen haberleşme protokolleri kullanılmış ve fiziksel bileşenler arasında iletişim kurulmuştur. Saldırların haberleşme mimarisi ile ilişkisi incelenmiştir [23].

Yanfei ve ekibi, Modbus tabanlı ZigBee kablosuz algılayıcısı için yeni bir yöntem geliştirmişlerdir [24,25]. Test yapmak için Modbus Poll aracını kullanmışlardır.

Beresford, PLC'lerin haberleşmesinde tercih edilen Profinet ve ISO-TSAP protokollerinin güvenlik zafiyetlerini ele almıştır. Bu protokollere yönelik Ortadaki Adam (Man in the Middle - MITM) ve Yeniden Yönlendirme saldırıları uygulanmıştır. Buna göre; PLC programlanmasına, işlemcinin çalışmasına, kimlik doğrulamasına ve parolalara zorla müdehale edilebilmiştir [26].

Chabukswar, kritik altyapılarda kullanılan SCADA sistemleri ve DDoS saldırıları üzerine bir çalışma yapmıştır. Kimya tesisi benzetim ortamına yönelik DDoS saldırıları uygulanmış ve hedefteki sistemin kaynakları aşırı şekilde kullanılmıştır. Bunun sonucunda SCADA sistemi kullanılan ortamdaki ağ trafiği çok fazla yavaşlamış ve sistem çalışması zarar görmüştür [27].

Devine yapmış olduğu çalışmada, günümüzdeki DDoS saldırılarının daha sistematik, anlaşılması zor yapıda gerçekleştirildiğini ve aynı anda birçok sisteme büyük zararlar verdiğini vurgulamştır. Çalışmada yapılan anketin sonuçlarına göre, kritik altyapıların kullanıldığı kurumlarda bile bu sorunların tam olarak anlaşılmadığı belirlenmiştir. Yetişmiş eleman eksikliği, gelişmiş teknolojilerin kullanılmaması, maddi yetersizlikler, siber saldırganların yöntemlerini geliştirmesi ve saldırıya uğrayabilecek potansiyel cihazların giderek artması gibi sorunlar saptanmıştır [28].

Petrovic ve Stojanovic, yaptıkları çalışmada son zamanlarda evrensel olarak endüstriyel kontrol merkezlerine saldırılar uygulandığını ve SCADA sistemlerindeki zafiyetlerin giderek arttığını belirtmiştir. Zafiyetleri kullanan saldırganların bazı bilgisayarları köle cihaz olarak belirlediğini ve sistemlere saldırırken bunları kullandığını açıklamışlardır. Elde ettikleri sonuçlara göre; zafiyetlerin tamamen giderilmesinin oldukça zor olduğu ve DDoS saldırılarına karşı sistemleri koruyabilecek sistemlerin olmadığı dile getirilmiştir. Saldırıların maddi ve işlevsel kayıplara sebep olabileceği de vurgulanmıştır [29].

Ciancamerla ve arkadaşları; SCADA bileşenlerinin, ağ tabanlı STS'nin, saldırganın ve yerel alan ağının bulunduğu bir ortam hazırlamıştır. Bu ortama MITM saldırısı uygulanmış ve Adres Çözümleme Protokolü (Address Resolution Protocol - ARP) zafiyeti kullanılarak PLC ve MDB arasına sızılmıştır. Bu saldırı sonucunda, bileşenler arasında gelip giden paketler üzerinde kontrol dışı değişimler yapılabilmiş [30].

Lee ve ekibi, Dağıtılmış Ağ Protokolü Sürüm 3'ün (Distributed Network Protocol Version 3.0 - DNP3) siber güvenliği üzerine bir çalışma yapmıştır. Çeşitli yazılımlar kullanarak ARP Zehirlenmesi (Poisoning), MITM ve Paket Yönlendirme (Packet Forwarding) saldırıları uygulamışlardır. Bu protokolün açıklıkları olduğu için saldırılar gerçekleştirilebilmiş ve ağa zorla müdehale edilerek paket değişimleri yapılabilmiştir [31].

Morris ve Gao, SCADA sistemlerine yönelik saldırıları DoS, Komut Enjeksiyonu (Command Injection), analiz, tepki ve tespit olarak gruplandırmış ve bu şekilde incelemiştir. Bu saldırılar endüstriyel kontrol sisteminin bulunduğu laboratuvar ortamında gerçekleştirilmiştir [32].

Aloui, Stuxnet zararlı yazılımını incelemiş ve PLC'lere özgü Dinamik Kod Enjeksiyonu (Dynamic Code Injection) saldırısının kolaylıkla uygulanabileceğini belirtmiştir. Bunu göstermek için uygun yazılımlar kullanarak saldırıyı hazırlamış, gerçekleştirmiş ve daha sonra güvenliğin sağlanması için önerilerde bulunmuştur [33].

Zhu ve arkadaşları, SCADA sistemlerine özgü saldırıları incelemiş; bunları haberleşme bileşenlerine, yazılımlara ve donanımlara yönelik uygulanan saldırılar olarak gruplandırmıştır. Haberleşme protokollerinde zafiyetlerin olduğu, Yapılandırılmış Sorgu Dili (Structured Query Language) enjeksiyonu gibi saldırıların yazılımlara yönelik uygulanabileceği ve yetkisiz/uzaktan erişimler ile cihazlarda alarmlar oluşturulabileceği gibi durum saptamalarında bulunulmuştur [34].

Gao ve ekibi, Mississippi State Üniversitesi SCADA Güvenliği Laboratuvarı'nı kullanarak zararlı Komut Enjeksiyonu saldırılarını uygulamıştır. Yapay sinir ağı temelli STS kullanmışlar ve saldırı tespitindeki hataları deneysel olarak incelemişlerdir. Bu STS'lerin gelecek vadeden güvenlik yöntemleri olabileceğini belirtmişlerdir [35].

Ten ve arkadaşları, kritik altyapıların siber güvenliğinin sağlanması için 4 aşama belirlemiştir. Bunlar takip, tespit, analiz ve azaltma aşamalarıdır. Analiz yapmak için güç sistemlerine yönelik saldırı yöntemi geliştirmişlerdir [36].

Shang ve ekibi endüstriyel kontrol sistemlerine yönelik uygulanan zararlı yazılımların tespitinin yapılması için kullanılan STS'leri analiz etmişlerdir. Ayrıca Modbus TCP protokolünün uygulama katmanında yapılan saldırılar için paket boyutunda derinlemesine analizler yapılmıştır. Çalışma sonucunda saldırıların etkisinin en aza indirilmesi için STS tabanlı Beyaz Liste Kuralları öneri olarak sunulmuştur [37].

Bo Chen ve arkadaşları akıllı şebekelerin siber güvenliğini araştırmak için Modbus TCP protokolü kullanılan bir deney düzeneği oluşturmuşlardır. Burada haberleşme ve güç sistemlerinin gerçek zamanlı olarak benzetimi yapılmıştır. Bu ortama yönelik çeşitli siber saldırılar uygulanmış, saldırı tespiti ve engellenmesi üzerine yorumlar yapılmıştır [38].

Xiong ve ekibi Modbus TCP protokolünün zafiyetleri üzerine geleneksel bulandırma yöntemlerini incelemişlerdir. Daha sonra, bu protokole göre uygun bir bulandırma yöntemi

geliştirmişlerdir. Benzetim ortamındaki sonuçlara, geliştirdikleri yöntemi uygulayarak geleneksel bulandırma yöntemlerine göre daha başarılı performans sonuçları elde etmişlerdir [39].

Bhatia ve arkadaşları, Sel (Flooding) saldırılarına karşı Modbus protokolünün zayıf noktalar içerdiğini ve bu saldırıların denetim sisteminin işlevlerini kullanım dışı bırakmayı hedeflediğini belirtmişlerdir. Saldırıları tespit etmek için anomali tabanlı bir STS ile imza tabanlı Snort modülü kıyaslanmıştır. İmza tabanlı STS'nin eşik değerlerinin dikkatli şeklide belirlenmesinin gerekliliği vurgulanmıştır. Anomali tabanlı STS'nin ise saldırıları tespit etmede çok az zaman gecikmesi yaşadığı gösterilmiştir [40].

Jung ve arkadaşlarının yaptığı çalışmada Modbus Seri protokolü ve Modbus Uzak Telemetri Birimi (Modbus Remote Telemetry Unit) modu kullanılmıştır. Modbus seri protokolünde RS232 ve RS485 portları kullanılmıştır. Burada mesaj göndermek ile ilgili zafiyet ele alınmıştır. Uzak Telemetri Birimi modda mesaj göndermek için belirli bir zaman aralığı olmalıdır. Bu durum, paket boştayken Koklayıcı (Sniffer) atağına olanak sağlamakta ve zafiyet oluşturmaktadır. Gerçekleştirilen deney düzeneğinde dijital/analog girdi/çıktı oluşturulmuş, ağa sızılmış ve Master ile Slave arasında Sniffer saldırısı yapılmıştır. Yapılan saldırı sonucunda elde edilen dıuruma göre bir çözüm yöntemi önerilmiştir [41].

Erkek ve arkadaşlarının yaptığı çalışmada ise Modbus TCP protokolü ve Uzak Telemetri Birimi modu kullanılmıştır. Modbus TCP protokolündeki 502 ve 503 portları kullanılmıştır. Burada iki zafiyet ele alınmıştır. Modbus TCP protokolünde kimlik doğrulama ve şifreleme yapılmamaktadır. Bu durum, MITM atağına olanak sağlamakta ve zafiyetler oluşturmaktadır. Gerçekleştirilen deney düzeneğine göre iç ağa sızılmış ve Master ile Slave arasında MITM saldırısı yapılmıştır. Yapılan saldırı sonucunda, benzetim ortamında akan Modbus paketleri açık metin olarak görüntülenmiştir. Ayrıca, yazmaç (register) değerleri okunup değiştirilmiştir. Bu zafiyetlere göre çözüm önerileri sunulmuş ve deney düzeneğinde uygulanmıştır. Buna göre akan paketlerin port ve ip bilgileri kontrol edilmiştir. Belirlenen port ve ip bilgileri dışındaki haberleşmeye izin verilmemiştir. Ayrıca yazmaç değerlerine üst sınır koyulmuştur. Çalışmada Kali Linux ortamı, Modbus Poll ve Modbus Slave benzetim araçları kullanmışlardır [42].

SCADA sistemlerinin güvensiz olduğunu belirten Skormi ve arkadaşları, güvenli siber-fiziksel sistemlerin tasarlanması konusunda çalışmaktadır. Buna göre, deney düzeneği oluşturulmuş, bazı saldırılar gerçekleştirilmiş, sistemin verdiği tepkiler izlenmiş ve tüm olaylara ait veriler toplanmıştır. MITM, Zehirlenme, DoS ve Enjeksiyon gibi saldırılar gerçekleştirilmiştir. Deney düzeneğinde PLC'ler, güç üniteleri ve ara yüzler kullanılmıştır. Sıvı kristal ekrana sahip monitörde doğru akım motorunun oransal-integral-türevsel denetleyici kontrol döngüsüne ait parametrelerin ayarlanması ve gerçek zamanlı voltaj bilgilerinin görüntülenmesi İMA ile sağlanmıştır. Deney düzeneğinde statik veri olarak cihaz açıklamaları, elektrik diyagramları, ağ diyagramları, PLC kodları gibi bilgiler ve dinamik veri olarak protokol mesajları, olay günlükleri, değişimlerin izleri gibi bilgiler toplanmıştır [43].

Farklı iletişim protokollerinin yer aldığı çalışmayı gerçekleştiren Hahn ve arkadaşları, NERC CIP007-1 Gereksinim Standartlarını ele almıştır. Buna göre "Sadece gerekli olan portlar ve servisler kullanılmalıdır. Varsayılan hesap bilgileri değiştirilmeli, devredışı bırakılmalı veya yeniden adlandırılmalıdır." gibi durumlara uymayan sistemler güvenlik zafiyetleri barındırmaktadır. Deney düzeneğinde UUB ile röle/en uç eleman haberleşmesinde Uluslararası Elektroteknik Komisyonu (International Electrotechnical Commission - IEC) 61850 protokolü; kontrol sunucuları ile UUB haberleşmesinde ise DNP3 protokolü kullanılmıştır. DoS, röleye yanlış komutlar gönderilmesi, röleden gelen verilerin değiştirilmesi, röle yapılandırmasının yeniden düzenlenmesi, yazmaça yanlış veri yazılması, yanlış alarm üretilmesi, alarm müdahaleleri gibi saldırılar gerçekleştirilmiş ve bunlara göre sistem tepkileri izlenmiştir. İMA, UUB, röle ve sanal özel ağ cihazları kullanılmıştır. Hahn ve arkadaşlarının sunduğu çözümlere göre, varsayılan parola ve şifreler değiştirilmelidir. Gereksiz şekilde açık bulunan portlar kapatılmalıdır [44].

Gaz boru hattı SCADA mimarisinde yeni bir veri kümesi oluşturan Morris ve arkadaşları, Komut Enjeksiyon atağı gibi 35 adet saldırı gerçekleştirmiştir. Bu saldırıları 7 gruba ayırmışlar ve saldırı gerçekleşmemiş durumu da ayrı bir grup olarak ele almışlardır. Modbus Seri protokolü üzerinde çalışmışlar ve 20 adet öznitelik belirlemişlerdir. Laboratuvar ölçekli olarak bir gaz boru hattı normal durumdayken ve saldırıya uğramış haldeyken, ağda etiketli veriler yakalanmıştır. Bu çalışmaya göre, oluşturulan veri kümesi 35 adet siber saldırıya ait bilgileri içermektedir. Ayrıca, bu veri kümesi STS tarafından kullanılan sınıflandırıcıları eğitmek ve test etmek için kullanılabilecek durumdadır [45].

Su dağıtım sistemi SCADA yapısı üzerinde çalışan Almalawi ve arkadaşları, benzetim ortamında saldırılar gerçekleştirmiştir. Ağ için ve grafiksel SCADA için benzetimler kullanılmıştır. DoS ve MITM saldırıları gerçekleştirilmiş ve saldırıların etkileri izlenmiştir [46].

SCADA sistemlerinin güvensiz olduğunu göstermek isteyen Wang ve arkadaşları bir benzetim ortamı kurmuştur. Bu ortamda UUB, İMA ve algılayıcı gibi bileşenler bulunmaktadır. Sisteme DoS ve Bütünlük (Integrity) saldırıları yapılmıştır. Saldırılar sonucunda ağ bağlantısına, MDB'ye ve UUB'ye sızma işlemleri gerçekleştirilmiştir [47].

Patriarca ve arkadaşları akıllı şebeke, gaz ve elektrik ağ ortamlarının benzetimini gerçekleştirmiştir. Kimlik doğrulama ve şifreleme yapılmaması zafiyetlerinden faydalanılarak sisteme DoS ve MITM saldırıları uygulanmıştır. Ortamda İMA, PLC ve protokol test cihazı kullanılmıştır. Uygulanan saldırıların sonuçları gözlemlenmiştir [48].

Su tesisi yapısı üzerinde çalışan Queiroz ve arkadaşları, benzetim ortamı oluşturmuş ve bu ortamda DDoS atağı gerçekleştirmiştir. Bu ortama mesafe ölçer gibi algılayıcıların ve pompa gibi aktüatörlerin de bağlanabileceğini göstermişlerdir. Böyle bir sisteme DDoS saldırısı yapılmış ve sistem tepkisi izlenmiştir [49].

Su depolama tankı ve gaz boru hattı sistemlerinin benzetimini gerçekleştiren Reaves ve arkadaşları, hem sanal hem de gerçek sistemler üzerinde çalışmıştır. Çalışmada Modbus Uzak Telemetri Birimi modu, Modbus TCP protokolü, kablosuz ağ bağlantıları ve radyo dalgaları kullanılmıştır. Tüm sisteme DDoS atağı yapılmış ve sonuç olarak bir veri kümesi elde edilmiştir. Saldırılardan sanal sistemin daha çok etkilendiği görülmüştür [50].

Su tankı sistemi ile çalışan Tesfahun ve arkadaşları Modbus TCP protokolü kullanarak bir benzetim ortamı hazırlamıştır. DDoS ve MITM saldırıları gerçekleştirilmiştir. Saldırıların tepkileri izlenmiş ve bir veri kümesi oluşturulmuştur [51].

Alhaidari ve arkadaşı KDDCup'99 veri kümesini kullanarak SCADA sisteminde DDoS saldırılarına karşı yeni bir çerçeve geliştirmiştir. Saldırı modelini belirlemek için J48, NB ve RF algoritmalarını kullanmıştır. En iyi sınıflandırma RF algoritması ile elde edilmiştir [52].

Başka bir çalışmada Hindy ve diğerleri, SCADA sistemi ile denetlenen su sistemindeki anomali olaylarını tespit eden yeni bir model sunmuştur. Bunun için hazır veri kümesi kullanılmıştır. Buradaki veriler algılayıcılardan toplanmış ve Modbus protokolü kullanılarak kontrol ve izleme ağına aktarılmıştır. Modelin oluşturulmasında ve değerlendirilmesinde altı makine öğrenmesi algoritması kullanılmıştır. Bunlar: Lojistik Regresyon (Logistic Regression - LR), Gaussian Naive Bayes (GNB), KNN, Destek Vektör Makinaları (Support Vector Machine - SVM), DT ve RF algoritmalarıdır. Sunulan model donanım hataları, sabotaj ve siber saldırılar gibi anomali olaylarını sınıflandırır. Normal, DoS, sahtecilik, engellenen ölçümler, naylon poşet bulunması, nem, ana tankta yüzen cisimler, ayrık algılayıcı hatası, nem, yanlış bağlantı ve kişilerin tanklara vurması gibi farklı senaryolar bulunmaktadır. Diğer tespit sistemlerinden farklı olarak önerilen çalışma, meydana gelen olay olasılığı ile bir anormallik meydana geldiğinde operatöre bildirimde bulunmaya ve saldırı etkisinin azaltılmasına odaklanmaktadır [53].

Beaver ve arkadaşları, gaz boru hattında Komut Enjeksiyonu ve Veri Enjeksiyonu (Data Injection) gibi saldırıları tespit etmede makine öğrenimi yöntemlerini kullanmaktadır. Potansiyel saldırı olaylarını tanımlamak için iyi huylu ve kötü huylu komut trafiği örnekleri denetlenmiştir. Hem normal işlemleri hem de saldırı senaryolarını içeren Modbus Uzak Telemetri Birimi modu veri kümesi kullanılmıştır. NB, RF, OneR, J48, NNge, SVM gibi makine öğrenmesi algoritmaları ile analizler yapılmıştır [54].

Hink ve arkadaşları, kritik altyapılardan olan güç sistemine karşı meydana gelen siber saldırıları ele almıştır. Sistemde var olan açıklıkların saldırının gizlenmesine ve operatörlerin aldatılmasına sebep olduğunu öne sürmektedir. Yaptıkları çalışmada, operatörü etkinleştirmek ve güç sistemine yapılan saldırıları tespit etmek için makine öğrenimi tekniklerini kullanmışlardır. Bu teknikler: NB, RF, OneR, NNge, SVM, JRipper, AB ve çalışmada önerilen teknik olarak AB + JRipper. Veriler, güç sistemi için binlerce ayrı ölçüm örneğini içeren 15 ayrı veri kümesinden alınmıştır [55].

Teixeira ve arkadaşları, siber güvenlik araştırmaları için kullanılan SCADA sistemi için test yatağı geliştirmişlerdir. Test yatağı, su arıtma ve dağıtım sürecindeki aşamalardan biri olan su depolama tankı kontrol sisteminden oluşmaktadır. Burada Modbus TCP protokolü kullanılmıştır. Sisteme Reconnaissance (adres taraması, port taraması, açıklardan sızma, cihaz tanımlaması gibi), DoS ve Komut Enjeksiyonu gibi karmaşık siber saldırılar yapılmış

ve bu saldırıların etkileri izlenmiştir. Saldırıya uğramamış ve uğramış ağ trafikleri toplanarak bir veri kümesi oluşturulmuştur. Sistemi analiz etmek ve saldırı tespiti yapmak için Makine öğrenmesi algoritmaları (RF, LR, NB, KNN, SVM) kullanılmıştır. Elde edilen sonuçlar, makine öğrenimi modellerinin saldırıları gerçek zamanlı olarak tespit etmedeki etkinliğini göstermektedir. Test ortamı, gerçek SCADA ortamlarına yapılan saldırıların etkileri ve sonuçları hakkında iyi bir bakış açısı sunmaktadır [56].

Benisha ve Ratna, SCADA ağındaki kötü amaçlı verilerin tespit edilmesi ve sınıflandırılması için yeni bir yöntem önermiştir. Yönteme göre, en uygun özelliklerin seçimi için kümeleme ve STS tabanlı olan Gelişmiş Guguk Kuşu Arama Optimizasyon (Enhanced Cuckoo Search Optimization) algoritması; sınıflandırma için ise Genetik Makine Öğrenmesi Tabanlı Sinir Ağı (Genetic Machine Learning based Neural Network) algoritması kullanılmıştır. Çalışmada kullanılan veri kümesi, su depolama sisteminin ağ saldırılarını içermektedir. Saldırıyı verilerden tespit etmek için belirli koşullar değerlendirilmiştir. Yeni yöntemle doğruluk, en az süre ile arttırılmıştır. Optimize edilmiş özelliklerin sıralaması sınıflandırıcıya verilmiştir. Performans analiz sonuçları geleneksel algoritmalardan daha iyi kümeleme, optimizasyon ve sınıflandırma çıktıları alındığını göstermiştir [57].

SCADA kontrol ağı ile kurumsal ağ arasında artan bağlantı talepleriyle birlikte, PLC'lerin veya UUB cihazlarının iletişiminde veya yönetiminde yeni siber saldırılar ortaya çıkmıştır. Perez ve arkadaşları tarafından Makine Öğrenmesi tekniklerinin SCADA sistemlerine yönelik ağ saldırılarını tespit edebildiği gösterilmiştir. Mississippi State Üniversitesi tarafından bir gaz boru hattı sisteminden toplanan gerçek bir veri kümesi kullanılmıştır. Çeşitli STS sınıflandırıcılarını uygulamak için SVM ve RF yöntemleri kullanılmıştır. Test kümesinin doğruluğu, hassasiyeti ve F1 değerinin kullanılması, performansların doğru ve kapsamlı bir şekilde değerlendirmesine olanak sağladığı sonucuna varılmıştır [58].

Wan ve arkadaşları, kamuya açık olmayan endüstriyel iletişim protokolleri için olay tabanlı bir anormallik algılama yaklaşımı önermiştir. Olay tabanlı HMM modelini kurarak endüstriyel iletişim protokolleri için anormal iletişim davranışlarının belirlenmesi için çalışılmıştır. Bilinmeyen protokol ve mesaj yapısı zorluklarının üstesinden gelmek ve oturumların olay dizilerini elde etmek amaçlanmıştır. Çalışmada benzetim ortamında Profinet protokolü kullanılmış ve veri üretilmiştir. Olay temelli HMM, hatalı davranışları tanımlamak için oluşturulmuştur. Önerilen yaklaşımı değerlendirmek için birçok deney

yapılmış; olay tabanlıı HMM, Sinir Ağları (Neural Networks - NN) ve NB karşılaştırılmıştır. Sınıflandırma doğruluğu ve algılama verimliliği açısından önerilen yöntemin avantajlara sahip olduğu görülmüştür [59].

Bir diğer çalışmada Grammatikis ve arkadaşları tarafından DNP3 kullanılan SCADA sistemleri için bir saldırı tespit ve önleme sistemi (DIDEROT adında) sunulmuştur. Bu sistem hem denetimli hem de denetimsiz makine öğrenimi algılama modellerine dayanmaktadır ve ağ akışının belirli bir DNP3 siber saldırısıyla veya anormallikle ilişkili olup olmadığını ayırt edebilmektedir. Bunun için kullanılan yöntemler: Minimum Covariance Determinant, Local Outlier Factor, Principal Component Analysis, Isolation Forest ve önerilen DIDEROT Autoencoder. Sistemde, bir trafo merkezinden alınan gerçek veriler kullanılmış ve önerilen sistemin verimliliği gösterilmiştir [60].

Skripcak ve Tanuska, SCADA sistemlerinde kullanılabilecek gerçek zamanlı ve çevrimiçi bilgi üretme bileşeni için ilk örneği tasarlamış ve bunun uygulamasını benzetim yaparak göstermiştir. Bu çalışmada deneysel ajan, ikili sınıflandırma problemi olarak kabul edilen süreç alarm tahmini senaryosuna odaklanmıştır. Önerilen bilgi üretimi kullanılan SCADA senaryosunda, çevrimiçi makine öğrenmesi yaklaşımına sahip Pasif-Girişken (Passive-Aggressive) algoritma sınıflandırıcısı kullanılmıştır. Ayrıca, sınıflandırmanın performansını değerlendirmek için Alıcı İşletim Özellikleri (Receiver Operating Characteristic – ROC) ile birlikte Matthews Korelasyon Katsayısı (Matthews Correlation Coefficient) değerleri ele alınmıştır. Önerilen ilk örnek, yeni SCADA çözümleri için çevrimiçi bilgi oluşturma bileşeninin nasıl tasarlanacağını ve uygulanacağını göstermektedir. Alarm tahmin aracının gerçek örneği, çevrimiçi makine öğrenmesi çerçevesinin üstünde geliştirilmiştir. Geleneksel olmayan ajan tabanlı SCADA/İMA çözümü önerilmekte ve ilk örnekte veri üretilmektedir [61].

Söğüt ve Erdem, gaz boru hattının denetlendiği sistemden üretilen bir veri kümesini kullanmış ve çalışmada saldırı tespitine odaklanmıştır. Bu veri kümesinde Modbus protokolüne özgü gerçekleştirilen DoS, Reconnaissance ve Komut Enjeksiyonu saldırılarına ait veri bulunmaktadır. Karar Kütüğü (Decision Stump – DS), Hoeffding Tree (HT), RT ve REP Tree algoritmaları kullanılmıştır [62].

Choubineh ve arkadaşları, bir gaz boru hattı SCADA sistemine yönelik siber saldırıları veya izinsiz girişleri tespit etmek için bir çalışma yapmıştır. Bunun için HT, NB, RT, BN ve OneR makine öğrenme algoritmaları kullanılmıştır. Önerilen algoritmanın performansını ve verimliliğini artırmak için farklı metotlar kullanılmış ve elde edilen sonuçlar kıyaslanmıştır [63].

Wang ve arkadaşları, Modbus protokolü kullanılan gaz boru hattı sistemine ve güç iletim sistemine ait veri kümelerini kullanarak SCADA sistemi için saldırı tespit sistemi geliştirmiştir. Hat bakımı, kısa devre hatası, Komut Enjeksiyonu, Veri Enjeksiyonu, röle ayar değişikliği ve DoS gibi saldırı senaryoları gerçekleştirilmiştir. Saldırı tespiti için NNge, RF, NB, AB, SVM, DT, OneR, J48, JRip, ABJRip ve önerilen derin öğrenme algoritmaları kullanılmıştır [64].

Basnet ve arkadaşları, SCADA kontrollü elektrikli araç şarj istasyonunda derin öğrenme tabanlı yeni fidye yazılımı algılama çerçevesi önermiştir. Bunun için benzetim ortamında Fidye Yazılımı Odaklı (Ransomware Driven) olan DDoS ve Hatalı Veri Enjeksiyonu (False Data Injection) saldırıları yapılmıştır. Saldırı tespiti için Derin Sinir Ağı, 1 Boyutlu CNN ve LSTM algoritmaları kullanılmıştır [65].

Rajesh ve arkadaşları, endüstriyel kontrol sistemlerine yönelik saldırı tespiti yapmak için gerçek zamanlı SCADA ağ trafiği içeren bir veri kümesi oluşturmuştur. Öznitelik değerlerinin düzenlemesi için Chi-Square, ANOVA ve LASSO with SVMS-MOTE metrikleri kullanılmıştır. Daha sonra saldırı tespiti için RF, SVM, KNN ve NB makine öğrenme algoritmaları uygulanmıştır [66].

Bu çalışma, SCADA mimarisinde DDoS saldırılarına odaklanmakta ve saldırıları tespit etmek için verimli şekilde çalışan modeller sunmaktadır. Literatürde SCADA sistemlerine yönelik saldırı tespiti yapan çalışmalar incelenmiş; tespit için RF, DT, LR, NB, KNN, SVM ve LSTM gibi makine öğrenme algoritmalarının diğer algoritmalara göre daha sık kullanıldığı görülmüştür. Bu çalışmada makine öğrenmesi tabanlı CNN, LSTM, CNN-LSTM hibrit, KS, LWL, KNN, LB, AB, NB, BN, ZeroR, PART, DTa, DT, RF ve RT modelleri (16 adet) kullanılmış ve yüksek başarı oranı elde eden modeller bu çalışma için önerilmiştir. Önerilen bu modeller, mevcut çalışmaların eksikliklerini gidermek ve ilgili alana katkı sunmak amaçlarıyla farklı yöntemlerin kullanımını ön plana çıkarmıştır. Ayrıca

saldırı tespitini gerçekleştirmek için SCADA sistemi kullanılarak üretilmiş ve literatürde benzer çalışmalarda denenmiş bir veri kümesi de test edilmiştir. İncelenen çalışmaların ve bu tez çalışmasının elde ettiği saldırı tespit doğruluk oranları 5.2. Tartışma bölümündeki tabloya yerleştirilmiştir. Böylece, çalışmalar için genel bir inceleme ve kıyaslama imkânı sunulmuştur.

