



MARMARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ



MAKİNE ÖĞRENMESİ ALGORİTMALARI İLE DDOS SALDIRI TESPİTİ VE SINIFLANDIRMASI

FURKAN SERDAROĞLU

YÜKSEK LİSANS TEZİ

Siber Güvenlik Anabilim Dalı

Bilgi Güvenliği Mühendisliği Programı

DANIŞMAN

Dr. Hüseyin YÜCE

İSTANBUL, 2021

TEŞEKKÜR

Tezi hazırlamamda bana yardımcı olan danışmanım Dr. Hüseyin YÜCE'ye ve bu süreçte bana destek olan babam Ali İhsan SERDAROĞLU'na ve annem Meral SERDAROĞLU'na teşekkür ederim.

Mart 2021

Furkan SERDAROĞLU



İÇİNDEKİLER

	SAYFA
TEŞEKKÜR	i
İÇİNDEKİLER	iii
ÖZET	v
ABSTRACT	vi
SEMBOLLER	vii
KISALTMALAR	viii
ŞEKİL LİSTESİ	ix
TABLO LİSTESİ	x
1. GİRİŞ	1
1.1. DDoS Saldırıları	2
1.1.1. DDoS Saldırı Çeşitleri	6
1.1.1.1. NTP DDoS	6
1.1.1.2. MSSQL DDoS	6
1.1.1.3. DNS DDoS	7
1.1.1.4. SNMP DDoS	7
1.1.1.5. UDP DDoS	8
1.1.1.6. LDAP DDoS	8
1.2 Saldırı Tespit Sistemleri	8
1.2.1 Veriyi toplama şekline göre saldırı tespit sistemleri	10
1.2.1.1 Ağ tabanlı saldırı tespit sistemleri	10
1.2.1.2 Ana bilgisayar tabanlı saldırı tespit sistemleri	11
1.2.2 Veriyi analiz şekline göre saldırı tespit sistemleri	11
1.2.2.1 İmza tabanlı saldırı tespit sistemi	11
1.2.2.2 Anomali tabanlı saldırı tespit sistemi	12
1.3 Benzer Çalışmalar	14
2. MATERYAL ve YÖNTEM	16
2.1 Çalışmada Kullanılan Veriler	16
2.2 Model Değerlendirme Yöntemleri ve Metrikleri	19
2.2.1 Karmaşıklık matrisi	19

2.2.2 Kesinlik metriği	19
2.2.3 Hatırlama metriği	19
2.2.4 F1 Skor metriği	19
2.2.5 Doğruluk metriği	20
2.2.6 Çapraz doğrulama metodu	20
2.3 Model Eğitimi İçin Özniteliklerin Belirlenmesi	20
2.3.1 Normal trafik tespiti için en önemli 10 öznitelik	21
2.3.2 NTP DDoS saldırı tespiti için en önemli 10 öznitelik	21
2.3.3 MSSQL DDoS saldırı tespiti için en önemli 10 öznitelik	22
2.3.4 SNMP DDoS saldırı tespiti için en önemli 10 öznitelik	23
2.3.5 UDP DDoS saldırı tespiti için en önemli 10 öznitelik	24
2.3.6 DNS DDoS saldırı tespiti için en önemli 10 öznitelik	24
2.3.7 Tüm veri türlerinin tespiti için en önemli 20 öznitelik	25
2.3.8 Model eğitiminde kullanılan öznitelikler	26
2.4 Sınıflandırıcıların Çapraz Doğrulama Metodu ile Testi	27
2.5 Modellerin Eğitilmesi ve Test Edilmesi	30
2.5.1 Modellerin eğitilmesi ve 1. testi	30
2.5.1.1 Random Forest algoritması ile model eğitimi ve eğitilen modelin 1. testi	31
2.5.1.2 Decision Tree algoritması ile model eğitimi ve eğitilen modelin 1. testi	34
2.5.1.3 Gaussian Naive Bayes algoritması ile model eğitimi ve eğitilen modelin 1. testi	36
2.5.1.4 Extra Trees algoritması ile model eğitimi ve eğitilen modelin 1. testi	38
2.5.1.5 AdaBoost algoritması ile model eğitimi ve eğitilen modelin 1. testi	40
2.5.1.6 Gradient Boosting algoritması ile model eğitimi ve eğitilen modelin 1. testi	43
2.5.2 Modellerin 2. testi	45
2.5.2.1 Random Forest algoritması ile eğitilen modelin 2. testi	45
2.5.2.2 Decision Tree algoritması ile eğitilen modelin 2. testi	47

2.5.2.3 Gaussian Naive Bayes algoritması ile eğitilen modelin 2. testi	49
2.5.2.4 Extra Trees algoritması ile eğitilen modelin 2. testi	51
2.5.2.5 AdaBoost algoritması ile eğitilen modelin 2. testi	53
2.5.2.6 Gradient Boosting algoritması ile eğitilen modelin 2. testi	55
2.5.3 Modellerin LDAP DDoS saldırısı ile testi	57
2.5.3.1 Random Forest algoritması ile eğitilen modelin LDAP DDoS saldırısını sınıflandırması	58
2.5.3.2 Decision Tree algoritması ile eğitilen modelin LDAP DDoS saldırısını sınıflandırması	58
2.5.3.3 Gaussian Naive Bayes algoritması ile eğitilen modelin LDAP DDoS saldırısını sınıflandırması	59
2.5.3.4 Extra Trees algoritması ile eğitilen modelin LDAP DDoS saldırısını sınıflandırması	60
2.5.3.5 AdaBoost algoritması ile eğitilen modelin LDAP DDoS saldırısını sınıflandırması	61
2.5.3.6 Gradient Boosting algoritması ile eğitilen modelin LDAP DDoS saldırısını sınıflandırması	62
3. BULGULAR ve TARTIŞMA	63
3.1 Modellere Yapılan 1. Testin Değerlendirmesi	63
3.2 Modellere Yapılan 2. Testin Değerlendirmesi	64
3.3 Modellere Yapılan LDAP DDoS Saldırı Testi Değerlendirmesi	65
3.4 Çalışma Sonuçlarının Benzer Çalışma Sonuçlarıyla Karşılaştırılması	65
4. SONUÇLAR	67
KAYNAKLAR	68
EKLER	73

ÖZET

MAKİNE ÖĞRENMESİ ALGORİTMALARI İLE DDoS SALDIRI TESPİTİ VE SINIFLANDIRMASI

DDoS saldırıları, kurum ve kuruluşları tehdit eden önemli siber saldırılardan biridir. Saldırı sonucu oluşabilecek zararı azaltmak için saldırının hızlı bir şekilde tespit edilip gerekli aksiyon alınarak engellenmesi gerekmektedir. Saldırının hızlı bir şekilde tespiti ve gerekli personelin saldırı konusunda bilgilendirilmesi için saldırı tespit sistemi kullanılmaktadır. Bu çalışmada, makine öğrenmesi algoritmaları kullanılarak normal trafik verisi, NTP DDoS trafik verisi, MSSQL DDoS trafik verisi, DNS DDoS trafik verisi, SNMP DDoS trafik verisi ve UDP DDoS trafik verisi türlerinin tespiti ve bu veri türlerinin sınıflandırması gerçekleştirilmiştir. Bunun yanı sıra makine öğrenmesi algoritmaları kullanılarak eğitilen modeller, model eğitim aşamasında kullanılmayan LDAP DDoS trafik verisi ile test edilmiş ve modellerin eğitim aşamasında görmediği saldırı türünü sınıflandırma becerisi sınanmıştır. Modellerin eğitim ve test işlemlerinde güncel trafik verileri içeren CIC-DDoS2019 ve CSE-CIC-IDS2018 veri setlerindeki veriler kullanılmıştır. Her bir veri türünün tespiti için önemli öznitelikler bulunmuş ve modellerin eğitimi için kullanılmak üzere öznitelik seçimleri yapılmıştır. Çalışmada kullanılan sınıflandırıcıların çapraz doğrulama metodu ile testi gerçekleştirilmiştir. Modelleri eğitmek için Random Forest, Decision Tree, Gaussian Naive Bayes, Extra Trees, AdaBoost ve Gradient Boosting algoritmaları kullanılmıştır. Eğitilen modeller testlerden geçirilmiş ve doğruluk, kesinlik, hatırlama ve F1 skor performans metrikleriyle değerlendirilmiştir. Çalışmadaki testler sonucunda makine öğrenmesi algoritmalarının DDoS saldırı tespiti ve sınıflandırmasında başarılı olduğu görülmüştür.

ABSTRACT

DDOS ATTACK DETECTION AND CLASSIFICATION BY MACHINE LEARNING ALGORITHMS

DDoS attacks are one of the important cyber attacks threatening institutions and organizations. In order to reduce the damage that may occur as a result of the attack, the attack must be detected quickly and prevented by taking the necessary action. Intrusion detection systems are used to quickly detect the attack and inform the necessary personnel about the attack. In this study, using machine learning algorithms, normal traffic data, NTP DDoS traffic data, MSSQL DDoS traffic data, DNS DDoS traffic data, SNMP DDoS traffic data and UDP DDoS traffic data types were determined and classification of these data types were performed. Besides, models trained with machine learning algorithms were tested with LDAP DDoS traffic data that was not used in the model training phase, and the ability to classify the type of attack that the models did not see during the training phase was tested. The data from the CIC-DDoS2019 and CSE-CICIDS2018 data sets, which contain up-to-date traffic data, were used in the training and testing of the models. Important features were found for determining each data type and feature selections were made to be used for training models. The classifiers used in the study were tested with the cross validation method. Random Forest, Decision Tree, Gaussian Naive Bayes, Extra Trees, AdaBoost and Gradient Boosting algorithms were used to train the models. Trained models were tested and evaluated with accuracy, precision, recall and F1 score performance metrics. As a result of the tests in the study, it was seen that machine learning algorithms were successful in DDoS attack detection and classification.

SEMBOLER



KISALTMALAR

ACK: Acknowledgement

DDoS: Distributed Denial of Service

DN: Doğru Negatif

DNS: Domain Name System

DoS: Denial of Service

DP: Doğru Pozitif

HTTP: Hyper-Text Transfer Protocol

ID3: Iterative Dichotomiser 3

LDAP: Lightweight Directory Access Protocol

MSSQL: Microsoft Structured Query Language

NetBIOS: Network Basic Input/Output System

NTP: Network Time 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

VPN: Virtual Private Network

YN: Yanlış Negatif

YP: Yanlış Pozitif

ŞEKİL LİSTESİ

- Şekil 1.1** Atak türlerine göre saldırı oranları
- Şekil 1.2** Aylara göre DDoS saldırı sayısı
- Şekil 1.3** Aylara göre DDoS saldırı trafik büyüklüğü
- Şekil 1.4** Saldırı türlerine göre DDoS atak trafik büyüklüğü ve atak sayısı oranları
- Şekil 1.5** DDoS saldırısı gerçekleştiren ülkeler haritası
- Şekil 1.6** DDoS saldırısına uğrayan ülkeler haritası
- Şekil 1.7** NTP DDoS saldırı görseli
- Şekil 1.8** DNS DDoS saldırı görseli
- Şekil 1.9** Ağ üzerinde switch cihazına bağlı saldırı tespit sistemi
- Şekil 1.10** İç ağ ile dış ağ arasındaki bağlantıya bağlı saldırı tespit sistemi
- Şekil 1.11** Dış ağ ile iç ağ arasına direkt yerleştirilen saldırı tespit sistemi
- Şekil 2.1** Random Forest algoritması ile eğitilen modelin karmaşıklık matrisi
- Şekil 2.2** Decision Tree algoritması ile eğitilen modelin karmaşıklık matrisi
- Şekil 2.3** Gaussian Naive Bayes algoritması ile eğitilen modelin karmaşıklık matrisi
- Şekil 2.4** Extra Trees algoritması ile eğitilen modelin karmaşıklık matrisi
- Şekil 2.5** AdaBoost algoritması ile eğitilen modelin karmaşıklık matrisi
- Şekil 2.6** Gradient Boosting algoritması ile eğitilen modelin karmaşıklık matrisi
- Şekil 2.7** Random Forest algoritması ile eğitilen modelin 2. test sonrası karmaşıklık matrisi
- Şekil 2.8** Decision Tree algoritması ile eğitilen modelin 2. test sonrası karmaşıklık matrisi
- Şekil 2.9** Gaussian Naive Bayes algoritması ile eğitilen modelin 2. test sonrası karmaşıklık matrisi
- Şekil 2.10** Extra Trees algoritması ile eğitilen modelin 2. test sonrası karmaşıklık matrisi
- Şekil 2.11** AdaBoost algoritması ile eğitilen modelin 2. test sonrası karmaşıklık matrisi
- Şekil 2.12** Gradient Boosting algoritması ile eğitilen modelin 2. test sonrası karmaşıklık matrisi

TABLO LİSTESİ

Tablo 2.1 Özniteliklerin belirlenmesi, modellerin eğitimi ve 1. testi için kullanılan veri setleri ve dosyalar

Tablo 2.2 Özniteliklerin belirlenmesi, modellerin eğitimi ve 1. testi için kullanılan veri türü örnek sayıları

Tablo 2.3 Modellerin 2. testi için kullanılan veri setleri ve dosyalar

Tablo 2.4 Modellerin 2. testi için kullanılan veri türü örnek sayıları

Tablo 2.5 Modellerin LDAP DDoS saldırısı ile testi için kullanılan veri seti ve dosya

Tablo 2.6 Modellerin LDAP DDoS saldırısı ile testi için kullanılan veri türü örnek sayısı

Tablo 2.7 Normal trafik tespiti için en önemli 10 öznitelik

Tablo 2.8 NTP DDoS saldırı tespiti için en önemli 10 öznitelik

Tablo 2.9 MSSQL DDoS saldırı tespiti için en önemli 10 öznitelik

Tablo 2.10 SNMP DDoS saldırı tespiti için en önemli 10 öznitelik

Tablo 2.11 UDP DDoS saldırı tespiti için en önemli 10 öznitelik

Tablo 2.12 DNS DDoS saldırı tespiti için en önemli 10 öznitelik

Tablo 2.13 Tüm veri türlerinin tespiti için en önemli 20 öznitelik

Tablo 2.14 Model eğitiminde kullanılan öznitelikler

Tablo 2.15 Random Forest algoritması ile eğitilen modelin çapraz doğrulama skoru sonuçları

Tablo 2.16 Decision Tree algoritması ile eğitilen modelde çapraz doğrulama skoru sonuçları

Tablo 2.17 Gaussian Naive Bayes algoritması ile eğitilen modelde çapraz doğrulama skoru sonuçları

Tablo 2.18 Extra Trees algoritması ile eğitilen modelde çapraz doğrulama skoru sonuçları

Tablo 2.19 AdaBoost algoritması ile eğitilen modelde çapraz doğrulama skoru sonuçları

Tablo 2.20 Gradient Boosting algoritması ile eğitilen modelin çapraz doğrulama skoru sonuçları

Tablo 2.21 Modellerin eğitimi ve 1. testi için kullanılan veri sayıları

Tablo 2.22 Modellerin eğitimi için kullanılan veri sayıları

Tablo 2.23 Modellerin 1. testi için kullanılan veri sayıları

Tablo 2.24 Random Forest algoritması ile eğitilen modelin 1. test metrik sonuçları

Tablo 2.25 Random Forest algoritması ile eğitilen modelin veri türlerine göre 1. test kesinlik metriği sonucu

Tablo 2.26 Random Forest algoritması ile eğitilen modelin veri türlerine göre 1. test hatırlama metriği sonucu

Tablo 2.27 Random Forest algoritması ile eğitilen modelin veri türlerine göre 1. test F1 skor metriği sonucu

Tablo 2.28 Decision Tree algoritması ile eğitilen modelin 1. test metrik sonuçları

Tablo 2.29 Decision Tree algoritması ile eğitilen modelin veri türlerine göre 1. test kesinlik metriği sonucu

Tablo 2.30 Decision Tree algoritması ile eğitilen modelin veri türlerine göre 1. test hatırlama metriği sonucu

Tablo 2.31 Decision Tree algoritması ile eğitilen modelin veri türlerine göre 1. test F1 skor metriği sonucu

Tablo 2.32 Gaussian Naive Bayes algoritması ile eğitilen modelin 1. test metrik sonuçları

Tablo 2.33 Gaussian Naive Bayes algoritması ile eğitilen modelin veri türlerine göre 1. test kesinlik metriği sonucu

Tablo 2.34 Gaussian Naive Bayes algoritması ile eğitilen modelin veri türlerine göre 1. test hatırlama metriği sonucu

Tablo 2.35 Gaussian Naive Bayes algoritması ile eğitilen modelin veri türlerine göre 1. test F1 skor metriği sonucu

Tablo 2.36 Extra Trees algoritması ile eğitilen modelin 1. test metrik sonuçları

Tablo 2.37 Extra Trees algoritması ile eğitilen modelin veri türlerine göre 1. test kesinlik metriği sonucu

Tablo 2.38 Extra Trees algoritması ile eğitilen modelin veri türlerine göre 1. test hatırlama metriği sonucu

Tablo 2.39 Extra Trees algoritması ile eğitilen modelin veri türlerine göre 1. test F1 skor metriği sonucu

Tablo 2.40 AdaBoost algoritması ile eğitilen modelin 1. test metrik sonuçları

Tablo 2.41 AdaBoost algoritması ile eğitilen modelin veri türlerine göre 1. test kesinlik metriği sonucu

Tablo 2.42 AdaBoost algoritması ile eğitilen modelin veri türlerine göre 1. test hatırlama metriği sonucu

Tablo 2.43 AdaBoost algoritması ile eğitilen modelin veri türlerine göre 1. test F1 skor metriği sonucu

Tablo 2.44 Gradient Boosting algoritması ile eğitilen modelin 1. test metrik sonuçları

Tablo 2.45 Gradient Boosting algoritması ile eğitilen modelin veri türlerine göre 1. test kesinlik metriği sonucu

Tablo 2.46 Gradient Boosting algoritması ile eğitilen modelin veri türlerine göre 1. test hatırlama metriği sonucu

Tablo 2.47 Gradient Boosting algoritması ile eğitilen modelin veri türlerine göre 1. test F1 skor metriği sonucu

Tablo 2.48 Modellerin 2. testi için kullanılan veri sayıları

Tablo 2.49 Random Forest algoritması ile eğitilen modelin 2. test metrik sonuçları

Tablo 2.50 Random Forest algoritması ile eğitilen modelin veri türlerine göre 2. test kesinlik metriği sonuçları

Tablo 2.51 Random Forest algoritması ile eğitilen modelin veri türlerine göre 2. test hatırlama metriği sonuçları

Tablo 2.52 Random Forest algoritması ile eğitilen modelin veri türlerine göre 2. test F1 skor metriği sonuçları

Tablo 2.53 Decision Tree algoritması ile eğitilen modelin 2. test metrik sonuçları

Tablo 2.54 Decision Tree algoritması ile eğitilen modelin veri türlerine göre 2. test kesinlik metriği sonuçları

Tablo 2.55 Decision Tree algoritması ile eğitilen modelin veri türlerine göre 2. test hatırlama metriği sonucu

Tablo 2.56 Decision Tree algoritması ile eğitilen modelin veri türlerine göre 2. test F1 skor metriği sonucu

Tablo 2.57 Gaussian Naive Bayes algoritması ile eğitilen modelin 2. test metrik sonuçları

Tablo 2.58 Gaussian Naive Bayes algoritması ile eğitilen modelin veri türlerine göre 2. test kesinlik metriği sonuçları

Tablo 2.59 Gaussian Naive Bayes algoritması ile eğitilen modelin veri türlerine göre 2. test hatırlama metriği sonucu

Tablo 2.60 Gaussian Naive Bayes algoritması ile eğitilen modelin veri türlerine göre 2. test F1 skor metriği sonucu

Tablo 2.61 Extra Trees algoritması ile eğitilen modelin 2. test metrik sonuçları

Tablo 2.62 Extra Trees algoritması ile eğitilen modelin veri türlerine göre 2. test kesinlik metriği sonuçları

Tablo 2.63 Extra Trees algoritması ile eğitilen modelin veri türlerine göre 2. test hatırlama metriği sonuçları

Tablo 2.64 Extra Trees algoritması ile eğitilen modelin veri türlerine göre 2. test F1 skor metriği sonucu

Tablo 2.65 AdaBoost algoritması ile eğitilen modelin 2. test metrik sonuçları

Tablo 2.66 AdaBoost algoritması ile eğitilen modelin veri türlerine göre 2. test kesinlik metriği sonuçları

Tablo 2.67 AdaBoost algoritması ile eğitilen modelin veri türlerine göre 2. test hatırlama metriği sonuçları

Tablo 2.68 AdaBoost algoritması ile eğitilen modelin veri türlerine göre 2. test F1 skor metriği sonuçları

Tablo 2.69 Gradient Boosting algoritması ile eğitilen modelin 2. test metrik sonuçları

Tablo 2.70 Gradient Boosting algoritması ile eğitilen modelin veri türlerine göre 2. test kesinlik metriği sonuçları

Tablo 2.71 Gradient Boosting algoritması ile eğitilen modelin veri türlerine göre 2. test hatırlama metriği sonuçları

Tablo 2.72 Gradient Boosting algoritması ile eğitilen modelin veri türlerine göre 2. test F1 skor metriği sonuçları

Tablo 2.73 Random Forest algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini veri türlerine göre sınıflandırma sonuçları

Tablo 2.74 Random Forest algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini sınıflandırma sonuçları

Tablo 2.75 Decision Tree algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini veri türlerine göre sınıflandırma sonuçları

Tablo 2.76 Decision Tree algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini sınıflandırma sonuçları

Tablo 2.77 Gaussian Naive Bayes algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini veri türlerine göre sınıflandırma sonuçları

Tablo 2.78 Gaussian Naive Bayes algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini sınıflandırma sonuçları

Tablo 2.79 Extra Trees algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini veri türlerine göre sınıflandırma sonuçları

Tablo 2.80 Extra Trees algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini sınıflandırma sonuçları

Tablo 2.81 AdaBoost algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini veri türlerine göre sınıflandırma sonuçları

Tablo 2.82 AdaBoost algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini sınıflandırma sonuçları

Tablo 2.83 Gradient Boosting algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini veri türlerine göre sınıflandırma sonuçları

Tablo 2.84 Gradient Boosting algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini sınıflandırma sonuçları

Tablo 3.1 Modellerin 1. testinde kullanılan veri sayıları

Tablo 3.2 Modellerin 1. test metrik sonuçları

Tablo 3.3 Modellerin 2. testinde kullanılan veri sayıları

Tablo 3.4 Modellerin 2. test metrik sonuçları

Tablo 3.5 Modellerin LDAP DDoS saldırı verilerini sınıflandırma sonuçları

Tablo 3.6 CIC-DDoS2019 veri seti kullanılarak yapılan çalışmanın sonuçları

Tablo 3.7 CICIDS2017 veri seti kullanılarak yapılan çalışmanın sonuçları

1. GİRİŞ

Denial of Service (DoS) saldırıları, kullanıcıların ağa veya diğer kaynaklara erişmesini engellemeyi amaçlayan saldırı türüdür. DoS saldırıları, ağ seviyesinde ve uygulama seviyesinde olmak üzere iki farklı şekilde gerçekleştirilebilmektedir. Ağ seviyesinde yapılan DoS saldırıları ağdaki kaynakları hedef alırken uygulama seviyesinde yapılan DoS saldırıları sunucu kaynaklarını hedef almaktadır [1]. Distributed Denial of Service (DDoS) saldırılarına ilk kez 1999 yılında rastlanmıştır [2]. DDoS saldırısında saldırganlar birden çok makine kullanarak, hedef sunucuya kaldıracılabileceğinden fazla miktarda yük bindirmeyi amaçlamaktadır [3]. DDoS saldırılarında DoS saldırılarından farklı olarak birden çok makine kullanılması sebebiyle DDoS saldırılarının önlenmesi DoS saldırılarına göre daha zordur. Bunun yanı sıra DDoS saldırılarının hedef sunucuya verdiği tahribat DoS saldırılarına göre daha fazladır [4].

