MARMARA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

DDOS SALDIRILARININ TESPİTİ VE SINIFLANDIRILMASI İÇİN DERİN ÖĞRENME MODELİ

ABDULLAH EMİR ÇİL

YÜKSEK LİSANS TEZİ

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Yüksek Lisans Programı

DANIŞMAN

Doç. Dr. Kazım YILDIZ

EŞ-DANIŞMAN

Prof. Dr. Ali BULDU

İSTANBUL, 2021

MARMARA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

DDOS SALDIRILARININ TESPİTİ VE SINIFLANDIRILMASI İÇİN DERİN ÖĞRENME MODELİ

ABDULLAH EMİR ÇİL

523618017

YÜKSEK LİSANS TEZİ

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Yüksek Lisans Programı

DANIŞMAN

Doç. Dr. Kazım YILDIZ

EŞ-DANIŞMAN

Prof. Dr. Ali BULDU

İSTANBUL, 2021

ÖNSÖZ

Tez çalışmamın araştırılmasında ve yürütülmesinde her daim destek olan, her fırsatta yardımını esirgemeyen değerli danışmanım Doç.Dr. Kazım YILDIZ'a, eşdanışmanım Prof. Dr. Ali BULDU'ya

Tez çalışmam boyunca desteği ve sabrı için kıymetli eşime ve bugünlere gelmemde büyük pay sahibi olan değerli anneme ve babama

Teşekkürlerimi sunarım.

ŞUBAT, 2021 **Abdullah Emir ÇİL**

İÇİNDEKİLER

ÖZET

DDOS SALDIRILARININ TESPİTİ VE SINIFLANDIRILMASI İÇİN DERİN ÖĞRENME MODELİ

Günümüzde internet ağları dünyayı birbirine bağlarken birçok uzak kaynağı da kullanıcının yanı başına getirmiştir. İnsanların yanı sıra nesnelerin de bu internet ağına katılmasıyla internet için geniş bir kullanım alanı ortaya çıkmıştır. Bu büyük ağlar, kullanıcılara bir yandan kolaylıklar sağlarken diğer taraftan saldırganların hedeflerine maruz kaldığı için kullanıcılara ve hizmet sağlayıcılara zorluklar da yaşatabilmektedir. Dağıtık hizmet reddi (DDoS) saldırıları, internet hizmetlerini kullanan kurum ve kuruluşlara zarar veren en yaygın siber saldırı türüdür. DDoS saldırıları, diğer siber saldırılardan farklı olarak maliyeti düşük ve güvenlik ürünleri tarafından engellenmesi zor bir türdür. DDoS saldırılarında gönderilen ağ trafiğinin büyük olması nedeniyle ağ trafiğini analiz etmek ve saldırı gerçekleşmeden önce tespit etmek çok önemlidir.

Bu tez çalışmasının amacı, anormal trafiği tespit eden ve ağ trafiğini sınıflandıran bir derin öğrenme modeli önermektir. Deep Neural Network (DNN), hem özellik çıkarma hem de sınıflandırma özelliklerini içeren çok katmanlı bir yapıya sahip olduğu için ağ trafiğinin analizinde önemli bir avantaj sağlamaktadır. DNN modeli önerebilmek ve eğitmek için CICDDoS2019, CICIDS2017 ve NSL-KDD gibi güncel verisetleri tercih edilmektedir. Ayrıca DDoS saldırılarını simüle edebilmek adına sanal ağ ortamı kurulmuş ve bu ağdan elde edilen paketlerle özgün bir veriseti hazırlanmıştır. Deneyler sonucunda önerilen DNN modeli sanal ağ ortamında oluşturulan veriseti üzerinde uygulanmıştır.

ŞUBAT, 2021 **Abdullah Emir ÇİL**

ABSTRACT

DEEP LEARNING MODEL FOR DETECTION AND CLASSIFICATION OF DDOS ATTACKS

Today, internet networks not only connect the Earth, but also bring many remote sources closer to the user. With participation of objects besides people to this internet network, a wide area of use for the internet has emerged. While these large networks provide convenience to the users, they may also cause difficulties for users and service providers as they are exposed to the targets of attackers. Distributed denial of service (DDoS) attacks are the most common type of cyber attack that harms organizations and institutions using internet services. Unlike other cyberattacks, DDoS attacks are low-cost and difficult to prevent by security products. Due to the large network traffic of packets sent in DDoS attacks, it is very important to analyze the network traffic and detect it before the attack occurs.

The aim of this thesis is to propose a deep learning model that detects abnormal traffic and classify network traffic. Deep Neural Network (DNN) provides an important advantage in network traffic analysis, as it has a multi-layer structure that includes both feature extraction and classification features. Current datasets such as CICDDoS2019, CICIDS2017 and NSL-KDD are preferred to propose and train the DNN model. In addition, in order to simulate DDoS attacks, a virtual network environment was established and a unique dataset was prepared with packets obtained from this network. The proposed DNN model as a result of the experiments is applied on the dataset generated in the virtual network environment.

FEBRUARY, 2021 **Abdullah Emir ÇİL**

SEMBOLLER

i	:	Gizli katman sayısı
j	:	Nöron sayısı
x	:	Girdi vektörü
w_{ij}	:	Nöronun ağırlık vektörü
z	:	Nöronun ön yargı değeri
α_j	:	Net girdi değeri
β_j	:	Nöronun çıktı değeri
g_i	:	Aktivasyon fonksiyonu
e	:	Euler sayısı
$\sum$	:	Toplam
q	:	Tahmin edilen olasılık
p	:	Gerçek olasılık
L	:	Kayıp fonksiyonu
log	:	Doğal logaritma
m_t	:	Birinci moment gradyanları
∇g_t	:	Gradyanlar
t	:	Adım sayısı
v_t	:	İkinci moment gradyanları
λ	:	Adım boyutu
ϵ	:	Çok küçük bir değer
W_t	:	Ağırlık vektörü
u_t	:	Üssel ağırlıklı sonsuzluk normu
θ_t	:	Güncellenmiş parametre
Ω	:	Üssel bozulma oranı

KISALTMALAR

ACK	**:**	Acknowledgement
ADAM	**:**	Adaptive Moment Estimation
ADAMAX	**:**	Adaptive Max Pooling
BotNet	**:**	Robot Network
CharGen	**:**	Character Generator Protocol
CLDAP	**:**	Connectionless Lightweight Directory Access Protocol
CNN	**:**	Convolutional Neural Network
DBN	**:**	Deep Belief Network
DCNN	**:**	Deep Convolutional Neural Network
DDoS	**:**	Distributed Denial of Service
DNN	**:**	Deep Neural Network
DNS	**:**	Domain Name System
DT	**:**	Decision Tree
FNN	**:**	Feed Forward Neural Network
HIDS	**:**	Host-based Intrusion Detection System
HIPS	**:**	Host-based Intrusion Prevention System
HTTP	**:**	Hypertext Transfer Protocol
HTTPS	**:**	Hypertext Transfer Protocol Secure
ICMP	**:**	Internet Control Message Protocol
IDPS	**:**	Intrusion Detection and Prevention System
IDS	**:**	Intrusion Detection System
IoT	**:**	Internet of Things
IP	**:**	Internet Protocol
IPS	**:**	Intrusion Prevention System
ISO	**:**	International Organization for Standardization
KNN	**:**	K- Nearest Neighbors
LDAP	**:**	Lightweight Directory Access Protocol
LSTM	**:**	Long Short Term Memory
MLP	**:**	Multilayer Perceptron
MSSQL	**:**	Microsoft SQL Server

NB : Naive Bayes

NETBIOS : Network Basic Input/Output System

NIDS : Network Intrusion Detection System

NIPS : Network Intrusion Prevention System

NSAE : Normalized Sparse Autoencoder

NTP : Network Time Protocol

OSI : Open Systems Interconnection

ReLu : Rectified Linear Unit

Rmsprop : Root Mean Square Propagation

RNN : Recurrent Neural Network

SDN : Software-Defined Networking

SGD : Stochastic Gradient Descent

SMTP : Simple Mail Transfer Protocol

SNMP : Simple Network Management Protocol

SSDP : Simple Service Discovery Protocol

SVM : Support Vector Machine

SYN : Synchronize

TCP : Transmission Control Protocol

TFTP : Trivial File Transfer Protocol

UDP : User Datagram Protocol

UPnP : Universal Plug and Play

URL : Uniform Resource Locator

ŞEKİL LİSTESİ

SAYFA

TABLO LİSTESİ

SAYFA

1. GİRİŞ

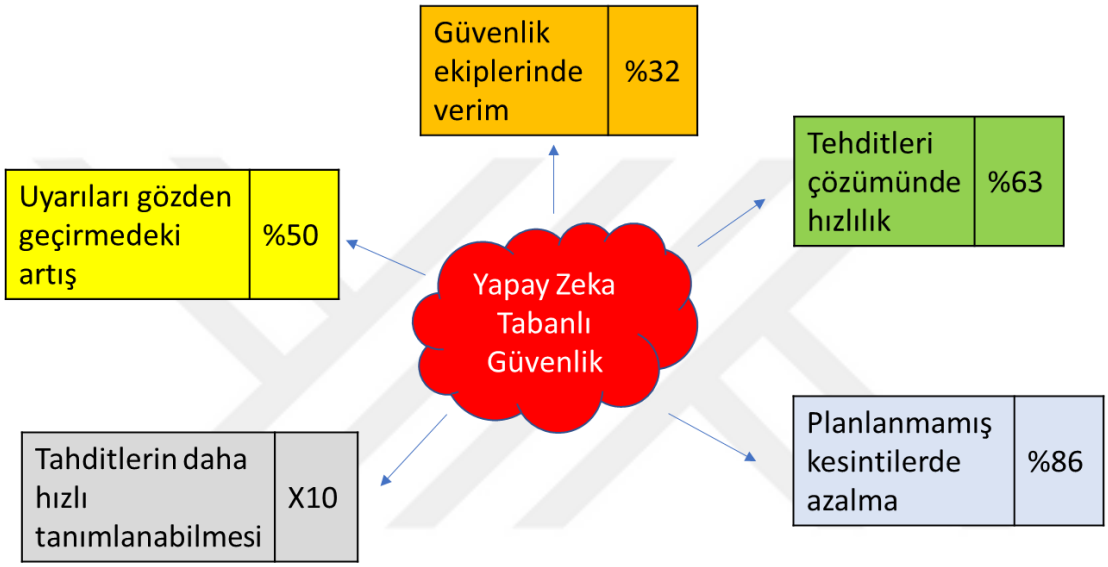
Birbirinden uzak yerleşimlerde yaşayan insan nüfusu için iletişim kanallarının geliştirilmesi en önemli gereksinim olmuştur. İnsanlar birbirleri ile irtibat kurmada tarih boyunca çeşitli iletişim araçları kullanmıştır. İletişim araçlarının gelişimi posta güvercinleri, mektuplar, ulaklar gibi canlı aracıların kullanıldığı yöntemlerden bir uçtan diğer uca bağlı ağ üzerinden elektrik akımıyla iletişimin sağlandığı telgraflar ile devam etmiştir. Teknolojinin gelişmesiyle kişisel kullanım amacıyla yaygınlaşan bilgisayarların birbiriyle konuşma gereksinimi doğmuştur. Bu gereksinimden günümüzün haberleşmesinin vazgeçilmezi olan bilgisayar ağlarından oluşmuş internet meydana gelmiştir.

İnternet sadece iletişim aracı olmakla kalmamış aynı zamanda hayatın devamlılığının sağlanmasında etkin rol oynamaya başlamıştır. İnternet kullanımının yaygınlaşmasıyla birçok sektör hizmetlerini bu kanal üzerinden vermeyi hedeflemiştir. Bu hedef doğrultusunda finansal işlemler, alışverişler, eğlence gibi birçok alan için oluşturulmuş internet siteleri kullanıcılarına hizmet vermektedir. İnternetin kapsama alanı bununla da kalmayıp nesneler de bu iletişim kanalını kullanmaya dahil olmuştur. Artık her alanda yer bulmaya başlayan bağlantılı cihazlarında internet ağına dahil olmasıyla Nesnelerin İnterneti (IoT) kavramı ortaya çıkmıştır.

İnsanların ve cihazların yaygın bir şekilde internet ağını kullanmasının saldırganların hedefi olması kaçınılmaz bir durumdur. Saldırganlar tarafından internet ve bilgisayar teknolojisinin kullanıldığı bu tür saldırılar, siber saldırı olarak adlandırılmıştır. Son zamanlarda siber saldırılar içerisinde kolay ve yaygın olarak (Distributed Denial of Service) DDoS saldırıları kullanılmaktadır [1]. DDoS saldırıları düzenlenirken saldırganlar genellikle kurbanların cihazlarına zararlı yazılımlar bulaştırmakta ve hedefleri doğrultusunda bu cihazları yönetmektedir. DDoS saldırıları interneti kullanan kuruluşların hizmetini kesintiye uğratmaktadır. Bu yüzden bu saldırıların tespit edilmesi ve önlenmesi büyük öneme sahiptir. İnsan etkileşimli çeşitli güvenlik ürünleri ve yazılımları kullanılmasına rağmen güvenliğin sağlanmasında yetersiz kalınabilmektedir. Dolayısıyla sistemlerin otomatikleştirilmesi ve yapay zekaya başvurulması DDoS ile mücadelede kritik bir rol oynayabilmektedir. Yapay zeka destekli güvenlik ürünleri insanların yapabileceğinden daha etkili sonuçlar üretebilmektedir. Yapılan bir çalışmada

yapay zeka tabanlı bir güvenlik ürünü kullanmanın avantajları görüldüğü gibi Şekil 1.1' de ölçeklendirilmiştir [2]. Siber güvenlik alanında yapay zeka kullanımı sayesinde tehditlerin çözüm hızında %63 oranında artış sağlanmakta, tehditler 10 kat daha hızlı tanımlanabilmekte ve planlanmamış kesintiler %86 oranında azalmaktadır. Ayrıca Yapay zeka tabanlı güvenlik ürünleri sayesinde güvenlik ekiplerinin verimi %32 oranında artarak gelen uyarıların gözden geçirilme hızı %50 oranında artmaktadır.

.



Şekil 1.1. Siber güvenlikte yapay zekâ kullanımının etkisi. [2]

1.1. Genel Bakış

DDoS saldırıları, diğer siber saldırılardan farklı olarak maliyeti düşük ve güvenlik ürünleri tarafından engellenmesi zor bir türdür. DDoS saldırıları için gerekli temel elemanlar "BotNet (Robot Network)" olarak adlandırılan zararlı yazılımlar ile kontrol altına alınmış cihazlar ve zafiyete açık legal sunuculardır. Günümüzde zararlı yazılım bulaşmış cihazların Şekil 1.2'deki gibi olduğunu göz önünde bulundurduğumuzda ve internet üzerinde çeşitli hizmetler vermek için kurulmuş birçok sunucunun mevcut olduğunu gözlemlediğimizde DDoS saldırılarının hızla artacağını beklemek yerinde olmaktadır [3].

Sıralama	Ülke	2020 Ç2	Ç1'den Ç2'ye Değişim
1.	ABD	896	%7
2.	Rusya	812	%32
3.	Hollanda	337	%61
4.	Almanya	185	%7
5.	Singapur	131	%157
6.	Fransa	108	%35
7.	Birleşik Krallık	89	%37
8.	Çin	74	-%15
9.	Bulgaristan	72	%38
10.	Macaristan	70	-

Şekil 1.2. Zararlı yazılım bulaşmış bilgisayar ağının (BotNet) zirvedeki 10 bölgesi [3].

Şekil 1.2 incelendiğinde zararlı yazılım bulaşmış bilgisayar sayısı bakımından ABD ve Rusya'nın diğer ülkelerden açık ara önde olduğu görülmektedir. Ayrıca Spamhaus'un yayınladığı bu raporda görüldüğü gibi 2020'nin 1. Çeyreği ile 2. Çeyreği arasındaki değişim incelendiğinde zararlı yazılım bulaşmış cihazlarda hızlı bir artış yaşanmaktadır.

Buna ek olarak Nexusguard'ın 2020 yılının 1.çeyreğinde yayınladığı tehdit raporuna göre DDoS saldırılarının 2019 yılının 1.çeyreğinde %278.17 arttığı, 2019 yılının 4. çeyreğinde ise %542.46 arttığı görülmektedir [4].

1.1.1. Problemin tanımı

DDoS saldırıları hızlı gerçekleştiği ve büyük paket boyutlarına ulaşabildiği için internet ağı üzerinden hizmet veren sistemlerin hizmet dışı kalmasına sebep olmaktadır. Aynı zamanda normal kullanıcıların internet servislerine yoğun erişim yaptığı dönemlerde saldırganlar bu durumu istismar ederek DDoS saldırıları gerçekleştirebilmektedir. İnternet üzerinden hizmet veren bu servislerin kullandığı ağı hızlı analiz edip anlık tespitler ve alarmlar üreten sistemler tasarlanmalıdır.

1.1.2. Amaç ve hedef

Bu tez çalışmasında ağdaki trafikte DDoS saldırısı olup olmadığını ayıran eğer DDoS saldırısı içeriyorsa ne tür bir saldırı olduğunu sınıflandıran bir derin öğrenme modeli geliştirilmesi amaçlanmıştır. Derin öğrenme modelinin hem özellik çıkarma hem de

sınıflandırma süreçlerini içeren yapısıyla sığ makine öğrenme algoritmalarına göre performans ve doğruluk açısından daha avantajlı olması derin öğrenme yöntemini benimsemedeki motivasyon olmuştur. Derin öğrenme modeli ile ağ analiz edilerek DDoS saldırılarının tespiti ve sisteme büyük zararlar verilmeden erken uyarı mekanizmasıyla saldırıların önlenmesine katkı sağlanması hedeflenmiştir.

1.1.3. Ana katkılar

Önerilen derin öğrenme modeliyle yaygın olarak kullanılan hazır verisetleri üzerinde eğitim yapılmış ve diğer yapılmış çalışmalardaki yöntemlerden daha başarılı sonuçlar elde edilmiştir. Python diliyle hazırlanmış DDoS saldırı çeşitlerinin simüle edileceği tamamen özgün bir ortam oluşturulduktan sonra elde edilen veriler üzerinde gerçek zamanlı denemeler ile saldırı tespitleri incelenmiştir. Ayrıca derin öğrenme modelinde kullanılacak optimizasyon algoritmalarının oluşturulma durumu araştırılmıştır.

1.1.4. Tez organizasyonu

Tez dört bölümden oluşmaktadır. "Giriş" bölümünde DDoS ile ilgili genel bilgilere, DDoS saldırıları ile ilgili istatistiklere ve literatür çalışmalarına yer verilmiştir. İkinci bölümde "Materyal ve Yöntem" bölümünde kullanılan verisetlerinden, derin öğrenme ile ilgili bilgilerden ve önerilen model ve mimarisinden bahsedilmiştir. Üçüncü olarak "Bulgular ve Tartışma" bölümünde deney ortamı, deney performansı ve sonuçları anlatılmıştır. Son bölümde "Sonuçlar" bölümünde ise çalışma genel olarak özetlenerek sonuca bağlanılmış ve gelecekte nasıl çalışmalar yapılacağı yer almıştır.

1.2. DDoS Nedir?

DDoS saldırısı, büyük miktarlarda paket göndermek için sahte Internet Protocol (IP) kaynaklarıyla ya da virüs bulaşmış bilgisayar topluluğuyla saldırının hedefindeki kurbanın makinesinin kaynağını tüketerek veya ağın bant genişliğini, kapasitesinin üzerindeki paketlerle taşırarak hizmet reddine sebep olan saldırı türüdür [5, 6]. DDoS saldırılarının temel amacı internet üzerinden alınan hizmetlere kullanıcıların erişimini engellemektir [7]. DDoS saldırıları, internet ağını kullanan servislerin hizmet kesintisine yol açtığı için önemli zararlara neden olmaktadır [5]. DDoS Saldırılarının verdiği maddi zarara örnek olarak 2015 yılında bir havayolu şirketine yapılmış büyük bir DDoS saldırısı

gösterilebilir. Şirketin sistemlerinin çökmesi sonucu 10 uçuşun iptali ve 12 uçuşun rötarı gerçekleşerek 1400 yolcu bu durumdan etkilenmiştir [8].

1.2.1. Saldırı örnekleri

DDoS saldırılarının büyüklüğünü arttırmak için iki önemli kaynak kullanılmaktadır. Bunlardan birisi bilgisayar ve IoT cihazlarına zararlı yazılımlar bulaştırılarak oluşturulan BotNet'ler, ikincisi ise çeşitli hizmetler veren sunuculardır.

1.2.1.1. IoT cihaz kullanımı

ABD'de Maryland Üniversitesi'nde yapılan bir çalışmaya göre gerçekleştirilen siber saldırıların manuel yapılmak yerine kod parçacıklarının kullanıldığı zararlı yazılımlar yardımıyla otomatik olarak yapıldığı tespit edilmiştir. Ayrıca bu çalışmaya göre IoT cihazlarının yönetildiği uygulama arayüzüne ya da kontrol panellerine ait parolaların daha basit ve tahmin edilebilir olması saldırganların bu cihazlara erişimini de kolaylaştırmaktadır. Sonuç olarak zararlı yazılımlarla otomatize edilmiş saldırıların IoT cihazlarıyla kullanımı DDoS saldırılarının artmasına sebep olmaktadır [9]. IoT cihazlar için kullanılan zararlı yazılımlardan ismini öne çıkartanlardan biri de "Mirai" zararlı yazılımıdır.

Mirai zararlı yazılımı, IoT cihazlarda sıklıkla kullanılan benzer kullanıcı adı-parola ikilisindeki zafiyetten yararlanan kötü amaçlı bir yazılım olup bu ikiliyi çözerek Telnet protokolü üzerinden IoT cihazların yönetim paneli oturumuna izinsiz erişim sağlar. Oturum açıldıktan bu panele bağlı IoT cihazları sömürerek DDoS saldırısı başlatmak için kullanmaktadır. 2016 yılında, Reddit, Paypal, Netflix, Spotify, Twitter gibi platformlarında Domain Name System (DNS) hizmeti aldığı DYN şirketine Mirai zararlı yazılımı kullanılarak IoT cihazları üzerinden çok büyük bir DDoS saldırısı gerçekleştirilmiştir. Saldırı sonucu bahsedilen platformlarda da hizmet kesintileri yaşanmıştır [10].

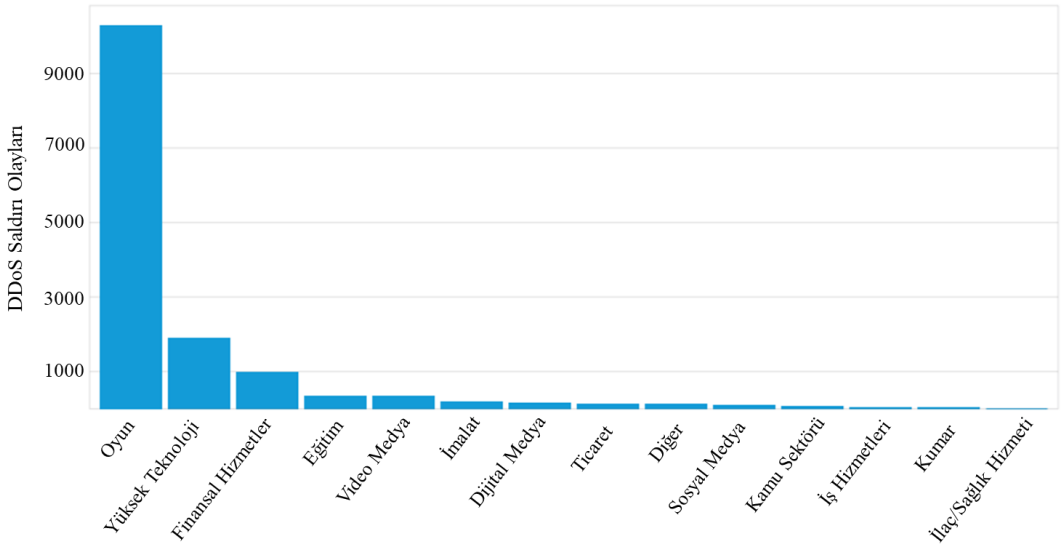
2016 yılının raporuna göre bilgisayarlarına zararlı yazılım bulaşmış ülkeler içerisinde Çin %49'luk ve Tayvan %47.34'lük bir oranla ilk sıralarda yer alırken %40.99 ile Türkiye üçüncü sırada gelmektedir. Ayrıca Akamai'ye göre DDoS saldırıları 2015'ten 2016 yılına %4 artarken 100Gbps ve üzeri büyüklüğe sahip saldırılar %140 arttığı rapor edilmiştir [11].

STM tarafından yayınlanan rapora göre 2017 yılında IoT cihazları aracılığıyla yapılan siber saldırıların 2016 yılına oranla %600'lük bir artış yaşandığı belirtilmektedir. IoT cihazların saldırı için kullanımında ülke bazında ilk sırayı %21 ile Çin alırken ardından sırasıyla ABD %10.6 ve Brezilya %6.9 oranla takip etmiş, Türkiye ise %4.1 ile yedinci olmuştur. Bunun yanında, IoT cihazlardan oluşturulan BotNet'ler aracılığıyla DDoS saldırıların yaygın olarak gerçekleştiği görülmektedir [12].

Akamai firmasının hazırladığı internet güvenliği raporuna göre 2017 yılında DDoS saldırılarında %28 artış olduğu kaydedilmiştir. Bu artışta Pbot zararlı yazılımının bulaştırıldığı BotNet kullanımının büyük etkisinin olduğu görülmüştür [13].

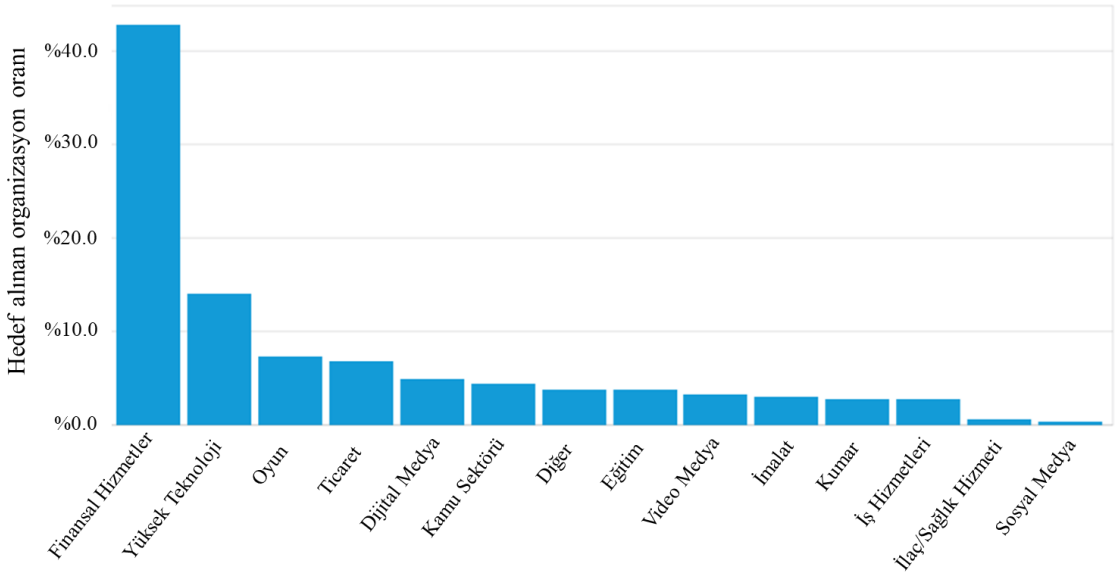
1.2.1.2. Küresel genel sunucuların kullanımı

Hizmete özel sunucuların istismar edilmesiyle gerçekleştirilen en büyük saldırılardan birisine verilecek en iyi örnek GitHub platformudur. 2018 yılında yazılım geliştiricilerin kod deposu için kullandığı GitHub web sitesine 1.35 Tbps büyüklüğünde DDoS saldırısı gerçekleşmiştir. Ardından başka bir ABD'li şirkete 1.7 Tbps büyüklüğünde bir DDoS saldırısı yapılmıştır. Bu iki saldırının da ortak noktası, web sitelerinin ve uygulamalarının hızını arttırmak için kullanılan dağıtılmış önbelleğe alma sistemi olan Memcached sunucularının kullanılmasıdır. Memcached sunucularına gönderilen sahte isteklerle paketlerin boyutunun arttırıldığı bir yansıma saldırısı yapılmıştır [14-16]. Akamai'nin Aralık 2017 ile Kasım 2019 tarihleri arası için hazırladığı raporda DDoS saldırılarının en çok hedefi olan ilk üç sektör Şekil 1.3'te yer alan grafikte görüldüğü gibi oyun, ileri teknoloji ve finansal hizmet sektörleri olmuştur [17].