3. KAVRAMSAL VE KURAMSAL ÇERÇEVE

Bu bölümde siber terör kavramı, SCADA sistemleri, SCADA sistem bileşenleri, siber güvenlik konusu ve DDoS saldırıları hakkında bilgiler verilmektedir. Verilen bu bilgilere ek olarak çalışmada kullanılan makine öğrenmesi tabanlı modeller ele alınmakta ve incelenmektedir.

3.1. Siber Terör

Siber tehditlerin uluslararası boyutta kendine yer bulmasıyla güvenlik sorunları ideolojik bakış açılarıyla birlikte değerlendirilmeye başlanmıştır. Siber güvenlikle ilgili yapılan çalışmalar sonucunda hazırlanan veriler siber terörün gelişimine ilişkin durumu ortaya koymaktadır. Siber dünyaya olan ilginin ve bağımlılığın giderek artması terörizme yeni bakış açıları kazandırmaktadır. Terörizmin farklı derecelendirmeler elde ederek boyut değiştirmesi ise yeni bir siber savaş olgusunu beraberinde getirmiştir [67]. Siber terör, terörizmin başkalaşmış bir boyutudur ve 21. yüzyılda ortaya çıkmıştır. Siber terör saldırılarının gerçekleştirilmesi fiziksel saldırılara göre daha kolaydır ve meydana gelecek zararlar hayal edilenin ötesinde olabilir. Karşılık verilmesi, müdahale ve mücadele edilmesi oldukça zor olan bir terör türüdür [68]. Siber dünyanın terörist faaliyetlerini sürdürmek amacıyla değerlendirilmesi sonucunda siber terör terimi ortaya çıkmıştır. Bu terimin herkes tarafından kabul edilen net bir tanımı bulunmamaktadır. Bilgisayar ağlarının veya internetin kullanılması ile kritik altyapı sistemlerinin işlemlerini ve süreçlerini bozmayı veya sistemleri kullanım dışı bırakmayı hedefleyen saldırılardır. Devletlerin çok iyi koruması gereken altyapılarda üretilen verilerin ele geçirilmesi, değiştirilmesi veya yasadışı faaliyetler için kullanılması da amaçlar arasında bulunmaktadır. Bunlara ek olarak siyasi, politik veya ekonomik anlamda halka zarar vermek için de siber terör saldırıları kullanılabilmektedir.

Geleneksel terör ile siber terör arasında bazı farklılıklar bulunmaktadır. Kötü niyetli kişilerin siber terör saldırılarını gerçekleştirme sebepleri ve motivasyon kaynakları farklıdır. Buna ek olarak saldırı için bilinçli olarak bilgi teknolojileri kullanılmaktadır [69]. Psikolojik savaşla birlikte internetin çok kısa sürede milyonlara ulaşma gücü kötü niyetli kişilerin saldırılarını da arttırmaktadır.

3.2. SCADA Sistemi, Bileşenler ve Protokoller

SCADA sistemlerinin anlaşılabilmesi için mimari yapı ve bileşenler hakkındaki bilgiler bu bölümde sunulmaktadır. SCADA sisteminin ne olduğu, bu sistemlerde hangi bileşenlerin ve iletişim protokollerinin kullanıldığı anlatılmaktadır.

3.2.1. SCADA sistemi

SCADA sistemleri kritik altyapıları izleyen, denetleyen ve kontrol eden sistemlerdir. Kritik altyapılar doğal gaz, petrol, su ve benzeri kaynakların üretilmesi veya bir yerden başka bir yere iletilmesi için kullanılmaktadır. Örneğin enerji üretim santralleri, rüzgâr enerjisi türbinleri, doğal gaz dağıtım tesisleri kritik altyapılara örneklerdir. Bunlara ek olarak belediyelerin şebeke suyu dağıtım tesisleri, havayolları, gemi sistemleri gibi daha birçok sistem de kritik altyapı sistemleridir. Ulusal anlamda değerli olduğu kadar uluslararası olarak da önemli bir yere sahiplerdir. SCADA sistemleri bahsedilen bu kritik altyapılar dışında üretim yapan tesislerde, fabrikalarda veya kamu kurumlarında da kullanılmaktadır [70].

Bu kritik altyapılar, günümüze kadar ağ bağımlılığı olmadan ve yalıtılmış durumda çalışmalarını sürdürmekteydi. Günümüzde ise yeni yöntemler, farklı ağ teknolojileri ve internet kullanımı ile bütünleşmeye başlamıştır. Bu gelişmeler yeni güvenlik sorunlarını doğurmuştur. Kritik altyapı sistemlerinde bir siber güvenlik zafiyetinin bulunması birçok soruna sebep olabilir. Örneğin sistemin uzaktan kontrol edilmesi veya sistemin kullanım dışı kalması saldırganlar tarafından gerçekleştirilebilir. Bu ve benzeri sorunlar; toplumu ve dünyayı etkileyebilecek, canlıların yaşamlarını tehlikeye sokabilecek daha büyük sıkıntıların doğmasını tetikleyebilir [71].

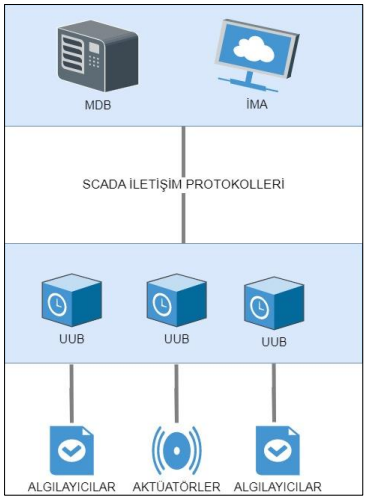
Bu durumların farkında olan ulusal veya uluslararası alanda çalışan kötü niyetli kişiler için farklı sektörlerdeki SCADA sistemleri cazip hedefler haline gelmektedir. SCADA sistemlerinin kullanıldığı alanlar ve sektörler Şekil 3.1’de gösterilmektedir.

Şekil 3.1.SCADA sistemlerinin kullanıldığı sektörler [70]

SCADA sistemleri su tesislerinde, telekominakasyon sistemlerinde, finans işlemlerinde, sağlık sektöründe, kimyasal üretim yapan tesislerde ve daha pek çok alanda kullanılmaktadır. SCADA sistemlerinin oldukça geniş kullanım alanı ve çeşitliliği bulunmaktadır. Bu alanların her biri çeşitli güvenlik tehditleri içerebilir ve bu durum kötü niyetli kişiler tarafından kullanılabilir [70].

3.2.2. SCADA sistem bileşenleri

SCADA sistemleri temel olarak 3 bileşenden oluşmaktadır. Bunlar; MDB, UUB'ler ve haberleşme ağıdır. Bu temel bileşenler Şekil 3.2'de gösterilmektedir. SCADA sistem bileşenleri alt başlıklar halinde incelenmektedir. Buna göre:



Şekil 3.2. SCADA sistemi temel bileşenleri [70]

MDB

MDB, sistemdeki cihazların, bilgisayarların veya sunucuların bağlantı halinde olmasını ve haberleşmesini sağlamaktadır. MDB'nin sağladığı haberleşme ortamı ile SCADA bileşenleri arasındaki işlemler sürdürülür ve izlenir. Burada bulunan İMA ile sistemdeki süreçler grafiksel olarak da takip edilebilir.

Ayrıca, İMA sayesinde sistemdeki süreç kontrolü ve veri toplanması da sağlanmaktadır. Sistemde veya uzak bölgelerde bulunan UUB'lere komut göndermek ve onlardan gelen komutları almak da MDB'nin görevleri arasında yer almaktadır [72].

UUB

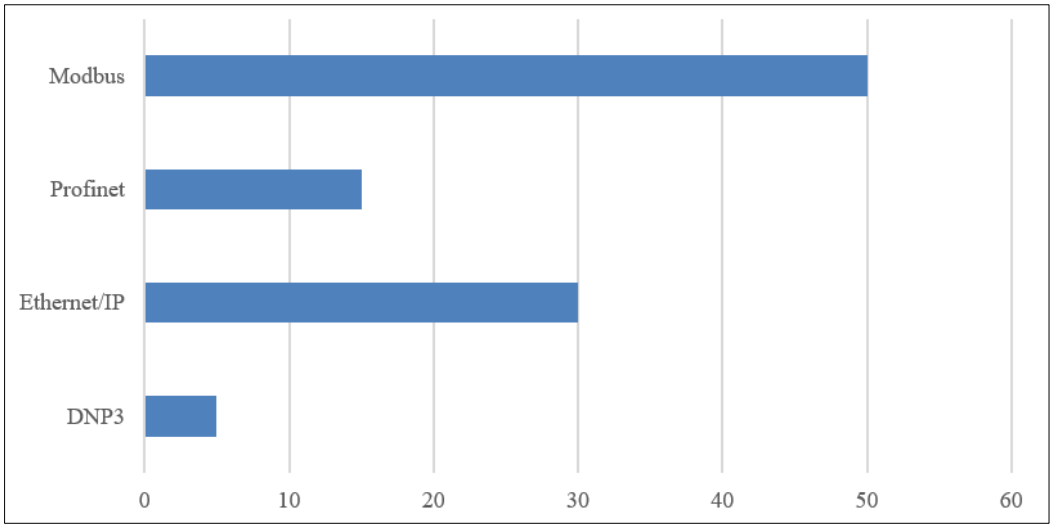
Bu bileşenler sistem tarafından izlenen ve kontrol edilen cihazlardır. Algılayıcılar, aktüatörler ve küçük bileşenler UUB'lara bağlıdır ve sahadaki değişimler bunlar sayesinde gözlemlenir. UUB'ler algılayıcılardan gelen veriyi (ısı, nem, sıcaklık, mesafe, basınç gibi) alır ve MDB'ye iletir. MDB bu veriyi işler ve gerekli gördüğü şekilde komutlar hazırlar. Bu komutlar UUB'lere gönderilir ve uygulanır. Buna göre aktüatörler (pompa, led, buzzer, röle gibi çıkış yapan birimler) çalıştırılır veya çalışma durumlarında değişiklikler yapılır. Sistemde anormal veya istenmeyen durumlar yaşanmaması için daha önceden olası senaryolar değerlendirilmekte ve bunlara uygun komutlar MDB tarafından üretilmektedir. Çerçevesi belirlenmiş olan durumlar veya senaryolar dışında olaylar yaşandığında, SCADA sistemini izleyen operatörlerin dikkatini çekmek için alarm çalıştırılması da bu bileşenler sayesinde gerçekleştirilmektedir [72].

Haberleşme ağları

Tüm sistemde yer alan bileşenler arasında iletişimin veya haberleşmenin sağlanması zorunludur. Bunu sağlamak için SCADA sistemlerinin mimarisine özgü iletişim protokollerinin yer aldığı haberleşme ağları kullanılmaktadır. Sistemlerde uydu, radyo dalgası, mikro dalga, telefon hatları, Yerel Alan Ağı bağlantısı, Geniş Alan Ağı bağlantısı, kablolu/kablosuz bağlantılar ve bulut teknolojisi kullanılabilmektdir [72-75]. Sistemdeki bileşenlerin özelliklerine, bileşenlerin sayısına, veri/komut gönderim hızına veya boyutuna göre farklı ağ yapıları tercih edilebilir.

3.2.3. SCADA sistemlerinde kullanılan iletişim protokolleri

SCADA sistemlerinde MDB ve UUB'ler arasında iletişimi sağlamak için haberleşme ağ ortamı veya ortamları tasarlanmıştır. Bu ortamlardaki ağ yapısına uygun şekilde haberleşme protokolleri yer alır ve bunların mimarileri birbirinden farklıdır. SCADA sistemlerinde sıklıkla kullanılan ve literatürde yer alan bazı haberleşme protokolleri şunlardır: Modbus, DNP3, Profinet, PROFIBUS, Ethernet/IP, RP-570, Conitel, IEC 60870 [76-79].



Şekil 3.3. SCADA sistemlerindeki protokollerin (%) kullanım oranları [79]

Şekil 3.3'e göre endüstriyel kontrol sistemlerinde ve SCADA ağlarında en çok kullanılan protokollerden biri Modbus protokolüdür. Açık kaynaklı olması ve kullanım kolaylığı sunması nedenleriyle cihaz bağlantılarında ve MDB-UUB arasındaki iletişimde sıklıkla tercih edilmektedir [80-82]. Bu bilgi, Modbus protokollerinin maruz kalabileceği saldırıların etkili olabileceğini, bu etkilerin ülkemizde ve dünya üzerinde herhangi bir yerde görülebileceğini anlatmaktadır. Bu durumlar göz önüne alındığında SCADA sistemlerine ve Modbus protokolüne özgü hazırlanacak saldırı tespit modelleri ile dünya genelinde kullanılan bu sistemlerin güvenliğinin daha etkin şekilde sağlanması kolaylaşacaktır.

Modbus protokolü

Bu protokol, 1979 yılında SCADA sistemlerine özgü hazırlanmış ve artık standart olarak kullanılan bir haberleşme protokolüdür. Çok sayıda üretici firma ve şirket bu protokolü kullanarak cihazlar ve sistemler geliştirmektedir. Bu protokol çeşitli ağ türlerine eklenmiş bileşenler arasındaki istemci-sunucu iletişiminde kullanılan uygulama katmanı mesajlaşma

protokolüdür. Bu protokol için varsayılan olarak 502. port kullanılmaktadır. Günümüz uygulamalarında farklı amaçlar için kullanılmaktadır. Bunlar:

- İnternet ile TCP/IP haberleşmesinin yapılması,
- Radyo frekansı, kablo, fiber optik, telefon hattı, mikrodalga veya uydu gibi farklı iletişim ortamları ile eşzamanlı olamayan seri haberleşmenin yapılması,
- Modbus Plus ile yüksek hızlı jeton geçirme ağı üzerinden haberleşmenin yapılması.

Modbus protokolünde istek mesajları belirlenen UUB'lere gönderilir ve bunlara ilişkin geri yanıtlar döner. Modbus TCP ve Modbus Seri olmak üzere iki farkı Modbus protokolü türü bulunmaktadır [77]. Modbus TCP protokolü IP tabanlı ağlarda çalışır ve MDB'ye çoklu işlemler yapabilme imkânı sunar. UUB'lerin paralel şekilde çalışmasına olanak sağlar.

Modbus Seri protokolü ise, iletişim katmanından bağımsızdır ve basit bir Protokol Veri Birimi tanımlar. Modbus mesajlarının belirli veri yollarına veya ağlara eşlenmesini sağlayarak uygulama veri biriminde ek alanlar sunulmasına imkân sunar [83]. Veriler iki farklı iletim modu üzerinden gönderilir ve alınır. Bunlardan ilki Bilgi Değişimi için Amerikan Standart Kodu (American Standard Code for Information Interchange, ASCII) modudur. Bu mod, verilerin uzun mesaj çerçevesine sahip olmasından dolayı sistemin yavaşlamasına sebep olur. Diğer mod olan Uzak Telemetri Birimi modu ise daha kısa çerçeveye sahip veriler ile ilgilenir. Ayrıca bu modda eşlik ve hata denetimi bulunmaktadır. Bu modda RS-232, RS-422 ve RS-485 gibi çeşitli ara yüz standartları yer almaktadır.

DNP3 protokolü

DNP3, 1990'ların başında Westtronic Şirketi tarafından geliştirilmiştir. Bu protokol, bir SCADA sistemindeki cihazların kontrol komutlarını nasıl ilettiğini ve verileri nasıl işlediğini tanımlar. DNP3, bir ana kontrol merkezi ve dış istasyon cihazları arasında üç basit iletişim modunu destekler. İlk iletişim olan tek noktaya yayın işleminde, ana birim adreslenmiş bir dış istasyon cihazına bir istek gönderir ve cihaz bir yanıt verir. İkinci iletişim modu olan bir yayın işleminde, ana birim ağdaki tüm dış istasyonlara bir istek gönderir. İstasyon dışı cihazlar yayın mesajına cevap vermez. Üçüncü iletişim modu ise dış istasyon cihazlarından gelen istenmeyen yanıtları içerir. Bu yanıtlar genellikle periyodik güncellemeler veya uyarılar sağlamak için kullanılır [84].

Profinet protokolü

PROFIBUS International tarafından yönetilen bu Profinet protokolü bir merkezi istasyona ve merkezi olmayan cihazlara dayalı sağlayıcı/tüketici iletişim modelini kullanır. Bu protool yapısında üç çeşit cihaz bulunur. Bunlardan ilki denetleyici cihazdır ve cihazların yapılandırılmaından sorumludur. Veri alışverişi bu cihaz tarafından kontrol edilir. İkinci cihaz ise döngüsel işlem verileri sağlayan saha cihazı ile elde edilir. Sonuncu danışman cihaz ise görev atamak veya tanıtım yapmak amaçlarını uygulamak için mühendislik istasyonunu veya bir İMA'yı temsil eder [85].

PROFIBUS protokolü

PROFIBUS, otomasyon teknolojisinde Fieldbus iletişimi için tanımlanmış uluslararası açık bir standarttır. PROFIBUS'ın üç özelliği vardır. İlki bilgisayarlar ve PLC'ler arasındaki veri iletişimi için PROFIBUS Fieldbus Mesaj Şartnamesidir. İkincisi PROFIBUS Fieldbus Merkezi Olmayan Çevre Birimleridir ve bunlar dağıtılmış saha cihazlarını merkezi bir denetleyiciye bağlar. Sonunucusu ise PROFIBUS Süreç Otomasyonudur. Tehlikeye açık alanlarda, patlama olasılığını azaltan düşük bir seviyede, aynı kablo üzerinden hem güç hem de veri taşıyan bir teknoloji ile geliştirilmiştir. PROFIBUS protokol yığınının ve telgrafların özelliklerinden dolayı bu protokolde gizlilik ve bütünlük kontrolleri yapılamamaktadır. Açık Sistem Ara Bağlantısı (Open Systems Interconnection - OSI) modelinin herhangi bir katmanında tanımlanmış kimlik doğrulama veya yetkilendirme kontrolleri yoktur ve telgraflar açık metin olarak iletilir. Bundan dolayı PROFIBUS kullanılan endüstriyel ağlar siber saldırılara açık durumdadır [86].

Ethernet/IP protokolü

İletişim bant genişliğini arttıran endüstriyel Ethernet üzerinden veri iletişimini destekleyen Ethernet/IP protokolü Rockwell Automation tarafından önerilmiş ve 2001 yılında kullanıma sunulmuştur. Günümüzde üretim otomasyonu için gelişmiş, olgun ve eksiksiz endüstriyel Ethernet çözümleri sunmaktadır. Kullanıcılar açık teknolojilerden ve internetten yararlandığı için bu protokol hızlı bir büyüme göstermiştir. Ethernet/IP, Elektrik ve Elektronik Mühendisleri Enstitüsü (The Institute of Electrical and Electronics Engineers - IEEE) 802.3 standardı ve TCP/IP paketi üzerinden ortak endüstriyel protokolü uygular [87].

RP-570 protokolü

RP570 Protokolü, 1990 yılının başında geliştirilmiştir. Bir istasyondaki UUB ile genellikle SCADA yazılımı arasında kullanılan bir protokoldür. Şu anda IEC 60870 olarak bilinen IEC 57 bölüm 5-1'e dayanmaktadır. Bilinen sürümleri RP571, ADLP80 ve ADLP180'dir [88].

Conitel protokolü

Continel protokolü, birçok SCADA sisteminde kullanılan eşzamanlı olmayan bir iletişim protokolüdür. Protokol, noktadan-noktaya, çoklu-bırakma yapılandırılmasında; yarım veya tam çift yönlü işlemlerde kullanılabilir. İletişim güvenliği, her mesaj bloğuna dâhil olan 5 bitlik bir döngüsel kod ile sağlanır. Conitel protokolündeki tüm iletişim değişimleri ana bilgisayar tarafından başlatılır. Uzaktan bağlanan bir cihaz ana bilgisayarla herhangi bir alışverişi başlatamaz ve başka bir uzaktan cihaz ile doğrudan adresleme veya iletişim kuramaz [88].

IEC 60870-5 protokolü

IEC 60870-5-104 iletim protokolü, SCADA sistemlerinde temel kontrol görevleri için kullanılabilen TCP/IP tabanlı IEC 60870-5-101 için ağ erişimi sunar. Bu protokol mesajları herhangi bir kimlik doğrulama mekanizması olmadan açık metin olarak iletir. Bu yüzden siber güvenlik sorunları barındırmaktadır [89].

3.3. SCADA Sistemlerinde Siber Güvenlik

SCADA sistemlerinin kullanıldığı yapıların çoğu internet ağına doğrudan bağlı değildir ve dış ağlardan ayrı bağımsız şekilde çalışmaktadır. Gelişen teknolojiler internet kullanım alanını genişletmekte ve bu durum SCADA sistemlerini de etkilemektedir. SCADA sistem güvenliğinin sağlanması da zorunlu hale gelmiştir. Bunun için öncelikle güvenlik açıklıklarını belirlemek ve gerçekleşen siber saldırıları incelemek gerekmektedir. Bu konularla ilgili bilgiler bu bölümde alt başlıklar halinde sunulmaktadır.

3.3.1. SCADA sistemlerinin güvenlik açıklıkları

Farklı teknolojilerin birlikte kullanılması, internet bağlantısından faydalanılması ve uzaktan sisteme erişilmesi gibi yenilikler SCADA sistemleri için yeni siber güvenlik sorunlarını doğurmuştur. Gelişen teknolojiye hızlı ayak uyduramayan SCADA sistemleri, mimarisi yapısı gereği birçok güvenlik sorununu da barındırmaktadır.

SCADA sistemleri ilk başta, dış ağdan bağımsız şekilde tasarlanmıştır. Kapalı devre çalışacak şekilde hazırlanmış ve tasarımında siber güvenlik mekanizmaları planlanmamıştır [90]. Siber güvenlik mekanizmalarına sahip olmadığı için güvenlik zafiyetleri barındırmaktadır. Örneğin SCADA sisteminde cihaz veya uç birimlerde kullanılan algılayıcı sayılarının artması, elemanlar arasında daha büyük veri iletiminin yapılması sistemde karmaşıklığı arttırmaktadır. Artık SCADA sistemlerinde internet kullanımı sayesinde yeni teknolojilerin kullanımı giderek artmaktadır. Sistem kullanıcıları varsayılan veya zayıf özellikli parola kullanabilmekte, başkalarıyla parola paylaşımı yapabilmekte ve sisteme uzaktan erişim özelliğini tercih edebilmektedir. Saldırı tespit sistemi, saldırı engelleme sistemi veya antivirüs yazılımları gibi güvenlik çözümleri de SCADA sistemlerinin güvenliğini tam olarak sağlayamamaktadır. Böylece SCADA sistemlerinde güvenlik zafiyetleri oluşmaktadır; saldırganların sisteme sızması ve zarar vermesi kolaylaşmaktadır. Bu güvenlik zafiyetleri DDoS gibi saldırı türleri ile ele alınarak, SCADA sistem bileşenlerinin manipüle edilmesine sebep olabilir [91]. Sistem bileşenlerinin anormal hareketleri veya hiç çalışmaması SCADA sistemini durdurabilir ve hatta bağlantılı farklı sistemlerin işleyişlerine de zarar verebilir. Bu durumların farkında olan ulusal veya uluslararası alanda uygulamalar gerçekleştiren kötü niyetli kişiler için farklı sektörlerdeki SCADA sistemleri dikkat çekici hedefler haline gelmektedir.

3.3.2. Modbus protokolünün güvenlik açıklıkları

Güvenli olmayan iletişim protokollerinin kullanılması da sistem güvenliğini tehlikeye atacak sorunlara yol açar. Modbus TCP/IP protokolü şifreli iletişim sağlamaz, kimlik doğrulama kontrolü yapmaz ve yetkilendirme yapmaz. Ayrıca Modbus TCP/IP çok fazla güvenlik açıklığı barındırmasına rağmen kolay kullanılabilirliğinden dolayı en çok tercih edilen iletişim protokollerinden biridir [81,82]. Modbus TCP/IP protokolü güvenlik zafiyetlerinden dolayı DoS, DDoS, MITM ve Komut Enjeksiyonu gibi saldırılara karşı savunmasızdır

[70,92]. DDoS saldırısı yöntemi ile Modbus TCP/IP protokolünün yetkilendirme eksikliği zafiyeti manipüle edilerek MDB cihazından UUB'lere mesajlar gönderilebilir. Böylece UUB'nin kaynakları tüketilebilir veya kullanılamaz hale getirilebilir. Örneğin Alabama'daki Browns Ferry Nükleer Santralinde büyük bir güvenlik sorunu yaşanmıştır. Bu santrale yönelik DDoS saldırıları gerçekleşmiş ve bu yüzden santral kullanım dışı kalmıştır [81].

3.3.3. SCADA sistemlerine yönelik siber saldırılar

SCADA sistemlerinin kullanıldığı yapılarda veya SCADA sistemlerinde; yeni bir güvenlik açıklığının fark edilmesi, eski bir açıklığın devam etmesi, varolan bir açıklığın sömürülmesi, sisteme zarar verilmesi veya sistemin çalışamaz hale getirilmesi gibi birçok senaryo günümüzde gerçekleşebilecek durumdadır. Sistemin uzaktan ele geçirilmesi veya sistemde güç kesintilerinin oluşturduğu aksamaların yaşanması olası senaryolar dâhilindedir. Örneğin elektrik üretim veya dağıtım tesislerinin hedef alınması ile siber saldırılar gerçekleştirilebilir. Bu saldırılar sonucunda şehirler bir anda karanlığa bürünebilir veya enerji kesintileri yaşanabilir. Gerçekleşen en önemli saldırılardan biri olan Stuxnet saldırısında hedef olarak seçilen nükleer santralde yer alan santrifüjlerin çalışması uzaktan bozulmuştur. Sisteme fiziksel olarak zarar verilmiş ve sorunlar operatörler tarafından yaklaşık 2 yıl sonra fark edilmiştir [93]. Bir başka örnek ise Florida Şehir Su Kaynağının uzaktan zehirlenmeye çalışılmasıdır. Saldırganlar tarafından su tesisi ele geçirilmiş ve şehir suyundaki Sodyum Hidroksit seviyesi arttırılmaya çalışılmıştır. Yetkililer durumu fark ettiği için hızlıca olaya müdahale etmişler ve saldırıyı engellemişlerdir [94]. Buna benzer yaşanmış saldırı örnekleri Çizelge 3.1'de özetlenmektedir [95].

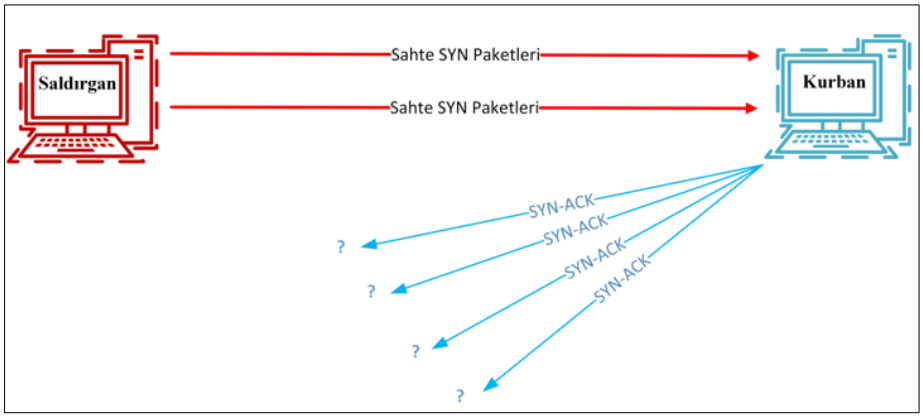
Çizelge 3.1. SCADA sistemlerine yönelik gerçekleşmiş siber saldırılar [95]

No	Saldırı Örneği	Etkilediği Alanlar/Bölgeler	Gerçekleştiği Yıl	Etkileri
1	Logical Bomb	Sibirya gaz boru hattı	1982	Sistemi yöneten bilgisayar devre dışı bırakıldı.
2	Titan Rain Attacks	Pentagon'daki bilgisayar ağlarında yer alan Amerikan bilgisayar sistemleri	1998	Redstone Arsenal, NASA ve Lockheed Martin Şirketi saldırıya uğratıldı.
3	Sven JASCHAn's Virus	Delta Hava Yolları	2004	Kıtalararası seferler iptal edildi.
4	Shady RAT Attacks	14 ülkedeki devlet kurum ve işletmeleri (enerji, sanayi, elektronik, haberleşme, inşaat, savunma alanları), Birleşmiş Milletler gibi uluslararası kuruluşlar	2006-2010	Devletler, kuruluşlar, büyük şirketler, savunma şirketleri ve uluslararası olimpiyat komiteleri hedef alındı. ABD, Japonya, Tayvan, İngiltere, Hindistan, Güney Kore, Vietnam ve Kanada gibi ülkeler zarara uğratıldı.
5	Hannaford Bros Attacks	Amerikan perakende zincirlerinden Hannaford Bros gıda perakendecisi	2007	Şirkete ait hassas bilgiler ve hesap bilgileri ele geçirildi. Şirket maddi zarara uğratıldı.
6	Estonia Cyber Attacks	Estonya kuruluşlarının internet siteleri	2007	Kurum ve kuruluşların web sitelerine siber saldırılar düzenlendi ve erişimler engellendi. Estonya'nın sosyal medyasında sahte haberler paylaşıldı.
7	Stuxnet Attack	Özellikle nükleer enerji sektöründe kullanılan sistemler	2010	İran, virüsten çok etkilendi ve milyonlarca dolar kaybetti. Nükleer santrallerdeki santrifüj makinelerinin olağanüstü hızlarda döndüğü anlaşıldı.
8	Disttrack/Shamoon Virus	Enerji sektöründeki sistemler	2012	Saudi Amarco Company firmasının yaklaşık 30.000 iş istasyonu saldırıya uğradı. Buralardaki operasyonlar olumsuz etkilendi.
9	Singapore Cyber Attacks	Singapur hükümeti web siteleri	2013	Anonim bilgisayar korsanlığı tarafından bir kaç gün boyunca saldırılar gerçekleştirildi.
10	OpIsrael Attacks	İsrail olarak kabul edilen web siteleri	2013	Okullara, gazetelere, küçük işletmelere, kuruluşlara ve bankalara ait web sitelerine saldırılar yapıldı.
11	Attack on the Ukrainian Power Grid	Ukrayna'nın Ivano-Frankivsk bölgesindeki bir elektrik dağıtım şebekesi	2015	Bu bölgede elektrik kesntileri oldu. İnsanlar saatlerce elektriksiz kaldı.
12	The Oldsmar Attack	Oldsmar Florida su arıtma tesisi	2021	Sudaki sodyum hidroksit içeriği geçici bir süreliğine zehirli düzeylere kadar çıkarıldı. Tesis operatörü durumu farkedip suyun değerlerini normal düzeye döndürmeyi başardı.

