T.C.
MİLLÎ SAVUNMA ÜNİVERSİTESİ
ATATÜRK STRATEJİK ARAŞTIRMALAR VE LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
SİBER GÜVENLİK TEZLİ PROGRAMI

MAKİNE ÖĞRENME YÖNTEMLERİ KULLANILARAK SALDIRI TESPİTİ

YÜKSEK LİSANS TEZİ

FIRAT KILINÇ
3211112

DANIŞMAN: DOÇ. DR. CAN EYÜPOĞLU

İSTANBUL
TEMMUZ 2023

T.C.
MİLLÎ SAVUNMA ÜNİVERSİTESİ
ATATÜRK STRATEJİK ARAŞTIRMALAR VE LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
SİBER GÜVENLİK TEZLİ PROGRAMI

MAKİNE ÖĞRENME YÖNTEMLERİ KULLANILARAK SALDIRI TESPİTİ

YÜKSEK LİSANS TEZİ

FIRAT KILINÇ
3211112

DANIŞMAN: DOÇ. DR. CAN EYÜPOĞLU

İSTANBUL
TEMMUZ 2023

T.C.
MİLLÎ SAVUNMA ÜNİVERSİTESİ
ATATÜRK STRATEJİK ARAŞTIRMALAR VE LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
SİBER GÜVENLİK TEZLİ PROGRAMI

MAKİNE ÖĞRENME YÖNTEMLERİ KULLANILARAK SALDIRI TESPİTİ

YÜKSEK LİSANS TEZİ

Fırat KILINÇ
3211112

Tezin Enstitüye Verildiği Tarih : 21.07.2023
Tezin Savunulduğu Tarih : 21.06.2023

Tez Oy birliği ile başarılı bulunmuştur.

	Unvan Ad Soyad	İmza
Tez Danışmanı	Doç. Dr. Can EYÜPOĞLU	
Jüri Üyeleri	Dr. Öğr. Üyesi Aytuğ BOYACI	
	Doç. Dr. Muhammed Ali AYDIN	

İSTANBUL
TEMMUZ 2023

ÖZGÜNLÜK RAPORU

Tez çalışmamın a) Kapak sayfası, b) Giriş, c) Ana bölümler ve ç) Sonuç kısımlarından oluşan toplam 75 sayfalık kısmına ilişkin, 21/07/2023 tarihinde şahsım tarafından Turnitin adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan özgünlük raporuna göre, tezimin benzerlik oranı %11'dir.

Uygulanan filtrelemeler:

1- Kaynakça hariç
2- Alıntılar hariç
3- 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Millî Savunma Üniversitesi Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü Lisansüstü Tez Çalışması Özgünlük Raporu Alınması ve Kullanılması Uygulama Usul ve Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Fırat KILINÇ
21.07.2023

ETİK BEYAN

Millî Savunma Üniversitesi Enstitüleri Dönem Projesi ve Lisansüstü Tez Hazırlama Kılavuzu'nda yer alan kurallarına uygun olarak hazırladığım bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu, bildirir; aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Bu tezdeki düşünce, görüş, varsayım, sav veya tezler bana aittir; Millî Savunma Bakanlığı, Millî Savunma Üniversitesi ve Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü sorumlu tutulamaz.

Fırat KILINÇ
21.07.2023

Türk havacılık tarihinin en önemli isimlerden birisi olan Vecihi Hürkuş'a ithafen.

TEŞEKKÜR

Yüksek lisans öğrenimim sırasında ve tez çalışmalarım boyunca gösterdiği her türlü destek ve yardımlarından dolayı çok değerli danışman hocam Doç. Dr. Can EYÜPOĞLU'na en içten dileklerimle teşekkür ederim. Tezli yüksek lisans geçiş sürecindeki yönlendirmelerinden dolayı Doç. Dr. Muhammed Ali AYDIN'a çok teşekkür ederim. Tez aşaması boyunca yardımlarını ve değerli fikirlerini esirgemeyen Araş. Gör. Dr. Ahmet ÖZCAN'a teşekkür ederim. Tezin hazırlanması süresince bütün sıkıntılarıma katlanan ve zor dönemlerimde yanımda olan sevgili eşim Hazal KILINÇ'a ve kızlarım Alya Su ve Azra KILINÇ'a teşekkürü bir borç bilirim. Eğitim hayatım boyunca maddi ve manevi desteklerini esirgemeyen ve her zaman yanımda olan aileme en içten dileklerimle teşekkür ederim.

İstanbul; Temmuz 2023 Fırat KILINÇ

İÇİNDEKİLER

Sayfa

TABLOLAR LİSTESİ

ŞEKİL LİSTESİ

KISALTMALAR

AIDS	**:**	Anomaly Intrusion Detection System (Anomali Tabanlı Saldırı Tespit Sistemi)
CIC	**:**	Canadian Institute for Cybersecurity (Kanada Siber Güvenlik Enstitüsü)
CNN	**:**	Convolutional Neural Networks (Evrişimli Sinir Ağları)
CSE	**:**	Canada Communications Security Establishment (Kanada İletişim Güvenliği Örgütü)
DDoS	**:**	Distrubuted Denial of Service (Dağıtık Hizmet Reddi Saldırısı)
DNN	**:**	Deep Neural Networks (Derin Sinir Ağları)
DoS	**:**	Denial of Service Attack (Hizmet Reddi Saldırısı)
DRCNN	**:**	Deep Residual Convolutional Neural Network (Derin Artık Evrişimli Sinir Ağı)
DT	**:**	Decision Tree (Karar Ağacı)
FTP	**:**	File Transfer Protocol (Dosya Aktarım Kuralı)
GRU	**:**	Gated Recurrent Unit (Geçitli Tekrarlayan Birim)
HIDS	**:**	Host Intrusion Detection System (Kullanıcı Tabanlı Saldırı Tespit Sistemi)
HTTP	**:**	Hyper-Text Transfer Protocol (Hiper Metin Transfer Protokolü)
HTTPS	**:**	Secure Hyper Text Transfer Protocol (Güvenli Hiper Metin Transfer Protokolü)
IDS	**:**	Intrusion Detection System (Saldırı Tespit Sistemi)
IoT	**:**	Internet of Things (Nesnelerin İnterneti)
IoV	**:**	Internet of Vehicles (Araçların İnterneti)
IPS	**:**	Intrusion Prevention System (Saldırı Önleme Sistemi)
KNN	**:**	k-Nearest Neighbors (En Yakın Komşu)
LSTM	**:**	Long Short Term Memory (Uzun Kısa Süreli Bellek)
MEC	**:**	Mobile Edge Computing (Mobil Uç Bilgi İşlem)
MKD	**:**	Multi Teacher Knowledge Distillation (Bilgi Sentezleme ile Çoklu Öğretme)
ML	**:**	Machine Learning (Makine Öğrenmesi)
MTL	**:**	Multi Task Learning (Çok Görevli Öğrenme)
NIDS	**:**	Network Intrusion Detection System (Ağ Tabanlı Saldırı Tespit Sistemi)
PAOS	**:**	Pareto Over Sample (Pareto Örneği)
PCA	**:**	Principal Component Analysis (Temel Bileşen Analizi)
PCC	**:**	Pearson Correlation Coefficient (Pearson Ürün Momenti Korelasyon Katsayısı)

PPPL	**:**	Proportional Progressive Pseudo Labeling (Orantı Aşamalı Sözde Etiketleme)
RF	**:**	Random Forest (Rastgele Orman)
RNN	**:**	Recurrent Neural Network (Özyinelemeli Sinir Ağı)
SHAP	**:**	Shapley Additive exPlanations (Shapley Katkısı Açıklamaları)
SIDS	**:**	Signature Based Intrusion Detection Systems (İmza Tabanlı Saldırı Tespit Sistemi)
SSH	**:**	Secure Shell (Güvenli Kabuk)
SVM	**:**	Support Vector Machine (Destek Vektör Makinesi)
WEKA	**:**	Waikato Environment for Knowledge Analysis (Waikato Bilgi Analiz Ortamı)

ÖZ

Makine Öğrenim Yöntemleri Kullanılarak Saldırı Tespiti
Fırat KILINÇ
Milli Savunma Üniversitesi Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü
İstanbul, Temmuz 2023

Çağımızda bilgi teknolojileri hızla gelişirken mobil ve nesnelerin interneti (Internet of Things-IoT) cihazlarının yaygınlaşması ile birlikte siber saldırganlar da her geçen gün yeni saldırı yöntemleri geliştirmektedir. Bu nedenle siber saldırılar kullanıcılarda büyük endişe yaratmaktadır ve bu endişelerin de giderek artacağı öngörülmektedir. Bu süreçte saldırı tespit sistemleri (Intrusion Detection System-IDS) ve saldırı önleme sistemleri (Intrusion Prevention System-IPS) önemli bir rol almaktadır. Bu tez çalışmasında ilk olarak ağ güvenlik duvarları, ağ saldırıları ve ağ ortamında gerçekleşen saldırı türlerine yer verilmiştir. Sonrasında ağ saldırı türleri için örnek senaryolar oluşturulmuş ve bu senaryolar üzerinde saldırıların nasıl gerçekleştirildiği şekillerle açıklanmıştır. Bu tez çalışmasında Kanada İletişim Güvenliği Kuruluşu (Canada Communications Security Establishment-CSE) ve Kanada Siber Güvenlik Enstitüsü (Canadian Institute for Cybersecurity-CIC) tarafından yaratılan CIC-IDS2017 veri setinde yer alan saldırı türlerine yer verilmiştir. Bu saldırı türleri saldırganlar tarafından yaygın olarak kullanılan hizmet reddi saldırısı (Denial of Service Attack-DoS), dağıtık hizmet reddi saldırısı (Distrubuted Denial of Service-DDoS), botnet, kaba kuvvet, port tarama, web uygulama ve sızma saldırılarıdır. Tez kapsamında saldırı tespiti için CIC-IDS2017 veri setinde yer alan Çarşamba günü gerçekleştirilen DoS atakları verileri kullanılmıştır. Saldırı tespiti yapılırken orijinal veri setinin kullanımına, temel bileşen analizine (Principal Component Analysis-PCA) ve özellik seçimine dayalı olmak üzere üç farklı metot kullanılmıştır. Veri bölme yaklaşımı olarak %80 eğitim-%20 test yüzdelik bölme oranı, 5-kat ve 10-kat çapraz doğrulama tekniklerinden yararlanılmıştır. Saldırıların sınıflandırılması için Naive Bayes, destek vektör makinesi (Support Vector Machine-SVM), lojistik regresyon (Logistic Regression-LR), *k*-en yakın komşu (*k*-Nearest Neighbors), karar ağacı (Decision Tree-DT (J48)), AdaBoost, rastgele orman (Random Forest-RF) ve bagging yöntemleri kullanılmıştır. Deneysel sonuçlar, OneR özellik seçimi yöntemi ve rastgele orman sınıflandırıcıya dayalı metodun %99,96 doğruluk oranı ile en iyi sonucu verdiğini göstermektedir.