Şekil 1.3. Aralık 2017–Kasım 2019 aralığında gerçekleştirilmiş DDoS saldırılarının sayısı [17].

Akamai'nin raporuna göre Aralık 2017 ile Kasım 2019 tarihleri arasında DDoS saldırısının hedef aldığı organizasyonlardan %40'ından fazlasını finansal hizmet veren kuruluşların oluşturduğu Şekil 1.4'te görülmektedir [17].



Şekil 1.4. Aralık 2017 – Kasım 2019 aralığında gerçekleştirilen DDoS saldırılarının hedef aldığı sektörlerdeki kuruluş sayılarının oransal gösterimi [17].

2019 Nisan ayında büyük bir bankaya, 160 Gbps bant genişliğine sahip saniyede 32 milyon paket gönderimiyle zirveye ulaşan bir DDoS saldırısı gerçekleşmiştir. Bu saldırıda Synchronize (SYN) Seli, User Datagram Protocol (UDP) Seli, UDP fragmentation, RESET Seli, Network Basic Input/Output System (NETBIOS) Seli, ve

Bağlantısız Hafif Dizin Erişim Protokolü (CLDAP) reflection olmak üzere 6 adet DDoS saldırı çeşidi kullanılmıştır [17].

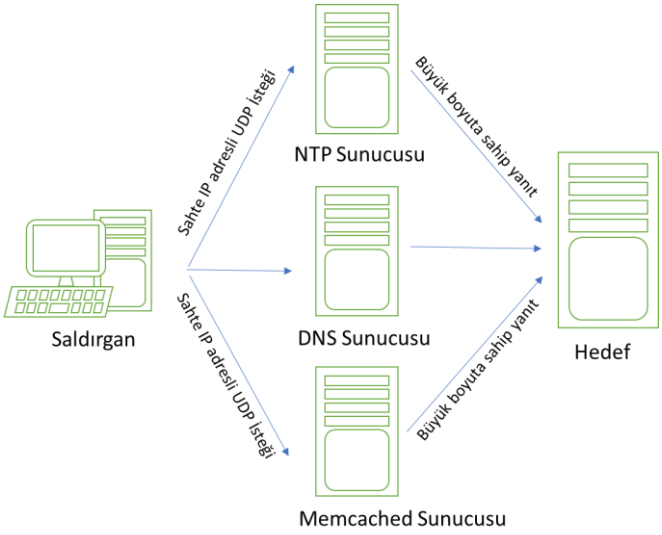
2019 yılında yeni bir versiyonu çıkan Gafgyt zararlı yazılımı, genellikle oyun sunucularına saldırmak ve BotNet ağı oluşturmak için Zyxel, Huawei ve Realtek gibi ev ve ofis tipi yönlendiricilere bulaşarak büyük bir DDoS saldırısı tehdidi oluşturmaktadır [10].

1.3. DDOS Saldırı Yöntemleri

DDoS Saldırıları gerçekleştirildiği ortamlar ve hedefe verdiği zarar yöntemlerine göre temelde Volümetrik, Protokol Katmanı, Uygulama Katmanı Saldırıları olmak üzere üç tipe ayrılmaktadır. Bu DDoS saldırı yöntemlerinde saldırganlar, ağ trafiğinin yoğunluğunu arttırıcı büyük miktarlarda paket göndermek için kurbanın sistemlerden istek talep ediyormuş gibi gösterildiği sahte IP kaynaklarıyla veya kurbanların bilgisayarlarına yerleştirilmiş kötü amaçlı yazılımlarla kontrol edilen bilgisayarları kullanır.

1.3.1. Volümetrik saldırılar

"Amplification (Kuvvetlendirmeli)" saldırılar olarak da bilinen Volümetrik DDoS saldırıları, ağa gönderilen paketlerle yüksek ağ trafiğine neden olarak internet bant genişliğini tükettiği için hizmet almak isteyen normal kullanıcıların isteklerine yanıt vermemesine neden olur. Dolayısıyla internet altyapısını kullanan tüm servisleri etkileyerek hepsini devre dışı bırakacaktır [18-20]. Bu tip saldırılara Geçiş Kontrol Protokolü (TCP)/UDP Seli, DNS/ Ağ Zaman Protokolü (NTP)/Memcached Kuvvetlendirmeli DDoS saldırıları örnek gösterilebilir. En yaygın kullanılan DDoS saldırı çeşidi olan bu saldırılarda, Şekil 1.5'te görüldüğü gibi saldırganlar genele hizmet veren sunuculardaki DNS, NTP, Basit Hizmet Bulma Protokolü (SSDP), Memcached vb. protokollerini kullanarak küçük boyutta gönderdiği paketlerini çok büyük boyutlara ulaştırmak için kullanmaktadır.



Şekil 1.5. Volümetrik DDoS saldırı yapısı.

1.3.2. Protokol saldırıları

İnternet üzerinden farklı cihazların birbirleriyle nasıl iletişim kuracağı Uluslararası Standardizasyon Örgütü (ISO) tarafından Açık Sistem Arabağlantısı (OSI) modeliyle belirlenmiştir. OSI Modelinde en alt katmandan başlayarak sırasıyla Fiziksel Katman, Veri Bağlantısı Katmanı, Ağ Katmanı, Taşıma/iletim Katmanı, Oturum Katmanı, Sunum Katmanı, Uygulama Katmanı olmak üzere 7 katman bulunmaktadır. Her katmanın içerisinde iletişim için çeşitli protokoller bulunmaktadır.

Protokol DDoS saldırıları, Ağ Katmanı veya Taşıma/iletim Katmanı protokolleri üzerinden gerçekleştirilerek bu katmanı kullanan Güvenlik Duvarları, Yönlendiriciler, Yük Dengeleme Cihazları gibi ağ ve güvenlik cihazlarını hedef alır. Bir oturum açma işlemi tamamlanmadan çok miktarda oturum açma talebinde bulunan bu saldırı, bu cihazların oturum kontrolü için tutulan tablolarını aşırı istekle doldurarak etkisiz hale getirir. Bu tip saldırılara SYN/SYN-ACK(Acknowledgement)/ACK Seli, Smurf DDoS, Ping of Death vb. örnek gösterilebilir.

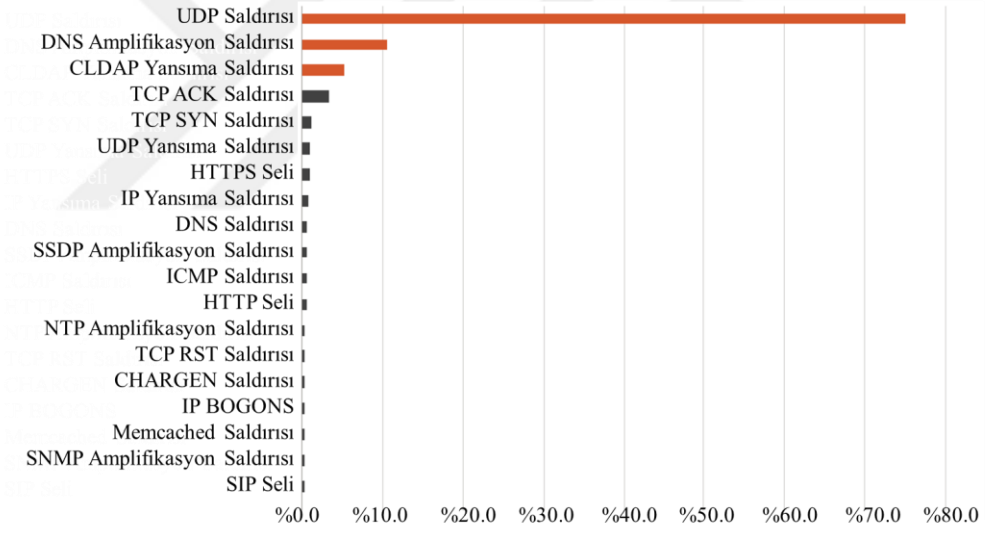
1.3.3. Uygulama katmanı saldırıları

Bu tip DDoS saldırıları, saldırı hedefindeki DNS, Basit Posta Aktarım Protokolü (SMTP) vb. web uygulama servislerine ait kaynak makinelerine gelen isteklere yanıt verme kapasitesini aşan paketlerin gönderilmesiyle hizmeti kesintiye uğratmayı amaçlayan saldırılardır. Bu tip saldırılara Hiper Metin Aktarım İletişim Protokolü (HTTP), Güvenli

Hiper Metin Aktarım İletişim Protokolü (HTTPS), SMTP ve DNS servislerine yapılan sel saldırıları örnek gösterilebilir [21].

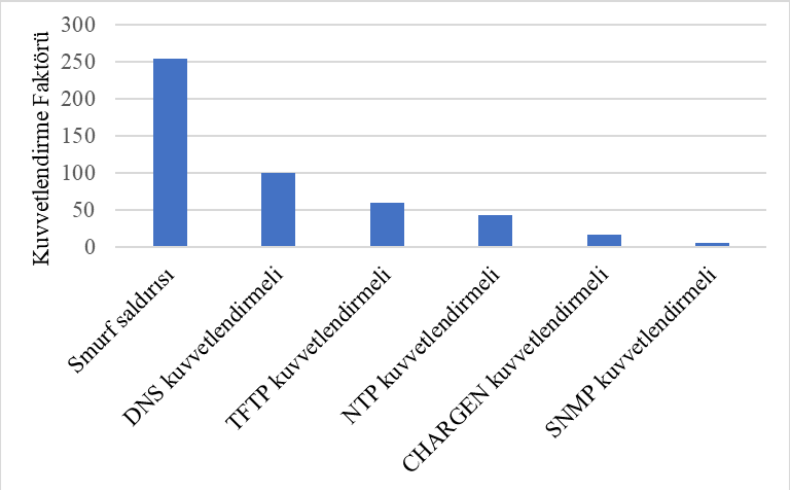
1.4. DDoS Saldırı Çeşitleri

DDoS saldırıları içinde "flood (sel)" saldırıları, yansıma saldırıları ve kuvvetlendirmeli saldırılar yaygın olarak kullanılmaktadır. Sel tipi saldırılar hedefteki kurban sisteme aralıksız istekler gönderilen simetrik bir saldırıdır [22]. Genellikle BotNet'lerin kullanıldığı bu saldırı tiplerine SYN, UDP, İnternet Kontrol Mesajı Protokolü (ICMP), HTTP sel saldırıları örnek verilebilir. Nexusguard'un 2020 yılı 1. çeyrek tehdit raporuna göre Şekil 1.6'daki grafikte UDP sel saldırıları tüm saldırıların %75'ini oluştururken DNS kuvvetlendirmeli ve CLDAP yansıma saldırıları sırasıyla %10.49 ve %5.27'ını oluşturmaktadır [4]. Sonuç olarak, sel saldırılarının saldırganlardan tarafından çok yoğun bir şekilde kullanıldığı görülmektedir.



Şekil 1.6. 2020 yılı 1.çeyrek dönemi için DDoS saldırı çeşitlerinin dağılımı [4].

Kuvvetlendirme anlamına gelen amplifikasyon tipi saldırılar, sel tipi saldırılardan farklı olarak küçük bir sorgu isteğiyle başlatılıp büyük yanıtların oluşturulmasını meydana getiren asimetrik saldırılardır [22]. Bu saldırı tipinde zafiyet bulunan DNS, Önemsiz Dosya Aktarım Protokolü (TFTP), NTP gibi sunucularında bulunduğu her çeşit sunucu saldırıyı kuvvetlendirmek amacıyla kullanılmaktadır. Şekil 1.7'de DDoS kuvvetlendirme saldırılarında en çok kullanılan sunucu çeşitlerinin saldırıyı kaç kat arttırabileceği görülmektedir [23].

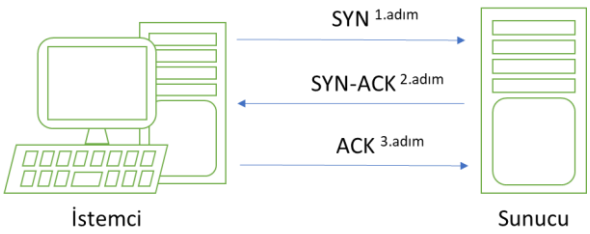


Şekil 1.7. Kullanılan kuvvetlendirme çeşitlerinin DDoS saldırılarının katlanmasına etkisi [23].

Kuvvetlendirme saldırıları sunucuların özelliğine göre çok yüksek boyutlu saldırılara sebep olabileceği için en tehlikeli saldırı tipi olmaktadır. Sonuç olarak iki ana kategoriye ayrılan DDoS saldırı çeşitleri bu bölümde tanıtılacaktır.

1.4.1. SYN Seli saldırısı

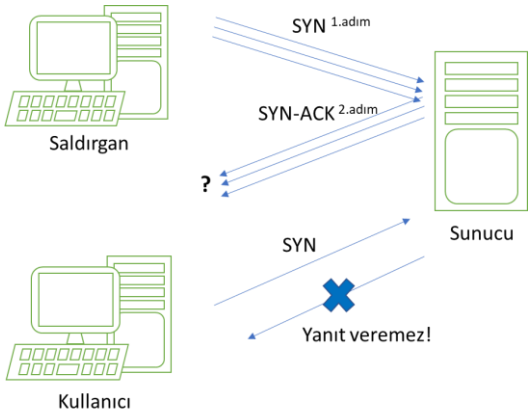
SYN Seli saldırısı, bir volümetrik saldırı yöntemi olup TCP bağlantısı sırasında "üç yönlü el sıkışma" yöntemi olarak bilinen bir zayıflıktan yararlanır. Şekil 1.8.'de görülen "üçlü yönlü el sıkışma" yönteminde, bir sunucuyla TCP bağlantısı başlatmak için ilk olarak istemci tarafından bir SYN isteği gönderilir.



Şekil 1.8. TCP bağlantısının kurulması.

İstemciden gelen SYN isteğine, sunucu tarafından SYN-ACK yanıtı verilmesi gerekir ve ardından istemciden gelen bir ACK yanıtı ile bağlantı onaylanır. Şekil 1.9'da gösterilen SYN Seli saldırısında, istekte bulunan istemcinin birden çok SYN isteği göndermesi ya da sahte bir IP adresinden SYN istekleri göndermesi sonucu SYN-ACK yanıtını veren sunucu isteklerin her biri için ACK yanıtı gelene kadar beklemeye devam eder. Yeni

bağlantı kurulamayacak şekilde kaynakları tükenen sunucunun durumu hizmet reddi ile sonuçlanır [24-26].



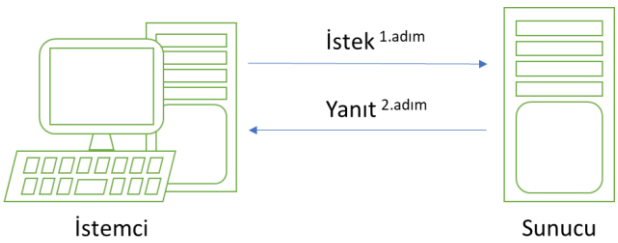
Şekil 1.9. SYN Seli DDoS saldırısı.

1.4.2. Neptune saldırısı

TCP bağlantısında yer alan üç yollu el sıkışma zafiyetinden yararlanılan bu saldırı tipi bir önceki başlıkta yer alan SYN Seli sadırısında anlatılan yöntemin aynısını kullanmaktadır. Saldırganlar hedef sunucuya çok sayıda SYN paketi göndererek sunucuyu ACK paketlerini beklemeye maruz bırakır. SYN paketleriyle meşgul olan sunucu yeni bağlantılara cevap veremeyerek hizmet dışı kalır [27,28].

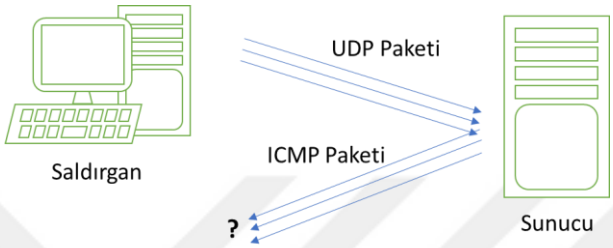
1.4.3. UDP Seli saldırısı

Bir UDP Seli, hedefteki bir sunucuyu UDP paketleri ile dolduran bir DDoS saldırısıdır. Şekil 1.10'da gösterilen UDP bağlantısında TCP'den farklı olarak üçlü el sıkışma gibi bir uçtan uca doğrulama mekanizması olmayıp istemcinin isteklerine cevap verilmesiyle veri iletişimi sağlanmaktadır. Bu nedenle UDP bağlantısında IP adresi doğrulama seçenekleri çok sınırlıdır [29].



Şekil 1.10. UDP bağlantısının kurulması.

UDP Seli saldırılarında sunucunun kaynaklarını tüketip çökertmek için çok sayıda kaynak IP kullanılarak sahte UDP paketleri hedef sunucuya gönderilir. Ayrıca, bu saldırının daha büyük etkiye sahip olması için hedef sunucunun port ve IP adresi sahte UDP paketlere dahil edilerek rastgele sunuculara veya ağ içindeki belirli bir sunucuya hedeflenebilir. Şekil 1.11'de gösterildiği gibi bu durum, hedef sunucunun söz konusu portu dinleyen uygulamayı tekrar tekrar kontrol etmesine ve uygulama bulunmadığında bir ICMP 'Hedefe Ulaşılamıyor' paketiyle yanıt vermesine neden olur [24,30].

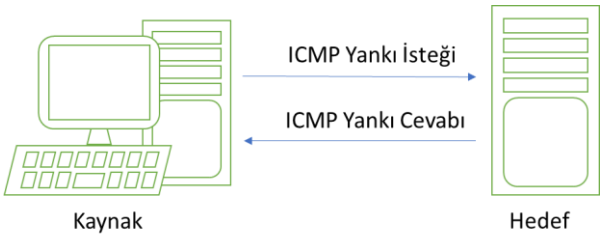


Şekil 1.11. UDP Seli DDoS saldırısı.

Sonuç olarak, sahte UDP paketlerinin hacmi, hedef sunucunun istekleri işleme ve yanıtlamaya yönelik maksimum kapasitesini aşarak hedef sunucunun kaynaklarının tükenmesine sebep olur.

1.4.4. ICMP Seli saldırısı

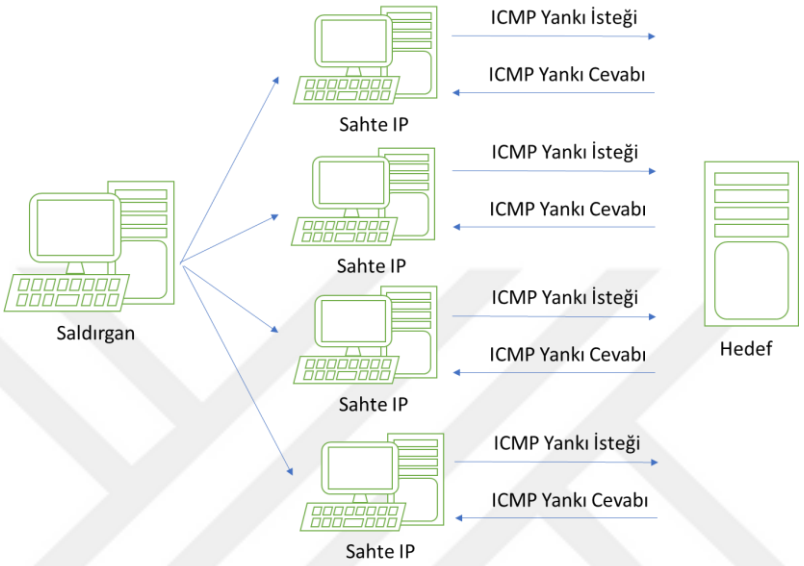
ICMP, UDP'ye benzeyen bir iletişim yapısına sahip olup ağ üzerindeki paketlerin durumu hakkında veya hata geribildirimleri için kullanılmaktadır. ICMP paketlerinin işleyişi, Şekil 1.12' de gösterildiği gibi kaynaktan hedef bilgisayara ICMP yankı istek mesajı gönderildikten sonra hedeften kaynağa ICMP yankı cevap mesajının gönderilmesiyle tamamlanmaktadır.



Şekil 1.12. ICMP mesaj paketlerinin işleyişi.

Şekil 1.13'te yer alan ICMP Seli saldırısı, çok sayıda IP kaynakları kullanılarak çok sayıda sahte ICMP paketinin gönderildiği bir saldırıdır. Bu saldırı, ağı ICMP yankı isteği veya yanıt paketleriyle doldurmayı hedefler. Hedef sunucusu çok miktarda sahte ICMP

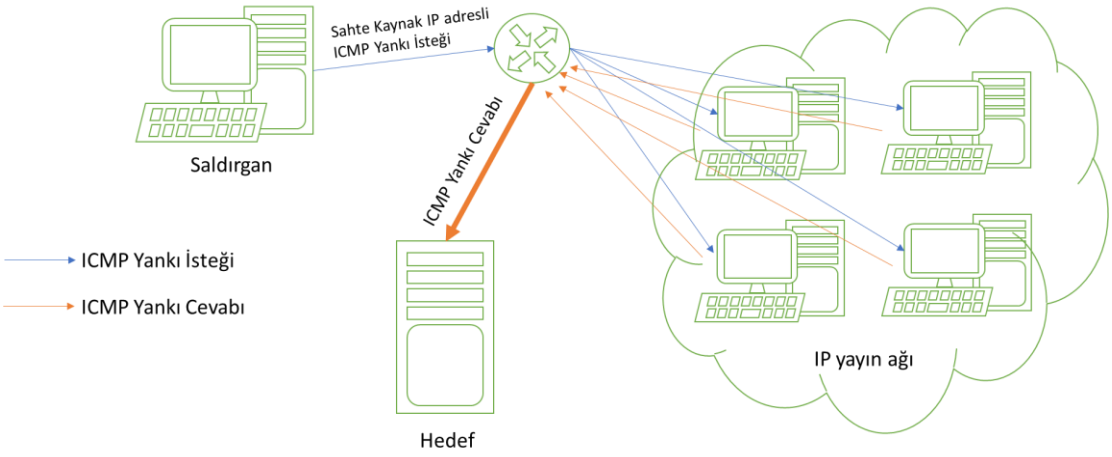
paketi isteklerine yanıt vermekle meşgul olduğundan kaynaklarını tüketerek sunucunun performansı büyük ölçüde düşmüş olur. Aynı zamanda ICMP Seli saldırısının düzenlendiği ağ üzerinden saldırganlar tarafından kaynak adresinin kurbanın adresi gibi gösterildiği çok sayıda IP paketi gönderilmesi sonucu ağın bant genişliği tüketildiğinden gerçek paketlerin de hedeflerine ulaşması önlenir [31].



Şekil 1.13. ICMP Seli DDoS saldırısı.

1.4.5. Smurf saldırısı

Smurf Saldırısı, ICMP paketlerini kullandığı için ICMP Seli saldırısına benzemekle birlikte hedef sunucuya ICMP yankı cevaplarının gönderilmesi yönünden farklılaşmaktadır. Şekil 1.14'te gösterilen bir smurf saldırısında saldırgan, sahte kaynak IP adresi kullanarak zafiyete açık cihazların bulunduğu IP yayın ağına sahte ICMP Yankı İstekleri göndermektedir. Gelen sahte ICMP Yankı İsteklerine karşılık olarak IP yayın ağında bulunan cihazlar tarafından sahte kaynak IP adresinde yer alan hedef sunucuya ICMP Yankı Cevabı iletilmektedir [27,32].



Şekil 1.14. Smurf DDoS saldırısı.

Sonuç olarak hedef sunucunun işleyemeyeceği büyüklükte bir ping Seli olduğundan hedef sunucu çalışamaz hale gelir.

1.4.6. Teardrop saldırısı

TCP/IP modelinde internet üzerinden veri iletilirken paketin büyüklüğüne göre parçalara bölünerek aktarım gerçekleşir. Bu bölme işlemi yapılırken iletilen bilgisayarda tekrar doğru şekilde birleştirme yapılması için paketlerin başlığında parçalanma işaretçisi (Fragment Offset) yer almaktadır. Daha sonra gelen bölünmüş paketlerin birleştirilmesi işlemi bu işaretçiler dikkate alınarak yapılır. Teardrop saldırısı, saldırgan tarafından hatalı parça işaretçisi içeren çok sayıda parçalanmış paketin hedef sunucuya gönderilmesinden oluşmaktadır. Sunucu işaretçisi hatalı olan bu paketleri yeniden birleştiremez ve bu durumun sonucunda hizmet reddi meydana gelir [33].

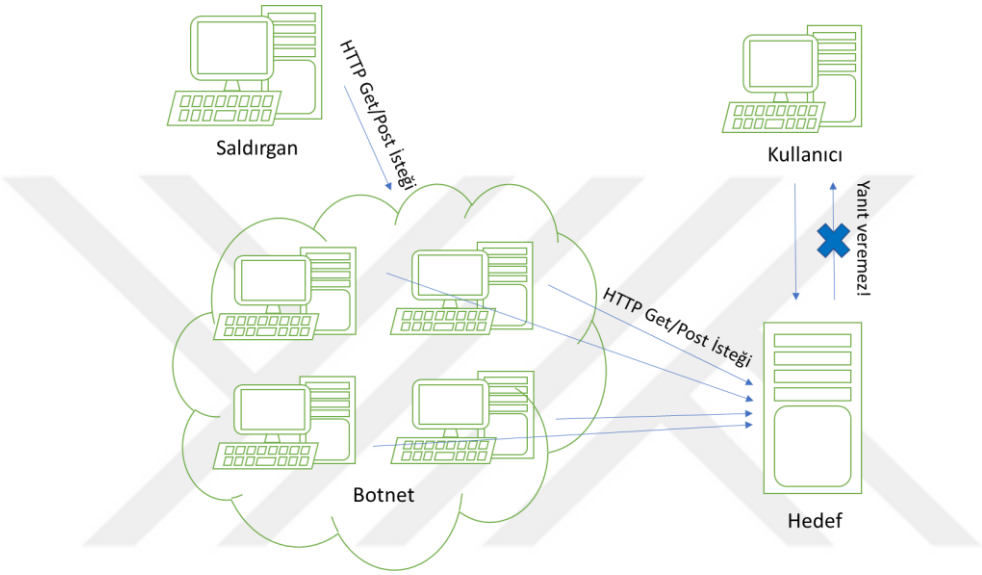
1.4.7. Back saldırısı

Back saldırısında, saldırgan çok sayıda eğik çizgi (“///…//”) içeren hatalı isteklerini Apache Web sunucusunun 80 numaralı bağlantı noktasına sürekli olarak göndererek sunucunun yavaşlamasına sebep olur [27,34,35].

