NESNELERİN İNTERNETİ TABANLI AĞ TRAFİĞİNDE İLERİ MAKİNE ÖĞRENİMİ VE DERİN ÖĞRENME YÖNTEMLERİ İLE ANOMALİ TESPİTİ

YÜKSEK LİSANS TEZİ

Yağız Onur KOLCU

Danışman
Dr. Öğr. Üyesi Ahmet Haşim YURTTAKAL

BİLGİSAYAR ANABİLİM DALI

Mayıs 2023

AFYON KOCATEPE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

NESNELERİN İNTERNETİ TABANLI AĞ TRAFİĞİNDE İLERİ MAKİNE ÖĞRENİMİ VE DERİN ÖĞRENME YÖNTEMLERİ İLE ANOMALİ TESPİTİ

Yağız Onur KOLCU

Danışman
Dr. Öğr. Üyesi Ahmet Haşim YURTTAKAL

BİLGİSAYAR ANABİLİM DALI

Mayıs 2023

TEZ ONAY SAYFASI

Yağız Onur KOLCU tarafından hazırlanan "Tez Onay Sayfası" adlı tez çalışması lisansüstü eğitim ve öğretim yönetmeliğinin ilgili maddeleri uyarınca 26 / 05 / 2023 tarihinde aşağıdaki jüri tarafından **oy birliği** ile Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü **Bilgisayar Anabilim Dalı'nda YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman **:** Dr. Öğr. Üyesi Ahmet Haşim YURTTAKAL

Başkan **:** Dr. Öğr. Üyesi Fahrettin HORASAN
Kırıkkale Üniversitesi, Mühendislik Fakültesi,
Bilgisayar Mühendisliği

Üye **:** Doç. Dr. Fatih ÖZDİNÇ
Afyon Kocatepe Üniversitesi, İktisadi İdari Bilimler Fakültesi,
Yönetim Bilişim Sistemleri

Üye **:** Dr. Öğr. Üyesi Ahmet Haşim YURTTAKAL
Afyon Kocatepe Üniversitesi, Mühendislik Fakültesi
Bilgisayar Mühendisliği

Afyon Kocatepe Üniversitesi
Fen Bilimleri Enstitüsü Yönetim Kurulu'nun
..... /..... /..... tarih ve
……. sayılı kararıyla onaylanmıştır.

…….
Prof. Dr. İbrahim EROL
Enstitü Müdürü

BİLİMSEL ETİK BİLDİRİM SAYFASI

Afyon Kocatepe Üniversitesi

Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- Görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- Başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- Atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- Kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- Ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

26 / 05 / 2023

Yağız Onur KOLCU

ÖZET

Yüksek Lisans Tezi

NESNELERİN İNTERNETİ TABANLI AĞ TRAFİĞİNDE İLERİ MAKİNE ÖĞRENİMİ VE DERİN ÖĞRENME YÖNTEMLERİ İLE ANOMALİ TESPİTİ

Yağız Onur KOLCU

Afyon Kocatepe Üniversitesi

Fen Bilimleri Enstitüsü

Bilgisayar Anabilim Dalı

Danışman: Dr. Öğr. Üyesi Ahmet Haşim YURTTAKAL

Nesnelerin İnterneti'nin (IoT) yaygınlaşması ve ağa bağlı cihaz sayısındaki hızlı artış hem faydaları hem de birçok sorunu beraberinde getiriyor. Bu sorunların en önemlisi siber saldırılardır. Bu siber saldırılar itibar ve zaman kaybının yanı sıra maddi kayıplara da neden olmaktadır. Bu kayıpları ortadan kaldırmak veya minimuma indirmek için saldırı tespit sistemleri (IDS) ve saldırı önleme sistemleri (IPS) kullanılmaktadır. IDS, imza tabanlı veya anormallik tabanlı olacak şekilde tasarlanmıştır ve şu anda makine öğrenimi yöntemleri olarak anomali tabanlı sistemler kullanılarak geliştirilmektedir. Bu çalışmanın amacı, botnet'i saldırı türlerinden biri olarak ele alarak, ağınıza yüksek başarı oranına sahip bir saldırı olup olmadığını tespit etmektir. Bu sistemin geliştirilmesi için makine öğrenmesi yöntemlerinden biri olan Kolektif Derin Sinir Ağı (DNN) kullanılarak en doğru sonuca yönelik çözüm yöntemlerinin araştırılması amaçlanmaktadır. Çalışmada bilimsel araştırma için UCI Machine Learning kütüphanesinde bulunan N-BaIoT veri seti kullanılmıştır. Veriler, 2 botnet tarafından taşınan 1 iyi huylu ağ akışı ve 9 kötü amaçlı ağ akışından oluşur. Sınıflandırma aşamasından itibaren CNN ağlarının kümelenmiş topluluğu kullanılmıştır. Önerilen yöntem %99 doğruluğa ulaşmış olup, sonuçlar gelecek çalışmalar için cesaret vericidir.

2023, viii + 85 sayfa

Anahtar Kelimeler: Nesnelerin interneti, Kolektif, Derin sinir ağları, Siber tehditler

ABSTRACT

M.Sc. Thesis

ANOMALY DETECTION IN INTERNET OF THINGS BASED NETWORK TRAFFIC WITH ADVANCED MACHINE LEARNING AND DEEP LEARNING METHODS

Yağız Onur KOLCU

Afyon Kocatepe University

Graduate School of Natural and Applied Sciences

Department of Computer

Supervisor: Asst. Prof. Ahmet Haşim YURTTAKAL

The widespread use of the Internet of Things (IoT) and the rapid increase in the number of devices connected to the network bring both benefits and many problems. The most important of these problems is cyber attacks. These cyber attacks cause financial losses as well as loss of reputation and time. Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are used to eliminate or minimize these losses. IDS are designed to be signature-based or anomaly-based, and are currently being developed using anomaly-based systems as machine learning methods. The aim of this study is to detect whether there is an attack on your network, with a high success rate, by considering botnet as one of the attack types. In order to develop this system, it is aimed to use Ensemble Deep Neural Networks (DNN), which is one of the machine learning methods, and to search for solution methods for the most accurate result. In the study, N-BaIoT dataset in the UCI Machine Learning library was used for scientific research. The data consists of 1 benign network stream and 9 malicious network streams carried by 2 botnets. Stacked ensemble of DNN networks has been used from the classification stage. The proposed method has achieved %99 accuracy and the results are encouraging for future studies.

2023, viii + 85 pages

Keywords: Botnet, Internet of things, Ensemble, Deep neural network, Cyber threats

TEŞEKKÜR

Bu araştırmanın konusu, deneysel çalışmaların yönlendirilmesi, sonuçların değerlendirilmesi ve yazımı aşamasında yapmış olduğu büyük katkılarından dolayı tez danışmanım Sayın Dr. Öğr. Üyesi Ahmet Haşim YURTTAKAL, araştırma ve yazım süresince yardımlarını esirgemeyen Sayın Dr. Berker BAYDAN'a her konuda öneri ve eleştirileriyle yardımlarını gördüğüm hocalarıma, arkadaşlarıma teşekkür ederim.

Bu araştırma boyunca maddi ve manevi desteklerinden dolayı aileme teşekkür ederim.

Yağız Onur KOLCU

Afyonkarahisar 2023

İÇİNDEKİLER DİZİNİ

Sayfa

ÖZET i
ABSTRACT ii
TEŞEKKÜR iii
İÇİNDEKİLER DİZİNİ iv
KISALTMALAR DİZİNİ vi
ÇİZELGELER DİZİNİ vii
RESİMLER DİZİNİ viii
1. GİRİŞ 1
1.1 Motivasyon 1
1.2 Tezin Organizasyonu 2
2. KURAMSAL TEMELLER 4
2.1 Yapay Zekâ 4
2.2 Makine Öğrenmesi 7
2.2.1 Denetimli Öğrenme 9
2.2.2 Denetimsiz Öğrenme 10
2.2.3 Takviyeli Öğrenme 11
2.3 Derin Öğrenme 12
2.3.1 Derin Sinir Ağları 14
2.3.2 Evrişimli Sinir Ağları 15
2.3.3 Yinelemeli Ağlar 17
2.3.4 Otomatik Kodlayıcı Sinir Ağı 18
2.3.5 Sinir Ağaçları 19
2.4 Kolektif Öğrenme 21
2.4.1 Torbalama 23
2.4.2 Yükseltme 25
2.4.3 Yığınlama 26
2.4.4 Oylama 27
2.5 Nesnelerin İnterneti 28
2.6 Ağ Saldırıları 30
2.6.1 DDOS 33
2.6.2 Fiziksel Saldırılar 36
2.6.3 Kimlik Avı 36

2.6.3 Saldırı Tespit Sistemleri 37
2.6.5 Botnet 38
2.7 Anomali Tespiti 43
3. LİTERATÜR BİLGİLERİ 45
4. MATERYAL ve METOT 56
4.1 Veri Kümesi 56
4.2 Önerilen Yöntem 57
5. BULGULAR 60
5.1 Performans Metrikleri 60
5.2 Performans Sonuçları 60
6. TARTIŞMA ve SONUÇ 65
7. KAYNAKLAR 68
ÖZGEÇMİŞ 85

KISALTMALAR DİZİNİ

Kısaltmalar	
AUC	Area Under the Curve (Eğri Altındaki Alan)
ASR	Automatic Speech Recognition (Otomatik Konuşma Tanıma)
C&C	Command and Control (Komut ve Kontrol)
CNN	Convolutional Neural Network (Evrişimli Sinir Ağı)
COVID-19	Coronavirus Disease (Koronavirüs Hastalığı)
DDoS	Distributed Denial of Service (Dağıtılmış Hizmet Reddi)
DNN	Deep Neural Network (Derin Sinir Ağı)
DoS	Denial of Service (Hizmet Reddi)
EA	Evolutionary Algorithm (Evrimsel Algoritma)
ECASP	Ensemble Classifier Algorithm with Stack Process (Yığın İşlemi ile Kolektif Sınıflandırıcı Algoritması)
ELBAD	Ensemble Learning Approach Based On Balanced Accuracy And Diversity (Dengeli Doğruluk ve Çeşitlilik Temelli Kolektif Öğrenme Yaklaşımı)
ELM	Extreme Learning Machine (Aşırı Öğrenme Makinesi)
ENN	Evolved Neural Network (Evrilen Sinir Ağı)
HTTP	Hypertext Transfer Protocol (Hipermetin Transfer Protokolü)
HTTPS	Hypertext Transfer Protocol Secure (Güvenli Hipermetin Transfer Protokolü)
IDS	Intrusion Detection System (Saldırı Tespit Sistemi)
IRC	Internet Relay Chat (İnternet Üzerinden Sohbet)
IP	Internet Protocol (İnternet Protokolü)
KNN	K-Nearest Neighbors Algorithm (K-En Yakın Komşu Algoritması)
LSTM	Long Short-Term Memory (Uzun Kısa Dönem Hafıza)
LOF	Local Outlier Factor (Yerel Aykırı Değer Faktörü)
MITM	Man in the Middle (Ortadaki Adam)
N-BaIoT	Ağ-based Internet of Things (Ağ Tabanlı Nesnelerin İnterneti)
NDT	Neural Decision Trees (Nöral Karar Ağaçları)
NIDS	National Institute for Discovery Science (Ulusal Keşif Bilimleri Enstitüsü)
NN	Neural Network (Sinir Ağı)
P2P	Peer to Peer (Eşten Eşe)
ROC	Receiver Operating Characteristic (Alıcı İşletim Karakteristiği)
SaaS	Software as a Service (Yazılım Hizmeti Olarak)
SSH	Secure Shell Protocol (Güvenli Kabuk Protokolü)
SQL	Structured Query Language (Yapılandırılmış Sorgu Dili)
SVM	Support Vector Machine (Destek Vektör Makinesi)
TPR	Total Physical Response (Toplam Fiziksel Tepki)
UCI	Unique Client Identifier (Benzersiz İstemci Tanımlayıcı)
UNIDS	Unsupervised Network Intrusion Detection System (Denetimsiz Ağ Saldırı Tespit Sistemi)
USB	Universal Serial Bus (Evrensel Seri Veri Yolu)

ÇİZELGELER DİZİNİ

Sayfa

Çizelge 4.1 Bütün Cihazların Trafik Dağılımı. 57

Çizelge 5.1.1 Karışıklık Matrisi. 60

Çizelge 5.1.2 Metriklerin Formülleri. 60

Çizelge 5.2 Performans Metrikleri. 63

RESİMLER DİZİNİ

Sayfa

Resim 2.1 Doğal Dil İşleme Uygulamaları 05
Resim 2.2.1 Makine Öğrenimi Süreci 07
Resim 2.2.2 Endüstride Makine Öğrenimi 09
Resim 2.3.1 Yapay Zekâ, Makine Öğrenimi ve Derin Öğrenme 12
Resim 2.3.2 Derin Sinir Ağı Katman Gösterimi 14
Resim 2.3.3 CNN Mimarisinin Nasıl Tasarlanacağını Gösteren textCNN Modeli 16
Resim 2.4.1 Kolektif Sınıflandırıcı 23
Resim 2.4.2 Bagging Tekniği 25
Resim 2.6.1 Siber Güvenlik Tehditleri 31
Resim 2.6.2 Başlıca Siber Güvenlik Tehditleri 33
Resim 2.6.3 DDoS Saldırısı 34
Resim 2.6.4 Botnet Nasıl Çalışır 40
Resim 4.2.1 Örnek DNN Mimarisi 58
Resim 4.2.2 Önerilen Model 58
Resim 5.2.1 Doğruluk - Epoch Grafiği 61
Resim 5.2.2 Test Seti Karışıklık Matrisi 62
Resim 5.2.3 ROC Eğrisi 64

1. GİRİŞ

1.1 Motivasyon

Nesnelerin İnterneti (IoT), fiziksel cihazların ve nesnelerin ağ yoluyla birbirine bağlanmasıdır (Elkhodr vd. 2013). En önemli faydası nesnelerin uzaktan algılanmasını ve kontrolünü sağlamasıdır. Ayrıca insan müdahalesini en aza indirerek ekonomi ve verimlilik sağlar. IoT, akıllı ev aletleri, su sayaçları, güvenlik kameraları gibi internete bağlı cihazlardan oluşmaktadır. Bu cihazlar, Linux cihazlar üzerinde çalışan işlemci ve IP adresli küçük bilgisayarlardır (Barrera vd. 2017). 2021 yılında en az 10 milyar aktif IoT cihazı bulunurken, 2030 yılında bu sayının 25,4 milyarı aşacağı tahmin edilmektedir (Huyghue 2021). IoT cihazları, operasyonları sırasında önemli miktarda veri üretir, işler ve değiştirir. IoT cihazları, iş kesintilerine, gizlilik ihlallerine ve hatta fiziksel yaralanmalara yol açabilecek çeşitli fiziksel, ağ ve uygulama katmanı saldırılarına eğilimlidir. Bu nedenle, güvenlik gereksinimleri, ürün yeniliği ile aynı öncelik düzeyine gelir (Skorin-Kapov vd. 2016). Çağımızın en büyük sorunu olan ağ güvenliği artık sadece bilgisayarlar için değil, internete bağlı her cihaz için büyük bir sorun haline geldi. Her gün milyonlarca yeni cihaz internete bağlanıyor. Ancak bu büyük gelişme büyük riskleri de beraberinde getiriyor. Her geçen gün siber suçlar hızla yayılmakta ve siber suçlular çeşitli saldırılar gerçekleştirmektedir (Gantz ve David 2012). Bu nedenle saldırı tespit sistemlerinin performansının arttırılması bilgi teknolojilerinin en önemli hedefleri arasındadır (Ahmetoğlu ve Daş 2019). Bot ağları, IoT güvenlik açıklarından en çok yararlanabilen tehditlerden biridir (Bezerra vd. 2019). Botnet, internete bağlı ve kötü amaçlı yazılım bulaşmış cihazların bir koleksiyonudur. Bu botlar, hizmet reddi ve çeşitli spam saldırıları için kullanılabilir (Bertino ve Islam 2017). Ayrıca, botlar yasa dışı kaynaklardan yanlış bilgi dağıtmayı, kimlik, şifre ve finansal verileri ele geçirmeyi ve ek ana bilgisayarlara erişim için şifreyi kırmak üzere verileri işlemeyi amaçlar. (Grizzard vd. 2007). Bu nedenle, botnet'lerin tespiti ve ortadan kaldırılması önemli siber güvenlik sorunlarıdır. Güvenilir ve ucuz Botnet tespit modelleri, iletim verilerini bozmadan riskleri tespit etmek ve uyarmak için gereklidir (Algelal vd. 2020). Bot ağlarının tespiti, kötü amaçlı yazılım tespit sistemlerinden veya anormallik tespit sistemlerinden farklıdır. Çünkü diğer saldırılar bireysel bir modeli temsil ederken, botnet saldırıları büyük bir saldırı ağının parçasıdır (Geer 2005). Yapay zekâ ve makine öğrenimi algoritmaları,

veriler üzerinde insan gözünün fark edemeyeceği karmaşık kalıpları öğrenerek hızlı, doğru, insandan bağımsız sonuçlar sağlar (El Naqa ve Murphy 2015). Son yıllarda donanım ve işlem kapasitesi teknolojisindeki gelişmelerle birlikte makine öğrenmesi ve yapay zekâ algoritmaları ağ güvenliği çalışmalarını daha başarılı kılmaktadır (Lu 2019). Stevanovic ve Pedersen (2016), botnet tanımlama çalışmalarında yapay sinir ağları gibi denetimli öğrenme yöntemlerini ve hiyerarşik kümeleme gibi denetimsiz öğrenme yöntemlerini vurgulamıştır (Stevanovic ve Pedersen 2016). Verma ve Ranga (2020), kolektif yöntemlerinin IoT ağlarındaki Hizmet Reddi (DoS) saldırılarını tespit etmede başarılı olduğunu buldu (Verma ve Ranga 2020). Altunay ve Albayrak (2021), siber saldırıları önlemek için Evrişimli Sinir Ağları (CNN) kullanarak özellik seçimine dayalı bir saldırı tespit uygulaması gerçekleştirmiştir. Verileri tehdit olarak algılama başarısı Brute Force için %98,7, DoS için %98,5, Botnet için %98,9 ve SQL Injection için %99,1 olmuştur (Altunay ve Albayrak 2021).

Nesnelerin İnterneti (IoT), fiziksel cihazların, araçların ve nesnelerin internet üzerinden bağlantı kurma ve veri alışverişi yapma biçiminde devrim yarattı. Verimlilik, üretkenlik ve rahatlık açısından dikkate değer faydalar sunarken, IoT cihazlarının yaygın kullanımı aynı zamanda önemli güvenlik sorunları da doğurmaktadır. Kullanıcı verilerini korumak, sistem bütünlüğünü sürdürmek ve potansiyel riskleri azaltmak için bu endişelerin ele alınması son derece önemlidir. Anomali tespiti, IoT cihazları alanında, güvenlik ihlallerine işaret edebilecek anormal kalıpları veya davranışları tanımlayabilen güçlü bir güvenlik yaklaşımı olarak ortaya çıkıyor. Kuruluşlar ve bireyler, anomali algılama yöntemlerini birleştirerek IoT cihazlarının güvenliğini güçlendirebilir ve gelişen siber tehditler karşısında verilerinin güvenliğini ve gizliliğini sağlayabilir. Bu çalışmada IoT cihazlarına yönelik botnet saldırılarının tespiti kolektif derin sinir ağı ile sınıflandırılmıştır. 2 botnet saldırısına ait 1 iyi huylu ve 9 zararlı olmak üzere 10 farklı IoT cihazının ağ trafikleri %99 doğrulukla sınıflandırıldı. Önerilen yöntem hızlı, güvenli ve yüksek doğrulukla otomatiktir.

1.2 Tezin Organizasyonu

Çalışmanın ikinci bölümü, literatürde yer alan akademik çalışmaların kapsamlı bir incelemesini içermektedir. Materyal metot kısmında yapay zekâ, makine öğrenmesi,

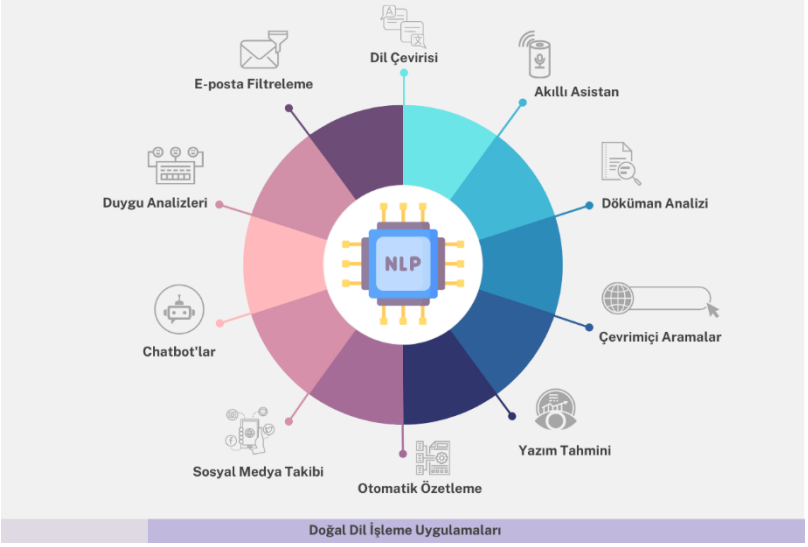
derin öğrenme gibi kavramların matematiksel alt yapıları verilmiştir. Bu bölümde ayrıca siber güvenlik ve botnet anlatılarak saldırı türlerine kapsamlı bir şekilde değinilmiştir. Dördüncü bölüm, önerdiğimiz yaklaşımın katmanlarını, karmaşıklığını, hiper parametrelerini ve modelin performansını değerlendirir. Son olarak tartışma ve sonuç kısmında önerilerin üzerinde yoğunlaşılmış ve bu şekilde tez çalışması sonlandırılmıştır.

2. KURAMSAL TEMELLER

2.1 Yapay Zekâ

Yapay zekâ (YZ), bilgisayarların ve diğer makinelerin insan benzeri düşünme, öğrenme ve problem çözme yeteneklerine sahip olmasını sağlayan bilim ve teknoloji dalıdır (Chintawar vd. 2023). Yapay zekâ, insanın doğal zekasından ilham alan ve insan beyninin karmaşıklığını ve çevikliğini taklit etmeye çalışan teknoloji alanıdır. Bu bilim dalı, insan gibi düşünen ve hareket eden makineler yaratmak için algoritmalar ve matematiksel modeller kullanarak makinelerin bilişsel yeteneklerini geliştirmeyi amaçlar. İnsan zekasının benzersiz özelliklerini taklit etmeyi amaçlayan bu alan, yazılım ve algoritmaların yardımıyla makinelerin karmaşık görevleri başarılı bir şekilde yerine getirmesini hedefler.

Yapay zekâ çalışmaları, bilgisayarların ve makinelerin çeşitli yeteneklere sahip olmasını sağlar; örneğin, dildeki anlam ve bağlamı anlama, görsel nesneleri tanıma ve insanlara yardımcı olacak şekilde kararlar verme gibi. Bu amaçla, yapay zekâ teknolojisi, insan zekasının özelliklerini anlamak ve modellemek için farklı disiplinlerden yararlanır, örneğin; psikoloji, felsefe, dil bilimi ve nörobilim. Doğal dil işleme, yapay zekâ teknolojisinin önemli bir bileşeni olarak, makinelerin insan dilini anlamasını ve doğru bir şekilde işlemesini sağlar (Young vd. 2018). Bu teknoloji, müşteri hizmetleri, otomatik çeviri ve bilgi edinme gibi pek çok alanda kullanılmaktadır. Yapay zekâ uygulamalarının başarısı, büyük ölçüde öğrenme yeteneklerine dayanır. Burada ön plana çıkan unsurlar; gözetimli öğrenme, gözetimsiz öğrenme ve pekiştirmeli öğrenme gibi farklı öğrenme yöntemleridir. Bu yöntemler, makinelerin deneyimlerinden ve verilerden öğrenerek, belirli görevlerde daha başarılı ve etkili hale gelmesini sağlar. Resim 2.1 de birçok alanda bulunan doğal dil işlemenin uygulama alanları görülmektedir



Resim 2.1 Doğal Dil İşleme Uygulamaları.

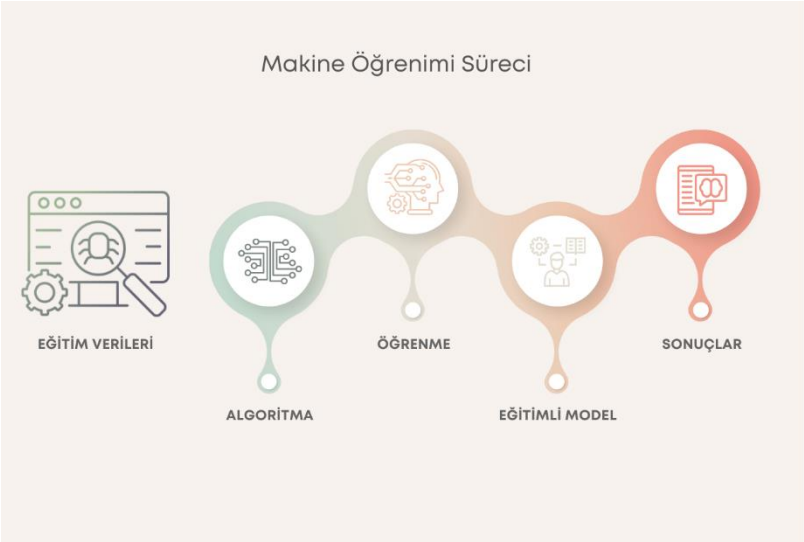
Doğal dil işleme uygulama alanlarının artması ile günümüzde yapay zekâ teknolojisi hızla gelişiyor ve günlük hayatımızda giderek daha fazla yer kaplıyor. Kişisel asistanlardan akıllı ev sistemlerine, tıbbi teşhisten mali analizlere kadar yapay zekâ uygulamaları insan hayatını kolaylaştırmak ve verimliliği artırmak için kullanılıyor. Yapay zekâ, tıbbi görüntüleme ve teşhis süreçlerinde önemli gelişmelere yol açarak, hastaların daha doğru ve hızlı tedavi almasına imkân tanımaktadır. Bu çalışmalar sayesinde, teşhis süreçlerinin maliyet ve zaman açısından verimliliği artmaktadır. Yapay zekâ, sağlık sektöründe tıbbi teşhis ve tedavi süreçlerini iyileştirmekte önemli bir rol oynamaktadır. Gelişmiş algoritmalar ve büyük veri analizi sayesinde, hastalıkların erken teşhisi ve uygun tedavi yöntemlerinin belirlenmesi daha hızlı ve doğru bir şekilde gerçekleştirilmektedir. Derin öğrenme, büyük veri kümelerinden özellik çıkarımı yaparak, görüntü ve ses işleme gibi alanlarda önemli başarılar elde etmiştir (LeCun vd. 2015). Bu sayede, makineler insanlar gibi algılayarak ve öğrenerek karmaşık problemleri çözme becerisi kazanmaktadır. Yapay zekâ ve makine öğrenimi yöntemleri, finans ve yatırım sektöründe risk analizi ve tahminlerde bulunma konusunda önemli gelişmelere yol açmaktadır. Finans sektöründe yapay zekâ, algoritmik ticaret ve risk analizi gibi alanlarda büyük veriyi analiz ederek, yatırımcılara daha iyi kararlar alabilecekleri bilgiler sağlamaktadır (Dhar 2016). Bu durum, finansal piyasaların daha etkin ve verimli çalışmasına katkıda bulunmaktadır. Otomotiv sektöründe, yapay zekâ ve otonom sürüş teknolojileri, sürüş deneyimini daha güvenli ve konforlu hale getirme potansiyeline sahiptir. Otonom sürüş teknolojilerinde

yapay zekâ, güvenli ve etkili bir sürüş deneyimi sunarak, ulaşım sektörünün geleceğini şekillendirmektedir (Milanes vd. 2014). Bu teknoloji sayesinde, trafik kazalarının azaltılması ve enerji tüketiminin optimize edilmesi hedeflenmektedir. Yapay zekâ destekli enerji yönetimi sistemleri, enerji tüketiminin optimize edilmesi ve kaynakların daha verimli kullanılması için enerji sektöründe önemli bir rol oynamaktadır (Zheng vd. 2018). Bu sistemler, enerji verimliliğini artırarak sürdürülebilir enerji hedeflerine ulaşmayı kolaylaştırmaktadır. Akıllı şebekeler ve enerji yönetimi sistemleri ile enerji tüketiminin optimize edilmesi ve kaynakların daha verimli kullanılması, sürdürülebilir bir enerji geleceği için önemli adımlar olarak görülmektedir. Otomotiv sektöründen tıbba, eğitimden finansa kadar pek çok sektörde, yapay zekâ uygulamaları sayesinde önemli başarılar elde edilmiştir.