Anahtar Sözcükler: Siber Saldırı Türleri, Saldırı Tespit Sistemleri, Saldırı Önleme Sistemleri, Makine Öğrenmesi, DoS Saldırısı

Bilim Kodu : 92403, 92407, 92431, 92432
Sayfa Sayısı : xv+75
Tez Danışmanı : Doç. Dr. Can EYÜPOĞLU

ABSTRACT

Intrusion Detection Using Machine Learning Methods

Fırat KILINÇ

Turkish National Defense University, Atatürk Strategic Studies and Graduate Institue

İstanbul, July 2023

While information technologies are developing rapidly in our age, with the spread of mobile and Internet of Things (IoT) devices, cyber attackers are developing new attack methods day by day. For this reason, cyber attacks cause great concern for users and it is predicted that these concerns will increase gradually. In this process, intrusion detection systems (Intrusion Detection System-IDS) and intrusion prevention systems (Intrusion Prevention System-IPS) play an important role. In this thesis, first of all, network firewalls, network attacks and attack types in the network environment are given. Afterwards, sample scenarios for network attack types were created and how the attacks were carried out on these scenarios was explained with figures. In this thesis, the attack types in the CIC-IDS2017 dataset created by the Canadian Communications Security Establishment (CSE) and the Canadian Institute for Cybersecurity-CIC are included. These attack types are Denial of Service Attack (DoS), Distributed Denial of Service (DDoS), botnet, brute force, port scanning, web application and penetration attacks, which are commonly used by attackers. Within the scope of the thesis, the data of DoS attacks carried out on Wednesday in the CIC-IDS2017 data set were used for attack detection. While detecting the attack, three different methods were used, based on the use of the original data set, principal component analysis (PCA) and feature selection. As a data splitting approach, 80% training-20% test percentage splitting, 5-fold and 10-fold cross-validation techniques were used. Naive Bayes, support vector machine (SVM), logistic regression (LR), k-nearest neighbor, decision tree (DT-(J48)), AdaBoost, Random Forest (RF) and bagging for classification of attacks methods have been used. Experimental results show that OneR feature selection method and method based on random forest classifier give the best results with 99.96% accuracy.

Keywords: Types of Cyber Attacks, Intrusion Detection Systems, Intrusion Prevention Systems, Machine Learning, DoS Attack

Science Code : 92403, 92407, 92431, 92432
Pages : xv+75
Supervisor : Assoc. Prof. Can EYÜPOĞLU, Ph.D.

1. GİRİŞ

1.1. Giriş

Son yıllarda siber saldırıların sayısında ve çeşitliliğinde önemli bir artış görülmektedir. Ev kullanıcıları, kurumsal işletmeler, devlet kurumları ve kritik altyapılar, siber saldırganlar tarafından hedef alınmaktadır. Birçok durumda ağlara ciddi zararlar vermeden önce saldırıları çok erken aşamalarda tespit etmek çok önemlidir. Bu amaçla, siber güvenlik araştırmacıları ve profesyonelleri tarafından gerçek zamanlı savunma araçlarından olan saldırı tespit sistemleri (Intrusion Detection System-IDS) ve saldırı önleme sistemleri (Intrusion Prevention System-IPS) geliştirilmektedir.

Günümüzde siber güvenlik riski, toplumda önemli bir endişe kaynağı olmuştur. Devlet kurumları ve kurumsal işletmelere ait bilgiler, hayati derecede önemli olmasından dolayı güvenli bir şekilde muhafaza edilmelidir. Bu bilgiler, yetkisiz veya üçüncü kişilerin erişemeyeceği bir yerde saklanmalıdır.

Güvenli bilgileri muhafaza etmek zordur ve her zaman saldırganlar tarafından bir güvenlik ihlali riski vardır. En yaygın tehditler, bir web sitesine karşı düşmanlık, siber yarışmalar, fidye, siyasi mesele, eğlence vb. nedenlerle web sunucularının çökertilmesine yönelik yapılan saldırılardır. Siber güvenliğin temelini oluşturan üç ilke (gizlilik, bütünlük ve erişilebilirlik), güvenlik sistemlerinde etkin bir şekilde uygulanmalıdır (James, 2019).

Bu tez çalışmasında CIC-IDS2017 veri setinde ağ güvenliği ve izinsiz giriş tespit amaçları için kullanılan saldırı senaryolarına yer verilmiştir. Çalışmanın diğer bölümleri şu şekilde düzenlenmiştir:

İkinci bölümde, "Genel Kısımlar" başlığı altında saldırı tespit sistemleri ve saldırı önleme sistemleri ele alınmıştır. Saldırganların amaçları ile kötü amaçlı yazılımların belirtileri incelenmiştir. Ağ ortamında gerçekleşen saldırı türleri (hizmet reddi saldırısı, dağıtık hizmet reddi saldırısı, botnet saldırısı, kaba kuvvet saldırısı, port tarama saldırısı, web uygulama saldırısı ve sızma saldırısı) hakkında detaylı bir inceleme yapılarak örnek senaryolar ile anlatılmıştır.

Üçüncü bölümde, CIC-IDS2017 veri seti ile ilgili detaylı bir incelemeye yer verilmiştir. Günümüzde yaygın olarak kullanılan makine öğrenme yöntemlerinden olan Naive Bayes, destek vektör makinesi, lojistik regresyon, k-en yakın komşu, karar ağacı (J48), AdaBoost, rastgele orman ve bagging algoritmaları incelenmiştir. Veri madenciliğinde yaygın olarak kullanılan WEKA uygulaması kısaca tanımlanmış ve bu uygulamanın kullanıldığı bilgisayarın teknik özelliklerine yer verilmiştir. Daha sonra CIC-IDS2017 veri seti üzerinde farklı yöntemler ile kullanılan akış diyagramları gösterilmiştir.

Dördüncü bölümde, CIC-IDS2017 veri seti orijinal, temel bileşen analizi özellik şeçimi ve WEKA uygulaması üzerinde yaygın olarak kullanılan özellik seçimi yöntemlerine yer verilmiştir. Bahsedilen bu metotlar üzerinde üç ana yöntemde de %80 eğitim - %20 test yüzdelik oranı ve 5-kat veya 10-kat çapraz doğrulama modeli olmak üzere 3 farklı metot kullanılmıştır. Bu süreçte Naive Bayes, destek vektör makinesi, lojistik regresyon, k-en yakın komşu, karar ağacı (J48), AdaBoost, rastgele orman ve bagging makine öğrenme yöntemleri kullanılmış ve ulaşılan sonuçlar tablolarda sunulmuştur.

Beşinci bölümde ise bu tez çalışması kapsamında ulaşılan sonuçlara istinaden genel bir değerlendirme yapılmıştır.

2. GENEL KISIMLAR

2.1. Saldırı Tespit ve Önleme Sistemleri

Siber güvenlik, günümüzde bilgi teknolojisinin gelişmiş olması nedeniyle çok önemlidir. Çeşitli saldırı metotlarını beraberinde getiren internetin gelişimi, siber saldırıları önlemek için de çok sayıda önlemle korunmaktadır. Bunlardan izinsiz giriş tespit sistemi dahil olmak üzere bu saldırılar içinde saldırının hem nicelik hem de niteliğinin yükselmesine yanıt olarak IDS, sürekli olarak geliştirilmeye devam edilmiş ve elde edilen bilgiler IDS'ye entegre edilmiştir. Bu çalışmada, makine öğrenme yöntemlerinden olan derin öğrenme, son derece takdir edilen ve gelecekte genişleme potansiyeline sahip olan ve karşılaştırıldığında ağ anormalliklerini yüksek doğrulukta tespit eden bir yöntem olduğunu göstermiştir. Diğer bir deyişle, derin öğrenme yöntemleri arasında da bir karşılaştırma yapılmıştır. Bu derin öğrenme yaklaşımları, tekrarlayan sinir ağı (Recurrent Neural Network-RNN), uzun kısa süreli bellek (Long Short Term Memory-LSTM) ve geçitli tekrarlayan birim'dir (Gated Recurrent Unit-GRU). CIC-IDS2017 ve CSE-CICIDS2018 olmak üzere iki veri kümesinde anomali tespiti yapılmaya çalışılmıştır. CIC-IDS2017 veri seti açısından LSTM ve GRU ile karşılaştırma (~%7) ile kıyaslandığında RNN'nin FPR'si daha yüksektir. Bunun anlamı, RNN'nin yanlış alarm oranı çok daha yüksektir. Ayrıca FNR, RNN, LSTM ve GRU'dan biraz daha büyüktür (~%2); bu ise daha yüksek bir kayıp oranını gösterir. GRU modeli, bir daha düşük FNR açısından LSTM'den daha iyi sonuç verdiğini tespit etmiştir (Hai & Nam, 2021).