DoS ve DDoS saldırılarına önlem olarak saldırı tespit sistemleri ve saldırı önleme sistemleri kullanılmaktadır [5]. Saldırı tespit sistemleri anomali tabanlı ve kötüye kullanım tabanlı olmak üzere iki sınıfta incelenebilmektedir [6]. Kötüye kullanım tabanlı saldırı tespit sistemleri için imza tabanlı saldırı tespit sistemleri ifadesi de kullanılmaktadır [7]. Kötüye kullanım tabanlı saldırı tespit sistemleri saldırıların imzalarına bakarak veri trafiğinin saldırı olup olmadığına karar vermektedir. Yeni bir metot ile saldırı yapılması durumunda kötüye kullanım tabanlı saldırı tespit sistemleri saldırının tespitinde başarısız olmaktadır. Anomali tabanlı saldırı tespit sistemleri geçmişte kaydedilen veri trafiğiyle yeni gelen veri trafiğini karşılaştırarak saldırı olup olmadığına karar vermektedir. Anomali tabanlı saldırı tespit sistemleri, yeni bir metot ile saldırı yapılması durumunda saldırıyı tespit edebilmektedir fakat saldırı olmadığı halde saldırı olarak tespit ettiği durumlar da bulunmaktadır [6].

Bu çalışmada makine öğrenmesi algoritmaları kullanılarak DDoS saldırı tespiti ve sınıflandırması yapılmaktadır. Çalışma gerçekleştirilirken scikit-learn'den faydalanılmıştır [8]. Scikit-learn, sınıflandırma, regresyon ve kümeleme algoritmalarını barındıran bir makine öğrenmesi kütüphanesidir [9]. Çalışmada kullanılan scikit-learn versiyonu 0.21.2 versiyonudur. DDoS saldırı tespiti ve sınıflandırması için modeller Random Forest, Decision Tree, Gaussian Naive Bayes, Extra Trees, AdaBoost ve

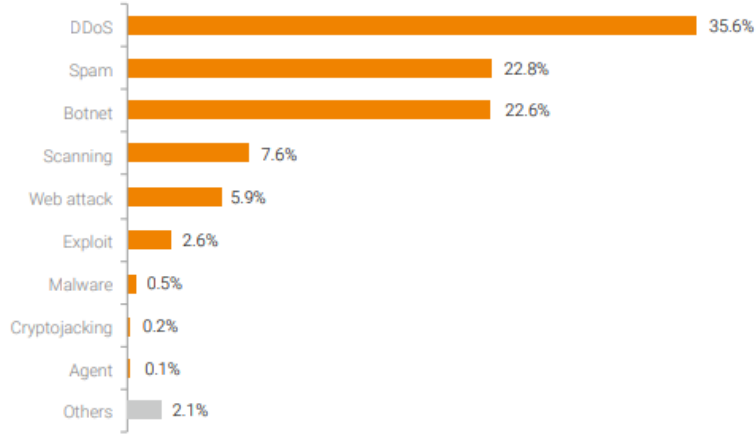
Gradient Boosting algoritmaları ile eğitilmiştir. Çalışmada kullanılan veriler CIC-DDoS2019 ve CSE-CIC-IDS2018 veri setlerinden alınmıştır [10], [11]. CSE-CIC-IDS2018 veri seti için Amazon Web Services'te bir web sayfası bulunmaktadır [12]. Model eğitiminde kullanılan veri türleri içerisinde, normal trafik verisi, Network Time Protocol (NTP) DDoS trafik verisi, Microsoft Structured Query Language (MSSQL) DDoS trafik verisi, Domain Name System (DNS) DDoS trafik verisi, Simple Network Management Protocol (SNMP) DDoS trafik verisi ve User Datagram Protocol (UDP) DDoS trafik verisi bulunmaktadır. Çalışmada kullanılan sınıflandırıcıların çapraz doğrulama metodu ile testi gerçekleştirilmiştir. Model eğitiminde kullanılan veri türlerinin, veri sayısı bakımından dengeli olmasına dikkat edilmiş ve bu sayede yanlış sonuç alınmasının engellenmesi amaçlanmıştır. Eğitilen modeller 2 kere testten geçirilmiş ve başarıları irdelenmiştir. Bununla beraber eğitilen modeller, modellerin eğitim aşamasında kullanılmayan Lightweight Directory Access Protocol (LDAP) DDoS saldırı verisiyle de test edilerek modellerin eğitim aşamasında görmediği saldırı türünü sınıflandırma becerisi de test edilmektedir. Model değerlendirmesinde doğruluk, kesinlik, hatırlama ve F1 skor performans metrikleri kullanılmıştır. Yapılan testler sonucunda makine öğrenmesi algoritmalarının DDoS saldırı tespiti ve sınıflandırmasında başarılı olup olmadığı değerlendirilmekte ve kullanılan algoritmalar birbirleriyle karşılaştırılarak araştırmacılara sunulmaktadır.

1.1 DDoS Saldırıları

DDoS saldırıları, saldırganların birden çok makine kullanarak gerçekleştirdiği, hedef sistemin kaynaklarını tüketen ve böylelikle hedef sistemi yavaşlatan veya işlevsiz hale getiren saldırı türüdür [13]. Saldırganın DDoS saldırısı yapmak için kullandığı diğer makinalara zombi denilirken, saldırı yapılan sisteme ise kurban denilmektedir [14]. Ekonomik kazanç sağlamak, hedef sistemin hizmetini kesmek veya hedef sistemin hizmetini yavaşlatmak isteği DDoS saldırılarının sebeplerindendir [15].

NSFOCUS'un yayınladığı 2019 CyberSecurity Insights raporuna göre saldırgan internet protokol adreslerinden gelen atak dağılımı incelendiğinde DDoS atakları, yapılan tüm ataklar içerisinde en büyük paya sahiptir. Ardından sırasıyla Spam ve Botnet saldırıları gelmektedir [16].

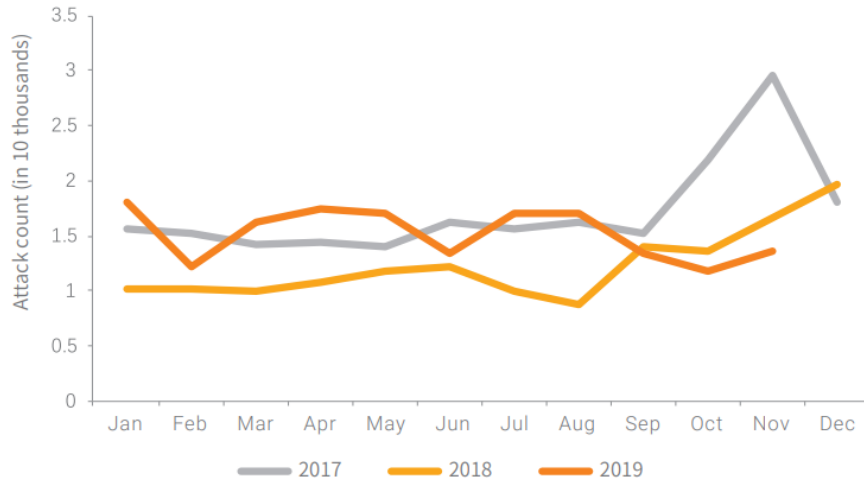
Atak türlerine göre saldırı oranları Şekil 1.1’de gösterilmektedir.



Şekil 1.1 Atak türlerine göre saldırı oranları [16]

NSFOCUS’un yayınladığı 2019 DDoS Attack Landscape raporuna göre 2019 Kasım ayına kadar 167,400 DDoS saldırısı tespit edilmiş ve bu saldırılarda toplamda 436,800 Terabayt büyüklüğünde trafik akışı olduğu görülmüştür. Yıllık bazda bakıldığında DDoS atak sayısında %30.2 oranında artış olmasına rağmen toplam DDoS saldırı trafik akışı büyüklüğü %26.4 oranında azalma göstermiştir [17].

2017, 2018 ve 2019 yıllarında aylara göre yapılan DDoS saldırı sayısı Şekil 1.2’de verilmiştir.

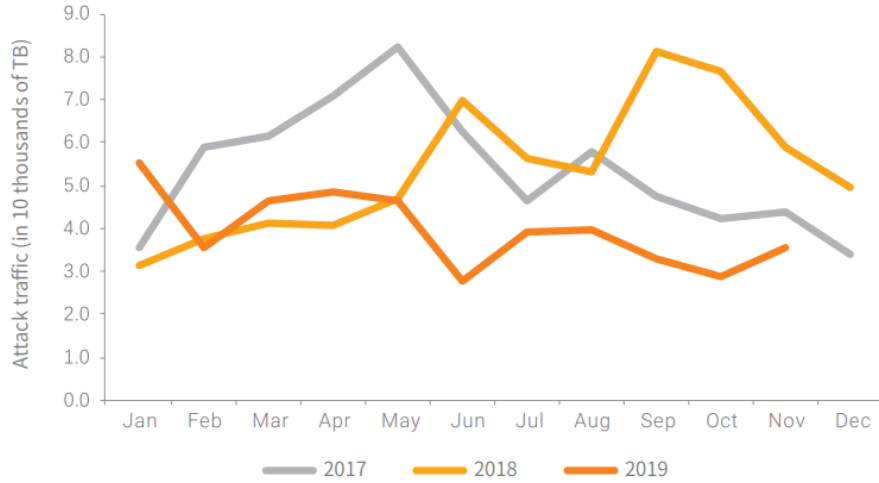


Şekil 1.2 Aylara göre DDoS saldırı sayısı [17]

Şekil 1.2’de görülen 2017 yılındaki hareketliliğin sebebi kripto para piyasasındaki hareketlenmeye ve buna bağlı olarak saldırganların kripto para madenciliği yapmasıyla

ilişkilendirilebilir. 2019 yılında ay bazında bakıldığında grafikte dramatik bir değişiklik olmadığı görülmektedir [17].

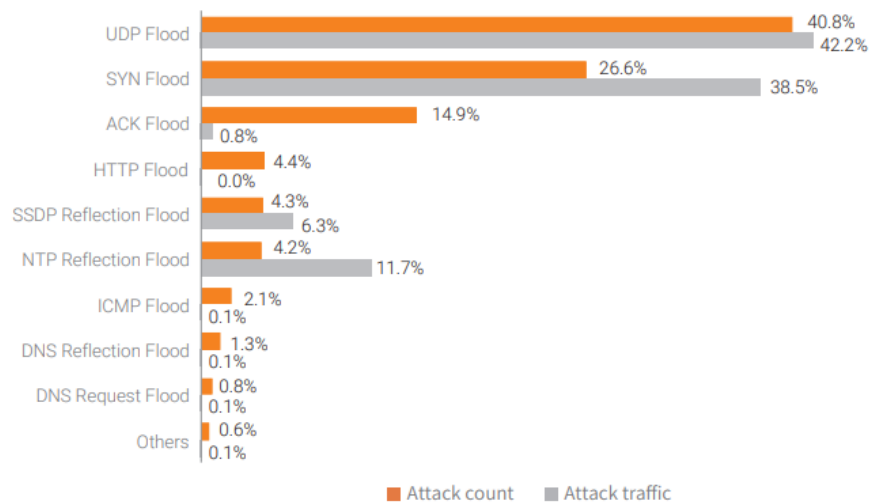
2017, 2018 ve 2019 yıllarında aylara göre yapılan DDoS saldırı trafik büyüklüğü Şekil 1.3'te verilmiştir.



Şekil 1.3 Aylara göre DDoS saldırı trafik büyüklüğü [17]

Şekil 1.3'te görülen 2019 yılındaki atak trafik büyüklüğü ve atak sayısı değişim durumları incelendiğinde trafik büyüklüğü ve trafik sayısı arasında korelasyon olduğu söylenebilmekteyken 2017 ve 2018 yılları için böyle bir durum bulunmamaktadır [17].

Saldırı türlerine göre DDoS atak trafik büyüklüğü ve atak sayısı oranlarını gösteren grafik Şekil 1.4'te gösterilmiştir.



Şekil 1.4 Saldırı türlerine göre DDoS atak trafik büyüklüğü ve atak sayısı oranları [17]

Şekil 1.4'te görülen DDoS atak tiplerine göre atak trafik büyüklüğü ve atak trafik sayısı incelendiğinde, UDP DDoS, Synchronize (SYN) DDoS ve Acknowledgement (ACK) DDoS atakları 2019 yılında görülen DDoS atak tiplerinin büyük çoğunluğunu oluşturmaktadır. Ardından bu atakları Hyper-Text Transfer Protocol (HTTP) DDoS, Simple Service Discovery Protocol (SSDP) DDoS ve NTP DDoS atakları izlemektedir [17].

DDoS saldırıları, sadece bir atak türü kullanılarak yapılmak zorunda değildir. Birden çok atağı aynı anda yaparak da DDoS saldırıları yapılabilir. Bu tip birden çok atağın aynı anda yapıldığı atak türüne çoklu vektör atağı denmektedir. Yapılan atakların %12.5'lik kısmı birden çok atak türünün bir arada bulunduğu çoklu vektör ataklarıdır [17].

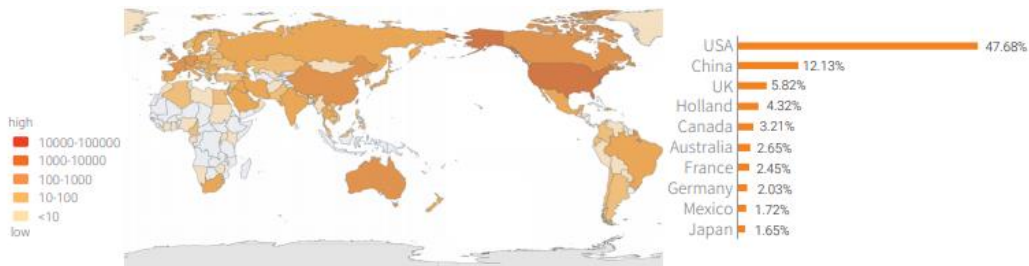
DDoS saldırısını en fazla gerçekleştiren ülkeler Şekil 1.5'te gösterilmiştir.



Şekil 1.5 DDoS saldırısı gerçekleştiren ülkeler haritası [17]

Şekil 1.5 incelendiğinde en çok DDoS saldırısı yapan ülkelerin sırasıyla %36.19 ile Çin, % 14.75 ile Amerika ve %7.81 ile İngiltere olduğu görülmektedir [17].

DDoS saldırısına en fazla maruz kalan ülkeler Şekil 1.6'da gösterilmiştir.



Şekil 1.6 DDoS saldırısına uğrayan ülkeler haritası [17]

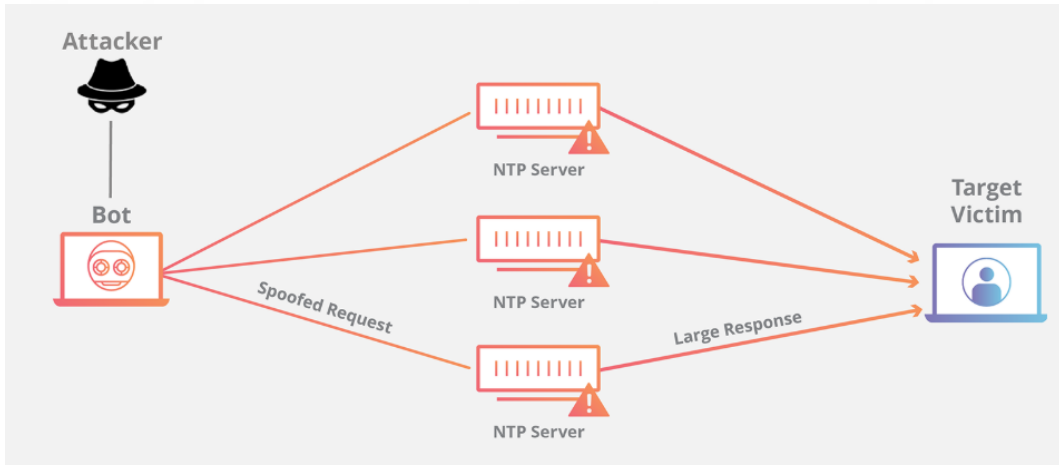
DDoS saldırısına en fazla maruz kalan ülkeler sıralamasında %47.68 ile Amerika ilk sırada bulunmaktadır. Ardından %12.13 ile Çin ve %5.82 ile İngiltere gelmektedir [17].

1.1.1 DDoS Saldırı Çeşitleri

Bu bölümde DDoS saldırılarından olan NTP DDoS, MSSQL DDoS, DNS DDoS, SNMP DDoS, UDP DDoS ve LDAP DDoS saldırıları hakkında bilgi verilmektedir.

1.1.1.1 NTP DDoS

NTP DDoS saldırısı, NTP sunucusu kullanılarak hedef sunucuya yüksek miktarda UDP trafiği gönderip hedefin dışarıyla olan veri trafiğinin engellenmesini amaçlamaktadır. Saldırgan birçok zombi bilgisayar kullanarak bu atağı gerçekleştirir [18]. Şekil 1.7’de NTP DDoS saldırı görseli verilmiştir.



Şekil 1.7 NTP DDoS saldırı görseli [18]

Zombi bilgisayarlar, sahte internet protokol adreslerini kullanarak, hedef bilgisayardan çok sayıda istek geliyor gibi gösterip NTP sunucusuna UDP paketleri göndermeye başlar. Gönderilen UDP paketlerine NTP sunucusu yanıt verir. Bu yanıt verme sırasında hedef sunucu NTP DDoS saldırısına uğrar ve sunucunun normal veri trafiği engellenmiş olur [18].

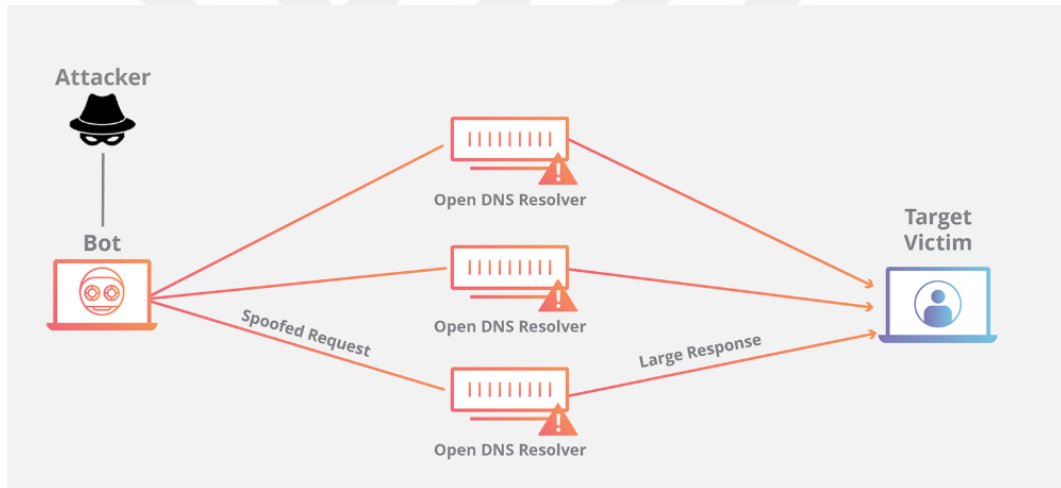
1.1.1.2 MSSQL DDoS

MSSQL DDoS saldırısı, zombi bilgisayarlar kullanılarak, MSSQL’in çözümleme protokolünü etkisiz hale getirmek amacıyla yapılan bir saldırdır. Bu protokol veritabanına istek gönderildiği zaman çalıştırılır. Saldırganlar, sahte internet protokol adreslerini kullanarak, hedef bilgisayardan çok sayıda istek geliyor gibi gösterip

veritabanına UDP paketleri göndermeye başlar. Veritabanı bu isteklere yanıt vermeye çalışırken veritabanının bulunduğu sunucunun veri trafiği engellenmiş olur [19].

1.1.1.3 DNS DDoS

DNS DDoS saldırısı, zombi bilgisayarlar kullanılarak, DNS sunucularına yüksek miktarda zararlı trafik gönderip hedef sunucunun dışarıyla olan veri trafiğinin engellenmesini amaçlamaktadır. Saldırganlar hedef sunucuyu gösteren sahte internet protokol adreslerinden fazla sayıda istek gönderir ve bu istekler hedef sunucudan geliyormuş gibi gösterirler. DNS sunucusu bütün bu isteklere cevap vermeye çalışır ve verilen cevapları hedef sunucuya gönderir. Hedef sunucuya çok fazla veri trafiği geldiği için sunucu erişilebilirliği zarar görmüş olur [20]. Şekil 1.8’de DNS DDoS saldırı görseli verilmiştir.



Şekil 1.8 DNS DDoS saldırı görseli [20]

1.1.1.4 SNMP DDoS

SNMP, sunucularda çalışan sunucunun o anki durumunu uzaktan bağlanarak görüntülemeye ve sunucuda gerekli değişiklikleri yapmaya imkan sağlayan servistir. SNMP, UDP protokolünü kullanır. SNMP DDoS saldırıları, zombi bilgisayarlar vasıtasıyla sahte internet protokol adresleri kullanılarak çok fazla sayıdaki SNMP isteğinin hedef sunucuya gönderilmesiyle gerçekleştirilir [21].