Yapay zekâ uygulamaları, farklı öğrenme yöntemleri ve disiplinlerle desteklenerek, günlük yaşamımıza ve iş dünyasına entegre olmaktadır. Bu sayede, yaşam kalitemizi arttırmak ve geleceğin şekillenmesinde önemli roller üstlenmektedir. Şehir planlaması ve yönetiminde şehirlerin daha yaşanabilir ve sürdürülebilir hale gelmesine katkı sağlamaktadır (Batty vd. 2012). Ulaşım, enerji, su ve atık yönetimi gibi alanlarda yapılan analizlerle, şehirlerin altyapısının iyileştirilmesi ve doğal kaynakların daha etkin kullanılması hedeflenmektedir. Özellikle makine öğrenimi ve derin öğrenme yöntemleri sayesinde, makinelerin büyük veri kümelerinden öğrenmesi ve bu bilgileri yeni durumlara uygulaması mümkün hale gelmiştir. Yapay zekâ algoritmaları, özellikle derin öğrenme, bilgisayarların açıkça programlanmadan öğrenmelerini sağlayarak görüntü tanıma görevlerinde kayda değer bir ilerleme kaydetmiştir (Chintawar vd. 2023, Surden 2019). Gelişen yapay zekâ, derin öğrenme ve sinir ağları kullanarak, görüntü işleme ve doğal dil işleme gibi alanlarda önemli başarılar elde etmeye devam etmektedir. Bu başarılar, yapay zekanın günlük yaşamımızda daha fazla yer almasına ve farklı sektörlerde etkin çözümler sunmasına olanak sağlamaktadır. Günümüzde yapay zekâ, sürekli gelişen bir alan olarak karşımıza çıkmaktadır. Özellikle büyük teknoloji şirketleri, yapay zekâ üzerine yaptıkları yatırımlar ve araştırmalarla bu alanda önemli adımlar atmaktadır. Bu kapsamda, dil anlama, görüntü tanıma ve doğal dil işleme gibi alanlarda yapılan çalışmalar, yapay zekanın günlük hayatımızda daha fazla yer almasını sağlamaktadır.

2.2 Makine Öğrenmesi

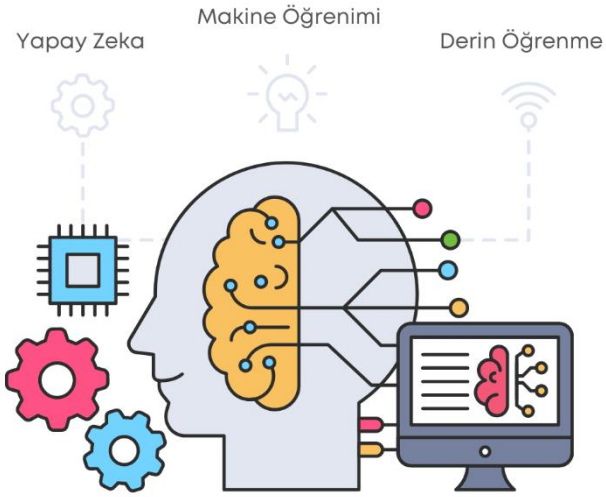
Makine öğrenimi, bilgisayarların insan müdahalesi olmaksızın tecrübe ve veriyle öğrenme yeteneği geliştiren bir yapay zekâ dalıdır. Temel amacı, algoritmaların ve modellerin veri üzerinde eğitilerek daha önce karşılaşmadıkları durumlar için tahminlerde bulunmalarını sağlamaktır. Makine öğrenimi, geçmiş verilerden öğrenebilen, kalıpları tanıyabilen ve bu verilere dayalı olarak mantıksal kararlar verebilen sistemler oluşturmaya odaklanan yapay zekanın bir alt kümesidir. Basit bir ifadeyle, makine öğrenimi, bilgisayarlara açıkça programlanmadan verilerden öğrenmeyi öğretme yöntemidir. Verilerdeki kalıpları otomatik olarak tanıyabilen ve daha sonra bu kalıpları tahminler veya kararlar vermek için kullanan algoritmalar geliştirmeyi içerir. Makine öğrenimi, verileri analiz ederek öğrenen ve bu öğrenmeyi, gelecekteki kararlar ve tahminler için kullanabilen algoritmaların geliştirilmesine odaklanan bir yapay zekâ alanıdır (Goodfellow vd. 2016). Bu alanda çalışan araştırmacılar, sürekli gelişen veri kümeleri ve teknolojiler ile başarılarına devam etmektedirler. Makine öğrenimi, özellikle büyük verilerin patlamasıyla günümüz dünyasında giderek daha önemli hale gelmektedir. Her gün çok büyük miktarda veri üretilirken, bu verileri analiz etmek ve anlamlandırmak için makine öğrenimi algoritmaları önem arz etmektedir. Makine öğreniminin sağlık, finans, pazarlama vb. gibi çeşitli alanlarda çok sayıda uygulaması bulunmaktadır.



Resim 2.2.1 Makine Öğrenimi Süreci.

Makine öğreniminin başlıca üç yöntemi vardır: gözetimli öğrenme, gözetimsiz öğrenme ve takviyeli öğrenme (Sutton vd. 2018). Resim 2.2.1 de bulunan süreçler ele alındığında bu yöntemler, farklı türde veri ve öğrenme görevleri için uygulanarak, algoritmaların başarılarını artırmaya yönelik çalışmaların temelini oluşturmaktadır. Denetimli öğrenmede bir algoritma, girdileri ve çıktıları ile birlikte kendisine sağlanan eğitim verilerinden öğrenir. Bu veriler, gelecekteki algoritmik tahminler için bir kılavuz olarak kullanılır. Bu tür makine öğrenimi, görüntü tanıma veya spam filtreleme gibi sınıflandırma görevleri için kullanılır (Bhowmick ve Hazarika 2016). Denetimsiz öğrenmede, yapısal özellikleri ve girdi verileriyle ilişkileri keşfetmek için bir algoritma eğitilir. Denetimsiz öğrenme algoritmaları, sınıflandırma ve kümeleme gibi veri madenciliği uygulamalarında yaygın olarak kullanılmaktadır. Takviyeli öğrenme, çevre ile etkileşime girerek ve geri bildirim alarak öğrenen algoritmalara dayanır. Bu geri bildirim genellikle ödüller ve cezalar şeklinde gelir.

Son yıllarda, derin öğrenme olarak adlandırılan makine öğreniminin bir alt dalı büyük ilgi görmüştür. Derin öğrenme, sinir ağlarının karmaşık yapılarından yararlanarak, veriden özellik çıkarımı ve öğrenme süreçlerini daha etkin hale getirmeyi amaçlar. Özellikle büyük veri kümelerinde ve görsel ve işitsel veri analizinde derin öğrenme yöntemleri önemli başarılar elde etmiştir. Derin öğrenme, makine öğrenimi alanının önemli bir alt dalıdır ve büyük veri kümelerinde, görsel ve işitsel veri analizinde önemli başarılar elde etmektedir (LeCun vd. 2015). Bu yöntem, karmaşık sinir ağları kullanarak, özellik çıkarımı ve öğrenme süreçlerini daha etkin hale getirmeyi amaçlar.



Resim 2.2.2 Endüstride Makine Öğrenimi.

Makine öğrenimi, teknolojinin hızla geliştiği günümüz dünyasında, pek çok endüstride ve sektörde verimlilik ve doğruluğun artırılması için kullanılmaktadır. Finans alanında, makine öğrenimi algoritmaları, yatırım kararlarına yardımcı olmak için piyasa verilerini analiz eder ve potansiyel riskleri belirlemeye çalışır. Bu sayede, yatırımcılar daha bilinçli ve doğru kararlar alabilirler.

2.2.1 Denetimli Öğrenme

Denetimli öğrenme, etiketli giriş ve çıkış verileri kullanılarak bir algoritmanın eğitildiği bir makine öğrenimi türüdür. Denetimli öğrenme, etiketli veri kümeleri üzerinde çalışarak, örüntüleri ve ilişkileri keşfeden algoritmaların geliştirildiği bir makine öğrenimi yöntemidir (Kotsiantis vd. 2007). Bu yöntem, çeşitli uygulamalar için doğru tahminler yapabilen modellerin oluşturulmasına olanak tanır. Başka bir deyişle, algoritmaya bilinen sonuçları olan bir dizi veri verilir ve etiketli eğitim verilerine dayalı olarak yeni veriler üzerinde tahminler yapmayı öğrenir. Bu tür bir öğrenme, istenen çıktı bilindiğinde ve algoritma, girdi verilerine dayalı olarak doğru tahminler yapmak üzere eğitilebildiğinde kullanışlıdır. Denetimli öğrenme genellikle, amacın bir girdi verilen bir sınıf etiketini tahmin etmek olduğu sınıflandırma problemlerinde kullanılır (Jadhav ve Channe 2016). Destek vektör makineleri (SVM), lojistik regresyon, Naive Bayes ve sinir ağları dahil olmak üzere denetimli öğrenmede çeşitli algoritmalar kullanılır. Destek

vektör makineleri (SVM), denetimli öğrenme algoritmaları arasında popüler ve başarılı bir yöntemdir ve sınıflandırma ve regresyon problemlerinde kullanılabilir (Cortes ve Vapnik 1995). SVM, genellikle yüksek doğruluk oranları ve düşük hata payları ile sonuçlar üretir. Bu algoritmalar, gerçek dünya senaryolarında doğru tahminler yapabilen modelleri eğitmek için kullanılır. Örneğin, denetimli öğrenme, konuşma tanıma, görüntü tanıma ve öneri sistemleri gibi uygulamalarda kullanılabilir. Denetimli öğrenmeye başka bir örnek, amacın bir metin verilen bir sınıf etiketini tahmin etmek olduğu metin sınıflandırmasıdır (Muhammad ve Yan 2015). Denetimli öğrenme, dolandırıcılık tespiti, kötü amaçlı yazılım tespiti ve veri girişi sırasında insan hatalarını belirleme dahil ancak bunlarla sınırlı olmamak üzere birçok pratik uygulamaya sahiptir (Dua ve Bais 2014).

2.2.2 Denetimsiz Öğrenme

Denetimli öğrenme, etiketli giriş ve çıkış verileri kullanılarak bir algoritmanın eğitildiği bir makine öğrenimi türüdür. Başka bir deyişle, algoritmaya bilinen sonuçları olan bir dizi veri verilir ve etiketli eğitim verilerine dayalı olarak yeni veriler üzerinde tahminler yapmayı öğrenir. Bu tür bir öğrenme, istenen çıktı bilindiğinde ve algoritma, girdi verilerine dayalı olarak doğru tahminler yapmak üzere eğitilebildiğinde kullanışlıdır. Denetimli öğrenme ile karşılaştırıldığında, denetimsiz öğrenme, veriye önceden atanmış etiketler veya kategoriler olmaksızın çalışır. Bu nedenle, denetimsiz öğrenme algoritmalarının amacı, verinin doğal gruplamalarını ve ilişkilerini öğrenerek, verinin içindeki özelliklerini ortaya çıkarmaktır. Denetimsiz öğrenme yöntemlerinin temel özellikleri arasında, veri kümesindeki benzerlikleri ve farklılıkları belirleyerek veriyi analiz etme ve verinin karmaşıklığını azaltarak daha anlaşılır hale getirme yer alır. Kümeleme ve boyut indirgeme, denetimsiz öğrenme algoritmalarının iki temel kategorisidir. Kümeleme, veriyi benzer özelliklere göre gruplara ayırmayı amaçlarken, boyut indirgeme, verinin temel özelliklerini koruyarak daha düşük boyutlu bir temsile sıkıştırır. Kümeleme, denetimsiz öğrenme algoritmaları arasında yaygın olarak kullanılan bir yöntemdir ve veriyi benzer özelliklere göre gruplara ayırmayı amaçlar (Jain 2010). Bu yöntem, veri madenciliği ve analizi gibi alanlarda önemli bir rol oynamaktadır. Denetimsiz öğrenme, makine öğreniminin önemli ve kullanışlı bir yöntemidir. Öz öğrenme (autoencoder) algoritmaları, denetimsiz öğrenme algoritmalarının başarılı bir

örneğidir ve veriyi daha düşük boyutlu bir temsile sıkıştırarak, daha sonra bu temsili kullanarak orijinal veriyi yeniden oluşturmayı amaçlar (Bengio vd. 2013). Bu teknik, veri sıkıştırma ve gürültü azaltma gibi uygulamalarda kullanılabilir. Etiketlenmemiş veri kümeleri üzerinde çalışarak, veri içindeki yapıları ve örüntüleri keşfeder ve bu sayede veriyi daha anlaşılır ve işlenebilir hale getirir. Günümüzde, denetimsiz öğrenme algoritmaları, çeşitli uygulama alanlarında başarı sağlamakta ve verinin doğal özelliklerini ve gruplamalarını ortaya çıkarmaya yardımcı olmaktadır.

2.2.3 Takviyeli Öğrenme

Takviyeli öğrenme, ajanlar adı verilen yapay zekâ unsurlarının etkileşimli ortamlarda optimal kararlar vererek performanslarını en üst düzeye çıkarmayı hedefleyen bir öğrenme yaklaşımıdır. Çeşitli alanlarda popülerlik kazanan güçlü bir öğrenme çerçevesidir. Bir aracının bir ortamda nasıl karar vereceğini deneme yanılma yoluyla öğrendiği Markov karar süreçlerine dayalı makine öğreniminin bir alt alanıdır. Bu süreçte, ajanlar deneyimlerinden ve alınan geri bildirimlerden yararlanarak, zaman içinde ödül sinyallerini maksimize eden eylemleri belirlerler (Zhou vd. 2017). Takviyeli öğrenme, belirli bir eylem için beklenen uzun vadeli ödülü tahmin etmek için bir değer fonksiyonu kullanmayı içermesinin yanı sıra (Zhou vd. 2017) yüksek boyutlu sistemlere uygulanabilen politika gradyan yöntemlerinin kayda değer istisnası dışında, model tabanlı veya modelsiz öğrenme olarak sınıflandırıldığı bilinmektedir (Zhou vd. 2017, Peters ve Schaal 2008). Bu, sürekli keşif ve deneme-yanılma yoluyla gerçekleştirilir. Takviyeli öğrenme, basit kontrol görevlerinden motor beceriler ve hareketler gibi birçok serbestlik derecesine sahip karmaşık öğrenme görevlerine kadar çeşitli alanlarda da uygulanabilir (Peters ve Schaal 2008).

Takviyeli öğrenme topluluğu tarafından önerilen yöntemlerin çoğu insansı robotlar gibi yüksek boyutlu sistemler için uygun olmasa da takviyeli öğrenme alanı hızla genişlemekte ve çeşitli alanlarda kullanılmaktadır (Kiran vd. 2021, Peters ve Schaal 2008). Takviyeli öğrenme, özellikle dinamik ve karmaşık problemlerin çözümünde, öğrenen sistemlerin uyum sağlama ve stratejilerini geliştirme yeteneği açısından büyük bir avantaj sunar.

2.3 Derin Öğrenme

Derin öğrenme, temsili öğrenme ile yapay sinir ağlarını kullanan bir tür makine öğrenimi ve yapay zekadır. Bu sinir ağları, kalıpları tanımak ve insanlara benzer sonuçlar çıkarmak için tasarlanmış algoritma katmanlarıdır. Karmaşık sorunları modellemek ve çözmek için yapay sinir ağlarını kullanan, hızla büyüyen bir makine öğrenimi alanıdır.

Resim 2.3.1 Yapay Zekâ, Makine Öğrenimi ve Derin Öğrenme.

Derin öğrenme üçten fazla katman içerir (giriş, çıkış ve gizli katmanlar) ve nöron sayısına bağlı bir doğrulukla rastgele bir işlevi yaklaşık olarak tahmin edebilir (Nakaura vd. 2020). Bu, daha doğru tahminler ve kararlar verebilen daha karmaşık modellerin geliştirilmesine olanak tanır. Derin öğrenme, geleneksel makine öğrenimi algoritmalarına kıyasla büyük ölçekli, gürültülü ve yapılandırılmamış verilerle başa çıkmada daha iyidir (Janiesch vd. 2021). Algoritma verilerini tarayabilir ve manuel özellik geliştirmeye gerek kalmadan ilgili özellikleri kendi başına belirleyebilir. Derin öğrenme algoritmaları, otomatikleştirilmiş özellik öğrenmeyi kullanarak el işi özellik mühendisliğinin sınırlamalarının üstesinden gelerek, verileri artan soyutlamanın birden çok katmanında temsil etmeyi otomatik olarak öğrenebilir (Janiesch vd. 2021, Bini 2018). Derin öğrenme, uyarlanabilir test, görüntü sınıflandırma, doğal dil işleme, nesne algılama ve daha fazlası için iş, bilim ve devlet alanlarında yaygın olarak kullanılmaktadır (Dargan vd. 2020).

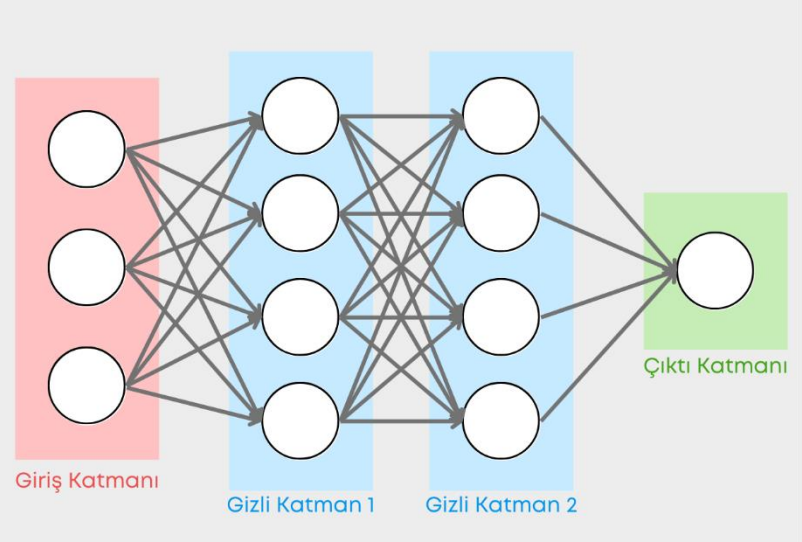
Derin öğrenmenin en önemli özelliklerinden biri resim, metin ve müzik gibi çok karmaşık verileri işleme yeteneğidir (Nakaura vd. 2020). Bununla birlikte, derin öğrenme algoritmaları, geleneksel makine öğrenimi algoritmalarına kıyasla daha karmaşıktır ve daha fazla veri ve hesaplama gücü gerektirir (Janiesch vd. 2021). Özetle, derin öğrenme, verilerin hiyerarşik temsillerini öğrenmek için çok katmanlı sinir ağlarını eğitmeyi içeren bir makine öğrenimi alt kümesidir ve çok karmaşık verileri işleme yeteneği ve derin katmanları kullanma becerisi açısından geleneksel makine öğrenimi algoritmalarından farklıdır. Derin öğrenme algoritmalarının çok yönlülüğü, onları çok çeşitli uygulamalar için uygun hale getirir ve büyük miktarda veriden öğrenme yetenekleri, onları özellikle veri açısından zengin alanlarda kullanışlı kılar (Butt vd. 2020). Derin öğrenme, en iyi özellikleri otomatik olarak öğrenen ve temsil eden güçlü bir yaklaşımdır. Önceki katmandan gelen girdi verilerini işleyen yapay nöron katmanlarından oluşan derin sinir ağları aracılığıyla gerçekleştirilir. İlk katmanlar, girdi verilerinin basit bir şekilde işlenmesini gerçekleştirirken, üst katmanlar karmaşık özellik öğrenmeyi gerçekleştirir (Sharma vd. 2021). Derin modeller, büyük ölçüde aşırı parametrelenmiştir (Belkin vd. 2018), bu da onların daha büyük verileri ve karmaşıklığı ele almalarını sağlar. Derin öğrenmedeki temel zorluk, modellerin eğitim verilerine tam olarak uyma eğiliminde olduğu ve test verilerinde zayıf genelleme performansına yol açan bir fenomen olan aşırı uyumdur (Belkin vd. 2018). Bununla birlikte, fazla uydurmaya rağmen, derin modeller test verilerinde iyi performans gösterir. Genelleme, optimizasyon sürecinden ziyade çekirdek fonksiyonunun özelliklerine bağlıdır (Belkin vd. 2018). Otomatik özellik öğrenme süreci, derin öğrenmeyi sağlam kılar ve evrişimli sinir ağları, tekrarlayan ağlar, çekişmeli ağlar ve otomatik kodlayıcılar gibi çeşitli derin sinir ağları türleri ile genelleştirilmiş bir yaklaşımdır (Ghosh vd. 2019). Derin öğrenme, önemli bir etkiye sahip olduğu görüntü bölümleme alanı da dahil olmak üzere gelecekte dikkate değer sonuçlar üretebilecek çeşitli uygulamalara sahiptir. Bununla birlikte, araştırma sürekli bir süreçtir ve gelecekte yeni mimariler gelişebilir (Sharma vd. 2021).

Derin öğrenme, bilgisayarla görme, doğal dil işleme ve konuşma tanıma gibi birçok alanda giderek daha popüler bir teknik haline geldi. Bilgisayar görüşünde derin öğrenmenin dikkate değer bir uygulaması, son yıllarda araştırmaların ana odak noktası

haline gelen tıbbi görüntülemedir (Esteva vd. 2019). Doğal dil işlemede, duygu analizi, dil çevirisi ve chatbot geliştirme gibi görevler için derin öğrenme kullanılır (Deng ve Liu 2018). Kelime gömme ve tekrarlayan sinir ağları, doğal dil işlemede kullanılan iki güçlü öğrenme modelidir (Yang vd. 2019). Derin öğrenmenin kullanımı, büyük verinin özelliklerini otomatik ve verimli bir şekilde yakalayarak, doğal dil işlemede çok başarılı olmuştur (Chai vd. 2021). Derin öğrenmenin kullanımı bu alanlarda devrim yaratmış ve yapay zekâ ve bilgisayar bilimlerinde önemli bir araştırma alanı haline gelmiştir (Yang vd. 2019).

2.3.1 Derin Sinir Ağları

Bir sinir ağı, insan beynine benzer hiyerarşik bir yapıda birbirine bağlı düğümleri veya nöronları kullanan bir makine öğrenme sürecidir. Bu sürece derin öğrenme denir ve karmaşık matematiksel modelleri kullanarak verileri karmaşık şekillerde işleyebilir (Hoyal Cuthill vd. 2019). Girdi ve çıktıdan oluşan ikiden fazla katmana sahip bir sinir ağı, derin öğrenme algoritması olarak kabul edilebilir. En basit haliyle, bir sinir ağının yalnızca iki katmanı vardır; bir giriş katmanı ve bir çıkış katmanı. Bununla birlikte, derin sinir ağları, daha yaygın olan tek gizli katmanlı sinir ağlarından farklıdır çünkü derinlikleri, daha karmaşık verileri işlemelerine izin verir (Peng vd. 2021).



Resim 2.3.2 Derin Sinir Ağı Katman Gösterimi.

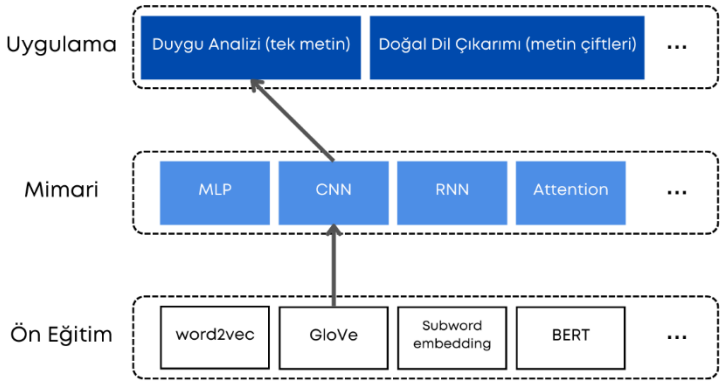
Sinir ağlarının gelişimi, derin öğrenmenin gelişiminde önemli bir itici faktör olmuştur.

(Schmidhuber 2015). O zamandan beri, evrişimli sinir ağları (CNN'ler) ve derin inanç ağları (DBN'ler) dahil olmak üzere sinir ağı mimarilerinde birçok ilerleme kaydedildi. Evrimsel sinir ağı (ENN), evrimsel algoritmanın (EA) uyarlanabilir mekanizmasını sinir ağı yapısıyla birleştiren uyarlanabilir bir yöntemdir (Ma ve Xie 2022, Miikkulainen vd. 2019). Bu ilerlemeler, derin sinir ağlarını her zamankinden daha güçlü ve genel hale getiriyor. Derin bir sinir ağının mimarisi genellikle, ağdan geçerken verileri işleyen ve dönüştüren birbirine bağlı çok sayıda düğüm veya nöron katmanından oluşurlar. Derin öğrenmenin altında yatan mimari olarak yapay sinir ağlarının kullanılması, algoritmanın birçok varyantının geliştirilmesine yol açmıştır. Derin sinir ağlarının mimarisini ve bileşenlerini anlamak, etkili makine öğrenimi modellerini tasarlamak ve uygulamak için çok önemlidir. Derin sinir ağlarının en önemli uygulamalarından biri görüntü ve konuşma tanımadır. Evrişimli sinir ağları (CNN'ler) gibi derin öğrenme mimarileri, otomatik konuşma tanıma (ASR) gerçekleştirmek için kullanılmıştır. CNN'ler ayrıca gürültü sınıflandırma görevleri için de kullanılmıştır ve derin öğrenme modelleri için ses verilerini işleyebilirler. Ayrıca, bilgisayarların görüntülerdeki örüntüleri tanımasına ve buna göre sınıflandırmasına izin veren, görüntü tanıma görevleri için derin sinir ağları kullanılmıştır (Alam vd. 2020). Derin sinir ağlarının görüntüleri ve konuşmayı doğru bir şekilde tanıma ve sınıflandırma yeteneği, tıp, güvenlik ve eğlence gibi alanlarda şimdiden büyük ilerlemelere yol açmıştır.

2.3.2 Evrişimli Sinir Ağları

Evrişimli sinir ağları (CNN'ler), öncelikle görsel görüntüleri analiz etmek için kullanılan makine öğrenimi ve yapay sinir ağlarının bir alt kümesidir. Özellikle görüntü tanıma ve sınıflandırma gibi görsel veri işleme problemlerine uygulanmak üzere tasarlanmış derin öğrenme modelleridir. Derin öğrenmede CNN, görsel görüntüleri analiz etmek için en yaygın olarak kullanılan bir yapay sinir ağları sınıfıdır (Sharma vd. 2018). Bir CNN, bir girdi görüntüsünü alan, görüntünün farklı yönlerine evrişim adı verilen bir süreç aracılığıyla anlam atayan ve görüntüdeki belirli nesneleri veya özellikleri tanımak ve sınıflandırmak için eğitilmiş bir derin öğrenme algoritmasıdır (saturncloud.io 2023). CNN'ler, yerel özelliklerin korunmasına ve öğrenilmesine odaklanarak, verilerin hiyerarşik yapılarını yakalamada etkili bir yaklaşım sunarlar. Evrişimli katmanlar, girdi

verileri üzerinde filtreler uygulayarak özellik haritaları oluşturur ve bu sayede ağ, temel özelliklerden karmaşık özelliklere doğru öğrenir. CNN'ler, evrişimli katmanlar, havuzlama katmanları ve tamamen bağlı katmanlar gibi çoklu yapı bloklarını kullanarak geri yayılım yoluyla özelliklerin uzamsal hiyerarşisini otomatik ve uyarlanabilir bir şekilde öğrenmeyi amaçlar (Yamashita vd. 2018). CNN mimarisi ve katmanları, CNN'lerin temel yapı taşlarıdır. Derin öğrenme CNN üç katmandan oluşur: evrişim katmanı, havuzlama katmanı ve tamamen bağlı katman (techtarget.com 2023). Evrişimli bir katman, özellikleri ayıklamak ve bir özellik haritası oluşturmak için bir girdi görüntüsüne bir dizi filtre uygular. Havuzlama katmanları, evrişimli sinir ağlarının başka bir önemli bileşenidir. Havuzlama katmanları, özellik haritalarının boyutsallığını azaltarak CNN'leri hesaplama açısından daha verimli hale getirir. Böylece, ağın daha önce görülmemiş verilere uygulanabilirliği sağlanır. Tamamen bağlantılı katmanlar, evrişimli ve havuzlama katmanlarının çıktısını alır ve görüntüleri sınıflandırır (upgrad.com 2023, Neshatpour vd. 2019). Bu katmanlar, girdi boyutunu ve hesaplamaların karmaşıklığını azaltarak ağı daha verimli kılar ve modelin genelleştirme yeteneğini artırır. Etkin süreklilik oranları, Evrişimli Sinir Ağları (CNN) için öğrenme sürecini optimize ederek, görüntü sınıflandırma performansında önemli bir artış sağlamaktadır (Yılmaz ve Demir 2022).



Resim 2.3.3 CNN Mimarisinin Nasıl Tasarlanacağını Gösteren textCNN Modeli.

CNN'lerin görüntü ve video tanımada çeşitli uygulamaları vardır. Yüz tanıma, nesne

tanıma ve tanıma, konuşma tanımada kullanılırlar (techtarget.com 2023). Son yıllarda CNN, çeşitli bilgisayarla görme görevlerine hâkim oldu ve tüm dünyadaki araştırmacıların ilgisini çekti (Yamashita vd. 2018). Özetle, CNN'ler güçlü bir makine öğrenimi aracıdır ve çeşitli görüntü ve video tanıma görevlerinde çok etkili oldukları kanıtlanmıştır. Görüntü ve video analitiği, tıbbi görüntüleme ve otonom araçlar gibi çeşitli alanlarda başarılı uygulamalara sahiptir ve gelecekte de bu tür problemlerin çözümünde önemli bir rol oynamaya devam edecektir.