1.4.8. HTTP Seli saldırısı

HTTP, internet üzerinde yer alan sunucu ve istemciler arasındaki iletişimde bilgilerin nasıl iletileceğini belirleyen uygulama katmanı protokolüdür. Bu protokol, web siteleri için kullanılmakta olup HTTP oturumu, istemci sunucudan GET ve POST metotlarıyla sayfa talebinde bulunduktan sonra sunucunun istenilen sayfa bilgisini istemciye

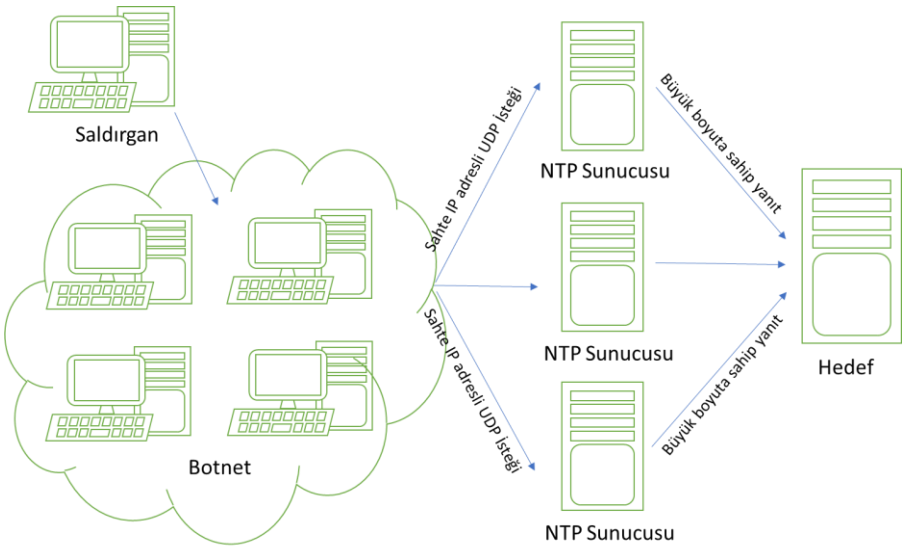
göndermesiyle tamamlanmaktadır. Şekil 1.15'te gösterilen HTTP Seli saldırısında saldırgan, çok sayıda meşru gözüken GET veya POST isteklerini bir sunucuya veya web uygulamasına göndererek sunucunun maksimum kaynakları kullanmaya zorlamaktadır. Bu saldırıda, HTTP isteğinin büyüklüğünü arttırmak için saldırganın kontrol sağladığı zararlı yazılım bulaştırılmış bilgisayarlardan oluşan "BotNet" olarak isimlendirilen ağlar kullanılmaktadır. Saldırının engellenmemesi için zararlı yazılım bulaştırılmış bilgisayarların gerçek IP adresleri kullanılmaktadır [36,37].



Şekil 1.15. HTTP Seli DDoS saldırısı.

1.4.9. NTP kuvvetlendirmeli DDoS saldırısı

NTP, bilgisayar sistemleri arasında saat senkronizasyonunu sağlayan bir ağ protokolüdür. NTP sunucuları saati düzenlenecek cihazın 123 nolu portu üzerinden UDP bağlantısı ile iletişim kurar. Şekil 1.16'da görülen NTP Kuvvetlendirmeli DDoS saldırısı, sahte kaynak IP kullanarak NTP sunucusundan yapılan sorguları hedef sunucuya yönlendirip ağ bant genişliğini doldurmayı amaçlamaktadır.

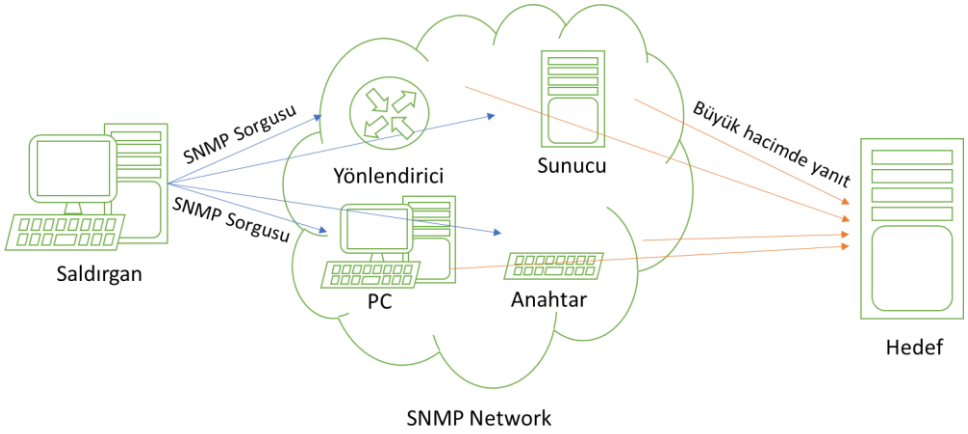


Şekil 1.16. NTP Kuvvetlendirmeli DDoS saldırısı.

Saldırgan, saldırının boyutunu arttırmak için BotNet ağıyla birlikte NTP uygulamasını kullanan son 600 makine listesini sorgulayan *monlist* komutunu kullanmaktadır. Saldırgan, BotNet üzerinden sahte IP adreslerine sahip UDP paketlerini *monlist* komutunun etkin olduğu bir NTP sunucusuna gönderir. Hedef sunucunun gerçek IP adresinin yer aldığı sahte UDP paketlerine NTP sunucusundan büyük bir yanıt gelir. Bu saldırı tipinde gönderilen isteğin neredeyse 200 katına çıkan yanıtlarla saldırı yapılma potansiyeli mevcuttur. Hedef sunucunun IP adresine gelen yanıtlar ağ bant genişliğini aşarak ağ altyapısını kullanan bütün cihazların trafiğin azalmasına neden olur. Bu durum hedef sunucunun servis dışı olmasıyla sonuçlanır [38].

1.4.10. SNMP kuvvetlendirmeli DDoS saldırısı

Basit Ağ Yönetim Protokolü (SNMP), ağa bağlı olan yönlendiriciler, anahtarlar, yazıcılar vb. tüm cihazların yönetim ve takibinin yapılmasını sağlayan uygulama katmanı protokolüdür. SNMP uygulamasında ağa bağlı cihazlarla iletişim UDP paketleri ile istek gönderme ve yanıt alma şeklindedir. SNMP yansıma saldırısı tek bir sahte IP adresine karşı büyük boyutta yanıt ortaya çıkarmayı hedefler. Şekil 1.17‘de gösterilen SNMP yansıma saldırısında, saldırgan tarafından ağ üzerindeki tüm cihazların yanıtlaması için sahte bir IP adresine (hedef sunucu) sahip çok sayıda SNMP sorgusu gönderilir.



Şekil 1.17. SNMP Kuvvetlendirmeli DDoS saldırısı.

Ağdaki tüm cihazlar tarafından hedef sunucuya gelen yanıtlar büyük hacimlere ulaşır. Hedef ağ, bu SNMP yanıtlarının toplu hacmi altına indirilinceye kadar, giderek daha fazla cihaz yanıt vermeye devam ettikçe saldırı hacmi büyür. Böylece saldırı, küçük bir sorgu ile başlayıp hedef sunucunun ağı üzerinde yüksek bir trafik meydana getirerek ağ bant genişliğinin taşmasıyla sonuçlanır [39].

1.4.11. LDAP saldırısı

Hafif Dizin Erişim Protokolü (LDAP), TCP/IP ağı üzerinde çalışan dizin bilgi servislerine erişmek, bunları sorgulamak ve değiştirmek için açık bir uygulama protokolüdür. LDAP, açık bir protokol olduğundan verilerin tutulduğu sunucu tipine bağlı olmaksızın verilere erişilebilmektedir. LDAP saldırısında saldırgan, hedef sunucuya ait sahte IP adresiyle LDAP sunucusundan küçük sorgular yaparak hedef sunucuya büyük yanıtların gönderilmesini amaçlamaktadır. Bu tip saldırılar küçük isteklerle büyük yanıtları oluşturduğu için büyük hacimde kuvvetlendirmeye sebep olmaktadır. Sonuç olarak çok sayıda yanıt gelen hedefteki sunucunun ağ trafiğinde artış meydana gelir [40].

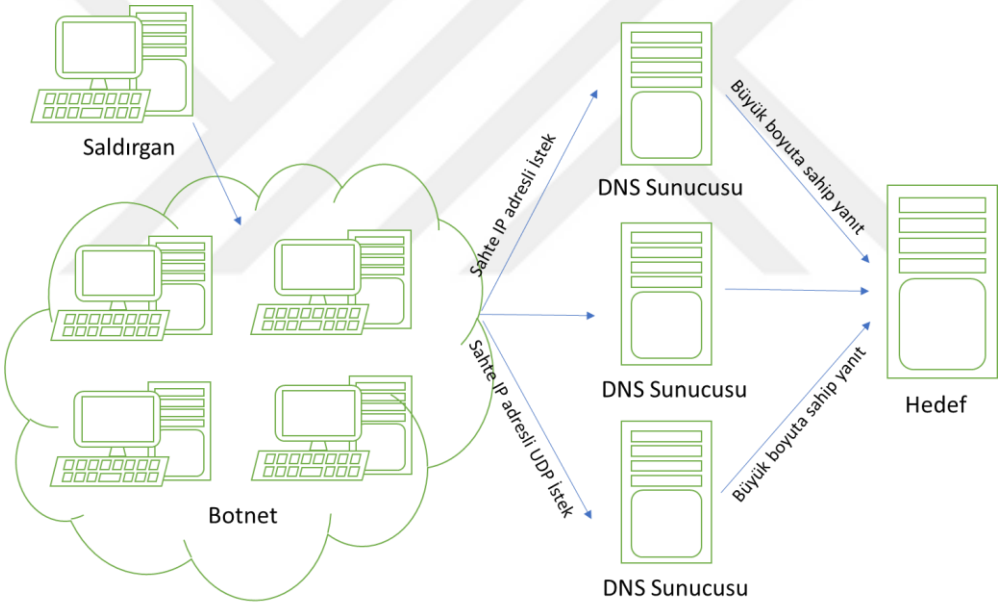
1.4.12. SSDP saldırısı

SSDP, 1900 nolu UDP bağlantı portunu kullanarak Evrensel Tak ve Çalıştır (UPnP) cihazlarını tespit etmeye ve durum bilgilerinin alınması için bir ağ protokolüdür. SSDP protokolü, UPnP cihazlarının varlıklarını ağdaki diğer cihazlara bildirmesine izin vermek için kullanılır. Bir SSDP saldırısında, ağa bağlı cihazların keşfi için uygun olan UPnP cihazlarının taranması sonucu yanıt veren cihazların listesi çıkartılır. Saldırgan tarafından hedef sunucunun sahte IP'si kullanılarak BotNet ile UPnP cihazlardan hizmetlerinin

açıklanmasını içeren sahte isteklerde bulunulur. Hedefteki sunucuya gelen 30 kat daha büyük veri içeren yanıtlar, sunucunun ağında aşırı yoğunluk oluşturarak hizmet reddine sebep olur [41].

1.4.13. DNS kuvvetlendirmeli DDoS saldırısı

DNS, TCP/IP ağ protokolünün kullanıldığı internet üzerinde küresel olarak çalışan Uniform Resource Locator (URL) adreslerini IP adreslerine çözümleyen bir protokoldür. DNS sunucuları, bir websitenin sayfasını görüntülemek için istemciden gönderilen URL isteğini sayfanın IP adresine çözümleyerek istemciye yanıt vermektedir. Şekil 1.18'de gösterilen DNS Kuvvetlendirmeli DDoS saldırısında, saldırının hacmini arttırmak için daha küçük isteklerin büyük yanıtlar vermesini sağlayacak DNS sunucuları kullanılmaktadır.



Şekil 1.18. DNS kuvvetlendirmeli DDoS saldırısı.

Saldırgan, saldırının boyutunu arttırmak için kullandığı BotNet ağı aracılığıyla hedef sunucunun adresi olarak ayarlanan sahte IP adresli UDP paket isteklerini DNS sunucusuna göndermektedir. Gelen isteklere DNS sunucularından verilen büyük bir yanıt Seli hedef sunucuya gönderilmektedir. Çok sayıda yanıta maruz kalan hedef sunucunun trafiği artarak ağın bant genişliği aşılır. Sonuç olarak ağ üzerindeki yoğun trafik hizmet kesintilerine neden olarak sunucunun ağını kullanan kullanıcıların hizmet reddine sebep olur [42].

1.4.14. CharGEN saldırısı

Character Generator Protocol (CharGen) [43], test ve performans ölçüm amaçları için kullanılan, TCP veya UDP bağlantıları üzerinden 19. portta çalışan bir TCP / IP protokolüdür. CharGen protokolünde istemci, bir sunucuyla TCP bağlantısı kurduğunda bağlantı kapanana kadar, UDP bağlantısı kurduğunda ise gönderdiği her mesaj için sunucudan yanıt dönülür. Sunucu, TCP/UDP bağlantısı üzerinden gönderilen paket isteklerine karakter sayısı [0 ... 512] byte aralığında olacak şekilde rastgele bir mesajla yanıt verir. CharGen saldırısında, saldırgan hedef sunucuya ait sahte IP adresiyle bu protokolün etkin olduğu cihazlara küçük UDP paketlerle sahte isteklerde bulunur. Sahte isteğin gönderildiği bu cihazlardan 512 byte'a ulaşan UDP yanıt paketleri hedef sunucuya gönderilir. Gelen yoğun yanıtlar sonucu hedef sunucunun kaynakları tükenerek hizmet veremez duruma gelir [44].

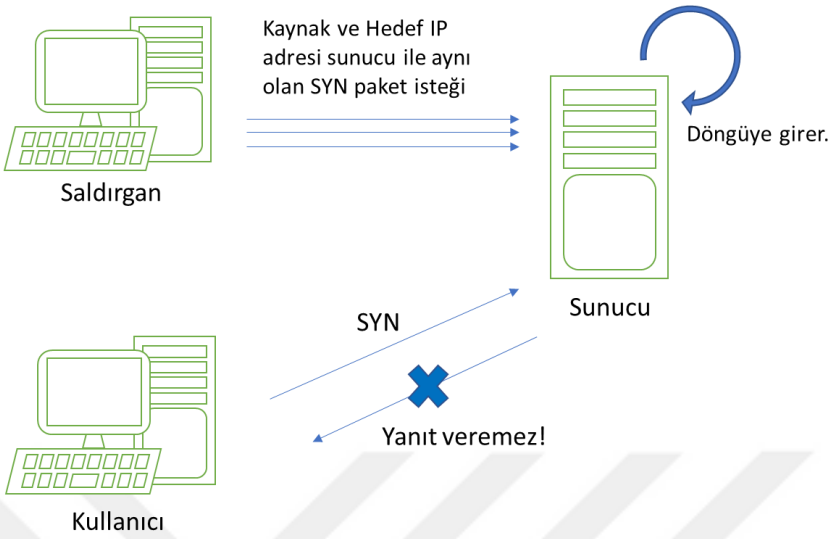
1.4.15.TFTP kuvvetlendirmeli DDoS saldırısı

TFTP, oturum açma veya erişim kontrol mekanizmaları olmaksızın istemcinin uzaktaki bir sunucudan dosya okunmasını (RRQ) veya sunucuya dosya yazılmasını (WRQ) sağlayan UDP bağlantısı üzerinden 69. portu (aktarım başlatılırken gönderici ve alıcı tarafından başka bir port seçilebilir) kullanan bir protokoldür. TFTP saldırısı, saldırgan tarafından kurban sunucunun sahte IP adresiyle TFTP sunucusundaki dosyanın okunması için küçük bir UDP paket isteği gönderilerek büyük bir yanıtın beklendiği bir çeşit DDoS kuvvetlendirme saldırısıdır. Bu TFTP kuvvetlendirmeli DDoS saldırısı sonucunda TFTP sunucularından gelen veri ve hata paketleriyle birlikte oluşan büyük ölçütlü UDP yanıtları, hedef sunucunun kaynak kullanımını arttırarak hizmet dışı kalmasına sebep olur [23,45,46].

1.4.16. Land Seli saldırısı

Land saldırısı TCP bağlantı protokolüne dayalı zafiyetten yararlanır. Şekil 1.19'da gösterilen saldırıda saldırgan, kurban sunucuya gönderilecek SYN paketinin kaynak IP ve hedef IP adreslerini saldırı yapılacak sunucuyla aynı olacak şekilde değiştirir. Gelen SYN paketlerinin kaynak ve hedef IP'leri hedef sunucuyla aynı olduğu için hedef sunucunun sahte IP'li SYN paket isteklerine gönderdiği yanıtlar kendi içinde döngü oluşturur. Bu durum, döngüye giren sunucunun işlemci ve bellek kaynakları tükenmesine

ve sunucunun çökmesine sebep olur. Sonuç olarak, hedef sunucuda hizmet reddi meydana gelir [47].



Şekil 1.19. Land Seli Saldırısı.

1.5. Saldırı Tespit Sistemleri

Saldırı Tespiti kavramı ilk defa 1980 yılında James Anderson tarafından bir bilgisayar sistemine zarar vererek kullanılamaz hale getirmek veya sisteme sızarak bilgilere yetkisiz girişler yapmak amacıyla saldırı ve tehdit girişimlerinde bulunulan olası olayların tespiti olarak tanımlanmıştır [48]. Saldırı Tespit Sistemi (IDS), ağ üzerinden bilgisayar sistemlerine yapılabilecek olası tehditlere karşı, ağın izlenerek risk içeren durumların analiz edilmesi süreçlerini içermektedir [49].

IDS'ler gelen verinin elde edildiği kaynağa göre Ağ Tabanlı Saldırı Tespit Sistemi (NIDS) ve Ana Bilgisayar Tabanlı Saldırı Tespit Sistemi (HIDS) temelde ikiye ayrılmaktadır. Giriş kaynağı olarak NIDS için ağ trafiğinden gelen veriler ve HIDS için ana bilgisayardan toplanan veriler kullanılmaktadır [50].

1.5.1. Ağ tabanlı saldırı tespit sistemi

NIDS, ağ üzerinden geçen paketlerin analizini yaparak şüpheli paketleri gerçek zamanlı olarak tespit eder. Kötüye kullanım ve anormallik saldırılarını tespit etmek için NIDS tarafından iki saldırı tespit yöntemi tanımlanmaktadır. Kötü amaçlı kullanımların tespitinde ağ üzerinden gelen veri paketlerine örüntü eşleştirme algoritması içeren bir

statik imza kümesi kullanılarak zararlı yazılımların gözlemlenmesi sağlanır. Anormallik tespitinde ağ trafiğinin gözlemlenmesi sonucu gelen verilerden istatistiksel çıkarımlar yapılmasıyla kötü amaçlı davranışlar tespit edilir [51].

NIDS, sunucuların bağlı olduğu bütün ağın trafiğini izlemesi sonucu veriler elde eder ve bu verilere göre kötü davranışlara karar verir. NIDS, ağa yapılan saldırıları gerçek zamanlı olarak algıladığı için yetkisiz giriş, hizmet reddi saldırıları, bağlantı noktası taramaları gibi zararlı faaliyetlerin önüne geçerek ağın zarar görme ihtimalini düşürür [52].

1.5.2. Ana bilgisayar tabanlı saldırı önleme sistemleri

Ana Bilgisayar Tabanlı Saldırı Tespit Sistemi (HIDS), ağ saldırı tespit sistemleri veya güvenlik duvarı gibi ağ güvenliğini sağlayan savunma mekanizmalarını geçen paketlerin belirli ana bilgisayarlara yetkisiz girişlerini önleyen sistemlerdir. HIDS, ana bilgisayarın güvenlik ihlali durumunun belirlenmesi için diğer bilgisayar ve cihazlardan gelen izinsiz giriş, sistem çağrıları, sistem günlükleri, uygulama eylemleri ve ana bilgisayar trafiği gibi verileri toplayarak tehdit içeren anormal davranışların tespitini sağlamaktadır [53]. Bu sistem tüm ağı izlemek yerine her bir ana bilgisayarı gözlemlediği için her ana bilgisayarda zararlı etkinlik durumuna ait raporlar daha belirleyici olmaktadır [52].

1.6. Saldırı Önleme Sistemleri

Saldırı Önleme Sistemleri (IPS), ağ üzerinden gelen saldırıları ve kötü niyetli etkinlikleri önlemek için gerçek zamanlı olarak karşılık verebilen her türlü donanım veya yazılım araçlarından oluşmaktadır. IPS temelde ana bilgisayar tabanlı sistemler ve ağ tabanlı sistemler olmak üzere iki şekilde sınıflandırılabilmektedir [54].

Ayrıca [55-57]'deki çalışmalarda bahsedildiği gibi saldırı tespit ve saldırı önleme sistemlerinin birleştirilmesinden oluşan Saldırı Tespit ve önleme Sistemleri (IDPS), ağ güvenliğinin sağlanması amacıyla kullanılmaktadır. Bu sistemler, güvenlik tehditlerini otomatik olarak algılayıp yanıt verdiği için ağlara ve ağları kullanan cihazlara yönelik saldırı riskini azaltmaktadır.

1.6.1. Ağ tabanlı saldırı önleme sistemi

Ağ Saldırı Önleme Sistemleri(NIPS), NIDS'lerde olduğu gibi ana bilgisayarların bağlı olduğu trafik ağının izlenmesiyle verileri elde ederek kötü amaçlı etkinliklere anlık olarak yanıt vermektedir. NIPS, kötü amaçlı kodların tespitinde sadece TCP/IP başlık içeriğini kontrol eden güvenlik duvarlarından farklı olarak anormal trafiğin tespiti için ağ üzerindeki paketlerin analizini yaparak saldırıları önlemektedir. Sistem çalışırken kötü amaçlı yazılımlara ait çok sayıda imzanın bulunduğu bir kural seti ile eşleştirme yapılmaktadır. NIPS, bu sayede herhangi şüpheli bir duruma karşı dinamik olarak engelleme özelliği ile öne çıkmaktadır [54, 58, 59].

1.6.2. Ana bilgisayar tabanlı saldırı önleme sistemi

Ana Bilgisayar Tabanlı Saldırı Önleme Sistemleri (HIPS), HIDS'lerde olduğu gibi ana bilgisayarlara gelen verilerin analiz edilme aşamalarını içermesinin yanında tespit edilen kötü niyetli etkinliklere otomatik olarak müdahale etmesiyle de aynı zamanda zafiyet açıklıklarını engelleyen bir teknolojidir. HIPS, zararlı bağlantıların engellenmesi için dijital imza tekniğiyle servislerin veya bağlantı noktalarının sonlandırılmasını [60], gelen komutların reddedilmesini, belirli IP adreslerinden gelen paketlerin engellenmesini, paketlerin izlenmesini ve sahte paketlerin kullanıcıya geri yollanmasını içeren işlemleri uygulayabilmektedir [61].

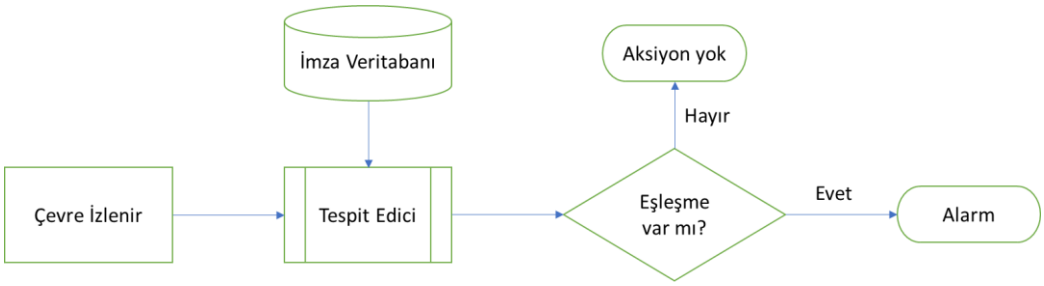
1.7. IDS'de Kullanılan Saldırı Tespit Yöntemleri

Genel olarak IDS'lerde imza tabanlı, anomali tabanlı ve durum protokolü analizi olmak üzere 3 tip tespit yöntemi kullanılmaktadır. Yapay zekanın siber güvenlik alanında kullanımının yaygınlaşmasıyla IDS'lerde derin öğrenme tabanlı yaklaşımlarında uygulanmaya başlanmıştır.

1.7.1. İmza tabanlı saldırı tespiti

İmza tabanlı saldırı tespit sistemi, belirli bir kural çerçevesinde ağ üzerinden yetkisiz erişimlerin varlığını tespit etmek amacıyla paketler için bir statik imza tanımlayan ve bu imzaların kontrolünü yapan sistemlerdir. Şekil 1.20'de mimarisi yer alan imza tabanlı IDS'ler sadece tanımlanmış izinsiz erişimleri tespit edebilmeleri yönünden antivirüs programlarına benzemektedir. Yeni keşfedilen saldırılar için tanımlanan imzalar manuel

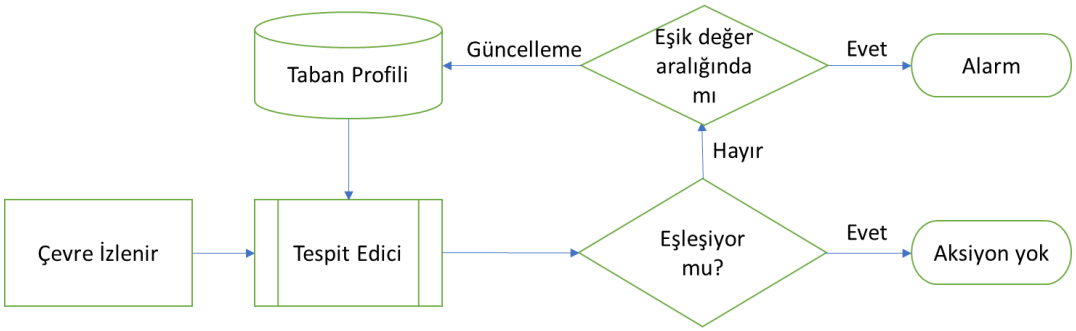
olarak veritabanına eklenmektedir. Dolayısıyla internet üzerinden gelen saldırıların sürekli artması veritabanında yer alan imzalarında güncellenmesini gerektirmektedir. Sonuç olarak bu güncelleme süresince, bu tespit yöntemini kullanan sistemlerin bilinmeyen yetkisiz erişimlere karşı güvenliği tehdit altındadır [62, 63].



Şekil 1.20. İmza tabanlı saldırı tespit sistemi mimarisi [56].

1.7.2. Anomali tabanlı saldırı tespiti

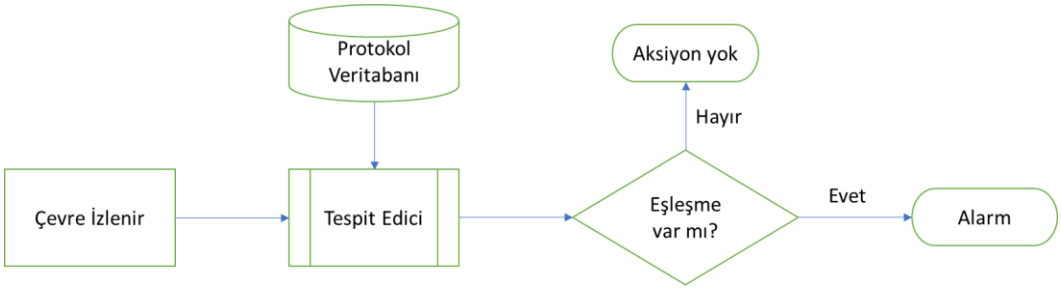
Anomali tabanlı IDS, ağ trafiğinden geçen veya ağı kullanan cihazlardan gelen verileri kullanılarak ağ üzerindeki normal davranışı öğrenen bir sistemdir. Ağın analiz edilmesi sonucu normal trafik için sabit ya da dinamik bir profil oluşturularak eşik değeri belirlenir. Sabit profiller oluşturulduktan sonra değişmezken dinamik profiller sistem işlerken güncellenebilmektedir. Ağ üzerindeki etkinliklerin durumu eşik değerine göre karşılaştırılarak saldırı olup olmadığına karar verilir. Şekil 1.21'deki bu sistem çalışırken dedektör tarafından ortamdaki olaylar normal davranış için belirlenen taban profiline göre incelenir. Gözlenen etkinlikler taban profiliyle eşleştiğinde herhangi bir işlem yapılmazken taban profiliyle eşleşmeyip eşik aralığının içinde yer alırsa profil güncellenmektedir. Gözlemlenen etkinlikler hem profille eşleşmeyip hem de eşik aralığının dışındaysa anormallik olarak belirlenip sistem uyarılır [56]. Anomali tespiti için istatistiksel, makine öğrenimi ve veri madenciliğinden elde edilen bilgi olmak üzere üç yöntem kullanılmaktadır [64, 65]. Anomali tabanlı IDS taban profilinin güncellenmesi aşamasında eşik değeri içerisindeki saldırıları belirleyemediği için sistem yanıltılabilmektedir.