1.1.1.5 UDP DDoS

UDP DDoS atağı, saldırganlar tarafından zombi bilgisayarlar kullanılarak çok sayıda UDP paketinin hedef sisteme gönderilmesi ve bunun sonucunda hedef sistemin erişilebilirliğinin zarar gördüğü bir atak türüdür. Saldırganlar atağı yaparken diğer ataklardaki gibi sahte internet protokol adresleri kullanırlar. Çok sayıda UDP paketi gelen saldırı altındaki sunucular, kaynakları bir süre sonra tükendiği için hizmet dışı kalacaklardır [22].

1.1.1.6 LDAP DDoS

LDAP, büyük ağ ve sistemlerde çok sık kullanılan bir servistir. Bu servis hem UDP protokolü ile hem de Transmission Control Protocol (TCP) protokolü ile çalışabilmektedir. LDAP UDP üzerinden haberleşmek için 389 portunu kullanmaktadır. Bir LDAP DDoS saldırısı yapılabilmesi için LDAP sunucusunda kullanılan protokol UDP olmalıdır [23].

Bu saldırıda saldırgan, sahte internet protokol adresi kullanarak LDAP sunucusuna birçok istek gönderir ve sahte internet protokol adresi kullanması sayesinde sunucudan dönen fazla miktardaki cevabı hedef sunucuya gönderir. Hedef sunucu kaynakları, gelen fazla miktardaki trafik sebebiyle tükenir ve sunucu artık hizmet veremez olur [23].

1.2 Saldırı Tespit Sistemleri

Kurumlar Virtual Private Network (VPN), güvenlik duvarı ve kimlik doğrulama mekanizmalarını kullanarak network altyapılarını ve internet üzerindeki iletişimlerini güvence altına almaktadırlar. Saldırı tespit sistemleri bu mekanizmalara ek olarak, kurumdaki sistemleri ve ağdaki trafiği izleyen ve izlediği trafiği de analiz ederek yapılan saldırıları tespit eden sistemlerdir. Saldırı tespit sistemleri, sistemlere yapılan saldırılara karşı ilgili personeli uyarır ve bu sayede sistemin yapılan saldırıdan zarar görmemesi için personelin aksiyon almasını sağlar [24]. İlk saldırı tespit sistemi, 1980 yılında yapılmıştır. Günümüze kadar çeşitli saldırı tespit sistemleri ağ güvenliği ihtiyaçlarını karşılamak amacıyla geliştirilmiştir [25].

Saldırı tespit sistemlerinin aşağıdaki gereklilikleri sağlıyor olması beklenmektedir.

- Saldırıyı tespit edememe ve normal trafiği saldırı olarak algılama oranları çok düşük olmalıdır.
- İzlediği sistemler zaman içerisinde eklenen yeni özellikler sebebiyle farklı davranışlar sergileyebilir. Saldırı tespit sistemleri bu değişikliklere göre karar verebilmelidir.
- Saldırı tespit sistemleri kapalı kutu şeklinde olmamalı yani dışardan bakan bir kişi içerdeki işleyişi anlayabilmelidir.
- Sistemdeki bazı mekanizmalar çökse bile saldırı tespit sistemleri hala çalışabilecek şekilde ayarlanmalı ve çöken mekanizmalar tekrar devreye alındığı zaman saldırı tespit sistemleri bu mekanizmalarla tekrardan bağlantı kurabilmelidir.
- Saldırı tespit sistemleri, düzgün ve istenilen şekilde çalıştığından emin olmak için kendisini de kontrol etmelidir.
- Saldırı tespit sistemleri, anormal trafiği ve davranışları fark edip bunları kaydetmelidir.
- Birçok sistemin kendi içerisinde farklı dizaynı bulunmaktadır. İdeal bir saldırı tespit sisteminin bu sistemlere uyum sağlayabiliyor olması gerekmektedir [26].

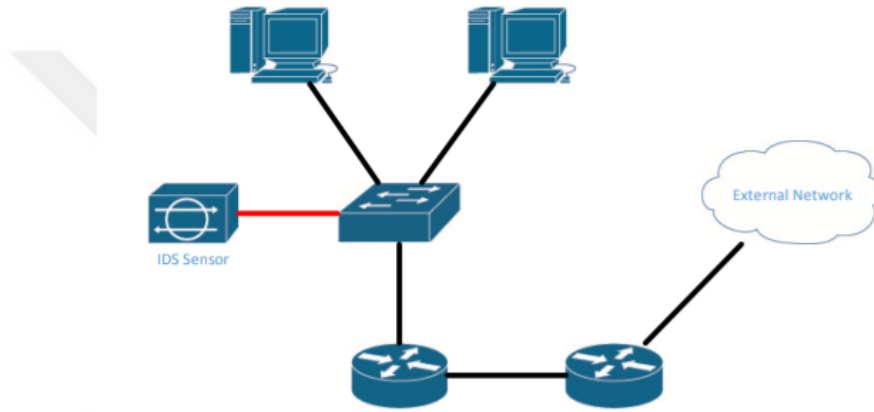
Saldırı tespit sistemleri ve güvenlik duvarlarının kullanımına rağmen saldırganların başarılı olması bu sistemlerin ve cihazların yeterli güvenliği sağlamadığını göstermektedir. Araştırmacılar makine öğrenmesi algoritmalarını kullanarak anomali tespiti ile bu problemin giderilebileceğini düşünmektedirler [27]. Saldırı tespit sistemlerinin performansını arttırmak için yapılan çalışmalarda, makine öğrenmesi yöntemlerini kullanan ve saldırıların öğrenilmesinde temel olarak denetimli ve denetimsiz öğrenme metotlarını kullanan saldırı tespit sistemleri üzerinde durulmuştur [28].

1.2.1 Veriyi toplama şekline göre saldırı tespit sistemleri

1.2.1.1 Ağ tabanlı saldırı tespit sistemleri

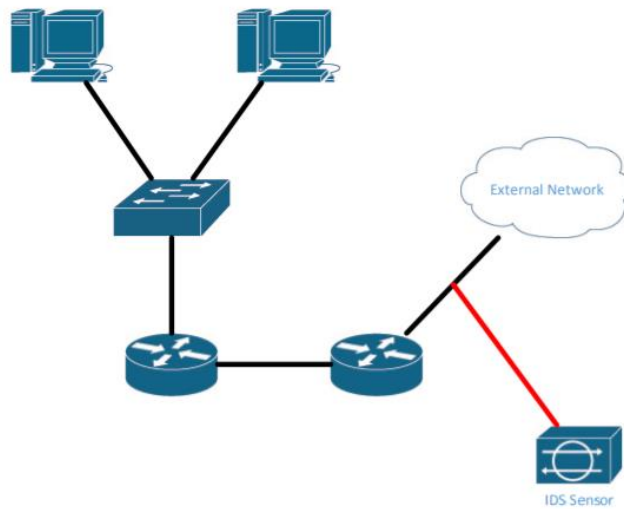
Ağ tabanlı saldırı tespit sistemleri, bir bilgisayarın veya cihazın içerisinde bulunmak yerine ağa bağlı ayrı bir unsur olarak yerleştirilir. Ağdaki trafiği analiz ederek saldırıları tespit edip gerekli aksiyonu alır veya saldırı durumunda ilgili personeli uyarır [26].

Saldırı tespit sistemi, ağ üzerinde switch cihazına bağlı olarak bulunabilir. Bu durumda switch analiz etmesi için saldırı tespit sistemine trafiğin aynısını kopyalar [26]. Şekil 1.9’da switch cihazına bağlı saldırı tespit sistemi örneği verilmiştir.



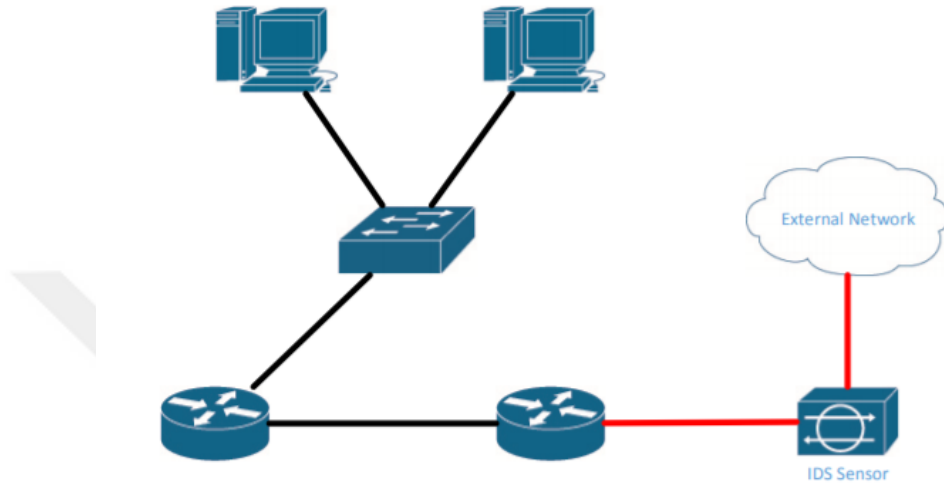
Şekil 1.9 Ağ üzerinde switch cihazına bağlı saldırı tespit sistemi [26]

Saldırı tespit sistemi, iç ağ ile dış ağ arasındaki bağlantı arasına ayrı bir ağ bağlantısı kurulması sayesinde veri trafiğinin bir kopyasını alıp analiz edebilir [26]. Şekil 1.10’da iç ağ ile dış ağ arasındaki bağlantıya bağlı saldırı tespit sistemi örneği verilmiştir.



Şekil 1.10 İç ağ ile dış ağ arasındaki bağlantıya bağlı saldırı tespit sistemi [26]

Saldırı tespit sistemi, iç ağ ile dış ağ arasına direkt olarak koyulabilir. Bu durumda dış ağdan iç ağa gelen trafik saldırı tespit sistemi üzerinden geçmek zorundadır. Bu sebeple saldırı tespit sistemindeki arıza durumu dış ağ ve iç ağ arasındaki trafiğin kesilmesi anlamına gelmektedir [26]. Şekil 1.11’de dış ağ ile iç ağ arasına direkt yerleştirilen saldırı tespit sistemi örneği verilmiştir.



Şekil 1.11 Dış ağ ile iç ağ arasına direkt yerleştirilen saldırı tespit sistemi [26]

1.2.1.2 Ana bilgisayar tabanlı saldırı tespit sistemleri

Ana bilgisayar tabanlı saldırı tespit sistemleri, bir cihazın veya bilgisayarın içerisinde bulunmaktadır. İçerisinde bulunduğu cihazın trafiğini izleyerek saldırıları tespit etmeyi ve saldırı durumunda gerekli personeli bilgilendirmeyi amaçlar. Bunun yanı sıra bir cihazın içerisinde bulunmasına rağmen, ağdaki trafiği de izleyebilen türleri bulunmaktadır [26].

1.2.2 Veriyi analiz şekline göre saldırı tespit sistemleri

1.2.2.1 İmza tabanlı saldırı tespit sistemi

İmza tabanlı saldırı tespit sistemleri, önceden yapılan ataklardan öğrenilen bilgilere göre karar veren sistemlerdir. Atağı yaparken belirli bir sıra veya düzen olup olmaması, önceki ataklardan öğrenilmiş olan bayt sırası ve bilinen sistem güvenlik açıkları gibi bilgiler bu sistemde tutulur [29].

Saldırı tiplerinin belirli şablonları ve imzaları vardır. Bir saldırıdaki imzalara örnek olarak sunucuya fazla sayıda istek gönderimi, fazla sayıda başarısız giriş ve yetkisiz erişim denemeleri verilebilir. Bu imzaları kullanarak saldırı tespit sistemi, gelecekte olabilecek benzer saldırıları tespit edip ilgili personeli saldırı hakkında uyarmak için kullanır [29].

İmza tabanlı saldırı tespit sistemleri yeni çıkan saldırı şablonları ve yöntemlerine karşı etkili değildir. Eğer saldırgan, saldırı tespit sisteminin bildiği bir şablon dışında hareket ederse saldırı tespit sistemi saldırının tespitinde başarısız olabilir. İmza tabanlı saldırı tespit sistemleri sürekli yeni atak türleri ve şablonlarına göre güncellenmelidir. Aksi takdirde yeni çıkan saldırı yöntemlerine karşı başarısız olacaktır [29].

1.2.2.2 Anomali tabanlı saldırı tespit sistemi

Anomali tabanlı saldırı tespit sistemleri, sistemin normal davranışından farklı bir davranış sergileyip sergilemediği ile ilgilenir. Sistemin normal davranış modeli önceden tanımlanmış olmalıdır. Normal davranış modeli oluşturulurken kullanılan kurallar iyi seçilmeli ve test edilmelidir. Normal davranış modeli için kuralların düzgün bir şekilde tanımlanması koşuluyla saldırı tespitinde, anomali tabanlı saldırı tespit sistemlerinin, imza tabanlı saldırı tespit sistemlerinden daha başarılı olduğu söylenebilir. Anomali tabanlı sistemlerde yapılan saldırıların bir imzasının sistemde bulunması şart değildir. Bu sayede yeni bir saldırı türünü tespit etme yeteneği bulunmaktadır. Anomali tabanlı saldırı tespit sistemleri 3 grupta incelenebilir [29].

İstatistiksel tabanlı

Bu yaklaşımda kullanıcı ve izlenen sistemin davranışları istatistiki veri olarak tutulur. Bir trafiğe saldırı olarak karar verebilmek için belirlenen eşik değer çok dikkatli bir şekilde seçilmelidir aksi takdirde saldırı tespit sistemi birçok yanlış alarm üretecektir. Gelen veri trafiği, normal trafiğin ortalama, varyans gibi değerlerinden belirli oranda sapma gösterirse alarm üretilir. Bu yaklaşımda sistemin ataklar hakkında bilgisi olmamasına rağmen saldırıları tespit etme yeteneği bulunmaktadır. DDoS gibi uzun süreli saldırıların tespiti bu yaklaşımla başarılı bir şekilde gerçekleştirilebilir [29].

Bilgi tabanlı

Bilgi tabanlı yaklaşım sayesinde, ataklar hakkındaki bilgileri kullanarak saldırıları ve sistemdeki zaafları tespit edebilmek mümkündür. Hem imza tabanlı saldırı tespit sistemleri hem de anomali tabanlı saldırı tespit sistemleri, bilgi tabanlı yaklaşım metodunu kullanabilir. Bu yaklaşımdaki problem, eğer saldırı hakkında sistemin önceden bir bilgisi yoksa sistem saldırı tespitinde başarısız olur. Fakat sistemde saldırı karakteristiği hakkında önceden bilgi bulunması durumunda yanlış alarm üretme oranı oldukça düşüktür. Bu sebeple bilgi tabanlı yaklaşımda saldırı karakteristik bilgileri güncel tutulmalıdır [29].

Makine öğrenmesi tabanlı

Makine öğrenmesi tabanlı yaklaşımda saldırı tespit sistemleri, geçmiş veri trafiğinden ve sistem hareketlerinden ilerde karşılaşılabilecek normal veya saldırı veri trafiği için nasıl bir tepki vereceği bilgisini kendiliğinden öğrenir. Makine öğrenmesinde veri çok önemlidir. Elimizdeki verinin doğruluğu ve uygunluğu modelimizin doğru sonuçlar üretmesini sağlayacaktır [29].

Makine öğrenmesi tabanlı saldırı tespit sisteminde denetimli öğrenme, yarı denetimli öğrenme ve denetimsiz öğrenme olmak üzere 3 adet öğrenme yöntemi bulunmaktadır [30].

Denetimli öğrenme

Denetimli öğrenme yönteminde, her bir verinin hangi sınıfa ait olduğu etiketlenmiş durumdadır. Bu yöntemde en az 2 sınıf bulunmalıdır. Örneğin modeli eğitmek için hazırlanan veri setinde bir paketin saldırı mı yoksa normal trafik mi olduğu belirtilir ve model buna göre eğitilirse denetimli öğrenme yöntemi uygulanmış olur. Yeni gelen ve saldırı mı yoksa normal trafik mi olduğu bilinmeyen paketler bu modele girdi olarak verilir ve gelen paketin saldırı mı normal mi olduğunu önceki verilerle eğitilen model karar verir. Bu yöntemdeki problemlerden birisi eğitmek için kullanılan veri setinin bütün saldırı türlerini kapsamamasının oldukça zor olmasıdır. Bununla beraber etiketlenmiş verilerin doğruluğunun kesin olmaması da modellerin yanlış sonuçlar vermesine sebep olabilmektedir [30].

Yarı denetimli öğrenme

Yarı denetimli öğrenme yönteminde, verilerin bazıları hangi sınıfa ait olduğu etiketlenmiş durumdayken bazıları ise etiketsiz durumdadır [30].

Denetimsiz öğrenme

Denetimsiz öğrenme yönteminde, verilerin hangi sınıfa ait olduğu bilinmemektedir. Bu yöntemde verilerin ne olduğu bilinmeden makine öğrenmesi algoritmaları kullanılarak veriler kendi içlerinde gruplara ayrılır [30].

1.3 Benzer Çalışmalar

Pham ve diğerleri, 2016 yılında yayınlanan çalışmalarında, web ataklarının makine öğrenmesi algoritmalarıyla tespiti üzerine çalışma yapmışlardır. Çalışmalarında CSIC 2010 HTTP veri setini kullanmışlardır. Bu veri setinde 223585 adet örnek vardır. Bu örneklerin 119585 tanesi atak trafik verisi, 104000 tanesi ise normal trafik verisidir. Makine öğrenmesi algoritması olarak Random Forest, Logistic Regression, Decision Tree, Adaboost Classifier ve SGDClassifier kullanmışlardır. Yaptıkları çalışmanın sonucunda Logistic Regression algoritmasının en iyi sonucu verdiğini tespit etmişlerdir. Çalışmalarında en iyi sonucu veren Logistic Regression algoritması ile normal trafik için %94.36 kesinlik değeri ve %96.97 F1 skor değeri, saldırı trafiği için ise %99.75 kesinlik değeri ve % 97.22 F1 skor değeri elde etmişlerdir [31].

Sharafaldin ve diğerleri, 2019 yılında yayınlanan çalışmalarında, DDoS ataklarının makine öğrenmesi algoritmalarıyla tespiti üzerine çalışma yapmışlardır. Çalışmalarını kendi ürettikleri CICDDoS2019 veri seti ile gerçekleştirmişlerdir. Veri üretimini 2 farklı günde gerçekleştirmişlerdir. İlk gün model eğitimi için gerekli olan veriyi, ikinci gün ise eğitilen modeli test için gerekli olan veriyi üretmişlerdir. Model eğitimi için üretilen saldırı verileri içerisinde NTP DDoS, DNS DDoS, LDAP DDoS, MSSQL DDoS, Network Basic Input/Output System (NetBIOS) DDoS, SNMP DDoS, SSDP DDoS, UDP DDoS, UDP-Lag DDoS, WebDDoS, SYN DDoS ve Trivial File Transfer Protocol (TFTP) DDoS saldırıları bulunmaktadır. Model testi için üretilen saldırı verileri içerisinde PortMap DDoS, NetBIOS DDoS, LDAP DDoS, MSSQL DDoS, UDP DDoS, UDP-Lag DDoS ve SYN DDoS saldırıları bulunmaktadır. Hem eğitim hem de test verileri içerisine

normal trafik içeren veriler de eklenmiştir. Çalışmalarında Decision Tree algoritmasından biri olan Iterative Dichotomiser 3 (ID3), Random Forest, Naive Bayes ve Multinomial Logistic Regression algoritmalarını kullanmışlardır. Çalışmalarında en iyi sonucu veren ID3 algoritması ile %78 kesinlik değeri, %65 hatırlama değeri ve %69 F1 skor değeri elde etmişlerdir [10].

Ll ve diğerleri, 2016 yılında yayınlanan çalışmalarında DDoS atak tespiti için makine öğrenmesi algoritmalarından Support Vector Machine (SVM) kullanan bir saldırı tespit sistemi ile normal saldırı tespit sistemlerinden olan SNORT'u karşılaştırmışlardır. Çalışmalarının sonucu olarak SNORT saldırı tespit sisteminin %89 doğruluk ve SVM algoritması çalışan saldırı tespit sisteminin %99 doğruluk ile çalıştığını tespit etmişlerdir [32].

Sharafaldin ve diğerleri, 2018 yılında yayınlanan çalışmalarında, kendi ürettikleri CICIDS2017 veri seti ile BruteForce, DoS, DDoS, web atakları ve bazı diğer atak türlerini makine öğrenmesi algoritmaları kullanarak tespiti için çalışma yapmışlardır. Çalışmalarında K-Nearest Neighbors, Random Forest, ID3, Adaboost, Multilayer Perceptron, Naive-Bayes ve Quadratic Discriminant Analysis makine öğrenmesi algoritmalarını kullanmışlardır. ID3 ile %98 kesinlik değeri, %98 hatırlama değeri, %98 F1 skor değeri ve 235.02 saniye çalışma zamanı elde etmişlerdir. Random Forest ile %98 kesinlik değeri, %97 hatırlama değeri, %97 F1 skor değeri ve 74.39 saniye çalışma zamanı elde etmişlerdir [33].

Bindra ve Sood, 2019 yılında yayınlanan çalışmalarında, CICIDS2017 veri setinin belirli bir bölümünü kullanarak DDoS ataklarının makine öğrenmesi algoritmaları kullanılarak tespiti için çalışma yapmışlardır. Logistic Regression, K-Nearest Neighbors, Gaussian Naive Bayes, Random Forest, Linear SVM, Linear Discriminant Analysis ve Quadratic Discriminant Analysis makine öğrenmesi algoritmalarını kullanmışlardır. Çalışmalarında Random Forest algoritması %96.2 oranla en iyi sonucu vermiştir [34].

Robinson ve Thomas, 2015 yılında yayınlanan çalışmalarında, 3 farklı veri seti ile DDoS ataklarının makine öğrenmesi algoritmaları kullanarak tespiti için çalışma yapmışlardır. Veri seti olarak LLS-DDoS1.0, CAIDA 2007, CAIDA Conficker kullanmışlardır. DDoS tespiti için Naive Bayes, Radial Basis Function Network, Multilayer Perceptron, Bayesnet, Instance Based learning, J48, Voting, Bagging + Random Forest, Random

Forest, Adaboost + Random Forest algoritmalarını kullanmışlardır. Algoritmalar arasından Adaboost + Random Forest kullanımının en iyi sonucu verdiği, Naive Bayes'in ise en kötü sonucu verdiği görülmüştür [35].