2.3.3 Yinelemeli Ağlar

Yinelemeli bir ağ, birçok girdi verisi yinelemesinden öğrenmek için tasarlanmış bir tür sinir ağıdır. Verileri tek bir geçişte işleyen geleneksel ileri beslemeli sinir ağlarının aksine, yinelemeli ağlar, verileri her biri bir öncekinin sonuçlarına dayanan bir dizi yinelemede işlemektedir. Bu, yinelemeli ağların verilerdeki daha karmaşık kalıpları ve ilişkileri öğrenmesine izin vererek, onları özellikle doğal dil işleme ve konuşma tanıma gibi görevler için kullanışlı hale getirir (Neshatpour vd. 2019). Yinelemeli ağlar, diğer sinir ağları türlerinden farklı benzersiz bir mimariye sahiptir. Genellikle, her biri girdi verilerini farklı bir şekilde işleyen birden çok katmandan oluşurlar. Her katmanın çıktısı daha sonra bir sonraki iterasyon için girdi olarak ağa geri beslenir. Bu süreç, ağ istenilen doğruluk düzeyine ulaşana veya bir durma kriteri sağlanana kadar devam eder (Neshatpour vd. 2018).

Yinelemeli bir ağdaki katmanlar, uygulamaya bağlı olarak evrişimli, tekrarlayan ve ters evrişimli katmanları içerebilir (Neshatpour vd. 2019). Yinelemeli ağlar, doğal dil işleme ve konuşma tanımada yaygın olarak kullanılmaktadır. Örneğin, metin verilerini analiz etmek ve sınıflandırmak, konuşma kalıplarını tanımak ve konuşulan dili tanımak için kullanılabilirler (Liu vd. 2020). Ayrıca, metni bir dilden diğerine çevirmek için kullanılan makine çevirisi sistemlerinin doğruluğunu artırmak için yinelemeli ağlar kullanılmıştır (Kiranyaz vd. 2021). Genel olarak yinelemeli ağlar, karmaşık verileri işlemek için güçlü araçlardır ve makine öğrenimi ve yapay zekâ alanında önemli bir araştırma alanıdır.

2.3.4 Otomatik Kodlayıcı Sinir Ağı

Otomatik kodlayıcı sinir ağları, son yıllarda veri yapılarını keşfetme ve sıkıştırıcı temsillerini geliştirme yetenekleri nedeniyle popülerlik kazanan bir yapay sinir ağı türüdür (jeremyjordan.me 2023). Bir otomatik kodlayıcı, tipik olarak boyut azaltma, veri sıkıştırma ve özellik çıkarma için girdi verilerini kodlamayı ve kodunu çözmeyi öğrenen denetimsiz bir öğrenme algoritmasıdır (Wang vd. 2020). Girdisini düşük boyutlu bir temsile sıkıştırarak ve ardından orijinal boyutlarına geri döndürerek yeniden yapılandırmayı öğrenen bir sinir ağıdır (simplilearn.com 2023). Basit bir ifadeyle, bir otomatik kodlayıcı sinir ağı, girdi verilerini daha verimli bir şekilde temsil etmeyi öğrenen bir veri sıkıştırma algoritması olarak düşünülebilir (mygreatlearning.com 2023). Sinirsel otomatik kodlayıcı ağları fikri onlarca yıldır vardır (stats.stackexchange.com 2023). 1988'de Bourlard ve Kamp ilk otomatik kodlayıcıyı önermiştir (Bank vd. 2020). O zamandan beri, her biri kendine özgü özelliklere ve uygulamalara sahip olan otomatik kodlayıcı sinir ağlarının birçok çeşidini geliştirilmiştir (iq.opengenus.org 2023). Oto kodlayıcılar için en yaygın sinir ağı türlerinden bazıları gürültü giderici oto kodlayıcıları, varyasyonel oto kodlayıcıları, evrişimli oto kodlayıcıları ve tekrarlayan oto kodlayıcıları içerir (towardsdatascience.com 2023). Otomatik kodlayıcı sinir ağları, verimli veri temsillerini denetimsiz bir şekilde öğrenme yetenekleri nedeniyle makine öğrenimi alanında popüler araçlar haline gelmiştir (Sun vd. 2016). Görüntü ve konuşma tanıma, doğal dil işleme ve anormallik tespiti gibi çeşitli alanlarda kullanılmaktadır (kdnuggets.com 2023). Otomatik kodlayıcı sinir ağları, verilerden anlamlı özellikler çıkarmak ve bunları daha kompakt temsillere sıkıştırmak için güçlü bir araçtır, bu da büyük miktarda veriyi depolamayı, iletmeyi ve işlemeyi kolaylaştırır (towardsdatascience.com 2023). Otomatik kodlayıcı sinir ağları, görüntü işleme ve veri sıkıştırma dahil olmak üzere çeşitli uygulamalara sahiptir. Otomatik kodlayıcılar, geri yayılımı kullanan ve hedef değerleri girişle eşleşecek şekilde ayarlayan denetimsiz makine öğrenimi algoritmalarıdır (medium.com 2023). Otomatik kodlayıcılar, popüler bir derin öğrenme kitaplığı olan Keras'ta görüntü sıkıştırma için kullanılabilir (blog.paperspace.com 2023). Sento ve ark. tarafından 2016'da derin sinir ağlarını kullanan bir görüntü sıkıştırma algoritması gösterilmiştir (Sento 2016). Otomatik kodlayıcılar, girdiyi gizli bir alana sıkıştırarak ve ardından çıktıyı bu sıkıştırılmış gösterimden yeniden yapılandırarak çalışmaktadır (towardsdatascience.com 2023). Bu

nedenle, sinirsel otomatik kodlayıcı ağları, verimli görüntü işleme ve veri sıkıştırma için kullanılabilir (iopscience.iop.org 2023). Otomatik kodlayıcı sinir ağları, anormallik tespiti ve aykırı değer analizi için de kullanılabilir. Otomatik kodlayıcılar, sinir ağlarının özelliklerini anormallik tespiti için ağları eğitmenin verimli bir yolunu elde etmek için özel bir şekilde kullanır (medium.com 2023). Sinir ağları hileli olmayan veriler üzerinde eğitilebilir ve daha sonra aykırı değerleri bulmak için hileli ve hileli olmayan verilerin bir karışımı üzerinde test edilebilir. Otomatik kodlayıcı, anormallikleri veya aykırı değerleri tespit etmek için yeniden yapılandırma hatalarını kullanan denetimsiz bir sinir ağı modelidir (pub.towardsai.net 2023). Bu nedenle, otomatik kodlayıcı sinir ağları, çeşitli uygulamalarda verimli anomali tespiti ve aykırı değer analizi için kullanılabilir. Otomatik kodlayıcı sinir ağları, özellik çıkarma ve veri görselleştirme için de kullanılabilir. Otomatik kodlayıcılar, girdilerinin sıkıştırılmış temsillerini öğrenmeye çalışan sinir ağı modelleridir (machinelearningmastery.com 2023). Çıkartılan özellikler daha sonra, temeldeki veri yapısı hakkında fikir edinmek için görselleştirilebilir. Otomatik kodlayıcı sinir ağları, denetimsiz özellik çıkarma için kullanılabilir. Bu, görüntü tanıma ve doğal dil işleme gibi çeşitli uygulamalar için kullanışlıdır (analyticsvidhya.com 2023). Bu nedenle, otomatik kodlayıcı sinir ağları, çeşitli uygulamalarda verimli özellik çıkarma ve veri görselleştirme için kullanılabilir.

2.3.5 Sinir Ağaçları

Sinir ağaçları, yapay sinir ağları ve karar ağaçları tekniklerinin bir araya getirilmesiyle oluşturulan hibrid bir makine öğrenimi modelidir. Doğrudan verilerden öğrenmek yerine arama yollarını öğrenmek için küçük sinir ağlarından oluşan bir hiyerarşi kullanan hibrit bir makine öğrenme şemasıdır. Sinir ağacı, doğrudan veri yerine arama yollarını öğrenmek için küçük sinir ağlarından oluşan bir hiyerarşi (ağaç) kullanan karma bir şemadır. Bu yaklaşım, karar ağaçlarının yorumlana bilirliği ve yapay sinir ağlarının esnekliği ve öğrenme kapasitesini birleştirerek, daha güçlü ve etkili bir öğrenme süreci sunar. Sinir ağaçları, sınıflandırma ve regresyon problemleri gibi çeşitli makine öğrenimi görevlerinde kullanılabilir (Zhou vd. 2020, Ojha ve Nicosia 2022). Sinir ağaçlarının temel mimarisi, karar ağacı düğümlerinde sinir ağları kullanarak daha karmaşık ve doğrusal olmayan ilişkileri öğrenmeyi sağlar. Karar ağacındaki her düğüm, gelen veriyi

analiz etmek ve bir sonraki düğüme yönlendirmek için küçük bir sinir ağı içerir. Bu sayede, sinir ağacı modeli, verinin doğrusal olmayan yapılarını daha iyi yakalayabilir ve daha doğru tahminler yapabilir (Xhemali vd. 2009). Sinir ağaçlarının diğer sinir ağı mimarilerine göre çeşitli avantajları vardır. Sinir ağaçları, karşılaştırılabilir performans elde etmek için daha az parametre gerektirdiklerinden derin sinir ağlarından hesaplama açısından daha verimlidir. Ayrıca, sinir ağaçlarımdaki karar ağaçları ve sinir ağlarının kombinasyonu, sınıf hiyerarşilerinin ve karar dallarının kullanımına izin vererek performansın artmasına yol açar (Chen vd. 2018). Yapay sinir ağlarının esnekliği sayesinde, sinir ağaçları modelleri karmaşık ve gürültülü veri kümelerinde daha iyi performans sergileyebilir. Ayrıca, karar ağaçlarının yorumlana bilirliği, modelin sonuçlarını ve öğrenme sürecini daha kolay anlamamıza ve analiz etmemize olanak tanır. Bu özellik, modelin uygulanabilirliğini artırarak, daha geniş bir uygulama yelpazesinde değerli sonuçlar elde etmeye yardımcı olur. Sinir ağaçları, karar ağaçlarının ve yapay sinir ağlarının güçlü özelliklerini bir araya getirerek, daha etkili ve güçlü bir makine öğrenimi modeli sunar. Yapay sinir ağı mimarisi, makine öğrenimi modellerinin başarısında, özellikle görüntü işleme ve örüntü tanımada kritik bir rol oynar. Özellik tabanlı segmentasyon ve nesne tanıma görevlerinde gelişmiş performans ve verimlilikleri nedeniyle sinir ağlarının kullanımı, klasik örüntü sınıflandırıcıların ve kümeleme tekniklerinin yerini alarak son yıllarda artmıştır (Egmont-Petersen vd. 2002). Bununla birlikte, mimariyi optimize etmek için en iyi yöntemin nasıl belirleneceği konusunda bir fikir birliği bulunmadığından, optimum sinir ağı yapılandırmasının belirlenmesi bir sorun olmaya devam etmektedir (Ciancio vd. 2016). Genel olarak, görüntü işleme ve sinir ağlarında örüntü tanıma tekniklerinin uygulanmasıyla ilgili hala çözülmemiş sorunlar olsa da yeni gelişmeler ve bu tekniklerin çeşitli uygulamalarda artan kullanımı nedeniyle bu alanda büyük ilerleme potansiyeli vardır (Egmont-Petersen vd. 2002). Sinir ağaçları, doğrudan verilerden öğrenmek yerine arama yollarını öğrenmek için küçük sinir ağlarından oluşan bir hiyerarşi kullanan hibrit bir yaklaşımdır. Derin öğrenmede sinir ağaçlarının uygulanmasının faydaları önemlidir. Sinir ağaçlarının doğası gereği yorumlanabilir olduğu bulunmuştur ve bu da onları derin öğrenme modellerinin nasıl karar verdiğini anlamak için yararlı bir araç haline getirir (Yang vd. 2018). Ayrıca sinir ağaçları, karmaşık veri yapılarını temsil etmek için gereken parametre sayısını azaltarak derin öğrenme modellerinin performansını iyileştirme potansiyeline sahiptir (Li vd.

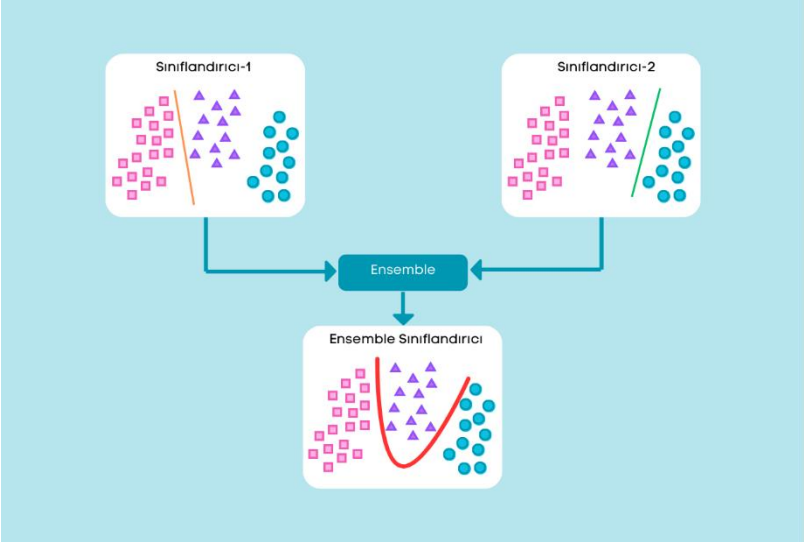
2022). Ancak sinir ağaçlarını tasarlamak ve uygulamak zor olabilir. En büyük zorluklardan biri, derin sinir ağlarının ve karar ağaçlarının büyük ölçüde bağımsız paradigmalar üzerinde çalışmasıdır (Tanno vd. 2019). Ayrıca sinir ağaçları, bazı uygulamalarda sınırlayıcı bir faktör olabilen arama yollarını etkili bir şekilde öğrenmek için büyük miktarda eğitim verisi gerektirir. Ayrıca, sinir ağaçlarının yorumlana bilirliği, karmaşık çok katmanlı uygulamalarda kullanıldığında zarar görebilir (Yang vd. 2018). Bu zorluklara rağmen sinir ağaçları, derin öğrenmede umut verici bir araştırma alanı olmaya devam ediyor.

İleriye bakıldığında, sinir ağaçlarının derin öğrenmedeki potansiyel uygulamaları çok fazladır. Örneğin, Nöral Karar Ağaçları (NDT), sınıf hiyerarşilerini ve karar dallarını uygulayan, onları sınıflandırma ve tahmin görevleri için güçlü araçlar haline getiren hibrit sinir ağı modelleridir (Jain ve Kumar 2007). Karar ağaçları ayrıca basit uygulama, az sayıda parametre ve farklı veri türlerine uyum sağlama yeteneği sunarak onları çeşitli uygulamalar için yararlı araçlar haline getirir (Arifuzzaman vd. 2023). Derin öğrenme geliştikçe, sinir ağaçlarının daha verimli ve etkili derin öğrenme modelleri geliştirmede giderek daha önemli bir rol oynaması muhtemeldir (Alzubaidi vd. 2021).

2.4 Kolektif Öğrenme

Kolektif öğrenimi, son bir tahmin yapmak için birden çok temel öğreniciyi birleştiren bir makine öğrenimi tekniğidir. Bu yöntem, diğer öğrenme yöntemlerine kıyasla sınıflandırma performansını başarılı bir şekilde geliştirir. Önerilen çerçevede, temel öğrenenlerin kombinasyonu doğrusal bir dönüşüme dönüştürülür ve amaç fonksiyonu, değişen yön çarpanı yöntemi ile verimli bir şekilde çözülebilir. Diğer öğrenme yöntemleriyle karşılaştırıldığında kolektif öğrenmenin büyük avantajları vardır. Örneğin, çeşitlilik ile bireysel doğruluğu dengelemeye çalışır (Mao vd. 2019). Kolektif seçimi, kolektif öğreniminde sıcak bir konudur ve bireyleri birleştirme süreci doğrusal dönüşümler içerebilir (Caruana vd. 2004). Optimum ağırlıklar, lineer dönüşümün optimal izdüşüm yönü izlenerek elde edilir. Kolektif öğrenmenin amacı, sınıflandırma performansını iyileştirmektir (Mao vd. 2019). Temel öğreniciler, farklı yöntemler kullanılarak bağımsız olarak üretilebilir ve seçilen bir temel sınıflandırıcı alt kümesi, tüm kolektif sisteminden daha iyi performans gösterebilir (Caruana vd. 2004). Kolektif

öğrenme, veri akışı analizi ve sınıflandırması için kullanılmış ve görüntü sınıflandırma, segmentasyon, yüz tanıma ve tıbbi görüntü analizinde başarı elde etmiştir. Kolektif yöntemlerinin bazı popüler örnekleri, Breiman tarafından önerilen AdaBoost, Bagging ve rastgele ormanlar ve farklı sınıfların benzer örneklerini ayırt etmek için ağaç kolektifleridir (Mao vd. 2019). ELBAD (Ensemble learning approach based on balanced accuracy and diversity), doğruluk ve çeşitliliği dengelemek için iki aşamalı bir yapay arı kolonisi algoritması kullanan ve 30 UCI veri setinde diğer popüler kolektif öğrenme algoritmalarından daha iyi performans gösteren, önerilen bir kolektif öğrenme yöntemidir. Bununla birlikte, ELBAD, bir kolektif sınıflandırıcı oluşturmak için gereken süreyi azaltmak için sistematik bir parametre ayarlama prosedürü gerektirir (Mao vd. 2019). Kolektif öğrenimi, sınıflandırma doğruluğunu iyileştirmek için birden çok temel öğreniciden oluşan bir kolektif oluşturan bir makine öğrenimi tekniğidir. İyi bir genelleme becerisine sahip güçlü bir kolektif oluşturmanın anahtarı, temel öğrenicilerin hem doğru hem de çeşitli olmasını sağlamaktır; bu, temel öğrenenler arasındaki çeşitliliği artırmak için etiketlenmemiş veriler kullanılarak elde edilebilir (Zhang vd. 2013). Yeni bir veri noktasını sınıflandırırken, her temel öğrencinin tahminleri, nihai bir tahmin elde etmek için (ağırlıklı) oylama yoluyla birleştirilir (Dietterich 2000). Sınıflandırma doğruluğunu daha da artırmak için son yıllarda hata düzeltme çıktı kodlaması, torbalama ve artırma gibi kolektif öğrenme algoritmaları geliştirilmiştir. Bir kolektif yöntemi, tipik olarak herhangi bir bireysel sınıflandırıcıdan daha iyi performans gösteren bir dizi sınıflandırıcı üreten bir öğrenme algoritmasıdır. Bayes ortalaması, orijinal kolektif yöntemi olarak kabul edilir (Dietterich 2000). Kolektif öğrenmenin, problem alanının farklı yönlerini yakalayan ve daha iyi tahminlere yol açabilen farklı sınıflandırıcı kolektifleri oluşturarak sınıflandırma doğruluğunu geliştirdiği gösterilmiştir (Dietterich 1997).



Resim 2.4.1 Kolektif Sınıflandırıcı.

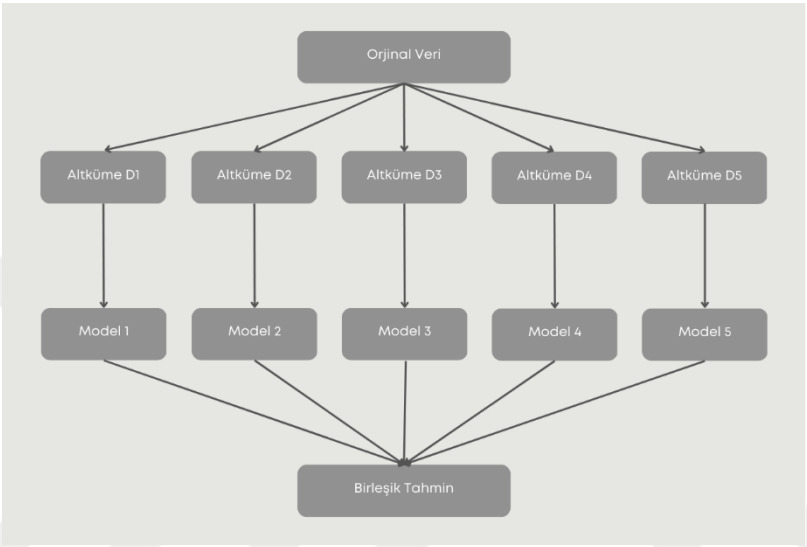
Kolektif öğrenimi, daha doğru tahminler oluşturmak için birden fazla bağımsız ön görücüden gelen tahminleri birleştiren bir mekanizmadır. Torbalama ve rastgele ormanlar, tahmin için bazı popüler kolektif yöntemleridir. Bu algoritmalar, genel tahmin doğruluğunu iyileştirmek için birlikte çalışan bir dizi model oluşturmak için farklı veri örneklerini ve özellik alt kümelerini kullanır (Dale vd. 2010). Kolektif öğrenimi, aşırı uydurmayı azaltabilir ve model sağlamlığını iyileştirebilir. Yöntem, çoğunluk kararı alarak veya farklı modellerin tahminlerinin ortalamasını alarak çalışır. Bu yaklaşım, farklı modellerin güçlü yanlarını birleştirerek hata düzeltme yoluyla tahminlerin genel doğruluğunu artırır. Kolektif öğrenmeyi bu kadar etkili kılan, modellerin çeşitliliğidir (Dale vd. 2010). Bu teknik, özellikle büyük miktarda veri olduğunda ve her bir veri kümesi için hangi modelin en uygun olduğunu belirlemenin zor olduğu durumlarda kullanışlıdır. Kolektif öğrenimi, görüntü tanıma, doğal dil işleme ve tıbbi tanı dahil olmak üzere çeşitli uygulamalarda öngörü performansını önemli ölçüde artırabileceğini gösteren çok sayıda çalışma ile aktif bir araştırma alanıdır.

2.4.1 Torbalama

Önyükleme birleştirme olarak da bilinen torbalama (Bagging), varyansı azaltarak ve fazla uydurmayı önleyerek model doğruluğunu iyileştirmek için makine öğreniminde kullanılan bir kolektif yöntemidir (blog.paperspace.com 2023). Torbalamada, orijinal

veri kümesinin farklı önyükleme örnekleri kullanılarak çoklu temel modeller eğitilir ve bu modellerin sonuçlarının ortalaması alınarak bir kolektif modeli oluşturulur (towardsdatascience.com 2023). Bu teknik, ek veri örnekleri üreterek tahmine dayalı bir modelin varyansını azaltmaya yardımcı olur (mygreatlearning.com 2023). Torbalama, makine öğrenimi modellerinin performansını ve doğruluğunu geliştirme yeteneği nedeniyle kolektif öğreniminde popüler bir teknik haline gelmiştir (simplilearn.com 2023). Torbalamanın, geleneksel makine öğrenimi yöntemlerine göre çeşitli avantajları vardır. Kararlılık sağlar ve bir model çok karmaşık olduğunda ve eğitim verilerinde iyi performans gösterirken yeni verilerde kötü performans gösterdiğinde meydana gelebilecek aşırı uyum riskini azaltır (educba.com 2023). Bu tekniğin, optimum performans için kritik olan modelin yanlılığını ve varyansını azaltmada etkili olduğu gösterilmiştir (mygreatlearning.com 2023). Rastgele ormanlar, ekstra ağaçlar ve torbalanmış karar ağaçları dahil olmak üzere çeşitli torbalama yöntemleri mevcuttur (scikit-learn.org 2023). Rastgele orman, temel model olarak karar ağaçlarını kullanan ve ağaçlar arasındaki korelasyonu azaltmak için her bölmede özelliklerin rastgele bir alt kümesini seçen popüler bir torbalama yöntemidir (blog.paperspace.com 2023). Öte yandan, Ekstra Ağaçlar, rastgele bölmelerle çok sayıda karar ağacı oluşturur ve rastgele bir özellik alt kümesinden en iyi ayrımı seçer (towardsdatascience.com 2023). Genel olarak torbalama, varyansı azaltarak ve fazla uydurmayı önleyerek makine öğrenimi modellerinin performansını ve doğruluğunu artırabilen güçlü bir kolektif öğrenme tekniğidir. Önyükleme toplaması olarak da bilinen torbalama, makine öğreniminde varyansı azaltmak ve fazla uydurmayı önlemek için güçlü bir kolektif yöntemidir (blog.paperspace.com 2023). Torbalamanın arkasındaki ana fikir, eğitim verilerinin farklı önyükleme örneklerini kullanarak birden çok modeli eğitmek ve ardından modellerin genel doğruluğunu iyileştirmek için tahminlerini birleştirmektir (towardsdatascience.com 2023). Torbalama, çoklu modellerden gelen tahminleri birleştirerek model varyansını azaltmaya ve genelleme performansını iyileştirmeye yardımcı olabilir (ibm.com 2023). Torbalama, karar ağaçları, rastgele ormanlar ve sinir ağları dahil olmak üzere çeşitli makine öğrenimi algoritmalarında başarıyla uygulanmıştır (mygreatlearning.com 2023). Bir kolektif yaklaşımında torbalamayı uygularken dikkate alınması gereken birkaç en iyi uygulama vardır. Farklı modellerin verilerdeki gürültüye karşı farklı hassasiyetleri olabileceğinden, önemli bir husus temel alınan modelin seçimidir. Ayrıca hem

kolektifteki model sayısı hem de önyükleme örneklerinin boyutu, modellerin performansını etkiler (ibm.com 2023). Doğruluk, kesinlik ve ayrımcılık gibi uygun metrikleri kullanarak torbalama modellerinin performansını değerlendirmek de önemlidir. Genel olarak, makine öğrenimi uygulayıcıları, en iyi uygulamaları izleyerek ve torbalamayı verimli bir şekilde uygulayarak model doğruluğunu ve güvenilirliğini iyileştirmek için bu kolektif yaklaşımının gücünden yararlanabilir.



Resim 2.4.2 Bagging Tekniği.

2.4.2 Yükseltme

Yükseltme (Boosting), tek bir güçlü öğrenci oluşturmak için birden fazla zayıf öğrenciyi birleştiren, makine öğreniminde kullanılan popüler bir kolektif yöntemidir. "Yükseltme" terimi, zayıf öğrenicilere yinelemeli olarak uyan, onları bir kolektif modeline ekleyen ve önceki zayıf öğrenicilerin hatalarını daha iyi hesaba katmak için eğitim veri setini güncelleyen bir algoritma ailesini ifade eder (towardsdatascience.com 2023). Güçlendirme, genellikle önyargı hatasını azaltan ve güçlü tahmin modelleri oluşturan sıralı bir kolektif yöntemidir (mygreatlearning.com 2023). Yöntem, tek bir zayıf öğrenicinin sonuçlarına ağırlıklar atar ve daha sonra önceki zayıf öğreniciler tarafından yanlış sınıflandırılan örneklere daha fazla ağırlık verir (aws.amazon.com 2023). Yükseltme, torbalama ve yığınlama gibi diğer kolektif yöntemlerine göre çeşitli avantajlara sahiptir. Güçlendirmenin ana avantajlarından biri, zayıf öğrenicilerin

doğruluğunu geliştirme ve böylece kolektif modelinin genel performansını geliştirme yeteneğidir. Ayrıca, yükseltme, gürültülü verileri ve aykırı değerleri diğer kolektif yöntemlerinden daha etkili bir şekilde işleyebilir (geeksforgeeks.org 2023). Yükseltme ayrıca çeşitli makine öğrenimi problemlerine uygulanabilen esnek bir yöntemdir. AdaBoost, klasik gradyan artırma ve modern gradyan artırma dahil olmak üzere farklı güçlendirme teknikleri vardır. AdaBoost, yanlış sınıflandırılmış örneklere daha yüksek ağırlıklar ve doğru sınıflandırılmış örneklere daha düşük ağırlıklar atayan popüler bir artırma algoritmasıdır (towardsdatascience.com 2023). Klasik gradyan yükseltme, her yeni ağacın bir önceki ağacın hatalarını düzelttiği bir kolektif modeline yinelemeli olarak karar ağaçları eklemeyi içerir. XGBoost ve LightGBM gibi modern gradyan yükseltme, model doğruluğunu daha da yükseltmek için daha gelişmiş optimizasyon teknikleri kullanır (ibm.com 2023). Kullanılan spesifik tekniğe bakılmaksızın, yükseltme, makine öğrenimi modellerinin performansını önemli ölçüde artırabilen güçlü bir kolektif tekniğidir (geeksforgeeks.org 2023).