Siber güvenlik camiasında, siber saldırılarda son yıllarda benzeri görülmemiş bir artış olayına tanık olunmuştur. Bu saldırganlar, hedef ve amaçlarına ulaşmada başarılı olduklarını kanıtlamışlardır. Bu sebeple, yıkıcı saldırılara karşı ana savunma noktası izinsiz giriş tespit ve önleme sistemlerinin geliştirilmesi devam etmektedir. Ancak, geçmişteki anomali veri kümelerinin çoğu ne günceldir ne de güvenilirliği kalmıştır. Araştırmacılar, makine öğrenimi kullanarak anomali tabanlı saldırıları sınıflandırma teknikleriyle bu tür saldırıların gelişimine ayak uydurabilmiş ve cesaret verici tahminlerde bulunmuşlardır. Bu süreçte bu tür izinsiz girişlerin tespitinde derin sinir

ağlarının, tespit ve karakterize etmede devrim niteliğinde olduğu ortaya çıkmıştır. Bu çalışmada, CIC-IDS2017 ve CSE-CICIDS2018 adlı iki kapsamlı veri kümesi kullanılarak derin sinir ağları tespit görüntü tabanlı bir yöntemle çeşitli saldırılar sınıflandırılmış ve sonrasında en iyi ağ akışı özelliklerinin bir listesi sunulmuştur. Bu saldırıları tespit etmek için evrişimli bir nöral konuşlandırılmış ve ağ modelinin, farklı saldırıları sınıflandırmak ve karakterize etmek için umut verici değerlendirme sonuçları görülmüştür (Kaur et al., 2020).

Kritik altyapıların ve bilgi sistemlerinin güvenliğini sağlamak her zaman zorlu bir iş olmuştur. IDS, ağ güvenliğinin sağlanmasında vazgeçilmez bir unsur haline gelmiştir. IDS sistemlerinin izinsiz giriş tespit performansını artırmak önemlidir. IDS sistemlerini iyileştirmek için birçok çalışma yapılmış olsa da hala eksiklikler vardır. Bu çalışmada, IDS sistemleri için yeni bir Switch port anomali tabanlı IDS (SPA-IDS) veri seti önerilmiştir. Bu araştırma, veri alınır normal internet trafiği ile anahtar bağlantı noktaları üzerinden yeni bir otomatik izinsiz giriş sınıflandırması sunmakta olup, toplanan sinyalleri kullanarak modellenmiştir. Yerel ağ katmanlarından 2'inci katmandan elde edilen bu sinyaller, otomatik sınıflandırma model, dikey mod ayrıştırma (VMD) ve istatistik, yinelemeli özellik kullanılarak özellik oluşturmadan oluşur seçim ve sınıflandırma aşamaları uygulanmış olur. Bu aşamalar, şu şekilde uygulanmaktadır:

1. Alınan sinyallere VMD uygulanır ve beş VMD katsayısı elde edilir. Sinyale ve hesaplanan VMD'ye 15 istatistiksel katsayılar uygulanır.
2. Çıkarılan özelliklere yinelemeli özellik seçimi uygulanır ve en değerli özellikler seçilir.
3. Seçilen özellikler, karar ağacı (decision tree-DT), torbalı ağaç (bagget tree-BT), destek vektör makinesi (support vector machine-SVM) kullanılarak sınıflandırılır ve SVM ve 10-kat çapraz doğrulama ile k-en yakın komşu (KNN) makine öğrenme yöntemleri kullanılır. Sunulan VMD ve yinelemeli özellik seçimi, tabanlı model %87,25, %95,98, %96,51 ve %97,74'e ulaşmış; KNN, SVM, DT ve BT sınıflandırıcılarını arka arkaya kullanarak doğrulukları tespit edilmiştir. Saldırı kategorizasyon sürecinden sonra çalışmanın ikinci aşamasında aynı sınıflandırıcıların başarı oranları sırasıyla %96,65, %98,52, %98,39 ve %99,11'e ulaşmıştır. Hesaplanan/elde edilen doğruluklar, açıkça sunulan VMD'nin başarısını göstermiş ve yinelemeli özellik seçimine dayalı

saldırı tespit sistemi modeli, en iyi sonucu vermiştir. Bu çalışmada sunulan yöntem nedeniyle gelen saldırıları önlemek için 2'inci katmanda alınan paketleri analiz ederek etkili ve hızlı bir IDS yaklaşımı sonucu ortaya çıkarılmıştır (Kilincer et al., 2023).

Nesnelerin interneti (IoT) cihazlarını kullanan kişi sayısı, son yıllarda artmıştır. Nesnelerin İnterneti cihazlarının çok sayıda alanda konuşlandırılmasındaki gelişmeler, onları saldırılara karşı savunmasız hale getirmektedir. Sınırlı kaynaklardan pille çalışan bu mütevazı cihazlarda, gelişmiş kriptografi oluşturulamamaktadır. Ancak kısıtlı cihazların benzersiz özelliklerinden dolayı mevcut çözümler, koruma sağlamak için yetersiz kalmaktadır. Bu sebeple saldırıları tespit etmek ve kategorize etmek için anomali tabanlı saldırı tespit sistemi kullanılır. Bu çalışmada, makine öğrenimi yöntemlerinden derin öğrenme (Deep Learning-DL) teknikleri kullanılarak konusunda yetenekli zekâyı IoT cihazlarına ve ağlarına yerleştirmek, çeşitli güvenlik sorunlarını çözebilir. Bu çalışmada, kötü amaçlı paketleri gerçek zamanlı olarak belirlemek için derin bir sinir ağı tabanlı izinsiz giriş tespit sistemi önerilmiştir. Modeli eğitmek için yeni geliştirilen kıyaslama Netflow tabanlı veri kümeleri kullanılmıştır. Önerilen modelde gerçek zamanlı saldırı tespiti için paket yakalama ve tespit algoritması doğruluğunu da göstermektedir (Vishwakarma & Kesswani, 2022).

Güvenlik sorunları, büyük veri ve bulut bilgi işlem internet ile ilişkili yeni teknolojilerin karşılaştığı en kritik zorluklardır. Güvenlik tehditlerini tespit etmek için güvenli ve verimli bir saldırı tespit sistemi çok önemlidir. Mevcut IDS'lerin birçok saldırıya karşı zayıf kaldığı bilinmektedir. Başta yüksek yanlış pozitif uyarı oranı olmak üzere, saldırıları tespit etmek için gereken uzun süre ve sıfırıncı günü tespit edememe, şirketleri saldırılara karşı zor durumda bırakacaktır. Bu çalışma, iki süreç aracılığıyla IDS algılama mekanizmalarını önerir ve geliştirir. İki varsayıma dayalı tehdit tespiti için yeni özelliklere sahip bir derin sinir ağı modeli kullanma, düşük bilgi işlem gücü ve kaynakları ile sıfır gün saldırılarının ele alınmasıyla ilgili ve kapsamlı DNN modelini ve temel bileşen analizini birleştirerek saptama çözümü, güvenliği ve performansı artırmaktadır. Önerilen algılama mekanizması, DNN, PCA, istatistiksel ve belirtildiği gibi mevcut IDS'den önemli ölçüde daha fazla verimlilik sunmak için analitik ve yazılım sonuçlarına göre bilgiye dayalı yaklaşımlardır. Büyük ağlar için önerilen algılama teknikleri analiz edilir ve tasarımdaki karmaşıklık, DNN modeli katmanlarının sayısı azaltılarak önlenir. Böylece algılama süresi gecikmesi ve

yanlışlık pozitifler ile ağ saldırılarına karşı güvenliği artırırken en aza indirilir. Önerilen DNN'yi PCA ile entegre etmek, bir yenilikçi katkı, algılama süresi gecikmesini önemli ölçüde iyileştirmek için sağlam güvenlik performansıdır. Önerilen model %98 doğruluk oranı göstermiştir. Çok sayıda saldırıya dayalı olarak belirtilen en yüksek doğruluk oranı %97 olarak ortaya çıkmıştır (Al-Fawa'reh et al., 2022).

Hizmet reddi saldırısı, yetkisiz kullanıcılar tarafından bilgi işlem kaynaklarından olan ağ bant genişliğine ve hedeflenen sisteme saldırı yaparak istemcilerin hizmet almasını engellemektir. Bu çalışmada, makine öğrenme yöntemlerinden özellik seçimi yapılan sinir ağı yöntemi kullanılmıştır. Önerilen yöntem üç aşamaya ayrılmıştır: Bunlar özellik seçimi, eğitim ve test verisi şeklindedir. İnternet ağında bulunan bulut bilişim ağında farklı türde DoS saldırıları mevcuttur. Bu araştırma çalışmasında, Kanada Bilimler Enstitüsü tarafından geliştirilen CIC-IDS2017 veri seti kullanılmıştır. Bu veri setinin %80 kullanılmıştır. Daha sonra iyi huylu trafik, kullanılan araçlara göre akış kayıtları Slowloris, Slowhttptest, Hulk ve Benign olarak etiketlenmiştir (Bhargav et al., 2022).

Dünya çapında bilgisayar ağlarının büyümesiyle birlikte, ağ üzerinden bulunan veri ve bilgilerin korunmasına yönelik daha büyük bir ihtiyaç oluşmuştur. İnternet ağında büyük miktarda hacimdeki artış, hız ve veri çeşitliliği, bir saldırıyı analiz edebilen daha sağlam ve doğru algılama sistemi gerektirir. Bu çalışma, bir saldırı tespit sisteminin oluşturulmasını önermektedir. Bu çalışmada, akış sınıflandırıcıları ve üç sınıflandırma katmanı kullanılarak kayıtların özellik sayısında bir azalma olmadan sınıflandırılmıştır. Önerilen sistem tarafından elde edilenler, diğerleriyle karşılaştırılmış ve doğrulamak için iki veri seti kullanılmıştır. Literatürde önerilen modeller, önerilen sistem her durumda, doğrulukta şu kadar kazanç sağlar: NSL-KDD veri setleri kullanılarak %18,52 ve CIC-IDS2017 veri seti %3,55 elde edilmiştir. Sınıflandırma süresinde azaltma yapıldığında ise NSL-KDD kullanılarak %35,51'e kadar ve CIC-IDS2017 veri seti %94,90'a kadar daha yüksek bir sonuç elde edilmiştir (Schuartz et al., 2022).