Çebi ve diğerleri, 2019 yılında yayınlanan çalışmalarında, makine öğrenmesi algoritmalarını kullanarak saldırı tespiti yapan modelleri karşılaştırmışlardır. Veri seti olarak NSL-KDD veri setini kullanmışlardır. Çalışmalarında K-En Yakın Komşu, Karar Ağacı, Yapay Sinir Ağları, Rastgele Orman, AdaBoost, Gradyan Arttırma ve Doğrusal Ayrımçılık Analizi algoritmalarını kullanmışlardır. AdaBoost algoritması ile eğitilen model ile %99,88 doğruluk, %93,13 F1 skor, %91,14 hatırlama ve %96,22 kesinlik sonucu elde etmişlerdir [36].

Karataş, yazmış olduğu doktora tezinde, CSE-CIC-IDS2018 veri setini kullanarak makine öğrenmesi ve derin öğrenme algoritmaları ile saldırı tespiti çalışması yapmıştır. Veri setindeki dengesizliği azaltmak için sentetik veri örnekleme modelini kullanmıştır. Karar Ağacı, Rastgele Orman, K En Yakın Komşu, AdaBoost, Gradyan Arttırma ve Doğrusal Diskriminant Analizi makine öğrenmesi algoritmaları ve CNN, RNN, BiRNN LSTM, BiLSTM, CNN-LSTM, GRU ve DAE derin öğrenmesi algoritmalarını kullanmıştır. Makine öğrenmesi algoritmaları arasından, örnekleme yapmadan aldığı sonuçlar içerisinde en başarılı sonucu %99,69 doğruluk, %99,70 kesinlik, %99,69 hatırlama ve %99,70 F1 skor değerleri ile AdaBoost algoritması vermiştir. Örnekleme yaptıktan sonra en başarılı sonucu %99,60 doğruluk, %99,60 kesinlik, %99,61 hatırlama ve %99,60 F1 skor değerleri ile yine AdaBoost algoritması vermiştir [37].

2. MATERYAL ve YÖNTEM

2.1 Çalışmada Kullanılan Veriler

Bu çalışmada kullanılan veriler CIC-DDoS2019 ve CSE-CIC-IDS2018 veri setlerinden elde edilmiştir. CIC-DDoS2019 veri setindeki normal veri trafiği sayısı az miktardadır. Normal trafik verisi veri miktarını arttırabilmek için CSE-CIC-IDS2018 veri setinden yararlanılmıştır. Saldırıları tespit edecek modeli eğitirken kullanılan veri ne kadar gerçeğe uygun ve düzgün hazırlanırsa alınacak sonuçlar da o kadar iyi olacaktır. CIC-DDoS2019

veri seti, gerçek network ekipmanları kullanılarak üretilmiştir. Model eğitimi ve model testi için farklı günlerde veri trafiği üretilmiştir [10].

Özniteliklerin belirlenmesi, modellerin eğitimi ve 1. testi için kullanılan dosyalar Tablo 2.1’de verilmiştir.

Tablo 2.1 *Özniteliklerin belirlenmesi, modellerin eğitimi ve 1. testi için kullanılan veri setleri ve dosyalar*

Veri Seti	Dosya Adı
CSE-CIC-IDS2018	Friday-16-02-2018
CSE-CIC-IDS2018	Wednesday-21-02-2018
CIC-DDoS2019	DrDoS_NTP (ilk 838000 veri)
CIC-DDoS2019	DrDoS_DNS (ilk 825000 veri)
CIC-DDoS2019	DrDoS_MSSQL (ilk 825000 veri)
CIC-DDoS2019	DrDoS_SNMP (ilk 825000 veri)
CIC-DDoS2019	DrDoS_UDP (ilk 825000 veri)

Dosyalardan okunan veriler bazı veri ön işleme işlemlerinden geçirilmiştir. Normal trafik, NTP DDoS, DNS DDoS, MSSQL DDoS, SNMP DDoS veya UDP DDoS’a ait olmayan veriler özniteliklerin belirlenmesinde, model eğitiminde ve ilk testinde kullanılmamıştır. Modelin yanlış sonuç vermemesi için model eğitiminde kullanılan veri setindeki veri türü örnek sayıları arasında çok fazla fark bulunmaması gerekmektedir. Tablo 2.2’de özniteliklerin belirlenmesi, modellerin eğitimi ve 1. testinde kullanılan veri türü örnek sayıları verilmiştir.

Tablo 2.2 *Özniteliklerin belirlenmesi, modellerin eğitimi ve 1. testi için kullanılan veri türü örnek sayıları*

Veri Türü	Örnek Sayısı
Normal Trafik Verisi	825753
NTP DDoS Verisi	824535
DNS DDoS Verisi	823045
MSSQL DDoS Verisi	824029
SNMP DDoS Verisi	824324
UDP DDoS Verisi	823919

Tablo 2.2 devam Özniteliklerin belirlenmesi, modellerin eğitimi ve 1. testi için kullanılan veri türü örnek sayıları

TOPLAM	4945605
--------	---------

Modellerin 2. testi için kullanılan dosyalar Tablo 2.3'te verilmiştir.

Tablo 2.3 Modellerin 2. testi için kullanılan veri setleri ve dosyalar

Veri Seti	Dosya Adı
CSE-CIC-IDS2018	Friday-23-02-2018 (ilk 325000 veri)
CIC-DDoS2019	MSSQL_test (ilk 325000 veri)
CIC-DDoS2019	UDP_test (ilk 365000 veri)

Dosyalardan okunan veriler bazı veri ön işleme işlemlerinden geçirilmiştir. Normal trafik, MSSQL DDoS veya UDP DDoS'a ait olmayan veriler modellerin 2. testinde kullanılmamıştır. Tablo 2.4'te modellerin 2. testinde kullanılan veri türü örnek sayıları verilmiştir.

Tablo 2.4 Modellerin 2. testi için kullanılan veri türü örnek sayıları

Veri Türü	Örnek Sayısı
Normal Trafik Verisi	326809
UDP DDoS Verisi	338867
MSSQL DDoS Verisi	338827
TOPLAM	1004503

Modellerin LDAP DDoS saldırısı ile testi için kullanılan dosya Tablo 2.5'te verilmiştir.

Tablo 2.5 Modellerin LDAP DDoS saldırısı ile testi için kullanılan veri seti ve dosya

Veri Seti	Dosya Adı
CIC-DDoS2019	DrDoS_LDAP (ilk 825000 veri)

Dosyalardan okunan veriler bazı veri ön işleme işlemlerinden geçirilmiştir. LDAP DDoS'a ait olmayan veriler modellerin LDAP DDoS saldırısı ile testinde kullanılmamıştır. Tablo 2.6'da modellerin LDAP DDoS saldırısı ile testinde kullanılan veri türü örnek sayısı verilmiştir.

Tablo 2.6 Modellerin LDAP DDoS saldırısı ile testi için kullanılan veri türü örnek sayısı

Veri Türü	Örnek Sayısı
LDAP DDoS Verisi	824352

2.2 Model Değerlendirme Yöntemleri ve Metrikleri

2.2.1 Karmaşıklık matrisi

Karmaşıklık matrisi bir modelin değerlendirmesini yaparken kullanılan yöntemlerden biridir. Modelin yaptığı sınıflandırma tahminlerini bu matrise bakarak görmek mümkündür. Saldırı ve normal trafik verilerini içeren 2 sınıflı bir veri seti için karmaşıklık matrisinde 4 farklı ihtimal bulunmaktadır. Bunlar doğru pozitif (DP), doğru negatif (DN), yanlış pozitif (YP) ve yanlış negatif (YN) ihtimalleridir. Doğru pozitif, saldırı olan bir verinin model tarafından saldırı olarak tahmin edilmesi durumudur. Doğru negatif, normal olan bir verinin model tarafından normal olarak tahmin edilmesi durumudur. Yanlış pozitif, normal olan bir verinin model tarafından saldırı olarak tahmin edilmesi durumudur. Yanlış negatif ise saldırı olan bir verinin model tarafından normal olarak tahmin edilmesi durumudur [6].

2.2.2 Kesinlik metriği

Modelin pozitif olarak tahmin ettiği veriler içerisinde gerçekte kaç tanesinin pozitif olduğunu belirtir. Doğru pozitiflerin, doğru pozitif ve yanlış pozitiflerin toplamına bölünmesiyle elde edilir [38].

2.2.3 Hatırlama metriği

Gerçekte pozitif olanlardan kaç tanesinin algoritma tarafından tespit edilebildiğini belirtir. Doğru pozitiflerin, doğru pozitif ve yanlış negatiflerin toplamına bölünmesiyle elde edilir [38].

2.2.4 F1 Skor metriği

Kesinlik ve hatırlama metriklerini kullanarak modelin performansı hakkında bilgi verir. Kesinlik ve hatırlama metriklerinin harmonik ortalaması alınarak elde edilir [38].

2.2.5 Doğruluk metriği

Doğru pozitif ve doğru negatiflerin toplamının, bütün tahminlerin sayısına bölünmesiyle elde edilir. Veri türü örnek sayılarının dengeli olmadığı veri setlerinde kullanılması uygun değildir [38].

2.2.6 Çapraz doğrulama metodu

Makine öğrenmesi algoritmaları ile model eğitimi ve test işlemleri için verileri eğitim ve test verisi olarak ayırmak gerekmektedir. Test için kullanılacak veri, model eğitilirken modele de girdi olarak verilmesi durumunda modelimiz o veriyi ezberleyecektir. Bu durumda modelimiz o test kümesi ile çok başarılı sonuçlar veriyor gibi gözükmesine rağmen daha önce görmediği bir veri kümesi ile test edilirse aslında başarısız olduğu anlaşılabacaktır [39].

Bununla beraber bazı durumlarda modelin testi için ayrılan belirli bölümler çok başarılı sonuç verirken verinin farklı bir yeri test için kullanıldığında başarısız sonuç verebilmektedir. Böyle bir durum olup olmadığını anlayabilmek için çapraz doğrulama metodu ile modelimizi test etmek faydalıdır. Çapraz doğrulama metodu Monte Carlo metotlarından bir tanesidir [40].

2.3 Model Eğitimi İçin Özniteliklerin Belirlenmesi

Modeli eğitmek için öncelikle kullanılacak özniteliklerin seçilmesi gerekmektedir. Özniteliklerin isimleri GitHub'ta bulunan bir web sayfasından alınmıştır [41]. Ayrıca bu web sayfasından özniteliklerin tanımları hakkında da bilgi alınabilmektedir. Kullanılan veri setlerinde ortak olmayan öznitelikler bulunmaktadır. Ortak olmayan öznitelikler veri setinden çıkartılmıştır. Modelin karar vermesine katkı sağlamayacak olan hedef port bilgisi, hedef protokol bilgisi ve zaman bilgisi öznitelikleri de veri setinden çıkartılmıştır. Hata alınması sebebiyle Flow Bytes/s ve Flow Packets/s özniteliklerine karşılık gelen sütunlar da veri setinden çıkartılmıştır. Yapılan bu işlemlerin ardından veri setinde bir tanesi etiket olmak üzere toplamda 75 adet öznitelik bulunmaktadır. 75 adet öznitelik içerisinde her bir sınıf için en önemli 10 öznitelik ve tüm sınıflar dahil olduğundaki en önemli 20 öznitelik belirlendi. Bu işlemler Random Forest sınıflandırıcısının feature_importances_ isimli özelliği kullanılarak yapılmıştır.

2.3.1 Normal trafik tespiti için en önemli 10 öznelik

Bütün veri, normal trafik ve normal olmayan trafik olmak üzere 2 sınıfa ayrıldı. Ardından tüm verinin %30'u test için %70'i ise eğitim için ayrıldı. Model Random Forest algoritmasıyla eğitildi ve test edildi.

Normal trafik tespiti için en önemli 10 öznelik ve önem değerleri sırasıyla Tablo 2.7'de gösterilmiştir.

Tablo 2.7 Normal trafik tespiti için en önemli 10 öznelik

	Öznelik	Önem Değeri
1	Subflow Bwd Packets	0.196385
2	Fwd Init Win Bytes	0.099959
3	Packet Length Min	0.098880
4	Fwd Packet Length Min	0.098596
5	Bwd Packets/s	0.098414
6	Total Bwd packets	0.098279
7	Bwd IAT Total	0.098276
8	Bwd IAT Min	0.098233
9	Fwd Packet Length Std	0.096534
10	Bwd IAT Mean	0.001918

Çalışma sonucunda karara etki eden en önemli 3 özneliğin sırasıyla Subflow Bwd Packets, Fwd Init Win Bytes ve Packet Length Min öznelikleri olduğu görülmektedir.

2.3.2 NTP DDoS saldırı tespiti için en önemli 10 öznelik

Bütün veri, NTP DDoS ve NTP DDoS olmayan trafik olmak üzere 2 sınıfa ayrıldı. Ardından tüm verinin %30'u test için %70'i ise eğitim için ayrıldı. Model Random Forest algoritmasıyla eğitildi ve test edildi.

NTP DDoS saldırı tespiti için en önemli 10 öznelik ve önem değerleri sırasıyla Tablo 2.8'de gösterilmiştir.

Tablo 2.8 NTP DDoS saldırı tespiti için en önemli 10 öznitelik

	Öznitelik	Önem Değeri
1	Subflow Fwd Packets	0.159404
2	Fwd IAT Mean	0.087585
3	Total Length of Fwd Packet	0.077471
4	Flow IAT Mean	0.069970
5	Fwd IAT Std	0.067168
6	Fwd Packet Length Max	0.064915
7	Fwd IAT Min	0.061607
8	Flow IAT Min	0.058116
9	FWD Packets/s	0.054225
10	Subflow Fwd Bytes	0.048132

Çalışma sonucunda karara etki eden en önemli 3 öznitelğin sırasıyla Subflow Fwd Packets, Fwd IAT Mean ve Total Length of Fwd Packet öznitelikleri olduğu görülmektedir.

2.3.3 MSSQL DDoS saldırı tespiti için en önemli 10 öznitelik

Bütün veri, MSSQL DDoS ve MSSQL DDoS olmayan trafik olmak üzere 2 sınıfa ayrıldı. Ardından tüm verinin %30'u test için %70'i ise eğitim için ayrıldı. Model Random Forest algoritmasıyla eğitildi ve test edildi.

MSSQL DDoS saldırı tespiti için en önemli 10 öznitelik ve önem değerleri sırasıyla Tablo 2.9'da gösterilmiştir.

Tablo 2.9 MSSQL DDoS saldırı tespiti için en önemli 10 öznitelik

	Öznitelik	Önem Değeri
1	Packet Length Min	0.207198
2	Fwd Segment Size Avg	0.126450
3	Fwd Packet Length Max	0.097938
4	Fwd Packet Length Min	0.075374
5	Total Length of Fwd Packet	0.073481
6	Packet Length Mean	0.060928

Tablo 2.9 devam MSSQL DDoS saldırı tespiti için en önemli 10 öznelik

7	Average Packet Size	0.053828
8	Fwd Packet Length Mean	0.053752
9	Packet Length Max	0.051079
10	Fwd IAT Mean	0.035701

Çalışma sonucunda karara etki eden en önemli 3 özneliğin sırasıyla Packet Length Min, Fwd Segment Size Avg ve Fwd Packet Length Max öznelikleri olduğu görülmektedir.

2.3.4 SNMP DDoS saldırı tespiti için en önemli 10 öznelik

Bütün veri, SNMP DDoS ve SNMP DDoS olmayan trafik olmak üzere 2 sınıfa ayrıldı. Ardından tüm verinin %30'u test için %70'i ise eğitim için ayrıldı. Model Random Forest algoritmasıyla eğitildi ve test edildi.

SNMP DDoS saldırı tespiti için en önemli 10 öznelik ve önem değerleri sırasıyla Tablo 2.10'da gösterilmiştir.

Tablo 2.10 SNMP DDoS saldırı tespiti için en önemli 10 öznelik

	Öznelik	Önem Değeri
1	Total Length of Fwd Packet	0.104685
2	Flow IAT Max	0.102524
3	Packet Length Mean	0.091918
4	Packet Length Max	0.088229
5	Packet Length Min	0.085718
6	Fwd Segment Size Avg	0.063604
7	Average Packet Size	0.058083
8	Fwd IAT Total	0.055433
9	Fwd Packet Length Mean	0.049740
10	Flow IAT Mean	0.037706

Çalışma sonucunda karara etki eden en önemli 3 özneliğin sırasıyla Total Length of Fwd Packet, Flow IAT Max ve Packet Length Mean öznelikleri olduğu görülmektedir.

2.3.5 UDP DDoS saldırı tespiti için en önemli 10 öznitelik

Bütün veri, UDP DDoS ve UDP DDoS olmayan trafik olmak üzere 2 sınıfa ayrıldı. Ardından tüm verinin %30'u test için %70'i ise eğitim için ayrıldı. Model Random Forest algoritmasıyla eğitildi ve test edildi.

UDP DDoS saldırı tespiti için en önemli 10 öznitelik ve önem değerleri sırasıyla Tablo 2.11'de gösterilmiştir.

Tablo 2.11 UDP DDoS saldırı tespiti için en önemli 10 öznitelik

	Öznitelik	Önem Değeri
1	Fwd Packet Length Max	0.145453
2	Fwd Packet Length Mean	0.099284
3	Packet Length Max	0.092858
4	Fwd Segment Size Avg	0.091826
5	Average Packet Size	0.068241
6	Packet Length Min	0.057858
7	Fwd IAT Max	0.054192
8	Total Length of Fwd Packet	0.045756
9	Fwd Packet Length Min	0.042235
10	Fwd IAT Total	0.041957

Çalışma sonucunda karara etki eden en önemli 3 özneliğin sırasıyla Fwd Packet Length Max, Fwd Packet Length Mean ve Packet Length Max öznelikleri olduğu görülmektedir.

2.3.6 DNS DDoS saldırı tespiti için en önemli 10 öznitelik

Bütün veri, DNS DDoS ve DNS DDoS olmayan trafik olmak üzere 2 sınıfa ayrıldı. Ardından tüm verinin %30'u test için %70'i ise eğitim için ayrıldı. Model Random Forest algoritmasıyla eğitildi ve test edildi.

DNS DDoS saldırı tespiti için en önemli 10 öznitelik ve önem değerleri sırasıyla Tablo 2.12'de gösterilmiştir.

Tablo 2.12 DNS DDoS saldırı tespiti için en önemli 10 öznitelik

	Öznitelik	Önem Değeri
1	Packet Length Min	0.307645
2	Fwd Packet Length Mean	0.069438
3	Fwd Packet Length Min	0.066388
4	Fwd IAT Max	0.064171
5	Fwd IAT Min	0.062372
6	Packet Length Mean	0.060812
7	Fwd IAT Total	0.047011
8	Total Length of Fwd Packet	0.038820
9	FWD Packets/s	0.035514
10	Average Packet Size	0.032242

Çalışma sonucunda karara etki eden en önemli 3 özniteliğin Packet Length Min, Fwd Packet Length Mean ve Fwd Packet Length Min öznitelikleri olduğu görülmektedir.

2.3.7 Tüm veri türlerinin tespiti için en önemli 20 öznitelik

Bütün verinin %30'u test için %70'i ise eğitim için ayrıldı. Model Random Forest algoritmasıyla eğitildi ve test edildi. Verilerin sınıflandırılmasına etki eden en önemli 20 öznitelik ve önem değerleri Tablo 2.13'te gösterilmiştir.

Tablo 2.13 Tüm veri türlerinin tespiti için en önemli 20 öznitelik

	Öznitelik	Önem Değeri
1	Fwd Packet Length Max	0.093674
2	Total Length of Fwd Packet	0.075703
3	Fwd Packet Length Min	0.062014
4	Fwd Act Data Pkts	0.061967
5	Fwd Packet Length Mean	0.057532
6	Average Packet Size	0.055589
7	Packet Length Min	0.052051
8	Packet Length Max	0.044520

Tablo 2.13 devam *Tüm veri türlerinin tespiti için en önemli 20 öznitelik*

9	Subflow Bwd Packets	0.043109
10	Subflow Fwd Packets	0.042424
11	Packet Length Mean	0.037428
12	Subflow Fwd Bytes	0.037301
13	Fwd IAT Mean	0.029951
14	Fwd IAT Total	0.028201
15	Fwd IAT Std	0.023255
16	Fwd Packet Length Std	0.021998
17	Fwd Init Win Bytes	0.021736
18	Bwd Packets/s	0.021665
19	Total Bwd packets	0.021620
20	Bwd IAT Total	0.021598

Çalışma sonucunda karara etki eden en önemli 3 özneliğin sırasıyla Fwd Packet Length Max, Total Length of Fwd Packet ve Fwd Packet Length Min öznelikleri olduğu görülmektedir.

2.3.8 Model eğitiminde kullanılan öznelikler

Yapılan çalışmaların sonucunda yukarda elde edilen tablolardaki öznelikler birleştirilmiş ve modellerin eğitiminde ve testinde kullanılmıştır. Tabloların birleştirilmesiyle 29 farklı öznelik elde edilmiştir. Sınıf türünü içeren etiket özneliğiyle birlikte toplamda 30 adet öznelik bulunmaktadır. Bu öznelikler Tablo 2.14’te verilmiştir.

Tablo 2.14 *Model eğitiminde kullanılan öznelikler*

	Öznitelik
1	Etiket
2	Total Length of Fwd Packet
3	Fwd Packet Length Min
4	Fwd Act Data Pkts
5	Fwd Packet Length Mean

Tablo 2.14 devam *Model eğitiminde kullanılan öznitelikler*

6	Average Packet Size
7	Packet Length Min
8	Packet Length Max
9	Subflow Bwd Packets
10	Subflow Fwd Packets
11	Packet Length Mean
12	Subflow Fwd Bytes
13	Fwd IAT Mean
14	Fwd IAT Total
15	Fwd IAT Std
16	Fwd Packet Length Std
17	Fwd Init Win Bytes
18	Bwd Packets/s
19	Total Bwd packets
20	Bwd IAT Total
21	Fwd Packet Length Max
22	Fwd IAT Max
23	Fwd IAT Min
24	FWD Packets/s
25	Fwd Segment Size Avg
26	Flow IAT Max
27	Flow IAT Mean
28	Flow IAT Min
29	Bwd IAT Min
30	Bwd IAT Mean

2.4 Sınıflandırıcıların Çapraz Doğrulama Metodu ile Testi

Eğitim işleminden geçirilmeyen sınıflandırıcılar çapraz doğrulama metodu ile test edilmiştir. Bu test işleminde, Tablo 2.2'deki verilerin %70 eğitim ve %30 test için ayrılmasıyla ortaya çıkan eğitim verileri kullanılmıştır. Çapraz doğrulama metodu ile test

işlemi scikit-learn'ün cross_val_score fonksiyonu kullanılarak yapılmıştır. Bu işlem gerçekleştirilirken StratifiedKFold fonksiyonu kullanılmıştır. StratifiedKFold fonksiyonuna shuffle parametresi True ve n_splits parametresi 5 verilmiştir.