2.4.3 Yığınlama

Kolektif yöntemleri, son tahminin doğruluğunu ve sağlamlığını geliştirmek için birden fazla modelin tahminlerini birleştiren makine öğrenme teknikleridir. Yığınlama (Stacking), makine öğrenimi modellerinin performansını iyileştirmek için en popüler kolektif yöntemlerinden biridir. Yığınlama, katılan kolektif üyelerinin tahminlerini en iyi şekilde nasıl birleştireceğini öğrenmek için bir meta modeli eğitir (machinelearningmastery.com 2023). Yığınlamanın arkasındaki mantık, her bir modelden daha iyi performans gösteren en iyi modeli oluşturmak için çoklu öğrenme algoritmaları kullanmaktır. Yığınlama, torbalama ve yükseltme gibi diğer kolektif yöntemlerinden farklıdır çünkü genellikle heterojen zayıf öğrenicileri dikkate alır (towardsdatascience.com 2023). Yığınlamanın ana avantajı, sınıflandırma ve regresyon problemlerini çözmek için bir dizi iyi performans gösteren modelin özelliklerini kullanabilmesidir (machinelearningmastery.com 2023, javatpoint.com 2023). Yığınlama, karar ağaçları, k-NN (k-en yakın komşu algoritması) ve destek vektör makineleri dahil olmak üzere her türlü modelle kullanılabilir. Ancak yığınlamanın dezavantajlarından biri, nihai modele ekstra karmaşıklık katmasıdır (towardsdatascience.com 2023).

Özetle, yığınlama, makine öğrenimi modellerinin performansını iyileştirebilen güçlü bir kolektif tekniğidir. Katkıda bulunan birden fazla modelden tahminleri birleştirmek için bir meta modelin eğitilmesini içerir. Artan doğruluk ve sağlamlık gibi birçok avantajı olmasına rağmen, artan karmaşıklık gibi bazı dezavantajları da vardır. Yine de yığınlama, makine öğrenimi modellerinin performansını artırmak için hala popüler bir tekniktir (javatpoint.com 2023, mygreatlearning.com 2023).

2.4.4 Oylama

Kolektif yöntemleri, sınıflandırma, regresyon, özellik seçimi ve aykırı değer tespiti problemlerinde tahmine dayalı doğruluğu, genellemeyi ve sağlamlığı geliştirme yetenekleri nedeniyle makine öğrenimi alanında kapsamlı bir şekilde incelenmiştir (Li vd. 2014). Bir kolektif yöntemi, tahminlerin ağırlıklı oylarını kullanarak yeni veri noktalarını sınıflandırarak tahminler yapmak için birden çok temel öğreniciyi birleştiren bir öğrenme algoritmasıdır (Dietterich 2000). Bayes ortalama alma ilk kolektif yöntemi olsa da son yıllarda hata düzeltme çıktı kodlaması, torbalama ve yükseltme gibi daha yeni algoritmalar tanıtıldı (Dietterich 2000). Özellik önem analizi, bir sonraki aşamada makine öğrenimi modelinin son girdi özellik uzayı için katkı tanımlayıcılarını seçmek ve böylece model için en bilgilendirici özellikleri seçmek için kullanılabilir (Li vd. 2014). Yığılmış kolektif yaklaşımının, diğer kolektif yöntemlerine kıyasla performansı etkili bir şekilde artıran, önerilen çerçevede bu öğrenicilerin doğrusal bir dönüşümünde birden fazla temel öğreniciyi birleştirebildiği için çeşitli problemlerde başarılı olduğu gösterilmiştir (Mao vd. 2019). Ayrıca hem çeşitliliği hem de bireysel doğruluğu maksimize eden yeni bir ağırlıklı kolektif öğrenmesi önerilmiştir. Bu önemlidir, çünkü kolektif sistemlerinde çeşitlilik genellikle göz ardı edilmektedir. Ancak tahmin doğruluğunu geliştirmede çok önemli bir rol oynar (Mao vd. 2019).

Doğruluk ve çeşitlilik fonksiyonlarını optimize etmek için Zhang ve ark. veri modellerinden yararlanmak için denetimsiz kümeleme ve bulanık atama yöntemlerini entegre etmiştir. Performansı artırmak amacıyla doğruluk ve çeşitlilik işlevlerini dengelemek için optimizasyon hedefleri oluşturmaktadır. Mao ve ark. (2019) tarafından

kolektif öğrenimi ile doğrusal dönüşüm arasındaki ilişkiye dayanan bir dönüşüm kolektif öğrenme çerçevesi önerilmiştir. Diğer taraftan Zhang ve ark. tarafından ise kolektif öğrenme performansını iyileştirmek için kolektif doğruluğunu ve çeşitliliğini dikkate almak için bir genetik algoritma kullanan bir kolektif sınıflandırıcı seçim yöntemi de önerilmiştir. Bu nedenle, oylama (Voting) mekanizmalarına odaklanarak kolektif yöntemlerinin doğruluğunu optimize etmek, makine öğrenimi modellerini geliştirme potansiyeline sahip önemli bir araştırma alanıdır.

2.5 Nesnelerin İnterneti

Nesnelerin İnterneti (IoT), sensörler, yazılım ve bağlantı ile gömülü fiziksel cihazlar, araçlar, cihazlar ve diğer nesnelerden oluşan bir ağı kapsar ve internet üzerinden otonom veri toplama ve alışverişi sağlar. Bu devrim niteliğindeki teknoloji, sağlık, ulaşım, tarım ve imalat gibi çeşitli sektörlerde çeşitli uygulamalar bulmuştur (Chatterjee ve Ahmed 2022). IoT cihazlarını günlük hayatımıza sorunsuz bir şekilde entegre ederek verimlilik, üretkenlik ve rahatlıkta önemli ilerlemeler sağlandı. IoT cihazlarının sunduğu sayısız avantaja rağmen, güvenlik endişeleri önemli bir zorluk olmaya devam ediyor. IoT cihazlarının yaygın olarak benimsenmesi, kullanıcı gizliliği ve sistem bütünlüğünde ihlallere yol açan güvenlik açıklarını ortaya çıkardı (Aljabri vd. 2023). IoT güvenliği, internete bağlı ve ağ tabanlı cihazları korumak için koruyucu önlemler uygulamaya odaklanır (techtarget.com 2023). Anomali tespiti, IoT cihazları alanında sağlam bir güvenlik yöntemi olarak öne çıkıyor. Anormallik tespiti, IoT cihazları tarafından toplanan verilerde, potansiyel güvenlik ihlallerinin veya tehditlerinin göstergesi olarak hizmet eden alışılmadık kalıpların veya davranışların tanımlanmasını içerir (Diro vd. 2021). Bu yöntem, alternatif güvenlik mekanizmalarını geride bırakarak IoT cihazlarının güvenliğini güçlendirmede muazzam bir potansiyele sahiptir. IoT cihazları her zamankinden daha yaygın hale geldikçe, güvenlik endişelerini ele alma ihtiyacı çok önemli hale geliyor (Khraisat ve Alazab 2021). Anomali tespit yöntemleri, güvenlik ihlallerinin tespit edilmesinde ve önlenmesinde, kullanıcı verilerinin güvenliğini ve gizliliğini sağlamada çok önemli bir rol oynamaktadır. IoT cihazlarının kullanımı artmaya devam ettikçe, potansiyel tehditlere ve güvenlik açıklarına karşı koruma sağlamak için esnek güvenlik önlemlerinin uygulanması zorunlu hale geliyor. IoT cihazlarının birbirine bağlı doğası ve ürettikleri ve ilettikleri hacimli veriler göz önüne alındığında, çeşitli

güvenlik risklerine karşı hassastırlar. Zayıf kimlik doğrulama ve yetkilendirme mekanizmaları, yetersiz şifreleme ve güvenli olmayan yazılım ve ürün yazılımı, IoT cihazlarında yaygın güvenlik açıklarını temsil eder (emnify.com 2023). Sonuç olarak, IoT cihazlarının güvenliğinin sağlanması hem bireyler hem de kuruluşlar için önemli bir endişe kaynağı haline geldi. IoT güvenlik ihlallerinin yansımaları ciddi olabilir; finansal kayıplar, itibar kaybı ve tehlikeye atılmış kişisel ve hassas veriler olabilir. Bazı durumlarda, bu ihlaller tıbbi cihazlar veya otonom araçlar bağlamında olduğu gibi fiziksel zarara bile neden olabilir (Aljabri vd. 2023). Bu nedenle, IoT cihazlarının güvenliğine öncelik verilmesi, olası zararların önlenmesi ve güvenlik ihlallerinin etkisinin en aza indirilmesi için vazgeçilmez hale geliyor. Anomali algılama yöntemleri, IoT cihazlarının güvenliğini artırmada çok önemli bir rol üstlenir. Bu teknikler, bir güvenlik ihlaline işaret edebilecek olağandışı davranışları veya kalıpları tespit etmeyi ve işaretlemeyi içerir. Örneğin, anormallik tespiti, bir siber saldırının göstergesi olan anormal ağ trafiğini veya cihaz davranışını belirleyebilir (Chatterjee ve Ahmed 2022, Mazhar vd. 2023). IoT cihazlarını ve bağlı oldukları ağları korumak için güvenlik teknolojilerinin, sürekli genişleyen IoT güvenlik açıkları ve riskleri yelpazesini ele alması gerekir (paloaltonetworks.com 2023). Bireyler ve kuruluşlar, etkili güvenlik önlemleri uygulayarak IoT cihazlarıyla ilişkili riskleri azaltabilir ve verilerinin güvenliğini ve gizliliğini sağlayabilir.

Anormallik tespiti, IoT güvenliğinde bu amaçla yaygın olarak kullanılan makine öğrenimi teknikleriyle IoT cihazlarının güvenliğini sağlamanın kritik bir yönü olarak ortaya çıkıyor (Han vd. 2022). Bu teknikler, modelleri cihazların normal davranış kalıplarını tanıması ve herhangi bir sapmayı anormallik olarak işaretlemesi için eğiterek siber tehditleri tespit etmede başarılı olduğunu kanıtlıyor (Chen vd. 2022). İstatistiksel yaklaşımlar, IoT cihazları için anormallik tespitinde de yaygın bir kullanım bulmaktadır ve istatistiksel aykırı değerleri potansiyel anormallikler olarak belirlemek için cihaz verilerinin analizini gerektirir (Chatterjee ve Ahmed 2022). Bu nedenle, makine öğrenimi ve istatistiksel yaklaşımlar, anormallikleri tespit ederek IoT cihaz güvenliğini artırmada etkili oluyor. Davranışsal analiz, bir güvenlik tehdidine işaret eden herhangi bir olağandışı etkinliği belirlemek için cihaz davranışının analizini içeren IoT cihazlarında anormallik tespitine yönelik başka bir yaklaşımı temsil eder (Shamim vd. 2023). Makine

öğrenimi tabanlı anormallik tespitinden yararlanmak, IoT ağlarında çok çeşitli siber tehditlere karşı etkili bir güvenlik çözümü olarak hizmet eder (Alanaziv e Aljuhani 2022). Anormallik tespit sistemleri, alternatif güvenlik mekanizmalarına kıyasla IoT cihazlarının güvenliğini sağlamada özellikle başarılıdır (Diro vd. 2021). Bu, IoT cihazlarındaki anormallikleri tespit etmek için davranış analizi ve makine öğrenimi tabanlı yaklaşımları benimsemenin önemini vurguluyor. IoT cihazlarının kapsamlı kullanımı artmaya devam ettikçe, güvenlik ve mahremiyet endişeleri daha büyük önem kazanıyor (Aljabri vd. 2023). Anomali tespit teknikleri, IoT ortamlarında performans ve güvenlikle ilgili saldırıları tespit etmek ve azaltmak için kullanılabilir (Achiluzzi vd. 2022). IoT cihazlarına özel olarak uyarlanmış ana bilgisayar tabanlı anormallik algılama yaklaşımları, cihazın sistem çağrısı verilerindeki olağandışı etkinlikleri tanımlamayı ve böylece olası güvenlik tehditlerini algılamayı amaçlar (Shamim vd. 2023). Anormallik algılama yöntemleri kullanılarak, IoT cihazlarının güvenliği artırılarak siber tehditlere karşı koruma sağlanabilir (Wang vd. 2022).

2.6 Ağ Saldırıları

Siber güvenlik, elektronik sistemleri, ağları, verileri ve mobil cihazları kötü niyetli saldırılardan koruma uygulamasıdır (usa.kaspersky.com 2023). Dijital teknolojiye artan güven ile bu, modern yaşamın önemli bir yönüdür. Siber güvenlik, bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak için önlemler ve kontroller içerir (csrc.nist.gov 2023). Kişisel olarak tanımlanabilir bilgiler ve korunan sağlık bilgileri dahil olmak üzere hassas bilgileri hırsızlık ve hasardan korumak önemlidir (upguard.com 2023). Siber güvenlik, hassas bilgileri siber saldırılardan korumak için proaktif adımlar atmak için bireyler, işletmeler ve hükümetler için kritik öneme sahiptir. Siber güvenlik tehditleri ve riskleri çoktur ve sürekli gelişmektedir. En yaygın siber tehditlerden bazıları kötü amaçlı yazılım, kimlik avı, ortadaki adam saldırıları ve parola saldırılarıdır (onlinedegrees.und.edu 2023, reciprocity.com 2023). Siber güvenlik riskleri arasında kötü amaçlı yazılım, parola hırsızlığı, trafik müdahalesi ve hassas bilgilere yetkisiz erişim yer alır. Siber güvenlik risklerinin finansal kayıp, kimlik hırsızlığı ve itibar kaybı gibi ciddi sonuçları olabilir (nist.gov 2023). Bu nedenle, en son siber güvenlik tehditlerinden haberdar olmak ve bunlara karşı korunmak için proaktif adımlar atmak önemlidir. Günümüzün dijital çağında, siber güvenlik her zamankinden daha önemlidir. Siber saldırı

tehdidi yaygındır ve başarılı bir saldırının sonuçları ciddi olabilir. Ağ güvenliği, hassas verilerin güvenliğini sağlamak ve çeşitli ağ saldırılarına karşı savunmak için gerekli bir koşuldur (audra.io 2023). Bu nedenle bireyler, işletmeler ve hükümetler siber güvenliğin önemini anlamalı ve hassas bilgileri siber tehditlerden korumak için etkin önlemler alınmalıdır. Resim 2.6.1 de karşılaşabileceğimiz güncel tehditler bulunmaktadır

Resim 2.6.1 Siber Güvenlik Tehditleri.

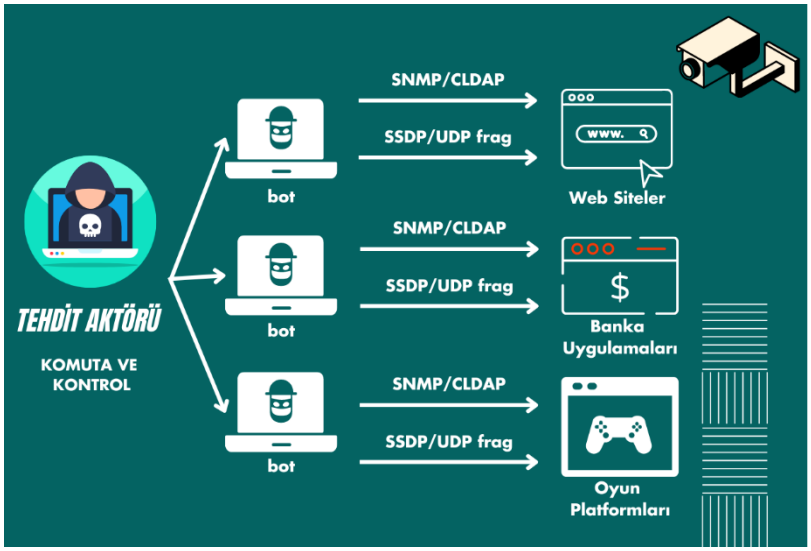
Siber saldırı, internete bağlı bir bilgi sistemini tehdit eden kötü niyetli bir olaydır. Bu saldırılar genellikle HTTP/HTTPS protokolü üzerinden gerçekleştirilir. Çoğu web saldırısı, yoğunlaştırılmış bir dizi saldırı tekniği kullanır. Bu saldırıları daha iyi anlamak ve daha güvenli uygulamalar geliştirmek için, yeni bir web saldırıları taksonomisi önerilmiş ve gerçek dünyadaki web saldırısı örnekleriyle gösterilmiştir (Álvarez ve Petrović 2003). Siber saldırılara karşı genel güvenlik açığını değerlendirmek için, yalnızca saldırganın saldırılarını tek tek değil, aynı zamanda kombinasyon halinde de değerlendirmek önemlidir (Jajodia vd. 2005). Saldırı taksonomileri, saldırı bilgisini otomasyona uygun hale getirerek davetsiz misafirleri tespit etmek için kullanılabilir (Álvarez ve Petrović 2003). Siber saldırıları anlamak, saldırgan davranışını daha geniş bir bağlamda incelemeyi gerektirir (Wang vd. 2005). Web saldırıları, ağ oluşturmadaki en önemli güvenlik sorunlarından biridir. Web sunucularına ve uygulamalarına uygun olmayan yetkilendirme, web saldırılarını başlatabilir (Lai vd. 2008). Saldırganlar, ağı farklı amaçlarla bozmak için farklı türde siber saldırılar ve başlatmak istedikleri saldırı

sınıfıyla ilgili araçları kullanmaktadır (Hoque vd. 2014). Bu saldırılar birçok şekilde olabilir, örneğin: Truva atı saldırısı, DoS/DDoS saldırısı veya tarama saldırısı (Hoque vd. 2014). Siber saldırılar, hedef ağdaki güvenlik açıklarından yararlanarak ağ güvenlik mekanizmalarını atlatmaya çalışır (Hoque vd. 2014). Saldırganlar genellikle güvenlik açıklarına göre bilgi toplayarak web sitelerini veya veri tabanlarını ve kurumsal ağları hedefler (Hoque vd. 2014). Ağ saldırılarının en yaygın türlerinden biri, meşru kullanıcılara hizmet vermemek için ağı aşırı trafikle aşırı yüklemeyi amaçlayan DDoS saldırısıdır (Hoque vd. 2014). Saldırganlar ayrıca normal ağ etkinliklerini bozmak için yazılım hizmetlerindeki güvenlik açıklarından, hatalardan ve yanlış yapılandırmalardan yararlanabilmektedir (Hoque vd. 2014). Bu saldırılar, ağ cihazı arızaları, ağ aşırı yüklemeleri, ağ veriminde ciddi düşüşler, kötü niyetli tarama ve diğer benzer faaliyetler dahil olmak üzere meşru ağ işlemlerini bozabilir. Bu saldırılar, davranışlarına ve potansiyel etki veya hasarın ciddiyetine göre farklı kategorilere ayrılır (Hoque vd. 2014). Siber saldırılar için finansal çıkarlar, merak, akran tanıma, güç, rekabet avantajı, intikam vb. gibi çeşitli motivasyonlar vardır (Nurse vd. 2014). Dışlanma veya arkadaşlara/aileye/ülkeye bağlılık korkusu da çalışanları saldırılara katılmaya motive edebilir (Nurse vd. 2014). Saldırganlar kişisel veya kurumsal kazanç için hassas bilgileri istismar edebildiğinden, içeriden gelen tehditler kuruluşlar için önemli bir endişe kaynağıdır. Bir siber saldırıyı gerçekleştirmenin anonimliği ve kolaylığı, onu düşük maliyetli ve ilişkilendirme açısından düşük riskli kılar (Kumar ve Carley 2016). Finansal kazanç ve intikama ek olarak, siber saldırılar politik olarak da motive edilebilir (Nurse vd. 2014). Geleneksel siber güvenlik kavramları, dış tehditlere odaklanır; ancak, dahili tehditler nedeniyle, bir kuruluşun güvenliğine yönelik daha büyük tehdit içeride olabilir (Nurse vd. 2014). Siber saldırıları daha iyi önlemek ve kontrol altına almak için arkasındaki farklı motivasyonları anlamak önemlidir.

Resim 2.6.2 Başlıca Siber Güvenlik Tehditleri.

2.6.1 DDOS

Dağıtılmış Hizmet Reddi (DDoS) saldırısı, ağ varlıklarının normal akışını bozmak için tasarlanmış bir ağ saldırısıdır. Bir DDoS saldırısında, birden fazla virüslü bilgisayar sistemi tek bir hedefe saldırır ve saldırıya uğrayan web sitesi veya hizmetin kullanıcılarına hizmet reddine neden olur (cloudflare.com 2023). Bu saldırı türü, hedef sistemi trafikle doldurmayı ve meşru kullanıcılar için erişilemez hale getirmeyi amaçlar (usa.kaspersky.com 2023). DDoS saldırıları, önemli mali kayıplara neden olabileceği ve bir şirketin itibarına zarar verebileceği için çevrimiçi işletmeler için ciddi bir tehdit oluşturmaktadır (techtarget.com 2023). DDoS saldırıları, hacimsel saldırılar, uygulama katmanı saldırıları ve protokol saldırıları dahil olmak üzere birçok biçimde olabilir. Toplu saldırılar, hedefi büyük hacimli trafikle doldururken, uygulama katmanı saldırıları, hedef sistemde çalışan belirli uygulamaları veya hizmetleri hedefler. Protokol saldırıları, hedef sistemleri tehlikeye atmak için ağ protokollerindeki güvenlik açıklarından yararlanır (ncsc.gov.uk 2023). Bu saldırılar aynı anda birden fazla kaynaktan başlatılabilir, bu da karşı önlemleri zorlaştırır (proofpoint.com 2023).



Resim 2.6.3 DDoS Saldırısı.

DDoS saldırılarını önlemek için kuruluşlar, güvenlik duvarları, izinsiz giriş tespit ve önleme sistemleri ve içerik dağıtım ağları dahil olmak üzere çeşitli güvenlik önlemleri uygulayabilir. Bu önlemler, DDoS saldırılarını gerçek zamanlı olarak tespit edip kontrol altına almaya ve hedef sistem üzerindeki etkiyi en aza indirmeye yardımcı olabilir (cloudflare.com 2023). Ek olarak, kuruluşlar, DDoS saldırılarına karşı kapsamlı koruma sağlamak için DDoS koruma hizmetlerini uygulamak üzere üçüncü taraf sağlayıcılarla ortaklık kurabilir (comptia.org 2023). Farklı DDoS saldırı türlerini anlamak ve etkili karşı önlemler uygulamak, kuruluşların bu büyüyen tehdide karşı savunma yapması için kritik öneme sahiptir (usa.kaspersky.com 2023). Dağıtılmış Hizmet Reddi (DDoS) saldırıları, web sitesi ve ağ kullanılabilirliği için önemli bir tehdit oluşturur. Bir DDoS saldırısında, kötü niyetli aktörler, hedeflenen bir sunucuyu, hizmeti veya ağı trafikle doldurmak, aşırı yüklemek ve meşru kullanıcılar için kullanılamaz hale getirmek için birden fazla bilgisayar veya cihaz kullanır (cloudflare.com 2023). DDoS saldırılarının, bir kuruluşun operasyonlarını olumsuz etkileyebilecek uzun süreli kesinti, düşük web sitesi performansı ve ağ kesintileri gibi ciddi sonuçları olabilir (techtarget.com 2023). Bu nedenle kuruluşlar, kullanılabilirliklerini sürdürmek ve iş sürekliliğini sağlamak için ağlarını ve web sitelerini DDoS saldırılarından korumak için proaktif adımlar atmalıdır. DDoS saldırıları ayrıca iş geliri ve itibar kaybına neden olabilir. Kapalı kalma süresi ve yavaş web sitesi performansı, satış kaybına, kaçırılan fırsatlara ve kurumsal itibarın zarar görmesine yol açabilir (a10networks.com 2023). Ayrıca, başarılı bir DDoS saldırısı, bir

şirketin marka itibarına ve müşteri güvenine ciddi şekilde zarar verebilir ve bunun uzun vadeli sonuçları olabilir (mass.gov 2023). Bu nedenle, şirketlerin bu tür saldırıların etkisini azaltmak için DDoS korumasına yatırım yapması çok önemlidir. DDoS saldırıları, güvenlik ekiplerini oltalama saldırıları gibi diğer kötü niyetli faaliyetlerden uzaklaştırmak için dikkat dağıtıcı olarak kullanılabilir (blog.netwrix.com 2023). Bu nedenle kuruluşlar, hassas verilerini siber tehditlerden korumak için DDoS korumasının yanı sıra veri şifreleme, erişim kontrolleri ve çalışan eğitimi gibi diğer önlemleri içeren kapsamlı bir güvenlik stratejisi uygulamalıdır. Dağıtılmış Hizmet Reddi (DDoS) saldırıları son yıllarda daha yaygın hale gelmiştir ve işletmeler ve kuruluşlar için önemli bir tehdit oluşturmaktadır. DDoS saldırısı, hedeflenen bir sunucunun, hizmetin veya ağın normal trafiğini trafik veya bağlantı istekleriyle doldurarak bozmaya yönelik kötü niyetli bir girişimdir (cloudflare.com 2023). Bu tür saldırıları önlemek için güvenlik duvarları, izinsiz giriş tespit ve önleme sistemleri ve içerik filtreleme gibi etkili ağ güvenlik önlemlerinin uygulanması çok önemlidir (techtarget.com 2023). Bu önlemler, kötü amaçlı trafiği hedef ağa ulaşmadan önce tespit edip engellemeye yardımcı olarak başarılı bir DDoS saldırısı riskini azaltır. İşletmelerin farkında olması gereken bir diğer tehdit de e-posta, kısa mesaj veya sosyal medya yoluyla bireyleri hedef alan bir tür sosyal mühendislik saldırısı olan kimlik avıdır. Kimlik avı saldırıları genellikle oturum açma kimlik bilgileri veya finansal bilgiler gibi kullanıcı kimlik bilgilerinin çalınmasıyla sonuçlanır (imperva.com 2023). Bu tür saldırıları önlemek için, çalışanları kimlik avı teknikleri ve şüpheli e-posta veya mesajların nasıl tanınacağı ve bildirileceği konusunda eğitmek önemlidir. Bu, düzenli eğitim ve simüle edilmiş kimlik avı saldırıları yoluyla yapılabilir (techtarget.com 2023). DDoS saldırılarına ve ilgili tehditlere karşı korunmak için düzenli güvenlik kontrolleri ve güncellemeleri de gereklidir. Bu denetimler, ağlar ve uygulamalardaki güvenlik açıklarının belirlenmesine yardımcı olabilir ve bu hatalar daha sonra yamalar ve güncellemeler yoluyla giderilebilir (ncsc.gov.uk 2023). Ek olarak bir DDoS koruma hizmetinin uygulanması, kötü amaçlı trafiği filtreleyerek ve meşru trafiğin hedefine ulaşmasına izin vererek bir saldırının etkisini azaltmaya yardımcı olabilir (cloudflare.com 2023). Şirketler, güvenlik önlemlerini düzenli olarak güncelleyerek ve gözden geçirerek başarılı bir DDoS saldırısı riskini azaltabilir ve ağlarını, verilerini ve müşterilerini zarar görmekten koruyabilir.

2.6.2 Fiziksel Saldırılar

Fiziksel saldırı, bir saldırganın bir ağa veya bilgisayar sistemine fiziksel erişim elde ettiği saldırıdır. Fiziksel saldırı, saldırganın zarar verme veya zarar verme niyetini içeren belirli bir fiziksel tehdit türüdür (knowww.eu 2023). Fiziksel saldırılar, güvenli bir veri merkezine girmek, bir binanın kısıtlı alanlarına gizlice girmek veya erişimlerinin olmadığı terminalleri kullanmak gibi birçok şekilde olabilir (csoonline.com 2023). Fiziksel saldırıların ciddi sonuçları olabilir. Bu saldırıların bunların gerçekleşmemesi için önlem almak son derece önemlidir. Fiziksel saldırılar çeşitli şekillerde gelebilir. Örneğin, bir saldırgan, internete bağlı bir anahtar kartlı erişim sistemini tehlikeye atarak, bir binaya fiziksel erişim vermelerine veya iptal etmelerine izin verebilir. Ortadaki adam (MITM) saldırıları, bir saldırganın ağdan paketleri yakaladığı, değiştirdiği ve yeniden yerleştirdiği başka bir fiziksel saldırı biçimidir (cisserv1.towson.edu 2023). Fiziksel erişim saldırıları, cihaz hırsızlığı, USB bağlantı noktasına erişim ve sabit sürücülerin uygunsuz şekilde imha edilmesi dahil olmak üzere herkesin bilgi çalabileceği yolları içerir. Bu nedenle, farklı fiziksel saldırı türlerinin farkında olmak ve bunları önlemek için gerekli önlemleri almak önemlidir. Fiziksel saldırılara karşı korunmak için ağ cihazlarının güvenli yerlerde tutulması gibi önlemler alınmalıdır. Ek olarak, güvenlik kameraları, erişim kontrol sistemleri ve güvenlik personeli gibi uygun fiziksel güvenlik önlemlerinin alınması çok önemlidir. Kuruluşlar ayrıca fiziksel güvenlik önlemlerindeki boşlukları belirlemek ve gidermek için düzenli güvenlik denetimleri yapabilir. Çalışanları fiziksel saldırı riskleri ve bunu önlemek için atabilecekleri adımlar konusunda eğitmek de önemlidir. Kuruluşlar bu önlemleri alarak fiziksel saldırı riskini önemli ölçüde azaltabilir ve ağlarını ve bilgisayar sistemlerini zarar görmekten koruyabilir.