Otonom araçlar dâhil olmak üzere modern araçlar, dünyamızda giderek artan bir şekilde çeşitli harici işlevler ve hizmetler sağlamaktadır. Fakat gelişen internet bağlantısı, internete bağlı araçlar (Internet of Vehicles-IoV) güvenlik açıkları, siber tehditlerin saldırı çeşitliliğini de artırır. Modern araç sistemlerini korumak için kimlik doğrulama ve şifreleme eksikliği nedeniyle araç ağlarındaki ağ saldırıları,

prosedürlerden koruyan IDS'ler temel yaklaşımlardır. Bu çalışmada, makine öğrenme yöntemlerinden olan transfer öğrenme, topluluk öğrenme tabanlı ve IoV sistemleri için ise evrişimli sinir ağları (Convolutional Neural Networks-CNN) ve hiper parametre optimizasyon teknikleri IDS önerilmiştir. Deneylerde, önerilen IDS %99,25'in üzerinde saptama oranları ve F1-skorları göstermiştir. Bu çalışmada en yaygın kullanılan veri setlerinde olan IoV güvenlik veri setlerinden olan Car-Hacking veri seti ve CIC-IDS2017 veri seti kullanılmıştır. Sonuç olarak siber saldırı tespiti için hem araç içi hem de harici araç ağlarında önerilen IDS'nin etkinliği incelenmiştir (Alhabshy et al., 2022).

Hem makine öğrenimi hem de derin öğrenme izinsiz giriş tespit sistemlerinin IDS'le geliştirilmesinde büyük ilerleme kaydetmiş olsa da iki kritik sorun devam etmektedir. Birincisi, kötü niyetli etkinliğin sürekli gelişen doğasıdır. Veri akışları ve paketler, aynı anda birkaç türde saldırı içerebilirken; makine öğrenimi ve derin öğrenme algoritmaları aynı anda yalnızca tek bir görevi öğrenebilir. İkinci olarak, yalnızca bir tür saldırıyı değerlendirmek için, halka açık veri kümeleri oluşturulur. Bu sorunları çözebilmek için bu çalışmada, aynı anda birkaç saldırı türünü tespit etme yeteneğine sahip derin sinir ağlarına (Deep neural networks-DNN) dayalı bir IDS için çok görevli öğrenme (Multi Task Learning-MTL) modeli önerilmektedir. Bunu yapmak için hem UNSW-NB15 hem de CIC-IDS2017 veri kümelerindeki karşılık gelen her örnek tek bir özellik vektöründe birleştirilmiştir. Bu durum hem eğitim hem de test setlerindeki veri akışlarının bir kısmının aynı anda iki tehdit içerdiğini garanti etmektedir. Deneysel sonuçlar, önerilen sistemin performansı maksimize ettiğini göstermektedir (Albelwi, 2022).

Siber güvenlik, bilişim sektöründe yükselen bir alandır. Sınırsız iletişim paradigmasının yükselişi ve son zamanlarda genişleyen ağa bağlı dijital cihaz yelpazesi nedeniyle siber güvenlik konusunda endişeler artmıştır. IDS, verileri veya sistemin bakımını amaçlayan iletişim teknolojisi ağ güvenliğinin önemli bir parçasıdır. Bilim adamlarının ilgisini çeken IDS, uzmanlık olarak makine öğrenimi teknikleri son zamanlarda yakalanmıştır. IDS, öncelikle ağı izler ve etkinlik ve güvenlik sorunlarının belirtilerini değerlendirir. Bu araştırma, izinsiz giriş tespit sistemlerinin çeşitli veri kümelerini kapsar ve çeşitli makine öğrenimi algoritmalarıdır. Teknolojiler, IDS sistemlerini oluşturmak için yaygın olarak kullanılır. Verimli sonuçları birçok alanda elde edilmiştir. Literatürde yayımlanan araştırmalar ve ayrıca bu araştırma, KDD Cup

99 üzerinde deneysel analizler gerçekleştirir ve ensemble ile birlikte CIC-IDS2017 veri kümeleri kullanılmıştır. Doğruluk, kesinlik, geri çağırma ve F1 skoru sonuçları görüntülenir. Araştırmanın gelişimi, hesaplama teknolojilerine dayalı IDS sistemlerinin makine öğrenmeye yardımcı olması beklenmektedir (Gosai et al., 2022).

İnsansız hava aracı kolonilerinin uyumu, bir ağda yüksek hareket kabiliyeti ve manevra kabiliyetlerine atfedilen zaman açısından güvenlik gözetimi, afet yönetimi, arama ve kurtarma operasyonları gibi kritik operasyonlar için konuşlandırılabilir hale getirir. Bu ağın güvenlik durumunun önemli ölçüde ihmal edilmesi, işgalcilerin saldırılarını teşvik eder. Böylece ağ bunun misyonunu engeller. Bu çalışmada, mobil uç bilgi işlem (Mobile Edge Computing-MEC) teknolojisi ve anormallik tabanlı izinsiz giriş tespit şeması ve makine öğrenme yöntemlerinden olan rastgele orman ve UAV-MEC sunucularına gömülü model kullanarak bu zorlukların üstesinden gelinmiştir. Seçim modellemek için öne çıkan özelliklerin ve hiperparametrelerin optimize edilmiş saldırı tahmincisi, Pearson korelasyon katsayısı ve rastgele arama çapraz doğrulama teknikleri tarafından etkinleştirilmiştir (Pearson Correlation Coefficient-PCC). Ayrıca, önerilen modelin eğitimi ve değerlendirilmesi için izinsiz giriş tespit veri seti olan CIC-IDS2017 verileri kullanılmıştır. Simülasyon tespitinde ve sınıflandırılmasında model tarafından elde edilen sonuçlar, ağdaki farklı saldırılar doğruluk = %99,87, kesinlik = %99,32 ve F1 puanı = %99,06 diğer optimize edilmiş makine öğrenimi modellerine göre üstünlük ve önceki araştırmalarda kullanılan bazı mevcut modellerdendir (Ihekoronye et al., 2022).

Son yıllarda kaydedilen tüm ilerlemelere rağmen, ağ sistemlerindeki anormalliklerin tespitinde görünmeyenlerin tespit edilmesinde sıfırıncı gün saldırıları gibi anormallikler hâlâ zorlu bir sorun olmaya devam etmektedir. Geleneksel imza tabanlı ağ tabanlı izinsiz giriş tespiti sistemleri (Network Intrusiin Detection System-NIDS), hiçbir anormallik olmadığı için bu tür anormallikleri tespit edemez. Makine Öğrenimi tabanlı NIDS, normal denetimli öğrenimle farklı bir kaynaktan geldikleri için eğitilmiş ve yöntem onları tespit edememiştir. Etki alanı uyarlama teknikleri, etiketli bir kaynak etki alanından etiketlenmemiş bir hedef etki alanına edinilen bilgilerin aktarılmasına yardımcı olur. Bu tür teknikler, üzerinde eğitilmiş bir model yapma potansiyeline sahiptir. Yeni türleri tespit etmek için birkaç ağ saldırısı içeren bir veri kümesi, gelecekte olabilecek anomalilerin ancak son zamanlarda etki alanı uyarlama yöntemleri çoğunlukla görüntüler için tasarlanmıştır ve ağ trafiğine uygulandığında

çok sınırlı faydalar sağlar. Bu yazıda, orantılı aşamalı sözde etiketleme (Proportional Progressive Pseudo Labeling-PPPL), daha fazlasını oluşturmak için etkili bir yaklaşım kullanılabilecek genel etki alanı uyarlama tekniği ağ sistemlerindeki görünmeyen anormallikleri tespit etmiştir. Başlangıçta eğitim aşamasında, PPPL kademeli olarak hedef alanı modeli doğrudan sözde etiketli ile eğiterek sınıflandırma hatası ile örnekleri hariç tutarken; hedef etki alanı örnekleri eğitimden yanlış olma olasılığı daha yüksek olan sözde etiketler, bu tür numuneler üzerinde eğitim ayarlamak ve ertelemek azaltır. Değerlendirmemiz CIC-IDS2017 veri seti üzerinde yapılan çalışmalar, PPPL'nin şunları yapabileceğini göstermektedir: görünmeyenleri tespit etmede diğer temel çizgilerden önemli ölçüde daha iyi performans gösterir. Ortalama F1'e göre %58'e varan iyileştirme ile anormallikler amaçlanmıştır (Hashemi et al., 2022).

Saldırganlar tarafından yapılan saldırılar ve izinsiz girişler, internet ağının birincil güvenlik konusu haline gelmiştir. Bu saldırılar, sistem arızası, ağ arızası, veri bozulması veya çalınmasına neden olabilir. Bir ağ saldırı tespit sistemi, kullanılan bilgisayar ağında yetkisiz ve kötü niyetli davranışları belirlemek için ağ trafiği gözlemleyen bir araçtır. Son teknolojiler, saldırı tespit sistemlerinin tamamını inceleyerek bir saldırıyı tespit etmek için tasarlanmıştır. IDS'nin yalnızca sistemde çalıştıktan sonra bir saldırıyı tespit edebilmesi, saldırı altında ve sisteme zarar vermiş olabilir. Bu çalışmada, uçtan uca bir ağ saldırılarını daha fazla zarara neden olmadan önce önlemek için öngörülemeyen saldırıları önlerken; sisteme zarar vermeden ve kesinti olmadan erken izinsiz giriş tespit sistemi önermişlerdir. Saldırı tanımlama için sınıflandırıcı ve makine öğrenim yöntemlerimden derin sinir ağı tabanlı kullanıyoruz. İlgili özellikleri ham dosyadan çıkarmak için denetimli bir şekilde manuel bir özelliğe güvenmek yerine, ağ trafiği verileri ilgili yaklaşımların çoğunda kullanılan seçim süreci uygulanmıştır. Ayrıca ne kadar erken olduğunu değerlendirmek için erkencilik adı verilen yeni bir metrik tanıtarak yaklaşım saldırıları tespit etmiştir. Çalışmada CIC-IDS2017 veri seti kullanılarak nihayetinde yaklaşımımızın iyi performans gösterdiği ve genel bir 0,803 dengeli doğruluk oranı yakaladığı belirtilmiştir (Ahmad et al., 2022).