Çizelge 3.1'de yer alan saldırı örneklerinden anlaşılacağı üzere, siber saldırılar SCADA sistemlerinin bir bölümünü veya tamamını etkileyebilir. Bunlara ek olarak, yaşanan problemler SCADA sistemleriyle bağlantılı bulunan diğer sistemleri de olumsuz şekilde etkileyebilir. Günümüzde halkın huzurunu bozacak, günlük yaşamını zorlaştıracak veya sağlığına zarar verecek eylemler SCADA sistemlerindeki açıklıklar kullanılarak gerçekleştirilebilir duruma gelmiştir. Bu sebeplerden dolayı SCADA sistemlerinin siber güvenliğinin sağlanması zorunlu hale gelmiştir.

3.3.4. DDoS saldırıları

SCADA sistemleri gerçekleştirdiği görevlerden, geleneksel mimari yapısından ve içerisinde kullanılan iletişim teknolojilerinden dolayı farklı saldırılara maruz kalmaktadır. Özellikle gelişen saldırı teknikleri ile daha fazla hedef haline gelmekte ve güvenlik riski her geçen gün artmaktadır. SCADA sistemlerine yönelik MITM, Veri Enjeksiyonu, Komut Enjeksiyonu, DoS ve DDoS gibi çeşitli saldırılar yapılmaktadır [96,97]. Bunlar arasında DDoS saldırıları her SCADA sistemini etkileyebilecek şekilde yaygın olarak görülen ve tehlikeli bir saldırı türüdür. Bu saldırılar kontrol ve süreç işleyişlerini bozmayı ve sistemi kullanım dışı bırakmayı amaçlar [98,99].



Şekil 3.4. DDoS saldırısı gösterimi [98-100]

Şekil 3.4'te görüldüğü üzere, DDoS saldırıları sistemlerin kullanıcılarına cevap vermesini engellemek amacıyla gerçekleştiren saldırılardır. Saldırıya uğrayan sistemlerin ağ kaynakları, saldırıya karşı koymakta zorlanmaktadır. Bu durum ağ altyapısının büyük çapta zarar görmesine sebep olmakta ve hizmetleri geçici veya kalıcı olarak çalışmaz hale getirmektedir. Saldırılar iki şekilde gerçekleştirilir. Birincisi, virüs bulaştırılan zombi

bilgisayarlar veya saldırganların kullandığı bilgisayarlar aracılığıyla hedef sistemin servislerine çok sayıda istek gönderilir. İkincisi ise hedef sisteme sızılarak sistemin ağ elemanlarının güvenlik açıklıkları tespit edilir ve bu açıklıklar kullanılarak hedef sistem kullanılamaz hale getirilir. DDoS saldırıları sonucunda sistemler hizmet veremediği için maddi zarar, itibar kaybı, zaman kaybı ve bilgi hırsızlığı meydana gelmektedir. Bu saldırı türlerinin bazıları şunlardır:

- Kullanıcı Veri Bloğu İletişim Kuralları Seli Atağı (User Datagram Protocol (UDP) Flooding Attack): Saldırgan cihaz çok sayıda sahte UDP paketini rastgele seçilen kurban sisteme veya sistemlere gönderir. Saldırgan, kurban sistemin ağında bulunan bant genişliğinin tümünü tüketmeyi amaçlar.
- Senkronize Seli Atağı (Synchronize (SYN) Flooding Attack): En sık görülen saldırılardan biridir. TCP bağlantılarının üçlü el sıkışma süreci saldırı amaçlı kullanılır. Saldırgan, kurban sistemlere çok sayıda TCP-SYN isteği gönderir ve kurban sistemler her SYN paketine cevap vermeye çalışır. Saldırgan Onay (Acknowledgement – ACK) paketlerine SYN-ACK paketiyle cevap vermez. Kurban sistemler, gönderdiği paketlere cevap alana kadar paket göndermeye devam eder. Bu durum hafızanın dolmasına, işlem gücünün azalmasına ve kaynakların giderek tüketilmesine sebep olur.
- Aktarım Denetimi Protokolü Seli Atağı (Transmission Control Protocol (TCP) Flooding Attack): SYN Saldırısına benzer mantıkta üretilen saldırılardır.
- IP Sahteciliği Seli Atağı (Spoofing Internet Protocol (IP) Flooding Attack)
- İnternet Kontrol Mesajı Protokolü Seli Atağı (Internet Control Message Protocol (ICMP) Flooding Attack): Saldırgan cihaz tarafından ICMP protokolü kullanılarak kısa sürede, anlamlı veya anlamsız veri paketlerinin kurban sistemlere gönderilmesidir. Kurban sistemin bu isteklere cevap verememesi hedeflenir.

SCADA sistemleri en çok DDoS saldırılarına maruz kalmaktadır. Bu saldırılar SCADA sistemindeki MDB veya uç elemanlara çok fazla istekler yollayarak yoğun bir trafiğe sebep olmaktadır. Böylece hedef makine gerçek isteklere bile yanıt veremez hale gelmektedir [100]. SCADA sisteminde bir makinenin gerçek kullanıcı isteklerine cevap verememesi bağlantılı bulunduğu diğer makineleri veya uç birimleri de etkilemekte ve veri/komut alışverişini durdurabilmektedir. Kritik altyapılarda kullanılan SCADA sistemlerine yönelik gerçekleşecek DDoS saldırıları kritik altyapının kullanım alanlarında tetikleyici ve yıkıcı etkilere sebep olabilir.

3.4. Kullanılan Makine Öğrenmesi Tabanlı Modeller

Literatür incelendiğinde SCADA sistemlerine yönelik saldırı tespitinin yapılmasında makine öğrenmesi yöntemlerinin de kullanıldığı görülmüştür. Bu çalışmada, SCADA sistemi kullanılan test yatağı ortamına yönelik DDoS saldırılarının tespiti ve DDoS saldırı türü belirlenmesi için makine öğrenmesi tabanlı modeller kullanılmıştır.

Makine öğrenmesi ile gerçek dünya problemlerine çözüm geliştirmeye yönelik bir model hazırlanırken verinin işlenecek hale getirilmesi, modelin oluşturulması, modelin eğitilmesi ve modelin test edilmesi gibi ana işlemler gerçekleştirilmektedir. Ayrıca, makine öğrenmesi modellerinin oluşturulması için pekiştirmeli, denetimli ve denetimsiz öğrenme gerçekleştirilmektedir [101]. Bu çalışmada kullanılan veriler etiketli (5 saldırı ve 1 normal durum senaryoları) olduğu için denetimli öğrenme kullanılmıştır.

Yaygın olarak kullanılan algoritmalardan CNN ve LSTM, tek başına ve farklı algoritmalarla birlikte literatürde ele alınmıştır. Bu tez çalışmasında literatüre katkı sunmak amacıyla CNN ve LSTM algoritmaları tek tek değerlendirilmiş ve testler yapılmıştır. Daha sora bu iki algoritma birlikte ele alınarak hibrit bir model oluşturulmuş ve testler yapılmıştır. CNN modeli ve LSTM modeli farklı özelliklerde ikişer tane test işleminden geçirilmiştir.

Bu modellerin dışında Tembel Öğrenme (Lazy Learning) Metotlarından KS, LWL ve KNN algoritmaları da kullanılmıştır. Meta Öğrenme Metotlarından LB ve AB algoritmaları; Bayes metotlarından NB ve BN değerlendirilmiştir. Kural (Rule) tabanlı olanlardan ZeroR, PART ve DTa algoritmaları ve Ağaç (Tree) tabanlı olanlardan DT, RF ve RT algoritmaları analiz edilmiştir. Hazırlanan tüm modeller daha önce bahsedilen performans metriklerine göre kıyaslanmıştır ve elde edilen sonuçlar Çizelge 5.1'e yerleştirilmiştir. Kullanılan modellere ait anlatımlara bu bölümde yer verilmiştir.

3.4.1. CNN modeli

CNN algoritması ileri beslemeli sinir ağının bir çeşididir. Birçok alanda ve sınıflandırma gibi farklı amaçlar için kullanılmaktadır [102]. CNN algoritmasının mimarisi çok katmanlı bir algılayıcıya benzer ve birbirine bağlı üç katmandan oluşur. Bunlar birden fazla olabilen

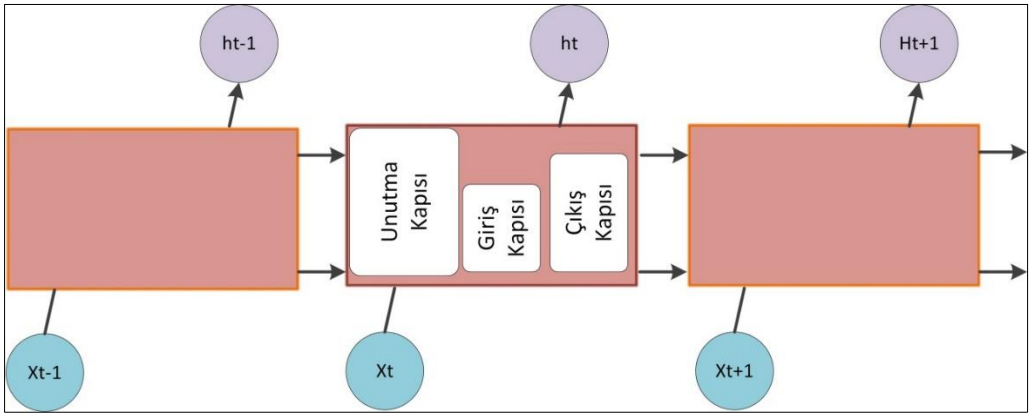
Evrişim Katmanı (Convolution Layer), Havuzlama Katmanı (Pooling Layer) ve Tamamen Bağlı Katmanlardır (Fully Connected Layer) [103].

Evrişim Katmanında çekirdekler (kernels) kullanılarak filtreleme ve boyut indirgeme yapılmaktadır. Böylece derin özniteliklerin elde edilmesi sağlanır. Filtreleme işleminde kullanılan filtrelere ait parametreler eğitim boyunca güncellenir. Veri setindeki gizli öznitelikleri çıkarmaya veya almaya yarayan birden çok filtre bu algoritmada yer almaktadır [104]. Havuzlama Katmanı öğrenme aşamasında meydana gelen bozulmaları azaltmak ve öğrenebilir parametre sayısını düşürmek için kullanılmaktadır. Bu katman alt örneklemeler yapar ve böylece öznitelik matrisinin boyutunu azaltır. En Fazla Havuzlama (Max Pooling), Ortalama Havuzlama (Average Pooling) ve Küresel Ortalama Havuzlama (Global Average Pooling) olarak üç tane havuzlama yöntemi bulunmaktadır [105]. Çalışmada En Fazla Havuzlama kullanılmıştır.

Evrişim ve Havuzlama Katmanlarından sonra Düzleştirme (Flatten) işlemi uygulanır. Tamamen Bağlı Katmanda, öznitelik matrisi tek boyutlu diziye dönüştürülür. Bir veya daha fazla Tamamen Bağlı Katman ile her giriş dizisi bir çıktıya bağlanır. CNN algoritmasında kullanılan son Tamamen Bağlı Katmanın çıkış dizisinin boyutu ile verideki sınıf sayısı aynı olmalıdır [105].

3.4.2. LSTM modeli

LSTM algoritması tekrarlayan bir sinir ağıdır ve son zamanlarda sıklıkla kullanılmaktadır. Yapısı gereği uzun süreli bağımlılıkları yakalamada çok etkilidir. Özel bellek hücresi mimarisi ile bilgiyi uzun süre depolayabilir [106]. LSTM algoritmasına ait temel mimari yapı Şekil 3.5’te gösterilmektedir.



Şekil 3.5. LSTM algoritmasının temel mimari yapısı [106]

Şekil 3.5'e göre, bu algoritma bellek blokları olarak bilinen ve tekrarlayan sıralı bloklardan oluşmaktadır. Burada hücreler arasında giriş çıkış yapan ve bilgi akışını düzenleyen Giriş, Çıkış ve Unutma Kapısı bulunmaktadır. Bir blok girişinden elde edilen çıkış, tekrar blok girişine gönderilir. Daha sonra kapılarla bağlantı kurulur. Yineleme işlemi için xt girdiyi oluşturur ve mevcut duruma göre öngörülen çıkış değeri elde edilir. Bir sonraki çıkış vektörü olarak ht oluşturulur. Varolan durumu sıfırlamak için ise Unutma Kapısı kullanılır.

3.4.3. CNN-LSTM Hibrit modeli

CNN ve LSTM modelleri birlikte kullanılarak hibrit bir model elde edilmiştir. Bu modelin mimarisinde yer alan parametre değerleri değiştirilmiş ve farklı test işlemleri gerçekleştirilmiştir.

3.4.4. KS modeli

KS algoritmasında bir bileşen diğer bileşene dönüştürülürken entropi hesabı yapılmaktadır. Burada bileşenler arasındaki mesafe metriği hesaplanmaktadır. Algoritmada yer alan tüm kategorilerdeki bileşenlerin, yeni bileşen ile mesafe olasılıkları toplanır. Daha sonra bu toplamın en az veya benzer değerde olduğu sınıf türü belirlenir ve yeni bileşen ile bu sınıf etiketlenir [107].

3.4.5. LWL modeli

LWL algoritması, örnek ağırlıkları bulmak için örnek tabanlı bir algoritma kullanarak öğrenmeyi gerçekleştirir. Sınıflandırma veya regresyon yapmak için kullanılır. Tembel

Öğrenme grubunda yer alan bu algoritma, kendi yapısı içerisinde sınıflandırıcı olarak farklı bir algoritma kullanmaktadır. Bu algoritmaya ait parametre değerlerini de almaktadır [108].

3.4.6. KNN modeli

KNN algoritması regresyon ve sınıflandırma problemlerinde sıklıkla kullanılan verimli bir yöntemdir. Öncelikle veri kümesindeki veriler etiketlenir ve eğitim veri kümesi hazırlanır. K tane sınıf merkezi belirlenir ve uzaklık fonksiyonu ayarlanır. Yeni bir veri kümesi üzerinde bu yöntem uygulanır. Yeni verinin, eğitim veri kümesinde yer alan veriyle olan mesafesi uzaklık fonksiyonu kullanılarak ölçülür. Uzaklığı en kısa olan k sayıda veri, eğitim veri kümesinden seçilir ve sınıflama kümesi oluşturulur. Seçilen veri sınıfı, oluşturulan sınıflama kümesinin en sık içerdiği sınıf olarak belirlenir ve yöntem sonlandırılır [109]. K sayısının ve farklı uzaklık fonksiyonlarının seçilmesi önemlidir ve bunlar yöntemin performansını etkiler.

3.4.7. LB modeli

Zayıf öğrenenleri güçlü öğrenenlere dönüştürmek için ağırlıklı ortalamaları kullanan bir algoritmadır. Farklı iterasyonlar gerçekleştirerek, çok sayıda zayıf öğrenicileri uyumlu bir sıraya yerleştirmeyi amaçlar [110].

3.4.8. AB modeli

AB modeli, zayıf öğrenme durumunu güçlendirmeyi amaçlar ve öğrenmeyi artırma yöntemini kullanır. Herhangi bir makine öğrenmesi algoritmasının performansını arttırmak için de kullanılabilir. Genellikle zayıf öğrenen bir algoritma olarak tek seviyeli bir DT kullanır. Bu algoritmadaki öğrenen sayısı arttıkça işlem yükü ve öğrenme performansı artar [111].

3.4.9. NB modeli

Bu algoritma olasılık ilkesine göre davranır. Girdi olarak kullanılan verinin sınıfını belirlemeyi amaçlar. Her sınıfın olasılığını hesaplar ve bunu farklı şekillerde kullanır. Büyük veri kümelerinde ve dengesiz olan veri kümelerinde de bu algoritma ile analizler yapılabilmektedir. Bu modelde analiz yapmak için öncelikle veri kümesi tanımlanır ve daha

sonra sınıflar belirlenir. Veri, eğitim yapılması için bölünür ve eğitim verilerinde her sınıfa ait örnekler bulunmalıdır. Buna göre olasılık işlemleri yapılmakta ve daha sonradan gelen test verilerine işlemler uygulanmaktadır. Test verilerinin de sınıfları tespit edilmektedir. Test verilerinin tespit oranlarının yüksek çıkması için daha fazla eğitim verisi kullanılmalı ve analiz edilmelidir [109].

3.4.10. BN modeli

Bu algoritma, değişkenleri birer düğüm olarak ele alır. Değişkenler kümesinde veya uzayında çalışan bu yöntem sayesinde, varolan değişken ilişkileri üst ve alt düğüm bağlantıları kurularak oklarla veya geçişlerle gösterilir [107].

3.4.11. ZeroR modeli

Sınıflandırıcı oluşturan ve oluşturduğu sınıflandırıcıyı kullanan bir algoritmadır. Sayısal değerlerden oluşan bir sınıf için ortalamayı tahmin edebilir [108].

3.4.12. PART modeli

Bu kural tabanlı sınıflandırıcı algoritması; böl ve fethet stratejisi ile ayır ve fethet stratejisini birleştirir. Varolan örnek kümesinde kısmi bir DT hazırlar ve bundan da bir kural oluşturur [112].

3.4.13. DTa modeli

Bu algoritma basit şekilde bir karar tablosu kullanır. Çoğunluk sınıflandırıcısı oluşturur ve sınıflandırma yapar [108].

3.4.14. DT modeli

DT, sayısal ve kategoriye ayrılmış veriler üzerinde çalışabilen bir sınıflandırma algoritmasıdır. Öğrenme aşamasında öğrenilen bilgi bir ağaç üzerinde modellenir ve ağaçtaki her düğüm bir özniteliği ifade eder. Öğrenme amaçlı kullanılan veri kümesi küçük kümelere bölünür ve sınıf üretme üzerinde etkisi kalmayana dek bölünme işlemi özyineli

şekilde devam eder. Bu algoritma eksik değerlerden ve öznitelikler-sınıflar arasındaki doğrusal olmayan ilişkilerden etkilenmez [113].

3.4.15. RF modeli

RF algoritması hem sınıflandırma hem de regresyon problemlerinde kullanılmakadır. Birden çok karar ağacı bir araya gelir ve RF algoritması sonucu farklı ormanlar oluşur. Bu ormanlar, sonuçlar için tahminlerde bulunur ve en yüksek başarıya sahip olan tahmin çözüm olarak önerilir. Sonuçların ortalaması alındığı için ve farklı değişkenlerle farklı ağaçlar ele alındığı için performansı yüksek bir algoritmadır [109].

3.4.16. RT modeli

RT algoritmasında her düğüm için K tane rastgele öznitelik seçilir ve buna göre uygun bir ağaç oluşturulur. Sınıflandırma yapan, regresyon yapan ve olasıklıları tahmin eden bir algoritmadır [108].

4. MATERYAL VE METOT

Bu bölümde hazırlanan test yatağı detaylı biçimde anlatılmaktadır. Test yatağına yönelik gerçekleştirilen saldırılar belirli senaryolar dâhilinde verilmiştir. Test yatağından elde edilen veri kümesi ve bu veri kümesinde hangi özniteliklerin olduğu hakkında bilgiler verilmiştir. Veri kümesinin analiz edilmesi için kullanılacak metrikler ve açıklamaları da bu bölümde yer almaktadır. Önerilen modellerin mimari yapıları hakkında bilgi verilmektedir. Bu bölümde yer alan başlıklar sırasıyla Şekil 1.1 üzerinde de özetlenmiştir.

4.1. Fiziksel Test Yatağı

Test ortamının amacı, bir tesisin veya fabrikanın endüstriyel kontrol sistemlerini tümüyle kopyalamadan ve mümkün olduğu kadarıyla yaklaşık olarak benzetimini yapmaktır [114]. Ayrıca ulusal ve uluslararası standartlarda ve yönergelerde yer alan endüstriyel kontrol sistemlerinin performansına katkılar sunmak amaçlanır. Bir test yatağının hazırlanması ve kullanılması gerçek siber saldırıların gerçekleştirilmesi ve hatta saldırı sonuçlarının gözlenmesi için uygun bir ortam sunar.

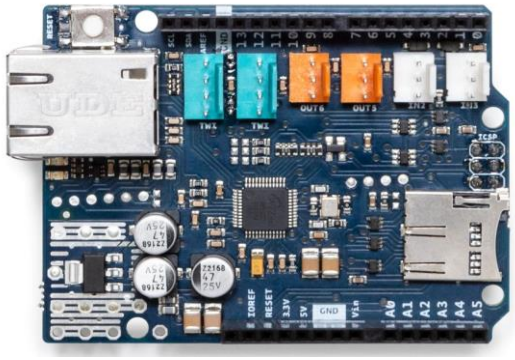
Siber güvenlik araştırmalarına katkı sunmak için çalışmada, SCADA sistemini içeren bir test yatağı ortamı hazırlanmıştır. Bu ortamda depolama tankları bulunmakta, belirli işlemler gerçekleştirilmekte ve Modbus TCP/IP haberleşmesi kullanılmaktadır. SCADA sistemi genellikle Modbus haberleşme protokolü ile bütünleştirilerek gerçekleştirilmektedir [80]. Bu test yatağı gerçek bir su tesisinin basitleştirilmiş halini göstermektedir. SCADA sistemi ile su devir daim süreçleri ve depolama tanklarının durumu kontrol edilmekte ve izlenmektedir. Bu bölümde, hazırlanan SCADA sistemi test yatağının yapılandırması ve mimari yapısı anlatılmaktadır. Test ortamında kullanılan ekipmanlar, gerçek SCADA sistemlerinde sıklıkla kullanılan bileşenlerden seçilmiştir. Test yatağında yer alan UUB1, UUB2, MDB ve saldırgan bölümlerinde kullanılan tüm ekipmanlara ve yazılımlara ait bilgiler Çizelge 4.1'de verilmektedir.

Çizelge 4.1. Test yatağında kullanılan ekipmanlar ve açıklamaları

Bölümler	Ekipmanlar	Yazılım Bilgisi	Açıklamalar
UUB1 ve UUB2	Sarı led: Normal Seviye	Arduino kodlaması Arduino kütüphaneleri: • NewPing.h • SPI.h • Ethernet.h • MgsModbus.h	Su seviyesi yükselip alçaldıkça sistem tepki verir. Mesafe algılayıcısı tarafından ölçülen değer aralığına göre meydana gelen olaylar: • 1-3 cm: röle, pompa, kırmızı led ve küçük zil aktif (alarm durumu) • 4-6 cm: sarı led aktif • 7 cm ve üzeri: mavi led ve küçük zil aktif (alarm durumu)
	Kırmızı led: En Yüksek Seviye		
	Mavi led: En Düşük Seviye		
	Küçük Zil: 12MM-12V-80dB Buzzer		
	Mesafe Algılayıcısı: HC-SR04 Ultrasonic Distance Sensor		
	Röle: 1 Channel 5V Relay Module		
	Su Pompası: DC 2.5V-6V 120 Liter/Hour Mini Submersible Water Pump		
	Su Borusu		
	Su Tankı		
	Uç Birim: Arduino Mega 2560 Revision3		
	Ağ/İnternet Modülü: Arduino Ethernet Shield Revision3		
Ortak	Yönlendirici: Asus DSL-N10 150Mbps Kablolu/Kablosuz ADSL2+ 4 Port Router	Asus Yönetici Paneli	Statik Ip yapılandırması Yerel Alan Ağı bağlantılarının sağlanması
MDB	Bilgisayar: Windows 10 Pro. 2.3 GHz Intel Core i5. 1TB Harddisk. 8GB RAM. 15.6" Samsung Dizüstü Bilgisayar	İşletim Sistemi: MS Windows 10 Pro	
		İMA/Benzetim Aracı 1: Generic Modbus/JBus Tester	UUB1 izlenmesi/kontrolü
		İMA/Benzetim Aracı 2: Modbus Poll-Mbpoll1	UUB2 izlenmesi/kontrolü
		Veritabanı: MS Excel	Ağ trafiği paketlerinin saklanması ve düzenlenmesi
		Ağ trafik paketleri işlemleri: Wireshark	Ağ trafik paketlerinin elde edilmesi ve yakalanması Ağ trafik paketlerinin analiz edilmesi
		Saldırı tespit işlemleri: Google Colab Python kodlama	Saldırı tespiti ve saldırı tür tespiti yapan modellerin hazırlanması
Saldırgan	Bilgisayar: MacOS Retina 2020. 1.1 GHz 4 Çekirdekli İntel Core i5. 500GB SSD. 8GB RAM. 13" Apple MacBook Air Dizüstü Bilgisayar	İşletim Sistemi: Kali Linux	
		Saldırı gerçekleştirme araçları: Nmap, Hping3, Metasploit Framework	Ağ taranması DDoS saldırılarının hazırlanması DDoS saldırılarının uygulanması

Çizelge 4.1.'de yer alan ekipmanlar; bileşenler, donanımlar, cihazlar ve bilgisayarlardan oluşmaktadır. Bu ekipmanlar üzerinde kullanılan yazılımlar ve gerçekleştirilen işlemler özetlenmiştir. Bu ortamda kullanılan ekipmanlara ait görseller ise Şekil 4.1 üzerinde gösterilmektedir.

a) Arduino Mega



b) Ağ/İnternet Modülü

c) Yönlendirici

d) Mesafe Algılayıcısı

e) Ledler

f) Röle

g) Su Pompası ve Su Borusu

h) Küçük Zil

Şekil 4.1. Test yatağında kullanılan ekipmanların gösterimleri [115]

Şekil 4.1'de yer alan Arduino Mega, ATmega2560 tabanlı bir mikrodenetleyici kartıdır ve kapsamlı uygulamalar hazırlamak için oluşturulmuştur. 54 adet sayısal giriş/çıkış pinine, USB girişine, 16 adet analog girişe, 4 adet donanımsal seri porta, güç girişine, 16 MHz kristal osilatöre, Devre-İçi Seri Programlama başlığına ve bir sıfırlama düğmesine sahiptir [116]. Birçok algılayıcıyı, aktüatörü desteklediği için ve kabolulu/kablosuz bağlantılara imkân sunduğu için Arduino Mega kartı bu tez kapsamında UUB olarak tercih edilmiştir. Ayrıca Modbus TCP bağlantısı için kodlama yapmaya da imkân sunmakta ve veri akışının incelenmesini de desteklemektedir. UUB olarak kullanılan bu bileşen ilgili su tankını, üzerindeki bileşenleri ve su devir daim işlemlerini sürdürmek için kodlanmıştır.