Tablo 2.15'te Random Forest sınıflandırıcısının çapraz doğrulama skoru sonuçları verilmiştir.

Tablo 2.15 Random Forest sınıflandırıcısının çapraz doğrulama skoru sonuçları

Çapraz Doğrulama	Sonuç
1. parça	0.9494
2. parça	0.9490
3. parça	0.9490
4. parça	0.9492
5. parça	0.9496
Ortalama	0.9493

Tablo 2.16'da Decision Tree sınıflandırıcısının çapraz doğrulama skoru sonuçları verilmiştir.

Tablo 2.16 Decision Tree sınıflandırıcısının çapraz doğrulama skoru sonuçları

Çapraz Doğrulama	Sonuç
1. parça	0.9493
2. parça	0.9488
3. parça	0.9487
4. parça	0.9491
5. parça	0.9494
Ortalama	0.9491

Tablo 2.17'de Gaussian Naive Bayes sınıflandırıcısının çapraz doğrulama skoru sonuçları verilmiştir.

Tablo 2.17 *Gaussian Naive Bayes sınıflandırıcısının çapraz doğrulama skoru sonuçları*

Çapraz Doğrulama	Sonuç
1. parça	0.6442
2. parça	0.6412
3. parça	0.6428
4. parça	0.6441
5. parça	0.6489
Ortalama	0.6442

Tablo 2.18’de Extra Trees sınıflandırıcısının çapraz doğrulama skoru sonuçları verilmiştir.

Tablo 2.18 *Extra Trees sınıflandırıcısının çapraz doğrulama skoru sonuçları*

Çapraz Doğrulama	Sonuç
1. parça	0.9495
2. parça	0.9490
3. parça	0.9489
4. parça	0.9492
5. parça	0.9497
Ortalama	0.9493

Tablo 2.19’da AdaBoost sınıflandırıcısının çapraz doğrulama skoru sonuçları verilmiştir.

Tablo 2.19 *AdaBoost sınıflandırıcısının çapraz doğrulama skoru sonuçları*

Çapraz Doğrulama	Sonuç
1. parça	0.8059
2. parça	0.7603
3. parça	0.7268
4. parça	0.8097
5. parça	0.8268
Ortalama	0.7859

Tablo 2.20’de Gradient Boosting sınıflandırıcısının çapraz doğrulama skoru sonuçları verilmiştir.

Tablo 2.20 Gradient Boosting sınıflandırıcısının çapraz doğrulama skoru sonuçları

Çapraz Doğrulama	Sonuç
1. parça	0.9424
2. parça	0.9424
3. parça	0.9426
4. parça	0.9430
5. parça	0.9429
Ortalama	0.9427

Çapraz doğrulama skoru sonuçlarına bakıldığında Random Forest, Decision Tree, Gaussian Naive Bayes, Extra Trees, ve Gradient Boosting sınıflandırıcılarındaki parçaların sonuçlarının birbirine yakın olduğu görülmektedir. AdaBoost sınıflandırıcısındaki parçaların sonuçları arasında diğer sınıflandırıcılara göre daha fazla fark bulunmaktadır.

2.5 Modellerin Eğitilmesi ve Test Edilmesi

Modellerin eğitiminde 6 farklı makine öğrenmesi sınıflandırma algoritması kullanılmıştır. Bu algoritmalar Random Forest, Decision Tree, Gaussian Naive Bayes, Extra Trees, AdaBoost ve Gradient Boosting algoritmalarıdır. Modellerin kesinlik, hatırlama ve F1 skor metrik sonuçları hesaplanırken average parametresi weighted olarak verilmiştir.

2.5.1 Modellerin eğitilmesi ve 1. testi

Bu bölümde modelin eğitimi ve testi için toplam 4945605 adet trafik verisi kullanılmıştır. Veriler %70 eğitim için ve %30 test için ayrılmıştır. Modellerin eğitimi ve 1. testi için kullanılan veri sayıları Tablo 2.21’de verilmiştir.

Tablo 2.21 Modellerin eğitimi ve 1. testi için kullanılan veri sayıları

Ayrılma Amacı	Veri Sayısı
Eğitim Amaçlı	3461923
Test Amaçlı	1483682
TOPLAM	4945605

Ayrılma işleminden sonra eğitim için kullanılan veri sayıları Tablo 2.22’de gösterilmiştir.

Tablo 2.22 Modellerin eğitimi için kullanılan veri sayıları

Eğitim Veri Türü	Veri Sayısı
Normal Trafik Verisi	577910
NTP DDoS Verisi	577675
DNS DDoS Verisi	576675
MSSQL DDoS Verisi	575754
SNMP DDoS Verisi	577574
UDP DDoS Verisi	576335
TOPLAM	3461923

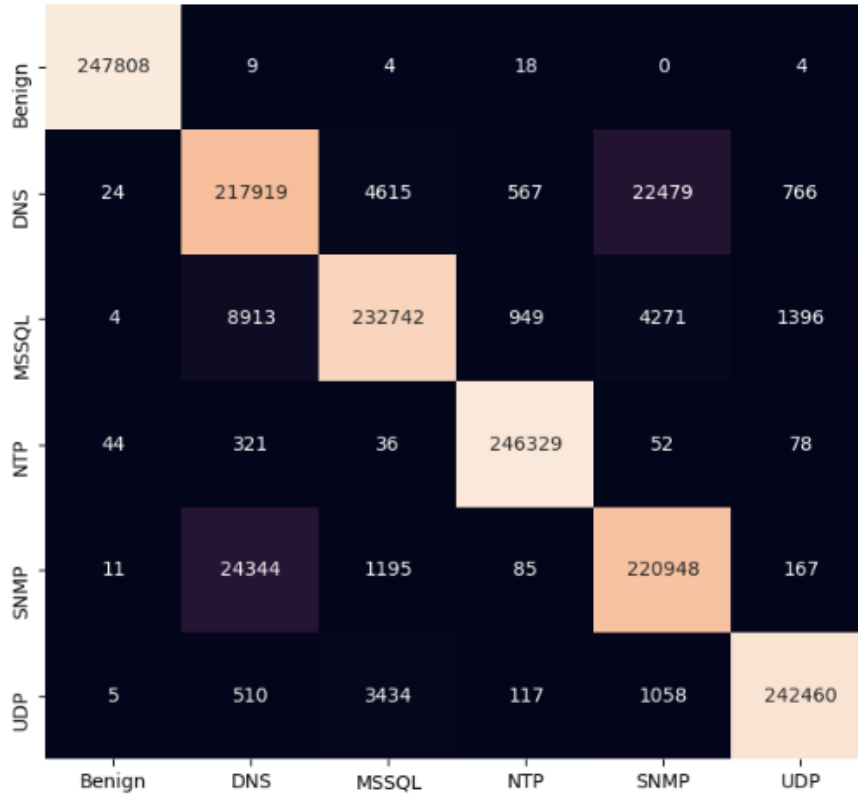
Ayrılma işleminden sonra 1. test için kullanılan veri sayıları Tablo 2.23’te gösterilmiştir.

Tablo 2.23 Modellerin 1. testi için kullanılan veri sayıları

Test Veri Türü	Veri Sayısı
Normal Trafik Verisi	247843
NTP DDoS Verisi	246860
DNS DDoS Verisi	246370
MSSQL DDoS Verisi	248275
SNMP DDoS Verisi	246750
UDP DDoS Verisi	247584
TOPLAM	1483682

2.5.1.1 Random Forest algoritması ile model eğitimi ve eğitilen modelin 1. testi

Verilerimiz eğitim ve test olarak ayrıldıktan sonra Random Forest algoritmasıyla model eğitilip ardından test edilmiştir. Random Forest algoritması ile eğitilen modelin karmaşıklık matrisi Şekil 2.1’de gösterilmiştir.



Şekil 2.1 Random Forest algoritması ile eğitilen modelin karmaşıklık matrisi

Karmaşıklık matrisi incelendiğinde modelimizin normal trafiği, NTP DDoS saldırısını, MSSQL DDoS saldırısını ve UDP DDoS saldırısını ayırt etme konusunda çok başarılı olduğu görülmektedir. Bununla beraber modelin bazı DNS DDoS verilerini SNMP DDoS olarak tahmin ettiği ve bazı SNMP DDoS verilerini de DNS DDoS olarak tahmin ettiği görülmektedir.

Modelin metrik sonuçları Tablo 2.24'te verilmiştir.

Tablo 2.24 Random Forest algoritması ile eğitilen modelin 1. test metrik sonuçları

Metrik	Sonuç
Doğruluk:	0.9491
Kesinlik:	0.9496
Hatırlama:	0.9491
F1 Skor:	0.9493

Random Forest algoritması ile eğitilen modelin veri türlerine göre kesinlik metriği sonuçları Tablo 2.25'te gösterilmiştir.

Tablo 2.25 *Random Forest algoritması ile eğitilen modelin veri türlerine göre 1. test kesinlik metriği sonucu*

Kesinlik	Sonuç
Normal Trafik Verisi	0.9996
DNS DDoS Verisi	0.8647
MSSQL DDoS Verisi	0.9616
NTP DDoS Verisi	0.9930
SNMP DDoS Verisi	0.8880
UDP DDoS Verisi	0.9902

Random Forest algoritması ile eğitilen modelin veri türlerine göre hatırlama metriği sonuçları Tablo 2.26’da gösterilmiştir.

Tablo 2.26 *Random Forest algoritması ile eğitilen modelin veri türlerine göre 1. test hatırlama metriği sonucu*

Hatırlama	Sonuç
Normal Trafik Verisi	0.9999
DNS DDoS Verisi	0.8845
MSSQL DDoS Verisi	0.9374
NTP DDoS Verisi	0.9978
SNMP DDoS Verisi	0.8954
UDP DDoS Verisi	0.9793

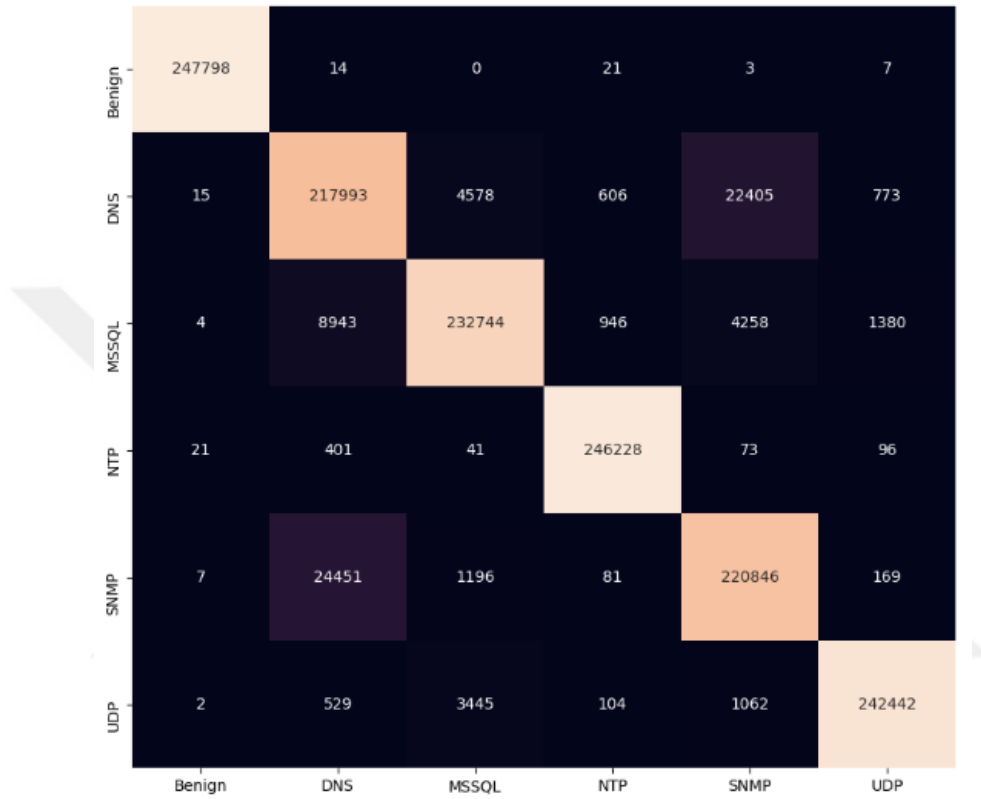
Random Forest algoritması ile eğitilen modelin veri türlerine göre F1 skor metriği sonuçları Tablo 2.27’de gösterilmiştir.

Tablo 2.27 *Random Forest algoritması ile eğitilen modelin veri türlerine göre 1. test F1 skor metriği sonucu*

F1 Skor	Sonuç
Normal Trafik Verisi	0.9998
DNS DDoS Verisi	0.8745
MSSQL DDoS Verisi	0.9494
NTP DDoS Verisi	0.9954
SNMP DDoS Verisi	0.8917
UDP DDoS Verisi	0.9847

2.5.1.2 Decision Tree algoritması ile model eğitimi ve eğitilen modelin 1. testi

Verilerimiz eğitim ve test olmak üzere ayrıldıktan sonra Decision Tree algoritmasıyla model eğitilip ardından test edilmiştir. Decision Tree algoritması ile eğitilen modelin karmaşıklık matrisi Şekil 2.2’de gösterilmiştir.



Şekil 2.2 Decision Tree algoritması ile eğitilen modelin karmaşıklık matrisi

Karmaşıklık matrisi incelendiğinde modelimizin normal trafiği, NTP DDoS saldırısını, MSSQL DDoS saldırısını ve UDP DDoS saldırısını ayırt etme konusunda çok başarılı olduğu görülmektedir. Bununla beraber modelin bazı DNS DDoS verilerini SNMP DDoS olarak tahmin ettiği ve bazı SNMP DDoS verilerini de DNS DDoS olarak tahmin ettiği görülmektedir.

Modelin metrik sonuçları Tablo 2.28’de verilmiştir.

Tablo 2.28 Decision Tree algoritması ile eğitilen modelin 1. test metrik sonuçları

Metrik	Sonuç
Doğruluk:	0.9490
Kesinlik:	0.9495

Tablo 2.28 devam *Decision Tree algoritması ile eğitilen modelin 1. test metrik sonuçları*

Hatırlama:	0.9490
F1 Skor:	0.9492

Decision Tree algoritması ile eğitilen modelin veri türlerine göre kesinlik metriği sonuçları Tablo 2.29’da gösterilmiştir.

Tablo 2.29 *Decision Tree algoritması ile eğitilen modelin veri türlerine göre 1. test kesinlik metriği sonucu*

Kesinlik	Sonuç
Normal Trafik Verisi	0.9998
DNS DDoS Verisi	0.8639
MSSQL DDoS Verisi	0.9617
NTP DDoS Verisi	0.9929
SNMP DDoS Verisi	0.8882
UDP DDoS Verisi	0.9901

Decision Tree algoritması ile eğitilen modelin veri türlerine göre hatırlama metriği sonuçları Tablo 2.30’da gösterilmiştir.

Tablo 2.30 *Decision Tree algoritması ile eğitilen modelin veri türlerine göre 1. test hatırlama metriği sonucu*

Hatırlama	Sonuç
Normal Trafik Verisi	0.9998
DNS DDoS Verisi	0.8848
MSSQL DDoS Verisi	0.9374
NTP DDoS Verisi	0.9974
SNMP DDoS Verisi	0.8950
UDP DDoS Verisi	0.9792

Decision Tree algoritması ile eğitilen modelin veri türlerine göre F1 skor metriği sonuçları Tablo 2.31’de gösterilmiştir.

Tablo 2.31 *Decision Tree algoritması ile eğitilen modelin veri türlerine göre 1. test F1 skor metriği sonucu*

F1 Skor	Sonuç
Normal Trafik Verisi	0.9998
DNS DDoS Verisi	0.8742
MSSQL DDoS Verisi	0.9494
NTP DDoS Verisi	0.9952
SNMP DDoS Verisi	0.8916
UDP DDoS Verisi	0.9846

2.5.1.3 Gaussian Naive Bayes algoritması ile model eğitimi ve eğitilen modelin 1. testi

Verilerimiz eğitim ve test olmak üzere ayrıldıktan sonra Gaussian Naive Bayes algoritmasıyla model eğitilip ardından test edilmiştir. Gaussian Naive Bayes algoritması ile eğitilen modelin karmaşıklık matrisi Şekil 2.3'te gösterilmiştir.



Şekil 2.3 *Gaussian Naive Bayes algoritması ile eğitilen modelin karmaşıklık matrisi*

Modelin metrik sonuçları Tablo 2.32’de verilmiştir.

Tablo 2.32 Gaussian Naive Bayes algoritması ile eğitilen modelin 1. test metrik sonuçları

Metrik	Sonuç
Doğruluk:	0.6460
Kesinlik:	0.7101
Hatırlama:	0.6460
F1 Skor:	0.6016

Gaussian Naive Bayes algoritması ile eğitilen modelin veri türlerine göre kesinlik metriği sonuçları Tablo 2.33’te gösterilmiştir.

Tablo 2.33 Gaussian Naive Bayes algoritması ile eğitilen modelin veri türlerine göre 1. test kesinlik metriği sonucu

Kesinlik	Sonuç
Normal Trafik Verisi	0.9966
DNS DDoS Verisi	0.7052
MSSQL DDoS Verisi	0.5411
NTP DDoS Verisi	0.9729
SNMP DDoS Verisi	0.4181
UDP DDoS Verisi	0.6265

Gaussian Naive Bayes algoritması ile eğitilen modelin veri türlerine göre hatırlama metriği sonuçları Tablo 2.34’te gösterilmiştir.

Tablo 2.34 Gaussian Naive Bayes algoritması ile eğitilen modelin veri türlerine göre 1. test hatırlama metriği sonucu

Hatırlama	Sonuç
Normal Trafik Verisi	0.9808
DNS DDoS Verisi	0.0009
MSSQL DDoS Verisi	0.9077
NTP DDoS Verisi	0.7072
SNMP DDoS Verisi	0.7159
UDP DDoS Verisi	0.5593

Gaussian Naive Bayes algoritması ile eğitilen modelin veri türlerine göre F1 skor metriği sonuçları Tablo 2.35'te gösterilmiştir.

Tablo 2.35 Gaussian Naive Bayes algoritması ile eğitilen modelin veri türlerine göre 1. test F1 skor metriği sonucu

F1 Skor	Sonuç
Normal Trafik Verisi	0.9887
DNS DDoS Verisi	0.0019
MSSQL DDoS Verisi	0.6780
NTP DDoS Verisi	0.8190
SNMP DDoS Verisi	0.5279
UDP DDoS Verisi	0.5910

2.5.1.4 Extra Trees algoritması ile model eğitimi ve eğitilen modelin 1. Testi

Verilerimiz eğitim ve test olmak üzere ayrıldıktan sonra Extra Trees algoritmasıyla model eğitilip ardından test edilmiştir. Extra Trees algoritması ile eğitilen modelin karmaşıklık matrisi Şekil 2.4'te gösterilmiştir.



Şekil 2.4 Extra Trees algoritması ile eğitilen modelin karmaşıklık matrisi

Karmaşıklık matrisi incelendiğinde modelimizin normal trafiği, NTP DDoS saldırısını, MSSQL DDoS saldırısını ve UDP DDoS saldırısını ayırt etme konusunda çok başarılı olduğu görülmektedir. Bununla beraber modelin bazı DNS DDoS verilerini SNMP DDoS olarak tahmin ettiği ve bazı SNMP DDoS verilerini de DNS DDoS olarak tahmin ettiği görülmektedir.

Modelin metrik sonuçları Tablo 2.36’da verilmiştir.

Tablo 2.36 *Extra Trees algoritması ile eğitilen modelin 1. test metrik sonuçları*

Metrik	Sonuç
Doğruluk:	0.9492
Kesinlik:	0.9497
Hatırlama:	0.9492
F1 Skor:	0.9494

Extra Trees algoritması ile eğitilen modelin veri türlerine göre kesinlik metriği sonuçları Tablo 2.37’de gösterilmiştir.

Tablo 2.37 *Extra Trees algoritması ile eğitilen modelin veri türlerine göre 1. test kesinlik metriği sonucu*

Kesinlik	Sonuç
Normal Trafik Verisi	0.9996
DNS DDoS Verisi	0.8643
MSSQL DDoS Verisi	0.9620
NTP DDoS Verisi	0.9929
SNMP DDoS Verisi	0.8884
UDP DDoS Verisi	0.9902

Extra Trees algoritması ile eğitilen modelin veri türlerine göre hatırlama metriği sonuçları Tablo 2.38’de gösterilmiştir.

Tablo 2.38 *Extra Trees algoritması ile eğitilen modelin veri türlerine göre 1. test hatırlama metriği sonucu*

Hatırlama	Sonuç
Normal Trafik Verisi	0.9998
DNS DDoS Verisi	0.8851

Tablo 2.38 devam Extra Trees algoritması ile eğitilen modelin veri türlerine göre 1. test hatırlama metriği sonucu

MSSQL DDoS Verisi	0.9375
NTP DDoS Verisi	0.9978
SNMP DDoS Verisi	0.8951
UDP DDoS Verisi	0.9793

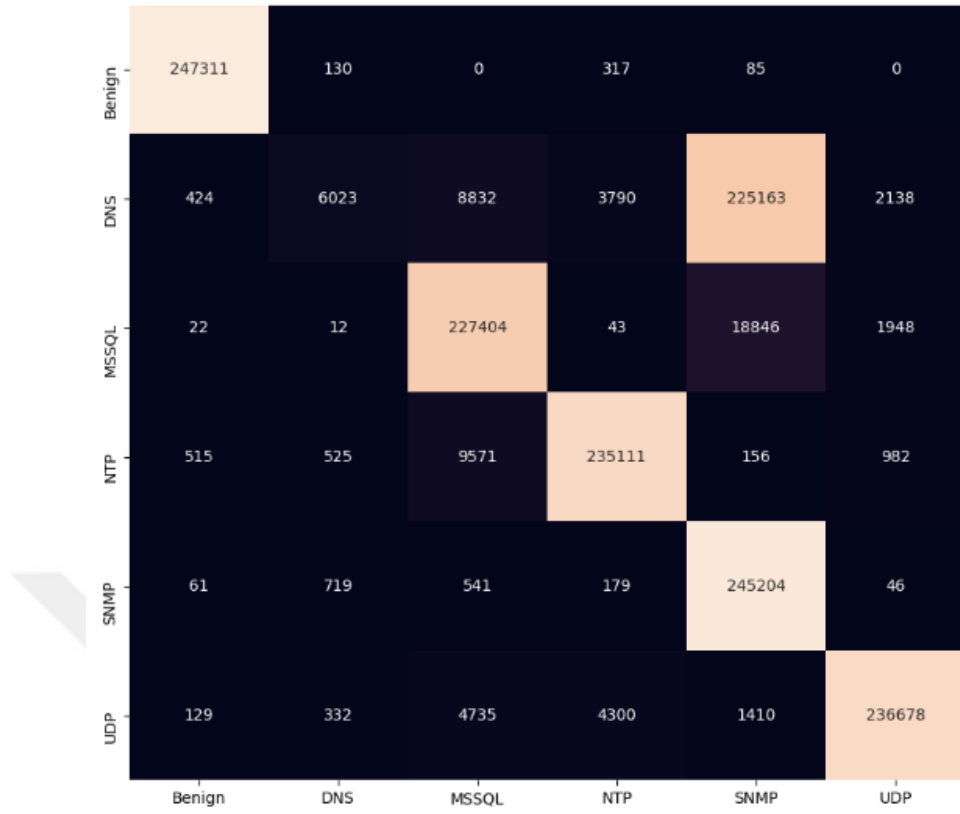
Extra Trees algoritması ile eğitilen modelin veri türlerine göre F1 skor metriği sonuçları Tablo 2.39’da gösterilmiştir.