Ağ kullanılırken çeşitli adreslerden saldırı gerçekleşir. Zarar verme eylemlerine iletişim sistemleri göre ağ işleyişi ve siber saldırı önemli bir konudur. Gizlilik, özgünlük veya bir kaynağın erişilebilirliği, yetkisiz kişiler tarafından tehlikeye atılabilir izinsiz giriş tespit sistemlerinin yapabileceği etkinlik veya saldırıları

belirlemeye yardımcı olur. Araştırmacılar, izinsiz giriş tespitinin geçmişi, bugünü ve potansiyeli hakkında makaleler, kablosuz ağlardaki sistemler, araştırma bulgularını keşfetmektedir. İstatistiksel modelleme ve derin öğrenme günlüklerin bulgularını analiz etmek için kullanılır. İzolasyon, doğru bilgi elde edebilen stratejilerden biridir. Yani ağ ölçümleri yapar ve yükselterek uygun seçimler üretir. Bu çalışmada, bir ağ izinsiz girişlerinin tespiti için karar ağacı tabanlı yöntem geliştirilmiştir. Veri kalitesini iyileştirmek için ve uygun eğitim, ağ veri ön işlemesi sağlamak ve entropiye dayalı nitelik seçimi özel olarak yürütülür. Daha sonra bir izolasyon ormanı sınıflandırıcısı, doğru saldırı tespiti için inşa edilmiştir. Deneysel iki veri setinin analizi, önerilen modelin güvenilir sonuçlar üretme yeteneği kullanarak CIC-IDS2017 ve NSL-KDD veri setleri, modelimizin doğruluğu sırasıyla %99,98 ve %99,82'dir. Mevcut sistemlerden alarm oranı, tespit oranı ve doğruluk ile karşılaştırıldığında modeller, yeni yaklaşımın yanlış açısından birçok faydası vardır (Singh & Deorari, 2022).

Son on yılda anomali tabanlı IDS, birçok çalışma ile kendini kabul ettirmiştir. Özellikle derin öğrenme modelleriyle etkinliğini kanıtlamıştır. Bununla birlikte, bu modeller daha karmaşık hale gelmiştir ve bu nedenle sistemin kararlarını açıklamak insanlar için zordur. IDS'lerin şeffaflığını artırmaya yönelik araştırmalar, araştırma topluluğundan yetersiz kalmaktadır. Bu çalışma, doğru bir şekilde yapabilen açıklanabilir bir NIDS önermektedir. Saldırıları tespit etmek ve bunun için açık açıklamalar sağlamak kararlar. IDS, Shapley Katkı Maddesini IDS kararlarını hesaba katmak için açıklamalar (Shapley Additive exPlanations-SHAP) çerçevesi kullanır. IDS'mize kararlarını hem yerel hem de global düzeyde kendi kendine açıklama konusunda küresel seviyeler de yardımcı olur. Yerel açıklama, IDS kararlarını açıklar ve her bir spesifik numune için global seviye ise özelliğin önemini ve saldırıların özelliklerini gösterir. Etkinliği göstermek için teklifimizi iki veri setinde değerlendiriyoruz. İyi bilinen IDS veri kümeleri, KDD Cup 99 ve CIC-IDS2017'dir. İçinde ek olarak, sadece makineyi yorumlamakla kalınmamış; öğrenme modeli değil, aynı zamanda derin öğrenme modeli tanımlanmıştır. Bu araştırmanın, güvenlik uzmanları için daha derin tespit yöntemi ve anomali tabanlı IDS'nin şeffaflığını artırması beklenmektedir (Nguyen et al., 2022).

Bu çalışmada, DDoS ve DNN akış tabanlı ağ bilgilerine dayalı ağ kullanan saldırı tespit yöntemi kullanılmıştır. Yöntemde özellik için radyal temel fonksiyon benimsenmiştir. DNN'nin doğruluğunu artırmak için CIC-IDS2017 veri kümesi

kullanılarak akış tabanlı algılamayı eğitmek ve test etmek için kullanılır. Deneysel sonuçlar, DDoS tespitinin önerilen yöntemin veri kümesi altındaki doğruluğu %99,37'dir (Leung & Lee, 2022).

Makine öğrenimine dayalı ağ akışı için anormallik algılama modelleri, son derece dengesiz eğitim verileri koşullarında zayıf algılama performansına ve ayrıca ağ uç cihazlarına dağıtırken yavaş algılama hızına ve büyük kaynak tüketimine sahiptir. Anormallik tespitine çoklu öğretmen bilgi distilasyonunu (Multi Teacher Knowledge Distillation-MKD) yerleştirmek, bilgiyi birden çok modelden tek bir modele aktarabilir. Bu çalışmada, algılama performansını iyileştirmek için son teknoloji bir model olan MKDNAD'ı çalışmışlardır. MKDNAD, küçük örnek sınıflarının algılama doğruluğunu geliştirmek için ağ akışında yer alan tek boyutlu sekans ve iki boyutlu görüntü bilgisini araştırır ve entegre eder. CIC-IDS2017 veri kümesindeki deneyler, yöntemimizin küçük örnek sınıflarla başa çıkmada algılama hızı ve algılama doğruluğundaki iyileştirmelerini doğrulamaktadır (Yang & Liu, 2022).

Dijital olarak birbirine bağlı dünyamızda veri ağları, iletişim alanında önemli bir rol oynamaktadır. Veri alışverişi, işlemler ve diğer alanlarda büyük büyüme hassas verilerin korunması gerekir. Ağlar arasında kusursuz veri iletimi için kötü amaçlı yazılım saldırılarından cihazlar ile korunulabilir. Kötü amaçlı yazılım saldırılarının bazı zararlı sonuçları, idari kontrol ve veri ihlallerine sebep olmaktadır. Kötü amaçlı yazılım tespiti, bunlardan kurtulmak için önemli bir görev haline gelmiştir. Bu çalışmada, kötü amaçlı yazılımlara karşı makine öğrenimi algoritmaları kullanılmakta olup algılama veri kümeleri NetML ve CIC-IDS2017 iken; trafik sınıflandırma veri kümesi vpn2016 olmayan veri kümesidir. Sonuçlar çok ümit vericidir ve elde edilen sonuçlarla doğrulanmıştır. NetML Network Traffic Analytics Challenge 2020 ACANETS tarafından CIC-IDS2017 ve nonvpn2016'daki veri kümeleri, temel sonuçlardan beş parçanın tümüne daha iyi performans göstermiştir (Katherasala et al., 2022).

Siber dünyada uygun güvenlik çözümleri, gerçek zamanlı ağ güvenlik açıklarına ve verilerine karşı ağ koruması sağlayarak ağ güvenliğini sağlamak çok önemlidir. Etkili bir izinsiz giriş tespit stratejisi, kritik sistemleri korumak için yetkisiz erişime veya saldırıya karşı bütüncül bir yaklaşım benimsemek gerekmektedir. Bu çalışmada, makine öğrenimi tabanlı kapsamlı bir güvenlik çözümü, topluluk denetimli makine öğrenimi kullanarak ağ izinsiz giriş tespiti için çerçeve ve topluluk özellik seçim

yöntemleri kullanılmıştır. Ek olarak, birkaç makine öğrenimi modelinin özellik seçim yöntemleri ile karşılaştırmalı bir analizi yapılmıştır.

Bu araştırmanın amacı, tasarım genel bir algılama mekanizması ve minimum yanlış pozitif oranlar (FPR) ile daha yüksek doğruluk elde etmektir. NSL-KDD, UNSW-NB15 ve CIC-IDS2017 veri setleri kullanılmıştır. Algılama modelimizin izinsiz girişlerin %99,3'ünü tanımlayabildiğini göstererek yanlış alarmların en düşük %0,5'i ile başarılı bir şekilde mevcut çözümlere kıyasla daha iyi performans gösterdiği sonucuna ulaşılmıştır (Das et al., 2021).

Ağ saldırı tespit sistemi, karmaşık ve değişken ağ ortamında önemli bir savunma aracıdır. Bu çalışmada, çoklu saldırıları belirlemek için derin öğrenme modeli ve ağdaki izinsiz girişler incelenmiştir. Model Pareto üzeri örneği ile ayrılmıştır (Pareto Over Sample-PAOS). Sınıf dengesizliği işleme modülü ve derin artık evrişimli sinir ağı (Deep Residual Convolutional Neural Network-DRCNN) saldırı tespit modülü azaltmak için kullanılır. Aşırı örneklenmiş veriler tarafından ortaya çıkan gürültüler ve ikinci olarak tek boyutlu evrişimli sinir sisteminin kalıntı yapısı, çeşitli saldırıları öğrenmek ve tanımlamak amaçlanmıştır. Bu çalışmada CIC-IDS2017 veri seti kullanılmıştır. Sınıflandırıcının ulaşabileceği 15 sınıf sınıflandırma doğruluğu %99,86'ya ulaşılmıştır. Sonuç olarak PAOS-DRCNN modelinin şunları yapabileceğini göstermektedir: DOS, DDoS, botnet ve port taraması gibi çeşitli farklı saldırıları etkili bir şekilde tanımlamıştır (Dang & Li, 2022).