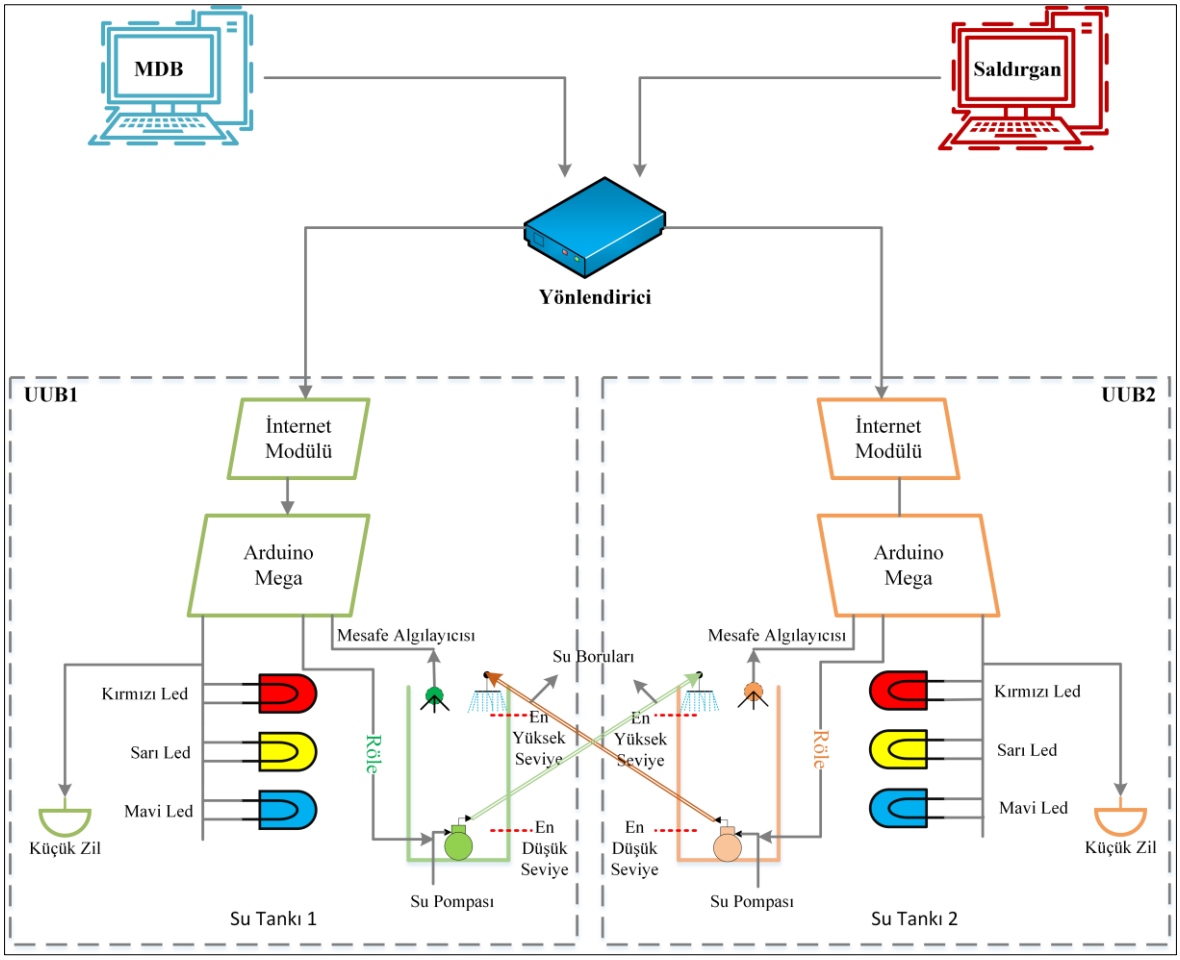
Arduino Mega ile diğer cihazların haberleşmesini sağlamak için Ağ/İnternet Modülü olan Arduino Ethernet Shield kullanılmış ve Modbus TCP bağlantıları yapılandırılmıştır. Modül, pinler doğru yere gelecek şekilde hizalanmış ve Arduino Mega üzerine yerleştirilmiştir. Modüldeki RJ45 bağlayıcısına kablo takılarak ağ bağlantısı kurulmuştur.

Tez çalışması kapsamında iki adet su tankı kullanılmış ve tanklar arasında su devir daim işlemlerinin gerçekleştirilmesi ayarlanmıştır. Her tankın üst tarafına mesafe algılayıcısı koyulmuş ve su seviyesi ölçümleri yapılmıştır. Tankların içinde su pompaları, su boruları; tankların dışında röleler, ledler ve küçük ziller bulunmaktadır. Su seviyesine göre küçük zilin, ledlerin, rölenin ve su pompasının çalışma durumları belirlenmiş ve Arduino Mega üzerinde kodlanmıştır. Röle, su pompasının çalışmasını ve durmasını sağlamaktadır. Ledler su seviyesinin izlenmesini sağlamaktadır. Ayrıca ledler ve küçük ziller yardımıyla su seviyesindeki alarm durumları sistemi izleyen operatöre iletilmektedir. Su seviyesi çok azaldığında alarm durumuna geçilmekte ve diğer tanktan su alımına başlanmaktadır. Su seviyesi çok arttığında ise taşmayı engellemek için diğer tanka suyun tahliye edilmesi başlamaktadır. Su seviyesi aralıkları ve bunlara göre gerçekleşecek olaylar şu şekildedir:

- 1-3 cm aralığında: röle, pompa, kırmızı led ve küçük zil bileşenleri aktif çalışacak (sistem alarm durumunda)
- 4-6 cm aralığında: sarı led aktif çalışacak (sistem normal işleyişinde)
- 7 cm ve üzeri aralıkta: mavi led ve küçük zil bileşenleri aktif çalışacak (sistem alarm durumunda)

Sistemdeki tüm ekipmanlar arasında ağ iletişimini sağlamak için yönlendirici kullanılmıştır. Yönlendirici yönetim paneli sayesinde Yerel Alan Ağı oluşturulmuş; MDB, UUB1 ve UUB2 cihazları için statik IP adresleri atanmıştır. Kablolu/kablosuz bağlantılara ve 4 porta kadar girişlere imkan sunan bir yönlendirici tercih edilmiştir.

Bahsedilen ekipmanlar ve yazılımlar kullanılarak hazırlanan test ortamının mimari yapısı ve genel görünümü ise Şekil 4.2.'de sunulmaktadır.

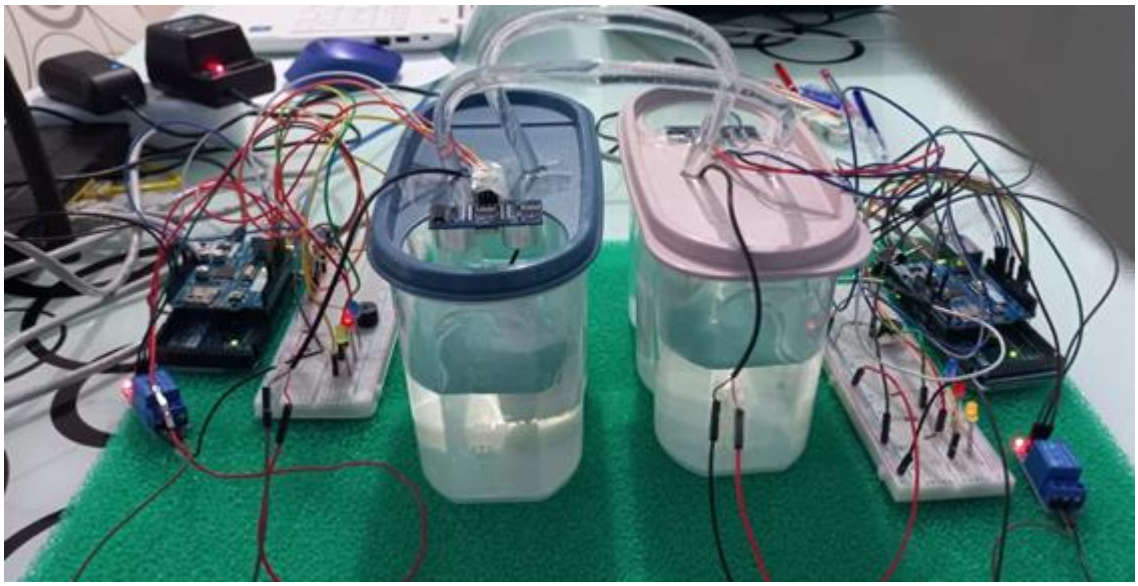


Şekil 4.2. Test yatağının mimari yapısı

Şekil 4.2'de gösterildiği gibi, UUB olarak iki adet su devir daim yapan, depolayan su tankı ve bunlara bağlı algılayıcılar, aktüatörler kullanılmıştır. Tankların taşması ve tanklardaki suların bitmesi gibi sorunların önüne geçmek için sürekli olarak su seviyesi kontrolleri yapılmaktadır. Buradaki süre, algılayıcının varsayılan hızıyla (330m/sn) ile ilgilidir. Su seviyesinin durumuna göre alarm üretmek ve sistemle ilgilenen operatörün dikkatini çekmek hedeflenmiştir.

Ortamda haberleşme için Modbus TCP/IP, kablolu ve kablosuz iletişim protokolleri kullanılmıştır. UUB'lerden alınan veri MDB'ye iletilmiş ve MDB üzerindeki İMA benzetim araçları aracılığıyla süreçler takip edilmiştir. Gelen veriler kontrol edilmiş, saklanmış ve yeni komutlar UUB'lere gönderilmiştir. Modbus TCP/IP protokolünün mimari yapısından dolayı, su tanklarıyla ilgili gelen veriler yazmaç üzerinde kaydedilmektedir. Örneğin su seviyesi, kırmızı led veya küçük zil durum bilgileri gibi sayısal değerler yazmaç üzerinde tutulmaktadır. Çalışmada UUB1 ve UUB2 izlenmesi için İMA/Benzetim Araçları kullanılmıştır.

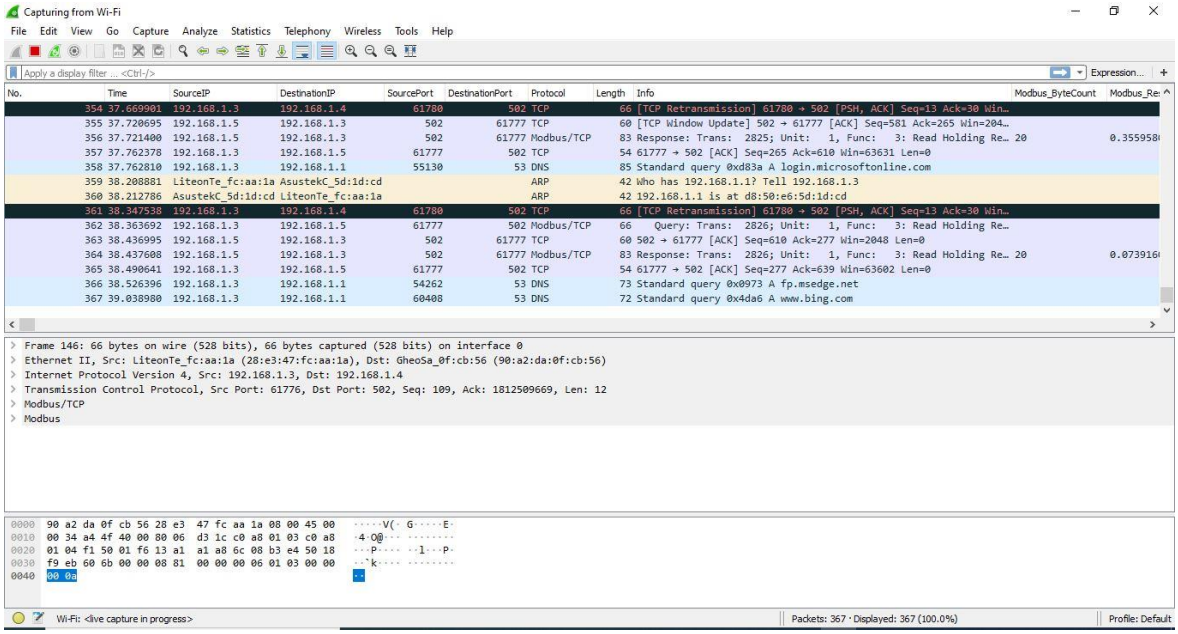
Kötü niyetli kişiler tarafından, saldırgan cihaz kullanılarak ağ içerisinde tarama yapılmış ve uygun olan UUB'ye yönelik saldırılar gerçekleştirilmiştir. Saldırılar gerçekleştirildiğinde fiziksel sistemin ve süreçlerin çalışma durumları genel olarak gözlenebilmektedir. Ayrıca yazmaç değerlerindeki değişimler de izlenebilmektedir. Testyatağı fiziksel olarak hazırlandıktan sonra elde edilen görünüm Şekil 4.3 ve Şekil 4.4'te verilmiştir.



Şekil 4.3. Test yatağındaki UUB'lerin görünümü

Şekil 4.4. Tüm test yatağının görünümü

Sistemde saldırı olup olmadığı MDB üzerinde kontrol edilmektedir. Saldırılar Kali Linux işletim sistemi yüklü saldırgan cihazındaki araçlar ile gerçekleştirilmektedir. Öncelikle ağ içerisinde IP, Port, işletim sistemi ve protokol bilgilerine ulaşmak için taramalar yapılmıştır. UUB'lerden bir tanesi seçilmiş ve ona özel beş farklı DDoS saldırısı hazırlanmıştır. Modbus TCP/IP protokolünün açıklıklarından da faydalanılarak DDoS saldırıları uygulanmıştır. Her bir saldırı için ayrı ayrı ağ trafik paketleri Wireshark programı ile dinlenmiş ve kaydedilmiştir. Ayrıca saldırı olmayan normal durum işleyişi için de aynı dinleme ve kayıt işlemleri yapılmıştır. Wireshark üzerinde dinleme yapma örneğine Şekil 4.5'te yer verilmiştir. Dinleme ve kayıt işlemlerinden sonra elde edilen paketler MS Excel programı ile düzenlenerek analize uygun hale getirilmiş ve ".csv" dosya biçimine çevrilmiştir.



Şekil 4.5. Wireshark programından anlık görüntü örneği

Tez çalışmasında elde edilen verinin analizinin yapılması için Google Colab ortamı kullanılmıştır. Google Research tarafından sunulan bir ortam olan Google Colab makine öğrenimi, veri analizi ve eğitimi için Python kodlamaya imkân sunmaktadır. Çalışmada elde edilen verinin analize uygun hale getirilmesi için bazı ön işlemler gerçekleştirilmiştir. Daha sonra bu ortama Pandas, Numpy, Sklearn, Keras ve Seaborn gibi birçok kütüphane eklenmiş, derin öğrenme ve makine öğrenmesi algoritmaları kullanılmış ve saldırı tespiti için farklı modeller üretilmiştir. Modellerin analiz sonuçları için görsel çıktılar da elde edilmiştir.

4.2. Test Yatağına Yönelik Saldırı Senaryoları

Bu bölümde, test yatağının normal durumu ve test yatağına yönelik gerçekleştirilen saldırılar anlatılmaktadır. SCADA sistemlerine sıkılıkla yapılan saldırılardan DDoS saldırıları ele alınmış ve saldırgan tarafından seçilen bir UUB'ye yönelik saldırılar gerçekleştirilmiştir. Farklı türlerde DDoS saldırı senaryoları uygulanmış ve sistemin işleyişinin etkilenmesi amaçlanmıştır. Bu senaryolar:

1. Normal (Saldırısız) Durum Senaryosu
2. TCP Seli Saldırı Senaryosu
3. UDP Seli Saldırı Senaryosu
4. SYN Seli Saldırı Senaryosu
5. IP Sahteciliği Seli Saldırı Senaryosu

6. ICMP Seli Saldırı Senaryosu

Normal durum senaryosunda SCADA sistemi saldırı altında değilken elde edilen ağ trafiği dinlenmiş ve kaydedilmiştir. Bu senaryoda, su tankları arasında su sürekli devir daim etmiş ve suyun seviyesindeki değişime göre gerekli işlemler programlandığı gibi kendiliğinden gerçekleşmiştir. UUB ile MDB arasında haberleşmenin sağlanması, sınanması ve paket alışverişinin olması için ping atma yöntemi kullanılmıştır. Bu yöntemde ICMP paketleri gönderilir ve paketlerin geri gelmesi beklenir [117].

Saldırgan tarafından Hping3 aracı kullanılarak her saldırı tipi için özel kodlamalar yapılmış ve hedef UUB'ye yönelik 5 farklı DDoS saldırısı gerçekleştirilmiştir. Hping3 aracı ile istenilen özelliklerde paketler üretilmektedir. Hedef UUB'ye yönelik TCP, UDP, SYN, IP Sahteciliği ve ICMP seli saldırılarının her biri farklı zamanlarda ve ayrı ayrı uygulanmıştır. Bu saldırı senaryolarının her biri yaklaşık 2 dakika boyunca uygulanmıştır. Saldırılar sırasında hedef UUB sistem süreçlerinde (işleyişinde) kısa süreli (1-5 sn aralığında) duraksamalar ve donmalar yaşanmıştır. Su devir daim işlemi ve alarm üretilmesi gibi şüreçler aksamıştır. Bu olumsuz durumlar diğer UUB sistemini de etkilemiş ve tüm test yatağının çalışması birkaç sn gecikmeli olarak kısa sürelerle (1-5 sn aralığında) kesilmiştir. Tankın su seviyesinin yanlış ölçülmesi, yanlış ledlerin yanması, zilin yanlış zamanda alarm vermesi ve hiç alarm vermemesi gibi anormal durumlar görülmüştür. Saldırı senaryolarının uygulanması sonlandığında sistem işleyişi 4-8 sn gibi zaman aralığı içerisinde toparlanmış ve eski haline dönmüştür. Sistem işleyişinin eski haline dönmesi için geçen sürenin tolere edilemeyecek kadar uzun olması, SCADA sistemleri için geri dönüşü olmayan büyük sorunlara yol açabilir. Bu yüzden SCADA sistemlerine saldırılar yapılması, saldırı tepkilerinin izlenmesi ve analiz edilmesi önem arz etmektedir.

Saldırı ve normal durum senaryoları uygulanırken yakalanan ağ trafiği hakkında elde edilen istatistiksel bilgiler Çizelge 4.2'de verilmektedir. Ağ trafiğinde yakalanan paketler, veri kümelerindeki örnekleri temsil etmektedir.

Çizelge 4.2. Saldırı senaryolarından elde edilen ağ paketleri hakkında bilgiler

Ölçümü Yapılan Değerler	Saldırı Senaryoları					
	Normal	TCP Seli	UDP Seli	SYN Seli	IP Sahteciliği	ICMP Seli
Toplam paket sayısı	3391	5253	3118	3238	3217	4551
Ortalama paket boyutu (bayt)	109	60	89	60	143	60
Toplam paket boyutu (bayt)	370724	315180	277679	194280	461615	273084
Yakalama süresi (ms)	530	294	253	163	286	271

Çizelge 4.2 incelendiğinde normal durum senaryosuna ait 3391 adet paket varken saldırılı durum senaryolarına ait toplam 19377 adet paket bulunmaktadır. 6 senaryo durumuna göre paket sayısı dağılımları dengelidir. Ortalama paket boyutu en büyük olan saldırı, IP Sahteciliği saldırısıdır. En az boyutlar ise TCP, SYN ve ICMP Seli saldırılarına aittir ve tümü aynı değere sahiptir. Saldırı senaryoları ayrı ayrı incelendiğinde toplam paket büyüklükleri farklı değerler almaktadır. Toplamda en fazla paket boyutu IP Sahteciliği saldırısına aittir. En az boyut ise SYN Seli saldırısı ile elde edilmiştir. Saldırı senaryolarına ait paketlerin yakalanması için en fazla süre normal durum için ve en az süre SYN Seli saldırı senaryosu için harcanmıştır.

4.3. Veri Kümesinin Elde Edilme Aşamaları

Bu bölümde, test yatağında ayrı ayrı gerçekleştirilen senaryolar sonucunda elde edilen toplam veri kümesi hakkında bilgiler verilmektedir. Wireshark ağ dinleme ve analiz aracı ile her senaryoya ait ağ trafik paketleri ayrı ayrı toplanmış ve daha sonra tek bir yerde birleştirilerek toplam veri kümesi oluşturulmuştur. Literatürde sıklıkla yer alan öznitelikler ve Modbus TCP/IP protokolüne özgü olan öznitelikler araştırılmıştır [7,9]. Bu veri kümesi için uygun olan 30 adet öznitelik belirlenmiştir. Çalışmada kullanılan öznitelikler ve açıklamaları Çizelge 4.3'te gösterilmektedir.

Çizelge 4.3. Veri kümesinde kullanılan özellikler ve açıklamaları

No	Öznitelikler	Açıklamaları
1	No	Paket/örnek sayısı
2	Time	Zaman
3	SourceIP	Kaynak İnternet Protokol adresi
4	DestinationIP	Hedef İnternet Protokol adresi
5	SourcePort	Kaynak port numarası
6	DestinationPort	Hedef port numarası
7	Protocol	Protokol bilgisi
8	Length	Paket uzunluğu
9	Info	Paket hakkındaki bilgiler
10	Modbus_ByteCount	Modbus protokolü veri alanı büyüklüğü (bayt)

Çizelge 4.3. (devam) Veri kümesinde kullanılan özellikler ve açıklamaları

11	Modbus_ResponseTime	Modbus protokolü cevap süresi
12	Modbus_ReqFrame	Modbus protokolü mesaj biçimi
13	DeltaTime	Bir işlemin başlangıcı ile bitişi arasında geçen süre
14	ModbusEventCount	Modbus cihazının işlem sayısı
15	TimeSince_FirstFrameInThisTCPStream	TCP akışındaki ilk çerçeve gönderiminden şimdiye kadar geçen süre
16	TimeSince_PreviousFrameInThisTCPStream	TCP akışındaki bir önceki çerçeve gönderiminden şimdiye kadar geçen süre
17	TimeDeltaFromPrevious_CapturedFrame	Bir önceki yakalanan çerçeve ile sonrası arasındaki zaman farkı
18	TimeDeltaFromPrevious_DisplayedFrame	Bir önceki görüntülenen çerçeve ile sonrası arasındaki zaman farkı
19	TimeSince_ReferenceOrFirstFrame	Referanstan veya ilk çerçeveden şimdiye kadar geçen süre
20	FrameLength_OnTheWire	Bağlantı üzerindeki çerçeve uzunluğu
21	FrameLength_StoredIntoTheCaptureFile	Yakalanan dosyadaki depolanan çerçeve uzunluğu
22	TimeToLive	Yaşam süresi
23	TotalLength	Toplam uzunluk
24	FrameLengthStoredIntoTheCaptureFile	Yakalanan dosyadaki depolanan çerçeve uzunluğu
25	ModbusTCPLength	Modbus TCP paketi uzunluğu
26	ModbusByteCount	Modbus paket bayt sayısı
27	ModbusTimeFromRequest	İstek yapılan Modbus paket süresi
28	TCPHeaderLength	TCP başlık uzunluğu
29	ModbusRegNum	Modbus yazmaç numarası
30	Register Value	Modbus yazmaç değeri
31	Class	Sınıflandırma sütunu (6 adet senaryo)

30 öznitelik, 1 belirleyici sınıf ve toplam 22.768 örnekten oluşan yeni ve kapsamlı bir veri kümesi elde edilmiştir. Veri kümesi hazırlanırken uygulanan saldırılar SCADA sistemi üzerinde gözlemlenmiş ve anormal bir durum olduğu operatör tarafından açıkça fark edilmiştir. Bu veri kümesi makine öğrenmesi modellerini ve farklı yöntemleri eğitmek ve test etmek için kullanıma uygun durumdadır. DDoS saldırısı olup olmadığının ve beş farklı DDoS saldırı türünün belirlenmesi amaçlanmıştır. Bu özelliklerden dolayı literatüre yeni bir bakış açısı sunulmaktadır.

4.4. Saldırı Tespitinde Kullanılacak Analiz Performans Metrikleri

Genel olarak problemlerin çözümünde hangi yöntemin daha etkili sonuca ulaştığının tespit edilmesi için, kullanılan her yöntemin elde ettiği performans bilgileri incelenir. Daha sonra en yüksek performansa sahip olan yani en yüksek başarım oranını yakalayan yöntem seçilir. Modeller için kullanılan makine öğrenmesi algoritmalarının değerlendirilmesi ve birbirleriyle kıyaslanması için literatürde sıklıkla kullanılan performans metriklerinden faydalanılmaktadır. Performans metrikleri için kullanılacak değerleri içeren karışıklık matrisi (confusion matrix) Çizelge 4.4'te gösterilmektedir.

Çizelge 4.4. Karışıklık matrisi

		Gerçek Değerler	
		Pozitif Durumlar	Negatif Durumlar
Tahmin Edilen Değerler	Pozitif Durumlar	DP	YP
	Negatif Durumlar	YN	DN

Karışıklık matrisinde verilen değerler, gerçekte var olan değerleri ve tahmin sonucu elde edilen değerleri göstermektedir [118]. Gerçekte pozitif etikete sahip olan değerin tahmin kısmında da pozitif etikete sahip olması Doğru Pozitif (DP - True Pozitive) olarak nitelendirilir. Gerçekte negatif etikete sahip fakat tahmin kısmında pozitif etiketlenen değerler ise Yanlış Pozitif (YP - False Positive) olarak ifade edilir. Gerçekte pozitif etikete sahip fakat tahmin kısmında negatif etiketlenen değerler Yanlış Negatif (YN - False Negative) olarak gösterilir. Gerçekte negatif etikete sahip olan değerin tahmin kısmında da negatif etikete sahip olması ise Doğru Negatif (DN - True Negatif) olarak belirtilir [119]. Karışıklık matrisindeki değerler ile hesaplanan başarı metrikleri aşağıda yer almaktadır.

Doğruluk (Accuracy), doğru tahmin edilen değerlerin sayısının toplam değer sayısına oranıdır. Bu durum Eşitlik 1'de gösterilmektedir.

$$\text{Doğruluk} = \frac{\text{DP+DN}}{\text{DP+YP+DN+YN}} \quad \text{(Eşitlik 1)}$$

Kesinlik (Precision), doğru tahmin edilen pozitif değerlerin sayısının, tahmin sonucu pozitif etikete sahip değerlerin sayısına oranıdır. Bu orana Eşitlik 2'de yer verilmektedir.

$$\text{Kesinlik} = \frac{\text{DP}}{\text{DP+YP}} \quad \text{(Eşitlik 2)}$$

Duyarlılık (Recall), doğru tahmin edilen pozitif değerlerin sayısının, gerçekte pozitif etikete sahip değerlerin sayısına oranıdır ve Eşitlik 3 bu oranı göstermektedir [120].

$$\text{Duyarlılık} = \frac{\text{DP}}{\text{DP+YN}} \quad \text{(Eşitlik 3)}$$

F-1 Değeri (Score) kesinlik ve duyarlılık değerlerinin harmonik ortalaması olarak tanımlanabilir. En yüksek 1 değerinin alabilirken en düşük alacağı değer 0'dır. Eşitlik 4 bu ortalamayı hesaplamaktadır.

$$\text{F1 Değeri} = 2 \text{ x} \frac{\text{Kesinlik x Duyarlılık}}{\text{Kesinlik+Duyarlılık}} \quad \text{(Eşitlik 4)}$$

Çalışmada, geleneksel performans metriklerinden Doğruluk, Kesinlik, Duyarlılık ve F-1 Değeri her model için kullanılmıştır. Literatürdeki çalışmalarla kıyaslama yapılırken, sıkılıkla kullanılan Doğruluk başarı metriği dikkate alınmıştır [121].

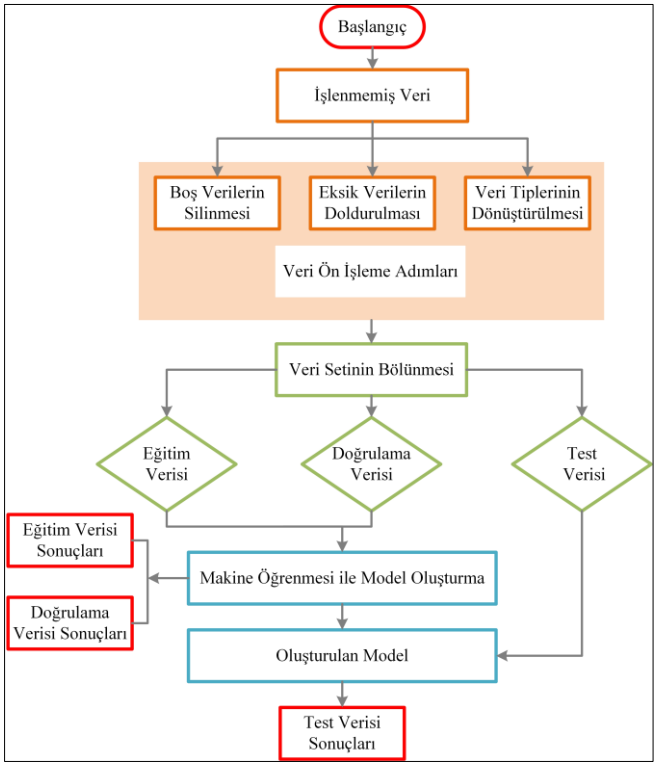
4.5. Saldırı Tespiti için Önerilen Modeller

Bu bölümde, SCADA sistemi içeren test yatağına yönelik saldırıların tespiti yapılmaktadır. Bunun için makine öğrenmesi modelleri, hazırlanan veri kümesi üzerinde uygulanmaktadır. Elde edilen analiz sonuçları belirli metriklere göre birbirleriyle kıyaslanmaktadır.