Tablo 2.39 Extra Trees algoritması ile eğitilen modelin veri türlerine göre 1. test F1 skor metriği sonucu

F1 Skor	Sonuç
Normal Trafik Verisi	0.9997
DNS DDoS Verisi	0.8746
MSSQL DDoS Verisi	0.9496
NTP DDoS Verisi	0.9953
SNMP DDoS Verisi	0.8917
UDP DDoS Verisi	0.9847

2.5.1.5 AdaBoost algoritması ile model eğitimi ve eğitilen modelin 1. testi

Verilerimiz eğitim ve test olmak üzere ayrıldıktan sonra AdaBoost algoritmasıyla model eğitilip ardından test edilmiştir. AdaBoost algoritması ile eğitilen modelin karmaşıklık matrisi Şekil 2.5’te gösterilmiştir.



Şekil 2.5 AdaBoost algoritması ile eğitilen modelin karmaşıklık matrisi

Karmaşıklık matrisi incelendiğinde modelimizin DNS DDoS ve SNMP DDoS sınıflandırması haricinde başarılı olduğu görülmektedir.

Modelin metrik sonuçları Tablo 2.40’da verilmiştir.

Tablo 2.40 AdaBoost algoritması ile eğitilen modelin 1. test metrik sonuçları

Metrik	Sonuç
Doğruluk:	0.8073
Kesinlik:	0.8539
Hatırlama:	0.8073
F1 Skor:	0.7582

AdaBoost algoritması ile eğitilen modelin veri türlerine göre kesinlik metriği sonuçları Tablo 2.41’de gösterilmiştir.

Tablo 2.41 AdaBoost algoritması ile eğitilen modelin veri türlerine göre 1. test kesinlik metriği sonucu

Kesinlik	Sonuç
Normal Trafik Verisi	0.9954
DNS DDoS Verisi	0.7781
MSSQL DDoS Verisi	0.9057
NTP DDoS Verisi	0.9646
SNMP DDoS Verisi	0.4995
UDP DDoS Verisi	0.9788

AdaBoost algoritması ile eğitilen modelin veri türü için hatırlama metriği sonuçları Tablo 2.42’de gösterilmiştir.

Tablo 2.42 AdaBoost algoritması ile eğitilen modelin veri türlerine göre 1. test hatırlama metriği sonucu

Hatırlama	Sonuç
Normal Trafik Verisi	0.9979
DNS DDoS Verisi	0.0244
MSSQL DDoS Verisi	0.9159
NTP DDoS Verisi	0.9524
SNMP DDoS Verisi	0.9937
UDP DDoS Verisi	0.9560

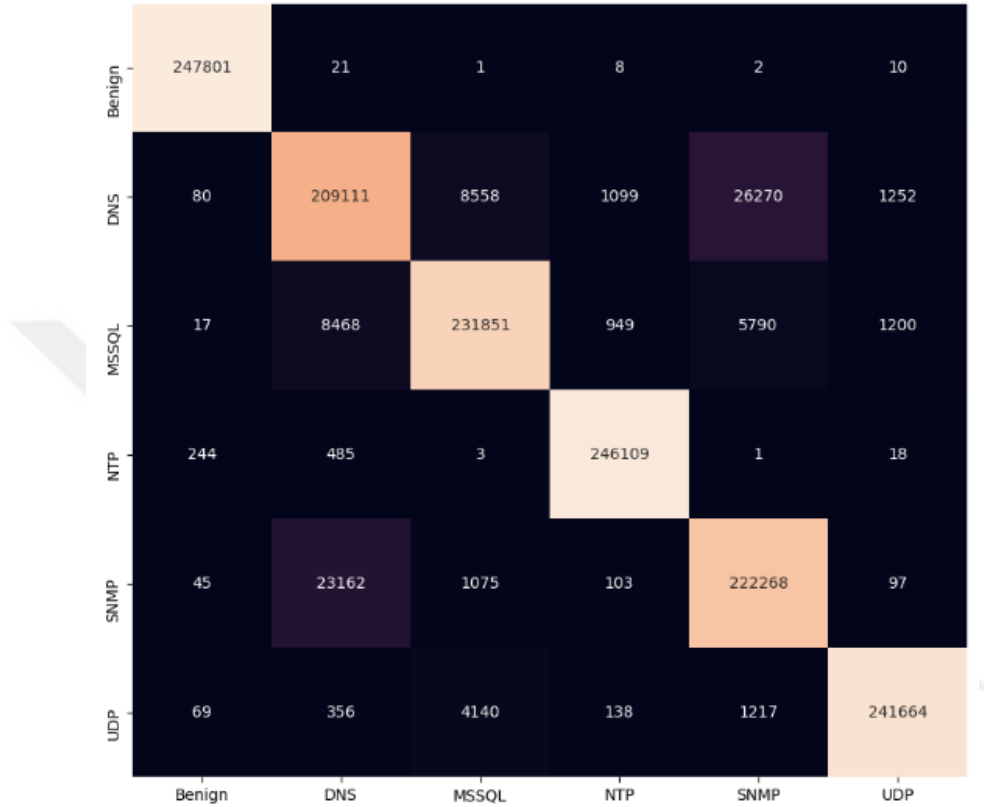
AdaBoost algoritması ile eğitilen modelin veri türlerine göre F1 skor metriği sonuçları Tablo 2.43’te gösterilmiştir.

Tablo 2.43 AdaBoost algoritması ile eğitilen modelin veri türlerine göre 1. test F1 skor metriği sonucu

F1 Skor	Sonuç
Normal Trafik Verisi	0.9966
DNS DDoS Verisi	0.0474
MSSQL DDoS Verisi	0.9108
NTP DDoS Verisi	0.9585
SNMP DDoS Verisi	0.6649
UDP DDoS Verisi	0.9673

2.5.1.6 Gradient Boosting algoritması ile model eğitimi ve eğitilen modelin 1. testi

Verilerimiz eğitim ve test olmak üzere ayrıldıktan sonra Gradient Boosting algoritmasıyla model eğitilip ardından test edilmiştir. Gradient Boosting algoritması ile eğitilen modelin karmaşıklık matrisi Şekil 2.6’da gösterilmiştir.



Şekil 2.6 Gradient Boosting algoritması ile eğitilen modelin karmaşıklık matrisi

Karmaşıklık matrisi incelendiğinde modelimizin sınıflandırmada genel olarak başarılı olduğu söylenebilmektedir. DNS DDoS ve SNMP DDoS sınıflandırması diğerlerine göre daha az başarılı olduğu görülmektedir.

Modelin metrik sonuçları Tablo 2.44’te verilmiştir.

Tablo 2.44 Gradient Boosting algoritması ile eğitilen modelin 1. test metrik sonuçları

Metrik	Sonuç
Doğruluk:	0.9428
Kesinlik:	0.9430
Hatırlama:	0.9428
F1 Skor:	0.9428

Gradient Boosting algoritması ile eğitilen modelin veri türlerine göre kesinlik metriği sonuçları Tablo 2.45'te gösterilmiştir.

Tablo 2.45 Gradient Boosting algoritması ile eğitilen modelin veri türlerine göre 1. test kesinlik metriği sonucu

Kesinlik	Sonuç
Normal Trafik Verisi	0.9982
DNS DDoS Verisi	0.8655
MSSQL DDoS Verisi	0.9439
NTP DDoS Verisi	0.9908
SNMP DDoS Verisi	0.8698
UDP DDoS Verisi	0.9894

Gradient Boosting algoritması ile eğitilen modelin veri türlerine göre kesinlik metriği sonuçları Tablo 2.46'da gösterilmiştir.

Tablo 2.46 Gradient Boosting algoritması ile eğitilen modelin veri türlerine göre 1. test hatırlama metriği sonucu

Hatırlama	Sonuç
Normal Trafik Verisi	0.9998
DNS DDoS Verisi	0.8488
MSSQL DDoS Verisi	0.9338
NTP DDoS Verisi	0.9970
SNMP DDoS Verisi	0.9008
UDP DDoS Verisi	0.9761

Gradient Boosting algoritması ile eğitilen modelin veri türlerine göre kesinlik metriği sonuçları Tablo 2.47'de gösterilmiştir.

Tablo 2.47 Gradient Boosting algoritması ile eğitilen modelin veri türlerine göre 1. test F1 skor metriği sonucu

F1 Skor	Sonuç
Normal Trafik Verisi	0.9990
DNS DDoS Verisi	0.8571
MSSQL DDoS Verisi	0.9389
NTP DDoS Verisi	0.9938

Tablo 2.47 devam Gradient Boosting algoritması ile eğitilen modelin veri türlerine göre 1. test F1 skor metriği sonucu

SNMP DDoS Verisi	0.8850
UDP DDoS Verisi	0.9827

2.5.2 Modellerin 2. testi

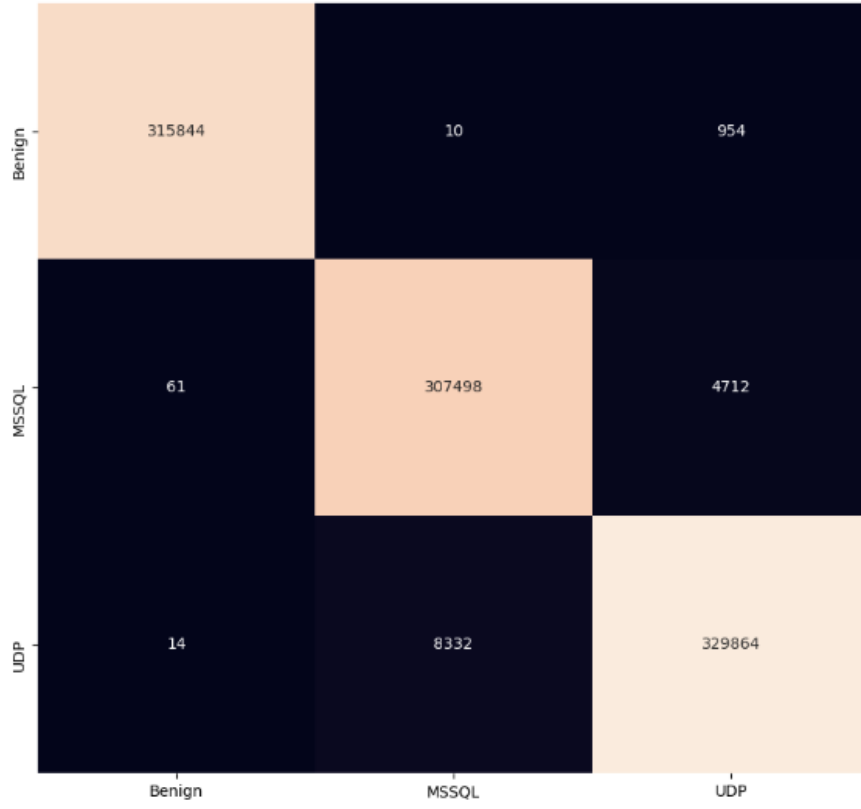
Modellerin 2. testi için kullanılan veri sayıları Tablo 2.48’de verilmiştir.

Tablo 2.48 Modellerin 2. testi için kullanılan veri sayıları

Veri Türü	Örnek Sayısı
Normal Trafik Verisi	326809
UDP DDoS Verisi	338867
MSSQL DDoS Verisi	338827
TOPLAM	1004503

2.5.2.1 Random Forest algoritması ile eğitilen modelin 2. testi

Daha önceden Random Forest algoritmasıyla eğitilen modelin 2. testi gerçekleştirilmiştir. Modelin karmaşıklık matrisi Şekil 2.7’de gösterilmiştir.



Şekil 2.7 Random Forest algoritması ile eğitilen modelin 2. test sonrası karmaşıklık matrisi

Modelin metrik sonuçları Tablo 2.49’da verilmiştir.

Tablo 2.49 Random Forest algoritması ile eğitilen modelin 2. test metrik sonuçları

Metrik	Sonuç
Doğruluk:	0.9489
Kesinlik:	0.9853
Hatırlama:	0.9489
F1 Skor:	0.9666

Random Forest algoritması ile eğitilen modelin veri türlerine göre kesinlik metriği sonuçları Tablo 2.50’de gösterilmiştir.

Tablo 2.50 *Random Forest algoritması ile eğitilen modelin veri türlerine göre 2. test kesinlik metriği sonuçları*

Kesinlik	Sonuç
Normal Trafik Verisi	0.9998
MSSQL DDoS Verisi	0.9736
UDP DDoS Verisi	0.9831

Random Forest algoritması ile eğitilen modelin veri türlerine göre hatırlama metriği sonuçları Tablo 2.51’de gösterilmiştir.

Tablo 2.51 *Random Forest algoritması ile eğitilen modelin veri türlerine göre 2. test hatırlama metriği sonuçları*

Hatırlama	Sonuç
Normal Trafik Verisi	0.9664
MSSQL DDoS Verisi	0.9075
UDP DDoS Verisi	0.9734

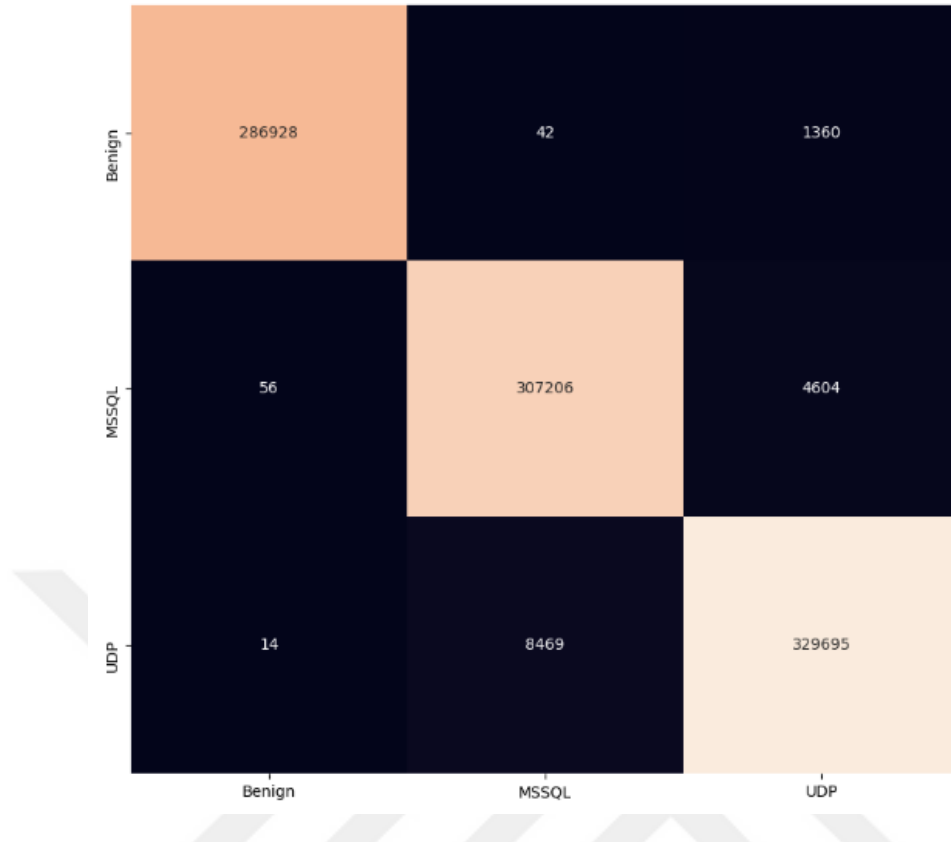
Random Forest algoritması ile eğitilen modelin veri türlerine göre F1 skor metriği sonuçları Tablo 2.52’de gösterilmiştir.

Tablo 2.52 *Random Forest algoritması ile eğitilen modelin veri türlerine göre 2. test F1 skor metriği sonuçları*

F1 Skor	Sonuç
Normal Trafik Verisi	0.9828
MSSQL DDoS Verisi	0.9394
UDP DDoS Verisi	0.9782

2.5.2.2 Decision Tree algoritması ile eğitilen modelin 2. testi

Daha önceden Decision Tree algoritmasıyla eğitilen modelin 2. testi gerçekleştirilmiştir. Modelin karmaşıklık matrisi Şekil 2.8’de gösterilmiştir.



Şekil 2.8 Decision Tree algoritması ile eğitilen modelin 2. test sonrası karmaşıklık matrisi

Modelin metrik sonuçları Tablo 2.53'te verilmiştir.

Tablo 2.53 Decision Tree algoritması ile eğitilen modelin 2. test metrik sonuçları

Metrik	Sonuç
Doğruluk:	0.9197
Kesinlik:	0.9848
Hatırlama:	0.9197
F1 Skor:	0.9506

Decision Tree algoritması ile eğitilen modelin veri türlerine göre kesinlik metriği sonuçları Tablo 2.54'te gösterilmiştir.

Tablo 2.54 *Decision Tree algoritması ile eğitilen modelin veri türlerine göre 2. test kesinlik metriği sonuçları*

Kesinlik	Sonuç
Normal Trafik Verisi	0.9998
MSSQL DDoS Verisi	0.9730
UDP DDoS Verisi	0.9822

Decision Tree algoritması ile eğitilen modelin veri türlerine göre hatırlama metriği sonuçları Tablo 2.55’te gösterilmiştir.

Tablo 2.55 *Decision Tree algoritması ile eğitilen modelin veri türlerine göre 2. test hatırlama metriği sonucu*

Hatırlama	Sonuç
Normal Trafik Verisi	0.8780
MSSQL DDoS Verisi	0.9067
UDP DDoS Verisi	0.9729

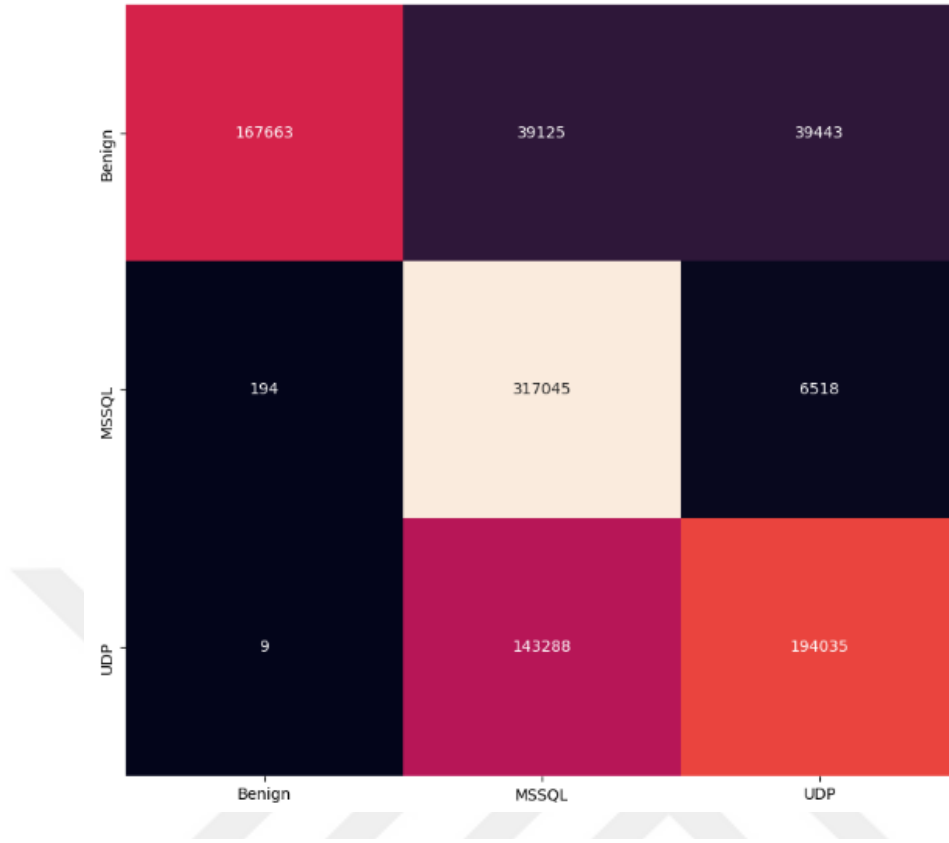
Decision Tree algoritması ile eğitilen modelde veri türlerine göre hatırlama metriği sonuçları Tablo 2.56’da gösterilmiştir.

Tablo 2.56 *Decision Tree algoritması ile eğitilen modelin veri türlerine göre 2. test F1 skor metriği sonucu*

F1 Skor	Sonuç
Normal Trafik Verisi	0.9349
MSSQL DDoS Verisi	0.9387
UDP DDoS Verisi	0.9776

2.5.2.3 Gaussian Naive Bayes algoritması ile eğitilen modelin 2. testi

Daha önceden Gaussian Naive Bayes algoritmasıyla eğitilen modelin 2. testi gerçekleştirilmiştir. Modelin karmaşıklık matrisi Şekil 2.9’da gösterilmiştir.



Şekil 2.9 Gaussian Naive Bayes algoritması ile eğitilen modelin 2. test sonrası karmaşıklık matrisi

Modelin metrik sonuçları Tablo 2.57’de verilmiştir.

Tablo 2.57 Gaussian Naive Bayes algoritması ile eğitilen modelin 2. test metrik sonuçları

Metrik	Sonuç
Doğruluk:	0.6757
Kesinlik:	0.8118
Hatırlama:	0.6757
F1 Skor:	0.7018

Gaussian Naive Bayes algoritması ile eğitilen modelin veri türlerine göre kesinlik metriği sonuçları Tablo 2.58’de gösterilmiştir.

Tablo 2.58 Gaussian Naive Bayes algoritması ile eğitilen modelin veri türlerine göre 2. test kesinlik metriği sonuçları

Kesinlik	Sonuç
Normal Trafik Verisi	0.9988
MSSQL DDoS Verisi	0.6348
UDP DDoS Verisi	0.8085

Gaussian Naive Bayes algoritması ile eğitilen modelin veri türlerine göre hatırlama metriği sonuçları Tablo 2.59’da gösterilmiştir.