2.6.3 Kimlik Avı

Kimlik Avı (Phishing), siber suçluların hassas bilgileri ele geçirmek amacıyla sahte elektronik iletişim araçları kullanarak hedeflerini kandırmaya çalıştığı kötü amaçlı bir tekniktir. 2019'da işletmelerin yaklaşık %90'ı kimlik avı saldırıları tarafından hedef alındığından, kimlik avı internet kullanıcıları, hükümetler ve hizmet sağlayıcılar için önemli bir tehdit haline geldi (Alkhalil vd. 2021). Kimlik avı saldırıları, kullanıcıları

hassas bilgileri ifşa etmeleri, kötü amaçlı yazılım indirmeleri veya sahte hesaplara para aktarmaları için kandırarak gerçekleştirilir (Alkhalil vd. 2021). Bu saldırılar, sesli kimlik avı (kimlik avı), sosyal medya saldırıları, SMS/metin kimlik avı (SMishing) ve kötü amaçlı USB düşürmeler dahil olmak üzere birçok biçimde olabilir (Alkhalil vd. 2021). Saldırganlar, meşru web sitelerinin davranışlarını kopyalayarak ve hedeflenen kurbanlara spam, metin mesajları veya sosyal ağlar aracılığıyla URL'ler göndererek web sitesi sayfaları oluşturur (Basit vd. 2021). Kullanıcılar kimlik avı saldırıları tarafından saldırıya uğradığında, hassas bilgileri çalınabilir ve bu da finansal dolandırıcılığa ve diğer güvenlik ihlallerine yol açabilir (Basit vd. 2021). Kimlik avı saldırıları son yıllarda istikrarlı bir şekilde arttı ve daha karmaşık hale geldi, siber araştırmacıların ve geliştiricilerin etkilerini belirlemek ve azaltmak için daha fazla dikkat çekti (Alkhalil vd. 2021). İstismar edilen vektörlere ilişkin bilgi, daha fazla istismarı önlemek ve yeni savunmasız vektörleri belirlemek için karşı önlemler tasarlamak için kullanılabilir. Bu tekniklerin sistematik olarak anlaşılması, daha etkili kimlik avı önleme tekniklerinin geliştirilmesine yol açabilir (Chiew vd. 2021). Giderek daha fazla kullanıcı günlük işleri için İnternet'e güvendikçe, daha iyi doğruluk ve yanıt süresi ile kapsamlı bir kimlik avı saldırı tespit çözümüne sahip olmak giderek daha önemli hale geliyor (Basit vd. 2021). Geçmişte birden fazla çözüm önerilmiş olsa da saldırganlar bu saldırıların üstesinden gelmek için önerilen çözümlerin güvenlik açıklarını göz önünde bulundururlar (Basit vd. 2021). COVID-19 pandemisi sırasında çevrimiçi iş birliği araçlarının kullanımının artmasıyla birlikte, kimlik avı saldırılarının sayısı da önemli ölçüde yükseldi (Basit vd. 2021). Bu durum, farkındalık ve korunma önlemlerinin daha da önemli hale gelmesine neden oldu. Dolayısıyla, bu tehditlere karşı bilinçli olmak, internet kullanırken dikkatli davranmak ve oltalama saldırılarına karşı etkili koruma stratejileri geliştirmek, güvenliğimizi koruma adına kritik öneme sahiptir.

2.6.3 Saldırı Tespit Sistemleri

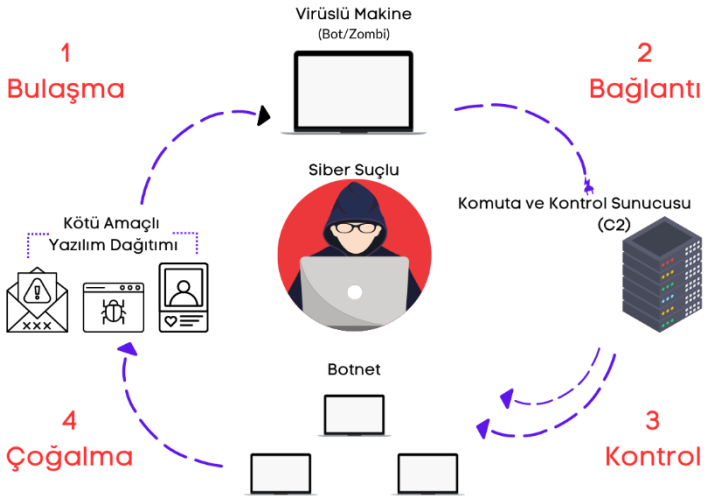
Saldırı Tespit Sistemi (IDS), ağ saldırılarını tespit etmek ve önlemek için önemli bir araçtır çünkü ağ saldırı tespiti, ağ operatörleri için önemli bir görevdir. Geleneksel olarak, iki ana IDS yaklaşımı vardır: imza tabanlı veya yanlış kullanım tespiti ve anormallik tespiti. İmza tabanlı IDS, normal çalışma için imzalar veya yapılandırma dosyaları

biçimindeki harici bilgilere dayanır ve son on yılda kapsamlı bir şekilde incelenmiştir. Öte yandan, anormallik tabanlı IDS'ler, normal trafik davranışından sapmaları tespit etmek için istatistiksel ve makine öğrenimi teknikleri kullanır ve izinsiz giriş tespiti için önemli bir araştırma ve geliştirme yönünü temsil eder (Casas vd. 2012). Bununla birlikte, anomali tabanlı siber saldırı tespiti için yeni teknikler ve veri kümeleri hakkında sistematik bir literatür çalışması yoktur. NIDS literatüründeki en dikkate değer açık kaynak sistemleri Bro ve SNORT'tur. Ayrıca, çoğu NIDS, gelen trafiği bir saldırı imzaları kitaplığıyla karşılaştırarak bilinen saldırıları tespit edebilen kötüye kullanım tespit tekniklerine dayanmaktadır. Ancak bu yaklaşımlar, siber saldırıları tespit etmek için imzalanmış veya işaretlenmiş trafik kayıtları şeklinde dış bilgi gerektirdiklerinden sınırlamalara sahiptir. NIDS'ye başka bir yaklaşım, imza, etiketli trafik veya eğitim kullanmadan bilinmeyen ağ saldırılarını tespit edebilen Denetimsiz Ağ Saldırı Tespit Sistemidir (UNIDS). UNIDS, saldırı oluşturan trafik örneklerini körlemesine ayıklamak için güçlü kümeleme tekniklerine güvenir (Casas vd. 2012). UNIDS, siber saldırıları tespit etmek için aykırı değerleri, yani çoğunluktan önemli ölçüde farklı örnekleri tanımlar. UNIDS tarafından kullanılan algoritma paralel hesaplama için çok uygundur ve KDD99 veri seti ve iki operasyonel ağdan gerçek trafik şeritleri dahil olmak üzere üç farklı trafik veri seti üzerinde değerlendirilmiştir. UNIDS, ağ izinsiz girişlerini ve saldırıları belirlemek için alt uzay kümelemesine ve çoklu kanıt toplama tekniklerine dayalı denetimsiz bir aykırı değer algılama yöntemi kullanır ve bilinmeyen saldırıları algılamak için geleneksel suistimal algılama tabanlı NIDS ile karşılaştırıldığında özellikle iyi performans gösterir (Casas vd. 2012).

2.6.5 Botnet

Botnet, üzerlerinde kötü amaçlı yazılım adı verilen kötü amaçlı kod yüklü olan, ele geçirilmiş, internete bağlı cihazlardan oluşan bir ağdır. Çok sayıda siber saldırı gerçekleştirmek için kullanılabilen bir kötü amaçlı yazılım türüdür (Limarunothai ve Munlin 2015, Plohmann ve Gerhards-Padilla 2012). "Botnet" terimi, "robot" ve "ağ" kelimelerinin birleşimidir. Bot ağları genellikle siber suçlular tarafından çeşitli dolandırıcılık ve siber saldırılar gerçekleştirmek için oluşturulur (usa.kaspersky.com 2023). Bu ağlar, kötü amaçlı etkinlikleriyle karakterize edilir ve kötü amaçlı yazılım,

DoS, kimlik avı ve enjeksiyon saldırıları gibi çeşitli siber saldırı türlerini gerçekleştirmek için kullanılır (Rahman ve Tomar 2021). Bot ağları dinamik ve esnektir ve ağ güvenliği için en büyük tehdit haline gelmiştir (Eslahi vd. 2012). Kötü amaçlı yazılım, DoS, kimlik avı ve enjeksiyon saldırıları dahil olmak üzere çeşitli saldırı türlerini başlatma yeteneğine sahiptirler (Rahman ve Tomar 2021). Bot ağları, merkezi veya merkezi olmayan bir mimariye sahip olabilir ve kötü amaçlı yazılım bulaştırma, sosyal mühendislik ve yazılım güvenlik açıklarından yararlanma gibi çeşitli teknikler kullanılarak oluşturulabilir (Limarunothai ve Munlin 2015). Bir cihaza kötü amaçlı yazılım bulaştığında, bir botnet'in parçası haline gelir ve çeşitli saldırılar için kullanılabilir. Bot yöneticileri, tespit edilmekten kaçınmak için botnet'leri izler ve düzenli olarak günceller (Eslahi vd. 2012). Tipik bir günde, internete bağlı 800 milyon bilgisayarın yaklaşık %40'ı botnet'lere aittir (Li vd. 2009). Bot ağları, İnternet güvenliği için ciddi bir tehdittir çünkü genellikle Bitcoin gibi sanal para birimlerine odaklanan para kazanma etkinlikleri veya dağıtılmış hizmet reddi (DDoS) saldırıları için kullanılabilirler (Plohmann ve Gerhards-Padilla 2012). Büyüklük ve coğrafi dağılım açısından ölçmek zor olabilir ve mevcut ve gelecekteki zorlukları nedeniyle, onları anlamak ve takip etmek önemlidir (Plohmann ve Gerhards-Padilla 2012, Limarunothai ve Munlin 2015). Bot ağları, gizli bilgileri çalmak, kötü amaçlı yazılım dağıtmak ve bilgisayar ağlarını kapatmak gibi kötü niyetli faaliyetler için siber suçlular tarafından oluşturulur ve sürdürülür (Karim vd. 2015). Bu saldırılar hizmetleri kesintiye uğratmak, verileri çalmak veya gücü kesmek için kullanılabilir (Karim vd. 2015). Bot ağları ayrıca spam göndermek, virüsleri ve solucanları yaymak ve Dağıtılmış Hizmet Reddi (DDoS) saldırıları başlatmak için kullanılır (Karim vd. 2015). Bot ağları genellikle spam kampanyalarında, tıklama sahtekarlığında ve dağıtılmış hizmet reddi (DDoS) saldırılarında kullanılır. DDoS saldırılarında, botnet'ler sistemleri çökertmek için kullanılır, bu da onların çökmesine veya meşru kullanıcılar tarafından kullanılamamasına neden olur (techtarget.com 2023). Yetkisiz kök erişimi, botnet saldırıları yoluyla da elde edilebilir (Karim vd. 2015). Ek olarak, botnet'ler yasa dışı aramalar yapmak ve kontrol panellerine erişmek için kullanılabilir (Karim vd. 2015). Botnet saldırıları genellikle siber suçlular Truva atı virüsleri enjekte ederek veya temel sosyal mühendislik tekniklerini kullanarak bir cihaza yetkisiz erişim elde ettiğinde başlar (securityscorecard.com 2023).



Resim 2.6.4 Botnet Nasıl Çalışır.

Suçlular, mobil botnet'leri uzaktan oluşturmak ve kontrol etmek için kusurlu mobil cihazları ve akıllı telefonları kullanır. Bir cihaza virüs bulaştığında, daha fazla saldırı başlatmak ve kötü amaçlı yazılımı diğer cihazlara yaymak için kullanılabilir. Bot ağları, kullanıcı verilerini bilgisi olmadan toplamak ve dosyalara ve fotoğraflara yetkisiz erişim elde etmek için de kullanılabilir. Botnet'e kaydolduktan sonra, virüslü cihazlar komuta ve kontrol (C&C) altyapısında bulunan cihazlarla iletişim kurabilir. Bu iletişim, suçluların mali çıkarlar elde etmesine veya web sitelerine veya ağlara saldırı başlatmasına olanak tanır. Ayrıca, toplanan veriler kimlik hırsızlığı, kredi kartı dolandırıcılığı, spam, web sitesi saldırıları ve kötü amaçlı yazılım dağıtımı için etik olmayan bir şekilde kullanılabilir (Karim vd. 2015). Bot ağları, siber suçlular için güçlü araçlar olabilir ve onlara geniş cihaz ağları üzerinde erişim ve kontrol sağlar. Bazı durumlarda, tek bir botnet cihazının güvenliği aynı anda birden fazla saldırgan tarafından ele geçirilebilir ve her saldırgan genellikle bunları farklı saldırı türleri için aynı anda kullanır (imperva.com 2023). Bot ağlarıyla ilişkili riskleri anlamak, bireylerin ve kuruluşların kendilerini potansiyel saldırılardan korumaları için kritik öneme sahiptir. Güçlü güvenlik önlemleri uygulayarak ve şüpheli etkinliklere karşı uyanık kalarak, bot ağları ve diğer siber saldırı türleri ile ilişkili riskleri azaltabilirsiniz. Botnet, ele geçirilmiş ve kötü amaçlı yazılım olarak bilinen kötü amaçlı kodla yüklenmiş, internete bağlı cihazlardan oluşan bir ağdır. Genellikle "bot" olarak adlandırılan bu cihazların her biri, genellikle bir siber suçlu veya bilgisayar korsanı olmak üzere bir varlığın kontrolü altındadır. Bot ağları, savunmasız cihazların

kontrolünü ele geçirmek için kötü amaçlı yazılımların kullanılmasını içeren bir bulaşma ve yayılma süreci aracılığıyla oluşturulur ve kontrol edilir (usa.kaspersky.com 2023). Bir cihaza virüs bulaştığında, dağıtılmış hizmet reddi (DDoS) saldırıları, veri hırsızlığı ve kötü amaçlı yazılım yayılımı dahil olmak üzere bir dizi kötü amaçlı etkinlik için kullanılabilir (datadome.co 2023). Bir botnet oluşturma ve kontrol etme süreci, cihazlara kötü amaçlı yazılım bulaştırmayı içerir; bu, saldırganların cihazların kontrolünü ele geçirmesine ve onları kötü amaçlı faaliyetler için kullanmasına olanak tanır. Bu süreç genellikle cihaza erişim elde etmek için yazılım veya donanımdaki güvenlik açıklarından yararlanmayı içerir. Bir cihaza virüs bulaştığında, bir botnet'in parçası haline gelir ve diğer cihazlara veya ağlara saldırmak için kullanılabilir (McDermott vd. 2018). Botnet komut ve kontrol (C&C) iletişimleri, saldırganlar tarafından botnet'leri yönetmek ve kontrol etmek için kullanılır. Bir DDoS saldırısı başlatmak veya veri çalmak gibi belirli eylemleri gerçekleştirmek için botlara komutlar gönderilir (datadome.co 2023). C&C altyapısı tipik olarak bot ile iletişim kurmak için merkezi bir sunucudan veya dağıtılmış bir sunucu ağından oluşur (datadome.co 2023). Botnet saldırıları mobil ağların çeşitli yönlerine odaklanır, mobil ağlardaki botnet saldırılarının işleyişine ilişkin farkındalık yaratır, mobil ağlara dayalı botnet'lerin olası tehditlerini ve güvenlik açıklarını analiz eder ve mobil kötü amaçlı yazılımın yayılmasını inceler. Botnet yaratıcıları ve kötü amaçlı yazılım programcıları, dikkate değer büyümesi nedeniyle Android platformunu hedeflerken, komutları yaymak için mikro bloglamayı kullanan bir mobil robot olan Andbot, onu gizli ve tespit edilmesini zorlaştırmaktadır (Karim vd. 2015). Ayrıca, bulut tabanlı push mobil botnet, komutları yaymak için push tabanlı bildirim hizmetlerini kullanır ve buluttan cihaza mesajlaşma hizmetleriyle yeni bir C&C kanalına sahiptir. Botnet saldırganları, yetkisiz erişim elde etmek için mobil cihazların istismar edilen güvenlik açıklarından yararlanır. Virüs bulaşmış mobil cihazlara, amaçları mobil kullanıcı cihazı kaynaklarına ve içeriğine erişim kazanmak ve bunları yönlendirmektir. Botnet'ler bağlı cihazlar için önemli bir tehdit oluşturuyor ve cihazları bulaşmaya karşı korumak ve mevcut olabilecek kötü amaçlı yazılımları tespit edip kaldırmak için adımlar atmak kritik önem taşıyor. Botnet türlerinden biri, büyük hacimlerde spam göndermek için kullanılan spam botnet'tir. Bu botnet'ler genellikle kötü amaçlı yazılım bulaşmış bilgisayarlar ve akıllı telefonlar gibi virüslü cihazlardan oluşur ve bot çobanları tarafından uzaktan kontrol edilebilir (techtarget.com 2023). Spam bot ağları, bireyleri kandırarak

oturum açma kimlik bilgileri ve kredi kartı numaraları gibi hassas bilgileri ifşa etmek için tasarlanmış kimlik avı e-postalarını yaymak için yaygın olarak kullanılır. Bu tür botnet'lerin İnternet altyapısı üzerinde önemli bir etkisi olabilmesinin yanı sıra e-posta sunucularının spam ile aşırı yüklenmesine neden olarak meşru kullanıcılar için daha yavaş e-posta teslim sürelerine sebep olabilmektedir. Başka bir botnet türü olan DDoS botnet, dağıtılmış hizmet reddi saldırılarını gerçekleştirmek için kullanılmaktadır. Bir DDoS saldırısı sırasında, bir botnet, hedeflenen bir sunucuya veya uygulamaya bir dizi istek göndererek, bunalmasına ve çökmesine neden olur (imperva.com 2023). DDoS bot ağları genellikle siber suçlular tarafından şirketlerden zorla para almak veya siyasi kuruluşların veya devlet kurumlarının operasyonlarını bozmak için kullanılır. Bu tür saldırılara karşı savunma yapmak zor olabilir çünkü binlerce hatta milyonlarca cihazı etkileyerek tüm saldırı trafiğinin tespit edilmesini ve engellenmesini zorlaştırır. Banka Truva Atı botnet'leri, bireylerden hassas finansal bilgileri çalmak için kullanılan başka bir botnet türüdür. Bu botnet'ler, tipik olarak, bireyler çevrimiçi bankacılık hesaplarına eriştiğinde kimlik bilgilerini ve diğer hassas bilgileri ele geçiren kötü amaçlı yazılımları cihazlara bulaştırır (dataprot.net 2023). Banka Truva Atı botnet'leri genellikle kimlik avı e-postaları veya kötü amaçlı web siteleri aracılığıyla dağıtılır ve bir kişinin finansal güvenliği üzerinde önemli bir etkiye sahip olabilir. Botnet, bir saldırganın sahiplerinin bilgisi olmadan kontrolünü ele geçirdiği, kötü amaçlı yazılım bulaşmış bilgisayarlardan veya cihazlardan oluşan bir ağdır (Arshad vd. 2011). Bot ağları farklı topolojilere ve mimarilere sahip olabilir ve farklı iletişim protokolleri ve enfeksiyon mekanizmaları kullanabilir (Amini vd. 2015). Bot ağları, merkezi ve eşler arası türler olarak sınıflandırılabilir. Merkezi botnet'ler, komut ve kontrol kanalları olarak IRC veya HTTP protokollerini kullanır (Arshad vd. 2011). Öte yandan, eşler arası botnet'ler, komut ve kontrol kanalları için P2P protokollerini kullanır (Arshad vd. 2011). Popüler P2P botnet'lerinin örnekleri Storm Worm ve Nugache'dir (Arshad vd. 2011). Bot ağları, bankacılık veri hırsızlığı, spam, dağıtılmış hizmet reddi, kimlik hırsızlığı ve kimlik avı gibi çeşitli amaçlar için kullanılabilir (Amini vd. 2015). Bu nedenle, kullanıcıların botnet'lerin oluşturduğu tehdidi ve cihazlarını botnet bulaşmasından korumak için gerekli önlemleri anlamaları önemlidir. IoT cihazları veya Nesnelerin İnternetine bağlı cihazlar, kolaylıkları ve günlük görevleri daha verimli hale getirme yetenekleri nedeniyle son yıllarda daha popüler hale gelmiştir. Bu cihazlar, akıllı termostatlar ve ev

yardımcılarından güvenlik kameralarına ve tıbbi ekipmanlara kadar her şeyi içermektedir. Bununla birlikte, IoT cihazlarının yükselişi, botnet saldırılarına karşı duyarlılığın artmasına da yol açmıştır (trendmicro.com 2023). Son yıllarda, IoT cihazlarını hedef alan birkaç büyük ölçekli botnet saldırısı gerçekleştiği bilinmektedir. Kötü şöhretli Mirai botnet, milyonlarca IoT cihazına bulaştı ve 2016'da büyük web sitelerine yapılan büyük bir DDoS saldırısından sorumluydu (securityintelligence.com 2023). Başka bir örnek, kontrolü ele geçirmek ve saldırılar başlatmak için IoT cihazlarındaki güvenlik açıklarını hedefleyen Reaper botnet'idir (trendmicro.com 2023). Bu saldırılar, IoT botnet saldırılarının potansiyel etkisini ve IoT cihazlarını gelecekteki saldırılara karşı korumanın önemini göstermektedir (einfochips.com 2023). IoT cihazları her yerde yaygınlaştıkça, botnet saldırılarını önlemek ve kişisel verileri ve çevrimiçi hizmetleri korumak için güvenliklerine öncelik vermek kritik hale gelmektedir (a10networks.com 2023). IoT cihazlarındaki botnet'leri tespit etmek, çok sayıda bağlı cihaz, karmaşık ağ trafiği ve botnet saldırılarının evrimi nedeniyle zor olabilir. Bununla birlikte, derin öğrenme teknikleri, IoT cihazlarında botnet'leri yüksek doğrulukla tespit etme konusunda umut vaat etmektedir (Celil vd. 2020, Alissa vd. 2022). Bu yöntemler, ağ trafiğini analiz etmek ve botnet etkinliğiyle ilişkili kalıpları belirlemek için makine öğrenimi algoritmalarını kullanır. Bot ağlarının erken tespiti, siber güvenlik uzmanlarının daha fazla hasarı önlemek ve saldırıların etkisini azaltmak için adımlar atmasını sağlar (Pokhrel vd. 2021, Catillo vd. 2023). Özetle, IoT cihazlarına yönelik botnet saldırılarını önlemek ve azaltmak, sağlam güvenlik önlemlerinin uygulanmasını, cihazların düzenli olarak güncellenmesini ve gelişmiş tespit yöntemlerinin kullanılmasını içeren kapsamlı bir yaklaşım gerektirir. Bağlı cihazların sayısı artmaya devam ettikçe, IoT cihazlarına saldıran botnet tehdidi artmaya devam edecektir (Alani 2022). Bu nedenle, IoT cihazlarını botnet saldırılarından korumak için tetikte olmak ve proaktif önlemler almak son derece önemlidir.

2.7 Anomali Tespiti

Anomali tespiti, beklenen davranış veya kalıplara uymayan gözlemleri veya veri noktalarını belirleme işlemidir (towardsdatascience.com 2023). Bir tür anomali, belirli bir veri noktasında meydana gelen izole bir anomaliyi ifade eden nokta anomalisidir. Bu anomaliler, tüm veri kümesiyle karşılaştırıldığında aykırı değerler olarak kabul edilir

(Hayes ve Capretz 2015). Nokta anormallikleri, verilerin ortalama ve standart sapma gibi istatistiksel özelliklerini inceleyerek ve beklenen aralığın dışında kalan veri noktalarını gözlemleyerek tanımlanabilir (Foorthuis 2021). Başka bir anormallik türü, bir dizi veri noktası içinde meydana gelen toplu bir anormalliktir. Toplu anormallikler, verilerde beklenen davranıştan sapan olağandışı modeller veya eğilimler gözlemlenerek tanımlanır (splunk.com 2023). Bu anormallikler, g gibi veri noktaları arasındaki ilişkilere bakılarak tespit edilebilir. Korelasyon veya kümeleme ve beklenen modellere uymayan veri noktası grupları tanımlanır (Foorthuis 2021). Bağlamsal anomaliler, verilerin analiz edildiği bağlam veya ortam nedeniyle ortaya çıkan başka bir anomali türüdür (Calikus vd. 2022). Koşullu aykırı değerler olarak da bilinen bağlamsal aykırı değerler, aynı bağlamda bulunan diğer veri noktalarından önemli ölçüde farklı olan veri noktalarını içerir (anodot.com 2023). Bu anormallikler, verilerle ilişkili bağlamsal bilgiler (zaman, konum veya kullanıcı davranışı gibi) incelenerek ve beklenen kalıplara uymayan herhangi bir veri noktası belirlenerek tanımlanabilir (Hayes ve Capretz 2015, rapidminer.com 2023). Anomali Tespiti, normal olmayan olay ve davranışları belirlemek ve bunları tanımlamak için kullanılan bir yöntem olarak kabul görebilmektedir. Bahsedilmekte olan bu yöntem, farklı sektörlerde kullanılmakta olup çeşitli anomali tespit yöntemleri bulunduğu bilinmektedir.

3. LİTERATÜR BİLGİLERİ

Bahşi vd. (2018) odak noktası olarak belirledikleri, makine öğrenimi tabanlı IoT botnet algılama yöntemlerinde sadeleştirme yöntemleri kullanmaktır. Bot ağları, kötü amaçlı saldırılar başlatmak için IoT cihazlarının istismar edilebilme tehlikesidir. Hedefleri boyut küçültme algoritmalarının botnet algılama performansını iyileştirme üzerindeki etkisini araştırmaktır. Çalışma, farklı boyut küçültme yöntemlerinin IoT botnet tespiti üzerindeki etkisini değerlendirmekte ve en etkili yöntemleri belirlemektedir. Elde edilen sonuçlar, önerilen boyut küçültme tekniğini kullanan sistemin botnet tespiti için daha yüksek doğruluk, hassasiyet ve özgünlüğe sahip olduğunu göstermektedir. Bu araştırma, boyut küçültme tekniklerini kullanarak IoT botnet tespiti için gelişmiş ve etkili çözümler sağlamaya yönelik önemli bir adım olarak görülebilir.

Alkahtani vd. (2021) Nesnelerin İnterneti (IoT) uygulamalarla ilgili botnet saldırılarının tespiti üzerine CNN-LSTM modellerini kullanmışlardır. Botnet saldırıları, IoT cihazlarının potansiyel saldırı noktaları halindedir. Çalışmalarında CNN-LSTM modelinin, IoT ağ trafiğini analiz ederek anormal davranışları tanımlayabildiği ve botnet saldırılarını başarılı bir şekilde tespit edebildiği sonucuna varmışlardır. Ayrıca, modelin doğruluk, duyarlılık ve yaratıcılık tarafında yüksek puan aldığı görülmüştür. Bu çalışma, IoT uygulamalarına yapılan botnet saldırılarını tespit etmek için yeni bir perspektif sunmakta ve CNN-LSTM modelinin kullanımını vurgulamaktadır.

Segun vd. (2021) IoT uç cihazlarında sıfırıncı gün botnet saldırılarını tespit etmek için birleşik bir derin öğrenme yöntemini incelemişlerdir. Sıfırıncı gün botnet saldırıları, bilinmeyen güvenlik açıklarından yararlanan tehditlerdendir. Hedeflenen, birleşik bir derin öğrenme yaklaşımının IoT uç cihazlarına yapılan botnet saldırılarını tespit etmedeki etkinliğini değerlendirmektir. Araştırma, dağıtık bir öğrenme yöntemiyle uç cihazlardan alınan yerel verileri kullanarak güncel ve doğru bir model oluşturmayı hedeflemektedir. Sonuçlar, ortak derin öğrenme yaklaşımının sıfırıncı gün botnet saldırılarını yüksek doğrulukla tespit etmede başarılı olduğunu göstermiştir. Ayrıca tekniğin uç cihazların mahremiyetini korurken güncelleme ve öğrenme gerçekleştirmek için düşük veri iletişim gereksinimleri sağladığı gözlemlendi. Bu çalışma, IoT uç cihazlarında sıfır gün botnet

saldırılarını tespit etmek için yeni bir yaklaşım önererek birleşik derin öğrenme yaklaşımlarının önemini göstermektedir.

Bacha vd. (2022) anomali tabanlı bir saldırı tespit sistemi geliştirmeyi ve bunun için bir Kernel Extreme Learning Machine yaklaşımında bulunmuşlardır. Anormallikler, IoT sistemlerindeki güvenlik açıklarını ve saldırıları belirlemek için önemli işaretlerdir. Araştırma, Kernel Extreme Learning Machine algoritmalarını kullanarak IoT ortamlarındaki anormallikleri tespit etmeyi amaçlamıştır. Çalışma, yöntemin etkisini ve performansını değerlendirir ve sonuçları analiz eder. Sonuçlar, Kernel Extreme Learning Machine'in IoT ortamındaki anormallikleri yüksek doğrulukla başarılı bir şekilde tespit ettiğini göstermektedir. Bu çalışma, IoT güvenlik alanında yeni bir anormallik algılama yaklaşımı önererek Kernel Extreme Learning Machine yaklaşımının verimliliğini vurgulamaktadır.