Şekil 1.21. Anomali tabanlı saldırı tespit sistemi mimarisi [56].

1.7.3. Durum protokolü analiz tespiti

Durum Protokol Analizi tabanlı IDS, IP, ICMP gibi ağ katmanı, TCP ve UDP gibi taşıma katmanı ve http, FTP, SNMP, SMTP gibi uygulama katmanı protokollerinin inceleyen yöntemden oluşmaktadır [66, 67]. Şekil 1.22'de mimarisi gösterilen Durum Protokol Analizinde, analiz edilecek protokollerin çalışma şeklini belirleyen standartlara göre oluşturulmuş modeller kullanılmaktadır. Bu modellerle protokollerin nasıl kullanılıp kullanılmayacağı belirlenmekte ve iyi huylu protokol etkinlikleri incelenerek riskli durumlar tanımlanmaktadır. Bu protokolleri kullanan paketlerin bağlantı ve oturum durumları analiz edilmek için kaydedilir [68]. Sonuç olarak, ana bilgisayarlar veya ağ üzerinden toplanan verilerle protokolü doğru kullanmayan saldırı tespit edilmektedir. Bu yöntemde, analizin karmaşıklığı nedeniyle yüksek kaynak gereksinimi duyulmaktadır [69, 70]. Ayrıca, protokolün doğru kullanımını baz alan bu yöntemde kabul edilebilir protokol davranışı gösteren saldırılar tespit edilemediğinden uygulama katmanı için tehdit oluşturmaktadır [71].



Şekil 1.22. Durum protokol analizi tabanlı saldırı tespit sistemi mimarisi [56].

1.7.4. Derin öğrenme tabanlı yaklaşım

Genel olarak derin öğrenme tabanlı yaklaşımda, makine öğrenmesi yöntemi olan derin öğrenme modeliyle ağ trafiğindeki küçük hacme sahip paketlerden ağın büyük kısmının profilini çıkarmak ve normal trafiği tespit etmek mümkün olabilmektedir [72]. Derin öğrenme, bu özellik sayesinde sığ makine öğrenme algoritmalarına göre avantaj sağlar. Bununla birlikte, derin öğrenme modeli, derin ağ yapısı nedeniyle daha uzun bir eğitim süresi ile sonuçlanır. Grafik işlemcilerin geliştirilmesi, derin öğrenme modelinin öğrenme süresini azaltır ve saldırıların hızlı ve doğru tespiti için yaygın kullanımına katkıda bulunur [5]. Bu yöntemde, sistem iki bileşenden oluşmaktadır. İlk kısımda, ağdaki paket akışını kaydeden ilk kısımda gelen paketlerden oluşturulan verisetine derin öğrenme algoritması uygulanmakta ve normal paketler işaretlenmektedir. İkinci kısımda ise ağ trafiğinden gelen paketler anlık olarak önceki işaretlenen paketlerle karşılaştırılmaktadır. Sonuç olarak uyuşmayan paketler düşürülerek sistemle bağlantısı kesilmektedir.

Bu tez çalışmasının konusu olan DDoS saldırı tespitinde derin öğrenme yöntemlerinin kullanımının, ağ trafiğinin güvenliği için kesin ve etkili sonuçlar sağladığı ilerleyen bölümlerde ele alınmıştır.

1.8. Literatür Çalışmaları

DDoS saldırı tespitinde derin öğrenmenin kullanımına ilişkin birçok çalışma vardır. Bu bölümde, DDoS saldırıları içeren veri kümeleri ile yapılan deneyler ve derin öğrenme modelinin kullanımına yönelik çalışmalar özetlenmektedir.

Srinivas & Manivannan [73], tıbbi IoT ağında DoS tabanlı Hello sel saldırılarını tespit etmek ve önlemek için bir derin öğrenme yaklaşımı önermektedir. Deep Belief Network (DBN) modeli, gönderilen çok sayıdaki Hello paketiyle ağın performansını düşürüldüğü bu saldırı türünü doğrulamak için kullanılmıştır. DBN modelinin daha optimum şekilde çalışması ve daha verimli sonuçlar üretmesi için Baypas Bağlantılı Saldırgan Güncellemesine dayalı Sürücü Optimizasyon Algoritması (BAU-ROA) kullanılmıştır. Deneylerde, algoritmaların karşılaştırılması sonucunda BAU-ROA algoritmasının DBN'nin etkin çalışması için diğer optimizasyon algoritmalarından daha yüksek performansa sahip olduğu görülmüştür.

Ujjan ve diğerleri [74] tarafından yapılan çalışmada, IoT için kullanılan Yazılım Tanımlı Ağ (SDN) tespit sisteminin ilk aşamasındaki ağ güvenliğinin sağlanmasında kullanılan örnekleme tabanlı yöntemin yetersizliği ile ilgili sorunu çözmek için bir derin öğrenme modeli önerilmiştir. Çalışmada bahsedilen iki tip yöntemle oluşturulan örneklemelerde saldırı tespitinin optimizasyonu için Yığınlı Otomatik Kodlayıcılar tipi derin öğrenme modeli kullanılmış ve deneyler ile doğruluk üzerine etkisi araştırılmıştır. Elde edilen iki örnekleme üzerinde yapılan deney sonucunda daha düşük merkezi işlemci kullanımı gözlemlenmiş, %91 ve %89 doğruluk oranları ile başarılı sonuçlar elde edilmiştir.

Priyadarshini & Barik [75] tarafından yapılan çalışmada, bulut bilişim ve sis bilişim ortamlarının güvenliği için SDN kontrol katmanında DDoS saldırısını tespit edebilen bir derin öğrenme modeli önerilmiştir. Deneyler sonucunda 3 gizli katman ve 128 düğümden oluşan Uzun Kısa Süreli Bellek (LSTM) derin öğrenme modeli uygun bulunmuştur. ISCX 2012 ve IDS CTU-13 BotNet veri setlerine LSTM uygulanarak elde edilen %98,88 doğruluk, modelin başarılı olduğunu göstermiştir.

Hasan ve diğerleri [76] tarafından yapılan çalışmada, Optik Anahtarlama ağındaki DDoS saldırılarının tespiti için Derin Evrişimli Sinir Ağları (DCNN) modeli önerilmiştir. Daha küçük veriseti örneğinde, sığ makine öğrenme algoritmaları trafik analizini istenen şekilde gerçekleştiremediği için DCNN kullanımı uygun görülmüştür. Deney sonuçlarına göre, sırasıyla %93, %88 ve %79 doğruluk değerlerine sahip olan K-En Yakın Komşu (KNN), Destek Vektör Makinesi (SVM), Naive Bayes sığ makine öğrenme algoritmalarına kıyasla DCNN'nin %99 doğruluk ile daha iyi performansa sahip olduğu görülmüştür.

Krishnan ve diğerleri [77], SDN güvenliğini sağlamak için Simetrik Olmayan Yığınlanmış Otomatik Kodlayıcı (NSAE) derin öğrenme modelini kullanan güvenlik çerçevesine sahip bir saldırı tespit sistemi önermektedir. Uzun eğitim süreleri, yüksek bellek ve işlemci gereksinimi gibi nedenlerle sığ makine öğrenimi sınıflandırıcılarında ortaya çıkan sorunların giderilmesi için derin öğrenme modeli tercih edilmiştir. DDoS saldırılarını tespit etmek için kullanılan modelin performansını görmek için NSL-KDD ve CICIDS2017 veri setleri kullanılmıştır. NSL-KDD ve CICIDS2017 veri setlerine NSAE modeli uygulanmasıyla elde edilen %99,60 ve %99,24 doğruluk değerleri, önerilen modelin saldırı tespit sisteminde kullanıma uygun olduğunu göstermektedir.

Zhu ve diğerleri [78] tarafından yapılan çalışmada ağ trafiğini analiz etmek ve DDoS saldırı algılamasını kullanmak için derin öğrenme modellerinden ikisi olan Evrişimli Sinir Ağları (CNN) ve İleri Beslemeli Sinir Ağları (FNN) modelinin kullanılması önerilmektedir. NSL-KDD veriseti üzerinde yapılan deneylerde, FNN ve CNN modellerinin, ağdaki anormallik türlerini belirlemede ve ağ anormallik tespitinde sığ makine öğrenme algoritmaları olan Naive Bayes, Rastgele Orman(RF), Karar Ağacı(J48), Rastgele Ağaç, SVM'den daha yüksek doğruluğa sahip olduğu gözlemlenmiştir.

Alzahrani ve Hong [79], yetkisiz erişim tespit sistemindeki DDoS saldırılarını tespit etmek için imza tabanlı yaklaşımla birlikte Yapay Sinir Ağı(YSA)'nın kullanımını önermektedir. Deneyler sonucunda imza temelli yaklaşım ve YSA kullanımı ayrı ayrı karşılaştırıldığında, bu iki yaklaşımın birlikte kullanımının %99,98 gibi daha yüksek bir doğruluk değerine ulaştığı görülmüştür.

Yukarıdaki çalışmaların incelenmesi sonucunda ağ trafiğinin analizinde ve DDoS saldırılarının tespitinde derin öğrenme modelinin yüksek düzeyde başarıya sahip olduğunu gözlemlenmektedir.

2. MATERYAL VE YÖNTEM

Bu tezde güncel ve literatürde yaygın olarak çalışılan verisetleri kullanarak derin öğrenme yöntemleri uygulanmıştır. Aynı zamanda modelin test edilmesi için sanal deney ortamı kurulmuş ve yeni bir deneysel veriseti oluşturulmuştur. Çalışmanın bu bölümünde, DDoS tespiti ve sınıflandırmasında kullanılan verisetleri, veri önişleme süreçleri ve derin öğrenme modeli hakkında detaylı bilgilere yer verilecektir.

2.1. Hazır Verisetleri

Bu çalışmada hazır veriseti olarak CICIDS2017, NSL-KDD, CICDDOS2019 veri setleri kullanılmıştır. Bu verisetleri diğer çalışmalarda güncel olarak kullanıldığı ve zengin bir ağ trafiği analizi içerdiği için tercih edilmiştir.

2.1.1. KDD-NSL veriseti

NSL-KDD'nin, KDD'99 verisetinin birçok gereksiz kayıt içermesi, test için ayrılmış veri setlerinde bulunan eğitim verisetinin bölümleri gibi problemleri çözmek için önerilmiştir. Verisetinde 41 özellik bulunmakta olup, eğitim için ayrılan verisetinde 23 saldırı sınıf etiketi ve test verisetinde 38 saldırı sınıf etiketi bulunmaktadır. Tablo 2.1'de NSL-KDD verisetinde bulunan DDoS saldırı tipleri gösterilmektedir. Ek olarak, eğitim verisetinde 125.973 kayıt ve test verisetinde 22.544 kayıt bulunmaktadır [80].

Tablo 2.1. NSL-KDD veriseti saldırı etiketleri [80].

Saldırıların İsimleri
Back, Land, Mailbomb, Neptune, Apache2, Pod, Processtable, Smurf, Teardrop, UDPstorm
Perl, Xterm, Buffer_Overflow, Httptunnel, LoadModule, Ps, SQLattack, Rootkit,
Guess_Password, Imap, MultiHop, Named, Phf, Ftp_Write, Sendmail, SnmpGetAttack, SnmpGuess, Spy, WarezClient, WarezMaster, Worm, Xlock, Xsnoop
Saint, Satan, Nmap, Mscan, Ipsweep, Portsweep

NSL-KDD verisetinin sınıf dağılımları Tablo 2.2'te verilmiştir. Çalışmada kullanılan NSL-KDD veriseti, DDoS saldırıları dışında siber saldırıları da içermektedir. Bu nedenle, DDoS dışındaki saldırılar 'diğer' olarak etiketlenmiştir ve sınıflandırma sürecinde kullanılmamıştır.

Tablo 2.2. NSL-KDD verisetinde etiketlenmiş paketlerin sayısı.

Sınıf Etiketi	Eğitim Seti	Test Seti
Normal	67343	9711
DDoS	45927	5741
Diğer	12703	7092
Toplam	125973	22544

2.1.2. CICIDS2017 veriseti

Sharafaldin ve diğerleri [81] tarafından hazırlanan CICIDS2017 veriseti, New Brunswick Üniversitesi (UNB) ağ güvenliği araştırma grubu Bilgi Güvenliği Mükemmeliyet Merkezi (ISCX) tarafından yayınlanmıştır. CICIDS2017 veriseti 6 saldırı türü ve 79 trafik özelliği içermektedir. Bu veriseti için 25 kullanıcının HTTP, HTTPS, FTP, SSH ve e-posta protokollerine göre kuramsal davranışı oluşturulmuştur. Uygulanan saldırılar arasında Brute Force FTP, Brute Force SSH, DoS, Heartbleed, Web Attack, Infiltration, Botnet ve DDoS bulunmaktadır. Oluşturulan ağ trafiğinden 80'den fazla ağ akışı özelliği çıkarılmış ve ağ akış verisetini bir CSV dosyası olarak sunulmuştur.

2.1.3. CICDDoS2019 veriseti

CICDDoS2019 veriseti, DDoS saldırılarını tespit etmek ve saldırı türlerini sınıflandırmak için Sharafaldin ve diğerleri [81] tarafından üretilmiştir. CICIDS2017 ve CICDDoS2019 verisetindeki paket özellikleri, ağ trafik akışını oluşturan ve akıştan özellikleri çıkaran açık kaynaklı CICFlowMeter [82] temel alınarak oluşturulmuştur. CICDDoS2019 verisetindeki saldırılar Şekil 2.1'de gösterildiği gibi yansıma ve sömürü olarak iki kategoriye ayrılmıştır.

Sömürü Tabanlı Saldırı			
WebDDoS	SYN	UDP	UDP-Lag
Yansıma Tabanlı Saldırı			
MSSQL	SSDP	DNS	LDAP
SNMP	PORTMAP	NTP	TFTP
NETBIOS			

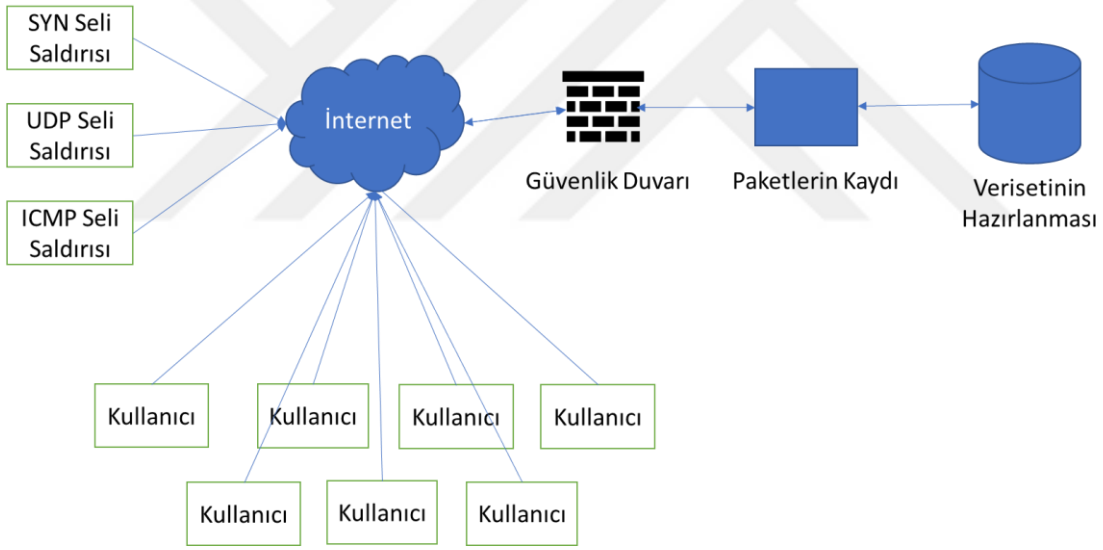
Şekil 2.1. CICDDoS2019 veriseti DDoS saldırı türleri.

Yansıma tabanlı DDoS saldırıları, Microsoft SQL Server (MSSQL), SSDP, Network Time Protocol (NTP), TFTP, DNS, LDAP gibi yasal sunucuları kullanır. Ağ üzerinden çeşitli hizmetler sağlayan, NETBIOS, SNMP, WebDDoS, SYN Seli, UDP Seli ve

UDPLag gibi sömürü tabanlı DDoS saldırıları, TCP ve UDP bağlantı protokollerindeki güvenlik açığından yararlanmaktadır.

2.2. Deneysel Veriseti

Deney amaçlı oluşturulan SWDDoS2020 adı verilen veriseti hazırlanırken en yaygın kullanılan üç tip DDoS saldırısı dikkate alınmıştır. SWDDoS2020 verisetinde SYN Seli, UDP Seli, ICMP Seli saldırıları ve normal trafik verileri yer almaktadır. Saldırı 3 Kasım 2020 Salı günü sabahı 9:48 -10:49 saatleri arasında 3 tip saldırı örneği içerecek şekilde ayarlanmıştır. DDoS saldırılarını simüle etmek için sanal ağ üzerinde hazırlanan deney ortamı Şekil 2.2'de görülmektedir. İnternet üzerinden normal kullanıcı işlemleri devam ederken ayrı ayrı SYN seli, UDP seli ve ICMP seli saldırıları aynı ağ üzerinden düzenlenmektedir. Saldırı yapılan sistemin güvenlik duvarında (firewall) izlenen paketler kayıt altına alındıktan sonra veriseti hazırlama aşaması için analiz edilmektedir.



Şekil 2.2. Sanal ağ üzerinde deneysel DDoS saldırı ortamı.

Paketler normal kullanıcı ve DDoS saldırılarına göre analiz edildikten sonra uygun bir veriseti formatında olması için ön işleme aşamalarından geçirilmiştir.

2.2.1. Kullanılan araçlar

Tez çalışması kapsamında önerilen derin öğrenme modelinin uygulandığı SWDDoS2020 verisetini oluşturmak için "scapy" ile "wireshark" programları kullanılmıştır. Scapy [83], kullanıcının ağ paketlerini göndermesini, koklamasını, incelemesini ve sahtesini

yapmasını sağlayan bir Python programıdır. Bu program aracılığıyla yapay olarak saldırganlar oluşturulmuş, bu saldırganların ağlara saldırabileceği bir ortam hazırlanmıştır. Scapy programında Python diliyle yazılmış kod parçacıkları çalıştırılarak hedef ağa çeşitli sahte IP adresleri ve portlardan saldırı amacıyla çok sayıda paket gönderilmiştir. Normal ağ trafiğini ve saldırı amacıyla gönderilen paketleri izlemek amacıyla yaygın olarak kullanılan Wireshark [84] ağ protokolü analizörü kullanılmıştır. Wireshark, anlık olarak Ethernet, IEEE 802.11, PPP ve Loopback gibi çeşitli ağ türlerini takip edebilen açık kaynaklı bir programdır.

2.2.2. Paketlerin yakalanması

Sanal deney ortamı kurulmasında, python programlama dili için hazırlanan scapy kütüphanesinden yararlanılmıştır. TCP, UDP ve ICMP protokolleri üzerinden gönderilecek paketler scapy aracılığıyla hazırlanmıştır. TCP protokolündeki üçlü el sıkışma (three-way handshake) zafiyetini kullanarak çok sayıda SYN paketleri hazırlanıp scapy'nin *send()* fonksiyonu ile hedef IP adresine gönderilmiştir. Bu gönderilerin paketler yine wireshark kullanılarak dinlenmiş ve sonrasında *pcap* formatında kaydedilmiştir. Aynı şekilde scapy'nin *send()* fonksiyonu ile hedef IP adresine çok sayıda UDP ve ICMP paketleri gönderilmiş ve wireshark kullanılarak dinlendikten sonra *pcap* formatında kaydedilmiştir.

Tablo 2.3'de kaydedilen paket içeriğinde yer alan IP başlığına ait niteliklere yer verilmiştir.

Tablo 2.3. Ağ paketi içerisindeki IP başlık içeriği.

Nitelik Adı	Açıklaması
version	internet protokol versiyonu
ihl (internet header length)	IPv4 başlığının boyutu
tos(the type of service)	servis türü alanı
len (total length)	başlık ve veriler dahil olmak üzere tüm paket boyutu
id (identification)	tek bir IP datagramının parça grubunu benzersiz şekilde tanımlama
flags	parçaları kontrol etmek veya tanımlamak için kullanılan alan
frag (fragment offset)	IP datagramının başlangıcına göre belirli bir parçanın ofsetini belirten alan
ttl (time to live)	bir datagramın ömrünün sınırlandığı alan
proto (protokol)	IP datagramının veri bölümünde kullanılan protokol
chksum (header checksum)	başlığın hata kontrolü için kullanıldığı alan
src (source address)	paketi gönderenin adresi
dst (destination address)	paketin alıcısının adresi

Tablo 2.4'de kaydedilen paket içeriğinde yer alan ICMP başlığına ait niteliklere ve açıklamalarına yer verilmiştir.

Tablo 2.4. Ağ paketi içerisindeki ICMP başlık içeriği.

Nitelik Adı	Açıklaması
type	Kontrol mesajlarının tanımlandığı değer
code	mesaj için ek bağlam bilgisinin verildiği alan
chksum (checksum)	ICMP başlığından hesaplanan hata denetimi
seq (sequence number)	yanıtı istekle eşleştirmek için kullanılan alan

Tablo 2.5'de kaydedilen paket içeriğinde yer alan UDP başlığına ait niteliklere ve açıklamalarına yer verilmiştir.

Tablo 2.5. Ağ paketi içerisindeki UDP başlık içeriği.

Nitelik Adı	Açıklaması
sport (source port)	Gönderen bağlantı noktasınının tanımlandığı alan
dport (destination port)	Alıcı bağlantı noktasınının tanımlandığı alan
len (length)	UDP başlığının ve UDP verilerinin bayt cinsinden uzunluğu
chksum	başlık ve verilerin hata denetimi için kullanıldığı alan

Tablo 2.6'de kaydedilen paket içeriğinde yer alan TCP başlığına ait niteliklere ve açıklamalarına yer verilmiştir.

Tablo 2.6. Ağ paketi içerisindeki TCP başlık içeriği.

Nitelik Adı	Açıklaması
sport (source port)	gönderen bağlantı noktasınının tanımlandığı alan
dport (destination port)	alıcı bağlantı noktasınının tanımlandığı alan
seq (sequence number)	gönderilen TCP paketindeki ilk veri baytının bayt numarası
ack (acknowledgment number)	alıcının almayı beklediği bir sonraki baytın sıra numarası
dataofs (data offset)	TCP başlığının boyutu
flags	sorun giderme veya bağlantı kontrolü için kullanılan değer
window (window size)	alıcıya ne kadar veri aktarılabileceğini gönderene gösteren alan
chksum (checksum)	TCP başlığının ve yükün hata denetiminin yapıldığı alan
urgptr (urgent pointer)	bir veri segmentinin acil olarak işaretlendiği işaretçi bayrağı

Yakalanan ağ paketleri normal ve anormal trafikler içermekte olup gerçekleştirilen saldırı tipleri ve verisetlerinin içerdiği protokoller Tablo 2.7'da verilmiştir.

Tablo 2.7. SWDDoS2020 veriseti paket çeşidi dağılımı.

Veriseti	TCP	UDP	ICMP	Diğer
UDP Seli	5622	396137	0	408
SYN Seli	224285	7952	0	173
ICMP Seli	745	531	216217	165

Pcap formatında kaydedilen ağ paketleri, scapy'nin *rdpcap()* fonksiyonu ile okunduktan sonra TCP, UDP ve ICMP protokollerine göre filtrelenmiştir. Filtreleme işleminden sonra

paket içeriğine göre düzenlenen veriler *to_csv()* fonksiyonu aracılığıyla csv dosyası olarak kaydedilmiştir.

2.2.3. Paketlerin analizi

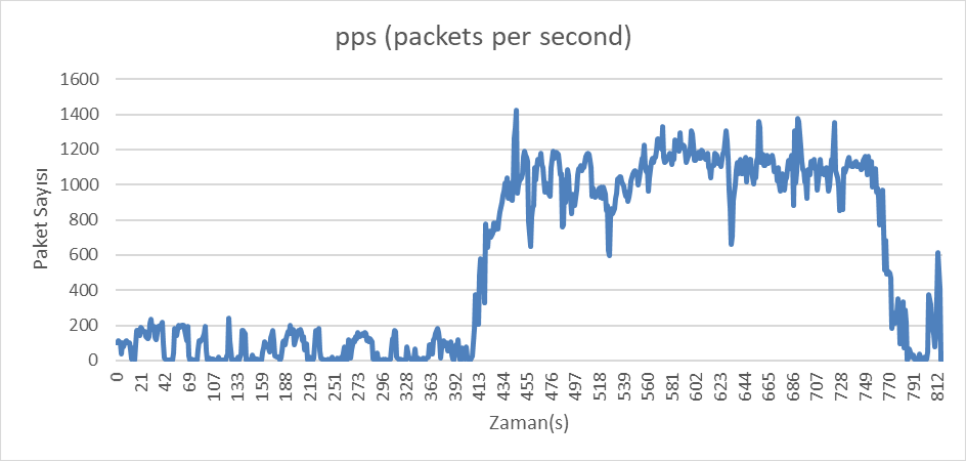
Bu bölümde deneysel ortamda hazırlanan SWDDoS2020 verisetindeki yakalanan paketlerin ayrıntılarından bahsedilmektedir.

Deneysel veriseti hazırlanırken normal ağ trafik akışı içerisinde DDoS saldırılarının yapıldığı zamanlamalar ve saldırı süresi kayıt altına alınmıştır. UDP sel saldırısının gerçekleştirildiği zamanlama bilgisi Tablo 2.8'de gösterildiği üzere düzenlenmiştir.

Tablo 2.8. UDP sel saldırı süresi ve zaman bilgisi.

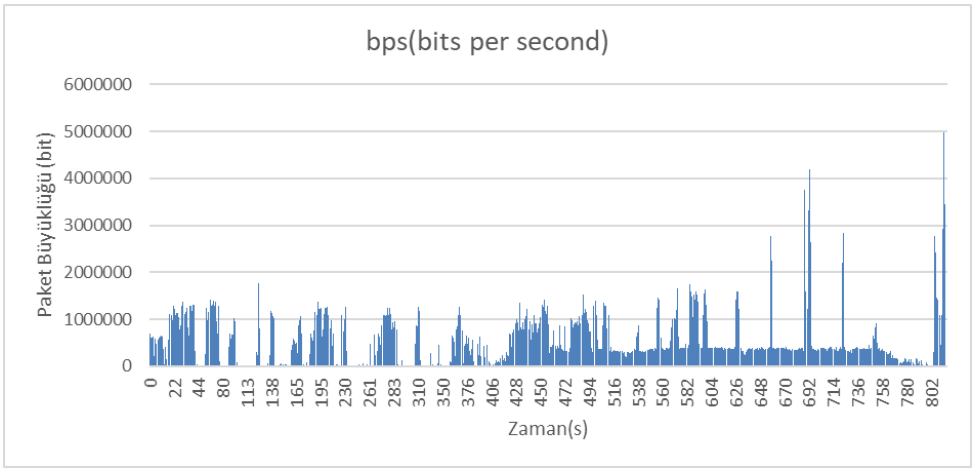
Saat	Aksiyon adı	Aksiyon Zamanı (Saniye)
09:48:56	Kayıt Başlangıç	0
09:55:44	UDP Saldırısı başlangıç	408
10:02:01	UDP Saldırısı bitiş	785
10:02:35	Kayıt Bitiş	819

Şekil 2.3'de gerçekleşen UDP sel saldırısına ait her saniye bir ağa gönderilen paket sayısının ağ üzerindeki toplam paket artışına etkisi gösterilmektedir.