Tablo 2.59 Gaussian Naive Bayes algoritması ile eğitilen modelin veri türlerine göre 2. test hatırlama metriği sonucu

Hatırlama	Sonuç
Normal Trafik Verisi	0.5130
MSSQL DDoS Verisi	0.9357
UDP DDoS Verisi	0.5726

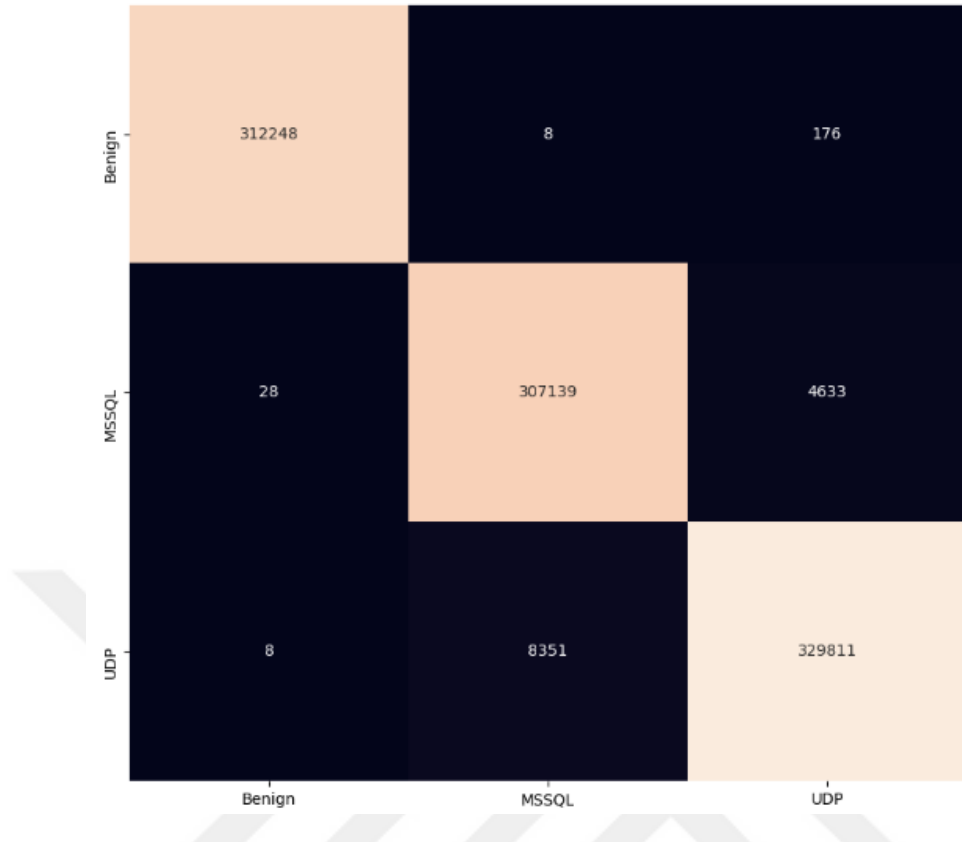
Gaussian Naive Bayes algoritması ile eğitilen modelin veri türlerine göre F1 skor metriği sonuçları Tablo 2.60’ta gösterilmiştir.

Tablo 2.60 Gaussian Naive Bayes algoritması ile eğitilen modelin veri türlerine göre 2. test F1 skor metriği sonucu

F1 Skor	Sonuç
Normal Trafik Verisi	0.6779
MSSQL DDoS Verisi	0.7564
UDP DDoS Verisi	0.6704

2.5.2.4 Extra Trees algoritması ile eğitilen modelin 2. testi

Daha önceden Extra Trees algoritmasıyla eğitilen modelin 2. testi gerçekleştirilmiştir. Modelin karmaşıklık matrisi Şekil 2.10’da gösterilmiştir.



Şekil 2.10 Extra Trees algoritması ile eğitilen modelin 2. test sonrası karmaşıklık matrisi

Modelin metrik sonuçları Tablo 2.61’de verilmiştir.

Tablo 2.61 Extra Trees algoritması ile eğitilen modelin 2. test metrik sonuçları

Metrik	Sonuç
Doğruluk:	0.9449
Kesinlik:	0.9862
Hatırlama:	0.9449
F1 Skor:	0.9650

Extra Trees algoritması ile eğitilen modelin veri türlerine göre kesinlik metriği sonuçları Tablo 2.62’de gösterilmiştir.

Tablo 2.62 Extra Trees algoritması ile eğitilen modelin veri türlerine göre 2. test kesinlik metriği sonuçları

Kesinlik	Sonuç
Normal Trafik Verisi	0.9999
MSSQL DDoS Verisi	0.9735
UDP DDoS Verisi	0.9856

Extra Trees algoritması ile eğitilen modelin veri türlerine göre hatırlama metriği sonuçları Tablo 2.63'te gösterilmiştir.

Tablo 2.63 Extra Trees algoritması ile eğitilen modelin veri türlerine göre 2. test hatırlama metriği sonuçları

Hatırlama	Sonuç
Normal Trafik Verisi	0.9554
MSSQL DDoS Verisi	0.9065
UDP DDoS Verisi	0.9733

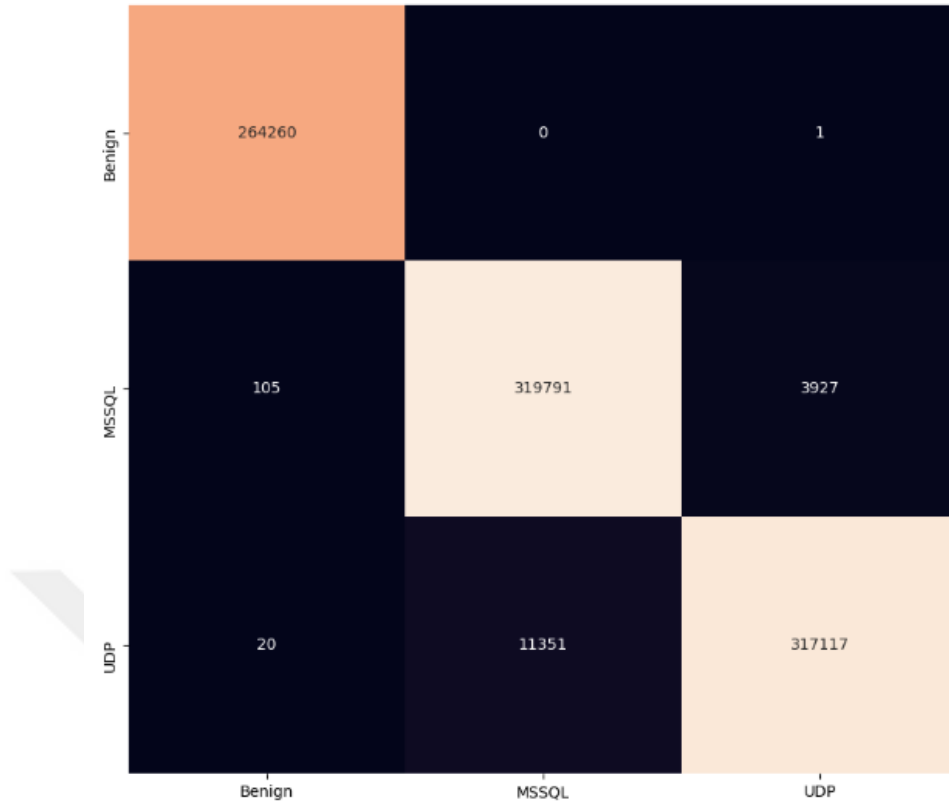
Extra Trees algoritması ile eğitilen modelin veri türlerine göre F1 skor metriği sonuçları Tablo 2.64'te gösterilmiştir.

Tablo 2.64 Extra Trees algoritması ile eğitilen modelin veri türlerine göre 2. test F1 skor metriği sonucu

F1 Skor	Sonuç
Normal Trafik Verisi	0.9772
MSSQL DDoS Verisi	0.9388
UDP DDoS Verisi	0.9794

2.5.2.5 AdaBoost algoritması ile eğitilen modelin 2. testi

Daha önceden AdaBoost algoritmasıyla eğitilen modelin 2. testi gerçekleştirilmiştir. Modelin karmaşıklık matrisi Şekil 2.11'de gösterilmiştir.



Şekil 2.11 AdaBoost algoritması ile eğitilen modelin 2. test sonrası karmaşıklık matrisi

Modelin metrik sonuçları Tablo 2.65’te verilmiştir.

Tablo 2.65 AdaBoost algoritması ile eğitilen modelin 2. test metrik sonuçları

Metrik	Sonuç
Doğruluk:	0.8971
Kesinlik:	0.9842
Hatırlama:	0.8971
F1 Skor:	0.9371

AdaBoost algoritması ile eğitilen modelin veri türlerine göre kesinlik metriği sonuçları Tablo 2.66’da gösterilmiştir.

Tablo 2.66 AdaBoost algoritması ile eğitilen modelin veri türlerine göre 2. test kesinlik metriği sonuçları

Kesinlik	Sonuç
Normal Trafik Verisi	0.9995
MSSQL DDoS Verisi	0.9657
UDP DDoS Verisi	0.9878

AdaBoost algoritması ile eğitilen modelin veri türlerine göre hatırlama metriği sonuçları Tablo 2.67’de gösterilmiştir.

Tablo 2.67 AdaBoost algoritması ile eğitilen modelin veri türlerine göre 2. test hatırlama metriği sonuçları

Hatırlama	Sonuç
Normal Trafik Verisi	0.8086
MSSQL DDoS Verisi	0.9438
UDP DDoS Verisi	0.9358

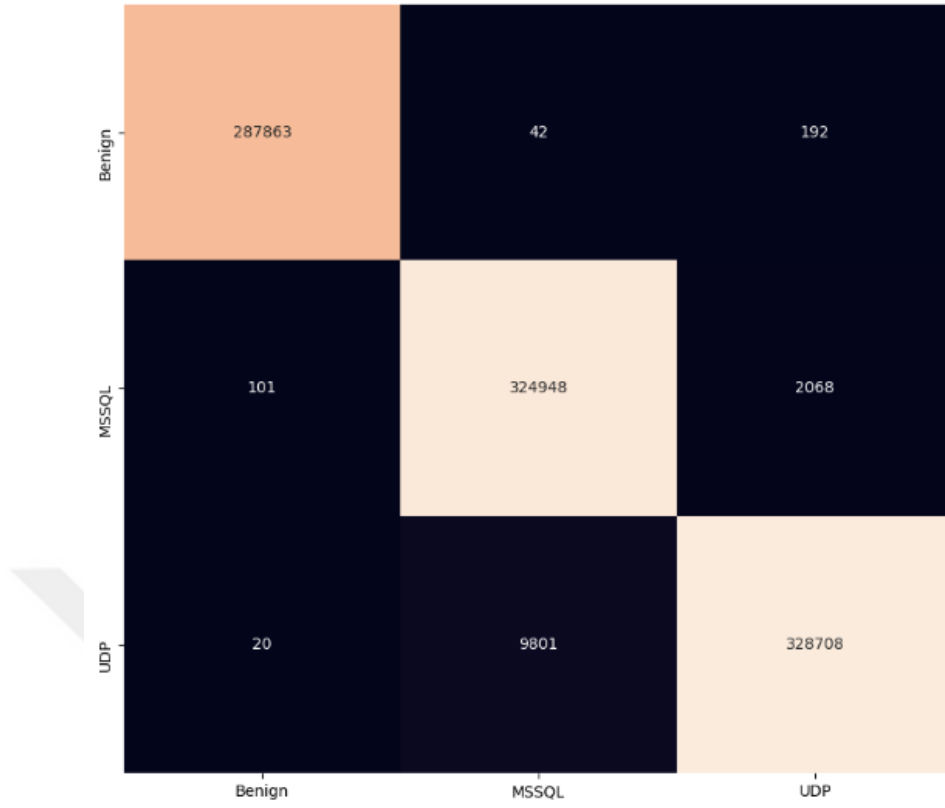
AdaBoost algoritması ile eğitilen modelin veri türlerine göre hatırlama metriği sonuçları Tablo 2.68’de gösterilmiştir.

Tablo 2.68 AdaBoost algoritması ile eğitilen modelin veri türlerine göre 2. test F1 skor metriği sonuçları

F1 Skor	Sonuç
Normal Trafik Verisi	0.8940
MSSQL DDoS Verisi	0.9546
UDP DDoS Verisi	0.9611

2.5.2.6 Gradient Boosting algoritması ile eğitilen modelin 2. testi

Daha önceden Gradient Boosting algoritmasıyla eğitilen modelin 2. testi gerçekleştirilmiştir. Modelin karmaşıklık matrisi Şekil 2.12’de gösterilmiştir.



Şekil 2.12 Gradient Boosting algoritması ile eğitilen modelin 2. test sonrası karmaşıklık matrisi

Modelin metrik sonuçları Tablo 2.69’da verilmiştir.

Tablo 2.69 Gradient Boosting algoritması ile eğitilen modelin 2. test metrik sonuçları

Metrik	Sonuç
Doğruluk:	0.9373
Kesinlik:	0.9876
Hatırlama:	0.9373
F1 Skor:	0.9612

Gradient Boosting algoritması ile eğitilen modelin veri türlerine göre kesinlik metriği sonuçları Tablo 2.70’te gösterilmiştir.

Tablo 2.70 Gradient Boosting algoritması ile eğitilen modelin veri türlerine göre 2. test kesinlik metriği sonuçları

Kesinlik	Sonuç
Normal Trafik Verisi	0.9996
MSSQL DDoS Verisi	0.9706
UDP DDoS Verisi	0.9932

Gradient Boosting algoritması ile eğitilen modelin veri türlerine göre hatırlama metriği sonuçları Tablo 2.71’de gösterilmiştir.

Tablo 2.71 Gradient Boosting algoritması ile eğitilen modelin veri türlerine göre 2. test hatırlama metriği sonuçları

Hatırlama	Sonuç
Normal Trafik Verisi	0.8808
MSSQL DDoS Verisi	0.9590
UDP DDoS Verisi	0.9700

Gradient Boosting algoritması ile eğitilen modelin veri türlerine göre F1 skor metriği sonuçları Tablo 2.72’de gösterilmiştir.

Tablo 2.72 Gradient Boosting algoritması ile eğitilen modelin veri türlerine göre 2. test F1 skor metriği sonuçları

F1 Skor	Sonuç
Normal Trafik Verisi	0.9365
MSSQL DDoS Verisi	0.9648
UDP DDoS Verisi	0.9815

2.5.3 Modellerin LDAP DDoS saldırısı ile testi

Eğitilen modelleri test etme yollarından biri de modelin eğitim aşamasında görmediği bir veri türünü sınıflandırma becerisidir. Modeller predict_proba fonksiyonu kullanılarak 824352 adet LDAP DDoS saldırı verisi ile test edilmiştir.

2.5.3.1 Random Forest algoritması ile eğitilen modelin LDAP DDoS saldırısını sınıflandırması

Random Forest algoritması ile eğitmiş olduğumuz modelimiz 824352 adet LDAP DDoS saldırı verisi ile test edilerek modelin tahmin sonuçları Tablo 2.73'te gösterilmiştir.

Tablo 2.73 *Random Forest algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini veri türlerine göre sınıflandırma sonuçları*

Veri Türü	Tahmin Sayısı
Normal Veri	18
DNS DDoS	635339
MSSQL DDoS	2494
NTP DDoS	62
SNMP DDoS	186369
UDP DDoS	70

Sonuçlar incelendiğinde Random Forest ile eğitilen modelin LDAP DDoS saldırısını yüksek oranda DNS DDoS saldırısı olarak tahmin ettiği görülmektedir. DNS DDoS saldırısından sonra en çok SNMP DDoS saldırısı olarak tahmin edilmiştir.

Modelin, LDAP DDoS saldırı verisini diğer saldırı verilerinden biri olarak sınıflandırması beklenmektedir. Tablo 2.74'te modelin LDAP DDoS saldırı verilerini normal veya saldırı olarak tahmin ettiği sayılar verilmiştir.

Tablo 2.74 *Random Forest algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini sınıflandırma sonuçları*

Veri Türü	Tahmin Sayısı
Toplam Veri	824352
Saldırı Trafiği	824334
Normal Trafik	18

2.5.3.2 Decision Tree algoritması ile eğitilen modelin LDAP DDoS saldırısını sınıflandırması

Decision Tree algoritması ile eğitmiş olduğumuz modelimiz 824352 adet LDAP DDoS saldırı verisi ile test edilerek modelin tahmin sonuçları Tablo 2.75'te gösterilmiştir.

Tablo 2.75 *Decision Tree algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini veri türlerine göre sınıflandırma sonuçları*

Veri Türü	Tahmin Sayısı
Normal Veri	11
DNS DDoS	636293
MSSQL DDoS	2025
NTP DDoS	54
SNMP DDoS	185892
UDP DDoS	77

Sonuçlar incelendiğinde Decision Tree ile eğitilen modelin de LDAP DDoS saldırısını yüksek oranda DNS DDoS saldırısı olarak tahmin ettiği görülmektedir. DNS DDoS saldırısından sonra en çok SNMP DDoS saldırısı olarak tahmin edilmiştir.

Tablo 2.76’da modelin LDAP DDoS saldırı verilerini normal veya saldırı olarak tahmin ettiği sayılar verilmiştir.

Tablo 2.76 *Decision Tree algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini sınıflandırma sonuçları*

Veri Türü	Tahmin Sayısı
Toplam Veri	824352
Saldırı Trafik	824341
Normal Trafik	11

2.5.3.3 Gaussian Naive Bayes algoritması ile eğitilen modelin LDAP DDoS saldırısını sınıflandırması

Gaussian Naive Bayes algoritması ile eğitilmiş olduğumuz modelimiz 824352 adet LDAP DDoS saldırı verisi ile test edilerek modelin tahmin sonuçları Tablo 2.77’de gösterilmiştir.

Tablo 2.77 Gaussian Naive Bayes algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini veri türlerine göre sınıflandırma sonuçları

Veri Türü	Tahmin Sayısı
Normal Veri	47
DNS DDoS	1322
MSSQL DDoS	3647
NTP DDoS	48
SNMP DDoS	819270
UDP DDoS	18

Sonuçlar incelendiğinde Gaussian Naive Bayes algoritması ile eğitilen modelin LDAP DDoS saldırısını çok yüksek oranda SNMP DDoS olarak tahmin ettiği görülmektedir.

Tablo 2.78’de modelin LDAP DDoS saldırı verilerini normal veya saldırı olarak tahmin ettiği sayılar verilmiştir.

Tablo 2.78 Gaussian Naive Bayes algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini sınıflandırma sonuçları

Veri Türü	Tahmin Sayısı
Toplam Veri	824352
Saldırı Trafiği	824305
Normal Trafik	47

2.5.3.4 Extra Trees algoritması ile eğitilen modelin LDAP DDoS saldırısını sınıflandırması

Extra Trees algoritması ile eğitmiş olduğumuz modelimiz 824352 adet LDAP DDoS saldırı verisi ile test edilerek modelin tahmin sonuçları Tablo 2.79’da gösterilmiştir.

Tablo 2.79 Extra Trees algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini veri türlerine göre sınıflandırma sonuçları

Veri Türü	Tahmin Sayısı
Normal Veri	21
DNS DDoS	636390
MSSQL DDoS	1945
NTP DDoS	53

Tablo 2.79 devam *Extra Trees algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini veri türlerine göre sınıflandırma sonuçları*

SNMP DDoS	185868
UDP DDoS	75

Sonuçlar incelendiğinde Extra Trees algoritması ile eğitilen modelin LDAP DDoS saldırısını yüksek oranda DNS DDoS saldırısı olarak tahmin ettiği görülmektedir. DNS DDoS saldırısından sonra en çok SNMP DDoS saldırısı olarak tahmin edilmiştir.

Modelin, LDAP DDoS saldırı verisini saldırı verisi olarak sınıflandırması beklenmektedir. Tablo 2.80’de modelin LDAP DDoS saldırı verilerini normal veya saldırı olarak tahmin ettiği sayılar verilmiştir.

Tablo 2.80 *Extra Trees algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini sınıflandırma sonuçları*

Veri Türü	Tahmin Sayısı
Toplam Veri	824352
Saldırı Trafığı	824331
Normal Trafik	21

2.5.3.5 AdaBoost algoritması ile eğitilen modelin LDAP DDoS saldırısını sınıflandırması

AdaBoost algoritması ile eğitmiş olduğumuz modelimiz 824352 adet LDAP DDoS saldırı verisi ile test edilerek modelin tahmin sonuçları Tablo 2.81’de gösterilmiştir.

Tablo 2.81 *AdaBoost algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini veri türlerine göre sınıflandırma sonuçları*

Veri Türü	Tahmin Sayısı
Normal Veri	114
DNS DDoS	985
MSSQL DDoS	4918
NTP DDoS	397
SNMP DDoS	817938
UDP DDoS	0

Sonuçlar incelendiğinde AdaBoost algoritması ile eğitilen modelin LDAP DDoS saldırısını yüksek oranda SNMP DDoS olarak tahmin ettiği görülmüştür.

Tablo 2.82’de modelin LDAP DDoS saldırı verilerini normal veya saldırı olarak tahmin ettiği sayılar verilmiştir.

Tablo 2.82 AdaBoost algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini sınıflandırma sonuçları

Veri Türü	Tahmin Sayısı
Toplam Veri	824352
Saldırı Trafiği	824238
Normal Trafik	114

2.5.3.6 Gradient Boosting algoritması ile eğitilen modelin LDAP DDoS saldırısını sınıflandırması

Gradient Boosting algoritması ile eğitmiş olduğumuz modelimiz 824352 adet LDAP DDoS saldırı verisi ile test edilerek modelin tahmin sonuçları Tablo 2.83’te gösterilmiştir.

Tablo 2.83 Gradient Boosting algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini veri türlerine göre sınıflandırma sonuçları

Veri Türü	Tahmin Sayısı
Normal Veri	112
DNS DDoS	621054
MSSQL DDoS	4807
NTP DDoS	44
SNMP DDoS	198326
UDP DDoS	9

Sonuçlar incelendiğinde Gradient Boosting ile eğitilen modelin LDAP DDoS saldırısını yüksek oranda DNS DDoS saldırısı olarak tahmin ettiği görülmüştür. DNS DDoS saldırısından sonra en çok SNMP DDoS saldırısı olarak tahmin edilmiştir.