Ağ trafiğindeki hızlı büyüme ve artan güvenlik tehditleri nedeniyle siber güvenlik alanında güvenlik sağlamak için saldırı tespitinde IDS'nin önemi giderek daha kritik hale gelmiştir. Sağlam bir yerel ağ tasarlamakta birçok zorluk vardır. Özellikle öngörülemeyen yüksek boyutlu anomali saldırıların verileriyle uğraşırken verimli ve doğru IDS ön plana çıkmaktadır. Bu çalışmada, dönüşüm tabanlı izinsiz giriş tespiti sistemini önermekte, boyut azaltma arasında bir denge kurmak için özellik gösterimlerini yeniden yapılandırmakta ve dengesiz veri kümelerinde özellikler ortaya çıkarılmaktadır. CIC-IDS2017 ve CIC-DDoS2019 adlı veri kümeleri ile klasik makine öğrenimi algoritmaları olan destek vektör makinesi ve derin ile karşılaştırmalı bir çalışma tekrarlayan sinir ağı, bulanık sinir ağı ve uzun önerilen yöntemin geçerliliğini göstermek için kısa süreli bellek ağı uygulanmıştır. Sonuç olarak RTIDS'in halka açık iki gerçek trafik izinsiz giriş tespiti üzerindeki etkinliğini ortaya çıkararak, sırasıyla %99,17 ve %98,48 F1 Puanı değerlerine ulaşılmıştır (Wu et al., 2022).

2.2. Ağ Güvenlik Duvarları

İnternet ağındaki veriler istemci bilgisayar kullanıcısına gönderilen ve hangi kaynaktan gelip, hangi hedefe ulaşması gerektiğine ilişkin bilgileri içermektedir. Ağ güvenlik duvarları ise istemci bilgisayar kullanıcılarını internet ağındaki kötü huylu saldırgan veri trafiklerinden savunan donanım ve yazılım araçları olarak tanımlanabilirler. Ağ yöneticisi tarafından ağ güvenlik cihazı üzerinde veri akış trafiğini denetlemek için kurallar tanımlanır. Ağ yöneticisi tarafından tanımlanmış olan kurallar yetkisiz kişilerin ve istenmeyen verilerin yerel ağlara girmesini engeller; bu sayede ağlar arasındaki güvenli veri trafiği düzenlenir ve ağ cihazları kötü amaçlı saldırılara karşı korunmuş olur. Bu kurallar dizisinde zararsız olduğu tanımlanan verilerin geçişine müsaade edilirken zararlı veri olduğu tespit edilenlerin ağ dışında kalması sağlanır. Ağ üzerindeki saldırıları tespit etmek ve önlemek için kullanılan sistemler literatürde temel olarak IDS ve IPS olmak üzere iki ana başlıkta incelenir.

2.2.1. Saldırı Tespit Sistemi

IDS'ler özel bir ağ aygıtı veya bir sunucu üzerine kurulabilen güvenlik duvarlarındaki kötü amaçlı trafikleri tespit etmek için kullanılır. Temelde bu trafiklerin kötü amaçlı olup olmadığı, kural tabanlı ve imza tabanlı olmak üzere iki farklı analiz yöntemi ile gerçekleştirilir (Taner, 2019). IDS tarafından söz konusu kötü amaçlı trafikler günlük olarak tespit edilir, yapılan tespitler sisteme kaydedilir ve ağ yöneticisine uyarı mesajı gönderilir. Özellikle, IDS tarafından kötü amaçlı trafiklere reaksiyon gösterilmez ve önlem alınmaz. Dolayısıyla, IDS'nin temel görevi saldırıları önlemek değil saldırıları tespit edip kaydetmek ve ağ yöneticisine raporlamak olarak ifade edilir.

IDS'nin en önemli dezavantajlarından birisi gerçekleştirdiği taramalar nedeniyle ağı yavaşlatmasıdır. Genellikle gecikme süresi olarak da ifade edilen bu yavaşlamayı engellemek amacı ile IDS'nin çevrim dışı çalıştırıldığı durumlar da söz konusudur (Taner, 2019). Bu yöntemde, sistemden geçiş yapacak veriler kopyalanarak ağ yöneticisi tarafından belirlenmiş kurallar kapsamında değerlendirilmesi maksadıyla çevrimdışı çalışan IDS'ye iletilir. Bunların dışında sunucu bilgisayarındaki işletim sisteminin (Linux ve Windows vb.) üzerine yüklenebilecek bir uygulama olarak da kullanılan IDS'ler mevcuttur.

2.2.2. Saldırı Önleme Sistemi

IPS'de IDS'de ifade edilen görevlere ilave olarak ağ güvenliğini sağlayacak aktif çözümler bulunmaktadır (Taner, 2019). IPS, aynı IDS'de olduğu gibi ağ yöneticisince belirlenen kurallar ışığında veri trafiğini analiz ederek kötü amaçlı trafikler tespit eder. Ancak, ilaveten kötü amaçlı trafiklerin sistemlere girişinin engellenmesi de sağlanır. Tüm bunların yanında IPS'nin yaptığı işlemler sisteme kaydedilerek ağ yöneticisine raporlanır ve bu sayede daha efektif performans analizi yapılmasına imkân sağlanmış olur.

2.3. Bilgisayar Ağ Saldırısı

Bilgisayar ağ saldırısı, yerel ağdaki bir veya daha fazla istemci bilgisayar, sunucu veya ağ cihazlarını kullanım dışı bırakmak maksadıyla yapılmaktadır. Bu saldırılarda ağ yöneticisinin veya kullanıcının izni olmadan cihazlara erişim sağlamak, cihazlarda kullanılan uygulamaları bozmak ya da kullanım dışı bırakmak amacıyla bilinçli olarak yapılır.

Kötü niyetli kişiler veya siber suçlular tarafından gerçekleştirilen bu saldırılar, yerel ağ güvenliğinin açıklarını kullanan virüsler, zararlı ve casus yazılımlar ile yapılır. Özellikle, bu tür saldırılar ile ağ cihazları devre dışı bırakılarak kurumsal işletmeler veri hırsızlığı gibi maddi ve manevi büyük zararlara uğratılabilir.

2.3.1. Saldırganların Amaçları

Uluslararası Cisco Ağ Akademisi tarafından bilgisayar ağ saldırılarının hangi amaçla yapıldığı aşağıda sunulmuştur (Cisco Ağ Akademisi):

- Bilgi hırsızlığı: Genellikle kötü amaçlı bir yazılım, oltalama (Phishing) ve kaba kuvvet (brute force) gibi yöntemlerle bir yerel ağa veya bir istemci kullanıcıya erişim sağlayarak verilerini ele geçirmek olarak tanımlanmaktadır (Gupta et al., 2016; Tams et al., 2015)
- Veri kaybı: Genellikle kullanıcıların izni olmadan bir virüs aracılığı ile yerel ağda bulunan bilgisayar sabit diskindeki verileri değiştirmek veya yok etmek olarak açıklanmaktadır. Bu önemli verilerin kayıplarının yanı sıra finansal kayıplara, kurumların itibar eksikliklerine ve hukuki sorunlara sebep olabilmektedir.

- Kimlik hırsızlığı: Genellikle kişisel bilgilerin ele geçirilmesi olarak tanımlanmaktadır. Bu bilgiler şahısların kendisine ait kimlik bilgileri, kredi kartı bilgileri ve çevrimiçi işlemlerde kullanılan parola işlemleri ile ilgili değerli verilerin ele geçirilmesi olarak bilinmektedir. Saldırgan bu bilgilerle saldırıya uğrayan kişi veya kurumları birçok süreçte (bankacılık işlemleri ve yasal işlemler vb.) maddi ve manevi zararlara uğratabilmektedir.
- Hizmet kesintisi: Genellikle yerel ağda bulunan istemci bilgisayarın ağ sisteminden, sunuculardan veya ilgili web sayfalarından hizmet almalarını devre dışı bırakarak sistemin çalışmasını engellemek olarak tanımlanmaktadır. Son zamanlarda devletler tarafından sunulan çevrim içi hizmetler ve bankacılık işlemleri kurumsal şirketler için ciddi tehditler içermektedir. Bunlar DoS veya DDoS saldırılarıdır (Sharafaldin et al., 2018; Akgun et al., 2022).

2.3.2. Kötü Amaçlı Yazılımları Belirtileri

Bilgisayar virüsü, solucan, truva atı, fidye virüsü, casus yazılım olarak bilinen kötü amaçlı yazılımların belirtileri aşağıdaki gibidir (Taner, 2019):

- Bilgisayarın işlemci kullanımında hızlı bir yükselme ve performansında bir yavaşlama olması,
- Bilgisayar sürücüsündeki verilerin değiştirilmiş veya yok edilmiş olması,
- Bilgisayarın web tarayıcısındaki başlangıç sayfası ve tarayıcı ayarlarının değiştirilmiş olması ya da bilinmeyen araç çubuklarının eklenmesi,
- Antivirüs programlarına erişilememesi ya da devre dışı bırakılması,