Önerilen modeller ile başarılı sonuçlar almak için veri ön işlemleri gerçekleştirilmekte ve deneyler yapılmaktadır. SCADA sistemi kullanılan bir fiziksel test yatağının siber güvenliğini sağlamak için yenilikçi ve farklı yaklaşımlar önerilmektedir.

4.5.1. Verinin hazırlanması ve modellere ulaştırılması

Veri kümesinin analiz edilecek duruma getirilmesine ve veri kümesine uygun olan modellerin tasarlanmasına bu bölümde yer verilmektedir. Şekil 4.6, bu bölümü özetlemektedir. Veri kümesinin incelenerek analize uygun hale getirilmesi için birkaç tane veri ön işlemi belirlenmiştir. Bu işlemlerden ilki gereksiz görülen veya çok fazla boş değer içeren özniteliklerin ve örneklerin silinmesidir. Bu işlemde 6 adet öznitelik kaldırılmıştır. Bunlar: No, Info, Modbus_ByteCount, ModbusEventCount, FrameLength_StoredIntoTheCaptureFile, ModbusRegNum. Daha sonraki işlem ise eksik veri içeren ve verilerin tamamlanması uygun görülen özniteliklerin Ortalama Alma (Mean Yöntemi) ile doldurulmasıdır. Bir diğer işlem de veri tiplerinin aynı türe dönüştürülmesidir. Bunun için de kategorik hale getirme işlemleri kullanılmıştır. Tüm bu işlemlerden sonra elde edilen veri kümesi 25 özniteliğe sahip olmuştur.



Şekil 4.6. Verinin işlenerek önerilen modellere kadar ulaştırılması

Veri kümesi, ön işlemlerden sonra bölünme işlemlerine gönderilmiştir. Buna göre veri kümesi eğitim, doğrulama ve test için bölünmüştür. Buradaki bölünme oranları kullanılan tüm modellerde sabit tutulmuştur. Elde edilen eğitim ve doğrulama verileri birleştirilerek önerilen modellere gönderilmiştir. Test verisi ile model üzerinde testler gerçekleştirilmiştir. Eğitim, doğrulama ve test verileri için analiz sonuçları elde edilmiştir. STS için en yüksek başarı oranını yakalayacak en uygun modelin elde edilmesi gereklidir ve bahsedilen bu aşamalar önem arz etmektedir.

Veri kümesinden alınan bir kısım veri eğitim işlemine tabi tutulmakta ve bu eğitimin başarısının ölçülmesi için kullanılmayan başka bir kısım veri de test amaçlı değerlendirilmektedir. Burada doğru değerlerin seçilmesi için bir doğrulama işlemine ihtiyaç duyulabilir. Bu yüzden test ve eğitim kısımlarında yer almayan bir kısım veri doğrulama yapmak için kullanılabilir. Literatürde, veri kümesinin bölünme oranları genellikle %70 ve %30 şeklinde tercih edilmektedir [122].

Modellerin eğitiminde %70 rasgele seçilmiş bir veri kümesi yani 15937 satır veri kullanılmıştır. Geri kalan %30'luk bölüm önerilen modelin testini ve doğrulamasını (validation) değerlendirmek için ikiye bölünmüştür. Buna göre 3415 satır veri doğrulama

için ve 3416 satır (sınıf sütunu dâhil edilerek) test için kullanılmıştır. Toplam 22768 satır veri (örnek) bulunmaktadır.

4.5.2. Önerilen modeller

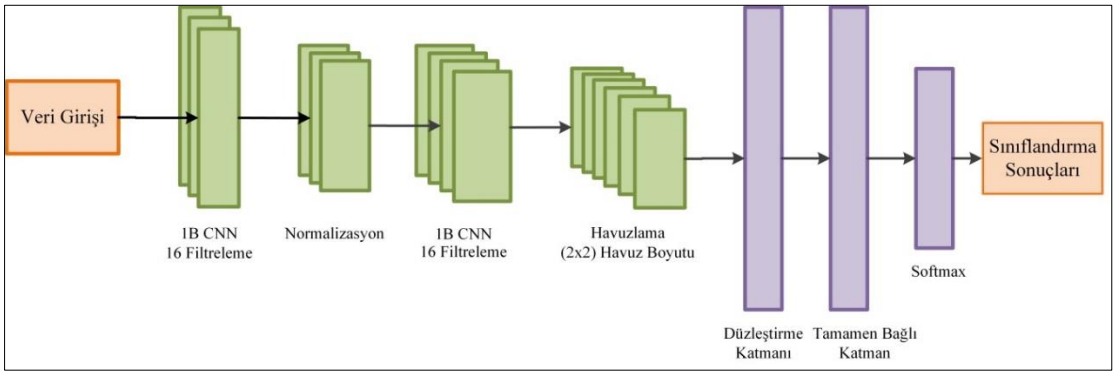
Makine öğrenmesi tabanlı CNN, LSTM, CNN-LSTM hibrit, KS, LWL, KNN, LB, AB, NB, BN, ZeroR, PART, DTa, DT, RF ve RT modelleri ayrı ayrı analiz edilmiş; saldırı tespit başarı oranları tartışılmıştır. Hazırlanan tüm modeller belirlenen başarı metriklerine göre kıyaslanmıştır ve elde edilen sonuçlar Çizelge 5.1'e yerleştirilmiştir. Kullanılan modellere, modellerin mimari yapılarına ve parametre değerlerine ait bilgilere bu bölümde yer verilmiştir.

CNN algoritması, daha fazla uzamsal özellik çıkarabilmek için kullanılır. Bu sebepten dolayı CNN katmanları giriş verilerindeki yararlı özellikleri seçmek için kullanılmıştır. LSTM algoritması ise bellek blokları kullanarak bir önceki zamandan gelen bilgiyi sonrakine aktarır. Zamansal bilgiyle iyi modelleme yapar. Bu yüzden LSTM katmanları sıralı verilerle işlem yapmak için kullanılmıştır. CNN ve LSTM modelleri tek başlarına kullanıldıktan sonra performans değerlerinin yükseltilmesi ve analiz sonuçlarının daha başarılı olması için CNN-LSTM Hibrit modeli hazırlanmıştır. Bu 3 adet modele ek olarak DT modeli de test edilmiştir. Elde edilen sonuçlara göre önerilen modellerden biri de DT modeli olmuştur.

Önerilen CNN, LSTM ve CNN-LSTM hibrit modellerinde kategorik veriler yer aldığı için Loss (Kayıp) Fonksiyonu olarak categorical_crossentropy seçilmiştir. Çok sayıda parametre içeren veri kümelerinde verimli şekilde çalıştığı için Optimizasyon Algoritması olarak Uyarlanabilir Moment Tahmini (Adaptive Moment Estimation - ADAM) tercih edilmiştir [123]. Kararlılık sağlamak amacıyla Düzeltilmiş Doğrusal Birimler (Rectified Lineer Unit – ReLU) aktivasyon fonksiyonu tercih edilmiştir. ReLU basit bir hesaplamaya sahiptir ve girdiyi değerlendirerek çıktıyı belirler [124]. Gruplar halinde işlenme (batch) boyutu varsayılan olarak bırakılmıştır. Sınıflandırmayı bitirmek için Softmax Fonksiyonu kullanılmıştır.

CNN tabanlı modeller

Çalışmada kullanılan CNN tabanlı makine öğrenmesi modellerinin temel mimarisine Şekil 4.7'de yer verilmiştir. Modellerin daha ayrıntılı anlatımı için Çizelge 4.5 hazırlanmıştır.



Şekil 4.7. CNN tabanlı makine öğrenmesi modellerinin temel mimarisi

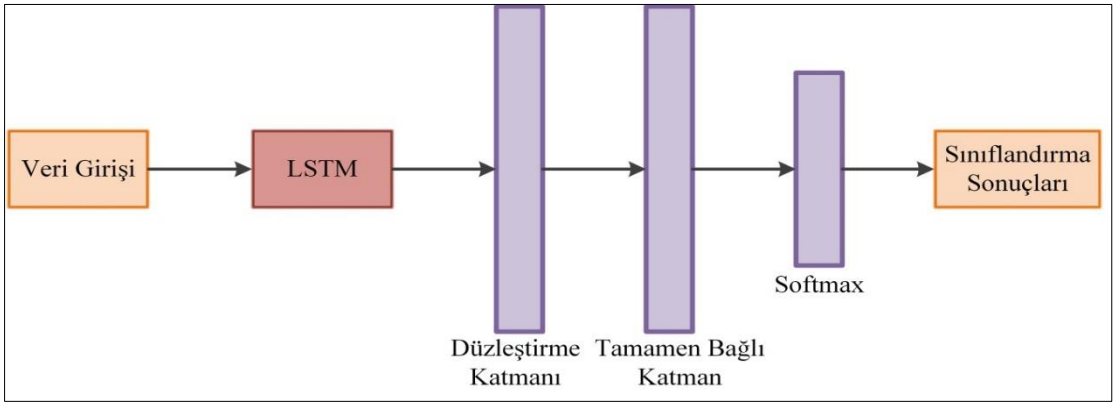
Çizelge 4.5. Önerilen CNN tabanlı makine öğrenmesi modellerinin parametreleri

Model	Katman	Parametre	Çıktı Boyutu
CNN1a (200 epok) CNN1b (300 epok)	Giriş	22768x25	
	1Boyutlu CNN	filtelemes:16, çekirdek:3, aktivasyon:relu	22x16
	Normalizasyon		22x16
	1Boyutlu CNN	filtreleme:16, çekirdek:3, aktivasyon:relu	20x16
	1Boyutlu Havuzlama	havuz boyutu:2	10x16
	Düzleştirme		160
	Tamamen Bağlı	nöron:100, aktivasyon:relu	100
	Çıkış	nöron:6, aktivasyon:softmax	6
	Derleme	kayıp='categorical_crossentropy', optimizasyon=adam, metrikler='accuracy'	

200 epok kullanılan CNN1a ve 300 epok kullanılan CNN1b modelleri kullanılarak makine öğrenmesi gerçekleştirilmiştir. 2 modelde de 1 boyutlu CNN Katmanı (Evrişim) ve Havuzlama Katmanı kullanılmıştır. Normalizasyon işlemleri yapılmıştır. Havuzlama Katmanından sonra Düzleştirme yapılmıştır. Son olarak Bağlı, Sınıflandırma ve Çıkış Katmanları kullanılmıştır. Bu modeller için seçilen diğer parametreler bölüm başında anlatılmaktadır.

LSTM tabanlı modeller

Bu tez çalışmasında LSTM tabanlı makine öğrenmesi modelleri üzerinde çeşitli analizler gerçekleştirilmiştir. Buna göre, ele alınan LSTM tabanlı modellerin temel mimarisine Şekil 4.8'de yer verilmiştir. Modellerin daha ayrıntılı anlatımı için Çizelge 4.6 hazırlanmıştır.



Şekil 4.8. LSTM tabanlı makine öğrenmesi modellerinin temel mimarisi

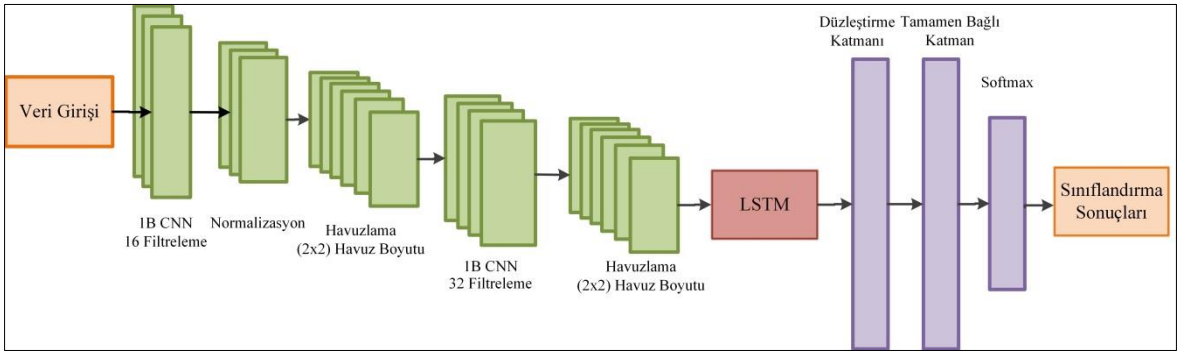
Çizelge 4.6. Önerilen LSTM tabanlı makine öğrenmesi modellerinin parametreleri

Model	Katman	Parametre	Çıktı Boyutu
LSTM1a (200 epok) LSTM1b (300 epok)	Giriş	22768x25	
	LSTM	nöron:100	100
	Düzleştirme		100
	Tamamen Bağlı	nöron:100, aktivasyon:relu	100
	Çıkış	nöron:6, aktivasyon:softmax	6
	Derleme	kayıp='categorical_crossentropy', optimizasyon=adamax, metrikler='accuracy'	6

LSTM algoritmasının kullanıldığı makine öğrenmesi kullanılmıştır. LSTM ağları sıralı bir giriş katmanı içermektedir. Önerilen LSTM temel ağ mimarisinde, Giriş Katmanından sonra LSTM Katmanı yerleştirilmiştir. Daha sonra bir Düzleştirme Katmanı gelmiştir. En sonunda Tamamen Bağlı, Sınıflandırma ve Çıkış Katmanları gelmiştir. Çalışmada 200 epok ve 300 epok parametrelerine sahip 2 tane LSTM modeli hazırlanmıştır (LSTM1a ve LSTM1b). Bu modeller için seçilen diğer parametreler bölüm başında bahsedilmiştir.

Hibrit tabanlı modeller

Çalışmada önerilen bu modelde CNN ve LSTM algoritmaları birlikte hibrit şekilde kullanılmakta ve analizler gerçekleştirilmektedir. Hibrit derin öğrenme kullanılarak 6 farklı model (HİBRİT1a, HİBRİT1b, HİBRİT2a, HİBRİT2b, HİBRİT3a, HİBRİT3b) hazırlanmıştır. İlk model (HİBRİT1) temel alınarak HİBRİT2 ve HİBRİT3 modelleri elde edilmiştir. HİBRİT1 mimarisine Şekil 4.9'da yer verilmiştir. Modellerin daha ayrıntılı anlatımı için Çizelge 4.7. hazırlanmıştır.



Şekil 4.9. Hibrit makine öğrenmesi modelinin (HİBRİT1) temel mimarisi

Çizelge 4.7. Önerilen HİBRİT modellerin parametreleri

Model	Katman	Parametre	Çıktı Boyutu
HİBRİT1a (200 epok) HİBRİT1b (300 epok)	Giriş	22768x25	
	1Boyutlu CNN	filteleme:16, çekirdek:3, aktivasyon:relu	22x16
	Normalizasyon		22x16
	1Boyutlu Havuzlama	havuz boyutu:2	11x16
	1Boyutlu CNN	filteleme:32, çekirdek:3, aktivasyon:relu	9x32
	1Boyutlu Havuzlama	havuz boyutu:2	4x32
	LSTM	nöron:200	4x200
	Düzleştirme		800
	Tamamen Bağlı	nöron:100, aktivasyon:relu	100
	Çıkış	nöron:6, aktivasyon:softmax	6
	Derleme	kayıp='categorical_crossentropy', optimizasyon=adam, metrikler='accuracy'	
HİBRİT2a (200 epok) HİBRİT2b (300 epok)	Giriş	22768x25	
	1Boyutlu CNN	filteleme:16, çekirdek:5, aktivasyon:relu	20x16
	Normalizasyon		20x16
	1Boyutlu Havuzlama	havuz boyutu:2	10x16
	1Boyutlu CNN	filteleme:16, çekirdek:5, aktivasyon:relu	6x16
	Normalizasyon		6x16
	1Boyutlu Havuzlama	havuz boyutu:2	3x16
	LSTM	nöron:100	3x100
	Düzleştirme		300
	Tamamen Bağlı	nöron:100, aktivasyon:relu	100
	Tamamen Bağlı	nöron:100, aktivasyon:relu	100
	Çıkış	nöron:6, aktivasyon:softmax	6
	Derleme	kayıp='categorical_crossentropy', optimizasyon=adam, metrikler='accuracy'	
HİBRİT3a (200 epok) HİBRİT3b (300 epok)	Giriş	22768x25	
	1Boyutlu CNN	filteleme:8, çekirdek:5, aktivasyon:relu	20x8
	Normalizasyon		20x8
	1Boyutlu Havuzlama	havuz boyutu:2	10x8
	1Boyutlu CNN	filteleme:8, çekirdek:5, aktivasyon:relu	6x8

Çizelge 4.7. (devam) Önerilen HİBRİT modellerin parametreleri

	1Boyutlu Havuzlama	havuz boyutu:2	3x8
	LSTM	nöron:100	3x100
	Düzleştirme		300
	Tamamen Bağlı	nöron:100, aktivasyon:relu	100
	Çıkış	nöron:6, aktivasyon:softmax	6
	Derleme	kayıp='categorical_crossentropy', optimizasyon=adam, metrikler='accuracy'	

Bu hibrit modellerde CNN ve LSTM algoritmaları kullanılarak makine öğrenmesi gerçekleştirilmiştir. HİBRİT modellerde 1 boyutlu CNN Katmanları ve Havuzlama Katmanları kullanılmıştır. Normalizasyon işlemleri yapılmış ve son Havuzlama Katmanından sonra LSTM katmanı modele yerleştirilmiştir. Düzleştirme, Tam Bağlı, Sınıflandırma ve Çıkış Katmanları kullanılmıştır. 200 olan epok sayısı ile HİBRİT1a ve 300 epok sayısı ile HİBRİT1b modelleri elde edilmiştir.

İkinci hibrit modelde (HİBRİT2), HİBRİT1'den farklı olarak normalizasyon ve aktivasyon işlemleri ikişer kez uygulanmıştır. Daha sonra modele 200 epok uygulanarak HİBRİT2a modeli ve 300 epok uygulanarak HİBRİT2b modeli elde edilmiştir.

HİBRİT1 modelindeki 1 boyutlu CNN katmanlarındaki çekirdek boyutu artırılmış ve filtreleme işlemlerinin sayısı azaltılmıştır. LSTM nöron sayısı da azaltılmıştır. Bu şekilde HİBRİT3 modeli elde edilmiştir. 200 epok için HİBRİT3a modeli ve 300 epok için HİBRİT3b modeli hazırlanmıştır.

DT tabanlı model

Çalışmada CNN, LSTM ve CNN-LSTM HİBRİT tabanlı makine öğrenmesi modelleri dışında DT modeli üzerinde de analizler gerçekleştirilmiştir. Buna göre, ele alınan DT tabanlı modelin daha ayrıntılı anlatımı için Çizelge 4.8 hazırlanmıştır.

Çizelge 4.8. Önerilen DT modelinin parametreleri

No	Parametreler	Açıklamalar	Kriterler
1	criterion	Bir bölmenin kalitesini ölçme işlevi	Gini
2	splitter	Her düğümde bölmeyi seçmek için kullanılan strateji	Best

Çizelge 4.8. (devam) Önerilen DT modelinin parametreleri

3	max_depth	Ağacın en yüksek derinliği	Yok (tüm yapraklar saf olana kadar)
4	min_samples_split	Dâhili bir düğümü bölmek için gereken en az örnek sayısı	2
5	min_samples_leaf	Bir yaprak düğümde olması gereken en az örnek sayısı	1
6	min_weight_fraction_leaf	Bir yaprak düğümde olması gereken toplam ağırlıkların oranı	0
7	max_leaf_nodes	En iyi şekilde bir ağaç büyütme sayısı	Yok (sınırsız sayıda yaprak düğümü)
8	min_impurity_decrease	Ağırlıklı saf olmayan durum azaltma	0
9	class_weight	Sınıflarla ilişkili ağırlıklar	Yok (tüm sınıflar bir ağırlığa sahiptir)
10	ccp_alpha	En az maliyet-karmaşıklık budaması için kullanılan karmaşıklık parametresi	0 (budama yapılmaz)

Çizelge 4.8'e göre DT modelinde ağaç, yapraklar, düğümler ve budama ile ilgili parametreler bulunmaktadır. Bu parametrelerin varsayılan olarak ayarlanan kriterleri analizlerde tercih edilmiştir.

5. SONUÇLAR VE ÖNERİLER

Önerilen makine öğrenmesi modellerinin analiz sonuçları bu bölümde ele alınmaktadır. Ayrıca, daha önce yapılmış çalışmaların ve bu çalışmanın saldırı tespit başarı oranları kıyaslanarak elde edilen sonuçlar tartışma bölümünde gösterilmiştir. Önerilen hibrit modelin farklı bir veri kümesi üzerinde yapılan analizlerinin sonuçları da Tartışma bölümünde yer alan tabloya yerleştirilmiştir. Bu bölümde yer almayan diğer analiz sonuçlarına Ekler bölümünde yer verilmiştir.

5.1. Deneysel Sonuçlar

Sisteme yönelik DDoS saldırısı olup olmadığı ve saldırı varsa hangi tür DDoS saldırısı olduğunun anlaşılması için testler ve analizler yapılmıştır. Bu şekilde çalışılarak STS için önerilerde bulunulmuştur. Elde edilen analiz sonuçları Çizelge 5.1'de sunulmuştur.

Çizelge 5.1. Kullanılan modellerin performans değerleri (ortalama)

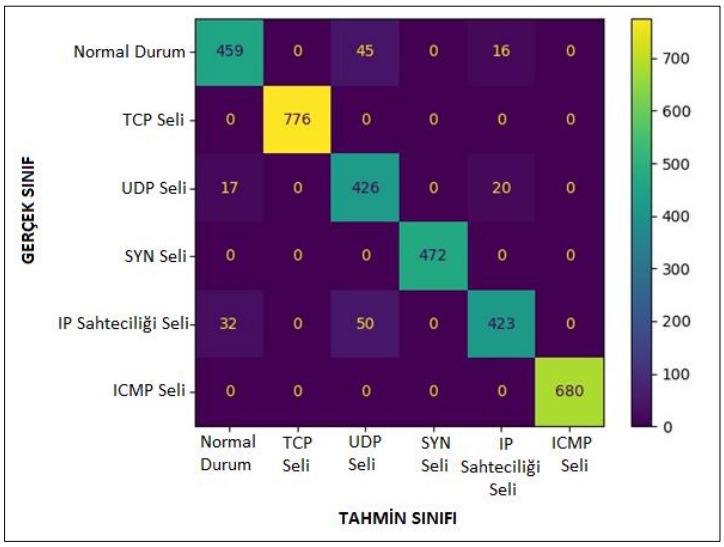
Modeller		Doğruluk (%)	Kesinlik (%)	Duyarlılık (%)	F1-Değeri (%)
CNN	CNN1a	93,53	94,01	93,53	93,57
	CNN1b	94,26	94,79	94,26	94,35
LSTM	LSTM1a	84,60	86,03	84,60	83,73
	LSTM1b	84,28	84,63	84,28	83,63
CNN-LSTM HİBRİT	HİBRİT1a	94,09	94,23	94,09	94,12
	HİBRİT1b	93,97	93,99	93,97	93,97
	HİBRİT2a	93,91	94,05	93,91	93,93
	HİBRİT2b	91,92	92,33	91,92	91,93
	HİBRİT3a	92,77	92,99	92,77	92,82
	HİBRİT3b	94,73	94,90	94,73	94,74
Tembel	KS	79,93	81,93	79,95	79,03
	LWL	66,00	59,62	66,02	58,53
	KNN	86,15	86,08	86,15	86,11
Meta	LB	83,91	88,33	83,93	83,13
	AB	42,96	-	43,01	-
Bayes	NB	84,03	85,43	84,00	83,54
	BN	85,24	86,44	85,20	84,82
Kural	ZeroR	22,55	-	22,51	-
	PART	79,24	91,32	79,23	77,14
	DTa	59,39	-	59,40	-
Ağaç	DT	98,77	98,77	98,77	98,77
	RF	95,84	97,21	95,84	96,51
	RT	83,07	85,71	83,14	82,44

Performans sonuçları incelendiğinde CNN-LSTM Hibrit modelleri içerisinde HİBRİT3b modelinin DDoS saldırı verilerini analiz etmede ve sınıflandırmada CNN ve LSTM

modellerine göre daha başarılı olduğu görülmüştür. Diğer makine öğrenmesi algoritmaları içerisinde ise en yüksek başarı oranı DT modeli ile elde edilmiştir. Ele alınan Doğruluk, Kesinlik, Duyarlılık ve F1-Değeri başarı metrikleri göz önüne alındığında bu iki modelin saldırı tespiti için en uygun modeller olduğu belirlenmiştir. LSTM modelleri ve ZeroR modeli saldırı tespitini en düşük başarı oranlarıyla gerçekleştirmiştir.

5.1.1. HİBRİT3b modeli ile elde edilen sonuçlar

HİBRİT3b modeli ile elde edilen karışıklık matrisi (Şekil 5.1) ve karışıklık matrisinden elde edilen değerler (Çizelge 5.2) aşağıda gösterilmiştir:



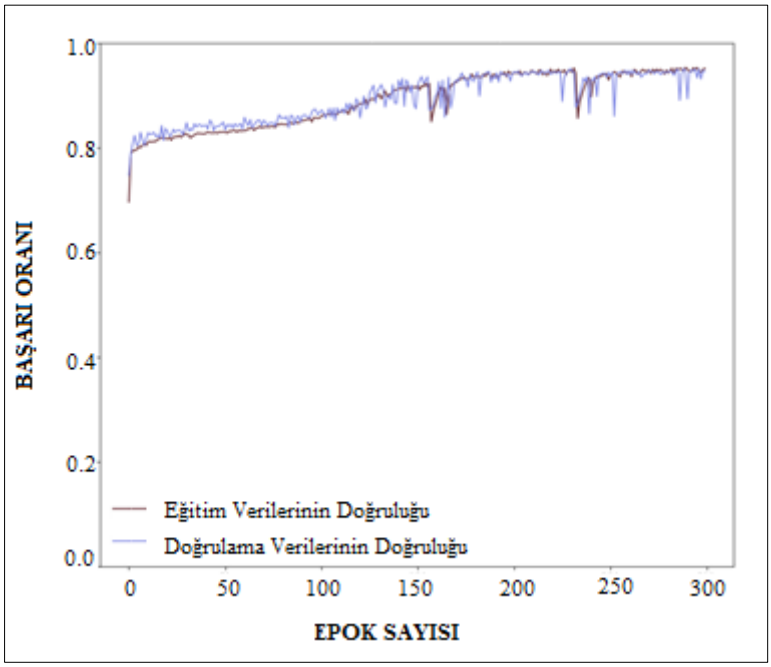
Şekil 5.1. Önerilen HİBRİT3b modelinin karışıklık matrisi

Çizelge 5.2. Önerilen HİBRİT3b modelinin karışıklık matrisi değerleri

		Tahmin Sınıfı							
		Normal (%)	TCP Seli (%)	UDP Seli (%)	SYN Seli (%)	IP Sahteciliği Seli (%)	ICMP Seli (%)	DP Oranı (%)	YN Oranı (%)
Gerçek Sınıf	Normal Durum	88,27	0,00	8,65	0,00	3,08	0,00	88,30	11,70
	TCP Seli	0,00	100	0,00	0,00	0,00	0,00	100	0,00
	UDP Seli	3,67	0,00	92,01	0,00	4,32	0,00	92,10	7,90
	SYN Seli	0,00	0,00	0,00	100	0,00	0,00	100	0,00
	IP Sahteciliği Seli	6,34	0,00	9,90	0,00	83,76	0,00	83,80	16,20
	ICMP Seli	0,00	0,00	0,00	0,00	0,00	100	100	0,00

Çizelge 5.2'de yer alan karışıklık matrisi değerleri, literatürde sıklıkla kullanılan Doğruluk metriğine göre değerlendirilmiştir. Buna göre, saldırı türleri arasında TCP, SYN ve ICMP Seli saldırılarının tümü %100 olarak doğru şekilde tespit edilmiştir. IP Sahteciliği Seli saldırısı %84 oranıyla en az tespit edilen saldırıdır. Bu saldırı için toplam 505 tane örneğin 423 tanesi doğru şekilde tespit edilmiştir. Saldırısız durumda ise 520 tane örneğin 459 tanesi saldırısız olarak belirlenmiş ve %88 gibi yüksek bir tespit oranı elde edilmiştir. UDP Seli saldırı tespiti de saldırısız durum tespitine yakın bir orana sahip olmuştur.

Veri kümesi test olarak ayrıldıktan sonra kalan %30'luk bölüm eğitim ve doğrulama için kullanılmıştır. Bu bölümlerin HİBRİT3b modeli ile analiz edilmesi sonucunda elde edilen Eğitim - Doğrulama Doğruluk başarı grafiği Şekil 5.2'de verilmiştir.