Şekil 2.3. Saniyede gelen UDP paket sayısı.

Şekil 2.4'de gerçekleşen UDP sel saldırısına ait her saniye başına ağa gönderilen paketlerin bit cinsinden boyutunun ağ bant genişliği üzerindeki etkisi gösterilmektedir.



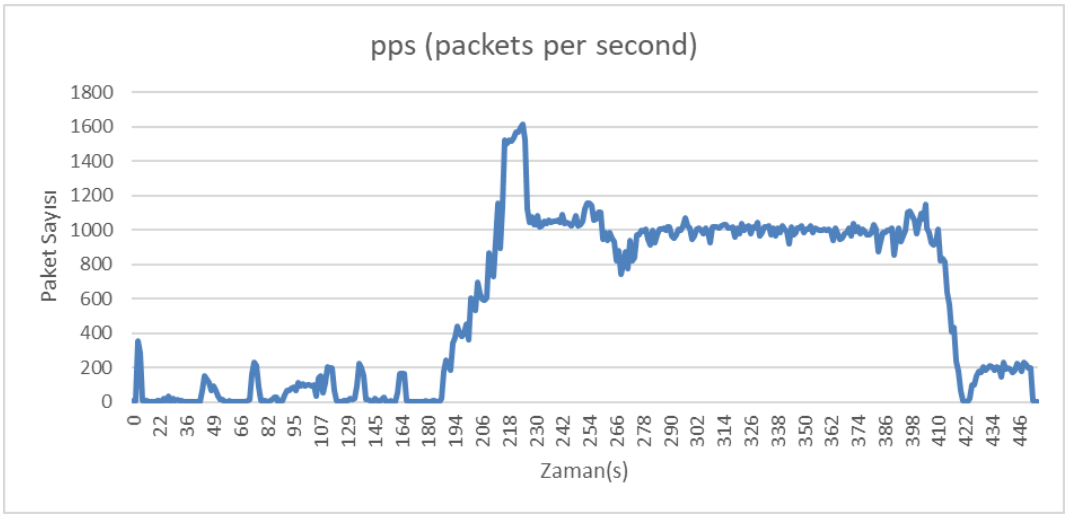
Şekil 2.4. Saniyede gelen UDP paket büyüklüğü.

Tablo 2.9'de gerçekleştirilen TCP sel saldırısına ait zamanlama bilgisi ve saldırı süresi ayrıntılı olarak gösterilmektedir.

Tablo 2.9. TCP sel saldırı süresi ve zaman bilgisi.

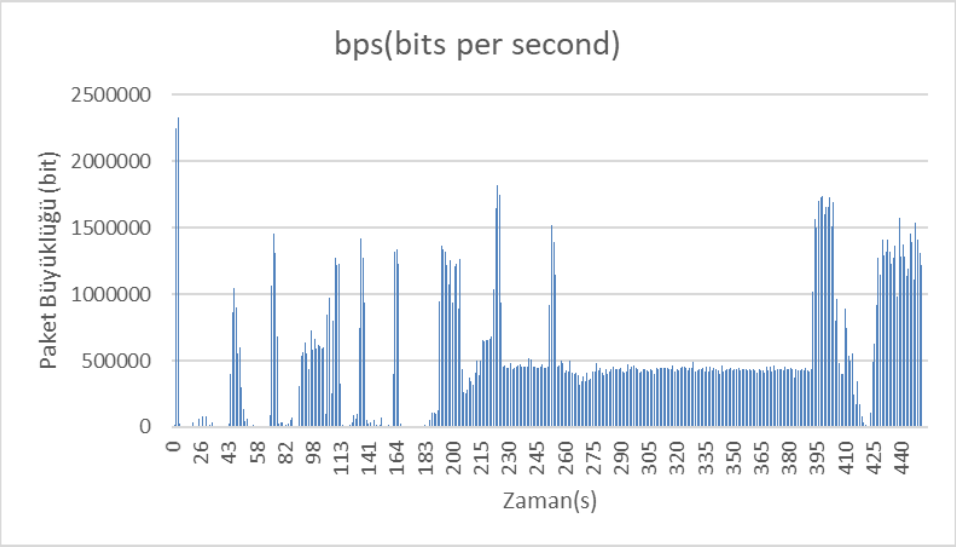
Saat	Aksiyon adı	Aksiyon Zamanı (Saniye)
10:03:59	Kayıt Başlangıç	0
10:07:08	TCP Saldırısı başlangıç	189
10:10:59	TCP Saldırısı bitiş	420
10:11:35	Kayıt Bitiş	455

Şekil 2.5'de TCP sel saldırısı başlatıldıktan sonra bir saniyede ağa gönderilen saldırı paketlerinin ağ üzerindeki etkisi gösterilmektedir.



Şekil 2.5. Saniyede gelen TCP paket sayısı.

Şekil 2.6'de gerçekleşen TCP sel saldırısına ait her saniye başına ağa gönderilen paketlerin bit cinsinden boyutunun ağ bant genişliği üzerindeki etkisi gösterilmektedir.



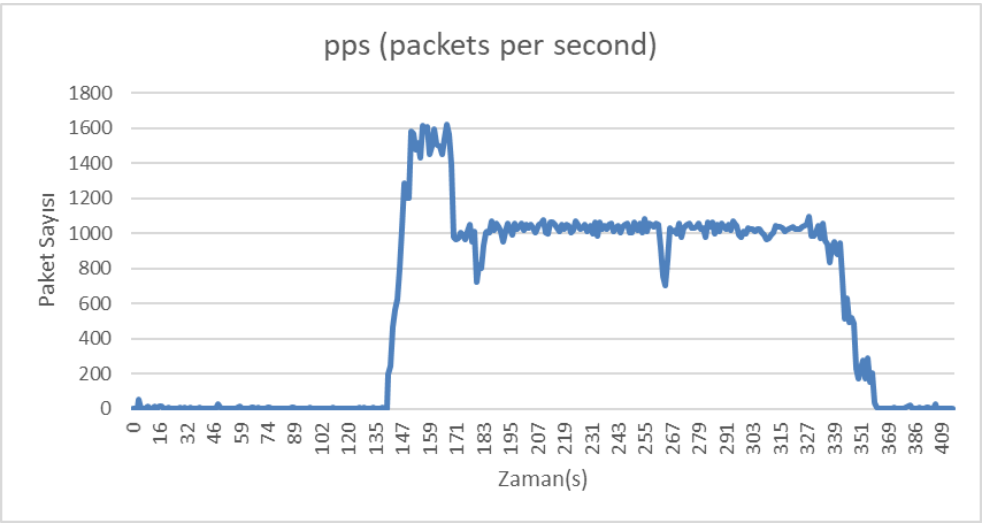
Şekil 2.6. Saniyede gelen TCP paket büyüklüğü.

Tablo 2.10'da ICMP sel saldırıları için ayarlanan zaman ve saldırı süresi ayrıntılı olarak verilmektedir.

Tablo 2.10. ICMP sel saldırı süresi ve zaman bilgisi.

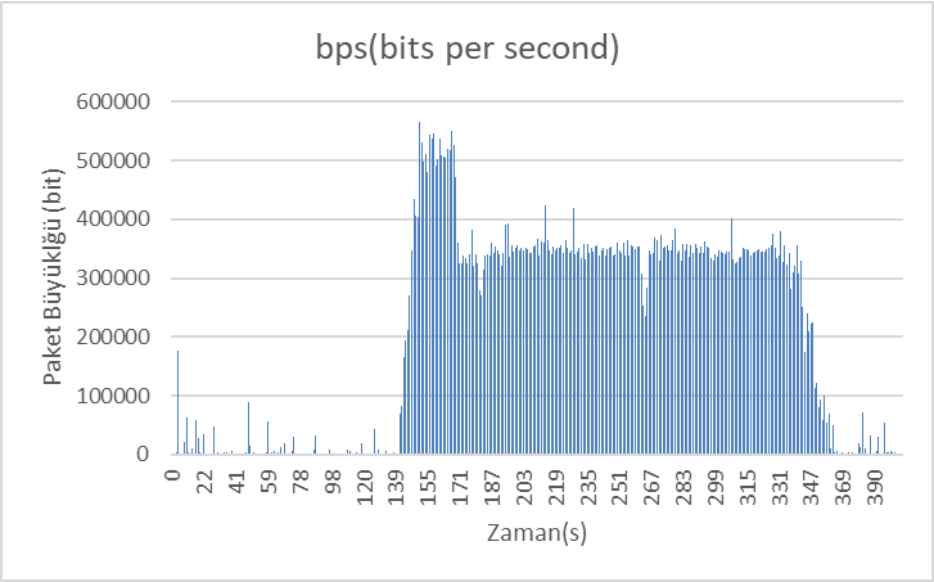
Saat	Aksiyon adı	Aksiyon Zamanı (Saniye)
10:42:37	Kayıt Başlangıç	0
10:44:58	ICMP Saldırısı başlangıç	141
10:48:34	ICMP Saldırısı bitiş	357
10:49:35	Kayıt Bitiş	418

Şekil 2.7'de bir ağda gerçekleşen ICMP sel saldırısına ait bir saniyede gönderilen paketlerin ağ üzerindeki etkisi gösterilmektedir.



Şekil 2.7. Saniyede gelen ICMP paket sayısı.

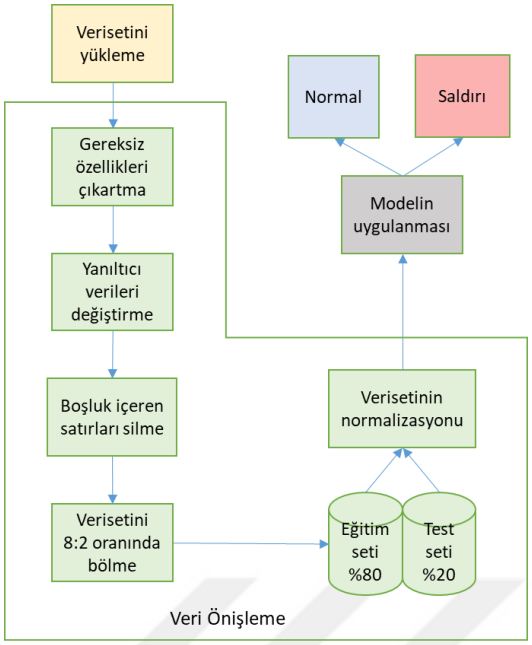
Şekil 2.8'de ağa yapılan ICMP sel saldırısına ait bir saniyede gelen paketlerin bit cinsinden boyutunun ağ bant genişliği üzerindeki etkisi gösterilmektedir.



Şekil 2.8. Saniyede gelen ICMP paket büyüklüğü.

2.3. Veri Önişleme

Modelin eğitimine geçmeden önce ham verisetlerinin boşluklardan, gereksiz ve yanıltıcı değerlerden temizlenmesi gerekmektedir. Bu bölümde kullanılan her bir veriseti için ayrı ayrı üzerinde yapılan önişleme süreçlerine yer verilmektedir. Veri önişleme yöntemi ve sınıflandırma sürecinden oluşan DDoS saldırı tespit mimarisi Şekil 2.9'de gösterilmektedir. Derin öğrenme modeli uygulanması için öncelikle hazır verisetleri sisteme yüklenmektedir. Daha sonra yüklenen verisetlerinde yer alan modelin eğitimine katkı sağlamadığı için gereksiz olarak nitelenen özelliklere ait sütunlar verisetinden silinmektedir. Bu işlemden sonra verisetinde yer alan sonsuz veya negatif değerler uygun değerlerle ile değiştirilmiştir. Boşluk içeren veya "NaN" yazan satırlar silinerek veriseti temizlenmiştir. Daha sonra veriseti %80 eğitim ve %20 test veriseti olmak üzere ikiye ayrılmıştır. Veriseti bölündükten sonra veriler 0-1 aralığında normalize edilmiştir. Bütün bu ön işleme aşamaları tamamlandıktan sonra eğitim veriseti modelin eğitimine hazır hale gelmiştir.



Şekil 2.9. DDoS saldırı tespit mimarisi.

CICIDS2017 verisetinden 225740 DDoS ağ trafiği içeren paketler alınmış ve veri setindeki sınıf etiketleri, "BENIGN" etiket değerleri “0” ve "DDoS" etiket değerleri “1” olacak şekilde sayısal kategorilere dönüştürülmüştür. “Hedef Port”, “Kaynak IP”, “Hedef IP”, “Protokol”, “Zaman Damgası” gibi paket içindeki özellikler, derin öğrenme modelin eğitimine uygun olmayan değerler içerdiği için eğitim verisetinden kaldırılmıştır. Verisetindeki diğer tüm özellikler modelin eğitimi için kullanılmıştır.

NSL-KDD verisetindeki sınıf etiketleri, “normal” etiket değerleri 0'a ve diğer saldırı türleri 1'e dönüştürülmüştür. Modelin eğitimine uygun olmayan “protokol türü”, “hizmet”, “bayrak” özellikleri eğitim verisetinden kaldırılmıştır. Verisetindeki diğer tüm özellikler kullanılmıştır.

CICDDoS2019 veriseti, büyük miktarda paket içerdiğinden model bütün verisetiyle eğitilmek yerine eğitimi kolaylaştırmak için verisetinden alınan örneklemlerle küçültülmüştür. Verisetinin yüklenmesinde küçültme işlemi yapılırken, örneklemin rastgele olması için rastgele aralıklarla satırlar atlanarak dosya okuma işlemi yapılmıştır. CICDDoS2019 verisetinde yer alan 86 özellik içinden model eğitimine uygun olmayan 17 özellik verisetinden kaldırılmış ve model 69 özellik ile eğitilmiştir. CICDDoS2019 veriseti, DDoS saldırı tespiti ve DDoS tür sınıflaması için 2 kategoriye ayrılmıştır. Birinci kategoride, ağ trafiğine yönelik bir saldırıyı tespit etmek için oluşturulan veriseti "BENIGN", "0" olarak ve diğer saldırılar "1" olarak etiketlenmiştir. İkinci kategoride,

saldırıların sınıflandırılması için Şekil 2.1'deki gibi iki gruba ayrılan saldırı türleri, sömürü ve yansıma tabanlı saldırı olarak etiketlenmiştir. Verisetinde bu sınıf etiketleri de "sömürü" tabanlı olanlar "0" ve yansıma tabanlı olanlar "1" olarak etiketlenmiş ve normal trafik bu verisetinden çıkartılmıştır.

SWDDoS2020 verisetinde yer alan 25 adet özellikten model eğitimi için uygun olmayan 16 özellik çıkartılmıştır. Sınıf etiketleme işlemi olarak normal trafik "0" ve TCP, UDP ve ICMP sel saldırıları "1" olarak etiketlenmiştir.

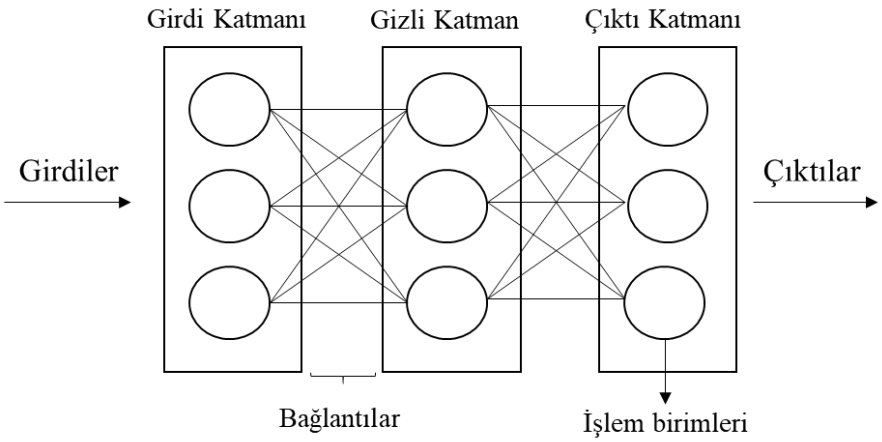
Bütün kullanılan verisetlerinde modelin eğitimini yanlış yönlendiren 'sonsuz' değeri '-1' ile değiştirilmiş ve 'NaN' değerlerini içeren satırlar silinmiştir. Verisetleri, eğitim ve test veriseti olarak 8:2 oranında bölünmüştür. Eğitim verisetindeki her özelliğe ait değerler için 0-1 değer aralığında ölçeklendirme yapılarak normalleştirme işlemi uygulanmıştır.

2.4. Derin Öğrenme Mimarisi

Bu bölümde önerilen model hakkında altyapı oluşturmak için modelde kullanılan özelliklerden, matematiksel arka planından ve derin öğrenme modelinin genel yapısından bahsedilmektedir.

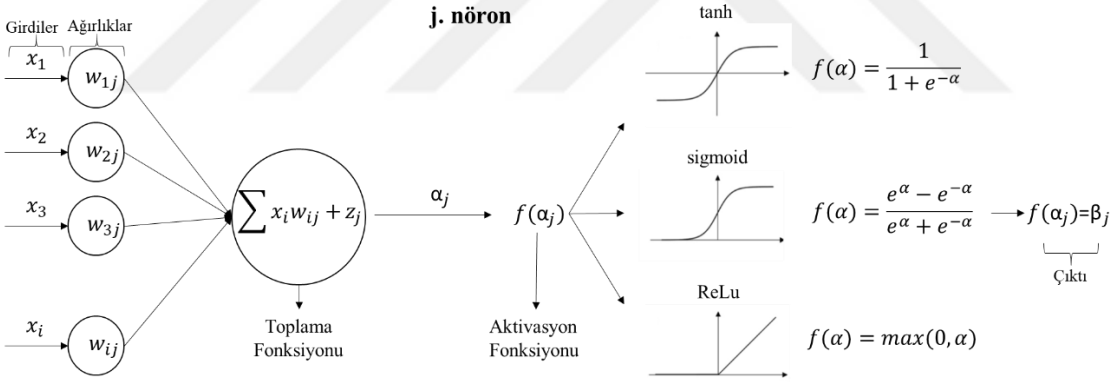
2.4.1. Yapay sinir ağları

Biyolojik sinir ağlarından esinlenen yapay sinir ağları (YSA), çok sayıda ara bağlantıya sahip basit işlem birimlerinden oluşan paralel hesaplama sistemleridir. Yapay bir nöron, doğal nöronlardan esinlenen hesaplamalı bir modeldir. Ağda yer alan düğümler "yapay nöronlar" olarak tanımlanan işlem birimleridir ve bunlar YSA'ları oluşturmaktadır. YSA'ların işlevi bilgiyi işlemek olduğu için ağırlıklı olarak örüntü tanıma, tahmin ve veri sıkıştırma gibi mühendislik amaçları için kullanılmaktadır [85]. YSA'lar genel olarak girdi katmanı, gizli katman ve çıktı katmanı olmak üzere 3 katmandan oluşmaktadır. Şekil 2.10'da YSA'ların genel yapısı gösterilmektedir.



Şekil 2.10. Bir YSA'nın genel yapısı.

Bir YSA modelinde verilerin girişi, girdi verisetinin girdi katmanıyla işleme sokulmasıyla ile başlamaktadır. Girdi katmanından gelen veriler işlem birimlerinde yer alan hesaplamalarla işlenmek üzere gizli katmana iletilmektedir. Daha sonra gizli katmandan gelen veriler çıktı katmanında işlenerek çıktı veriseti elde edilmektedir. Şekil 2.11'de işlem birimleri olan bir yapay nöronun işleyişi ile ilgili yapıya yer verilmiştir.



Şekil 2.11. Bir yapay nöronun yapısı ve matematiksel formülasyonu.

Şekil 2.11'de oklarla gösterilen ve bilgi akışını temsil eden değerlerine girdiler denmektedir. Bir nöronda girdilerle aktarılan bilginin önem ve hücreye olan etkisi *w* ile gösterilen ağırlıklar ile belirlenmektedir. Ağırlık ne kadar yüksek değere sahipse, girdinin etkisinin güçlü olacağı belirlenmektedir. Giriş nöronlarının yalnızca bir girişi olduğundan, çıktıları aldıkları girdinin bir ağırlıkla çarpımı olacaktır. Girdiler bir nöronda yer alan ağırlıklarla çarpıldıktan sonra her katmanda bulunun ön yargılar (*z*) eklenir ve toplama fonksiyonu kullanılarak α ile gösterilen net girdi hesaplanır. Bu net girdi nöronun matematiksel bir fonksiyonu olan aktivasyon fonksiyonuyla işleme girmektedir. Sonuç

olarak β ile gösterilen çıktı elde edilmiştir [85]. YSA'nın her gizli katmanın düğümünü temsil eden g_i fonksiyonunun matematiksel yapısı aktivasyon fonksiyonu f ile gösterilecek şekilde aşağıdaki gibi verilmiştir [86]:

$$g_i(\boldsymbol{x}) = f(\boldsymbol{x}^T\boldsymbol{w}+z) \quad (2.1)$$

Yapay bir nöronun ağırlıklarını ayarlayarak, belirli girdiler için istenilen çıktı elde edebilmektedir. Fakat yüzlerce veya binlerce nörondan oluşan bir YSA olduğunda, gerekli tüm ağırlıkları elle bulmak oldukça karmaşık olmaktadır. Ancak ağdan istenen çıktıyı elde etmek için yardımcı algoritmalar aracılığıyla YSA'nın ağırlıkları ayarlanabilmektedir. Bu ağırlık ayarlama sürecine öğrenme veya eğitim denmektedir. Eğitim rastgele ağırlıklarla başlar ve hataların minimum düzeyde olacak şekilde ayarlanmasını amaçlamaktadır[87].

2.4.2. Çok katmanlı ağ yapısı

Bu tezde önerilen derin öğrenme modeli, YSA'nın derin sinir ağlarında kullanımı yaygın olan çok katmanlı algılayıcılar (MLP) yapısına dayanmaktadır. Bu derin sinir ağı aynı zamanda İleri Beslemeli Sinir Ağı (FNN) adı verilen derin öğrenme modelidir. FNN, modelin çıktılarıyla kendisini beslemesini sağlayan geri bildirim bağlantılarına sahip olmaması yönünden Tekrarlayan Sinir Ağlarından (RNN) farklıdır. FNN, giriş katmanı, çıktı katmanı ve gizli katman olmak üzere en az üç katmandan oluşur. Sinir ağının yapısını oluşturan bu katmanlar, modelin derinliğini ifade etmekte ve derin öğrenmenin adı buradan gelmektedir. Ağdaki her gizli katman, vektör değerlerinden oluşur ve gizli katmanların boyutu, modelin genişliği olarak tanımlanmaktadır [86,88]. FNN'nin gizli katmanlarını (2.1) nolu denklemden yola çıkarak iç içe geçmiş zincir formunda (2.2) nolu denklemdeki gibi gösterebiliriz:

$$y=g_i(g_{i-1}(\ldots(g_1(\boldsymbol{x})))) \quad (2.2)$$

Gizli katmanların zincir şeklindeki bu yapısı derin sinir ağlarını oluşturmaktadır. FNN'nin (2.2) nolu matematiksel tanımında, her gizli katmanın düğümleri için hesaplanacak fonksiyon g_i, gizli katman sayısı i, girdi vektörü x, çıktı vektörü y notasyonu ile ifade edilir.

2.4.3. İleri besleme

İleri besleme, yapay sinir ağlarında yer alan ilk ve en temel özelliktir. İleri besleme özelliğine sahip ağlarda bilgi akışı daime sırasıyla girdi katmanı, gizli katmanlar ve çıktı katmanı olacak şekilde ileri doğru ve tek yönlüdür [89].

2.4.4. Aktivasyon fonksiyonları

Bir nörondan çıktı elde edebilmek için kullanılan bir fonksiyondur. Aynı zamanda "Transfer Fonksiyonu" olarak da adlandırılır. "Var" veya "Yok" gibi ikili sonuçlar için oluşturulmuş sinir ağlarının çıktısını belirlemek için kullanılır. Seçilen aktivasyon fonksiyonuna göre "0 ile 1" veya "-1 ile 1" arasında değerler elde edilir. Problemin çeşidine göre çeşitli aktivasyon fonksiyonlar tercih edilebilmektedir. Yaygın kullanılan aktivasyon fonksiyonlarından bazıları; *Sigmoid*, *Tanh*, (Rectified Linear Unit) *ReLu*, *Softmax* fonksiyonları olarak gösterilebilir [85].

2.4.5. Kayıp fonksiyonu

Genellikle sinir ağlarında sonuçlardan elde edilen hata en aza indirgenmeye çalışılmaktadır [86]. Hatanın en aza indirgenmesi için kayıp fonksiyonları olarak tanımlanan fonksiyonlar geliştirilmiştir. "ortalama kare hata", "çapraz entropi" gibi fonksiyonlar derin öğrenme modellerinde yaygın olan bazı kayıp fonksiyonlarıdır.

2.4.6. Optimizasyon algoritması

Bir optimizasyon algoritması, optimum veya tatmin edici bir sonuç bulunana kadar çeşitli sonuçları karşılaştırarak yinelemeli olarak yürütülen bir prosedürdür. Optimizasyon, hataları azaltmak için sinir ağının ağırlık ve öğrenme hızı gibi özelliklerini değiştiren algoritmalar veya yöntemlerdir. Optimize ediciler, daha hızlı sonuç alınmasına yardımcı olmaktadır. "Stochastic Gradient Descent (SGD)", "Adagrad", "Root Mean Square Propagation (Rmsprop)", "Adaptive Moment Estimation (ADAM)" ve "Adaptive Max Pooling (ADAMAX)" derin öğrenme modellerinde sık kullanılan optimizasyon algoritmalarıdır [90].

2.4.7. “mini-batch” boyutu

Batch boyutu, derin öğrenme modelinde yer alan parametreleri güncellemeden önce üzerinde çalışılması gereken eğitim verisetinden alınacak örneklerin sayısını tanımlayan bir hiperparametredir. Verisetinde yer alan bütün verileri aynı anda işlemek, zaman ve bellek bakımından maliyetli olduğu için girdinin parçalar halinde işlenmesine “mini-batch” denilmektedir. Model tasarımında aynı anda ne kadar verinin işleneceğini ifade eden değer mini-batch parametresidir [90].

2.4.8. “epoch” zamanı

Epoch(dönem), modelin eğitiminde belli sayıda parçalara bölünmüş verisetinin tamamını kaç kez gördüğünü ifade etmek için kullanılır. Dolayısıyla, algoritma verisetindeki bütün örnekleri her gördüğünde, bir dönem tamamlanmış olur [90].

2.5. Ağ Analizinde Tespit ve Sınıflandırma için Önerilen Modeli

Bu bölümde DDoS saldırı tespiti ve sınıflandırılmasında kullanılan derin öğrenme modelin oluşturulma aşamalarından ve modelin mimarisinden bahsedilmektedir.

Önerilen MLP tabanlı (Deep Neural Network) DNN modeline karar verilme aşamasında ön modeller oluşturulmuş ve bunlar hazır verisetleri üzerinde test edilerek modelin olgunluğa ulaşması hedeflenmiştir. Bu yüzden literatür incelemeleri de göz önünde bulundurularak gizli katman, nöron sayıları, aktivasyon fonksiyonları ve optimizasyon algoritmalarından oluşturulmuş farklı deneysel DNN modelleri test edilmek için hazırlanmıştır. Modellerin eğitimi için batch boyutu 64 olarak belirlenmiştir. NSL-KDD CICIDS2017 ve CICDDoS2019 verisetlerinin DDoS Saldırı Tespiti için kullanımının yanı sıra CICDDoS2019 veriseti DDoS saldırılarının sınıflandırılması için de kullanılmıştır. Bahsedilen üç veriseti üzerinde denenecek ön modellerin ayrıntıları Tablo 2.11’de verilmektedir.