2.4. Bilgisayar Ağ Ortamında Gerçekleşen Saldırı Türleri

2.4.1. Hizmet Reddi Saldırısı

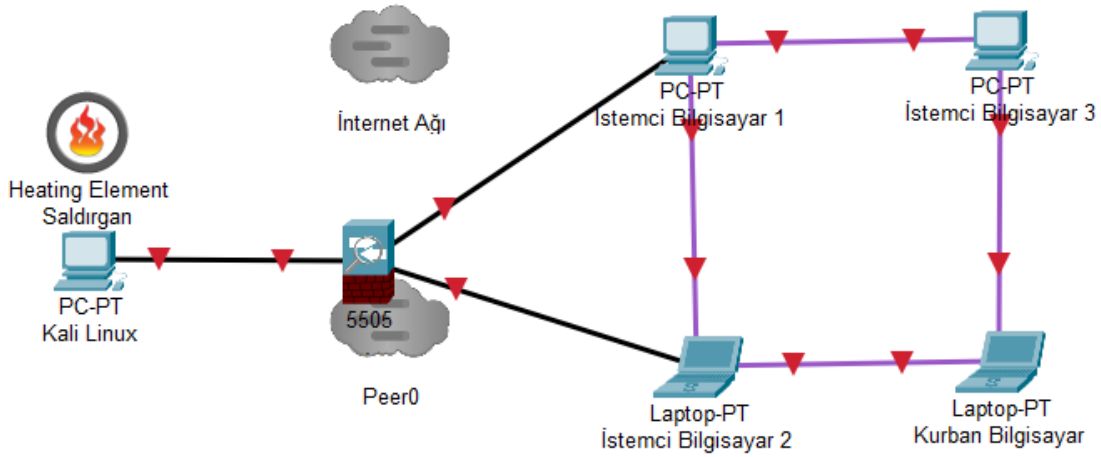
DoS saldırısı, bir saldırganın masum bir son kullanıcının bilgisayarını ve yerel ağ kaynağını kullanamamasına sebep olması olarak tanımlanmaktadır (Sharafaldin et al., 2018). DoS saldırıları uygulamada iki ana başlık altında incelenmektedir:

- Yoğun trafik miktarı: Saldırgan tarafından bir ağa, sunucu bilgisayarlarına veya uygulamalara cevap veremeyeceği kadar hızda çok büyük miktarlarda veri gönderilmesidir. Bu durum iletimin ve yanıt sürelerinin yavaşlamasına veya bir cihazın ya da hizmetin kilitlenmesine neden olmaktadır.

- Kötü amaçlı biçimlendirilmiş paketler: Saldırgan tarafından bir ağa, sunucu bilgisayarlarına veya uygulamalara bir veri paketi gönderilir, ancak alıcı bu veriyi işleyememesi nedeniyle istemci bilgisayarının yavaş çalışması veya kullanım dışı kalması gibi sonuçlar doğmaktadır.

DoS saldırıları bilgisayar ağlarındaki veri iletişiminde aksamaya sebep olduklarında bireyler ve kurumsal şirketler için zaman ve para kaybına neden olacakları için büyük bir risk faktörü olarak görülmektedir (Sharafaldin et al., 2018). Genellikle bu saldırıların profesyonel olmayan yeni başlamış saldırganlar tarafından yapılması oldukça kolaydır.

DoS saldırıları genelde açık sistem ara bağlantısı (Open System Interconnection-OSI) katmanlarından gerçekleşmektedir (Ajayi et al., 2022). Bunlardan özellikle uygulama katmanında yapılan DoS saldırıları genellikle kendilerini ağ düzeyinde göstermediğinden geleneksel ağ katmanı tabanlı saldırı tespit sistemlerinden kaçınabilmektedir. Bu nedenle siber güvenlik araştırma topluluğu, özel olarak uygulama katmanı DoS saldırılarını algılama ve azaltma mekanizmalarına odaklanmaktadır. Ancak, bu saldırılara karşı güvenilir ve verimli savunma mekanizmalarının oluşturulması için, siber güvenlik araştırmacıları tarafından uygulama katmanında yapılan DoS saldırılarının kapsamlı bir şekilde anlaşılması gerekmektedir. Şekil 2.1'de örnek bir DoS saldırısı gösterilmiştir.



Şekil 2.1:Örnek bir DoS saldırı senaryosu.

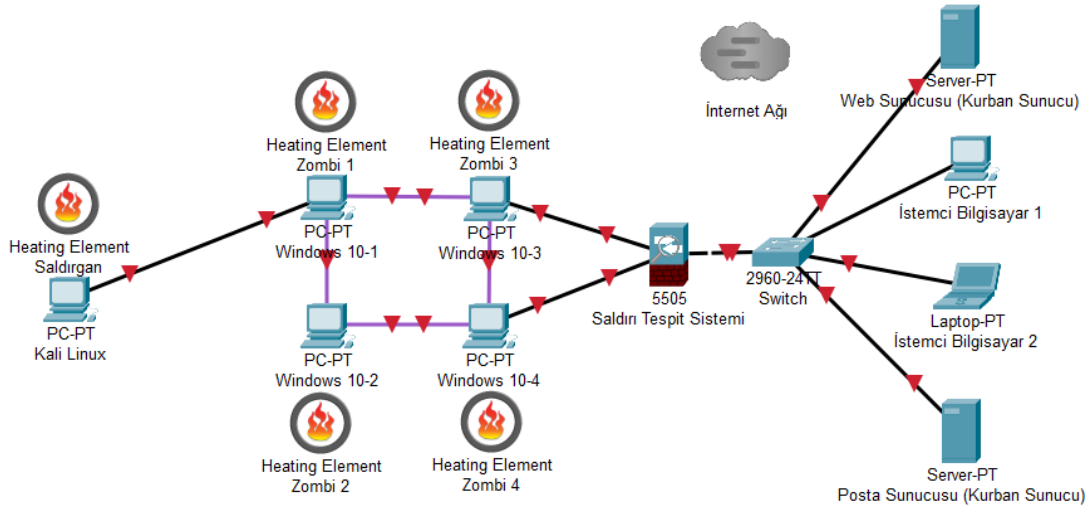
Şekilde görüldüğü üzere gibi Kali Linux bilgisayarına sahip bir saldırgan internet ağı üzerinden IDS'yi geçerek yerel ağda bulunan dört masum kullanıcı bilgisayarından bir

tanesine saldırmaktadır. Bu sayede kurban bilgisayar kullanıcısının iş yapamaz ve çalışamaz duruma gelmesi ve devre dışı kalması sağlanmıştır.

2.4.2. Dağıtık Hizmet Reddi Saldırısı

DDoS genellikle büyük ölçekte gerçekleştirilen ve anlık istekler göndererek servis sağlayıcısının kaldırabileceği yükün çok üzerinde kaynakları tüketerek sunduğu servislerin tamamen durmasına neden olan bir saldırı olarak tanımlanmaktadır (Akgun et al., 2022).

DDoS saldırısı saldırganlar tarafından bireysel kullanıcılar, kurumsal şirketler ve devlet kurumlarına ait web sunucusu kaynaklarına karşı yapılarak son kullanıcı istemcilerinin erişimini azaltmak veya engellemek amacıyla zombi adı verilen birden çok istemci bilgisayar ile yapılmaktadır. Bu süreçte virüs bulaşmış istemci bilgisayarlar zombi olarak adlandırılır. Zombi bilgisayarlar, her zaman yerel ağda virüs bulaştıracak istemci bilgisayarlar arayarak ve bu bilgisayarlara virüs bulaştırarak daha fazla zombi bilgisayarlar yaratmakta ve ağını genişletmektedir. Bu nedenle yüzlerce hatta bazen binlerce bilgisayar tarafından gerçekleştirilen DDoS saldırılarını zamanında tespit edip engellemek oldukça zor bir süreçtir (Taner, 2019). Şekil 2.2'de örnek bir DDoS saldırısı gösterilmektedir.



Şekil 2.2: Örnek bir DDoS saldırı senaryosu.

Şekilde görüldüğü üzere Kali Linux bilgisayarına sahip bir saldırgan internet ağı üzerinden sızma aracılığıyla ele geçirdiği bilgisayarlar ile kendisine yeni bir zombi ağı oluşturmuştur. Daha sonra bu zombi bilgisayarlar farklı zamanlarda IDS'yi geçerek yerel ağda bulunan web sunucusu veya mail sunucusuna taşıyamayacağı kadar veriyi

gönderip sunucunun devre dışı kalmasını sağlayarak ağda bulunan istemci bilgisayar kullanıcılarının sunuculardan hizmet alamamasına ve web/mail sistemlerinin devre dışı kalmasına neden olmuştur.

Web sunucuları birçok nedenden dolayı çevrimdışı olabilmektedir (Singh et al., 2018). Bunun en önemli nedenlerinden biri de web sunucusuna yapılan DDoS saldırılarıdır. Bu saldırılar yalnızca sunucu kaynaklarını tüketmekle kalmaz, aynı zamanda normal istemcilere de zarar verebilir. Bu nedenle, DDoS saldırılarının tespiti mevcut araştırmacıların birincil hedeflerinden biri haline gelmektedir.

Web sunucularında yapılan DDoS saldırıları genel olarak OSI katmanlarındaki ağ katmanı ve taşıma katmanına yapılan saldırılar olmak üzere ikiye ayrılmaktadır. Ağ katmanındaki DDoS saldırısı internet kontrol mesajı protokolü (Internet Control Message Protocol-ICMP) veya kullanıcı datagram protokolü (User Datagram Protocol-UDP) portlarından yapılırken taşıma katmanındaki ise taşıma kontrol protokolü (Transmission Control Protocol-TCP) portlarındaki sistem açıklıklarından sızarak gerçekleştirilmektedir.

Son yıllarda internete bağlanan cihazların sayısı giderek artmaktadır. Ancak bu artışı sadece bilgisayar kullanımının yaygınlaşması ile ifade etmek yanıltıcı olabilir. Çünkü günümüzde bilgisayarların yanı sıra nesnelerin interneti (Internet of Things-IoT) olarak tanımlanan cihazların kullanımındaki artış yadsınamayacak kadar büyüktür. Bu yaygınlaşma, DDoS saldırılarının da kendi içinde yüksek ve düşük oranlı DDoS saldırıları olarak ayrılmasına neden olmuştur. Yüksek oranlı DDoS saldırıları genellikle sunucu sistemlerine yapılırken düşük oranlı DDoS saldırıları ise diğer internete bağlı nesnelere yönelik gerçekleştirilmektedir (Toklu & Şimşek, 2018).