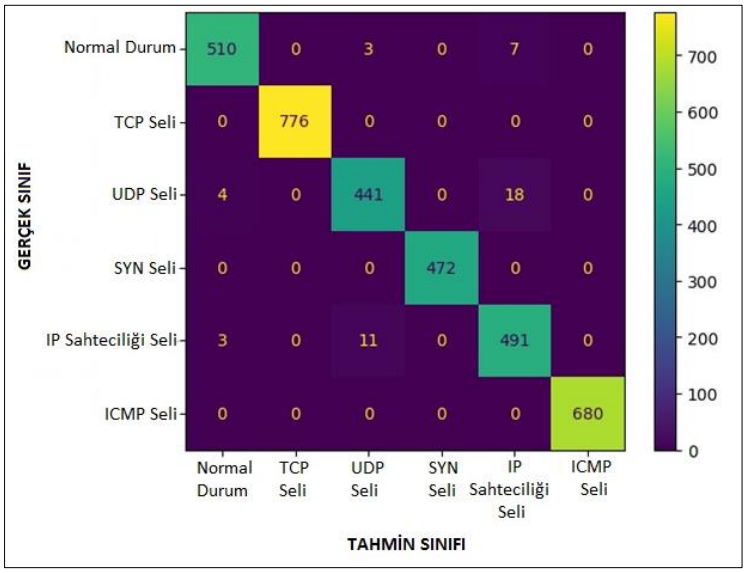


Şekil 5.2. Önerilen HİBRİT3b modelinin Eğitim - Doğrulama Doğruluk başarı grafiği

Eğitim ve doğrulama örnekleri 300 epok olarak analiz edilmiştir. Grafik incelendiğinde eğitim ve doğrulama performansının birbirine yakın başarı değerleri elde ettiği görülmüştür. Eğitim verilerinin doğruluğu arttıkça doğrulama verilerinin de doğruluğu artmaktadır. Böylece önerilen bu modelin başarısı grafik ile desteklenmiştir.

5.1.2. DT modeli ile elde edilen sonuçlar

DT modeli ile elde edilen karışıklık matrisi (Şekil 5.3) ve karışıklık matrisinden elde edilen değerler (Çizelge 5.3) aşağıda gösterilmiştir:



Şekil 5.3. Önerilen DT modelinin karışıklık matrisi

Çizelge 5.3. Önerilen DT modeli karışıklık matrisi değerleri

		Tahmin Sınıfı							
		Normal (%)	TCP Seli (%)	UDP Seli (%)	SYN Seli (%)	IP Sahteciliği Seli (%)	ICMP Seli (%)	DP Oranı (%)	YN Oranı (%)
Gerçek Sınıf	Normal Durum	98,08	0,00	0,58	0,00	1,34	0,00	98,10	1,90
	TCP Seli	0,00	100	0,00	0,00	0,00	0,00	100	0,00
	UDP Seli	0,86	0,00	95,25	0,00	3,89	0,00	95,30	4,70
	SYN Seli	0,00	0,00	0,00	100	0,00	0,00	100	0,00
	IP Sahteciliği Seli	0,59	0,00	2,18	0,00	97,23	0,00	97,30	2,70
	ICMP Seli	0,00	0,00	0,00	0,00	0,00	100	100	0,00

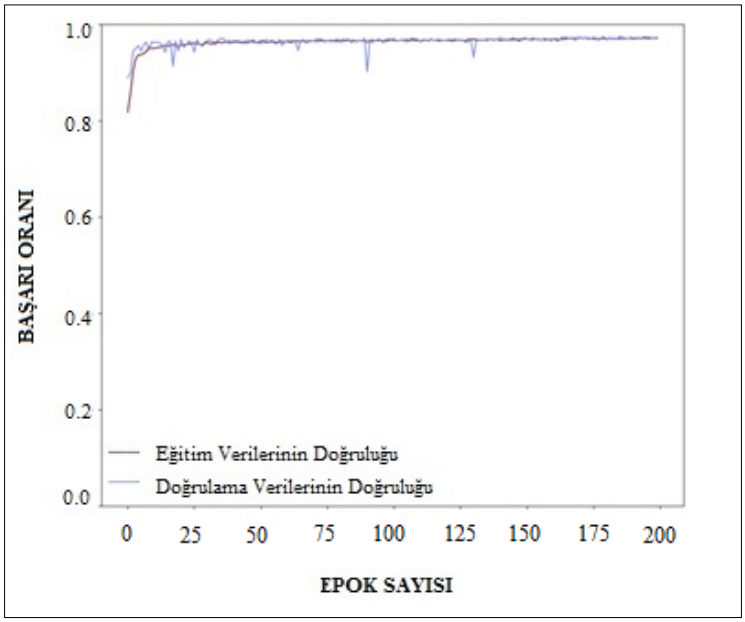
Çizelge 5.3'teki değerler de Doğruluk metriğine göre değerlendirilmiştir. HİBRİT3b modelinde olduğu gibi DT modelinde de TCP, SYN ve ICMP Seli saldırılarının tümü %100 olarak doğru şekilde tespit edilmiştir. UDP Seli saldırısı %95 oranıyla en az tespit edilen saldırıdır. Bu saldırı için toplam 463 tane örneğin 441 tanesi doğru şekilde tespit edilmiştir. Saldırısız durumda ise 520 tane örneğin 510 tanesi saldırısız olarak belirlenmiş ve %98 gibi

yüksek bir tespit oranı elde edilmiştir. IP Sahteciliği Seli saldırı tespiti de saldırısız durum tespitine yakın bir orana sahip olmuştur.

5.1.3. HİBRİT3b modeli ile literatürdeki bir veri kümesinin analiz sonuçları

Önerilen HİBRİT3b modelinin başarısını desteklemek için literatürde yer alan ve kullanılan bir veri kümesi üzerinde testler yapılmıştır. Bu veri kümesi Mississippi State Üniversitesi SCADA Laboratuvarı'nda üretilmiş ve su tankı kontrol sistemine ait veriler barındırmaktadır [14]. Veri kümesinde sınıf sütununda Normal Durum (1. Öznitelik), Komut Enjeksiyonu Saldırıları (2. - 6. Öznitelikler), DoS Saldırısı (7. Öznitelik) ve MITM Saldırısı (8. Öznitelik) yer almaktadır. Sınıf sütunu dışında 23 adet öznitelik bulunmaktadır. Morris ve arkadaşları yaptıkları çalışmada saldırı tespiti için Sinir Ağlarını kullanmışlar ve ortalama olarak %83 sınıflandırma başarı oranı elde etmişlerdir. Bu tez çalışmasında ise HİBRİT3b modeli ile testler gerçekleştirilmiş ve saldırıların tespitinde ortalama %98 oranında bir performans sağlanmıştır. Böylece, %15 oranında daha yüksek bir başarı oranı elde edilmiştir.

Su tankı kontrol sistemi veri kümesinin %30'luk bölümü eğitim ve doğrulama için ayrılmıştır. Bu bölümün HİBRİT3b modeli ile analiz edilmesi sonucunda elde edilen Eğitim - Doğrulama Doğruluk başarı grafiği Şekil 5.4'te verilmiştir.



Şekil 5.4. Önerilen HİBRİT3b modelinin farklı bir veri kümesi üzerinde Eğitim - Doğrulama Doğruluk başarı grafiği

Eğitim ve doğrulama örnekleri 200 epok olarak analiz edilmiştir. Grafik incelendiğinde eğitim ve doğrulama performansının birbirine yakın ve %100'e varan başarı değerleri elde ettiği görülmüştür. Eğitim verilerinin doğruluğunun artması, doğrulama verilerinin de doğruluğunu arttırmaktadır. Böylece önerilen bu modelin başarısı da grafik ile desteklenmiştir.

5.2. Tartışma ve Sınırlılıklar

Bu bölümde analiz sonuçlarından yola çıkılarak yapılan karşılaştırmalar ve yorumlar yer almaktadır.

5.2.1. Tartışma

Çalışmada önerilen modeller arasında en yüksek başarı oralarına sahip iki modelin analiz sonuçları ve literatürde incelenen çalışmaların bir kısmının analiz sonuçları kıyaslanmıştır. Elde edilen bilgilere Çizelge 5.4'te yer verilmiştir.

Çizelge 5.4. Literatürdeki çalışmaların kıyaslanması

Referanslar	Veri Kümeleri	Saldırı Türleri	Algoritmalar	Saldırı Tespit Oranları (Ortalama Doğruluk %)
3	Su dağıtım sistemi gerçek veri kümesi	Pompaların durumunu, suyun akış hızını ve basıncını değiştiren saldırılar	Destek Vektör Veri Tanımı	84,00
			Güçlü SVM	76,00
			Slab SVM	82,00
			Önerilen Metot	91,00
4	Kendi veri kümeleri	MITM	Hibrit SCADA-STS	100
5	DUWWTP veri kümesi	MITM	KNN	92,86
6	CyberGym SCADA Laboratuvarı veri kümesi Negev Ben-Gurion Üniversitesi SCADA Laboratuvarı veri kümesi	Enjeksiyon Saldırıları	ANN-SOM	85,00
			HMM	88,88
7	Kendi veri kümeleri	MITM, DoS, Pompa / tank / eşik değer durumlarıyla ilgili saldırılar	FNN	99,00
			LSTM	99,00
			FNN-LSTM	99,00
8	Kendi veri kümeleri	Ağ Tarama, MITM, DoS	OCVM	96,30
9	Kendi veri kümeleri	MITM, DoS	Çoktan Bire LSTM	99,00
			Çoktan Çoğa LSTM	98,00
10	ADFA-LD veri kümesi	DoS	IWP-CSO + SVM	91,50
			HNA-NN	83,20
			IWP-CSO + HNA-NN	93,10
			SVM	74,90

Çizelge 5.4. (devam) Literatürdeki çalışmaların kıyaslanması

Referanslar	Veri Kümeleri	Saldırı Türleri	Algoritmalar	Saldırı Tespit Oranları (Ortalama Doğruluk %)
14	Mississippi State Universitesi SCADA Laboratuvarı: su tankı kontrol sistemi veri kümesi	Komut Enjeksiyonu, MITM, DoS	Sinir Ağları	83,00
56	Kendi veri kümeleri	Port, Cihaz, Adres Tarama ve Sızma	RF	99,89
			DT	99,89
			LR	99,59
			NB	99,60
			KNN	72,29
Çalışmamız	Oluşturduğumuz veri kümesi	DDoS	HİBRİT3b Modeli	94,73
			DT Modeli	98,77
	Mississippi State Universitesi SCADA Laboratuvarı: su tankı kontrol sistemi veri kümesi	Komut Enjeksiyonu, MITM, DoS	HİBRİT3b Modeli	98,09

Çalışma, SCADA sistemlerinin kullanıldığı fiziksel test yatağına yönelik DDoS saldırılarının tespit edilmesini ele almaktadır. Bunun için makine öğrenmesine dayalı yaklaşımlar kullanılmıştır. Literatürde hazır veri kümesi kullanarak saldırı tespiti yapan çalışma sayısı çok fazladır. Saldırı tespiti için test yatağı oluşturan, kendi veri kümesini hazırlayan ve veri kümesi kullanarak analizler yapan çalışma sayısı daha azdır. İki tür çalışmaya da yer verilmiş ve incelemeler yapılmıştır.

Saldırı tespitinde genellikle KNN, NB, RF ve LSTM gibi makine öğrenmesi tabanlı sınıflandırıcı yöntemleri ve Sinir Ağları kullanılmıştır. Çizelge 5.4'te görüldüğü gibi, SCADA sistemlerine yönelik saldırı tespitinde farklı algoritmalar farklı veri kümeleri için kullanılmıştır. Her veri kümesi farklı karakteristik özelliklere sahiptir ve kendi içinde değerlendirilmelidir.

Literatürde incelenen çalışmalarda makine öğrenmesi yaklaşımları, SCADA sistemlerine yönelik saldırı tespitinde ortalama %90 üzerinde başarı sağlamıştır. Bu çalışmada yapılan analizler sonucunda makine öğrenmesi tabanlı olmak üzere iki model önerilmiştir. CNN ve LSTM algoritmalarının birlikte kullanıldığı hibrit model ile %95 oranında başarı sağlanmıştır. DT tabanlı model ile %99 gibi daha yüksek bir başarı oranı elde edilmiştir.

Oluşturduğumuz test yatağı, kullandığımız teknolojiler ve hazırladığımız veri kümesi ile literatüre göre katma değeri yüksek bir çalışma elde ettik. Önerdiğimiz makine öğrenmesi tabanlı hibrit modelin performansını göstermek için farklı bir metot daha kullanılmıştır. Literatürde sıklıkla kullanılan ve kıyaslama tablosunda yer alan bir veri kümesi seçilmiş ve

analiz yapmak için değerlendirilmiştir. Morris ve arkadaşlarının hazırladığı bu veri kümesi önerdiğimiz HİBRİT3b Modeli ile analiz edilmiş ve saldırı tespiti için yüksek oranda başarı elde edilmiştir. Elde edilen sonuç Çizelge 5.4'ün son satırında gösterilmiştir.

5.2.2. Sınırlılıklar

Önerdiğimiz modellerin literatürdeki diğer modellere göre daha yüksek veya çok yakın değerde performanslara sahip olduğu görülmüştür. Saldırıların farklı hale gelmesi ve geliştirilmesi sebepleriyle yeni analiz çalışmalarının farklı ortamlar üzerinde de gerçekleştirilmesi gerekmektedir ve bu çalışmada bu durum gerçekleştirilmiştir. Sonuç olarak SCADA sistemlerine yönelik saldırı tespit çalışmalarının sıklıkla güncellenmesi ve çeşitlilik kazanması önem arz etmektedir.

5.3. Sonuç

Kritik altyapı sistemlerinin ve operasyonların sorunsuz çalışması SCADA sisteminin işlevselliğinin devamlılığına bağlıdır. SCADA sistemine yönelik DDoS saldırıları ile sistem kesintiye uğrayabilir ve işlevsellik yitirilebilir. SCADA sisteminin çalışmasında kesinti yaşanması ciddi maddi kayıplara veya zaman kaybına neden olabilmektedir. Çalışmada önerilen yöntemler SCADA sistemlerinin siber saldırılara karşı savunmasını daha güçlü hale getirecektir. Bu sayede sisteme yönelik bir DDoS saldırısının erken tespiti sağlanacak ve olması muhtemel felaket senaryolarının önüne geçilmesi kolaylaşacaktır.

Bu çalışmada, SCADA sistemi kullanılarak hazırlanan test yatağına yönelik DDoS saldırıları gerçekleştirilmiştir. Saldırılar sırasında ve saldırısız durumda elde edilen veriler kaydedilmiştir. Gerekli görülen ön işlemlerden geçirilen veri kümesi üzerinde CNN, LSTM, CNN-LSTM Hibrit ve diğer makine öğrenmesi modelleri ile testler yapılmıştır. Modellere ait parametreler değiştirilerek farklı sürümler elde edilmiş ve testlerde kullanılmıştır. SCADA sistemine yönelik DDoS saldırı tespiti için önerilen makine öğrenmesi tabanlı CNN-LSTM hibrit model ile %95 ve DT modeli ile %99 gibi sınıflandırma doğruluğu yakalanarak yüksek verim elde edilmiştir. Hibrit modelin başarısını desteklemek ve güvenirliğini göstermek için literatürde sık kullanılan bir veri kümesi üzerinde de testler gerçekleştirilmiştir. Bu veri kümesi kullanılarak literatürde yapılan çalışmanın %83 olan

doğruluk oranı geçilmiş ve %98 gibi daha yüksek bir doğruluk oranı elde edilerek başarılı bir performans sağlanmıştır.

DDoS saldırı tespitine ek olarak DDoS saldırı türü tespiti de yapılmıştır. Makine öğrenmesi tabanlı modeller ile TCP, SYN ve ICMP Seli saldırılarının tümü doğru şekilde tespit edilmiştir. SCADA sistemlerine yönelik oluşabilecek bu tip saldırıların tespitinde bu modeller yüksek oranda başarı ve verimlilik sağlayacaktır. Bu yönüyle de literatüre katkı sunulması ve ileriki çalışmalar için yol gösterilmesi amaçlanmıştır.

5.4. Öneriler

SCADA sistemlerine yönelik DDoS saldırılarının etkilerini azaltmak için daha fazla tespit çalışmaları yapılmalıdır. SCADA sistemleri çok farklı sektörlerde ve alanlarda kullanıldığı için farklı ve yeni teknolojiler kullanılarak çalışmalar çeşitlendirilmelidir. Gelecek çalışmalarda SCADA sistem test yatağı ortamının daha kapsamlı ve etkin şekilde hazırlanması hedeflenmektedir. Farklı protokollerin (DNP3, Profinet gibi) ortama dâhil edilmesi, bu ortama yönelik DDoS saldırılarından farklı saldırılar (MITM, Reconnaissance gibi) uygulanması ve bunların tespit edilmesi için kullanılacak modellerin (Yapay Sinir Ağları, farklı hibrit yapılar gibi) çeşitlendirilmesi amaçlanmaktadır. Farklı protokoller, saldırılar ve tespit modelleri uygulanarak literatürde yer alan çalışmalardan daha yüksek performans sağlanması ve bu kapsamda katkılar sunulması ileriki hedefler arasındadır.

KAYNAKLAR

1. Fanuscu, M.Ç., Koçak, A., Alkan, M. (2022). *Detection of Counter-Forensic Incidents Using Security Information and Incident Management (SIEM) Systems.* 15. Uluslararası Bilgi Güvenliği ve Kriptografi Konferansı (ISCTURKEY) (s. 74-79). Ankara, Turkey.

2. Dominguez, M., Prada, M. A., Reguera, P., Fuertes, J. J., Alonso, S., Moran, A. (2017). Cybersecurity training in control systems using real equipment. *IFAC-PapersOnLine,* 50(1), 12179-12184.

3. Nader, P., Honeine, P., Beauseroy, P. (2016). *Detection of cyberattacks in a water distribution system using machine learning techniques.* In 2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC) (pp. 25-30). IEEE.

4. Yang, Y., McLaughlin, K., Sezer, S., Littler, T., Im, E. G., Pranggono, B., Wang, H. F. (2014). Multiattribute SCADA-specific intrusion detection system for power networks. *IEEE Transactions on Power Delivery,* 29(3), 1092-1102.

5. Almalawi, A., Yu, X., Tari, Z., Fahad, A., Khalil, I. (2014). An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems. *Computers & Security,* 46, 94-110.

6. Kalech, M. (2019). Cyber-attack detection in SCADA systems using temporal pattern recognition techniques. *Computers & Security,* 84, 225-238.

7. Gao, J., Gan, L., Buschendorf, F., Zhang, L., Liu, H., Li, P., Lu, T. (2021). Omni SCADA intrusion detection using deep learning algorithms. *IEEE Internet of Things Journal,* 8(2), 951-961.

8. Maglaras, L. A., Jiang, J., Cruz, T. (2014). Integrated OCSVM mechanism for intrusion detection in SCADA systems. *Electronics Letters,* 50(25), 1935-1936.

9. Gao, J., Gan, L., Buschendorf, F., Zhang, L., Liu, H., Li, P., Dong, X., Lu, T. (2019). *LSTM for SCADA intrusion detection.* In 2019 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM) (pp. 1-5). Victoria, BC, Canada.

10. Shitharth, S., Winston D, P. (2017). An enhanced optimization based algorithm for intrusion detection in SCADA network. *Computers & Security,* 70, 16-26.

11. İnternet: ADFA Intrusion detection datasets. (2013). Web: https://research.unsw.edu.au/projects/adfa-ids-datasets. Son Erişim Tarihi: 17.03.2020.

12. Sayegh, N., Chehab, A., Elhajj, I. H., Kayssi, A. (2013). *Internal Security Attacks on SCADA Systems.* The 3rd International Conference on Communications and Information Technology, 22–27, Beyrut, Lübnan.

13. Koutsandria, G., Gentz, R., Jamei, M., Scaglione, A., Peisert, S., McParland, C. (2015). *A real-time testbed environment for cyber-physical security on the power grid.* Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, 67–78, Colorado, ABD.

14. Morris, T., Srivastava, A., Reaves, B., Gao, W., Pavurapu, K., Reddi, R. (2011). A control system testbed to validate critical ınfrastructure protection concepts. *International Journal of Critical Infrastructure Protection,* 4(2), 88–103.

15. Hahn, A. (2013). *Cyber Security of the Smart Grid: Attack Exposure Analysis, Detection Algorithms, and Testbed Evaluation,* Doktora Tezi, Computer Engineering of Iowa State University, ABD.

16. Hahn, A., Ashok, A., Sridhar, S., Govindarasu, M. (2013). Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. *IEEE Transactions on Smart Grid,* 4(2), 847–855.

17. Kuipers, D. (2008). *Common cyber security vulnerabilities observed in control system assessments by the inl nstb program.* Idaho National Lab. (INL), Idaho Falls, ID (United States), Tech. Rep.

18. Bergman, D. C., Jin, D., Nicol, D. M., Yardley, T. (2009). *The virtual power system testbed and ınter-testbed integration*. Proceedings of the 2nd conference on Cyber Security Experimentation and Test, 1-6, ABD.

19. Dondossola, G., Garrone, G., Szanto, J., Deconinck, G., Loix, T., Beitollahi, H. (2009). *ICT resilience of power control systems: Experimental results from the crutial testbeds*. Proceedings of the International Conference on Dependable Systems and Networks, 554–559, Lizbon, Portekiz.

20. Dondossola, G., Deconinck, G., Garrone, F., Beitollahi, H. (2009). *Testbeds for assessing critical scenarios in power control systems.* International Workshop on Critical Information Infrastructures Security, 223–234, Berlin, Almanya.

21. Mallouhi, M., Al-Nashif, Y., Cox, D., Chadaga, T., Hariri, S. (2011). *A testbed for Analyzing Security of SCADA Control Systems (TASSCS)*. IEEE PES Innovative Smart Grid Technologies Conference Europe, ISGT Europe, 1–7, Anaheim, ABD.

22. Wu, J. H., Shyan, S., Alexandru, S., Ahmed, F., Ching, L. C., Pavel, G., Manimaran, G. (2011). *An ıntrusion and defense testbed in a cyber-power system environment.* Power and Energy Society General Meeting, 1–5, İrlanda.

23. Queiroz, C., Mahmood, A., Tari, Z. (2011). SCADASim A Framework for Building SCADA Simulations. *IEEE Transactions on Smart Grid,* 2(4), 589–597.

24. Yanfei, L., Cheng, W., Chengbo, Y., Xiaojun, Q. (2009). *Research on zigbee wireless sensors network based on modbus protocol.* Proceedings - 2009 International Forum on Information Technology and Applications, IFITA 2009, 1, Nisan, 487–490.

25. Yanfei, L., Cheng, W. (2009*). An improved design of zigbee wireless sensor network.* 2009 2nd IEEE International Conference on Computer Science and Information Technology, 515–518, Beijing, Çin.

26. Beresford, D. (2011). *Exploiting Siemens Simatic S7 PLCs.* Black Hat USA, 16(2), 723-733.

27. Chabukswar, R., Sinópoli, B., Karsai, G., Giani, A., Neema, H., Davis, A. (2010). *Simulation of Network Attacks on SCADA Systems.* First Workshop on Secure Control Systems, 1-8, ABD.

28. İnternet: ITProPortal. The Evolution of DDoS. (2017). Web: http://www.itproportal.com/features/the-evolution-of-ddos. Son Erişim Tarihi: 04.07.2018.

29. Petrovic, J. D., Stojanovic, M. D. (2013). *Analysis of SCADA System Vulnerabilities to DDoS Attacks.* 2013 11th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services, TELSIKS, 2, 591–594.

30. Ciancamerla, E., Fresilli, B., Minichino, M., Patriarca, T., Iassinovski, S. (2014). *An Electrical Grid and Its SCADA under Cyber Attacks: Modelling Versus a Hybrid Testbed.* 2014 International Carnahan Conference on Security Technology (ICCST), 1–6, Roma, İtalya.

31. Lee, D., Kim, H., Kim, K., Yoo, P. D. (2014*). Simulated Attack on DNP3 Protocol in SCADA System.* In Proceedings of the 31th Symposium on Cryptography and Information Security, 1–6, Kagoshima, Japonya.

32. Morris, T. H., Gao, W. (2013). *Industrial Control System Cyber Attacks.* Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research, 22–29, Leicester, İngiltere.

33. Aloui, N. B. (2016). *Industrial Control Systems Dynamic Code Injection.* GreHack, Grenoble, Fransa.

34. Zhu, B., Joseph, A., Sastry, S. (2011*). A Taxonomy of Cyber Attacks on SCADA Systems.* Proceedings - 2011 IEEE International Conferences on Internet of Things and Cyber, Physical and Social Computing, iThings/CPSCom 2011, 380–388, Dalian, Çin.

35. Gao, W., Morris, T., Reaves, B., Richey, D. (2010). On SCADA Control System Command and Response Injection and Intrusion Detection. General Members Meeting and eCrime Researchers Summit, Dallas, ABD.

36. Ten, C. W., Manimaran, G., Liu, C. C. (2010). Cybersecurity for critical ınfrastructures: attack and defense modeling. *Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans,* 40(4), 853–865.

37. Shang, W. L., Li, L., Wan, M., Zeng, P. (2015). *Security defense model of modbus tcp communication based on zone / border rules.* Network Security and Communication Engineering: Proceedings of the 2014 International Conference on Network Security and Communication Engineering, 79-86 Londra, İngiltere.

38. Chen, B., Pattanaik, N., Goulart, A., Butler-Purry, K. L., Kundur, D. (2015). Implementing Attacks for Modbus/TCP Protocol in a Real-Time Cyber Physical System Testbed. Proceedings - CQR 2015: 2015 IEEE International Workshop Technical Committee on Communications Quality and Reliability, 1-6, Charleston, ABD.

39. Xiong, Q., Liu, H., Xu, Y., Rao, H., Yi, S., Zhang, B., Deng, H. (2015), *A vulnerability detecting method for modbus-TCP based on smart fuzzing mechanism.* IEEE International Conference on Electro Information Technology, 404–409, Dekalb, ABD.

40. Bhatia, S., Kush, N., Djamaludin, C., Akande, J., Foo, E. (2014). Practical modbus flooding attack and detection. *Conferences in Research and Practice in Information Technology Series,* 149, 57–65.

41. Jung, S., Song, J. G., Kim, S. (2008). Design on SCADA test-bed and security device. *International Journal of Multimedia and Ubiquitous Engineering,* 3(4), 75-86.

42. Irmak, E., Erkek, İ. (2018). Endüstriyel kontrol sistemleri ve SCADA uygulamalarının siber güvenliği: Modbus TCP Protokolü örneği. *Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji,* 6(1), 1-16.

43. Korkmaz, E., Dolgikh, A., Davis, M., Skormin, V. (2016). *Industrial control systems security testbed*. 11th Annual Symposium on Information Assurance (ASIA '16). Albany, NY, USA.

44. Hahn, A., Kregel, B., Govindarasu, M., Fitzpatrick, J., Adnan, R., Sridhar, S., Higdon, M. (2010). *Development of the PowerCyber SCADA security testbed.* In Proceedings of the sixth annual workshop on cyber security and information intelligence research (p. 21). ACM.

45. Morris, T., Thornton, Z., Turnipseed, I. (2015). *Industrial control system simulation and data logging for ıntrusion detection system research.* 7th Annual Southeastern Cyber Security Summit. Huntsvile, AL.

46. Almalawi, A., Tari, Z., Khalil, I., Fahad, A. (2013). *SCADAVT-A framework for SCADA security testbed based on virtualization technology.* Proceedings - Conference on Local Computer Networks, LCN. 639-646.

47. Wang, C., Fang, L., Dai, Y. (2010). A simulation environment for SCADA security analysis and assessment. In *2010 International Conference on Measuring Technology and Mechatronics Automation* (Vol. 1, pp. 342-347). Changsha City.

48. Patriarca, T., Minichino, M., Fresilli, B., Ciancamerla, E. (2016). *Cyber attacks on scada of critical infrastructures by an Hybrid Testbed.* In the 6th International Defense and Homeland Security Simulation Workshop, DHSS 2016. Dime University of Genoa.

49. Queiroz, C., Mahmood, A., Hu, J., Tari, Z., Yu, X. (2009). Building a SCADA security testbed. In *2009 Third International Conference on Network and System Security* (pp. 357-364). IEEE.

50. Reaves, B., Morris, T. (2012). An open virtual testbed for industrial control system security research. *International Journal of Information Security*, *11*, 215-229.

51. Tesfahun, A., Bhaskari, D. L. (2016). A SCADA testbed for investigating cyber security vulnerabilities in critical infrastructures. *Automatic Control and Computer Sciences*, *50*, 54-62.

52. Alhaidari, F. A., AL-Dahasi, E. M. (2019). New approach to determine DDoS attack patterns on SCADA system using machine learning. 2019 International Conference on Computer and Information Sciences (ICCIS), (pp. 1-6). Sakaka, Saudi Arabia, 2019, pp. 1-6.

53. Hindy, H., Brosset, D., Bayne, E., Seeam, A., Bellekens, X. (2019). Improving SIEM for critical SCADA water infrastructures using machine learning. In *Computer Security: ESORICS 2018 International Workshops, CyberICPS 2018 and SECPRE 2018, Barcelona, Spain, September 6–7, 2018, Revised Selected Papers 2* (pp. 3-19). Cham: Springer International Publishing.

54. Beaver, J. M., Borges-Hink, R. C., Buckner, M. A. (2013). *An evaluation of machine learning methods to detect malicious SCADA communications.* In 2013 12th International Conference on Machine Learning and Applications (Vol. 2, pp. 54-59). Miami, FL, ABD.