Tablo 2.11. NSL-KDD, CICIDS2017, CICDDoS2019 verisetleri için modeller.

Model adı	Düğüm	Aktivasyon	Optimizasyon	Katman	Model adı	Düğüm	Aktivasyon	Optimizasyon	Katman
Model 1	10	sigmoid	adam	2	Model 19	10	sigmoid	adam	3
Model 2	10	sigmoid	adamax	2	Model 20	10	sigmoid	adamax	3
Model 3	10	tanh	adam	2	Model 21	10	tanh	adam	3
Model 4	10	tanh	adamax	2	Model 22	10	tanh	adamax	3

Model 5	10	relu	adam	2	Model 23	10	relu	adam	3
Model 6	10	relu	adamax	2	Model 24	10	relu	adamax	3
Model 7	50	sigmoid	adam	2	Model 25	50	sigmoid	adam	3
Model 8	50	sigmoid	adamax	2	Model 26	50	sigmoid	adamax	3
Model 9	50	tanh	adam	2	Model 27	50	tanh	adam	3
Model 10	50	tanh	adamax	2	Model 28	50	tanh	adamax	3
Model 11	50	relu	adam	2	Model 29	50	relu	adam	3
Model 12	50	relu	adamax	2	Model 30	50	relu	adamax	3
Model 13	100	sigmoid	adam	2	Model 31	100	sigmoid	adam	3
Model 14	100	sigmoid	adamax	2	Model 32	100	sigmoid	adamax	3
Model 15	100	tanh	adam	2	Model 33	100	tanh	adam	3
Model 16	100	tanh	adamax	2	Model 34	100	tanh	adamax	3
Model 17	100	relu	adam	2	Model 35	100	relu	adam	3
Model 18	100	relu	adamax	2	Model 36	100	relu	adamax	3

Yaygın kullanılan ve derin öğrenme problemine uygun olduğu düşünülen çeşitli aktivasyon fonksiyonu ve optimizason algoritmalarından oluşan 36 adet DNN modeli verisetleriyle uygulanmak için hazırlanmıştır.

2.5.1. Aktivasyon fonksiyonları

Modeller oluşturulurken Relu, Sigmoid, Hiperbolik Tanjant aktivasyon fonksiyonları yaygın kullanıldığı için tercih edilmiştir. Gizli katmanlarda kullanılan bu üç aktivasyon fonksiyonlarından ReLu fonksiyonu (2.3) nolu denklemde, sigmoid fonksiyonu (2.4) nolu denklemde ve hiperbolik tanjant aktivasyon fonksiyonu (2.5) nolu denklemde verilmiştir [86]:

$$relu(x)=max(0,x) \tag{2.3}$$

$$sigmoid(x) = \frac{1}{e^{-x}+1} \tag{2.4}$$

$$tanh(x)= \frac{e^{2x}-1}{e^{2x}+1} \tag{2.5}$$

softargmax [90] veya normalleştirilmiş üstel fonksiyon olarak da bilinen softmax fonksiyonu lojistik fonksiyonun çoklu boyutlara genellemesidir. Önerilen DNN modellerinin çıktı katmanı için kullanılan softmax aktivasyon fonksiyonu (2.6) nolu denklem ile verilmiştir [86]:

$$\text{softmax}(x_i) = \frac{e^{x_i}}{\sum_{j=1}^{n} e^{x_j}} \tag{2.6}$$

2.5.2. Kayıp fonksiyonu

Modellerin öğrenmesinin doğruluğunu artırmak için kayıp fonksiyonu olarak ikili çapraz entropi fonksiyonu kullanılmış ve aşağıdaki denklem ile verilmiştir [91]:

$$q_0 = 1 - \hat{y},\ q_1 = \hat{y} \quad (2.7)$$

$$p_0 = 1 - y,\ p_1 = y \quad (2.8)$$

$$L = -\sum_i p_n \log q_n = -y \log \hat{y} - (1 - y)\log(1 - \hat{y}) \quad (2.9)$$

burada sırasıyla *L* kayıp fonksiyonunu, *log* doğal logaritmayı, p_n gerçek olasılığı, y gerçek olasılık değerini, q_n tahmin edilen olasılığı, ŷ tahmin edilen olasılık değerini, n sayısı {0,1} değerlerini göstermektedir.

2.5.3. Optimizasyon algoritmaları

DNN modellerinde kullanımı yaygın olan iki optimizasyon algoritması tercih edilmiştir. Birinci olarak kullanılan algoritma ADAM optimizasyon algoritmasıdır. SGD tabanlı bir optimizasyon yöntemi olan ADAM [92], yalnızca daha az bellek gereksinimi olan birinci dereceden gradyanlar gerekli olduğu için etkilidir. Spesifik uyarlanabilir öğrenme oranları hesaplanarak, gradyanların birinci ve ikinci momentlerinin tahminlerinden farklı parametreler elde edilir. ADAM 'ın güncelleme formülü parametre şu şekilde verilir:

$$m_t = \Omega_1 m_{t-1} + (1 - \Omega_1) g_t \quad (2.10)$$

$$v_t = \Omega_2 v_{t-1} + (1 - \Omega_2)(g_t)^2 \quad (2.11)$$

$$m_t^{corrected} = \frac{m_t}{1 - (\Omega_1)^t} \quad (2.12)$$

$$v_t^{corrected} = \frac{v_t}{1 - (\Omega_2)^t} \quad (2.13)$$

$$W_t = W_{t-1} - \lambda \frac{m_t^{corrected}}{\sqrt{v_t^{corrected}} + \epsilon} \quad (2.14)$$

burada g_t, *t* adımdaki gradyanları, m_t birinci moment gradyanları, v_t ikinci moment gradyanları, Ω_1, $\Omega_2 \in [0,1)$ üssel bozulma oranlarını, λ adım boyutu, ϵ sıfıra bölünmeyi önlemek için küçük bir değeri, W_t ağırlık vektörünü(güncellenecek parametre) temsil etmektedir. Makine öğrenmesi problemlerinde λ=0.001, Ω_1=0.9, Ω_2=0.999 *ve* $\epsilon = 10^{-8}$ varsayılan değerlerinin kullanımı daha iyi sonuçlar vermektedir [92].

İkinci optimizasyon algoritması olarak "ADAMAX" kullanılmıştır. ADAMAX [92], ADAM optimizasyon algoritması kuralının sonsuzluk normu ile güncellenmesiyle elde

edilmiştir. ADAMAX 'ın optimizasyon algoritması için matematiksel formül şu şekilde verilmiştir:

$$m_t = \Omega_1 m_{t-1} + (1 - \Omega_1) g_t \quad (2.15)$$

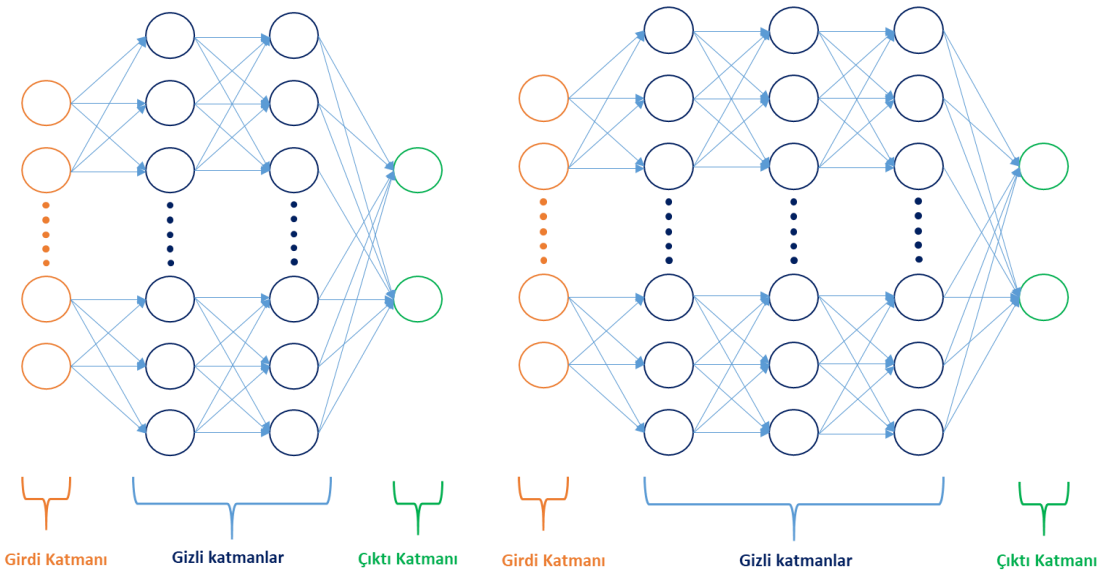
$$u_t = \max(\Omega_2 u_{t-1}, |g_t|) \quad (2.16)$$

$$\theta_t = \theta_{t-1} - (\frac{\lambda}{1-\Omega_1^t}) \frac{m_t}{v_t} \quad (2.17)$$

burada t zaman adımı olarak, g_t, t adımdaki gradyanlar olarak, m_t ilk moment vektörü olarak, u_t üssel ağırlıklı sonsuzluk normu olarak, Ω_1, $\Omega_2 \in [0,1)$ üssel bozulma oranları olarak, λ adım boyutu olarak, θ_t güncellenmiş parametre olarak gösterilmektedir. Yukarıdaki (2.15), (2.16), (2.17) nolu denklemler ile verilen algoritmanın t=0 anındaki m_t'nin başlangıç değeri m_0=0 ve u_t'un başlangıç değeri u_0=0 olarak alınır. Bu algoritmada λ=0.002, Ω_1=0.9, Ω_2=0.999 varsayılan değerlerinin kullanımı problemlerin çözümünde daha uygundur [92].

2.5.4. Derin öğrenme modelinin mimarisi

Özellik çıkarma ve sınıflandırma süreçleri DNN modelinin yapısında birleştirildiği için, DNN modeli hem denetimli öğrenme hem de denetimsiz öğrenme avantajlarına sahiptir [88]. Şekil 2.12'de gösterilen önerilen 2 ve 3 gizli katmanlı DNN modelleri bir giriş, bir çıkış ve gizli katmanlardan oluşmaktadır.



Şekil 2.12. Önerilen 2 ve 3 katmanlı DNN modellerinin genel yapısı.

2 ve 3 gizli katmana sahip modeller tasarlanırken sırasıyla optimizasyon algoritması olarak ADAM ve ADAMAX, her gizli katmanda aktivasyon fonksiyonu olarak Relu, Sigmoid ve hiperbolik tanjant ve gizli katmanlarda yer alan nöron sayısı ise 10, 50, 100 adet olarak kullanılmış ve oluşturulan 36 adet model denenerek DNN modeli için optimum sonuçlar veren mimariye ulaşılmak istenmiştir. Deneylerde DDoS saldırı tespit ve sınıflandırma işlemleri 2 etiketten oluştuğu için çıkış katmanında 2 düğüm kullanılmıştır. Çıktı katmanında, aktivasyon fonksiyonu *softmax* kullanılmıştır. Ayrıca CICDDoS2019 verisetinde DDoS saldırı tespitinin yanı sıra saldırı tipi sınıflama işlemleri için de bu 36 model uygulanmıştır.

3. BULGULAR VE TARTIŞMA

Bu bölümde DDoS saldırıların tespiti ve sınıflandırılmasında önerilen modelin uygulandığı deney ortamından, deneylerin değerlendirilme ölçütlerinden, önerilen DNN modelinin kullanılan verisetleri üzerinde test edilmesinden, elde edilen deney sonuçlarından ve modelin başarı durumundan bahsedilmektedir.

3.1. Deney Ortamı

Deneyler için kullanılan bilgisayar Windows 10 OS, Intel Core i7-7700K CPU 4.2 GHz işlemci, 32GB RAM, 2X512GB SSD ve NVIDIA GTX 1080 Ti Graphics Coprocessor özelliklerini içermektedir. Geliştirme ortamı olarak Spyder IDE[93], programlama dili olarak Python 3.7 tercih edilmiş ve derin öğrenme modeli için Tensorflow [94], Keras [95], Pandas [96] kütüphaneleri kullanılarak deneysel ortam hazırlanmıştır.

3.2. Performans Metrikleri

Modelin performansını ölçmek için karıştırma matrisi kullanılarak elde edilen Doğruluk, Kesinlik, Geri Çağırma(Duyarlılık), F ölçümü gibi değerler kullanılmıştır. Tablo 3.1'deki karmaşıklık matrisi performans ölçümlerini içermektedir [97].

Tablo 3.1. Karmaşıklık Matrisi.

	Pozitif Tahmin	**Negatif Tahmin**
Gerçek Pozitif	Doğru Pozitif (TP)	Yanlış Negatif (FN)
Gerçek Negatif	Yanlış Pozitif (FP)	Doğru Negatif (TN)

Doğruluk: (3.1) nolu denklem ile tanımlanan doğruluk, tüm doğru tahminlerin sayısının tüm verisetine bölünmesiyle hesaplanır.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \tag{3.1}$$

Kesinlik: (3.2) nolu denklem tarafından tanımlanan kesinlik, doğru pozitif tahminlerin sayısının tüm pozitif tahminlerin sayısına bölünmesiyle hesaplanır.

$$\text{Precision} = \frac{TP}{TP+FP} \tag{3.2}$$

Hatırlama: Aynı zamanda tahminin duyarlılığı olan (3.3) nolu denklem ile tanımlanan geri çağırma, gerçek pozitif tahminlerin sayısının verisetindeki gerçek pozitiflerin sayısına bölünmesiyle bulunur.

$$\text{Recall} = \frac{TP}{TP+FN} \tag{3.3}$$

F Puanı: (3.4) nolu denklem ile tanımlanan F puanı, duyarlılık ve geri çağırma arasındaki dengeyi gösterir.

$$\text{F Score} = 2 \text{ x } \frac{Kesinlik\ x\ Geri\ Çağırma}{Kesinlik + Geri\ Çağırma} \tag{3.4}$$

3.3. Deney Sonuçları

Bölüm 2.5'te bahsedilen derin öğrenme modeli öncelikle CICIDS2017 ve NSL-KDD veri setlerinde kullanılmıştır. Modelin öğrenme zamanı, kullanılan ekipman ve verisetinin büyüklüğüne göre değişeceğinden çalışmada performans göstergesi olarak değerlendirilmemektedir. uygulanan sırasıyla Üç gizli katmana sahip DNN modelin her gizli katmanında 10, 50, 100 düğüm kullanılarak üç farklı deney modeli oluşturulmuştur. Bu üç deney modeli için ayrı ayrı 10, 25, 50 epoch ayarlanarak bu iki veriseti üzerinde model eğitimi gerçekleştirilmiştir.

NSL-KDD verisetine uygulanan üç model için Tablo 3.2'deki sonuçlar elde edilmiştir.

Tablo 3.2. NSL-KDD verisetinde DNN modelinin değerlendirilmesi.

Epoch	Model	Doğruluk	Kesinlik	Duyarlılık	F1	Model	Doğruluk	Kesinlik	Duyarlılık	F1
10	Model 1	0,9758	0,9771	0,9627	0,9699	Model 19	0,9765	0,9834	0,9582	0,9706
25	Model 1	0,9885	0,9802	0,9916	0,9859	Model 19	0,9825	0,9864	0,9703	0,9783
50	Model 1	0,9938	0,9892	0,9956	0,9924	Model 19	0,9937	0,9887	0,9959	0,9923
10	Model 2	0,9747	0,9826	0,9544	0,9683	Model 20	0,9752	0,9817	0,9567	0,9690
25	Model 2	0,9767	0,9833	0,9589	0,9709	Model 20	0,9781	0,9782	0,9675	0,9728
50	Model 2	0,9895	0,9869	0,9873	0,9871	Model 20	0,9909	0,9871	0,9904	0,9888
10	Model 3	0,9920	0,9862	0,9943	0,9902	Model 21	0,9933	0,9886	0,9949	0,9917
25	Model 3	0,9932	0,9897	0,9937	0,9917	Model 21	0,9943	0,9880	0,9979	0,9929
50	Model 3	0,9937	0,9866	0,9981	0,9923	Model 21	0,9944	0,9889	0,9974	0,9931
10	Model 4	0,9866	0,9863	0,9805	0,9834	Model 22	0,9890	0,9900	0,9828	0,9863
25	Model 4	0,9923	0,9903	0,9907	0,9905	Model 22	0,9932	0,9860	0,9973	0,9916
50	Model 4	0,9927	0,9888	0,9931	0,9910	Model 22	0,9943	0,9882	0,9977	0,9929
10	Model 5	0,9937	0,9921	0,9924	0,9923	Model 23	0,9944	0,9931	0,9930	0,9931
25	Model 5	0,9949	0,9905	0,9969	0,9937	Model 23	0,9948	0,9933	0,9940	0,9936
50	Model 5	0,9960	0,9924	0,9979	0,9951	Model 23	0,9953	0,9899	0,9986	0,9942
10	Model 6	0,9861	0,9863	0,9793	0,9828	Model 24	0,9916	0,9867	0,9928	0,9897
25	Model 6	0,9929	0,9906	0,9918	0,9912	Model 24	0,9949	0,9924	0,9950	0,9937

50	Model 6	0,9952	0,9905	0,9977	0,9941	Model 24	0,9953	0,9923	0,9963	0,9943
10	Model 7	0,9741	0,9954	0,9403	0,9671	Model 25	0,9873	0,9724	0,9969	0,9845
25	Model 7	0,9922	0,9840	0,9969	0,9904	Model 25	0,9823	0,9945	0,9617	0,9778
50	Model 7	0,9907	0,9971	0,9799	0,9884	Model 25	0,9937	0,9934	0,9911	0,9922
10	Model 8	0,9736	0,9784	0,9560	0,9671	Model 26	0,9743	0,9813	0,9549	0,9679
25	Model 8	0,9853	0,9830	0,9806	0,9818	Model 26	0,9889	0,9870	0,9855	0,9863
50	Model 8	0,9909	0,9866	0,9911	0,9889	Model 26	0,9842	0,9904	0,9705	0,9804
10	Model 9	0,9932	0,9875	0,9960	0,9917	Model 27	0,9937	0,9919	0,9927	0,9923
25	Model 9	0,9943	0,9891	0,9970	0,9930	Model 27	0,9943	0,9898	0,9962	0,9930
50	Model 9	0,9957	0,9914	0,9980	0,9947	Model 27	0,9955	0,9912	0,9978	0,9945
10	Model 10	0,9901	0,9889	0,9867	0,9878	Model 28	0,9926	0,9933	0,9884	0,9908
25	Model 10	0,9943	0,9897	0,9963	0,9930	Model 28	0,9949	0,9896	0,9978	0,9937
50	Model 10	0,9950	0,9935	0,9941	0,9938	Model 28	0,9952	0,9945	0,9937	0,9941
10	Model 11	0,9946	0,9936	0,9932	0,9934	Model 29	0,9942	0,9893	0,9965	0,9929
25	Model 11	0,9946	0,9880	0,9988	0,9933	Model 29	0,9949	0,9888	0,9987	0,9937
50	Model 11	0,9960	0,9921	0,9981	0,9951	Model 29	0,9969	0,9944	0,9981	0,9962
10	Model 12	0,9950	0,9901	0,9976	0,9938	Model 30	0,9942	0,9902	0,9956	0,9929
25	Model 12	0,9948	0,9904	0,9967	0,9936	Model 30	0,9949	0,9892	0,9983	0,9937
50	Model 12	0,9959	0,9944	0,9954	0,9949	Model 30	0,9961	0,9951	0,9953	0,9952
10	Model 13	0,9767	0,9948	0,9476	0,9706	Model 31	0,9869	0,9717	0,9968	0,9841
25	Model 13	0,9940	0,9890	0,9963	0,9926	Model 31	0,9935	0,9886	0,9955	0,9920
50	Model 13	0,9939	0,9869	0,9982	0,9925	Model 31	0,9937	0,9866	0,9979	0,9922
10	Model 14	0,9727	0,9798	0,9524	0,9659	Model 32	0,9730	0,9782	0,9546	0,9662
25	Model 14	0,9899	0,9849	0,9902	0,9876	Model 32	0,9826	0,9781	0,9790	0,9785
50	Model 14	0,9749	0,9974	0,9405	0,9681	Model 32	0,9875	0,9944	0,9747	0,9845
10	Model 15	0,9917	0,9904	0,9891	0,9897	Model 33	0,9930	0,9875	0,9952	0,9914
25	Model 15	0,9953	0,9900	0,9986	0,9943	Model 33	0,9960	0,9925	0,9977	0,9951
50	Model 15	0,9957	0,9940	0,9955	0,9947	Model 33	0,9959	0,9941	0,9959	0,9950
10	Model 16	0,9921	0,9864	0,9942	0,9903	Model 34	0,9941	0,9893	0,9964	0,9928
25	Model 16	0,9947	0,9911	0,9958	0,9935	Model 34	0,9959	0,9925	0,9974	0,9949
50	Model 16	0,9953	0,9903	0,9981	0,9942	Model 34	0,9946	0,9912	0,9956	0,9934
10	Model 17	0,9952	0,9909	0,9974	0,9941	Model 35	0,9949	0,9915	0,9960	0,9937
25	Model 17	0,9952	0,9928	0,9954	0,9941	Model 35	0,9962	0,9945	0,9960	0,9953
50	Model 17	0,9960	0,9952	0,9949	0,9951	Model 35	0,9959	0,9913	0,9987	0,9949
10	Model 18	0,9945	0,9934	0,9931	0,9932	Model 36	0,9945	0,9916	0,9949	0,9933
25	Model 18	0,9953	0,9921	0,9965	0,9943	Model 36	0,9952	0,9893	0,9989	0,9941
50	Model 18	0,9962	0,9926	0,9981	0,9953	Model 36	0,9945	0,9883	0,9982	0,9932

Tablo 3.2'de yer alan sonuçlar incelendiğinde ağdaki DDoS varlığının tespitinde doğruluk ile birlikte duyarlılık değerinin ön plana çıktığı görülmekte ve bu değerleri en yüksek veren yapının 25 epochta Model 11 ve Model 36 olmak üzere iki DNN modeli olduğu yorumu çıkarılabilmektedir.

DDoS saldırılarını tespit etmek için ağ trafiği paketlerini içeren CICIDS2017 verisetine de aynı üç deney modeli uygulanmıştır. Tablo 3.3, modelin eğitimi ve testi için kullanılan CICIDS2017 verisetinde bulunan paketlerin sayısını vermektedir.

Tablo 3.3. CICIDS2017 verisetinin dağılımı.

Classes	Train Dataset	Test Dataset
Normal	102442	25585
DDoS	78150	19563
Toplam	180592	45148

DNN modelinin CICIDS2017 verisetindeki test sonuçları Tablo 3.4'te kaydedilmiştir. CICIDS2017 veriseti için 36 adet DNN modelinin DDoS saldırı tespiti için uygulama sonuçları değerlendirilmektedir.

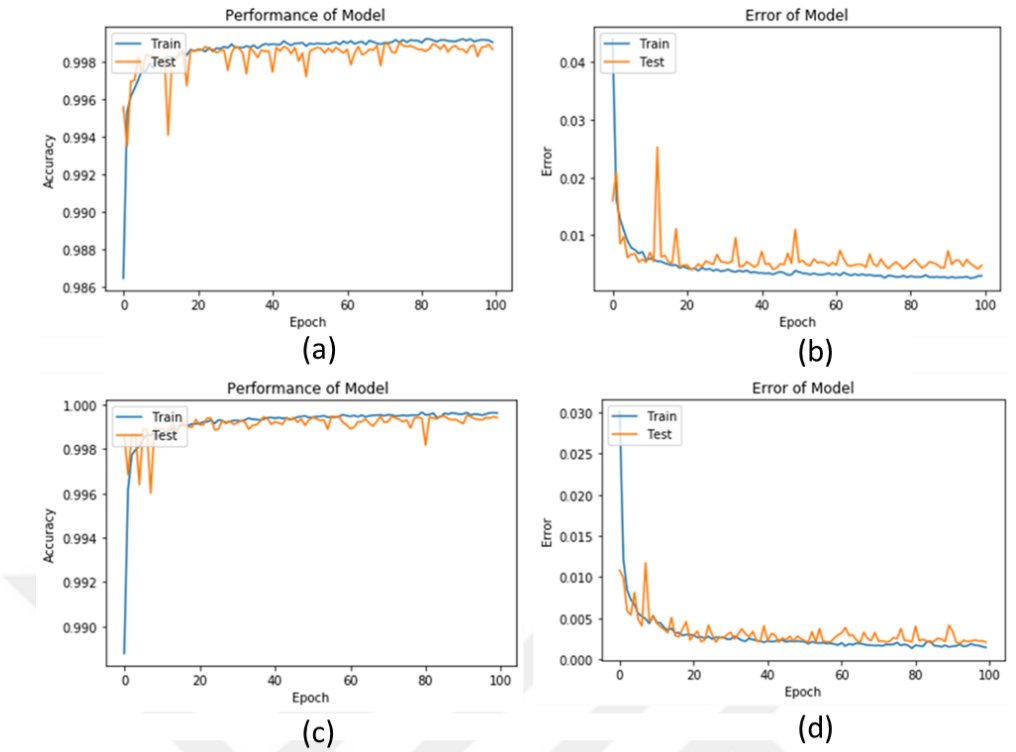
Tablo 3.4. CICIDS2017 verisetinde DNN modelinin değerlendirilmesi.