Modelin, LDAP DDoS saldırı verisini saldırı verisi olarak sınıflandırması beklenmektedir. Tablo 2.84’te modelin LDAP DDoS saldırı verilerini normal veya saldırı olarak tahmin ettiği sayılar verilmiştir.

Tablo 2.84 Gradient Boosting algoritması ile eğitilen modelin LDAP DDoS saldırı verilerini sınıflandırma sonuçları

Veri Türü	Tahmin Sayısı
Toplam Veri	824352
Saldırı Trafiği	824240
Normal Trafik	112

3. BULGULAR ve TARTIŞMA

Bu bölümde, çalışmada yapılan testlere göre modellerin başarısı değerlendirilmektedir.

3.1 Modellere Yapılan 1. Testin Değerlendirmesi

Model eğitiminde Random Forest, Decision Tree, Gaussian Naive Bayes, Extra Trees, AdaBoost ve Gradient Boosting algoritmaları kullanılmıştır. Eğitilen modeller Tablo 3.1'deki verilerle test edilmiştir.

Tablo 3.1 Modellerin 1. testinde kullanılan veri sayıları

Test Veri Türü	Örnek Sayısı
Normal Trafik Verisi	247843
NTP DDoS Verisi	246860
DNS DDoS Verisi	246370
MSSQL DDoS Verisi	248275
SNMP DDoS Verisi	246750
UDP DDoS Verisi	247584
TOPLAM	1483682

Tablo 3.2'de makine öğrenmesi ile eğitilen modellerin 1. test metrik sonuçları bir arada verilmektedir.

Tablo 3.2 Modellerin 1. test metrik sonuçları

Metrik	RF	DT	ET	GNB	AB	GB
Doğruluk:	0.9491	0.9490	0.9492	0.6460	0.8073	0.9428
Kesinlik:	0.9496	0.9495	0.9497	0.7101	0.8539	0.9430
Hatırlama:	0.9491	0.9490	0.9492	0.6460	0.8073	0.9428
F1 Skor:	0.9493	0.9492	0.9494	0.6016	0.7582	0.9428

RF: Random Forest, DT: Decision Tree, ET: Extra Trees, GNB: Gaussian Naive Bayes, AB: AdaBoost, GB: Gradient Boosting

Sonuçlara bakıldığında Random Forest, Decision Tree, Extra Trees ve Gradient Boosting algoritmalarıyla eğitilen modellerin saldırı tespiti ve sınıflandırmasında birbirine yakın ve çok başarılı sonuçlar verdiği görülmektedir. AdaBoost algoritması ile eğitilen modelin sonucu da başarılı olarak değerlendirilebilir. Gaussian Naive Bayes algoritması ile eğitilen modelin diğer modellere kıyasla başarısız sonuç verdiği görülmektedir. Extra Trees algoritması ile eğitilen modelin doğruluk, kesinlik, hatırlama ve F1 skor metriklerinde en başarılı sonucu verdiği görülmektedir.

3.2 Modellere Yapılan 2. Testin Değerlendirmesi

2. test kapsamında modeller Tablo 3.3'teki verilerle test edilmiştir.

Tablo 3.3 Modellerin 2. testinde kullanılan veri sayıları

Veri Türü	Örnek Sayısı
Normal Trafik Verisi	326809
UDP DDoS Verisi	338867
MSSQL DDoS Verisi	338827
TOPLAM	1004503

Tablo 3.4'te makine öğrenmesi ile eğitilen modellerin 2. test metrik sonuçları bir arada verilmektedir.

Tablo 3.4 Modellerin 2. test metrik sonuçları

Metrik	RF	DT	ET	GNB	AB	GB
Doğruluk:	0.9489	0.9197	0.9449	0.6757	0.8971	0.9373
Kesinlik:	0.9853	0.9848	0.9862	0.8118	0.9842	0.9876
Hatırlama:	0.9489	0.9197	0.9449	0.6757	0.8971	0.9373
F1 Skor:	0.9666	0.9506	0.9650	0.7018	0.9371	0.9612

RF: Random Forest, DT: Decision Tree, ET: Extra Trees, GNB: Gaussian Naive Bayes, AB:AdaBoost, GB:Gradient Boosting

Sonuçlara bakıldığında Random Forest, Decision Tree, Extra Trees ve Gradient Boosting algoritmalarıyla eğitilen modellerin saldırı tespiti ve sınıflandırmasında birbirine yakın ve çok başarılı sonuçlar verdiği görülmektedir. AdaBoost ile eğitilen modelin sonucu da başarılı olarak değerlendirilebilir. Bütün modeller incelendiğinde Random Forest ile eğitilen modelin doğruluk, hatırlama ve F1 skor metriklerinde en başarılı sonucu verdiği görülmektedir. Gradient Boosting algoritması ile eğitilen modelin kesinlik metriğinde

diğerlerinden daha başarılı sonuç verdiği görülmektedir. 1. testte olduğu gibi bu testte de Gaussian Naive Bayes ile eğitilen modelin diğer modellere kıyasla başarısız sonuç verdiği görülmektedir.

3.3 Modellere Yapılan LDAP DDoS Saldırı Testi Değerlendirmesi

Bu bölümde modellere eğitim aşamasında görmediği LDAP DDoS saldırı verileriyle yapılan testlerin genel bir değerlendirme yapılmaktadır. Tablo 3.5'te her bir modelin LDAP DDoS saldırı verilerini sınıflandırma sonuçları verilmektedir.

Tablo 3.5 Modellerin LDAP DDoS saldırı verilerini sınıflandırma sonuçları

Veri Türü	RF	DT	ET	GNB	AB	GB
Normal Veri	18	11	21	47	114	112
DNS DDoS	635339	636293	636390	1322	985	621054
MSSQL DDoS	2494	2025	1945	3647	4918	4807
NTP DDoS	62	54	53	48	397	44
SNMP DDoS	186369	185892	185868	819270	817938	198326
UDP DDoS	70	77	75	18	0	9

RF: Random Forest, DT: Decision Tree, ET: Extra Trees, GNB: Gaussian Naive Bayes, AB:AdaBoost, GB:Gradient Boosting

Modellerin LDAP DDoS saldırı verilerini diğer saldırı türlerinden biri olarak tahmin etmesi beklenmektedir. Eğer model LDAP DDoS saldırısını diğer modellere göre fazla miktarda normal veri olarak tahmin ettiyse daha az başarılı olarak ele alınmalıdır. Sonuçlar incelendiğinde bütün modellerin LDAP DDoS saldırı verilerini çok az miktarda normal veri olarak tahmin ettiği görülmektedir. Tablo 3.5'teki verilere bakıldığında en başarılı modelin Decision Tree ile eğitilen model olduğu görülmektedir.

3.4 Çalışma Sonuçlarının Benzer Çalışma Sonuçlarıyla

Karşılaştırılması

2019 yılında yayınlanan çalışmalarında Sharafaldin ve diğerleri, kendi ürettikleri veri seti olan CIC-DDoS2019 veri setini kullanarak DDoS ataklarının makine öğrenmesi algoritmalarıyla tespiti üzerine çalışma yapmışlardır [10]. Sharafaldin ve diğerlerinin çalışmalarında aldıkları sonuçlar Tablo 3.6'da gösterilmektedir.

Tablo 3.6 CIC-DDoS2019 veri seti kullanılarak yapılan çalışmanın sonuçları [10]

Metrik	RF	ID3	NB	LR
Doğruluk:	-	-	-	-
Kesinlik:	0.77	0.78	0.41	0.25
Hatırlama:	0.56	0.65	0.11	0.02
F1 Skor:	0.62	0.69	0.05	0.04

RF: Random Forest, ID3: Iterative Dichotomiser 3, NB: Naive Bayes, LR: Logistic Regression

Sonuçlar incelendiğinde en başarılı sonucu veren modelin ID3 algoritması ile eğitilen model olduğu görülmektedir. Aldıkları sonuçlarla, bu çalışmada alınan sonuçlar kıyaslandığında Sharafaldin ve diğerlerinin çalışmalarında daha az başarılı sonuçlar elde ettiği görülmektedir. Bunun yanı sıra çalışmalarında, eğitim aşamasında modelin görmediği veriyle testinin sonucu bulunmadığı için bu konuda karşılaştırma yapılamamıştır.

2018 yılında yayınlanan çalışmalarında Sharafaldin ve diğerleri, kendi ürettikleri veri seti olan CICIDS2017 veri setini kullanarak BruteForce, DoS, DDoS, web atakları ve bazı diğer atak türlerinin makine öğrenmesi algoritmalarıyla tespit üzerine çalışma yapmışlardır [33]. Çalışmalarında aldıkları sonuçlar Tablo 3.7’de gösterilmektedir.

Tablo 3.7 CICIDS2017 veri seti kullanılarak yapılan çalışmanın sonuçları [33]

Metrik	KNN	RF	ID3	AB	MLP	NB	QDA
Doğruluk:	-	-	-	-	-	-	-
Kesinlik:	0.96	0.98	0.98	0.77	0.77	0.88	0.97
Hatırlama:	0.96	0.97	0.98	0.84	0.83	0.04	0.88
F1 Skor:	0.96	0.97	0.98	0.77	0.76	0.04	0.92

KNN: K-Nearest Neighbors, RF: Random Forest, ID3: Iterative Dichotomiser 3, AB: AdaBoost, MLP: Multilayer Perceptron, NB: Naive Bayes, QDA: Quadratic Discriminant Analysis

Sonuçlar incelendiğinde en başarılı sonucu veren modelin ID3 algoritması ile eğitilen model olduğu görülmektedir. Aldıkları sonuçlarla, bu çalışmada alınan sonuçlar kıyaslandığında Sharafaldin ve diğerlerinin çalışmalarında daha başarılı sonuçlar elde ettiği görülmektedir. Bunun yanı sıra çalışmalarında, eğitim aşamasında modelin

görmediği veriyle testinin sonucu bulunmadığı için bu konuda karşılaştırma yapılamamıştır.

4. SONUÇLAR

Bu çalışmada makine öğrenmesi algoritmaları ile eğitilen modellerin DDoS saldırı tespiti ve sınıflandırma başarısı test edilmiştir. Model eğitiminde Random Forest, Decision Tree, Gaussian Naive Bayes, Extra Trees, AdaBoost ve Gradient Boosting algoritmaları kullanılmıştır. Model eğitilirken ve test edilirken kullanılan veriler güncel veri setlerinden alınmıştır. Çalışmada her bir veri türünü ayırt etmek için kullanılan en önemli özelliklerin bilgisi de verilmiştir. Bunun yanı sıra kullanılan sınıflandırıcıların çapraz doğrulama metodu ile testi gerçekleştirilmiştir.

Eğitilen modellerin başarısı testler yapılarak değerlendirilmiştir. Tablo 3.2’de verilen 1. test sonuçlarına ve Tablo 3.4’te verilen 2. test sonuçlarına göre Random Forest, Decision Tree, Extra Trees ve Gradient Boosting algoritmalarının birbirine yakın ve çok başarılı sonuçlar verdiği görülmektedir. Test yöntemlerinden biri de modellerin eğitim aşamasında kullanılmayan bir veri türünü sınıflandırma becerisidir. Bu kapsamda modeller LDAP DDoS saldırı verileriyle test edilmiştir. Tablo 3.5’te verilen LDAP DDoS saldırı verisi sınıflandırma sonuçlarına bakıldığında Decision Tree algoritması kullanılarak eğitilen model en başarılı sonucu veren model olmuştur. Bunun yanı sıra diğer modellerin de LDAP DDoS saldırı verilerini sınıflandırmada başarılı olduğu görülmektedir. Gerçekleştirilen testlerden elde edilen sonuçlar dikkate alındığında, DDoS saldırı tespiti ve sınıflandırmasında, makine öğrenmesi algoritmaları kullanılarak başarılı sonuçlar alınabileceği görülmüştür.

KAYNAKLAR

- [1] Z. He, T. Zhang, ve R. B. Lee, “Machine Learning Based DDoS Attack Detection from Source Side in Cloud”, içinde *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, New York, NY, USA, Haz. 2017, ss. 114-120, doi: 10.1109/CSCloud.2017.58.
- [2] S. T. Zargar, J. Joshi, ve D. Tipper, “A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks”, *IEEE Commun. Surv. Tutor.*, c. 15, sy 4, ss. 2046-2069, 2013, doi: 10.1109/SURV.2013.031413.00127.
- [3] A. Yaar, A. Perrig, ve D. Song, “Pi: a path identification mechanism to defend against DDoS attacks”, içinde *Proceedings 19th International Conference on Data Engineering (Cat. No.03CH37405)*, Berkeley, CA, USA, 2003, ss. 93-107, doi: 10.1109/SECPRI.2003.1199330.
- [4] C. Douligeris ve A. Mitrokotsa, “DDoS attacks and defense mechanisms: classification and state-of-the-art”, *Comput. Netw.*, c. 44, sy 5, ss. 643-666, Nis. 2004, doi: 10.1016/j.comnet.2003.10.003.
- [5] E. Balkanli, J. Alves, ve A. N. Zincir-Heywood, “Supervised learning to detect DDoS attacks”, içinde *2014 IEEE Symposium on Computational Intelligence in Cyber Security (CICS)*, Orlando, FL, USA, Ara. 2014, ss. 1-8, doi: 10.1109/CICYBS.2014.7013367.
- [6] M. Almseidin, M. Alzubi, S. Kovacs, ve M. Alkasassbeh, “Evaluation of machine learning algorithms for intrusion detection system”, içinde *2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY)*, Subotica, Serbia, Eyl. 2017, ss. 277-282, doi: 10.1109/SISY.2017.8080566.
- [7] N. Farah, Md. Avishek, F. Muhammad, A. Rahman, M. Rafni, ve D. Md., “Application of Machine Learning Approaches in Intrusion Detection System: A Survey”, *Int. J. Adv. Res. Artif. Intell.*, c. 4, sy 3, 2015, doi: 10.14569/IJARAI.2015.040302.
- [8] F. Pedregosa vd., “Scikit-learn: Machine Learning in Python”, *J. Mach. Learn. Res.*, c. 12, sy 85, ss. 2825-2830, 2011.
- [9] “scikit-learn”, *Wikipedia*. Oca. 14, 2021, Erişim: Oca. 23, 2021. [Çevrimiçi]. Erişim adresi: <https://en.wikipedia.org/w/index.php?title=Scikit-learn&oldid=1000398987>.

- [10] I. Sharafaldin, A. H. Lashkari, S. Hakak, ve A. A. Ghorbani, “Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy”, içinde *2019 International Carnahan Conference on Security Technology (ICCST)*, CHENNAI, India, Eki. 2019, ss. 1-8, doi: 10.1109/CCST.2019.8888419.
- [11] “IDS 2018 | Datasets | Research | Canadian Institute for Cybersecurity | UNB”. <https://www.unb.ca/cic/datasets/ids-2018.html> (erişim Mar. 14, 2020).
- [12] “A Realistic Cyber Defense Dataset (CSE-CIC-IDS2018) - Registry of Open Data on AWS”. <https://registry.opendata.aws/cse-cic-ids2018/> (erişim Oca. 22, 2021).
- [13] B. Zhang, T. Zhang, ve Z. Yu, “DDoS detection and prevention based on artificial intelligence techniques”, içinde *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, Chengdu, Ara. 2017, ss. 1276-1280, doi: 10.1109/CompComm.2017.8322748.
- [14] G. Dayanandam, E. S. Reddy, ve D. B. Babu, “Regression algorithms for efficient detection and prediction of DDoS attacks”, içinde *2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, Aralık 2017, ss. 215-219, doi: 10.1109/ICATCCT.2017.8389136.
- [15] K. M. Prasad, A. R. M. Reddy, ve K. V. Rao, “DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms -A Survey”, c. 14, sy 7, 2014.
- [16] “2019 Cybersecurity Insights Report”, *NSFOCUS, Inc., a global network and cyber security leader, protects enterprises and carriers from advanced cyber attacks*. <https://nsfocusglobal.com/2019-cybersecurity-insights-report/> (erişim May. 18, 2020).
- [17] “2019 DDoS Attack Landscape Report”, *NSFOCUS, Inc., a global network and cyber security leader, protects enterprises and carriers from advanced cyber attacks*. <https://nsfocusglobal.com/2019-ddos-attack-landscape-report/> (erişim May. 18, 2020).
- [18] “NTP Amplification DDoS Attack”, *Cloudflare*. <https://www.cloudflare.com/learning/ddos/ntp-amplification-ddos-attack/> (erişim Haz. 10, 2020).

- [19] “MS SQL Reflection Attack”, *DDOS-GUARD*. https://ddos-guard.net/en/terminology/attack_type/ms-sql-reflection-attack (erişim Haz. 10, 2020).
- [20] “DNS Amplification DDoS Attack”, *Cloudflare*. <https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/> (erişim Haz. 10, 2020).
- [21] B. Technical Working Group, “SNMP Reflected Amplification DDoS Attack Mitigation”, *SSRN Electron. J.*, 2012, doi: 10.2139/ssrn.2701498.
- [22] “UDP Flood DDoS Attack”, *Cloudflare*. <https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/> (erişim Haz. 12, 2020).
- [23] L. Segal, “Old Protocols, New Exploits: LDAP Unwittingly Serves DDoS Amplification Attacks”, *F5 Labs*, Tem. 06, 2017. <https://www.f5.com/labs/articles/threat-intelligence/old-protocols-new-exploits-ldap-unwittingly-serves-ddos-amplification-attacks-22609> (erişim Tem. 21, 2020).
- [24] M. M. Tiwari, R. Kumar, A. Bharti, ve J. Kishan, “INTRUSION DETECTION SYSTEM”, c. 5, sy 2, ss. 38-44, 2017.
- [25] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, ve F. Ahmad, “Network intrusion detection system: A systematic study of machine learning and deep learning approaches”, *Trans. Emerg. Telecommun. Technol.*, Eki. 2020, doi: 10.1002/ett.4150.
- [26] L. H. Yeo, X. Che, ve S. Lakkaraju, “UNDERSTANDING MODERN INTRUSION DETECTION SYSTEMS: A SURVEY”, 2017, doi: arXiv:1708.07174.
- [27] Ö. Kasim, “An efficient and robust deep learning based network anomaly detection against distributed denial of service attacks”, *Comput. Netw.*, c. 180, s. 107390, Eki. 2020, doi: 10.1016/j.comnet.2020.107390.
- [28] M. T. Nguyen ve K. Kim, “Genetic convolutional neural network for intrusion detection systems”, *Future Gener. Comput. Syst.*, c. 113, ss. 418-427, Ara. 2020, doi: 10.1016/j.future.2020.07.042.

- [29] S. Jose, D. Malathi, B. Reddy, ve D. Jayaseeli, “A Survey on Anomaly Based Host Intrusion Detection System”, *J. Phys. Conf. Ser.*, c. 1000, sy 1, s. 012049, Nis. 2018, doi: 10.1088/1742-6596/1000/1/012049.
- [30] A. A. Aburomman ve M. Bin Ibne Reaz, “Survey of learning methods in intrusion detection systems”, içinde *2016 International Conference on Advances in Electrical, Electronic and Systems Engineering (ICAEES)*, Putrajaya, Malaysia, Kas. 2016, ss. 362-365, doi: 10.1109/ICAEES.2016.7888070.
- [31] T. S. Pham, T. H. Hoang, ve V. Van Canh, “Machine learning techniques for web intrusion detection — A comparison”, içinde *2016 Eighth International Conference on Knowledge and Systems Engineering (KSE)*, Hanoi, Eki. 2016, ss. 291-297, doi: 10.1109/KSE.2016.7758069.
- [32] M. S. Hoyos Ll, G. A. Isaza E, J. I. Vélez, ve L. Castillo O, “Distributed Denial of Service (DDoS) Attacks Detection Using Machine Learning Prototype”, içinde *Distributed Computing and Artificial Intelligence, 13th International Conference*, c. 474, S. Omatu, A. Semalat, G. Bocewicz, P. Sitek, I. E. Nielsen, J. A. García García, ve J. Bajo, Ed. Cham: Springer International Publishing, 2016, ss. 33-41.
- [33] I. Sharafaldin, A. Habibi Lashkari, ve A. A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization”:, içinde *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, Funchal, Madeira, Portugal, 2018, ss. 108-116, doi: 10.5220/0006639801080116.
- [34] Naveen Bindra ve Manu Sood, “Detecting DDoS Attacks Using Machine Learning Techniques and Contemporary Intrusion Detection Dataset”, *Autom. Control Comput. Sci.*, c. 53, sy 5, ss. 419-428, Eyl. 2019, doi: 10.3103/S0146411619050043.
- [35] R. R. Rejimol Robinson ve C. Thomas, “Ranking of machine learning algorithms based on the performance in classifying DDoS attacks”, içinde *2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS)*, Trivandrum, Ara. 2015, ss. 185-190, doi: 10.1109/RAICS.2015.7488411.
- [36] C. B. Çebi, O. K. Sahingoz, F. S. Bulut, H. Firat, ve G. Karataş, “Saldırı Tespit Sistemlerinde Makine Öğrenmesi Modellerinin Karşılaştırılması”, *Erzincan*

Üniversitesi Fen Bilim. Enstitüsü Derg., c. 12, sy 3, ss. 1513-1525, Ara. 2019, doi: 10.18185/erzifbed.573648.

- [37] Karataş, G. (2020) Derin Öğrenme Tabanlı Saldırı Tespit Sistemi. Doktora Tezi, Marmara Üniversitesi Fen Bilimleri Enstitüsü, İstanbul, Türkiye.
- [38] M. Vakili, M. Ghamsari, ve M. Rezaei, “Performance Analysis and Comparison of Machine and Deep Learning Algorithms for IoT Data Classification”, s. 13, 2020, doi: arXiv:2001.09636.
- [39] “3.1. Cross-validation: evaluating estimator performance — scikit-learn 0.24.0 documentation”. https://scikit-learn.org/stable/modules/cross_validation.html (erişim Tem. 25, 2020).
- [40] D. Berrar, “Cross-Validation”, içinde *Encyclopedia of Bioinformatics and Computational Biology*, Elsevier, 2019, ss. 542-545.
- [41] “ahlashkari/CICFlowMeter”, *GitHub*. <https://github.com/ahlashkari/CICFlowMeter/blob/master/ReadMe.txt> (erişim Şub. 01, 2021).

EKLER



ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

İsim-Soyisim: Furkan SERDAROĞLU

EĞİTİM BİLGİLERİ

Lisans: İstanbul Üniversitesi Bilgisayar Mühendisliği

Lise: Levent Aydın Anadolu Lisesi

İŞ TECRÜBESİ

2018 Temmuz'dan beri

TÜBİTAK BİLGEM'de Yazılım Geliştirici

2017 Temmuz - 2018 Temmuz

Türk Hava Yolları A.O. Bilgi Teknolojileri'nde Linux Sistem Yöneticisi