55. Hink, R. C. B., Beaver, J. M., Buckner, M. A., Morris, T., Adhikari, U., Pan, S. (2014). *Machine learning for power system disturbance and cyber-attack discrimination.* In 2014 7th International symposium on resilient control systems (ISRCS) (pp. 1-8). Denver, CO, USA.

56. Teixeira, M. A., Salman, T., Zolanvari, M., Jain, R., Meskin, N., Samaka, M. (2018). SCADA system testbed for cybersecurity research using machine learning approach. *Future Internet*, 10(8), 76.

57. Benisha, R. B., Ratna, S. R. (2020). Detection of Intrusion using Enhanced Machine Learning Model in SCADA Wireless Network. *International Journal of Future Generation Communication and Networking*, 13(1), 85-98.

58. Perez, R. L., Adamsky, F., Soua, R., Engel, T. (2018). *Machine learning for reliable network attack detection in SCADA systems.* In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 633-638). New York, NY, USA.

59. Wan, M., Yao, J., Jing, Y., Jin, X. (2018). Event-based anomaly detection for non-public industrial communication protocols in SDN-based control systems. *CMC: Comput. Mater. Continua*, *55*(3), 447-463.

60. Radoglou-Grammatikis, P., Sarigiannidis, P., Efstathopoulos, G., Karypidis, P. A., Sarigiannidis, A. (2020). *DIDEROT: an intrusion detection and prevention system for DNP3-based SCADA systems*. In Proceedings of the 15th International Conference on Availability, Reliability and Security. (pp. 1-8). New York.

61. İnternet: Skripcak, T., Tanuska, P. (2013). Utilisation of On-line Machine Learning for SCADA System Alarms Forecasting. Web: www.conference.thesai.org. Son Erişim Tarihi: 14.03.2020.

62. Söğüt, E., Erdem, O. A. (2020). Endüstriyel kontrol sistemlerine (scada) yönelik siber terör saldırı analizi. *Politeknik Dergisi*, *23*(2), 557-566.

63. Choubineh, A., Wood, D. A., Choubineh, Z. (2020). Applying separately cost-sensitive learning and Fisher's discriminant analysis to address the class imbalance problem: A case study involving a virtual gas pipeline SCADA system. *International Journal of Critical Infrastructure Protection, 29,* 100357.

64. Wang, W., Harrou, F., Bouyeddou, B., Senouci, S. M., Sun, Y. (2022). A stacked deep learning approach to cyber-attacks detection in industrial systems: application to power system and gas pipeline systems. *Cluster Computing,* 25(1), 561–578.

65. Basnet, M., Poudyal, S., Ali, M. H., 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.

66. Rajesh, L., Satyanarayana, P. (2022). Evaluation of Machine Learning Algorithms for Detection of Malicious Traffic in SCADA Network. *Journal of Electrical Engineering and Technology,* 17(2), 913–928.

67. Güntay, V. (2017). Uluslararası sistem ve güvenlik açısından değişen savaş kurgusu; Siber Savaş örneği. *Güvenlik Bilimleri Dergisi,* 6(2), 81-108.

68. Yılmaz, S. (2012). Türkiye'nin iç güvenlik yapılanmasında değişim ihtiyacı. *Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 21(3), 17-40.

69. Hekim, H., Başıbüyük, O. (2013). Siber suçlar ve Türkiye'nin siber güvenlik politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi, 4*(2), 135-158.

70. Söğüt, E., Erdem, O. A. (2023). A multi-model proposal for classification and Detection of DDoS Attacks on SCADA Systems. *Applied Sciences,* 13(10), 5993.

71. Turnipseed, I. P. (2015). *A new scada dataset for intrusion detection research.* Mississippi State University.

72. Erkek, İ. (2018). *Modbus Temelli Scada Sistemlerinin Siber Güvenliği İçin Yeni Bir Yaklaşim.* Yüksek Lisans Tezi, Bilgi Güvenliği Mühendisliği, Gazi Üniversitesi Fen Bilimleri Enstitüsü.

73. Shahzad, A., Musa, S., Aborujilah, A., Irfan, M. (2014). The SCADA Review: System Components, Architecture, Protocols and Future Security Trends. *American Journal of Applied Sciences,* 11(8), 1418–1425.

74. Mcdonald, J. D. (1993*). Developing and Defining Basic SCADA System Concepts.* Rural Electric Power Conference, 1993 Papers Presented at the 37th Annual Conference, 93, 1–5, Kansas City, ABD.

75. Patel, S. C., Bhatt, G. D., Graham, J. H. (2009). Improving the Cyber Security of SCADA Communication Networks. *Communications of the ACM,* 52(7), 139–142.

76. Turnipseed, I. (2015). *A new scada dataset for intrusion detection system research,* Master's Thesis, Mississippi State University, Electrical and Computer Engineering, Mississippi State.

77. Özbilen, A. (2012). *TCP/IP tabanlı dağıtık endüstriyel denetim sistemlerinde güvenlik ve çözüm önerileri*. Doctoral Thesis, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

78. TMMOB Elektrik Mühendisleri Odası. (2012). *Kontrol sistemleri-scada.* TMMOB Elektrik Mühendisleri Odasi Yayınları, EK/2012/524, Ankara

79. Erkek, İ. (2012). *Modbus temelli scada sistemlerinin siber güvenliği için yeni bir yaklaşım.* Master's Thesis, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

80. Yang, Y. S., Lee, S. H., Chen, W. C., Yang, C. S., Huang, Y. M., Hou, T. W. (2022). Securing SCADA Energy Management System under DDos attacks using token verification approach. *Applied Sciences*, 12(1), 530.

81. Kamal, P., Abuhussein, A., Shiva, S. (2017). Identifying and Scoring Vulnerability in SCADA Environments.

82. Yadav, G., Paul, K. (2021). Architecture and security of SCADA systems: A review. In *International Journal of Critical Infrastructure Protection* (Vol. 34). Elsevier B.V.

83. Fovino, I. N., Carcano, A., Masera, M., Trombetta, A. (2009). *Design and implementation of a secure modbus protocol.* In Critical Infrastructure Protection III: Third Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Hanover, New Hampshire, USA, March 23-25, 2009, Revised Selected Papers 3 (pp. 83-96). Springer Berlin Heidelberg.

84. East, S., Butts, J., Papa, M., Shenoi, S. (2009). *A Taxonomy of Attacks on the DNP3 Protocol.* In Critical Infrastructure Protection III: Third Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Hanover, New Hampshire, USA, March 23-25, 2009, Revised Selected Papers 3 (pp. 67-81). Springer Berlin Heidelberg.

85. Dias, A. L., Sestito, G. S., Turcato, A. C., Brandão, D. (2018, November). *Panorama, challenges and opportunities in PROFINET protocol research.* In 2018 13th IEEE International Conference on Industry Applications (INDUSCON) (pp. 186-193). IEEE.

86. Watson, V., Lou, X., Gao, Y. (2017). *A Review of PROFIBUS Protocol Vulnerabilities-Considerations for Implementing Authentication and Authorization Controls.* In SECRYPT (pp. 444-449).

87. Yu, W., Wang, Y., Song, L. (2019). A two stage intrusion detection system for industrial control networks based on ethernet/IP. *Electronics*, 8(12), 1545.

88. Kang, D. J., Robles, R. J. (2009). Compartmentalization of protocols in SCADA communication. *International Journal of Advenced Science and Technology*, 8, 27-36.

89. Yang, Y., McLaughlin, K., Sezer, S., Yuan, Y. B., Huang, W. (2014, July). *Stateful intrusion detection for IEC 60870-5-104 SCADA security.* In 2014 IEEE PES General Meeting Conference & Exposition (pp. 1-5). IEEE.

90. East, S., Butts, J., Papa, M., Shenoi, S. (2009). A taxonomy of attacks on the DNP3 protocol. *IFIP Advances in Information and Communication Technology*, 311, 67–81.

91. Wang, W., Harrou, F., Bouyeddou, B., Senouci, S. M., Sun, Y. (2022). A stacked deep learning approach to cyber-attacks detection in industrial systems: application to power system and gas pipeline systems. *Cluster Computing,* 25(1), 561–578.

92. Chen, B., Pattanaik, N., Goulart, A., Butler-Purry, K. L., Kundur, D. (2015). Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed. Proceedings - CQR 2015: 2015 IEEE International Workshop Technical Committee on Communications Quality and Reliability.

93. Farwell, J. P., Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, *53*(1), 23-40.

94. İnternet: Ryan Naraine. Remote Hacker Caught Poisoning Florida City Water Supply. (2021). Web: https://www.securityweek.com/remote-hacker-caught-poisoning-florida-city-water-supply. Son Erişim Tarihi: 05.01.2023.

95. Gürkaş-Aydin, Z., Gürtürk, U. (2023). Cyber Threats and Critical Infrastructures in the Era of Cyber Terrorism. In 4th International Conference on Artificial Intelligence and Applied Mathematics in Engineering: ICAIAME 2022 (pp. 274-287). Cham: Springer International Publishing.

96. Tesfahun, A., Bhaskari, D. L. (2016). A SCADA testbed for investigating cyber security vulnerabilities in critical infrastructures. *Automatic Control and Computer Sciences*, 50(1), 54-62.

97. de Brito, I. B., de Sousa Jr, R. T. (2022). Development of an open-source testbed based on the modbus protocol for cybersecurity analysis of nuclear power plants. *Applied Sciences*, 12(15), 7942.

98. Khan, A. A. Z. (2019). Misuse intrusion detection using machine learning for gas pipeline SCADA networks. In Proceedings of the international conference on security and management (SAM) (pp. 84-90). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

99. Polat, H., Türkoğlu, M., Polat, O., Şengür, A. (2022). A novel approach for accurate detection of the DDoS attacks in SDN-based SCADA systems based on deep recurrent neural networks. *Expert Systems with Applications,* 197, 116748.

100. Shitharth, S., Winston, D. P. (2015). A Comparative Analysis between Two Countermeasure Techniques to Detect DDoS with Sniffers in a SCADA Network. *Procedia Technology,* 21, 179–186.

101. Altunay, H. C., Albayrak, Z., Özalp, A. N., Çakmak, M. (2021). *Analysis of Anomaly Detection Approaches Performed Through Deep Learning Methods in SCADA Systems*. In the 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). (pp. 1-6). Ankara, Turkey.

102. Ercan, N. M., Sert, M. (2021). Anomaly Detection in Smart Home Environments using Convolutional Neural Network. In 2021 IEEE International Symposium on Multimedia (ISM) (pp. 27-30). IEEE.

103. Yapici, M. M., Tekerek, A., Topaloglu, N. (2018). *Convolutional neural network based offline signature verification application.* In 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT) (pp. 30-34), Ankara, Türkiye.

104. Atacak, İ., Kılıç, K., Doğru, İ. A. (2022). Android malware detection using hybrid ANFIS architecture with low computational cost convolutional layers. *PeerJ Computer Science*, *8*, e1092.

105. Kapucuoğlu, K. (2022). *Derin Öğrenme Ağları Kullanılarak Doğal Ortamda Hastalıklı Domateslerin Belirlenmesi.* Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Lisansüstü Eğitim Enstitüsü, İstanbul.

106. Oyucu, S., Polat, H. (2022). A language model optimization method for turkish automatic speech recognition system. *Politeknik Dergisi*, 1, 1-1.

107. Akgül, E. S. (2019). *Makine Öğenmesi İle Statik Kaynak Kod Analizi.* Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

108. Kara, Ş. E., Şamlı, R. (2021). Yazılım projelerinin maliyet tahmini için WEKA'da makine öğrenmesi algoritmalarının karşılaştırmalı analizi. *Avrupa Bilim ve Teknoloji Dergisi*, (23), 415-426.

109. Çelik, B. D. (2022). *Makine Öğrenmesi Yöntemleri İle Hava Kirliliği Tahmini: Manisa ve Zonguldak Örneği*. Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

110. Koçak, A., Söğüt, E., Alkan, M., Erdem, O. A. (2023). Detection of different windows PE malware using machine learning methods. *Politeknik Dergisi*, 1, 1-1.

111. Seçkin, A. Ç., Coşkun, A. (2019). Hierarchical fusion of machine learning algorithms in indoor positioning and localization. *Applied Sciences*, 9(18), 3665.

112. Hussain, S., Dahan, N. A., Ba-Alwib, F. M., Ribata, N. (2018). Educational data mining and analysis of students' academic performance using WEKA. *Indonesian Journal of Electrical Engineering and Computer Science*, *9*(2), 447-459.

113. Güllü, M. (2021). *Optimizasyon Temelli Öznitelik Seçme Yöntemleri İle Desteklenen Topluluk Öğrenme Yaklaşımına Dayalı Yazar Tanıma.* Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

114. İnternet: An Industrial Control System Cybersecurity Performance Testbed. (2015). Web: http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8089.pdf. Son Erişim Tarihi: 25.11.2022.

115. İnternet: Arduino Store. (2021). Web: https://store.arduino.cc/products/. Son Erişim Tarihi: 20.02.2023.

116. İnternet: Arduino MEGA 2560 Rev3 Product Reference Manual. (2023). Web: https://docs.arduino.cc/hardware/mega-2560. Son Erişim Tarihi: 11.01.2023.

117. Sindiren, E., Ciylan, B. (2019). Application model for privileged account access control system in enterprise networks. *Computers & Security*, 83, 52-67.

118. Güllü, M., Akcayol, M. A., Barışçı, N. (2022). Machine Learning-Based Comparative Study For Heart Disease Prediction. *Advances in Artificial Intelligence Research*, 2(2), 51-58.

119. Atacak, İ., Şencan, Ö. A. (2022). Mamdani ve Sugeno Tip Bulanık Çıkarım Sistemleri ile Sosyal Medya Haber Popülerliğinin Tahmini. *International Journal of Engineering Research and Development*, Special Issue 2022, 303-320.

120. Duman, E. (2022). Implementation of XGBoost method for healthcare fraud detection. *Scientific Journal of Mehmet Akif Ersoy University*, 5(2), 69-75.

121. Demirtas, M., Koc, K. (2022). Parameter extraction of photovoltaic cells and modules by INFO algorithm. *IEEE Access*, 10, 87022-87052.

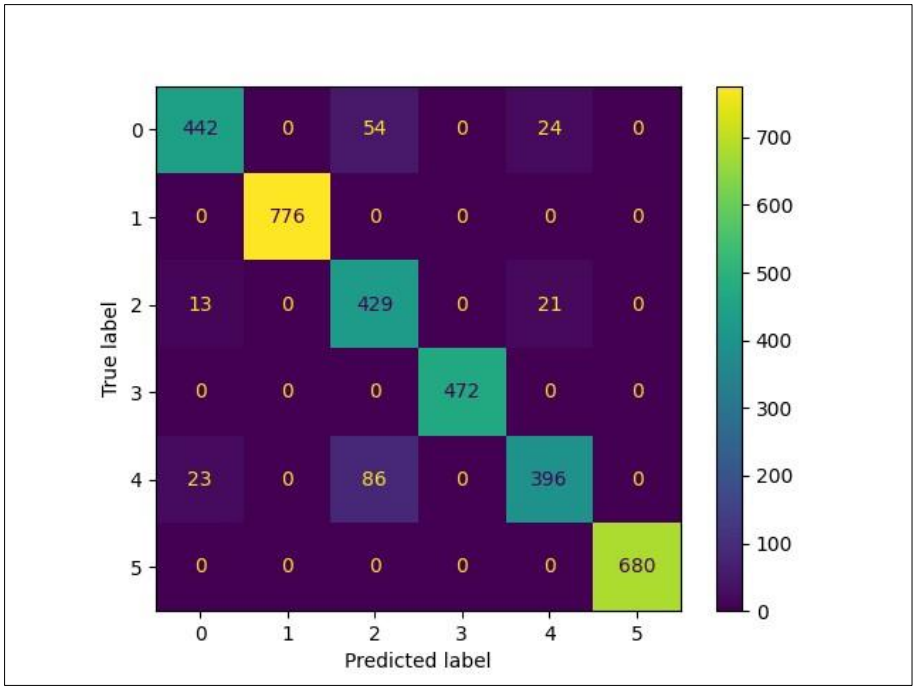
122. Ünal, Z. (2019). *Likert Tipi Verilerde Bulanık Mantık ve Derin Öğrenme Entegrasyonu.* Doktora Tezi, Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü, Antalya.

123. Hernandez-Suarez, A., Sanchez-Perez, G., Toscano-Medina, L. K., Olivares-Mercado, J., Portillo-Portilo, J., Avalos, J. G., García Villalba, L. J. (2022). Detecting Cryptojacking Web Threats: An Approach with Autoencoders and Deep Dense Neural Networks. *Applied Sciences*, *12*(7), 3234.

124. Chartuni, A., Márquez, J. (2021). Multi-classifier of DDoS attacks in computer networks built on neural networks. *Applied Sciences*, *11*(22), 10609.

EKLER

EK-1. CNN modelleri ile elde edilen sonuçlar

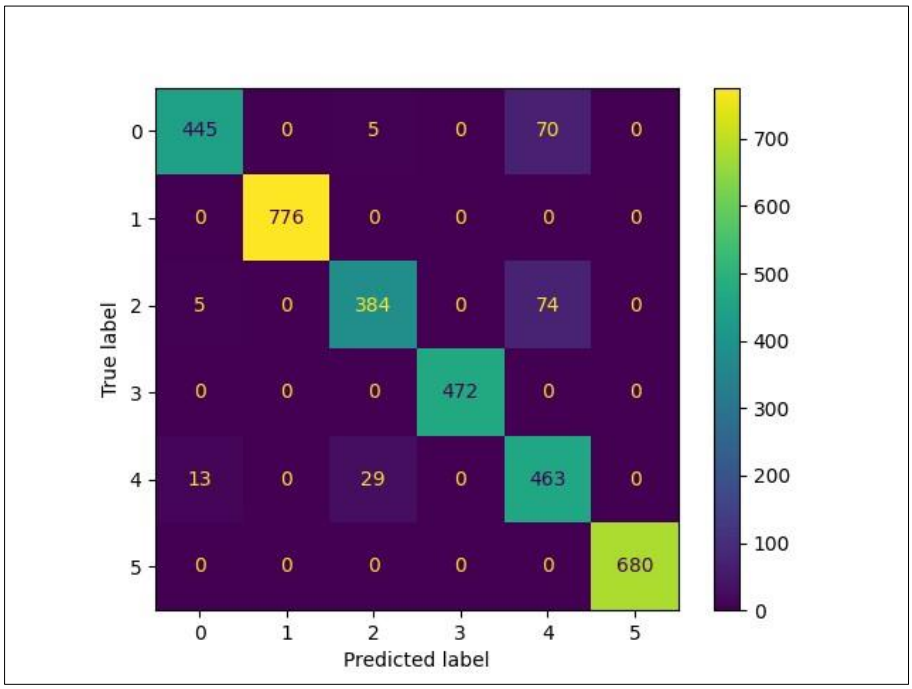


Şekil 1.1. CNN1a modelinin karışıklık matrisi

	precision	recall	f1-score
0	0.92	0.85	0.89
1	1.00	1.00	1.00
2	0.75	0.93	0.83
3	1.00	1.00	1.00
4	0.90	0.78	0.84
5	1.00	1.00	1.00
accuracy			0.94
macro avg	0.93	0.93	0.93
weighted avg	0.94	0.94	0.94

Şekil 1.2. CNN1a modelinin test sonuçları

EK-1. (devam) CNN modelleri ile elde edilen sonuçlar

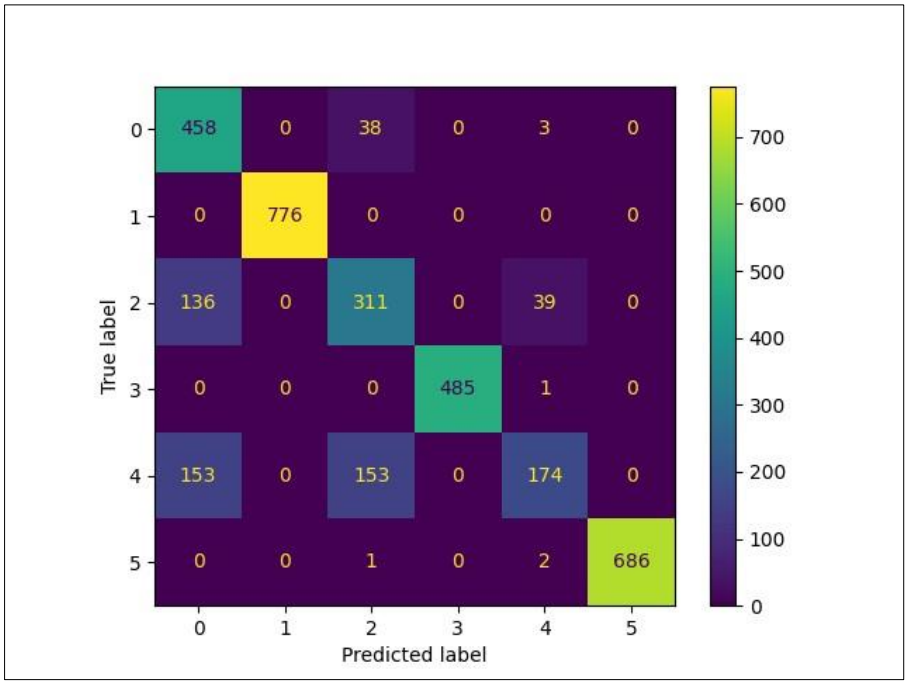


Şekil 1.3. CNN1b modelinin karışıklık matrisi

	precision	recall	f1-score
0	0.96	0.86	0.91
1	1.00	1.00	1.00
2	0.92	0.83	0.87
3	1.00	1.00	1.00
4	0.76	0.92	0.83
5	1.00	1.00	1.00
accuracy			0.94
macro avg	0.94	0.93	0.93
weighted avg	0.95	0.94	0.94

Şekil 1.4. CNN1b modelinin test sonuçları

EK-2. LSTM modelleri ile elde edilen sonuçlar

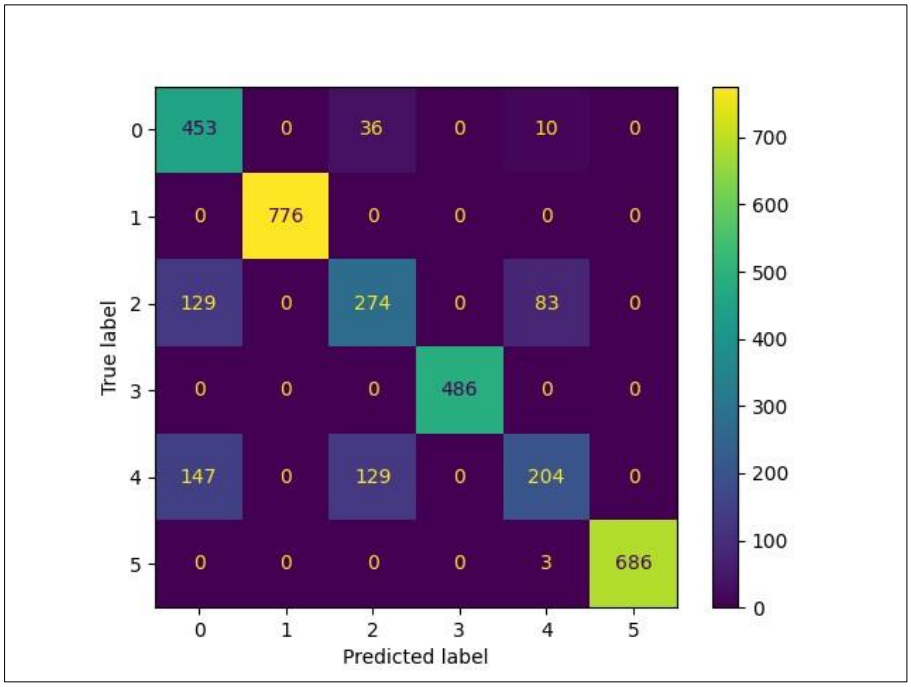


Şekil 2.1. LSTM1a modelinin karışıklık matrisi

	precision	recall	f1-score
0	0.61	0.92	0.74
1	1.00	1.00	1.00
2	0.62	0.64	0.63
3	1.00	1.00	1.00
4	0.79	0.36	0.50
5	1.00	1.00	1.00
accuracy			0.85
macro avg	0.84	0.82	0.81
weighted avg	0.86	0.85	0.84

Şekil 2.2. LSTM1a modelinin test sonuçları

EK-2. (devam) LSTM modelleri ile elde edilen sonuçlar

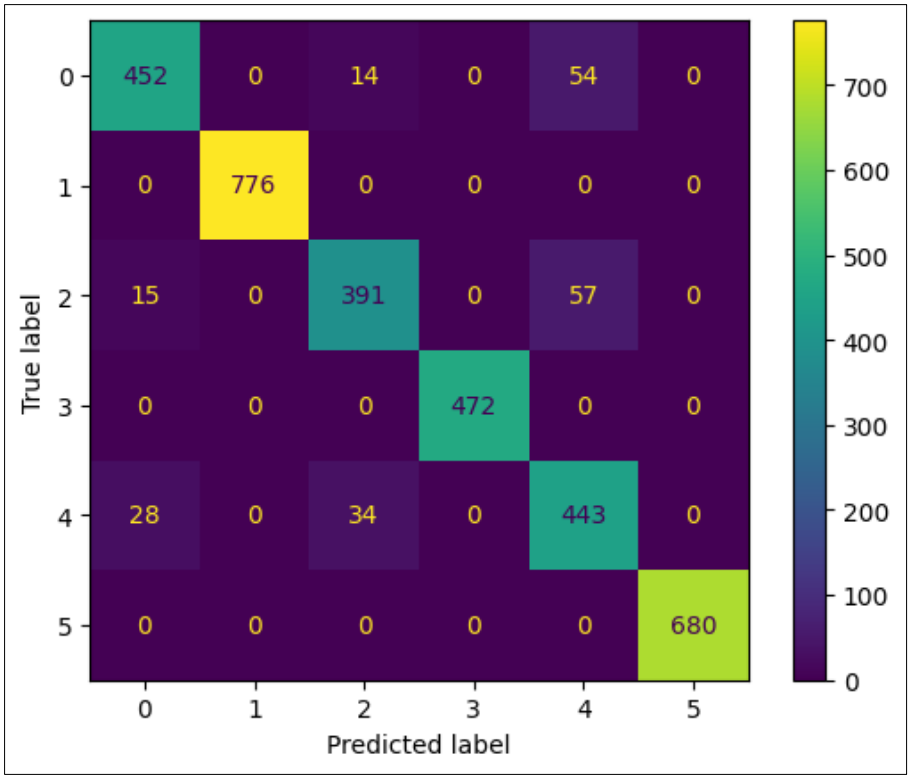


Şekil 2.3. LSTM1b modelinin karışıklık matrisi

	precision	recall	f1-score
0	0.62	0.91	0.74
1	1.00	1.00	1.00
2	0.62	0.56	0.59
3	1.00	1.00	1.00
4	0.68	0.42	0.52
5	1.00	1.00	1.00
accuracy			0.84
macro avg	0.82	0.82	0.81
weighted avg	0.85	0.84	0.84

Şekil 2.4. LSTM1b modelinin test sonuçları

EK-3. HİBRİT modeller ile elde edilen sonuçlar

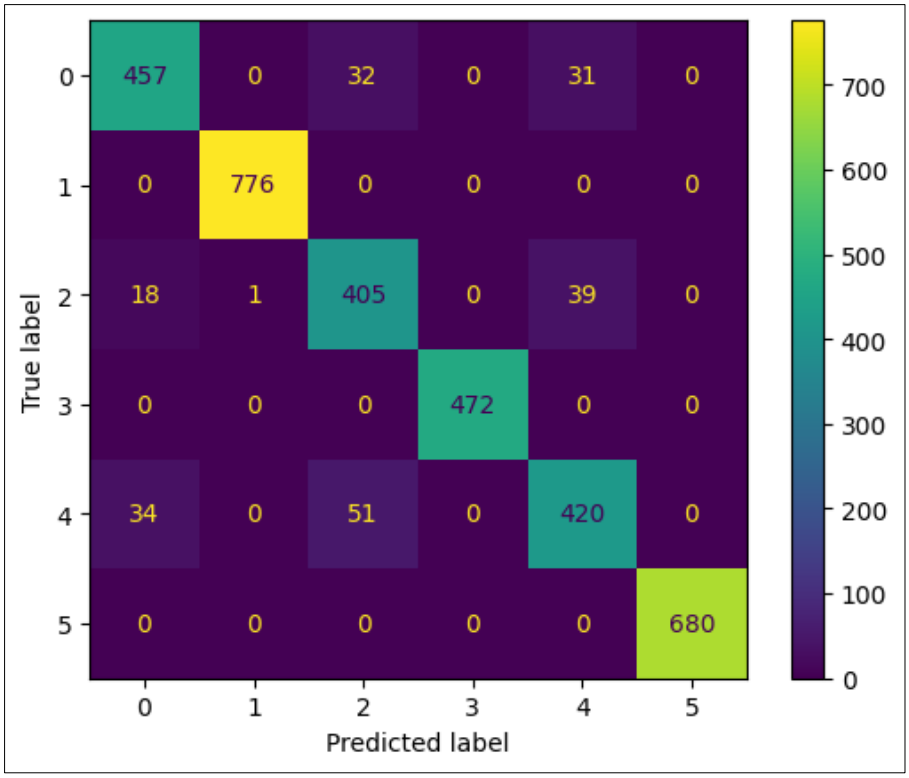


Şekil 3.1. HİBRİT1a modelinin karışıklık matrisi

	precision	recall	f1-score
0	0.91	0.87	0.89
1	1.00	1.00	1.00
2	0.89	0.84	0.87
3	1.00	1.00	1.00
4	0.80	0.88	0.84
5	1.00	1.00	1.00
accuracy			0.94
macro avg	0.93	0.93	0.93
weighted avg	0.94	0.94	0.94