Epoch	Model	Doğruluk	Kesinlik	Duyarlılık	F1	Model	Doğruluk	Kesinlik	Duyarlılık	F1
10	Model 1	0,9846	0,9741	0,9994	0,9866	Model 19	0,9932	0,9889	0,9991	0,9940
25	Model 1	0,9870	0,9780	0,9996	0,9887	Model 19	0,9862	0,9767	0,9996	0,9880
50	Model 1	0,9861	0,9763	0,9998	0,9879	Model 19	0,9828	0,9709	0,9996	0,9850
10	Model 2	0,9808	0,9676	0,9995	0,9833	Model 20	0,9821	0,9697	0,9996	0,9844
25	Model 2	0,9825	0,9703	0,9996	0,9848	Model 20	0,9818	0,9692	0,9996	0,9842
50	Model 2	0,9809	0,9677	0,9997	0,9834	Model 20	0,9802	0,9666	0,9997	0,9829
10	Model 3	0,9877	0,9790	0,9997	0,9892	Model 21	0,9441	0,9105	0,9996	0,9530
25	Model 3	0,9846	0,9736	0,9999	0,9866	Model 21	0,9887	0,9957	0,9843	0,9900
50	Model 3	0,9857	0,9754	1,0000	0,9876	Model 21	0,9868	0,9777	0,9995	0,9885
10	Model 4	0,9811	0,9680	0,9997	0,9836	Model 22	0,9763	0,9601	0,9998	0,9795
25	Model 4	0,9753	0,9584	0,9998	0,9786	Model 22	0,9806	0,9672	0,9997	0,9832
50	Model 4	0,9821	0,9695	0,9998	0,9844	Model 22	0,9495	0,9989	0,9119	0,9535
10	Model 5	0,9825	0,9702	0,9998	0,9848	Model 23	0,9826	0,9703	0,9999	0,9849
25	Model 5	0,9983	0,9978	0,9992	0,9985	Model 23	0,9951	0,9987	0,9926	0,9956
50	Model 5	0,9901	0,9832	0,9996	0,9913	Model 23	0,9936	0,9997	0,9889	0,9943
10	Model 6	0,9810	0,9679	0,9997	0,9835	Model 24	0,9846	0,9739	0,9995	0,9866
25	Model 6	0,9844	0,9735	0,9996	0,9864	Model 24	0,9956	0,9982	0,9940	0,9961
50	Model 6	0,9885	0,9998	0,9799	0,9898	Model 24	0,8685	0,9989	0,7688	0,8689
10	Model 7	0,9846	0,9739	0,9996	0,9866	Model 25	0,9985	0,9983	0,9991	0,9987
25	Model 7	0,9889	0,9815	0,9994	0,9903	Model 25	0,9953	0,9926	0,9993	0,9959
50	Model 7	0,9827	0,9704	0,9999	0,9849	Model 25	0,9900	0,9833	0,9994	0,9913
10	Model 8	0,9829	0,9712	0,9995	0,9851	Model 26	0,9857	0,9761	0,9993	0,9876
25	Model 8	0,9821	0,9697	0,9996	0,9844	Model 26	0,9823	0,9701	0,9996	0,9846
50	Model 8	0,9834	0,9718	0,9996	0,9855	Model 26	0,9842	0,9732	0,9996	0,9862
10	Model 9	0,9824	0,9700	0,9999	0,9847	Model 27	0,9850	0,9746	0,9995	0,9869
25	Model 9	0,9993	0,9993	0,9995	0,9994	Model 27	0,9953	0,9975	0,9942	0,9958
50	Model 9	0,9968	0,9995	0,9948	0,9972	Model 27	0,9992	0,9994	0,9992	0,9993
10	Model 10	0,9819	0,9693	0,9997	0,9843	Model 28	0,9812	0,9681	0,9998	0,9837
25	Model 10	0,9810	0,9677	0,9998	0,9835	Model 28	0,9828	0,9709	0,9996	0,9850

50	Model 10	0,9808	0,9673	0,9999	0,9833	Model 28	0,9844	0,9735	0,9996	0,9864
10	Model 11	0,9850	0,9995	0,9740	0,9866	Model 29	0,9946	0,9907	0,9999	0,9953
25	Model 11	0,9898	0,9996	0,9823	0,9909	Model 29	0,9990	0,9987	0,9995	0,9991
50	Model 11	0,9898	0,9998	0,9822	0,9909	Model 29	0,9450	0,9997	0,9032	0,9490
10	Model 12	0,9988	0,9986	0,9992	0,9989	Model 30	0,9828	0,9708	0,9997	0,9850
25	Model 12	0,9761	0,9991	0,9587	0,9785	Model 30	0,9406	0,9999	0,8953	0,9447
50	Model 12	0,9529	0,9991	0,9177	0,9566	Model 30	0,8921	0,9998	0,8097	0,8948
10	Model 13	0,9881	0,9801	0,9993	0,9896	Model 31	0,9863	0,9769	0,9995	0,9881
25	Model 13	0,9878	0,9795	0,9995	0,9894	Model 31	0,9945	0,9910	0,9993	0,9951
50	Model 13	0,9854	0,9751	0,9998	0,9873	Model 31	0,9979	0,9975	0,9989	0,9982
10	Model 14	0,9832	0,9717	0,9995	0,9854	Model 32	0,9830	0,9713	0,9996	0,9852
25	Model 14	0,9831	0,9715	0,9996	0,9853	Model 32	0,9832	0,9716	0,9996	0,9854
50	Model 14	0,9822	0,9699	0,9997	0,9846	Model 32	0,9832	0,9715	0,9996	0,9854
10	Model 15	0,9823	0,9697	0,9999	0,9846	Model 33	0,9860	0,9765	0,9993	0,9878
25	Model 15	0,9866	0,9771	0,9998	0,9883	Model 33	0,9883	0,9804	0,9994	0,9898
50	Model 15	0,9983	0,9973	0,9996	0,9985	Model 33	0,9979	0,9966	0,9997	0,9981
10	Model 16	0,9802	0,9665	0,9998	0,9829	Model 34	0,9819	0,9694	0,9996	0,9843
25	Model 16	0,9813	0,9683	0,9998	0,9838	Model 34	0,9855	0,9759	0,9990	0,9873
50	Model 16	0,9848	0,9739	0,9999	0,9867	Model 34	0,9941	0,9903	0,9994	0,9948
10	Model 17	0,9704	0,9999	0,9479	0,9732	Model 35	0,9880	0,9997	0,9791	0,9893
25	Model 17	0,9959	0,9994	0,9934	0,9964	Model 35	0,9878	0,9997	0,9787	0,9891
50	Model 17	0,9959	0,9992	0,9935	0,9964	Model 35	0,9951	0,9996	0,9917	0,9956
10	Model 18	0,9988	0,9986	0,9992	0,9989	Model 36	0,9876	0,9988	0,9793	0,9890
25	Model 18	0,9990	0,9993	0,9989	0,9991	Model 36	0,9934	0,9998	0,9887	0,9942
50	Model 18	0,9856	0,9999	0,9746	0,9871	Model 36	0,9890	0,9994	0,9811	0,9902

Tablo 3.4'teki sonuçlar yorumlandığında NSL-KDD verisetinde en iyi sonuçları veren DNN modelinin CICIDS2017 veriseti için de geçerli olabileceği gözlemlenmektedir. Bunun yanı sıra CICIDS2017 verisetinde 50 epoch ile Model 3 DNN modeliyle DDoS saldırı tespiti için %98,57 doğruluk ve %100 duyarlılık, 50 epoch ile Model 27 DNN modeliyle saldırı tespiti için %99,92 doğruluk ve %99,92 duyarlılık ile en yüksek başarıların elde edildiği görülmektedir.

Şekil 3.1'de, CICIDS2017 veriseti ve NSL-KDD veriseti için önerilen modelin eğitim performansı ve hata oranı gözlemlenmektedir.



Şekil 3.1. (a) Modelin NSL-KDD verisetindeki performansı; (b) Model NSL-KDD verisetinin hata oranı; (c) CICIDS2017 verisetindeki modelin performansı; (d) CICIDS2017 verisetindeki modelin hata oranı.

DNN modelinin DDoS saldırılarının tespiti ve sınıflandırılmasında daha etkin kullanılabilmesi için CICDDoS2019 veriseti Tablo 3.5'teki gibi iki farklı formata dönüştürülmüştür. Dataset1, ağ trafiğindeki DDoS saldırılarını tespit etmek için normal ve saldırı içeren iki çeşit trafik olacak şekilde etiketlenmiştir. Dataset2'de CICDDoS2019 verisetinden normal trafik paketleri çıkartılmış ve sınıflandırma işlemini kolaylaştırmak için iki çeşit DDoS saldırı kaynağına göre veriseti etiketlenmiştir.

Tablo 3.5. CICDDoS2019 Verisetinin Bölümleri.

	Eğitim Veriseti	**Test Veriseti**
Dataset1	292379	73095
Dataset2	291904	72977

DNN modellerinin eğitimi için kullanılan CICDDoS2019 veriseti Dataset1 ve Dataset2 olacak şekilde iki ayrı verisetine ayrılarak deneyler yapılmıştır. Tablo 3.6'da DNN modellerinin Dataset1 veriseti üzerinde yapılan deney sonuçları yer almaktadır.

Tablo 3.6. Dataset1 verisetinde DNN modelinin değerlendirilmesi.

Epoch	Model	Doğruluk	Kesinlik	Duyarlılık	F1	Model	Doğruluk	Kesinlik	Duyarlılık	F1
10	Model 1	0,9996	0,9999	0,9998	0,9998	Model 19	0,9997	0,9999	0,9998	0,9998
25	Model 1	0,9997	0,9999	0,9998	0,9998	Model 19	0,9997	0,9998	0,9998	0,9998
50	Model 1	0,9996	0,9998	0,9998	0,9998	Model 19	0,9996	0,9999	0,9997	0,9998
10	Model 2	0,9985	0,9985	1	0,9993	Model 20	0,9997	1	0,9998	0,9999
25	Model 2	0,9996	0,9997	0,9999	0,9998	Model 20	0,9998	0,9999	0,9999	0,9999
50	Model 2	0,9996	0,9998	0,9998	0,9998	Model 20	0,9997	0,9998	0,9998	0,9998
10	Model 3	0,9994	0,9997	0,9997	0,9997	Model 21	0,9996	1	0,9995	0,9998
25	Model 3	0,9996	0,9999	0,9997	0,9998	Model 21	0,9996	1	0,9996	0,9998
50	Model 3	0,9996	0,9999	0,9997	0,9998	Model 21	0,9997	0,9999	0,9998	0,9998
10	Model 4	0,9996	0,9998	0,9998	0,9998	Model 22	0,9997	1	0,9997	0,9999
25	Model 4	0,9997	1	0,9998	0,9999	Model 22	0,9996	0,9998	0,9999	0,9998
50	Model 4	0,9996	0,9999	0,9997	0,9998	Model 22	0,9998	0,9999	0,9999	0,9999
10	Model 5	0,9995	0,9998	0,9997	0,9998	Model 23	0,9996	0,9998	0,9998	0,9998
25	Model 5	0,9996	0,9998	0,9999	0,9998	Model 23	0,9997	0,9998	0,9999	0,9998
50	Model 5	0,9997	0,9999	0,9999	0,9999	Model 23	0,9997	0,9998	0,9999	0,9999
10	Model 6	0,9998	0,9999	0,9999	0,9999	Model 24	0,9997	0,9999	0,9998	0,9998
25	Model 6	0,9998	1	0,9999	0,9999	Model 24	0,9996	0,9999	0,9997	0,9998
50	Model 6	0,9996	0,9999	0,9997	0,9998	Model 24	0,9996	0,9998	0,9998	0,9998
10	Model 7	0,9996	0,9998	0,9998	0,9998	Model 25	0,9997	0,9998	0,9999	0,9999
25	Model 7	0,9994	0,9997	0,9998	0,9997	Model 25	0,9997	0,9998	0,9999	0,9999
50	Model 7	0,9995	0,9998	0,9997	0,9997	Model 25	0,9995	0,9999	0,9996	0,9998
10	Model 8	0,9996	0,9997	0,9999	0,9998	Model 26	0,9997	0,9999	0,9998	0,9998
25	Model 8	0,9995	0,9996	0,9999	0,9998	Model 26	0,9997	0,9998	0,9999	0,9998
50	Model 8	0,9996	0,9997	0,9999	0,9998	Model 26	0,9997	0,9998	0,9999	0,9998
10	Model 9	0,9994	0,9997	0,9997	0,9997	Model 27	0,9992	1	0,9992	0,9996
25	Model 9	0,9996	0,9999	0,9997	0,9998	Model 27	0,9996	0,9999	0,9997	0,9998
50	Model 9	0,9995	0,9997	0,9998	0,9998	Model 27	0,9997	0,9998	0,9999	0,9998
10	Model 10	0,9995	0,9997	0,9999	0,9998	Model 28	0,9997	0,9999	0,9997	0,9998
25	Model 10	0,9996	0,9998	0,9998	0,9998	Model 28	0,9996	0,9999	0,9997	0,9998
50	Model 10	0,9996	0,9999	0,9997	0,9998	Model 28	0,9995	1	0,9995	0,9997
10	Model 11	0,9995	0,9998	0,9998	0,9998	Model 29	0,9995	1	0,9995	0,9998
25	Model 11	0,9996	0,9998	0,9998	0,9998	Model 29	0,9998	0,9999	0,9998	0,9999
50	Model 11	0,9997	0,9998	0,9999	0,9998	Model 29	0,9997	1	0,9997	0,9998
10	Model 12	0,9996	0,9998	0,9999	0,9998	Model 30	0,9996	0,9999	0,9997	0,9998
25	Model 12	0,9996	0,9998	0,9998	0,9998	Model 30	0,9996	1	0,9997	0,9998
50	Model 12	0,9996	0,9998	0,9999	0,9998	Model 30	0,9997	0,9998	0,9999	0,9999
10	Model 13	0,9996	0,9998	0,9998	0,9998	Model 31	0,9997	0,9998	0,9998	0,9998
25	Model 13	0,9995	0,9997	0,9998	0,9997	Model 31	0,9995	0,9999	0,9995	0,9997
50	Model 13	0,9995	0,9998	0,9997	0,9997	Model 31	0,9997	0,9998	0,9999	0,9998
10	Model 14	0,9996	0,9997	1	0,9998	Model 32	0,9997	0,9998	0,9998	0,9998
25	Model 14	0,9995	0,9996	0,9999	0,9998	Model 32	0,9997	0,9998	0,9998	0,9998
50	Model 14	0,9996	0,9997	0,9999	0,9998	Model 32	0,9997	0,9999	0,9997	0,9998
10	Model 15	0,9996	0,9999	0,9997	0,9998	Model 33	0,9997	1	0,9997	0,9999

25	Model 15	0,9995	0,9999	0,9996	0,9998	Model 33	0,9994	0,9998	0,9997	0,9997
50	Model 15	0,9996	0,9998	0,9998	0,9998	Model 33	0,9996	1	0,9996	0,9998
10	Model 16	0,9997	1	0,9998	0,9999	Model 34	0,9997	1	0,9997	0,9998
25	Model 16	0,9996	0,9999	0,9997	0,9998	Model 34	0,9997	1	0,9997	0,9998
50	Model 16	0,9995	0,9998	0,9997	0,9998	Model 34	0,9996	1	0,9996	0,9998
10	Model 17	0,9995	0,9996	0,9999	0,9998	Model 35	0,9996	1	0,9996	0,9998
25	Model 17	0,9996	0,9999	0,9998	0,9998	Model 35	0,9995	1	0,9995	0,9998
50	Model 17	0,9996	0,9999	0,9998	0,9998	Model 35	0,9996	1	0,9996	0,9998
10	Model 18	0,9998	0,9999	0,9999	0,9999	Model 36	0,9998	1	0,9998	0,9999
25	Model 18	0,9996	0,9998	0,9998	0,9998	Model 36	0,9997	0,9999	0,9998	0,9998
50	Model 18	0,9995	0,9997	0,9998	0,9998	Model 36	0,9997	1	0,9997	0,9998

Tablo 3.7'da DNN modellerinin Dataset2 veriseti üzerinde yapılan deney sonuçları yer almaktadır.

Tablo 3.7. Dataset2 verisetinde DNN modelinin değerlendirilmesi.

Epoch	Model	Doğruluk	Kesinlik	Duyarlılık	F1	Model	Doğruluk	Kesinlik	Duyarlılık	F1
10	Model 1	0,9257	0,8524	0,7409	0,7927	Model 19	0,9451	0,8176	0,9264	0,8686
25	Model 1	0,926	0,8542	0,7409	0,7935	Model 19	0,9474	0,7981	0,9795	0,8795
50	Model 1	0,9456	0,8426	0,8809	0,8613	Model 19	0,9478	0,8364	0,912	0,8725
10	Model 2	0,9253	0,8531	0,7375	0,7911	Model 20	0,9247	0,8703	0,7232	0,79
25	Model 2	0,9257	0,8526	0,7406	0,7927	Model 20	0,9358	0,7984	0,8996	0,846
50	Model 2	0,9487	0,8379	0,9085	0,8718	Model 20	0,9483	0,8466	0,8987	0,8719
10	Model 3	0,9467	0,848	0,8799	0,8637	Model 21	0,9455	0,8406	0,8909	0,865
25	Model 3	0,9486	0,8418	0,9014	0,8705	Model 21	0,9451	0,8489	0,8754	0,8619
50	Model 3	0,9567	0,8263	0,9801	0,8967	Model 21	0,9469	0,8474	0,889	0,8677
10	Model 4	0,926	0,8527	0,7424	0,7937	Model 22	0,9523	0,82	0,9691	0,8883
25	Model 4	0,9485	0,8407	0,9024	0,8705	Model 22	0,9457	0,8469	0,8822	0,8642
50	Model 4	0,949	0,8414	0,9044	0,8718	Model 22	0,9499	0,8248	0,9449	0,8808
10	Model 5	0,9499	0,8407	0,9116	0,8747	Model 23	0,9452	0,8054	0,9497	0,8716
25	Model 5	0,9484	0,8447	0,8955	0,8694	Model 23	0,9499	0,8246	0,9456	0,881
50	Model 5	0,9489	0,8414	0,9042	0,8716	Model 23	0,9455	0,8222	0,9206	0,8686
10	Model 6	0,9281	0,8709	0,7342	0,7967	Model 24	0,9457	0,8473	0,8815	0,8641
25	Model 6	0,9378	0,8525	0,817	0,8344	Model 24	0,9443	0,8532	0,8644	0,8588
50	Model 6	0,9495	0,8422	0,9067	0,8732	Model 24	0,9425	0,8258	0,8955	0,8592
10	Model 7	0,9256	0,8515	0,7414	0,7926	Model 25	0,9489	0,8053	0,9751	0,8821
25	Model 7	0,9499	0,8402	0,9123	0,8748	Model 25	0,9488	0,8376	0,9161	0,8751
50	Model 7	0,9485	0,843	0,8988	0,87	Model 25	0,9511	0,816	0,9689	0,8859
10	Model 8	0,9255	0,8539	0,7378	0,7916	Model 26	0,9438	0,849	0,8675	0,8581
25	Model 8	0,9268	0,8682	0,7291	0,7926	Model 26	0,9462	0,8481	0,8835	0,8655
50	Model 8	0,9488	0,8437	0,8996	0,8707	Model 26	0,9572	0,8306	0,9816	0,8998
10	Model 9	0,9555	0,8285	0,9688	0,8932	Model 27	0,9446	0,8047	0,9473	0,8702
25	Model 9	0,9478	0,842	0,8962	0,8683	Model 27	0,9496	0,8028	0,9843	0,8844
50	Model 9	0,9501	0,8029	0,9808	0,883	Model 27	0,9458	0,8026	0,9589	0,8738

10	Model 10	0,9432	0,7833	0,9729	0,8679	Model 28	0,945	0,8462	0,8788	0,8622
25	Model 10	0,9481	0,838	0,9042	0,8698	Model 28	0,9461	0,8439	0,8892	0,8659
50	Model 10	0,9549	0,8203	0,979	0,8927	Model 28	0,9549	0,8348	0,9597	0,8929
10	Model 11	0,9531	0,8348	0,9417	0,8851	Model 29	0,9339	0,8209	0,8478	0,8341
25	Model 11	0,9528	0,8117	0,9819	0,8887	Model 29	0,9501	0,8051	0,9832	0,8853
50	Model 11	0,954	0,817	0,9798	0,891	Model 29	0,927	0,746	0,9512	0,8362
10	Model 12	0,9489	0,8458	0,8973	0,8708	Model 30	0,9453	0,8494	0,876	0,8625
25	Model 12	0,9491	0,8448	0,8998	0,8714	Model 30	0,9459	0,7925	0,9806	0,8765
50	Model 12	0,9486	0,8457	0,8952	0,8698	Model 30	0,9473	0,8436	0,8971	0,8695
10	Model 13	0,9258	0,8517	0,7424	0,7933	Model 31	0,9521	0,815	0,9771	0,8887
25	Model 13	0,9485	0,843	0,8988	0,87	Model 31	0,9569	0,8312	0,9788	0,899
50	Model 13	0,9483	0,8434	0,8973	0,8695	Model 31	0,9495	0,8379	0,92	0,877
10	Model 14	0,9256	0,8523	0,7404	0,7924	Model 32	0,9467	0,842	0,8962	0,8683
25	Model 14	0,9403	0,8117	0,897	0,8523	Model 32	0,9485	0,8463	0,9005	0,8725
50	Model 14	0,9559	0,8287	0,9706	0,8941	Model 32	0,9565	0,8282	0,9815	0,8984
10	Model 15	0,9548	0,8318	0,9578	0,8904	Model 33	0,9104	0,7403	0,8362	0,7853
25	Model 15	0,9332	0,8044	0,861	0,8317	Model 33	0,9398	0,7815	0,9614	0,8622
50	Model 15	0,9331	0,8055	0,8584	0,8311	Model 33	0,9443	0,8014	0,9513	0,87
10	Model 16	0,9479	0,8421	0,8968	0,8686	Model 34	0,9482	0,8157	0,9503	0,8779
25	Model 16	0,9484	0,8399	0,9034	0,8705	Model 34	0,9486	0,8439	0,9051	0,8734
50	Model 16	0,9524	0,8116	0,9796	0,8877	Model 34	0,9238	0,8122	0,795	0,8035
10	Model 17	0,9498	0,8332	0,9231	0,8758	Model 35	0,9493	0,8017	0,985	0,884
25	Model 17	0,9554	0,8209	0,9819	0,8942	Model 35	0,947	0,7962	0,9807	0,8789
50	Model 17	0,957	0,8271	0,9806	0,8973	Model 35	0,9288	0,7486	0,9584	0,8406
10	Model 18	0,9505	0,8397	0,9172	0,8768	Model 36	0,9518	0,8314	0,9454	0,8848
25	Model 18	0,9513	0,8085	0,9775	0,885	Model 36	0,9488	0,799	0,9868	0,883
50	Model 18	0,951	0,8076	0,9773	0,8844	Model 36	0,9519	0,8313	0,9465	0,8852

CICDDoS2019 verisetinden elde edilen Dataset1 ve Dataset2 verisetlerine 2 ve 3 gizli katmanlı DNN modeli uygulanmış ve denenen her model için farklı sonuçlara ulaşılmıştır. Tablo 3.6'da yer alan sonuçlar yorumlandığında 10 epochta Model 14 mimarisine sahip olan DNN modelinin DDoS saldırılarının sınıflamasında %99,96 doğruluk ve %100 duyarlılık ile en başarılı sonuca ulaştığı görülmektedir. Tablo 3.7'de yer alan sonuçlar yorumlandığında ise 50 epochta Model 26 mimarisine sahip olan DNN modelinin DDoS saldırılarının tespitinde %95,72 doğruluk ile daha iyi sonuçlara ulaştığı gözlemlenmiştir. Saldırı tespiti için saldırı varlığını kaçırmamayı temsil eden duyarlılık oranının yüksek olması çok önemlidir. Bu yüzden, DNN modelinin yüksek duyarlılık oranına sahip olması, saldırı tespit sistemlerinde erken eylem için güvenilirliği temsil etmektedir. Bu yüzden DDoS saldırı tespiti ve sınıflandırması için ortak bir DNN modeli deneyler sonucu Tablo 3.8'de değerlendirilmektedir.

Tablo 3.8. Önerilen DNN modellerinden performansların karşılaştırması.

		Doğruluk				Duyarlılık			
Epoch	**Model**	**NSL-KDD**	**CICIDS2017**	**Dataset1**	**Dataset2**	**NSL-KDD**	**CICIDS2017**	**Dataset1**	**Dataset2**
25	Model 11	0,9946	0,9898	0,9996	0,9528	0,9988	0,9823	0,9998	0,9819
25	Model 36	0,9952	0,9934	0,9997	0,9488	0,9989	0,9887	0,9998	0,9868
50	Model 3	0,9937	0,9857	0,9996	0,9567	0,9981	1,0000	0,9997	0,9801
50	Model 27	0,9955	0,9992	0,9997	0,9458	0,9962	0,9992	0,9999	0,9589
10	Model 14	0,9727	0,9832	0,9996	0,9256	0,9524	0,9995	1,0000	0,7404
50	Model 26	0,9842	0,9842	0,9997	0,9572	0,9705	0,9996	0,9998	0,9816
	Ortalama	**0,9893**	**0,9893**	**0,9996**	**0,9478**	**0,9858**	**0,9949**	**0,9998**	**0,9383**

36 adet DNN modeliyle yapılan deneyler sonucunda her verisetinde farklı modelin daha başarılı olduğu gözlemlenmiştir. Her veriseti için en uygun olabilecek ortak bir modele karar vermek için Tablo 3.8'de verilen 6 modelin ortalamaları alınmış ve bu ortalamalara yakın olarak Model 27 ve Model 36 tespit edilmiştir. Fakat Dataset2 sınıflandırma için oluşturulan veriseti olduğundan bu veriseti için Duyarlılıktan ziyade Doğruluk değeri daha önemlidir. Bunun üzerine iki model arasında tekrar yapılan değerlendirme sonucunda Model 27'nin daha başarılı olduğuna karar verilmiştir.

Sonuç olarak kullanılan 3 farklı hazır DDoS verisetlerinde 3 katmanlı, 50 nöronlu, aktivasyon fonksiyonu tanh ve optimize edicisi adam olan DNN modelinin DDoS saldırılarınında en iyi tespit eden model olduğu sonucuna ulaşılmıştır.

Ayrıca CICDDoS2019 verisetinden alınan örneklem için elde ettiğimiz sonuçlar, derin öğrenme ve ağ trafiği analizinin küçük veritabanları kullanımında etkili bir başarı elde ettiğini göstermektedir. Toplanan ağ trafiği paketleri büyük olduğu için, önerilen DNN modelini küçük örnekler üzerinde uygulayarak daha kısa sürede hızlı ve doğru sonuçlar elde edilebilmektedir.

Hazır DDoS verisetleri ile olgunlaştırılan DNN modelinin başarısının geçerliliğini test etmek için model deneysel ortamda hazırlanan SWDDoS2020 verisetine de uygulanmıştır. Tablo 3.9'de SWDDoS2020 verisetinde DNN modelin test sonuçları verilmektedir.

Tablo 3.9. SWDDoS2020 verisetinde önerilen DNN modelinin değerlendirilmesi.

DDoS Saldırıları	**Doğruluk**	**Kesinlik**	**Duyarlılık**	**F1**
SYN Seli	1,00	1,00	1,00	1,00
UDP Seli	1,00	1,00	1,00	1,00

ICMP Seli	1,00	1,00	1,00	1,00

Tablo 3.9'deki sonuçlar incelendiğinde önerilen DNN modelinin DDoS tespitinde %100 güvenilir sonuçlar elde edebileceği gözlemlenmektedir. SWDDoS2020 veriseti deneysel ortamda oluşturulduğu için teorik olarak sonuçların iyi olması doğal olup pratikte gerçek bir ağ üzerinde incelenmesi gerekmektedir.

3.4. Diğer Çalışmalar ile Karşılaştırma

Deneyler sonucu olgunlaştırılan DNN modelinin başarısı verisetlerinde sınandıktan sonra literatürde aynı verisetleri üzerinde yapılan çalışmalarda kullanılan diğer sığ makine öğrenmesi ve derin öğrenme modellerinin doğruluk değerleriyle kıyaslanmıştır. Önerilen DNN modeli, doğruluk değeri bakımından diğer çalışmalarda kullanılan yöntemlerle Tablo 3.10'da karşılaştırılmıştır.

Tablo 3.10. Önerilen DNN modelinin diğer çalışmalarla karşılaştırılması.

Veriseti	Çalışma	Yıl	Yöntem	Doğruluk	Veriseti	Çalışma	Yıl	Yöntem	Doğruluk
NSL-KDD	[98]	2020	Autoencoder	98,60	CICIDS 2017	[81]	2018	RF	98,00
			NB	98,60		[6]	2018	ANN	99,00
	[86]	2019	DNN	80,1		[102]	2019	LSTM + CNN	97,16
	[99]	2019	Ensemble	99,1		[103]	2019	CNN	99,48
	[100]	2018	GBM	90,75		[86]	2019	DNN	96,3
			Distributed RF	93,26		[72]	2020	CNN	99,67
	[101]	2018	NB	98,0		[104]	2020	CNN	99,45
	Model 27	**2020**	**DNN**	**99,55**		**Model 27**	**2020**	**DNN**	**99,92**

Çalışmalarda yaygın olarak NSL-KDD ve CICIDS2017 versetleri kullanıldığı için diğer çalışmalar ile önerilen DNN modelinin karşılaştırılmasında bu verisetleri tercih edilmiştir. Tablo 3.10'daki sonuçlar incelendiğinde YSA tabanlı çalışmaların daha yüksek doğruluk değerlerine ulaştığı görülmektedir. Ayrıca önerilen Model 27'nin, NSL-KDD verisetinde %99,55 doğrulukla ve CICIDS2017 verisetinde %99,92 doğrulukla DDoS saldırılarının tespitinde diğer çalışmalarda kullanılan yöntemlerden daha etkili bir sonuca ulaşmaktadır. Sonuç olarak her iki veriseti için önerilen DNN modelinin yüksek doğrulukla, diğer sığ makine öğrenme algoritmalarından ve derin öğrenme modellerinden daha iyi sonuçlara sahip olduğu görülmektedir.