Al-Garadi vd. (2020) IoT güvenliği için makine ve derin öğrenme yaklaşımlarını inceleyen bir anket çalışmasıdır. Araştırmada, IoT sistem güvenliği için çeşitli makine ve derin öğrenme yöntemlerine odaklanmışlardır. Örneğin, bu yöntemler güvenlik ihlallerini tespit etmek, saldırıları önlemek ve kötü niyetli davranışları sınıflandırmak için kullanılır. Çalışma, literatürdeki farklı makine ve derin öğrenme yaklaşımlarını analiz etmekte ve bunların IoT güvenliğindeki katkılarını değerlendirmektedir. Sonuçlar, farklı yaklaşımların farklı IoT güvenlik senaryolarında başarıyla kullanılabileceğini ve genel olarak IoT güvenliğine önemli katkılar sağlayabileceğini göstermektedir. Makine ve derin öğrenme yaklaşımlarının IoT güvenliğindeki rolünü ve niteliğini kapsamlı bir şekilde inceleyen bu çalışma, gelecekteki araştırma ve uygulamalar için önemli bir kaynak haline gelmiştir

Alotaibi vd. (2020) Nesnelerin İnterneti ortamındaki siber saldırıları tespit etmek için çeşitli derin öğrenme yöntemlerini incelemişlerdir. Araştırmada, siber saldırıların derin öğrenme yöntemleri kullanılarak tespit edilmesine odaklanmıştır. Çalışma, birden fazla derin öğrenme modelini birleştirerek oluşturulmuş bir model yığınının işlevini ve performansını değerlendirmektedir. Sonuçlar, bu yığılmış derin öğrenme yaklaşımının IoT'deki siber saldırıları yüksek doğrulukla başarılı bir şekilde tespit edebildiğini

göstermektedir. Bu yaklaşımın ayrıca karmaşık saldırı türlerini tespit ettiği ve yanlış pozitif oranını düşük tuttuğu bulunmuş. Sonuç olarak bu çalışma, IoT ortamındaki siber saldırıları tespit etmek için yeni bir yaklaşım önererek derin öğrenme yöntemlerinin başarısını arttırmaktadır.

Zhang vd. (2018) köprü çatlaklarının tespitinde evrişimli sinir ağı modellerinin uygulanmasını araştırmıştır. Araştırmada IoT cihazlarına yerleştirilen sensörlerin veri topladığı ve bu verileri evrişimli sinir ağı modeline girdi olarak kullandığı bir sistemin tasarlandığı görülmektedir. Sonuçlar, yöntemin köprü çatlaklarını yüksek doğrulukla tespit etmede başarılı olduğunu göstermektedir. Ayrıca IoT teknolojisi sayesinde köprünün durumunun sürekli olarak izlenebildiği ve zamanında müdahale edilebildiği tespit edilmiştir.

Okur ve Dener (2020) IoT botnet saldırılarını tespit etmek için makine öğrenimi yöntemlerinin kullanımını incelemektedir. Araştırma, IoT ortamlarında botnet saldırılarını tespit etmeye odaklanmıştır. Ayrıca çeşitli makine öğrenmesi yöntemleri kullanılarak botnet saldırılarını tespit etmeye yönelik bir sistem geliştirilebildiğini göstermiştir. Sonuçlar, bu yöntemlerin botnet saldırılarını tespit etmede etkili olduğunu ve yüksek doğruluk sağladığını göstermektedir. Sistemde kullanılan öznitelik seçme ve sınıflandırma algoritmalarının da tanıma performansını iyileştirdiği görülmüştür.

Meidan vd. (2018) derin otomatik kodlayıcılar kullanarak IoT botnet saldırılarının ağ tabanlı tespitine odaklanmıştır. Bu çalışmanın amacı IoT ortamlarında botnet saldırılarını ağ trafiği analizi ile tespit etmektir. Çalışmada derin otomatik kodlayıcıya sahip bir N-BaIoT (Network-based Internet of Things) modeli geliştirilmiştir. Model, normal ve anormal ağ trafiği dinamiklerini öğrenerek IoT botnet saldırılarını tespit etmeyi amaçlar. Elde edilen sonuçlar, N-BaIoT modelinin yüksek kesinlik ve duyarlılık değerlerine sahip olduğunu göstermektedir. Bu çalışma, IoT botnet saldırılarını tespit etmek için derin otomatik kodlayıcıların ve ağ tabanlı yöntemlerin başarılı bir şekilde uygulandığını vurgulamakta ve güvenliğe önemli katkılar sağlamaktadır.

Mirsky vd. (2018) çevrimiçi siber saldırıları tespit etmeye yönelik bir dizi otomatik

kodlayıcı olan Kitsune yöntemini sunmuştur. Araştırma, otomatik kodlayıcıların toplama modellerini kullanarak İnternet'teki ağ tabanlı saldırıları tespit etmeye yönelik bir yaklaşım sergiliyor. Kitsune, ağ trafiğini gerçek zamanlı olarak analiz etmek ve anormal davranışları tespit etmek için tasarlanmıştır. Elde edilen sonuçlar, Kitsune yönteminin daha yüksek doğruluk ve tespit oranına sahip olduğunu göstermektedir. Ek olarak, düşük yanlış pozitif oranıyla çeşitli saldırı türlerini başarıyla tespit ettiği bulunmuştur. Bu çalışma, bir otomatik kodlayıcı topluluğu olan Kitsune yönteminin çevrimiçi siber saldırıları tespit etmenin etkili bir yolu olduğunu vurgulamaktadır. Bu, siber güvenlik açısından önemli bir adım olarak görülebilir.

Pokhrel vd. (2021) IoT ortamında botnet leri tespit etmek için makine öğrenimi yöntemlerinin kullanımını incelemiştir. Araştırmada, IoT sistemlerinde botnet saldırılarını tespit etmeyi hedeflemişlerdir. Tespite yönelik bir sistem gerçekleştirilmiştir. Sonuçlarında, bu yöntemlerin botnet saldırılarını yüksek doğrulukla etkili bir şekilde tespit edebildiğini göstermektedir. Bu çalışma, bir IoT ortamındaki botnet saldırılarını tespit etmek için makine öğrenimi yöntemlerinin başarılı bir şekilde uygulanmasını vurgulamaktadır.

Naveed vd. (2021) botnet tespiti için otomatik sinir ağı yapı seçiminin nasıl gerçekleştirileceğini araştırmışlardır. Araştırmalarının odak noktası, IoT ortamlarındaki botnet saldırılarını tespit etmek için en etkili sinir ağı mimarisini otomatik olarak seçmektir. Çalışmada, farklı sinir ağı yapıları ve yapı seçim algoritmaları kullanılarak bir otomatik sinir ağı yapı seçim sistemi tasarlanmıştır. Sonuçlar, bu otomatik yapı seçiminin IoT botnet tespitinde önemli bir gelişme sağladığını ve doğruluk oranını artırdığını göstermektedir. Ayrıca bu sistem sayesinde daha iyi performans için sinir ağı yapısının optimize edilebileceği ve algılama yeteneklerinin geliştirilebileceği tespit edilmiştir. Bu çalışma, IoT ortamlarında botnet saldırılarını tespit etmek için otomatik sinir ağı mimarisi seçiminin önemini vurgulamakta ve daha etkili ve verimli tespit yöntemleri sunmaktadır.

Cid-Fuentes vd. (2018) yeni botnet türlerini tespit etmek için uyarlanabilir bir çerçeve sağlamayı amaçlamaktadır. Araştırmaları, botnet saldırılarının hızlı değişimine ve gelişimine uyum sağlayabilecek bir algılama sistemi geliştirmeye odaklanmıştır.

Çalışmalarında çeşitli öznitelik çıkarımı ve makine öğrenimi teknikleri kullanılarak uyarlamalı bir tanıma çerçevesi tasarlanmıştır. Elde edilen sonuçta, uyarlamalı çerçevenin yeni ve bilinmeyen botnet türlerini yüksek doğrulukla başarılı bir şekilde tespit edebildiğini göstermektedir. Bu çalışma, güvenlik uzmanlarının hızla gelişen tehditlere daha etkin bir şekilde yanıt vermesini sağlayan, botnet saldırısı tespitine uyarlanabilir bir yaklaşım sunmaktadırlar.

AsSadhan ve Moura'nın (2014) çalışmadaki amacı, botnet trafiğindeki periyodik davranışı tespit etmek için etkili bir kontrol uçağı trafik analizi yöntemi önermektir. Araştırma, botnet saldırılarını tespit etmede periyodik davranışın önemini vurgulamaya odaklanıyor. Bu çalışmada, kontrol uçağı trafiği analiz edilerek botnet trafiğindeki periyodik kalıpları tespit etmek için etkili bir yöntem geliştirilmiştir. Elde edilen sonuçlar, yöntemin botnet trafiğindeki periyodik davranışları tespit etmedeki yüksek başarı oranını ve etkinliğini göstermektedir. Ayrıca yöntemin geleneksel yöntemlere göre daha etkili olduğu, botnet saldırılarının daha hızlı ve daha doğru tespit edilmesini sağladığı görüldü. Bu çalışma, kontrol düzlemi trafik analizine dayalı botnet saldırısı tespitine yeni bir yaklaşım sunarak güvenlik uzmanlarının saldırıları daha etkili bir şekilde önlemesine yardımcı olur. Araştırmacılarımızın bu çalışması, botnet saldırılarında periyodik kalıpları tespit etmek için daha etkili araçlar sağlayarak sektöre benzersiz bir katkıdır.

Alauthman vd. (2020) etkili bir pekiştirmeli öğrenmeye dayalı botnet algılama yöntemi önermektedir. Çalışmanın odak noktası, botnet saldırılarını tespit etmek için takviyeli öğrenme yöntemleri kullanmanın önemini vurgulamaktadır. Bu çalışmada verilen özelliklerden yola çıkılarak pekiştirmeli öğrenme modeli tasarlamışlardır. Sonuçlar, yöntemin botnet saldırılarını yüksek doğrulukla tespit etmek için etkili bir şekilde kullanılabileceğini göstermektedir. Çalışma, güvenlik uzmanlarının saldırıları daha verimli bir şekilde tespit etmesine yardımcı olabilecek, botnet saldırısı tespitine yönelik takviyeli öğrenmeye dayalı bir yaklaşım sunmaktadır.

Mathur vd. (2018) ağ trafiğini inceleyerek botnet'leri tespit etmek için klasik çözümlerin dışında bir öneri sunmayı hedefliyor. Çalışmanın odak noktası olarak botnet saldırılarını tespit etmek için ağ trafiğini analiz etmenin önemini vurgulamak olduğu

söylenebilmektedir. Bu araştırmada, ağ trafiğini analiz etmek ve botnet saldırılarını tespit etmek için bir yöntem geliştirilmiştir. Verilere dayanarak, yöntemin botnet saldırılarını yüksek doğrulukla tespit etmek için etkili bir araç olduğu görülmektedir. Ayrıca ağ trafiği analiz edilerek botnet saldırılarının daha doğru sınıflandırılabileceği ve yanlış pozitif oranının azaltılabileceği tespit edilmiştir. Bu makale, güvenlik araştırmacılarının saldırıları daha etkili bir şekilde tespit etmesine yardımcı olmak için ağ trafiği keşif tekniklerine odaklanmış bir botnet saldırı tespit yöntemi sunmaktadır.

Satılmış ve Akleylek (2021) makine öğrenimi ve derin öğrenme modellerinin IoT cihazlarındaki güvenlik açıklarının ortadan kaldırılmasındaki sonuçlara yoğunlaşmışlardır. Çalışmada, farklı makine öğrenimi ve derin öğrenme modellerine kapsamlı bir genel bakış sunar. Sonuçlar, bu modellerin IoT güvenliği alanında önemli bir rol oynadığını ve çeşitli güvenlik tehditlerini etkili bir şekilde tespit edip bunlara karşı koyabildiğini göstermektedir. Ayrıca bu inceleme, IoT güvenliği için makine öğrenimi ve derin öğrenme modellerinin farklı uygulama senaryolarında nasıl kullanıldığını ve ne gibi avantajlara sahip olduğunu gösterir. Bu çalışma, IoT güvenliği alanındaki araştırmalara genel bir bakış sunar ve güvenlik uzmanlarına ve bu alanda yoğun araştırmalar sunanlara daha iyi bir anlayış kazanmalarına yardımcı olur. Araştırmacılar tarafından hazırlanan bu inceleme, alanında özgün bir kaynak olarak kabul edilebilir ve IoT güvenliği için makine öğrenimi ve derin öğrenme modellerinin yararını vurgulamaktadır.

Satılmış ve Akleylek (2021), IoT cihazlarındaki güvenlik açıklarının giderilmesinde makine öğrenimi ve derin öğrenme modellerine ağırlık vermiştir. Çalışmada, bu modellerin çeşitli güvenlik risklerini güçlü bir şekilde belirleyerek karşı koyabildiği ve IoT cihazları güvenliği için farklı yöntem senaryolarında nasıl kullanıldığına dair geniş bir bakış sunmuşlardır. Bu araştırma, IoT güvenliği alanında yapılan çalışmalara geniş bir bakış sunulurken, makine öğrenimi ve derin öğrenme modellerinin güvenlik uzmanlarına sağladığı avantajları ve katkıları belirtmektedirler.

Vinayakumar vd. (2020) IoT ağlarındaki botnet saldırılarını tespit etmede derin öğrenme tekniklerinin etkinliğini vurgulamayı amaçlamışlardır. Çalışmalarında görselleştirme

yöntemleri ile derin öğrenme algoritmalarını birleştiren bir botnet tespit sistemi geliştirilmiştir. Elde edilen bulgular, sistemin IoT ağlarındaki botnet saldırılarını yüksek doğrulukla başarılı bir şekilde tespit ettiğini göstermektedir. Sistemin ayrıca görselleştirme yetenekleri nedeniyle saldırı analizi ve takibinin daha iyi anlaşılmasına izin verdiği görülmüştür. Çalışmada, akıllı şehir IoT ağlarındaki botnet saldırılarını tespit etmek için derin öğrenmeye dayalı bir yaklaşım sunmakta ve güvenlik profesyonellerinin saldırılara daha etkin bir şekilde yanıt vermesine yardımcı olmaktadır. Sonuç olarak, alanında özgün bir katkı olup, IoT ağlarında botnet saldırılarını tespit etmek için yeni bir görselleştirme sistemi sunmaktadır.

Anthi vd. (2019) yapmış oldukları bu çalışmasında denetimli öğrenme algoritmasından yararlanarak bir izinsiz giriş tespit sistemi geliştirmişlerdir. Elde edilen sonuçlar, sistemin akıllı ev IoT cihazlarının sızmasını yüksek doğrulukla başarıyla karşıladığını göstermektedir. Ayrıca, sistemin güvenlik olaylarını analiz etmek ve güvenlik ihlallerini tespit etmek için etkili bir araç olduğu kanıtlanmıştır. Bu çalışma, akıllı ev IoT cihaz güvenliği için, kullanıcıların güvenlik açıklarını daha etkili bir şekilde tespit etmesine yardımcı olabilecek, öğrenme tabanlı bir denetimli penetrasyon tespit sistemi sunmaktadır.

Shafiq vd. (2020) IoT ağlarında kötü amaçlı bot IoT trafiğini tespit etmede makine öğrenimini kullanmayı amaçlamışlardır. Çalışmada CorrAUC adlı bir yöntem, trafiğin özelliklerini analiz etmek için geliştirilmiştir. Elde edilen bulgular, yöntemin IoT ağlarındaki kötü amaçlı bot IoT trafiğini yüksek doğrulukla başarıyla tespit ettiğini göstermektedir. Ayrıca, CorrAUC'nin diğer trafik analiz yöntemlerine kıyasla daha etkili olduğu ve yanlış pozitif oranlarını azalttığı bulunmuştur. Yapılan bu çalışma, güvenlik araştırmacılarının saldırıları daha verimli bir şekilde tespit etmesine yardımcı olabilecek, IoT ağlarındaki kötü amaçlı bot IoT trafiğini tespit etmeye yönelik makine öğrenimi tabanlı bir yöntem olan CorrAUC'yi sunmaktadır.

Eskandari vd. (2020) Passban IDS adlı bir izinsiz giriş tespit sistemi geliştirdiler. Elde edilen sonuçlar, sistemin IoT uç cihaz penetrasyonlarına yüksek tespit oranı ile başarılı bir şekilde karşı koyduğunu göstermektedir. Ayrıca Passban IDS'nin normal davranışı

modellemek ve anormallikleri tespit etmek için zekâ tabanlı algoritmalar kullanarak daha etkili olduğu bulundu. Bu çalışma, güvenlik uzmanlarının daha etkili saldırı önlemleri almasına yardımcı olabilecek, IoT uç cihazlarındaki sızma olaylarını tespit etmek için anomali tabanlı bir akıllı algılama yöntemi olan Passban IDS'yi sunmaktadır.

Al Shorman vd. (2020) denetimsiz öğrenme yöntemlerinin IoT ağlarındaki botnet saldırılarını tespit etmedeki etkileri üzerine bir çalışma yapmışlardır. Çalışmada, tek sınıflı destek vektör makinesi ve gri kurt optimizasyon algoritması birleştirilerek akıllı bir sistem tasarlanmıştır. Sonuçlarda, sistemde kullanılan denetimsiz öğrenme yönteminin IoT botnetlerini yüksek doğrulukla başarılı bir şekilde tespit ettiğini göstermektedir. Bu çalışma, IoT ağlarına yapılan botnet saldırılarını tespit etmek için katılımsız, zekaya dayalı bir yaklaşım sunmakta ve güvenlik uzmanlarının saldırıları daha verimli bir şekilde tespit etmesine yardımcı olmaktadır. Bu çalışma, IoT botnet'lerini tespit etmek için yeni bir akıllı sistemi ortaya çıkaran, alana özgün bir katkıdır.

Alkahtani ve Aldhyani (2021) CNN (Convolutional Neural Network) ve LSTM (Long Short Term Memory) modellerini birleştiren bir botnet saldırı tespit modeli geliştirdiler. Sonuçlar, modelin IoT uygulamalarında botnet saldırılarını yüksek doğrulukla başarılı bir şekilde tespit ettiğini göstermektedir. Ayrıca CNN ve LSTM kombinasyonundan dolayı modelin zamansal örüntüleri ve detaylı öznitelikleri etkin bir şekilde analiz edebildiği de bulunmuştur. Bu çalışma, güvenlik araştırmacılarının saldırıları daha verimli bir şekilde tespit etmesine yardımcı olabilecek, IoT ortamlarındaki botnet saldırılarını tespit etmek için derin öğrenmeye dayalı bir model olan CNN-LSTM'yi sunmaktadır.

Shareena vd. (2021) IoT ortamlarında botnet saldırılarını tespit etmek için derin öğrenme yöntemlerini kullanmışlardır. Bu çalışmada, derin sinir ağları ve öznitelik çıkarma teknikleri kullanılarak bir penetrasyon tespit sistemi geliştirilmiştir. Sonuçlar, sistemin IoT botnet saldırılarını yüksek doğrulukla başarılı bir şekilde tespit ettiğini göstermektedir. Ayrıca, derin öğrenme yöntemlerinin, saldırıları algılamak ve sınıflandırmak için karmaşık özellikleri etkili bir şekilde analiz ettiği bulunmuştur. Bu çalışmada, güvenlik araştırmacılarının saldırıları daha etkin bir şekilde tespit etmesine yardımcı olmak için Nesnelerin İnterneti ortamında derin öğrenme tabanlı bir botnet

saldırı tespit sistemi sunulmuştur.

Liu vd. (2021) bu alanda, IoT veri kümesi CCD-INID-V1'de gömülü özellik seçimi ve sınıflandırma için CNN'leri kullanmayı amaçlar. Araştırma, IoT veri setlerinde gömülü özellik seçiminin ve CNN modellerinin sınıflandırılmasının kullanılabilirliğini vurgulamaya odaklanmaktadır. Bu çalışmada CCD-INID-V1 veri setine gömülü özellik seçme yöntemi uygulanmış ve elde edilen önemli özellikler kullanılarak bir CNN modeli eğitilmiştir. Sonuçlar, yöntemin CCD-INID-V1 veri setinde yüksek sınıflandırma doğruluğu sağladığını ve özellik seçimi yoluyla CNN modellerinin performansını iyileştirdiğini göstermektedir. Ayrıca gömmelerin öznitelik seçimi sayesinde gereksiz özniteliklerin azaldığı ve modelin örüntüleri daha iyi tanıyabildiği görülmüştür. Bu çalışma, IoT veri kümelerinde gömülü özellik seçimi ve CNN modelleri kullanarak sınıflandırma performansını iyileştirmek için kendine özgü bir yaklaşım sergilemektedir.

Hwang vd. (2019) otomatik kodlayıcılar ve evrişimli sinir ağları kullanarak Nesnelerin İnternetindeki kötü niyetli trafiği tespit etmeyi hedeflemişlerdir. Hedefledikleri çalışmalarına otomatik kodlayıcı ve evrişimli sinir ağı modeli kullanılarak bir algılama sistemi olarak yansımaktadır. Geliştirdikleri modelleri, IoT trafiğinin özelliklerini çıkararak normal trafiği kötü amaçlı trafikten ayrıştırmışlardır. Sonuçlar, yöntemin IoT ortamındaki kötü amaçlı trafiği yüksek doğrulukla başarılı bir şekilde tespit ettiğini göstermektedir. Ayrıca, otomatik kodlayıcı ve evrişimli sinir ağı modelinin kombinasyonu sayesinde, derin özniteliklerin etkin bir şekilde analiz edilebildiği ve kötü amaçlı trafik kalıplarının tespit edilebildiği bulunmuştur. Bu araştırma, güvenlik uzmanlarının kötü amaçlı trafiği daha etkili bir şekilde tespit etmesine yardımcı olabilecek benzersiz bir IoT güvenliği yaklaşımı sunmaktadır.

Reddy ve Shyam (2022) güvenli bir SaaS çerçevesine dayalı bir sistem geliştirilmiştir. Sistem, ağ trafiğini analiz etmek ve saldırıları tespit etmek için çeşitli makine öğrenimi algoritmaları kullanır. Sonuçlar, bu yaklaşımın saldırıları etkili bir şekilde tespit edip etkisiz hale getirebileceğini gösteriyor. Ayrıca, güvenli bir SaaS çerçevesi kullanmanın sistem güvenliğini iyileştirdiği ve daha güçlü saldırı savunma yetenekleri sağladığı bulundu. Bu araştırma, güvenli bir hizmet olarak sunulan yazılım çerçevesi ile saldırı

algılama ve önleme için makine öğrenimi tabanlı bir yaklaşımı birleştirerek bilgi güvenliği alanında önemli bir katkı sağlamaktadır. Bu çalışma, güvenliğin önemli olduğu SaaS tabanlı sistemler için etkili bir çözüm sunmaktadır.

Savic vd. (2021) elde ettikleri bu yöntemin hücresel IoT sistemlerindeki anomalileri başarıyla tespit ettiğini ve lojistik uygulamalarda etkin bir şekilde kullanılabileceğini göstermişlerdir. Bu çalışma derin öğrenme tekniklerinin hücresel IoT sistemlerindeki anormallikleri tespit etmek için güçlü araçlar olduğunu göstermektedir. Bu araştırma, akıllı lojistik endüstrisinde verimliliği artırmaya ve sorunları hızla keşfetmeye yönelik önemli bir adımdır. Araştırmacıların çalışması, bu alanda aykırı bir görüş sunuyor ve hücresel IoT sistemlerindeki anormallikleri tespit etmek için önemli bir bilgi kaynağı olarak kabul edilebilir.

Mahfouz vd. (2020) faaliyetlerinde, kolektif sınıflandırıcılarının yeni siber saldırı kayıtlarındaki performansını değerlendirmeyi hedeflemiştir. Deneysel çalışmalar, kolektif sınıflandırıcıların siber saldırıları başarılı bir şekilde tespit etmede etkili olduğunu göstermektedirler. Ayrıca, yeni veri setinin diğer mevcut veri setlerinden farklı özelliklere sahip olduğu ve bu veri setindeki kolektif sınıflandırıcısının daha iyi performans gösterdiği görülmüştür. Araştırmacıların çalışmalarında, kolektif sınıflandırıcıların siber saldırılara karşı etkili olabileceğini göstermişlerdir. Bu çalışma, yeni veri seti kullanılarak elde edilen sonuç ve analizlerle benzer diğer çalışmalardan farklılık göstermektedir.

Alotaibi ve Alotaibi (2020) üzerinde yoğunlaştıkları, IoT cihazlarındaki siber saldırıları tespit etmek için birçok derin öğrenme yöntemi kullanılmaktadır. Araştırmanın odak noktası, derin öğrenme modellerini birbirine bağlayarak oluşturulan yığın yapısının siber saldırıları tespit etme performansını artırabileceği üzerine odaklanmaktadır. Deneysel çalışmalar, bu yaklaşımın IoT ağlarındaki siber saldırıları etkili ve başarılı bir şekilde tespit edebildiğini göstermektedir. Ayrıca yığınlı derin öğrenme modellerinin tek başına kullanılan derin öğrenme modellerine göre daha iyi sonuçlar verdiği görülmüştür. Araştırmacılarımızın çalışması, IoT güvenliği alanında ileriye doğru atılmış önemli bir adımdır ve derin öğrenme model yığınlarının siber saldırıları tespit etmek için güçlü

araçlar olduğunu gösterir. Bu çalışmanın benzersiz özgünlüğü, onu derin öğrenme ve IoT güvenliği alanındaki diğer çalışmalardan önemli kılmaktadır. Araştırmacıların çalışması, IoT ağlarını siber saldırılardan korumanın yeni bir yolunu daha sunmakta ve bu alanda daha fazla araştırmaya ışık tutmaktadır.

4. MATERYAL ve METOT

4.1 Veri Kümesi

Çalışmada kullanılan veri seti, Meidan ve ark. (Meidan vd. 2018) tarafından oluşturulan N-BaIoT, akademik çalışmalar için açık erişime sahip IoT cihazlarına yapılan botnet saldırılarını tespit etmek için kullanılan genel bir veri setidir.

Ağ trafiği, 2 botnet tarafından taşınan 10 IoT cihazına, 9 saldırı sınıfına ve 1 iyi huyluya aittir. IoT'ler bir termostat, bebek monitörü, web kamerası, iki farklı kapı zili ve dört farklı ucuz güvenlik kamerasından oluşur. Danmini (Kapı Zili), Ecobee (Termostat), Ennio (Kapı Zili), Philips_B120N10 (Bebek Monitörü), Provision_PT_737E (Güvenlik Kamerası), Provision_PT_838 (Güvenlik Kamerası), Samsung_SNH_1011_N (Web Kamerası), SimpleHome_XCS7_1002_WHT (Güvenlik Kamerası), SimpleHome_XCS7_1003_WHT(Güvenlik Kamerası), kötü huyluydu. Bu özel ağ, güvenlik kameralarından birine gerçek bir Mirai botnet kötü amaçlı yazılım örneği bulaştırılarak oluşturuldu (Mirsky vd. 2018).

Mirai, çoğunlukla ağa bağlı akıllı ev ve tüketici cihazlarını hedefleyen ve onları uzak botlardan oluşan bir zombi ağına dönüştürebilen kötü amaçlı bir yazılımdır (Antonakakis vd. 2017). 2016 yılındaki en büyük dağıtılmış hizmet reddi (DDoS) saldırısı Mirai botnet tarafından gerçekleştirildi. IoT kullanan cihaz sayısının giderek artacağı öngörüldüğünde Mirai botnet tespiti önemlidir (Ryu ve Yang 2018).

Sınıflandırmaya dayalı temel özellikler, akış trafiğini özetleyen bilgiler, trafiğin titremesini özetleyen bilgiler, zaman çerçevesi bilgileri, son zamanlarda ortaya çıkan öğelerin sayısı ve iki akışın varyanslarıdır. Veri seti 165645 örnekten oluşurken, sınıflandırmaya esas olan öznitelik sayısı 115'tir.

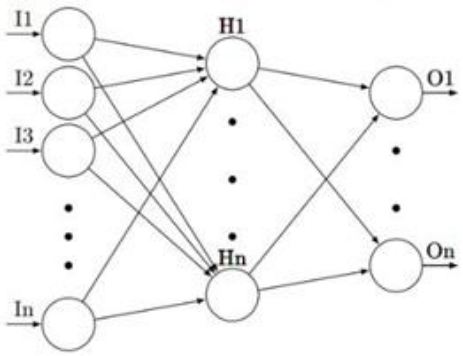
İyi huylu trafik IoT cihazları arasında farklılık gösterebilse de kötü amaçlı saldırı trafiğiyle karşılaştırıldığında fark edilir derecede düşük kalır. Bu durum bütün cihazların trafik dağılımı Çizelge 4.1'de verilmiştir.

ID	Adı	Cihaz Türü	Cihaz Başına Trafik
0	benign	Bütün Cihazlar	555932
1	Danmini	Kapı Zili	968750
2	Ecobee	Termostat	822763
3	Ennio	Kapı Zili	316400
4	Philips_B120N10	Bebek Monitörü	923437
5	Provision_PT_737E	Güvenlik Kamerası	766106
6	Provision_PT_838	Güvenlik Kamerası	738377
7	Samsung_SNH_1011_N	Web Kamerası	323072
8	SimpleHome_XCS7_1002_WHT	Güvenlik Kamerası	816471
9	SimpleHome_XCS7_1003_WHT	Güvenlik Kamerası	831298

Çizelge 4.1 Bütün Cihazların Trafik Dağılımı.