Şekil 3.2. HİBRİT1a modelinin test sonuçları

EK-3. (devam) HİBRİT modeller ile elde edilen sonuçlar

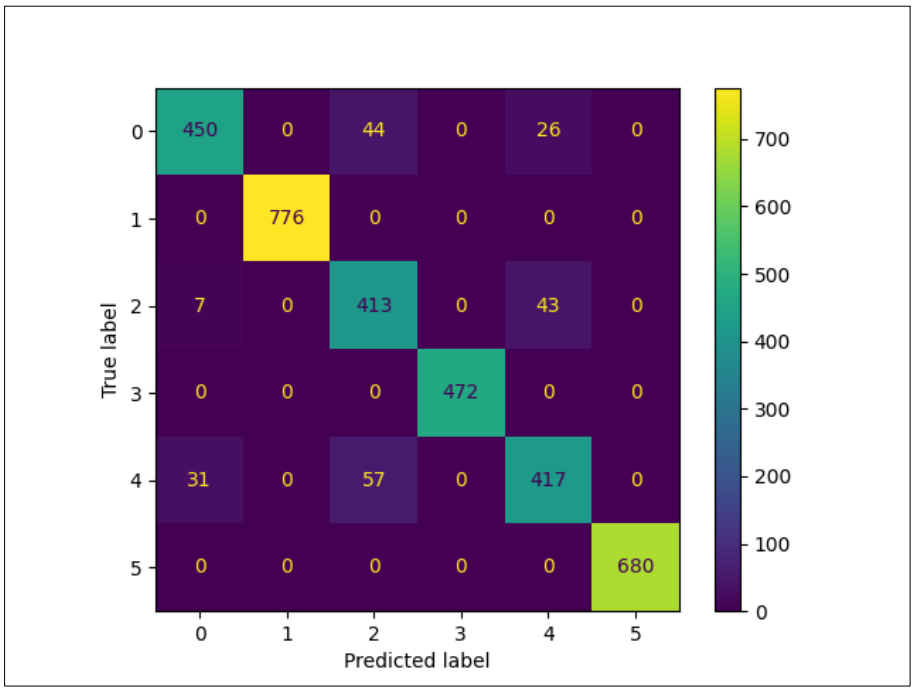


Şekil 3.3. HİBRİT1b modelinin karışıklık matrisi

	precision	recall	f1-score
0	0.90	0.88	0.89
1	1.00	1.00	1.00
2	0.83	0.87	0.85
3	1.00	1.00	1.00
4	0.86	0.83	0.84
5	1.00	1.00	1.00
accuracy			0.94
macro avg	0.93	0.93	0.93
weighted avg	0.94	0.94	0.94

Şekil 3.4. HİBRİT1b modelinin test sonuçları

EK-3. (devam) HİBRİT modeller ile elde edilen sonuçlar

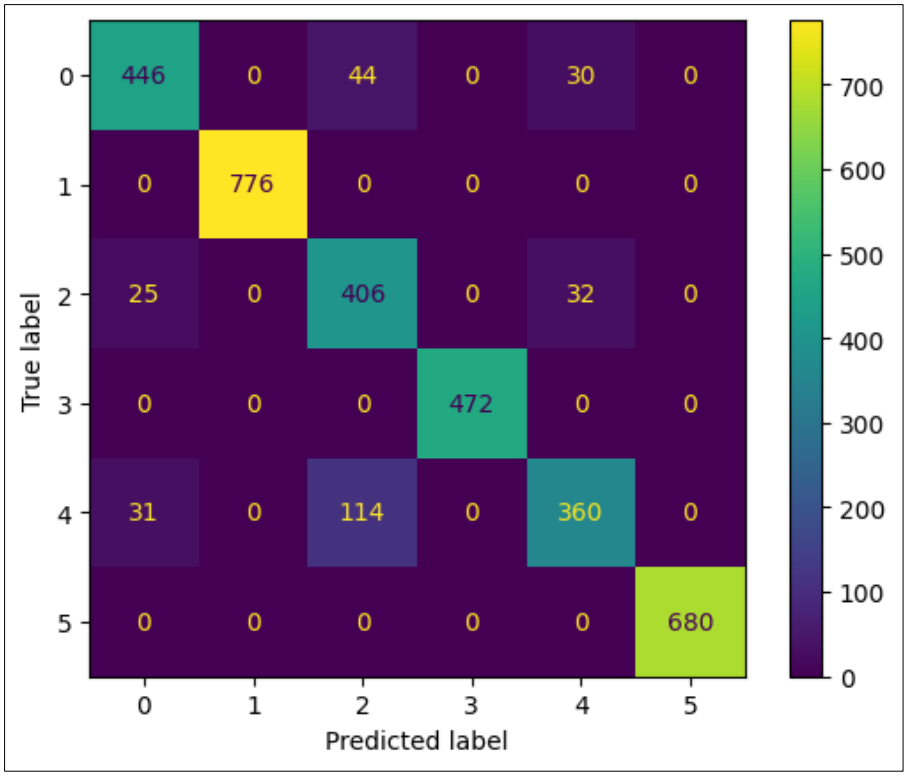


Şekil 3.5. HİBRİT2a modelinin karışıklık matrisi

	precision	recall	f1-score
0	0.92	0.87	0.89
1	1.00	1.00	1.00
2	0.80	0.89	0.85
3	1.00	1.00	1.00
4	0.86	0.83	0.84
5	1.00	1.00	1.00
accuracy			0.94
macro avg	0.93	0.93	0.93
weighted avg	0.94	0.94	0.94

Şekil 3.6. HİBRİT2a modelinin test sonuçları

EK-3. (devam) HİBRİT modeller ile elde edilen sonuçlar

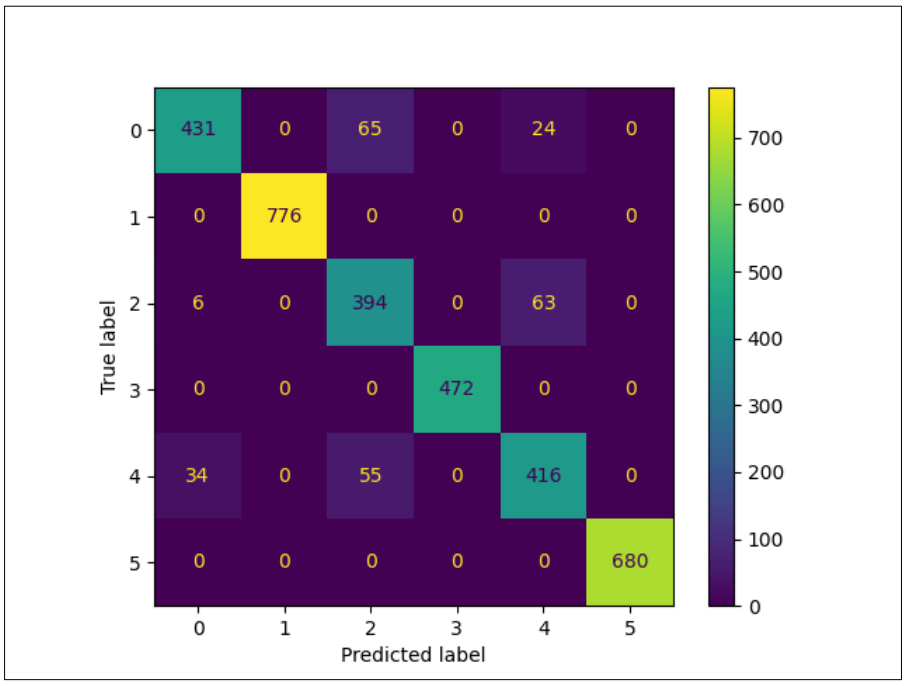


Şekil 3.7. HİBRİT2b modelinin karışıklık matrisi

	precision	recall	f1-score
0	0.89	0.86	0.87
1	1.00	1.00	1.00
2	0.72	0.88	0.79
3	1.00	1.00	1.00
4	0.85	0.71	0.78
5	1.00	1.00	1.00
accuracy			0.92
macro avg	0.91	0.91	0.91
weighted avg	0.92	0.92	0.92

Şekil 3.8. HİBRİT2b modelinin test sonuçları

EK-3. (devam) HİBRİT modeller ile elde edilen sonuçlar

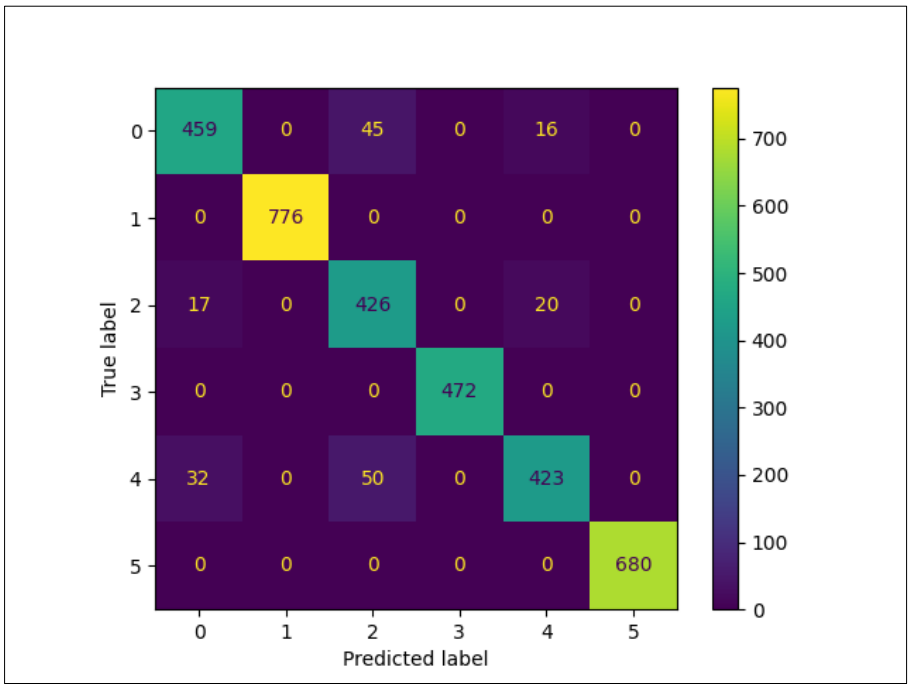


Şekil 3.9. HİBRİT3a modelinin karışıklık matrisi

	precision	recall	f1-score
0	0.92	0.83	0.87
1	1.00	1.00	1.00
2	0.77	0.85	0.81
3	1.00	1.00	1.00
4	0.83	0.82	0.83
5	1.00	1.00	1.00
accuracy			0.93
macro avg	0.92	0.92	0.92
weighted avg	0.93	0.93	0.93

Şekil 3.10. HİBRİT3a modelinin test sonuçları

EK-3. (devam) HİBRİT modeller ile elde edilen sonuçlar



Şekil 3.11. HİBRİT3b modelinin karışıklık matrisi

	precision	recall	f1-score
0	0.90	0.88	0.89
1	1.00	1.00	1.00
2	0.82	0.92	0.87
3	1.00	1.00	1.00
4	0.92	0.84	0.88
5	1.00	1.00	1.00
accuracy			0.95
macro avg	0.94	0.94	0.94
weighted avg	0.95	0.95	0.95

Şekil 3.12. HİBRİT3b modelinin test sonuçları

EK-4. KS modeli ile elde edilen sonuçlar

	Precision	Recall	F-Measure
0	0,743	0,804	0,772
1	0,733	0,992	0,843
2	0,752	0,676	0,712
3	0,976	0,444	0,610
4	0,676	0,684	0,680
5	1,000	0,997	0,999
Weighted Avg	0,819	0,799	0,790

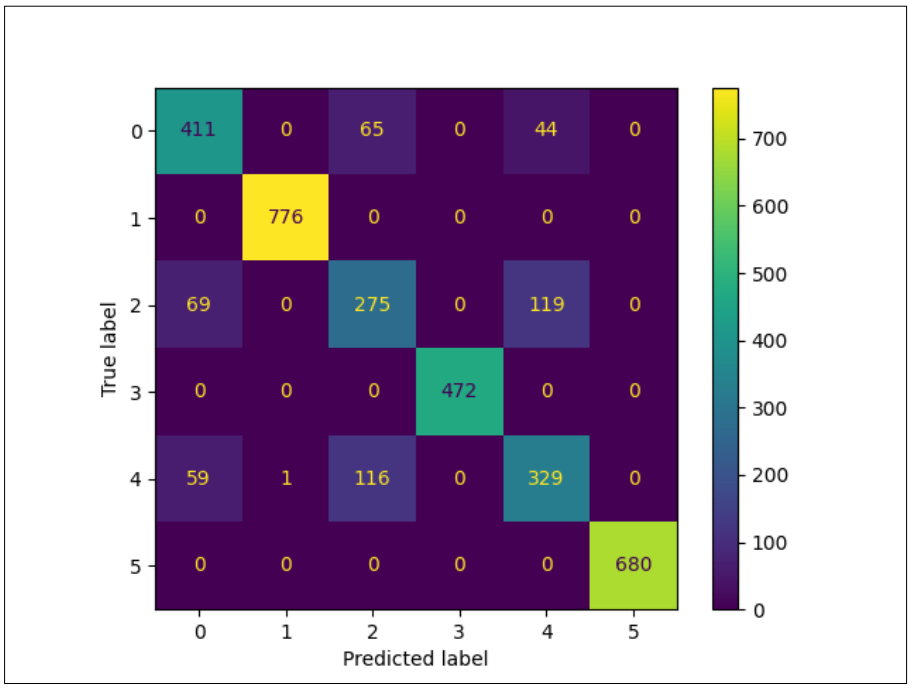
Şekil 4.1. KS modelinin test sonuçları

EK-5. LWL modeli ile elde edilen sonuçlar

	Precision	Recall	F-Measure
0	0,404	0,447	0,424
1	0,649	1,000	0,787
2	0,306	0,041	0,072
3	0,709	0,978	0,822
4	0,479	0,106	0,173
5	0,868	0,998	0,928
Weighted Avg	0,596	0,660	0,585

Şekil 5.1. LWL modelinin test sonuçları

EK-6. KNN modeli ile elde edilen sonuçlar



Şekil 6.1. KNN modelinin karışıklık matrisi

	precision	recall	f1-score
0	0.76	0.79	0.78
1	1.00	1.00	1.00
2	0.60	0.59	0.60
3	1.00	1.00	1.00
4	0.67	0.65	0.66
5	1.00	1.00	1.00
micro avg	0.86	0.86	0.86
macro avg	0.84	0.84	0.84
weighted avg	0.86	0.86	0.86
samples avg	0.86	0.86	0.86

Şekil 6.2. KNN modelinin test sonuçları

EK-7. LB modeli ile elde edilen sonuçlar

	Precision	Recall	F-Measure
0	0,519	0,965	0,675
1	1,000	1,000	1,000
2	0,929	0,377	0,536
3	0,998	1,000	0,999
4	0,755	0,481	0,588
5	1,000	0,999	1,000
Weighted Avg.	0,883	0,839	0,831

Şekil 7.1. LB modelinin test sonuçları

EK-8. AB modeli ile elde edilen sonuçlar

	Precision	Recall	F-Measure
0	?	0,000	?
1	0,648	1,000	0,786
2	?	0,000	?
3	?	0,000	?
4	?	0,000	?
5	0,313	1,000	0,477
Weighted Avg.	?	0,430	?

Şekil 8.1. AB modelinin test sonuçları

EK-9. NB modeli ile elde edilen sonuçlar

	Precision	Recall	F-Measure
0	0,791	0,817	0,804
1	0,772	1,000	0,871
2	0,800	0,775	0,787
3	0,984	0,543	0,700
4	0,760	0,752	0,756
5	1,000	0,997	0,999
Weighted Avg.	0,854	0,840	0,835

Şekil 9.1. NB modelinin test sonuçları

EK-10. BN modeli ile elde edilen sonuçlar

	Precision	Recall	F-Measure
0	0,795	0,828	0,811
1	0,795	0,999	0,885
2	0,795	0,785	0,790
3	0,997	0,602	0,751
4	0,780	0,758	0,769
5	1,000	0,997	0,999
Weighted Avg.	0,864	0,852	0,848

Şekil 10.1. BN modelinin test sonuçları

EK-11. ZeroR modeli ile elde edilen sonuçlar

	Precision	Recall	F-Measure
0	?	0,000	?
1	0,225	1,000	0,368
2	?	0,000	?
3	?	0,000	?
4	?	0,000	?
5	?	0,000	?
Weighted Avg.	?	0,225	?

Şekil 11.1. ZeroR modelinin test sonuçları

EK-12. PART modeli ile elde edilen sonuçlar

	Precision	Recall	F-Measure
0	0,421	1,000	0,593
1	1,000	1,000	1,000
2	1,000	0,187	0,315
3	1,000	1,000	1,000
4	1,000	0,293	0,453
5	1,000	0,997	0,999
Weighted Avg.	0,913	0,792	0,771

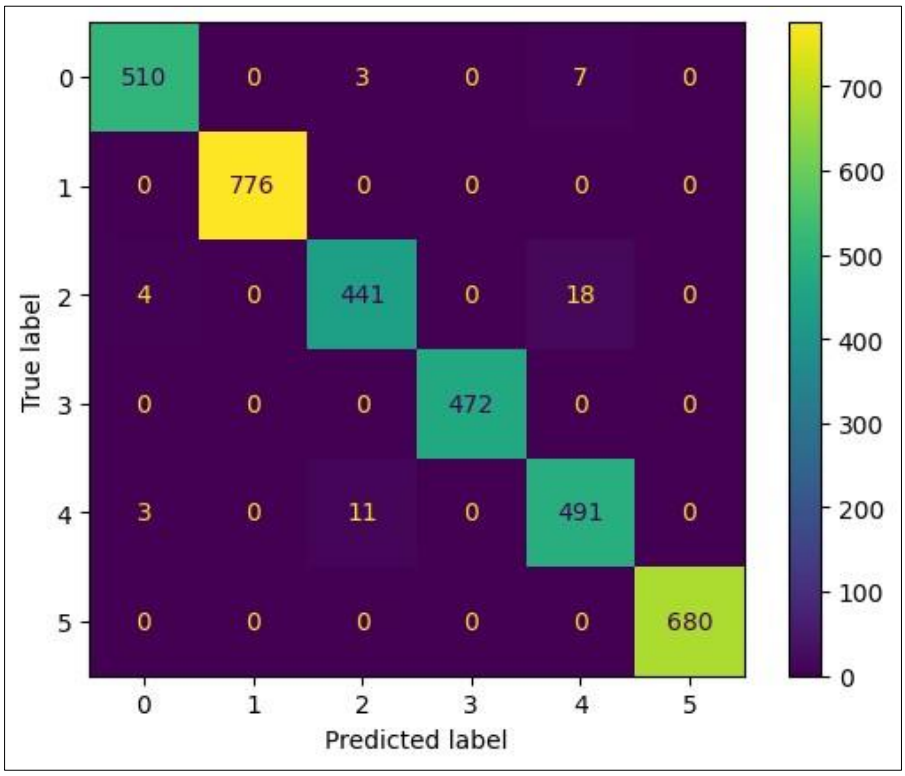
Şekil 12.1. PART modelinin test sonuçları

EK-13. DTa modeli ile elde edilen sonuçlar

	Precision	Recall	F-Measure
0	0,323	0,899	0,475
1	0,427	0,306	0,356
2	0,958	0,651	0,775
3	?	0,000	?
4	0,802	0,704	0,750
5	1,000	0,999	1,000
Weighted Avg.	?	0,594	?

Şekil 13.1. DTa modelinin test sonuçları

EK-14. DT modeli ile elde edilen sonuçlar

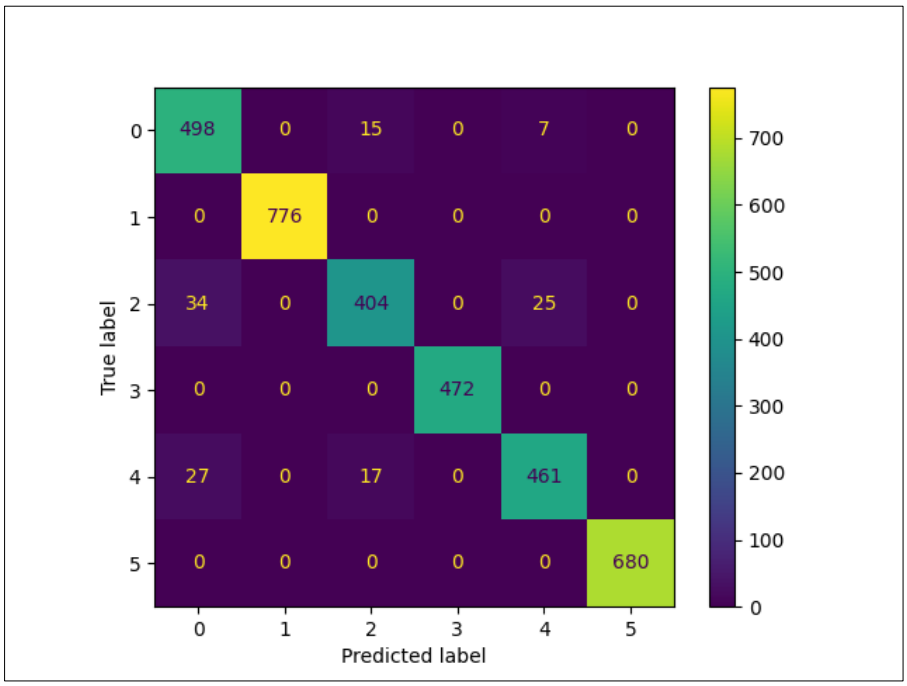


Şekil 14.1. DT modelinin karışıklık matrisi

	precision	recall	f1-score
0	0.99	0.98	0.98
1	1.00	1.00	1.00
2	0.97	0.95	0.96
3	1.00	1.00	1.00
4	0.95	0.97	0.96
5	1.00	1.00	1.00
micro avg	0.99	0.99	0.99
macro avg	0.98	0.98	0.98
weighted avg	0.99	0.99	0.99
samples avg	0.99	0.99	0.99

Şekil 14.2. DT modelinin test sonuçları

EK-15. RF modeli ile elde edilen sonuçlar



Şekil 15.1. RF modelinin karışıklık matrisi

	precision	recall	f1-score
0	0.94	0.93	0.93
1	1.00	1.00	1.00
2	0.93	0.87	0.90
3	1.00	1.00	1.00
4	0.94	0.91	0.92
5	1.00	1.00	1.00
micro avg	0.97	0.96	0.97
macro avg	0.97	0.95	0.96
weighted avg	0.97	0.96	0.97
samples avg	0.96	0.96	0.96

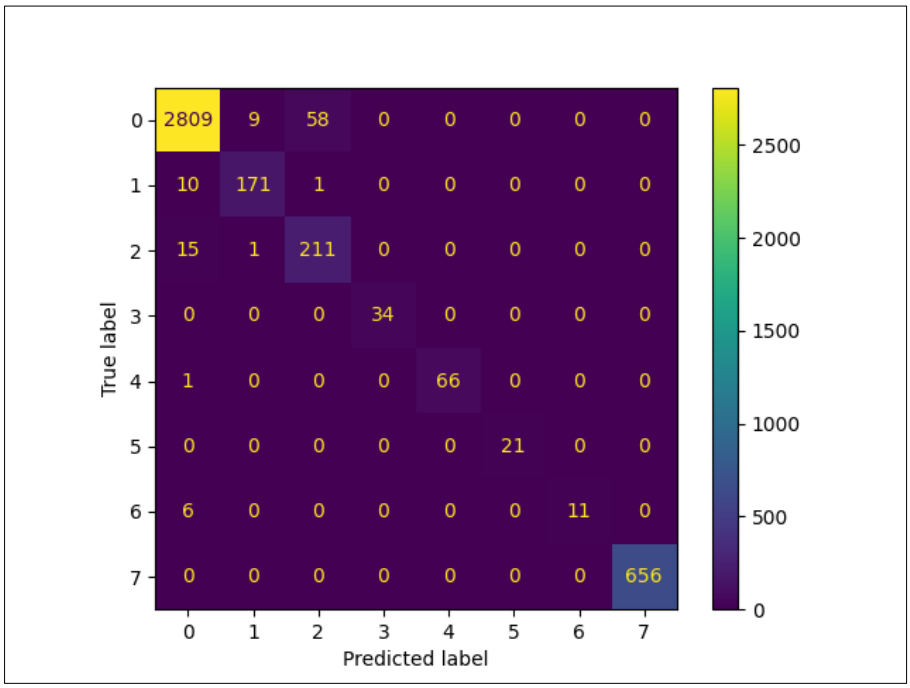
Şekil 15.2. RF modelinin test sonuçları

EK-16. RT modeli ile elde edilen sonuçlar

	Precision	Recall	F-Measure
0	0,647	0,868	0,742
1	0,850	1,000	0,919
2	0,916	0,579	0,710
3	1,000	0,783	0,878
4	0,954	0,561	0,706
5	0,812	0,999	0,896
Weighted Avg	0,857	0,831	0,824

Şekil 16.1. RT modelinin karışıklık matrisi

EK-17. HİBRİT3b modelinin farklı veri kümesi üzerindeki sonuçları



Şekil 17.1. HİBRİT3b modelinin farklı veri kümesindeki karışıklık matrisi

	precision	recall	f1-score
0	0.99	0.98	0.98
1	0.94	0.94	0.94
2	0.78	0.93	0.85
3	1.00	1.00	1.00
4	1.00	0.99	0.99
5	1.00	1.00	1.00
6	1.00	0.65	0.79
7	1.00	1.00	1.00
accuracy			0.98
macro avg	0.96	0.93	0.94
weighted avg	0.98	0.98	0.98

Şekil 17.2. HİBRİT3b modelinin farklı veri kümesindeki test sonuçları

2. Söğüt, E., Erdem, O. A. (2023). A Multi-Model Proposal for Classification and Detection of DDoS Attacks on SCADA Systems. *Applied Sciences*, 13(10), 5993.

3. Koçak, A., Söğüt, E., Alkan, M., Erdem, O. A. (2023). Detection of Different Windows PE Malware Using Machine Learning Methods. *Politeknik Dergisi*, 1, 1-1.

4. Söğüt, E. , Oyucu, S., Erdem, O. A. (2021). Detecting Different Types of Distributed Denial of Service Attacks. *Gazi University Journal of Science Part C: Design and Technology*, 9(1), 12-25.

5. Söğüt, E., Erdem, O. A. (2020). Endüstriyel kontrol sistemlerine (scada) yönelik siber terör saldırı analizi. *Politeknik Dergisi*, 23(2), 557-566.

6. Polat, H., Polat, O., Söğüt, E., Erdem, O. A. (2019). *Performance analysis of between software defined wireless network and mobile ad hoc network under dos attack*. The 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) (pp. 1-5). IEEE, Ankara, Türkiye.

7. Söğüt, E., Erdem, O. A. (2019). *Performance Comparison of the IEEE 802.15.4 Standard (ZigBee) Topologies*. The 8th International Conference on Advanced Technologies (ICAT'19), Sarajevo, Bosnia and Herzegovina, pp. 315-319.

8. Söğüt, E., Erdem, O. A. (2019). A review of research studies on cyber terror. Applying Methods of Scientific Inquiry Into Intelligence, Security, and Counterterrorism, 179-202. IGI Global.

9. Söğüt E., Erdem, O. A. (2017). *Early Diagnosis of Breast Cancer Using Data Mining And Machine Learning Methods.* The 3rd International Conference On Engineering and Natural Sciences (ICENS 2017), Budapest, Hungary, pp.163.

10. Söğüt, E., Oyucu, S., Erdem, O. A., Polat, H. (2017). *Recommendations for xDSL Technologies and Applications*. The 3rd International Conference on Engineering and Natural Sciences (ICENS 2017), Budapest, Hungary, pp.1166-1172.

11. Söğüt E., Erdem, O. A., Çetin, A. (2017). *Saldırı Tespit Sistemlerinde Ajan Sistemlerin Kullanımı - Using Agent system in intrusion detection system*. The X. International Conference on Information Security and Cryptology, Ankara, Türkiye, pp. 52-55.

12. Söğüt, E., Erdem, O. A. (2017). *Günümüzün vazgeçilmez sistemleri: nesnelerin haberleşmesi ve kullanılan teknolojiler*. Akademik Bilişim Konferansları (AB2017), Aksaray, Türkiye, pp.1-8, 2017.

Hobiler

Öykü Yazmak, Punch İşlemek, Yüzmek, Ebru Yapmak

Gazili olmak ayrıcalıktır