SONUÇLAR

Bu tez çalışmasında, ağ trafiği üzerindeki DDoS saldırılarının tespiti ve sınıflandırılmasında derin öğrenme modeli önerilmiştir. Literatürde yapılan çalışmalar incelendiğinde DDoS saldırı tespitinde derin öğrenme modellerinin makine öğrenimi algoritmalarından daha iyi sonuçlar elde ettiğini görülmüştür. Bu yüzden tez çalışmasında DDoS saldırılarının tespiti için derin öğrenme yaklaşımı benimsenmiş ve MLP tabanlı bir DNN modeli oluşturma amacıyla deneysel modeller hazırlanmıştır. 36 adet farklı mimarilerde hazırlanan DNN modelleri veri kümelerine ayrı ayrı uygulanmış ve elde edilen sonuçların değerlendirilmesi doğrultusunda 3 gizli katmanlı DNN modelinin DDoS saldırılarının tespitinde ve sınıflandırılmasında daha başarılı olduğu gözlemlenmiştir.

Hazır verisetleri ile test edilen modelin başarısı aynı verisetini kullanan diğer çalışmalarla karşılaştırılmıştır. Tablo 3.10'da yer alan sonuçlara göre önerilen DNN modeli, NSL-KDD veriseti için %99,55 ve CICIDS2017 veriseti için %99,92 doğruluk oranına sahip olmuş ve DDoS saldırılarını tespit etmede diğer sığ makine öğrenmesi ve derin öğrenme yöntemlerinden daha yüksek başarı göstermiştir. Aynı zamanda bu durum derin öğrenme modelinin hem özellik çıkarma hem de sınıflandırma yapısı sayesinde sığ makine öğrenme algoritmalarına göre performans ve doğruluk açısından bir avantaj sağladığını göstermektedir. Ek olarak, önerilen modelde uygun optimizasyon algoritması, aktivasyon fonksiyonu ve kayıp fonksiyonu seçiminin, diğer derin öğrenme modellerine kıyasla daha yüksek doğruluğa ulaşmada daha etkili olmuştur.

Önerilen DNN modeliyle CICDDoS2019 veriseti için DDoS saldırı tespitinde %99,97 doğruluk elde edilmiş ve neredeyse saldırı kaçırılmayarak %99,99 duyarlılığa ulaşılmıştır. DDoS saldırı tespitinden farklı olarak %94,58 doğruluk ile saldırı tiplerinin ayırt edilmesi ise saldırı tipi sınıflandırma işleminde önerilen DNN mimarisinin başarılı olduğunu göstermiştir. Önerilen modelin neredeyse kesin sonuçlar vermesi, IDS ve SDN gibi siber güvenlik alanında güvenilir bir araç olarak kullanılabileceğini göstermektedir. Önerilen modelin IDS ve SDN tabanlı ağ trafiğinin yönetildiği sistemlerde kullanılması, gelecekteki DDoS saldırılarının erken tespitine ve önlenmesine katkıda bulunacaktır.

Bunlara ek olarak önerilen DNN modelinin başarısının sınanması için deneysel ortamda düzenlenen DDoS saldırılarından elde edilen SWDDoS2020 adında bir veriseti

oluşturulmuştur. DDoS saldırı tespiti için kararlaştırılan DNN modelinin SWDDoS2020 verisetinde uygulanması sonucu elde edilen %100 doğruluk ile doğru bir model olduğunu göstermiştir. Veriseti hazırlama için oluşturulan deneysel ortam sayesinde aynı zamanda gelecek DDoS saldırılarının davranışlarının analiz edilmesi mümkün olabilecektir.

Ayrıca tez kapsamında önerilen MLP tabanlı DNN modelinin bir uygulaması olan [105]'deki makalede elde edilen sonuçlar, DDoS saldırılarının %99,97 oranında doğru tespit edildiğini göstermiştir. Böylece önerilen modelin DDoS saldırı tespitinde etkili olduğu görülmektedir.

Önerilen DDoS modelinin Saldırı Tespit Sistemlerine (IDS) entegre edilmesiyle gerçek zamanlı olarak ağda test edilmesi hedeflenmektedir. Böylelikle gerçek ağ trafiğinde DDoS saldırı verileri ile eğitilen modelin başarısının test edilmesi mümkün olacaktır. Bununla beraber yeni nesil DDoS saldırılara karşı modelini güncelleyerek kendi kendine öğrenen bir mimari oluşturulması gelecek çalışma olarak hedeflenmektedir.

KAYNAKLAR

[1] CISCO, What Are the Most Common Cyber Attacks?, https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html (Erişim Tarihi: 10 Ekim 2020)

[2] Winder, D. (2019) Recording Data for Cyberdefence. Cybersecurity, 0570, 1-12, https://raconteur.uberflip.com/i/1084979-cybersecurity-2019/9?m4= (Erişim Tarihi: 10 Ekim 2020)

[3] Spamhaus (2020) Spamhaus Botnet Threat Update Q2 2020 Report, https://www.spamhaus.org/news/images/botnet-report-2020-q2/2020-q2-spamhaus-botnet-threat-report.pdf (Erişim Tarihi: 11 Ekim 2020)

[4] Nexusguard (2020) DDoS Threat Q1 2020 Report, https://blog.nexusguard.com/threat-report/ddos-threat-report-2020-q1

[5] Khuphiran P., Leelaprute P., Uthayopas P., Ichikawa K. and Watanakeesuntorn W. (2018). Performance Comparison of Machine Learning Models for DDoS Attacks Detection. 2018 22nd International Computer Science and Engineering Conference (ICSEC), 21-24 November 2018, Chiang Mai, Thailand, 1-4.

[6] Ali O. and Cotae P. (2018). Towards DoS/DDoS Attack Detection Using Artificial Neural Networks. 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 8-10 November, New York City, NY, USA, 229-234.

[7] Deepa V., Sudar K. M. and Deepalakshmi P. (2018). Detection of DDoS Attack on SDN Control plane using Hybrid Machine Learning Techniques. 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT), 13-14 December 2018, Tirunelveli, India, 299-303.

[8] STM (2019) 2019 Ocak-Mart Dönemi Siber Tehdit Durum Raporu, https://thinktech.stm.com.tr/uploads/raporlar/pdf/2942019145655920_stm_siber_tehdit_durum_raporu_ocak_mart_2019.pdf (Erişim Tarihi: 12 Ekim 2020)

[9] STM (2017) 2017 Ocak-Mart Dönemi Türkiye Siber Tehdit Durum Raporu, https://thinktech.stm.com.tr/uploads/raporlar/pdf/288201811541572_sibertehditdurumraporuocak_mart2017.pdf (Erişim Tarihi: 12 Ekim 2020)

[10] STM (2019) 2019 Ekim-Aralık Dönemi Siber Tehdit Durum Raporu, https://thinktech.stm.com.tr/uploads/raporlar/pdf/2312020175942772_stm_siber_tehdit_durum_raporu_ekim_aralik_2019.pdf (Erişim Tarihi: 13 Ekim 2020)

[11] Akamai (2016) Akamai's [state of the internet] / Security Q4 2016 Report, https://www.akamai.com/uk/en/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-security-report.pdf (Erişim Tarihi: 14 Ekim 2020)

[12] STM (2017) 2017 Temmuz-Eylül Dönemi Siber Tehdit Durum Raporu, https://thinktech.stm.com.tr/uploads/raporlar/pdf/2882018113556699_siber_tehdit_durum_raporu_temmuz_eylul_2017.pdf (Erişim Tarihi: 15 Ekim 2020)

[13] Akamai (2017) [state of the internet] / security Q2 2017 Report, https://www.akamai.com/de/de/multimedia/documents/state-of-the-internet/q2-2017-state-of-the-internet-security-report.pdf (Erişim Tarihi: 15 Ekim 2020)

[14] Akamai (2018) Memcached-fueled 1.3 Tbps Attacks. The Akamai Blog (2018), https://blogs.akamai.com/2018/03/memcached-fueled-13-tbps-attacks.html (Erişim Tarihi: 16 Ekim 2020)

[15] Kumar, M. (2018) Biggest-Ever DDoS Attack (1.35 Tbs) Hits Github Website. The Hacker News (2018), https://thehackernews.com/2018/03/biggest-ddos-attack-github.html (Erişim Tarihi: 16 Ekim 2020)

[16] Morales, C. (2018) NETSCOUT Arbor Confirms 1.7 Tbps DDoS Attack; The Terabit Attack Era Is Upon Us. NETSCOUT's ATLAS Security Engineering & Response Team (ASERT) Blogs (2018), https://www.arbornetworks.com/blog/asert/netscout-arbor-confirms-1-7-tbps-ddos-attack-terabit-attack-era-upon-us/ (Erişim Tarihi: 17 Ekim 2020)

[17] Hering, O., LaSeur, L, Katz, O., Calhoon, S., Poulos and B., Towne, R. (2020) Financial Services-Hostile Takeover Attempts. [State of the Internet] / Security, 6(1), https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-financial-services-hostile-takeover-attempts-report-2020.pdf (Erişim Tarihi: 27 Ekim 2020)

[18] Wang, B., Zheng, Y., Lou, W. and Hou, Y. T. (2014). DDoS Attack Protection in the Era of Cloud Computing and Software-Defined Networking. 2014 IEEE 22nd International Conference on Network Protocols, 21-24 October 2014, Raleigh, NC, 624-629.

[19] Yan, Q. and Yu, F. R. (2015). Distributed denial of service attacks in software-defined networking with cloud computing. IEEE Communications Magazine, 53(4), 52-59.

[20] Prakash, A., and Priyadarshini, R. (2018). An Intelligent Software defined Network Controller for preventing Distributed Denial of Service Attack. 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), 20-21 April 2018, Coimbatore, 585-589.

[21] Li, J., Liu, M., Xue, Z., Fan, X. and He, X. (2020). RTVD: A Real-Time Volumetric Detection Scheme for DDoS in the Internet of Things. IEEE Access, 8, 36191-36201.

[22] Imperva, DNS Flood, https://www.imperva.com/learn/ddos/dns-flood/#:~:text=DNS%20flood%20attacks%20should%20be,of%20much%20larger%20DNS%20responses.&text=DNS%20floods%20are%20symmetrical%20DDoS%20attacks (Erişim Tarihi: 22 Ekim 2020)

[23] Sieklik, B., Macfarlane, R., Buchanan, W.J. (2016). Evaluation of TFTP DDoS amplification attack. Computers & Security, 57, 67-92.

[24] Balaban, D. (2020). Are you Ready for These 26 Different Types of DDoS Attacks?. Security (2020), https://www.securitymagazine.com/articles/92327-

are-you-ready-for-these-26-different-types-of-ddos-attacks (Erişim Tarihi: 22 Ekim 2020)

[25] Imperva, TCP SYN Flood, https://www.imperva.com/learn/application-security/syn-flood/ (Erişim Tarihi: 22 Ekim 2020)

[26] Poremba, S.M. (2017). Types of DDoS Attacks. eSecurity Planet (2017), https://www.esecurityplanet.com/network-security/types-of-ddos-attacks.html (Erişim Tarihi: 23 Ekim 2020)

[27] Haddadi, M. and Beghdad, R. (2018). DoS-DDoS: Taxonomies Of Attacks, Countermeasures, And Well-Known Defense Mechanisms In Cloud Environment. The EDP Audit, Control, and Security Newsletter (EDPACS), 57(5), 1-26.

[28] Chang, R. K. (2002). Defending against flooding-based distributed denial-of-service attacks: A tutorial. IEEE Communications Magazine, 40(10), 42–51.

[29] Imperva, UDP Flood, https://www.imperva.com/learn/application-security/udp-flood/ (Erişim Tarihi: 22 Ekim 2020)

[30] Javapipe, 35 Types of DDoS Attacks Explained, https://javapipe.com/blog/ddos-types/#udp-flood (Erişim Tarihi: 21 Ekim 2020)

[31] McAfee (2013) McAfee Network Security Platform 9.2.x Product Guide, https://docs.mcafee.com/bundle/network-security-platform-9.2.x-product-guide/page/GUID-1020A9BF-580B-4E66-8A90-59F28AFBAEA2.html (Erişim Tarihi: 23 Ekim 2020)

[32] Nazario, J. (2008). DDoS attack evolution. Network Security, 2008(7), 7–10.

[33] Cambiaso, E., Papaleo, G., Chiola, G., and Aiello, M. (2013). Slow DoS attacks: Definition and categorisation. International Journal of Trust Management in Computing and Communications, 1(3–4), 300–319.

[34] Li, J., Liu, Y., and Gu, L. (2010). DDoS attack detection based on neural network. 2010 2nd International Symposium on Aware Computing, 1-4 November 2010, Tainan, 196-199.

[35] Bora, G., Bora, S., Singh, S. and Sheikh, M. (2014). OSI Reference Model: An Overview. International Journal of Computer Trends and Technology, 7(4), 214-218.

[36] Peng, T., Leckie, C., and Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys (CSUR), 39(1), 3.

[37] İTÜ BİDB, HTTP & HTTPS. Seyir Defteri (2013), https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/06/http-https (Erişim Tarihi: 10 Ekim 2020)

[38] Kızılçınar, S. (2020). NTP Amplification Attack Nedir?. CyberMag (2020), https://www.cybermagonline.com/ntp-amplification-attack-nedir (Erişim Tarihi: 1 Ekim 2020)

[39] Mason, A.G. and Newcomb, M.J. (2001). Cisco Secure Internet Security Solutions, 1st Edition, Cisco Press, Inc., 201 West 103rd Street, Indianapolis, USA.

http://armstrong.craig.free.fr/eBooks/Cisco/Cisco%20Press%20Cisco%20Secure%20Internet%20Security%20Solutions.pdf (Erişim Tarihi: 14 Ekim 2020)

[40] Banach, Z. (2020). What is LDAP Injection and How to Prevent It. Web Security Blog (2020), https://www.netsparker.com/blog/web-security/ldap-injection-how-to-prevent/ (Erişim Tarihi: 14 Ekim 2020)

[41] Cloudflare, SSDP DDoS Attack. Learning Center, https://www.cloudflare.com/learning/ddos/ssdp-ddos-attack/ (Erişim Tarihi: 5 Ekim 2020)

[42] Cloudflare, DNS Amplification Attack. Learning Center, https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/ (Erişim Tarihi: 5 Ekim 2020)

[43] Postel J. (1983). Character Generator Protocol, IETF RFC 864.

[44] Meghanathan, N. (2014). A Tutorial on Network Security: Attacks and Controls. 1. 10.4018/978-1-4666-4789-3.ch011.

[45] Sollins K.R. (1981). The TFTP Protocol (Revision 1). Internet Standard RFC 783 (1981), https://tools.ietf.org/html/rfc783 (Erişim Tarihi: 4 Ekim 2020)

[46] Sollins K.R. (1992). The TFTP Protocol (Revision 2). Internet Standard RFC 1350 (1992), https://tools.ietf.org/html/rfc1350 (Erişim Tarihi: 4 Ekim 2020)

[47] Marchette, D. J. (2001). Computer intrusion detection and network monitoring: A statistical viewpoint. Springer Science & Business Media.

[48] Anderson J.P. (1980). Computer Security Threat Monitoring and Surveillance. Technical report, Fort Washington, PA, 1980.

[49] Hoque, M.S., Mukit, A. and Bikas, A.N. (2012). An Implementation of intrusion detection system using genetic algorithm. International Journal of Network Security and Its Applications (IJNSA), 4(2), 109-120.

[50] Lin, Y., Zhang, Y. and Ou, Y., (2010). The Design and Implementation of Host-Based Intrusion Detection System. 2010 Third International Symposium on Intelligent Information Technology and Security Informatics, 2-4 April 2010, Jinggangshan, 595-598.

[51] Salim, R. and Rao, G.S.V.R.K. (2006). Design and Development of Network Intrusion Detection System Detection Scheme on Network Processing Unit. 2006 8th International Conference Advanced Communication Technology, 20-22 February 2006 Phoenix Park, 1023-1025.

[52] Asif, M. K., Khan, T. A., Taj, T. A., Naeem, U. and Yakoob, S. (2013). Network Intrusion Detection and its strategic importance. 2013 IEEE Business Engineering and Industrial Applications Colloquium (BEIAC), 7-9 April 2013, Langkawi, 140-144.

[53] Hu, J. (2010). Host-Based Anomaly Intrusion Detection. In: Stavroulakis P., Stamp M. (eds) Handbook of Information and Communication Security, Springer, Berlin, Heidelberg, 235-255.

[54] Hochberg, J., Jackson, K., Stallings, C., McClary, J. F., DuBois, D. and Ford, J. (1993). NADIR: An automated system for detecting network intrusion and misuse. Computers & Security, 12(3), 235-248, 1993.

[55] Kashif, M. and Zahoor-ul-haq (2015). An Optimal Use of Intrusion Detection and Prevention System (IDPS). 2015 European Intelligence and Security Informatics Conference, 7-9 September 2015, Manchester.

[56] Mudzingwa D. and Agrawal R. (2012). A study of methodologies used in intrusion detection and prevention systems (IDPS). 2012 Proceedings of IEEE Southeastcon, 15-18 March 2012, Orlando, FL, 1-6.

[57] Poongodi M. and Bose S. (2013). Design of Intrusion Detection and Prevention System (IDPS) using DGSOTFC in collaborative protection networks. 2013 Fifth International Conference on Advanced Computing (ICoAC), 18-20 December 2013, Chennai, 172-178.

[58] White, G., Fisch, E. and Pooch. U. (1994). Cooperating security managers: A peer-based intrusion detection system. IEEE Network, 10(1), 20-23.

[59] Jiang, H., Yang, Y., Guan, H., Xie, G. and Salamatian, K. (2019). A Massively Multi-Tenant Virtualized Network Intrusion Prevention Service on NFV Platform. 2019 28th International Conference on Computer Communication and Networks (ICCCN), 29 July-1 August 2019, Valencia, Spain, 1-9.

[60] Yildiz, K., Buldu, A., and Saritas, H. (2016). Elliptic curve coding technique application for digital signature. Security Communication Networks, 9(17), 4242-4254.

[61] Labbe, Rowe and Fulp (2006). A Methodology for Evaluation of Host-Based Intrusion Prevention Systems and Its Application. 2006 IEEE Information Assurance Workshop, 21-23 June 2006, West Point, NY, 378-379.

[62] BO, J., Jiajun, L., Xingyu, W. (2000). Intrusion Detection Technology Review East China University of Technology. 26(2), 191-197.

[63] Amiri, F., Yousefi, M.R., Lucas, C., Shakery, A. and Yazdani, N. (2011). Mutual information-based feature selection for intrusion detection systems. Journal of Network and Computer Applications, 34(4), 1184-1199.

[64] Ganeshkumar, P. and Pandeeswari, N. (2016). Adaptive neuro-fuzzy-based anomaly detection system in cloud. International Journal of Fuzzy Systems, 18(3), 367-378.

[65] Ohtahara, S., Kamiyama, T. and Oyama, Y. (2009). Anomaly-based Intrusion Detection System Sharing Normal Behavior Databases among Different Machines. Proceedings of Ninth IEEE International Conference on Computer and Information Technology, 11-14 Oct. 2009, Xiamen.

[66] Patil, S., Rane, P. and Meshram, B. B. (2012). IDS vs IPS. International Journal of Computer Networks and Wireless Communications, 2(1).

[67] Scarfone, K. and Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems(IDPS), NIST Publication.

[68] Rao, U.H. and Nayak, U. (2014). The Infosec Handbook, 1st Edition., Apress, 125-243.

[69] Gupta, V., Singh, M. and Bhalla, V.K. (2014). Pattern matching algorithms for intrusion detection and prevention system: A comparative analysis. 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 24-27 September 2014, New Delhi, 50-54.

[70] Vaidya, N. and Godbole, P. (2015). Hardware Implementation of Key Functionalities of NIPS for High Speed Network. 2015 International Conference on Computing and Network Communications (CoCoNet), 16-19 December 2015, Trivandrum.

[71] Koch, R., Golling, M. and Rodosek, G. D. (2014). Behavior-based intrusion detection in encrypted environments. IEEE Communications Magazine, 52(7), 124-131.

[72] Doriguzzi-Corin, R., Millar, S., Scott-Hayward, S., Martínez-del-Rincón, J., and Siracusa, D. (2020). Lucid: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection. IEEE Transactions on Network and Service Management, 17(2), 876-889.

[73] Srinivas, T.A.S., and Manivannan, S.S. (2020). Prevention of hello flood attack in IoT using combination of deep learning with improved rider optimization algorithm. Computer Communications, 163, 162-175.

[74] Ujjan, R.M.A., Pervez, Z., Dahal, K., Bashir, A.K., Mumtaz, R., and González, J. (2019). Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN. Future Generation Computer Systems, 111, 763-779.

[75] Priyadarshini, R., and Barik, R. (2019). A deep learning based intelligent framework to mitigate DDoS attack in fog environment. Journal of King Saud University - Computer and Information Sciences, 1319-1578.

[76] Hasan, Md.Z., Hasan, K.M.Z., and Sattar, A. (2018). Burst Header Packet Flood Detection in Optical Burst Switching Network Using Deep Learning Model. Procedia Computer Science, 143, 970-977.

[77] Krishnan, P., Duttagupta, S., and Achuthan, K. (2019). VARMAN: Multi-plane security framework for software defined networks. Computer Communications, 148, 215-239

[78] Zhu, M., Ye, K., and Xu, CZ. (2018). Network Anomaly Detection and Identification Based on Deep Learning Methods. In: Luo M., Zhang LJ. (eds) Cloud Computing – CLOUD 2018. CLOUD 2018. Lecture Notes in Computer Science, 10967. Springer, Cham

[79] Alzahrani, S., and Hong, L. (2018). Detection of Distributed Denial of Service (DDoS) Attacks Using Artificial Intelligence on Cloud. 2018 IEEE World Congress on Services (SERVICES), 2-7 July 2018, San Francisco, CA, 35-36.

[80] Tavallaee, M, Bagheri, E., Lu, W., and Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, 8-10 July 2009, Ottawa, ON.

[81] Sharafaldin I., Lashkari A.H., and Ghorbani A.A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. 4th International Conference on Information Systems Security and Privacy (ICISSP), January 2018, Portugal.

[82] Lashkari A.H. (2020). CICFlowMeter. GitHub, https://github.com/ISCX/CICFlowMeter (Erişim Tarihi: 08 Kasım 2020)

[83] Biondi, P., Scapy, https://scapy.net/ (Erişim Tarihi: 07 Kasım 2020)

[84] Combs, G. (1997), Wireshark Project, https://www.wireshark.org/ (Erişim Tarihi: 07 Kasım 2020)

[85] Öztemel, E. (2016). Yapay sinir ağları, 4. Baskı, Papatya Yayıncılık Eğitim, İstanbul, Türkiye.

[86] Vinayakumar, R., Alazab, M., Soman, K.P., Poornachandran, P., Al-Nemrat, A., and Venkatraman, S. (2019). Deep Learning Approach for Intelligent Intrusion Detection System. IEEE Access, 7, 41525-41550.

[87] Gupta, N. (2013). Artificial Neural Network. Network and Complex Systems, 3(1), 24-28.

[88] Liu, H., and Lang, B. (2019). Machine Learning and Deep Learning Methods for Intrusion Detection System:A Survey. Applied Sciences, 9(20), 4396.

[89] Aşkın, D , İskender, İ , Mamızadeh, A . (2013). Farklı Yapay Sinir Ağları Yöntemlerini Kullanarak Kuru Tip Transformatör Sargısının Termal Analizi. Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 26 (4), 905-913.

[90] Goodfellow, I., Bengio, Y. and Courville, A. (2016). Deep Learning, 1st Edition., MIT Press, Cambridge, Massachusetts, USA.

[91] Murphy, K., (2012). Machine Learning: A Probabilistic Perspective, 1st Edition., MIT Press, Cambridge, Massachusetts, USA.

[92] Kingma, D.P., and Ba, J. (2015). Adam: A Method for Stochastic Optimization. 3rd International Conference for Learning Representations, 7-9 May 2015, San Diego.

[93] Raybaut, P. (2009). Spyder IDE, https://www.spyder-ide.org/ (Erişim Tarihi: 07 Ocak 2020)

[94] The Google Brain team (2015). TensorFlow, https://www.tensorflow.org/ (Erişim Tarihi: 07 Ocak 2020)

[95] Chollet, F. (2015). Keras, https://keras.io/ (Erişim Tarihi: 07 Ocak 2020)

[96] McKinney, W. (2009). Pandas, https://pandas.pydata.org/ (Erişim Tarihi: 07 Ocak 2020)

[97] Fawcett, T. (2006). An introduction to ROC analysis, Pattern Recognition Letters, 27(8), 861-874.

[98] Rashid, A., Siddique, M.J., and Ahmed, S.M. (2020). Machine and Deep Learning Based Comparative Analysis Using Hybrid Approaches for Intrusion

Detection System. 2020 3rd International Conference on Advancements in Computational Sciences (ICACS), February 2020, Lahore, Pakistan.

[99] Das, S., Mahfouz, A. M., Venugopal, D., and Shiva, S. (2019). DDoS Intrusion Detection Through Machine Learning Ensemble. 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C), 22-26 July 2019, Sofia, Bulgaria.

[100] Hoon, K. S., Yeo, K. C., Azam, S., Shunmugam, B., and De Boer, F. (2018). Critical review of machine learning approaches to apply big data analytics in DDoS forensics. 2018 International Conference on Computer Communication and Informatics (ICCCI), 4-6 January, 2018, Coimbatore.

[101] Mohammed, S. S. et al. (2018). A New Machine Learning-based Collaborative DDoS Mitigation Mechanism in Software-Defined Network. 2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 15-17 October 2018, Limassol, 1-8.

[102] Roopak, M., Tian, G.Y. and Chambers, J. (2019). Deep Learning Models for Cyber Security in IoT Networks. 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 7-9 January 2019, Las Vegas, NV, USA.

[103] Haider, S., Akhunzada, A., Ahmed, G., and Raza, M. (2019). Deep Learning based Ensemble Convolutional Neural Network Solution for Distributed Denial of Service Detection in SDNs. 2019 UK/ China Emerging Technologies (UCET), 21-22 August 2019, Glasgow, United Kingdom.

[104] Haider, S. et al., (2020). A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks. IEEE Access, 8, 53972-53983.

[105] Cil A. E., Yildiz K. and Buldu A. (2021). Detection of DDoS attacks with feed forward based deep neural network model. Expert Systems with Applications, 169, 114520.

ÖZGEÇMİŞ

Adı Soyadı **:** Abdullah Emir ÇİL

Öğrenim Durumu

Derece	**Bölüm/Program**	**Üniversite/Lise**	**Mezuniyet Yılı**
Lise	Anadolu Lisesi	Gelenbevi Anadolu Lisesi	Haziran 2010
Lisans	Matematik Mühendisliği	İstanbul Teknik Üniversitesi	Şubat 2017

İş Deneyimi

Yıl	**Firma/Kurum**	**Görevi**
2017	Ziraat Teknoloji A.Ş.	İş Analisti
2018	Bankacılık Düzenleme ve Denetleme Kurumu	Bankacılık Uzman Yrd.

Bilimsel Eserler:

1. Cil A. E. ve Aydın, M. (2019). Kurum İçi Uygulamaların EBYS ile Entegrasyonunda Yapay Zekânın Önemi Üzerine Bir İnceleme. Bilgi Yönetimi ve Bilgi Güvenliği, 5, 197-209.
2. Cil A. E., Yildiz K. and Buldu A. (2021). Detection of DDoS attacks with feed forward based deep neural network model. Expert Systems with Applications, 169, 114520.