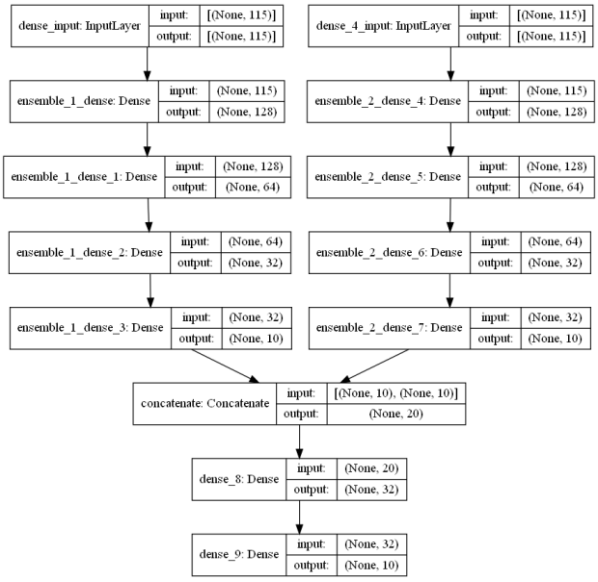
4.2 Önerilen Yöntem

Makine öğrenimi, büyük veri kümelerinden yararlı bilgileri otomatik olarak bulan kullanışlı bir yapay zekâ tekniğidir. Derin öğrenme, makine öğreniminin bir dalıdır (Liu ve Lang 2019). Pek çok güvenlik alanı olduğu için makine öğrenimi bu alan için önemlidir. Botlar, normal akışlardan farklı akışlar üretir. Bu şekilde, makine öğrenimi (Kolektif sınıflandırıcı algoritmaları) akışları en yüksek doğrulukla sınıflandırabilir (Algelal vd. 2020). Botnet'i tespit etmek için makine öğrenimini kullanmak daha mantıklı görünüyor (Rezai 2021). Derin sinir ağları (DNN), I girişi olan bir f fonksiyonunun yakınsamasını O değerine eşleyerek en iyi yaklaşımı sağlayan parametreleri öğrenir. Bilgi, I'den başlayarak hesaplanan fonksiyon boyunca akar, ara hesaplamalar ile f fonksiyonundan geçer ve O'nun çıktı değerine ulaşır. Modelin çıktısında kendisine beslenen geri bildirim bağlantıları yoktur. f(I)=f3(f2(f1(I))) modeli bir zincir gibi birbirine bağlı fonksiyonlardan oluşabilir. Bu durumda f1 ağın birinci katmanını, f2 ise ağın ikinci katmanını oluşturur. Tüm zincirin uzunluğu desenin derinliğini verir. Derin bir sinir ağında derinlik kavramının geldiği yer burasıdır. Yapay sinir ağının giriş ve çıkış katmanları arasındaki katmanlar gizli katmanlardır. Gizli katmanların boyutları modelin genişliğini verir. Derin sinir ağının son katmanı çıkış katmanını verir (Goodfellow vd. 2016). Örnek DNN yapısı Resim 4.2.1'de verilmiştir.



Resim 4.2.1 Örnek DNN Mimarisi.

Kolektif öğrenme, modeli birden fazla öğrenciyle oluşturmaya izin veren öğrenmedir. Modellerin problemin çözümünde daha doğru kararlar vermesini amaçlar. Boosting, Bagging, Stacking, Voting gibi farklı kolektif öğrenme teknikleri vardır. Çalışmada yığınlama takımı kullanılmıştır (Rokach 2010). Yığınlama, birkaç sınıflandırıcının tahminlerini birleştirerek farklı bir sınıflandırıcının eğitilmesini içerir. İlk aşamada mevcut veriler sınıflandırıcılar ile eğitilir. Daha sonra, birinci aşama algoritmalarının tahminlerini ek girdiler olarak kullanarak nihai bir meta-öğrenci algoritması ile eğitilir (Wolpert 1992). Çalışmanın tüm kodları açık kaynak kodlu Python ortamında geliştirilmiştir. Veri setinin %70'i eğitim için, %30'u test için ayrılmıştır. Önerilen kolektif modeli, daha önce diyabet tespitinde başarılı olan model temelinde geliştirilmiştir (Yurttakal ve Baş 2021). Önerilen modelin mimari yapısı Resim 4.2.2'te verilmiştir.



Resim 4.2.2 Önerilen Model.

İlk aşamada 2 adet DNN modelinden çıktı tahmin değerleri alınmıştır. Bu aşamada kullanılan modelin nöron sayıları 128-64-32-10'dur. Ara katmanların aktivasyon fonksiyonu ReLu iken, çıkış katmanının aktivasyon fonksiyonu Softmax'tir. Meta Learner aşamasında kullanılan DNN yapısında 32-10 olmak üzere iki katman kullanılmıştır. Birinci aşamada kullanılan modellerin öğrenilebilir parametre sayısı 25514 iken tüm modelin toplam öğrenilebilir parametre sayısı 52030 dur.

5. BULGULAR

5.1 Performans Metrikleri

Sınıflandırma süreçlerinde tahmin edilen değerleri gerçek verilerle karşılaştırmak için karışıklık matrisi kullanılır. Geliştirilen modelin performans metrikleri de karışıklık matrisi kullanılarak elde edilmiştir. Karışıklık matrisi Çizelge 5.1.1'de verilmiştir.

		Gerçek Değerler	
		Pozitif	Negatif
Tahmin Edilen Değerler	Pozitif	TP	FP
	Negatif	FN	TP

Çizelge 5.1.1 Karışıklık Matrisi.

Karışıklık matrisinde, verilen terimler çeşitli metrikleri hesaplamak için kullanılabilir. Değerlendirmede kullanılan metriklerin formülleri aşağıda Çizelge 5.1.2'de eşitliklerde verilmiştir.

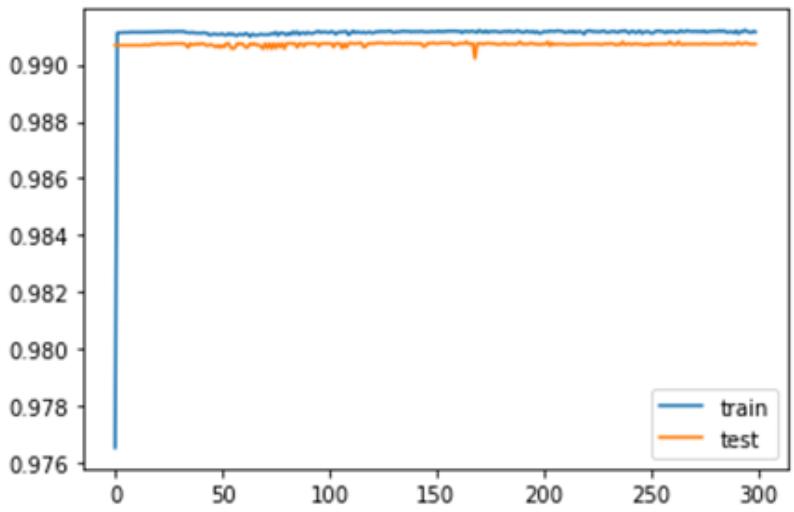
Duyarlılık	TP / (TP + FN)
Kesinlik	TP / (TP + FP)
Doğruluk	(TP + TN) / (P + N)
F1 Skoru	2TP / (2TP + FP + FN)

Çizelge 5.1.2 Metriklerin Formülleri.

5.2 Performans Sonuçları

Doğruluk - epoch ilişkisini temsil eden bir grafik, makine öğrenimi modelinin zaman içinde nasıl performans gösterdiğinin görsel bir yansımasıdır. Grafik, epoch (dönem) olarak adlandırılan eğitim yinelemelerinin sayısına dayalı olarak modelin doğruluk düzeyini gösterir (Altun vd. 2023). Makine öğrenimi modellerinin performansını değerlendirmek ve iyileştirilecek alanları bulmak için vazgeçilmez bir araçtır (Qurashi ve Holmes 2019). Doğruluk - epoch grafiği, makine öğrenimi uzmanlarının modellerinin performansını doğru bir şekilde yorumlamalarına yardımcı olan çok önemli bir öğedir. Grafiği inceledikten sonra, modelin en yüksek doğruluğuna ne zaman ulaştığını belirleyebilir ve daha fazla eğitim yinelemesinin gerekli olup olmadığına karar

verebilirler. Ayrıca, doğruluk - epoch grafiği, farklı modellerin performansını karşılaştırmak ve belirli bir görev için en uygun olanı seçmek için kullanılabilir (Anwar vd. 2022). Sonuç olarak, doğruluk - dönem grafiği, makine öğrenimi modellerinin verimliliğini ve kesinliğini artırmada önemli bir yere sahiptir. Modelin zaman içindeki performansının grafiksel gösterimi, uygulayıcıların eksiklikleri belirlemesi ve verilere dayalı bilinçli kararlar alması için bir kılavuz görevi görür. Bu nedenle, doğruluk - epoch grafiğinin yorumunu ve kullanımını anlamak, modelinin etkinliğini artırmak isteyen herhangi bir makine öğrenimi uzmanı için gerekli bir adımdır (Altun vd. 2023). Çalışmamızda birinci katmandaki ağlar 500 epoch çalıştırılırken, Stacked Kolektif modeli 300 epoch çalıştırılmıştır. Optimize edici olarak Adam Optimizer kullanıldı. Eksik işlev, kategorik çapraz entropidir. Resim 5.2.1 3, eğitim süreci için doğruluk dönemi grafiğini gösterir

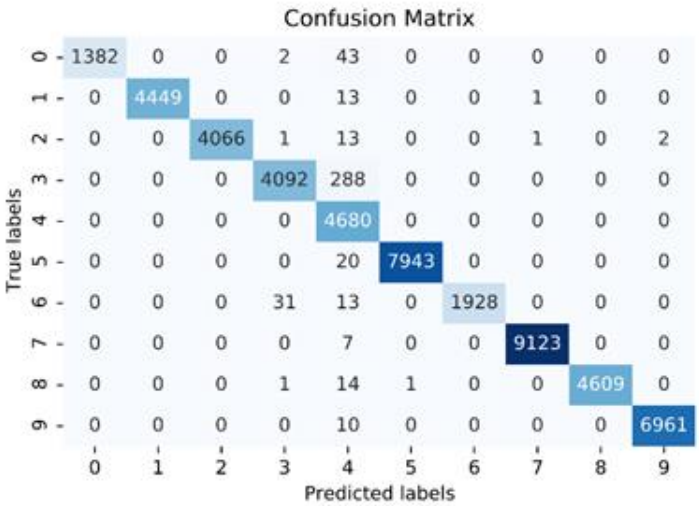


Resim 5.2.1 Doğruluk - Epoch Grafiği.

Bir makine öğrenimi modelinin verimliliğini değerlendirmek için karışıklık matrisi olarak bilinen bir tablo kullanılır. Bu matris, model tarafından üretilen tahmini değerleri test verilerinin gerçek değerleri ile yan yana getirerek, modelin gerçek pozitifler, gerçek negatifler, yanlış pozitifler ve yanlış negatifler açısından performansına genel bir bakış sunar. Gerçek pozitifler, modelin bir koşulun veya özelliğin varlığını doğru bir şekilde tanımladığı durumları gösterirken gerçek negatifler, modelin bir koşulun veya özelliğin eksikliğini doğru bir şekilde tanımladığı durumları gösterir. Yanlış pozitifler, modelin bir

koşulun veya özelliğin varlığını yanlış bir şekilde tanımladığı durumlardır, yanlış negatifler ise modelin bir koşulun veya özelliğin eksikliğini yanlış bir şekilde tanımladığı durumları gösterir (sciencedirect.com 2023). Makine öğreniminde, karışıklık matrisi, bir modelin etkinliğinin kapsamlı bir şekilde değerlendirilmesine izin veren önemli bir araçtır. Geliştiricilere, modelin kesinliğini, hatırlamasını, F1 puanını ve doğruluğunu ölçmek için bir araç sağlar (v7labs.com 2023). Bu ölçümler, modelin etkinliğini değerlendirmede ve iyileştirme gerektiren yönleri belirlemede çok önemlidir. Belirli bir sınıfa yönelik bir önyargıya sahip olabileceğinden, yüksek bir doğruluk puanının iyi bir performans garantisi olmadığına dikkat etmek önemlidir (towardsdatascience.com 2023). Bu nedenle, karışıklık matrisini yorumlamak, bir modelin zayıf ve güçlü yanlarını anlamak için esastır. Etkili bir model, yüksek oranlarda gerçek pozitif ve gerçek negatiflere sahip olurken, yüksek yanlış pozitif ve yanlış negatif oranları, modelin iyileştirme kullanabileceği alanları gösterir (guru99.com 2023). Karışıklık matrisi, makine öğreniminde bir modelin performansına ilişkin anlamlı bilgiler sunan ve geliştiricilerin bilinçli karar vermesini sağlayan paha biçilmez bir araçtır.

Verilen resme göre eğitim ve test gruplarının eğitim süreçleri birbiriyle uyumludur. Bu durum, modelin eğitiminde aşırı uyum olmadığını ve önerilen modelin genelleme kapasitesinin yüksek olduğunu göstermektedir. Resim 5.2.2'te test setinin karışıklık matrisi verilmiştir.



Resim 5.2.2 Test Seti Karışıklık Matrisi.

Şekle göre, örneklerin çoğu doğru tahmin edilmiştir. Doğruluk, kesinlik, duyarlılık, F1 puanı performans ölçütleri sırasıyla 0,99, 0,991, 0,986, 0,988'dir. Her sınıf için ayrı ayrı hesaplanan performans metrik değerleri Çizelge 5.2'te verilmiştir.

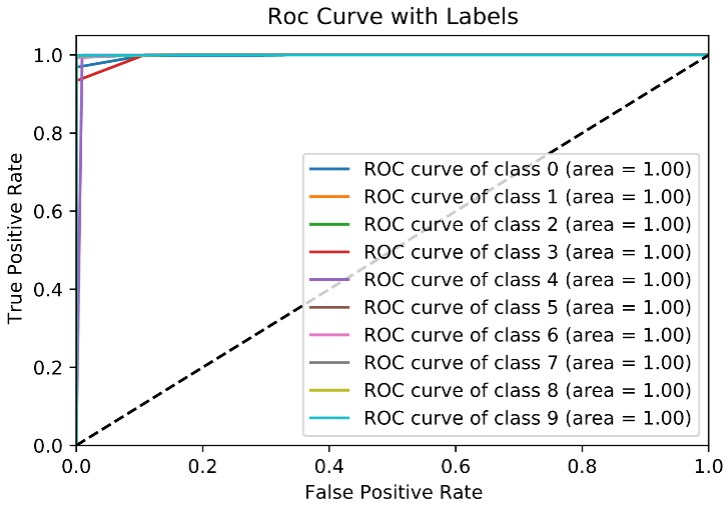
Çizelge 5.2 Performans Metrikleri.

Sınıf	Kesinlik	Duyarlılık	F1 Skoru	Örnek Sayısı
0	1.00	0.97	0.98	1427
1	1.00	1.00	1.00	4463
2	1.00	1.00	1.00	4083
3	0.99	0.93	0.96	4380
4	0.92	1.00	0.96	4680
5	1.00	1.00	1.00	7963
6	1.00	0.98	0.99	1972
7	1.00	1.00	1.00	9130
8	1.00	1.00	1.00	4625
9	1.00	1.00	1.00	6971

Elde edilen sonuçlara göre en düşük 0,96 F1 skoru 3 olarak kodlanan kapı zili ve 4 olarak kodlanan bebek telsizinin kötü huylu ağ trafiğinde elde edilmiştir.

Bir ikili sınıflandırıcı sistemin teşhis yeterliliği, ROC (alıcı çalışma özelliği) eğrisi aracılığıyla görsel olarak tasvir edilir. Bu eğri, y ekseninde gerçek pozitif oranı (TPR) veya duyarlılığı ve x ekseninde yanlış pozitif oranı (FPR) veya 1-özgünlüğü gösterir. ROC eğrisi, farklı teşhis testlerinin veya sınıflandırıcıların yeteneklerini, iki sınıf arasında ayrım yapma yetenekleri açısından incelemeye ve karşılaştırmaya hizmet eder. ROC eğrisi altındaki alanın değeri (AUC), sınıflandırıcı performansını değerlendirmek için sıklıkla kullanılan bir ölçüdür. AUC için 0,5 değeri rastgeleliği, 1,0 değeri ise mutlak kesinliği gösterir. Bir ROC eğrisi oluşturma süreci, zaten oluşturulmuş sınıf etiketlerine sahip bir grup veri noktasına bir sınıflandırıcı uygulamayı içerir. Buradan, akla gelebilecek her karar eşiği için hem gerçek pozitif oranı (TPR) hem de yanlış pozitif oranı (FPR) hesaplanır. Elde edilen bu TPR ve FPR çiftleri daha sonra ayrı noktalar olarak ROC eğrisi üzerine çizilir. ROC eğrisindeki köşegen çizgi, rastgele bir sınıflandırıcının performansını temsil eder (online.stat.psu.edu 2023). TPR'yi maksimize eden ve FPR'yi minimuma indiren eğri üzerindeki noktayı seçerek, bir sınıflandırıcı için en uygun karar eşiğini belirlemek için ROC eğrisi kullanılabilir (acutecaretesting.org 2023).

Resim 5.2.3 her bir etiket için ROC eğrisini göstermektedir. Sonuçlar, her bir etiket için AUC değerinin %100'e yakın olduğunu göstermektedir.



Resim 5.2.3 ROC Eğrisi.

6. TARTIŞMA ve SONUÇ

Dijital dönüşüm çağında IoT, hiç şüphesiz hem kurumların hem de bireylerin hayatında devrim yaratan teknolojilerin başında geliyor. IoT, bir IP adresine sahip olan, internete bağlanan ve birbirleriyle veri paylaşan fiziksel cihazların haberleşmesidir. Bu teknoloji sanayi devriminin kilit noktası olmakla birlikte akıllı ev, akıllı tarım ve akıllı sağlık uygulamalarında da sıklıkla kullanılmaktadır. Birbirleriyle iletişim kuran IoT cihazları, ağlar için güvenlik tehdidi oluşturabilir. Görünüşte basit bir cihaz bile saldırganlar tarafından ele geçirildiğinde ciddi tehlikeler oluşturabilir. Örneğin, bir bilgisayar korsanı tarafından yakalanan bir bebek kamerası casusluk için kullanılabilir. Saldırganlar ağ hizmetlerini bozabilir, verileri çalabilir, fiziksel zarara neden olabilir ve hatta insanlara zarar verebilir. Botnet, IoT cihazları için en büyük tehditlerden biridir. Bu nedenle yapay zekâ tabanlı botnet tespiti üzerine birçok çalışma yapılmıştır. Botnet, IoT cihazları için en büyük tehditlerden biridir. Bu nedenle yapay zekâ tabanlı botnet tespiti üzerine birçok çalışma yapılmıştır. Ahmetoğlu ve Daş (2019), tam bağlantılı bir yapay sinir ağı ile iyi huylu, FTP patator, SSH-patator, DoS, Heartbleed, Brute Force, Web Attack–SQL Injection, DDOS, Port attack, Botnet saldırı tiplerini tespit etmeye çalışmışlardır (Ahmetoğlu ve Daş 2019). Wai ve ark. (2018), makine öğrenimine dayalı bir botnet trafiği algılama tekniği önerdi. Araştırmaları, otomatik trafik tespiti için ağ trafiğini analiz etmek için çok katmanlı algılayıcılara ve karar ağaçlarına dayanmaktadır (Wai vd. 2018). IoT ağında oluşturulan büyük miktardaki verinin davranışsal analizini oluşturmada derin öğrenme yöntemlerinin etkili olduğu görülmektedir. Derin öğrenme mekanizmalarının, yapılandırılmamış ve heterojen verileri kullanan çoklu alanlarda diğer olasılık çözümlerinden daha iyi performans gösterdiği tespit edilmiştir. Geleneksel makine öğrenimi algoritmalarıyla ilgili sorun, kendi oluşturdukları bir ortamda iyi çalışabilseler de ağa daha fazla cihaz dahil edildikçe verilerin artması ve bu modellere eskime görüntüsü vermesidir. Derin öğrenme algoritmaları daha fazla veriden daha fazlasını öğrendiği için bu alanda derin öğrenmenin bu sorunu çözdüğü çalışmalar mevcuttur. Ayrıca botnet tespiti için karar ağacı ve yapay sinir ağları gibi son teknoloji algoritmalar kullanılmaktadır. Bu algoritmaların karşılaştırılması için bu çalışmada ağ trafiği veri setini içeren CTU-13 kullanılmıştır. Sinir ağı ve karar ağacı sırasıyla 0.91 ve 0.98 doğruluk değerine sahiptir. Önerdiğimiz çözümün 0.99 olan F1 puanı bu iki algoritmadan daha doğrudur (Ryu ve Yang 2018). Başka bir çalışmada, IRC için kullanılan port

numarası olarak 6667 ve http olarak da 80 numaralı trafik paketlerini içeren Cyber Clean Center veri seti yer almaktadır. Botnet tespit algoritmaları olarak Extreme Learning Machine (ELM), Support Vector Machine (SVM), Convolutional Sinir Ağ (CNN) ve Kolektif Classifier Algorithm with Stack Process (ECASP) kullanıldı. Botnet tespiti F1 skorunun karşılaştırmasına göre, önerdiğimiz algoritma ELM (%91,6), CNN (%92,56), SVM (%93,36) ve ECAP'tan (%94,08) (Srinivasan ve Kumar 2023) daha iyidir. Meidan ve arkadaşlarının IoT'sinde botnet algılama, önerilen yöntemde derin otomatik kodlayıcılar kullanıldı. Bu çalışmada IoT botnet saldırılarının tespiti için N-BaIot veri seti kullanılmıştır. En popüler IoT tabanlı botnet'ler olan Mirai ve Bashlite, her cihaz için enfekte edildi. Meidan ve arkadaşlarının model yapısı, giriş katmanının boyutlarını %75, %50, %33 ve %25 oranında küçülten dört gizli kodlayıcı katmanı tarafından oluşturuldu. Sonraki diğer katmanlar, kodlayıcılarla benzer boyutta kod çözücüler içeriyordu. Modellerinin gerçek pozitif oranının bu yapısı, bizim önerdiğimiz gerçek pozitif oran çözümümüze %100 benzer. Yerel Aykırı Değer Faktörü (LOF), Tek Sınıf SVM ve İzolasyon Ormanı da Meidan ve arkadaşlarının çalışmasında değerlendirilen diğer algoritmalardır. Önerilen TPR çözümü, LOF ve SVM ile benzerdir ve İzolasyon Ormanından daha doğrudur (Meidan vd. 2018). Başka bir çalışmada, Algelal ve arkadaşlarının botnet algılama yöntemleri, CTU-13 veri seti ve 10 kat çapraz doğrulama ile eğitilmiş ve test edilmiştir. Önerilen modelin doğruluğu %99,84'tür. Bu çalışmadaki kolektif sınıflandırıcıları AdaBoost ve Jrip algoritmalarından oluşmaktadır. Kolektif derin sinir ağları aracılığıyla IoT botnet tespiti, AdaBoost ve Jrip algoritmaları ile hemen hemen benzer doğruluğa sahiptir. Clusering (%98,39), Sinir Ağı (%89,38), Recurrrent Sinir Ağı (%83,09), K-medoids, L-means, LSTM, karar ağaçları olan yöntemin geri kalanı, botnet tespiti için önerilen modelden daha az doğruluğa sahiptir. (Algelal vd. 2020). ISCX veri setinin kullanıldığı başka bir çalışma, Ensemble of Classifie algoritması ile botnet trafiğini analiz etti. Bu veri seti, normal trafiği ve botnet trafiğini içeriyordu. Bu çalışma aynı zamanda Ada-Boost with Decision Tree (%94,78) ve Soft Voting of KNN & Decision Tree (%96.41) kolektif sınıflandırıcı algoritmalarının, önerdiğimiz modelin doğruluğu kadar botnet tespitinin doğruluğunu artırdığını da gösterdi (Bijalwan vd. 2016). Bu çalışmada N-BaIoT veri setine ait 9 zararlı ve 1 iyi huylu olmak üzere 10 cihazın ağ trafiği kolektif DNN tabanlı bir yaklaşımla sınıflandırılmıştır. Elde edilen sonuçlara göre önerilen yöntem %99 doğrulukla çalışmaktadır. Yapısı gereği karmaşık

ve çok sınıflandırmalı bir problem olan problem, önerilen yöntem sayesinde hızlı, kullanıcıdan bağımsız ve yüksek doğrulukla çalışmaktadır. Bireysel ve kurumsal güvenlik sorunlarına çözümler sunarak endişeleri giderir. Sonuçlar gelecek çalışmalar için ümit verici ve cesaret vericidir.

7. KAYNAKLAR

Achiluzzi E, Li M, Georgy M F A, Kashef R, 2022, Exploring the Use of Data-Driven Approaches for Anomaly Detection in the Internet of Things (IoT) Environment, arXiv preprint arXiv:2301.00134.

Ahmetoğlu H, Daş R, 2019, Derin Öğrenme ile Büyük Veri Kümelerinden Saldırı Türlerinin Sınıflandırılması, IDAP, 455–463, Malatya, Türkiye.

Al Shorman A, Faris H, Aljarah I, 2020, Unsupervised intelligent system based on one class support vector machine and Grey Wolf optimization for IoT botnet detection, Journal of Ambient Intelligence and Humanized Computing, 11, 2809–2825.

Alam M, Samad M D, Vidyaratne L, Glandon A, Iftekharuddin K M, 2020, Survey on deep neural networks in speech and vision systems, Neurocomputing, 417, 302–321.

Alanazi M, Aljuhani A, 2022, Anomaly detection for internet of things cyberattacks. Computers, Materials & Continua, 72(1), 261–279.

Alani M M, 2022, BotStop: Packet-based efficient and explainable IoT botnet detection using machine learning, Computer Communications, 193, 53–62.

Alauthman M, Aslam N, Al-Kasassbeh M, Khan S, Al-Qerem A, Choo K K R, 2020, An efficient reinforcement learning-based Botnet detection approach, Journal of Network and Computer Applications, 150, 102479.

Al-Garadi M A, Mohamed A, Al-Ali A K, Du X, Ali I, Guizani M, 2020, A survey of machine and deep learning methods for internet of things (IoT) security, IEEE Communications Surveys & Tutorials, 22(3), 1646–1685.

Algelal Z, vd., 2020, Botnet Detection Using Ensemble Classifiers of Network Flow, International Journal of Electrical and Computer Engineering (IJECE), 10(3), 2543.

Alissa K, Alyas T, Zafar K, Abbas Q, Tabassum N, Sakib S, 2022, Botnet Attack Detection in IoT Using Machine Learning, Computational Intelligence and Neuroscience, 2022.

Aljabri M, Alahmadi A A, Mohammad R M A, Alhaidari F, Aboulnour M, Alomari D M, Mirza S, 2023, Machine Learning-Based Detection for Unauthorized Access to IoT Devices, Journal of Sensor and Actuator Networks, 12(2), 27.

Alkahtani H, Aldhyani T H, 2021, Botnet attack detection by using CNN-LSTM model for Internet of Things applications, Security and Communication Networks, 2021, 1–23.

Alkhalil Z, Hewage C, Nawaf L, Khan I, 2021, Phishing attacks: A recent comprehensive study and a new anatomy, Frontiers in Computer Science, 3, 563060.

Alotaibi B, Alotaibi M, 2020, A stacked deep learning approach for IoT cyberattack detection, Journal of Sensors, 2020, 1–10.

Altun M, Gürüler H, Özkaraca O, Khan F, Khan J, Lee Y, 2023, Monkeypox detection using CNN with transfer learning, Sensors, 23(4), 1783.

Álvarez G, Petrović S, 2003, A new taxonomy of web attacks suitable for efficient encoding, Computers & Security, 22(5), 435–449.

Alzubaidi, L, Zhang J, Humaidi A J, Al-Dujaili A, Duan Y, Al-Shamma O, vd., 2021, Review of deep learning: Concepts, CNN architectures, challenges, applications, future directions, Journal of big Data, 8, 1–74.

Amini P, Araghizadeh M A, Azmi R, 2015, A survey on Botnet: Classification, detection and defense, In 2015 International Electronics Symposium (IES), 233–238, IEEE.

Anthi E, Williams L, Słowińska M, Theodorakopoulos G, Burnap P, 2019, A supervised intrusion detection system for smart home IoT devices, IEEE Internet of Things Journal, 6(5), 9042–9053.

Anwar M, Omar K, Abbas A, Abdelmonim F, Refaie M, Medhat W, vd., 2022, Smart Customer Care: Scraping Social Media to Predict Customer Satisfaction in Egypt Using Machine Learning Models, In 2022 20th International Conference on Language Engineering (ESOLEC), 27–34, IEEE.

Arifuzzaman M, Hasan M R, Toma T J, Hassan S B, Paul A K, 2023, An Advanced Decision Tree-Based Deep Neural Network in Nonlinear Data Classification, Technologies, 11(1), 24.

Arshad S, Abbaspour M, Kharrazi M, Sanatkar H, 2011, An anomaly-based botnet detection approach for identifying stealthy botnets, In 2011 IEEE International Conference on Computer Applications and Industrial Electronics (ICCAIE), 564-569, IEEE.

AsSadhan B, Moura J M, 2014, An efficient method to detect periodic behavior in botnet traffic by analyzing control plane traffic, Journal of Advanced Research, 5(4), 435–448.

Bacha S, Aljuhani A, Abdellafou K B, Taouali O, Liouane N, Alazab M, 2022, Anomaly-based intrusion detection system in IoT using kernel extreme learning machine, Journal of Ambient Intelligence and Humanized Computing, 1–12.

Bahşi H, Nõmm S, La Torre F B, 2018, Dimensionality reduction for machine learning based iot botnet detection, In 2018 15th International Conference on Control, Automation, Robotics and Vision (ICARCV), 1857–1862, IEEE.

Bank D, Koenigstein N, Giryes R, 2020, Autoencoders, arXiv preprint arXiv:2003.05991.

Barrera D, Molloy I, Huang H, 2017, IDIoT: Securing the Internet of Things like it's 1994, arXiv preprint arXiv:1712.03623.

Basit A, Zafar M, Liu X, Javed A R, Jalil Z, Kifayat K, 2021, A comprehensive survey of AI-enabled phishing attacks detection techniques, Telecommunication Systems, 76, 139–154.

Batty M, Axhausen K W, Giannotti F, Pozdnoukhov A, Bazzani A, Wachowicz M, vd., 2012, Smart cities of the future, The European Physical Journal Special Topics, 214(1), 481–518.

Belkin M, Ma S, Mandal S, 2018, To understand deep learning we need to understand kernel learning, In International Conference on Machine Learning, 541–549, PMLR.

Bertino E, Islam N, 2017, Botnets and Internet of Things Security, Computer, 50(2), 76–79.

Bezerra V H, vd., 2019, IoTDS: A One-Class Classification Approach To Detect Botnets in Internet of Things Devices, Sensors, 19(14), 3188.

Bhowmick A, Hazarika S M, 2016, Machine learning for e-mail spam filtering: review, techniques and trends, arXiv preprint arXiv:1606.01042.

Bini S A, 2018, Artificial intelligence, machine learning, deep learning, and cognitive computing: what do these terms mean and how will they impact health care?, The Journal of arthroplasty, 33(8), 2358–2361.

Butt U A, Mehmood M, Shah S B H, Amin R, Shaukat M W, Raza S M, vd., 2020, A review of machine learning algorithms for cloud computing security, Electronics, 9(9), 1379.

Calikus E, Nowaczyk S, Bouguelia M R, Dikmen O, 2022, Wisdom of the contexts: active ensemble learning for contextual anomaly detection, Data Mining and Knowledge Discovery, 36(6), 2410–2458.

Caruana R, Niculescu-Mizil A, Crew G, Ksikes A, 2004, Ensemble selection from libraries of models, In Proceedings of the Twenty-First International Conference on Machine Learning, 18.

Casas P, Mazel J, Owezarski P, 2012, Unsupervised network intrusion detection systems: Detecting the unknown without knowledge, Computer Communications, 35(7), 772–783.

Catillo M, Pecchia A, Villano U, 2023, A Deep Learning Method for Lightweight and Cross-Device IoT Botnet Detection, Applied Sciences, 13(2), 837.

Chai J, Zeng H, Li A, Ngai E W, 2021, Deep learning in computer vision: A critical review of emerging techniques and application scenarios, Machine Learning with Applications, 6, 100134.

Chatterjee A, Ahmed B S, 2022, IoT anomaly detection methods and applications: A survey, Internet of Things, 19, 100568.

Chen J, Wang Z, Tomizuka M, 2018, Deep hierarchical reinforcement learning for autonomous driving with distinct behaviors, In 2018 IEEE Intelligent Vehicles Symposium (IV), 1239–1244, IEEE.

Chen Y, Yang T J, Emer J, Sze V, 2018, Understanding the limitations of existing energy-efficient design approaches for deep neural networks, Energy, 2(L1), L3.

Chen Z, Liu J, Shen Y, Simsek M, Kantarci B, Mouftah H T, Djukic P, 2022, Machine learning-enabled IoT security: Open issues and challenges under advanced persistent threats, ACM Computing Surveys, 55(5), 1–37.

Chiew K L, Yong K S C,Tan C L, 2018, A survey of phishing attacks: Their types, vectors and technical approaches, Expert Systems with Applications, 106, 1–20.

Chintawar S, Gattani V, Vyas S, Dawre S, 2023, Role of Artificial Intelligence in Machine Learning for Diagnosis and Radiotherapy, In S. Gupta & R. Taneja (Eds.), Bioinformatics Tools for Pharmaceutical Drug Product Development, 315–344.

Ciancio C, Ambrogio G, Gagliardi F, Musmanno R, 2016, Heuristic techniques to optimize neural network architecture in manufacturing applications, Neural Computing and Applications, 27, 2001–2015.

Cid-Fuentes J Á, Szabo C, Falkner K, 2018, An adaptive framework for the detection of novel botnets, Computers & Security, 79, 148–161.

Cortes C, Vapnik V, 1995, Support-vector networks, Machine learning, 20(3), 273–297.

Dale J M, Popescu L, Karp P D, 2010, Machine learning methods for metabolic pathway prediction, BMC Bioinformatics, 11(1), 1–14.

Dargan S, Kumar M, Ayyagari M R, Kumar G, 2020, A survey of deep learning and its applications: a new paradigm to machine learning, Archives of Computational Methods in Engineering, 27, 1071–1092.

Deng L, Liu Y, 2018, A joint introduction to natural language processing and to deep learning, In deep learning in natural language processing (1–22), Springer.

Dhar V, 2016, Data science and prediction, Communications of the ACM, 56(12), 64–73.

Dietterich T G, 1997, Machine-learning research, AI Magazine, 18(4), 97–97.

Dietterich T G, 2000, Ensemble methods in machine learning, In Multiple Classifier Systems: First International Workshop, MCS 2000 Cagliari, Italy, June 21–23, 2000 Proceedings 1, 1–15, Springer Berlin Heidelberg.

Diro A, Chilamkurti N, Nguyen V D, Heyne W, 2021, A comprehensive study of anomaly

detection schemes in IoT networks using machine learning algorithms, Sensors, 21(24), 8320.

Dua P, Bais S, 2014, Supervised learning methods for fraud detection in healthcare insurance, In S. S. Pattnaik, R. N. Mishra, & M. K. Nayak (Eds.), Machine learning in healthcare informatics, 261–285.

Egmont-Petersen M, de Ridder D, Handels H, 2002, Image processing with neural networks—a review, Pattern recognition, 35(10), 2279–2301.

El Naqa I, Murphy M J, 2015, What is Machine Learning? In Machine Learning in Radiation Oncology, 3–11, Springer, Cham.

Elkhodr M, Shahrestani S, Cheung H, 2013, The Internet of Things: Vision & Challenges, IEEE 2013 Tencon-Spring, 218–222.

Eskandari M, Janjua Z H, Vecchio M, Antonelli F, 2020, Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices, IEEE Internet of Things Journal, 7(8), 6882–6897.

Eslahi M, Salleh R, Anuar N B, 2012, Bots and botnets: An overview of characteristics, detection and challenges, In 2012 IEEE International Conference on Control System, Computing and Engineering, 349–354, IEEE.

Esteva A, Robicquet A, Ramsundar B, Kuleshov V, DePristo M, Chou K, vd., 2019, A guide to deep learning in healthcare, Nature medicine, 25(1), 24–29.

Foorthuis R, 2021, On the nature and types of anomalies: A review of deviations in data, International Journal of Data Science and Analytics, 12(4), 297–331.

Gantz J, David R, 2012, The digital universe in 2020: Big Data, Bigger Digital Shadows and Biggest Growth in the Far East, IDC iView: IDC Analyze the future 2007-2012, 1–16.

Geer D, 2005, Malicious Bots Threaten Network Security, Computer, 38(1), 18–20.

Ghosh S, Das N, Das I, Maulik U, 2019, Understanding deep learning techniques for image segmentation, ACM Computing Surveys (CSUR), 52(4), 1–35.

Goodfellow I, Bengio Y, Courville A, 2016, Deep learning, MIT Press.

Grizzard J B, Sharma V, Nunnery C, Kang B B, Dagon D, 2007, Peer-to-Peer Botnets:

Overview and Case Study, HotBots, 7, 1–8.

Han S, Wu Q, Yang Y, 2022, Machine learning for Internet of Things anomaly detection under low-quality data, International Journal of Distributed Sensor Networks, 18(10).

Hayes M A, Capretz M A, 2015, Contextual anomaly detection framework for big sensor data, Journal of Big Data, 2(1), 1–22.

Hoque N, Bhuyan M H, Baishya R C, Bhattacharyya D K, Kalita J K, 2014, Network attacks: Taxonomy, tools and systems, Journal of Network and Computer Applications, 40, 307–324.

Hoyal Cuthill J F, Guttenberg N, Ledger S, Crowther R, Huertas B, 2019, Deep learning on butterfly phenotypes tests evolution's oldest mathematical model, Science Advances, 5(8), eaaw4967.

Huyghue B D, 2021, Cybersecurity, Internet of Things, and Risk Management for Businesses, (Doctoral Dissertation), Utica College, Utica, NY.

Hwang R H, Peng M C, Huang C W, 2019, Detecting IoT malicious traffic based on autoencoder and convolutional neural network, In 2019 IEEE Globecom Workshops (GC Wkshps), 1–6, IEEE.

Jadhav S D, Channe H P, 2016, Comparative study of K-NN, naive Bayes and decision tree classification techniques, International Journal of Science and Research (IJSR), 5(1), 1842–1845.

Jain A K, 2010, Data clustering: 50 years beyond K-means, Pattern recognition letters, 31(8), 651–666.

Jain A, Kumar A M, 2007, Hybrid neural network models for hydrologic time series forecasting, Applied Soft Computing, 7(2), 585–592.

Jajodia S, Noel S, O'berry B, 2005, Topological analysis of network attack vulnerability, In Managing Cyber Threats: Issues, Approaches, and Challenges, 247–266.

Janiesch C, Zschech P, Heinrich K, 2021, Machine learning and deep learning, Electronic Markets, 31(3), 685–695.

Karim A, Ali Shah S A, Salleh R B, Arif M, Noor R M, Shamshirband S, 2015, Mobile

botnet attacks-an emerging threat: classification, review and open issues, KSII Transactions on Internet and Information Systems (TIIS), 9(4), 1471–1492.

Khraisat A, Alazab A, 2021, A critical review of intrusion detection systems in the internet of things: Techniques, deployment strategy, validation strategy, attacks, public datasets and challenges, Cybersecurity, 4, 1–27.

Kiran B R, Sobh I, Talpaert V, Mannion P, Al Sallab A A, Yogamani S, Pérez P, 2021, Deep reinforcement learning for autonomous driving: A survey, IEEE Transactions on Intelligent Transportation Systems, 23(6), 4909–4926.

Kiranyaz S, Avci O, Abdeljaber O, Ince T, Gabbouj M, Inman D J, 2021, 1D convolutional neural networks and applications: A survey, Mechanical Systems and Signal Processing, 151, 107398.

Kotsiantis S B, Zaharakis I, Pintelas P, 2007, Supervised machine learning: A review of classification techniques, In T. Watanabe, D. J. Abraham, & I. Ramos (Eds.), Emerging artificial intelligence applications in computer engineering, 3–24.

Kumar S, Carley K M, 2016, Understanding DDoS cyber-attacks using social media analytics, In 2016 IEEE Conference on Intelligence and Security Informatics (ISI), 231–236, IEEE.

Lai J Y, Wu J S, Chen S J, Wu C H, Yang C H, 2008, Designing a taxonomy of web attacks, In 2008 International Conference on Convergence and Hybrid Information Technology, 278–282, IEEE.

LeCun Y, Bengio Y, Hinton G, 2015, Deep learning, Nature, 521(7553), 436–444.

Li C, Jiang W, Zou X, 2009, Botnet: Survey and case study, In 2009 Fourth International Conference on Innovative Computing, Information and Control (ICICIC), 1184–1187, IEEE.

Li H, Song J, Xue M, Zhang H, Ye J, Cheng L, Song M, 2022, A survey of neural trees, arXiv preprint arXiv:2209.03415.

Li L, Hu Q, Wu X, Yu D, 2014, Exploration of classification confidence in ensemble learning, Pattern Recognition, 47(9), 3120–3131.

Limarunothai R, Munlin M A 2015, Trends and challenges of botnet architectures and

detection techniques, Journal of Information Science and Technology, 5(1), 51–57.

Litjens G, Kooi T, Bejnordi B E, Setio A A A, Ciompi F, Ghafoorian M, vd., 2017, A survey on deep learning in medical image analysis, Medical image analysis, 42, 60–88.

Liu R, Liu Y, Yan Y, Wang J Y 2020, Iterative deep neighborhood: A Deep learning model which involves both input data points and their neighbors, Computational Intelligence and Neuroscience, 2020.

Liu Z, Thapa N, Shaver A, Roy K, Siddula M, Yuan X, Yu A, 2021, Using embedded feature selection and CNN for classification on CCD-INID-V1—a new IoT dataset, Sensors, 21(14), 4834.

Lu Y, 2019, Artificial Intelligence: A Survey on Evolution, Models, Applications and Future Trends, Journal of Management Analytics, 6(1), 1–29.

Ma Y, Xie Y, 2022, Evolutionary Neural Networks for Deep learning: A review, International Journal of Machine Learning and Cybernetics, 13(10), 3001-3018.

Mahfouz A, Abuhussein A, Venugopal D, Shiva S, 2020, Ensemble classifiers for network intrusion detection using a novel network attack dataset, Future Internet, 12(11), 180.

Mao S, Chen J W, Jiao L, Gou S, Wang R, 2019, Maximizing diversity by transformed ensemble learning, Applied Soft Computing, 82, 105580.

Mathur L, Raheja M, Ahlawat P, 2018, Botnet detection via mining of network traffic flow, Procedia Computer Science, 132, 1668–1677.

Mazhar T, Talpur D B, Shloul T A, Ghadi Y Y, Haq I, Ullah I, vd., 2023, Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence. Brain Sciences, 13(4), 683.

McDermott C D, Majdani F, Petrovski A V, 2018, Botnet detection in the internet of things using deep learning approaches, In 2018 international joint conference on neural networks (IJCNN), 1–8, IEEE.

Meidan Y, Bohadana M, Mathov Y, Mirsky Y, Shabtai A, Breitenbacher D, Elovici Y,

2018, N-baiot network–based detection of iot botnet attacks using deep autoencoders, IEEE Pervasive Computing, 17(3), 12–22.

Miikkulainen R, Liang J, Meyerson E, Rawal A, Fink D, Francon O, vd., 2019, Evolving deep neural networks, In Artificial Intelligence in the Age of Neural Networks and Brain Computing, 293–312, Academic Press.

Milanes V, Shladover S E, Spring J, Nowakowski C, Kawazoe H, Nakamura M, 2014, Cooperative adaptive cruise control in real traffic situations, IEEE Transactions on Intelligent Transportation Systems, 15(1), 296–305.

Mirsky Y, Doitshman T, Elovici Y, Shabtai A, 2018, Kitsune: an ensemble of autoencoders for online network intrusion detection, arXiv preprint arXiv:1802.09089.

Muhammad I, Yan Z, 2015, Supervised Machine Learning Approaches: A Survey, ICTACT Journal on Soft Computing, 5(3).

Nakaura T, Higaki T, Awai K, Ikeda O, Yamashita Y, 2020, A primer for understanding radiology articles about machine learning and deep learning, Diagnostic and Interventional Imaging, 101(12), 765–770.

Naveed K, Wu H, 2021, Poster: Automated neural network Structure Selection for IoT Botnet Detection, In 2021 IFIP Networking Conference (IFIP Networking) (1–3), IEEE.

Neshatpour K, Behnia F, Homayoun H, Sasan A, 2018, ICNN: An iterative implementation of convolutional neural networks to enable energy and computational complexity aware dynamic approximation, In 2018 Design, Automation & Test in Europe Conference & Exhibition (DATE), 551–556, IEEE.

Neshatpour K, Homayoun H, Sasan A, 2019, ICNN: The iterative convolutional neural network, ACM Transactions on Embedded Computing Systems (TECS), 18(6), 1–27.

Nicosia G, Ojha V, La Malfa E, La Malfa G, Jansen G, Pardalos P M, vd., 2022, Machine Learning Optimization and Data Science: 7th International Conference, LOD 2021, Grasmere, UK, October 4–8, 2021, Revised Selected Papers, Part II 13164, Springer Nature.

Nurse J R, Buckley O, Legg P A, Goldsmith M, Creese S, Wright G R, Whitty M, 2014, Understanding insider threat: A framework for characterising attacks, In 2014 IEEE Security and Privacy Workshops, 214–228, IEEE.

Ojha V, Nicosia G, 2022, Backpropagation neural tree, Neural Networks, 149, 66–83.

Okur C, Dener, M. 2020, Detecting IoT Botnet Attacks Using Machine Learning Methods, In 2020 International Conference on Information Security and Cryptology (ISCTURKEY), 31–37, IEEE.

Peng W, Varanka T, Mostafa A, Shi H, Zhao G, 2021, Hyperbolic Deep Neural Networks: A survey, IEEE Transactions on Pattern Analysis and Machine Intelligence, 44(12), 10023–10044.

Peters J, Schaal S, 2008, Reinforcement learning of motor skills with policy gradients, Neural Networks, 21(4), 682–697.

Plohmann D, Gerhards-Padilla E, 2012, Case study of the miner botnet, In 2012 4th International Conference on Cyber Conflict (CYCON 2012), 1–16, IEEE.

Pokhrel S, Abbas R, Aryal B, 2021, IoT security: botnet detection in IoT using machine learning, arXiv preprint arXiv:2104.02231.

Popoola S I, Ande R, Adebisi B, Gui G, Hammoudeh M, Jogunola O, 2021, Federated deep learning for zero-day botnet attack detection in IoT-edge devices, IEEE Internet of Things Journal, 9(5), 3930–3944.

Qurashi A W, Holmes V, 2019, Comparison of Deep Neural Network approach in text and image classification using CPU and GPU systems, Emerging Technology Conference (1–4), University of Huddersfield.

Rahman R U, Tomar D S, 2021, Botnet threats to e-commerce web applications and their detection, In Research Anthology on Combating Denial-of-Service Attacks, 104–137, IGI Global.

Reddy S, Shyam G K, 2022, A machine learning based attack detection and mitigation using a secure SaaS framework, Journal of King Saud University-Computer and Information Sciences, 34(7), 4047–4061.

Satılmış H, Akleylek S, 2021, IoT Güvenliği için Kullanılan Makine Öğrenimi ve Derin

Öğrenme Modelleri Üzerine Bir Derleme, Bilişim Teknolojileri Dergisi, 14(4), 457–481.

Savic M, Lukic M, Danilovic D, Bodroski Z, Bajović D, Mezei I, vd., 2021, Deep learning anomaly detection for cellular IoT with applications in smart logistics, IEEE Access, 9, 59406–59419.

Schmidhuber J, 2015, Deep learning in neural networks: An overview, Neural networks, 61, 85–117.

Sento A, 2016, Image compression with auto-encoder algorithm using Deep Neural Network (DNN), In 2016 Management and Innovation Technology International Conference (MITicon), MIT–99, IEEE.

Shafiq M, Tian Z, Bashir A K, Du X, Guizani M, 2020, CorrAUC: a malicious bot-IoT traffic detection method in IoT network using machine-learning techniques, IEEE Internet of Things Journal, 8(5), 3242–3254.

Shamim N, Asim M, Baker T, Awad A I, 2023, Efficient Approach for Anomaly Detection in IoT Using System Calls, Sensors, 23(2), 652.

Shareena J, Ramdas A, AP H, 2021, Intrusion detection system for iot botnet attacks using deep learning, SN Computer Science, 2(3), 205.

Sharma N, Jain V, Mishra A, 2018, An analysis of convolutional neural networks for image classification, Procedia computer science, 132, 377–384.

Sharma N, Sharma R, Jindal N, 2021, Machine learning and deep learning applications-a vision, Global Transitions Proceedings, 2(1), 24–28.

Skorin-Kapov N, vd., 2016, Physical-Layer Security in Evolving Optical Networks, IEEE Communications Magazine, 54(8), 110–117.

Stevanovic M, Pedersen J M, 2016, On the Use of Machine Learning for Identifying Botnet Network Traffic, Journal of Cyber Security and Mobility, 4, 109–128.

Sun W, Shao S, Zhao R, Yan R, Zhang X, Chen X, 2016, A sparse auto-encoder-based deep neural network approach for induction motor faults classification. Measurement, 89, 171–178.

Surden H, 2019, Artificial intelligence and law: An overview, Georgia State University

Law Review, 35, 19–22.

Sutton R S, Barto A G, 2018, Reinforcement learning: An introduction, MIT Press.

Tanno R, Arulkumaran K, Alexander D, Criminisi A, Nori A, 2019, May, Adaptive Neural trees, In International Conference on Machine Learning, 6166–6175. PMLR.

Verma A, Ranga V, 2020, Machine learning Based Intrusion Detection Systems for IoT Applications, Wireless Personal Communications, 111(4), 2287–2310.

Vinayakumar R, Alazab M, Srinivasan S, Pham Q V, Padannayil S K, Simran K, 2020, A visualized botnet detection system based deep learning for the internet of things networks of smart cities, IEEE Transactions on Industry Applications, 56(4), 4436–4456.

Wang J, Liu C, Xu J, Wang J, Hao S, Yi W, Zhong J, 2022, IoT-DeepSense: Behavioral Security Detection of IoT Devices Based on Firmware Virtualization and Deep Learning, Security and Communication Networks, 2022.

Wang S, Chen H, Wu L, Wang J, 2020, A novel smart meter data compression method via stacked convolutional sparse auto-encoder, International Journal of Electrical Power & Energy Systems, 118, 105761.

Wang Y M, Liu Z L, Cheng X Y, Zhang K J, 2005, An analysis approach for multi-stage network attacks, In 2005 International Conference on Machine Learning and Cybernetics, 3949–3954, IEEE.

Xhemali D, Hinde C J, Stone R, 2009, Naïve bayes vs. decision trees vs. neural networks in the classification of training web pages.

Yamashita R, Nishio M, Do R K G, Togashi K, 2018, Convolutional Neural Networks: An overview and application in radiology, Insights into Imaging, 9, 611–629.

Yang H, Luo L, Chueng L P, Ling D, Chin F, 2019, Deep learning and its applications to natural language processing, Deep learning: Fundamentals, theory and applications, 89–109.

Yang Y, Morillo I G, Hospedales T M, 2018, Deep neural decision trees, arXiv preprint arXiv:1806.06988.

Yılmaz A, Demir F, 2022, Efficient continuity ratios for convolutional neural networks in image classification tasks, Journal of Artificial Intelligence Research.

Young T, Hazarika D, Poria S, Cambria E, 2018, Recent trends in deep learning based natural language processing, IEEE Computational Intelligence Magazine, 13(3), 55–75.

Yurttakal A H, Baş H, 2021, Possibility Prediction Of Diabetes Mellitus At Early Stage Via Stacked Ensemble Deep Neural Network. Afyon Kocatepe Üniversitesi Fen Ve Mühendislik Bilimleri Dergisi, 21(4), 812–819.

Zhang L, Zhou G, Han Y, Lin H, Wu Y, 2018, Application of internet of things technology and convolutional neural network model in bridge crack detection, IEEE Access, 6, 39442–39451.

Zhang M L, Zhou Z H, 2013, Exploiting unlabeled data to enhance ensemble diversity, Data Mining and Knowledge Discovery, 26, 98–129.

Zhou J, Cui G, Hu S, Zhang Z, Yang C, Liu Z, vd., 2020, Graph Neural Networks: A review of methods and applications, AI open, 1, 57–81.

Zhou Z, Li X, Zare R N, 2017, Optimizing chemical reactions with deep reinforcement learning, ACS central science, 3(12), 1337–1344.

İnternet Kaynakları

1- https://saturncloud.io/, 04.05.2023

2- https://www.techtarget.com/, 07.05.2023

3- https://www.upgrad.com/blog/basic-cnn-architecture/, 01.05.2023

4- https://www.jeremyjordan.me/autoencoders/, 29.04.2023

5- https://www.simplilearn.com/, 14.04.2023

6- https://www.mygreatlearning.com/blog/autoencoder/, 27.04.2023

7- https://stats.stackexchange.com/, 07.04.2023

8- https://iq.opengenus.org/types-of-autoencoder/, 05.05.2023

9- https://towardsdatascience.com/, 06.03.2023

10-https://www.kdnuggets.com/2019/11/all-about-autoencoders.html, 15.01.2023

11-https://medium.com/edureka/autoencoders-tutorial-cfdcebdefe37, 14.01.2023

12-https://blog.paperspace.com/autoencoder-image-compression-keras/, 28.01.2023

13-https://iopscience.iop.org/, 02.03.2023

14-https://medium.com/analytics-vidhya/anomaly-detection-in-cardio-dataset-using-deep-learning-technique-autoencoder-fd24ca9e5c69, 15.01.2023

15-https://pub.towardsai.net/, 02.02.2023

16-https://machinelearningmastery.com/autoencoder-for-classification, 05.01.2023

17-https://www.analyticsvidhya.com/, 17.03.2023

18-https://blog.paperspace.com/bagging-ensemble-methods/, 29.04.2023

19-https://www.mygreatlearning.com/blog/bagging-boosting/, 18.04.2023

20-https://www.educba.com/bagging-and-boosting/, 20.04.2023

21-https://scikit-learn.org/stable/modules/ensemble.html, 11.03.2023

22-https://www.ibm.com/topics/bagging, 07.05.2023

23-https://aws.amazon.com/tr/what-is/boosting/, 07.05.2023

24-https://www.geeksforgeeks.org/, 06.03.2023

25-https://www.ibm.com/topics/boosting, 07.05.2023

26-https://machinelearningmastery.com/, 23.04.2023

27-https://www.javatpoint.com/stacking-in-machine-learning, 19.02.2023

28-https://www.emnify.com/iot-glossary/iot-security, 12.02.2023

29-https://www.paloaltonetworks.com/cyberpedia/what-is-iot-security, 12.02.2023

30-https://usa.kaspersky.com/, 30.04.2023

31-https://csrc.nist.gov/glossary/term/cybersecurity, 12.02.2023

32-https://www.upguard.com/blog/cybersecurity-important, 21.04.2023

33-https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/, 20.04.2023

34-https://reciprocity.com/resources/what-are-cybersecurity-threats/, 14.04.2023

35-https://www.nist.gov/, 26.01.2023

36-https://audra.io/blog/Importance-cyber-security-in-the-digital-world-in-2022, 27.01.2023

37-https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/, 15.04.2023

38-https://usa.kaspersky.com/resource-center/threats/ddos-attacks, 18.04.2023

39-https://www.ncsc.gov.uk/, 26.01.2023

40-https://www.proofpoint.com/us/threat-reference/ddos, 13.03.2023

41-https://www.comptia.org/, 12.02.2023

42-https://www.a10networks.com/blog/5-most-famous-ddos-attacks/, 02.02.2023

43-https://www.mass.gov/info-details/types-of-cyber-threats, 09.03.2023

44-https://blog.netwrix.com/, 24.03.2023

45-https://knowww.eu/nodes/5bd5bfdd7bb7bca48fe42d18, 04.01.2023

46-https://www.csoonline.com/, 08.02.2023

47-https://cisserv1.towson.edu/, 08.02.2023

48-https://usa.kaspersky.com/resource-center/threats/botnet-attacks, 14.03.2023

49-https://www.techtarget.com/searchsecurity/definition/botnet, 15.03.2023

50-https://securityscorecard.com/blog/what-is-a-botnet-attack/, 12.03.2023

51-https://www.imperva.com/learn/ddos/botnet-ddos/, 26.04.2023

52-https://datadome.co/, 28.03.2023

53-https://dataprot.net/articles/what-is-botnet/, 10.03.2023

54-https://www.trendmicro.com/vinfo/us/security/definition/iot-botnet, 27.02.2023

55-https://securityintelligence.com/, 21.04.2023

56-https://www.einfochips.com/, 10.04.2023

57-https://www.a10networks.com/glossary/what-is-a-botnet-iot-botnet/, 04.03.2023

58-https://www.splunk.com/en_us/data-insider/anomaly-detection.html, 06.04.2023

59-https://www.anodot.com/blog/what-is-anomaly-detection/, 06.04.2023

60-https://rapidminer.com/glossary/anomaly-detection/, 08.04.2023

61-https://www.sciencedirect.com/topics/engineering/confusion-matrix, 10.02.2023

62-https://www.v7labs.com/blog/confusion-matrix-guide, 10.02.2023

63-https://towardsdatascience.com, 20.02.2023

64-https://www.guru99.com/confusion-matrix-machine-learning-example.html, 21.02.2023

65-https://online.stat.psu.edu/stat504/lesson/7/7.4, 05.05.2023

66-https://acutecaretesting.org/en/articles/roc-curves-what-are-they-and-how-are-they-used, 07.05.2023