DDoS saldırıları, en yaygın siber tehdit biçimi haline gelmekte olup her geçen yıl hem sayı hem de hacim olarak artmaktadır. Temel motivasyon kaynağının finansal kazançlar olduğu ifade edilen DDoS saldırılarının özellikle kurumsal web siteleri veya bankaların internet servis sağlayıcıları üzerinde odaklandığı söylenebilir (Kumari & Jain, 2023).

2.4.3. Botnet Saldırısı

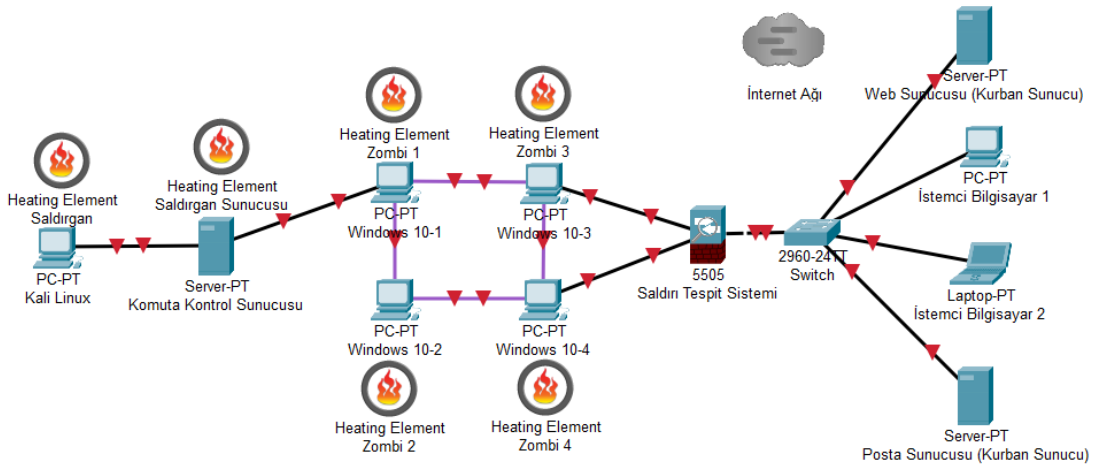
Botnet saldırısı bir birey veya bir grup saldırgan tarafından kontrol edilen ve internet üzerinden birbirine bağlanmış bilgisayarlar vasıtası ile yapılmaktadır. Botnet saldırısına maruz kalan bilgisayarlar, virüslü bir medya dosyasını veya bir spam e-

posta ekini açarak ya da zararlı bir web sitesini ziyaret ederek enfekte olurlar. Bir başka deyişle, botnet, bir komuta ve kontrol bilgisayarı ile botnet ağındaki diğer bilgisayarların yönetilmesi olarak tanımlanmaktadır (Rumsey, 2016). Saldırgan öncelikli olarak masum kullanıcıya ait bilgisayarın kullanıcı adı ve şifresini ele geçirerek kendi ağındaki komuta ve kontrol sistemindeki botnet ağına dâhil eder. Saldırgan kendi ağındaki bilgisayarları komuta ve kontrol bilgisayarı aracılığı ile aynı anda bir DDOS veya kaba kuvvet saldırısı yapmak için kullanabilir. Hatta siber suçlular botnet bilgisayarlarını siber saldırılar gerçekleştirilmesi için üçüncü şahıslara kiralayabilirler.

Bot bilgisayarlar kullanıcıların bilgisi olmadan ve kullanıcı farkına varmadan çalışmaları nedeniyle genellikle tespit edilemezler. Botnet saldırılarına karşı anti virüs programları kullanılarak ve web tarayıcılarının açıklıklarını kapatarak önlem alınabilir. Genellikle botnet saldırıları aşağıdaki özellikleri sergilerler (Taner, 2019):

- Zararlı yazılım barındıran bilgisayarlar internet ağı aracılığı ile bir komuta ve kontrol bilgisayarına bağlıdır,
- Web/posta sunucusu çökmeden önce sistem yöneticisine IDS ile uyarı logları gönderilir,
- Web/posta sunucusu üzerinde veya kurban bilgisayarda bilinmeyen dosyalar, programlar veya masaüstü simgeleri vardır,
- Web/posta sunucusu üzerinde veya kurban bilgisayarda bulunan uygulamalar kendilerini kapatıyor ya da yeniden kendilerini konfigüre ediyorlardır,
- Kullanıcının izni olmadan spam e-postalar gönderiliyordur.

Şekil 2.3’te örnek bir botnet saldırısı gösterilmiştir.



Şekil 2.3: Örnek bir Botnet saldırı senaryosu.

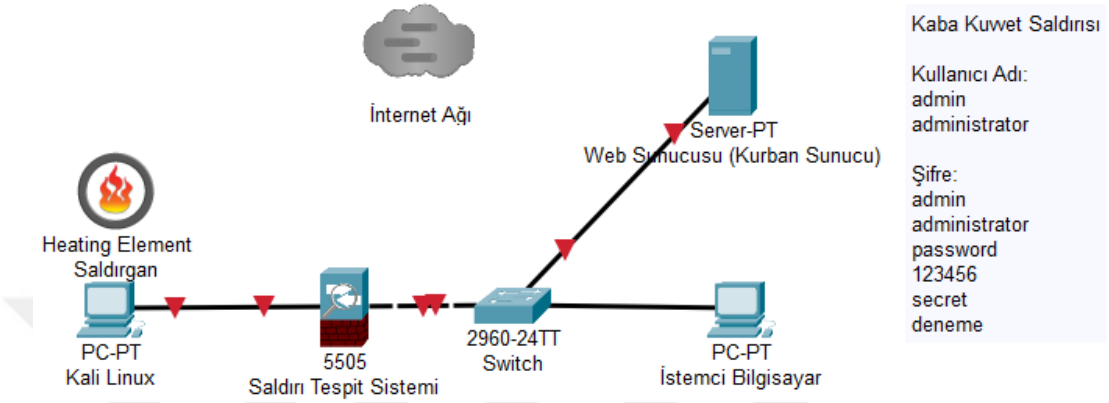
Şekilde gösterildiği gibi Kali Linux bilgisayarına sahip bir saldırgan internet ağında sızma ile ele geçirdiği bilgisayarlar üzerinden kendisine yeni bir botnet ağı kurmuştur. Saldırgan, komuta kontrol sunucusu üzerinden botnet ağında bulanan aktif zombi bilgisayarlarına web/posta sunucusuna atak yapılmak üzere aynı anda saldırı emri verir. Bu süreçte IDS'yi aşarak ağda bulunan sunucuların kaynaklarını tüketerek istemcilerin hizmet alamamasına sebep olur.

2.4.4. Kaba Kuvvet Saldırısı

İnternet ağı üzerinden web tarayıcıları aracılığı ile kurumsal şirketlerin ve devlet kurumlarının hizmet verdiği web sayfalarının yönetim paneli giriş bilgilerinin, siber saldırganlar tarafından deneme ve yanılma yöntemi ile çok sayıda kombinasyon denenerek ele geçirilmesidir. Web sayfası yöneticileri tarafından oluşturulan yönetim paneli kullanıcı adı ve parola bilgileri harf, rakam ve özel karakterlerden oluşmaktadır. Bu bilgiler ne kadar karmaşık ve zor olursa kaba kuvvet ataklarına karşı daha dayanıklı olurlar. Bu saldırganlar başarılı olduklarında şirket hakkında hassas bilgilere erişirler. Ayrıca web sayfası aracılığı ile reklam spam'lerine ve şirket saygınlığının zarar görmesine neden olurlar.

Kaba kuvvet saldırısı, siber saldırganlar tarafından en fazla kullanılan ataklardan biridir. Genelde bu atak türü oturum açmak için gerekli olan kullanıcı adı ve şifreyi deşifre etmek için kullanılmaktadır. Ek olarak web sayfası uygulamaları aracılığı ile gizli sayfalarda kullanılan bilgileri keşfetmek için de kullanılmaktadır (Sharafaldin et al., 2018).

Eylül 2017 yılında McAfee Labs tarafından yayımlanan üç aylık raporda, kaba kaba kuvvet saldırısının kuvvet saldırılarının toplam ağ saldırılarının içerisinde yaklaşık olarak %20'sini oluşturduğu ve bu saldırıların web sayfası tabanlı güvenlik açıklarıyla yapıldığı belirtilmiştir (Salamatian et al., 2019). Şekil 2.4'te örnek bir kaba kuvvet saldırısı gösterilmiştir.

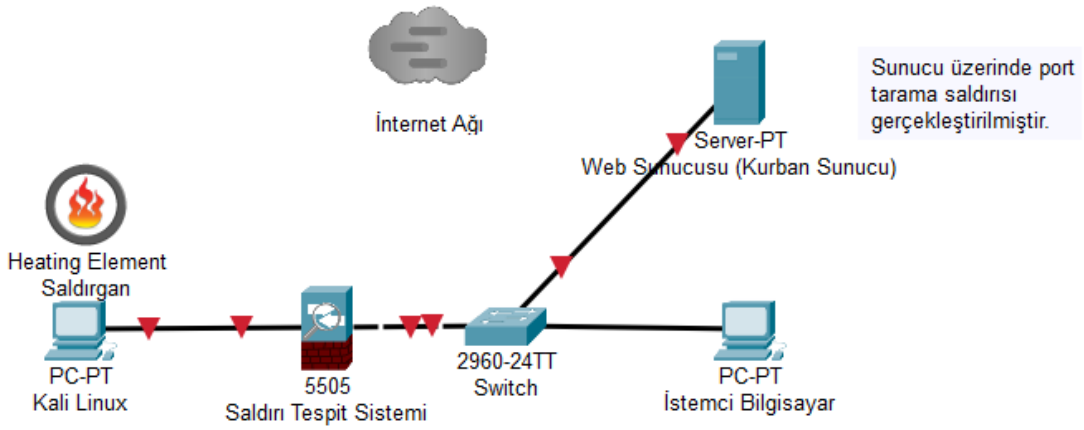


Şekil 2.4: Örnek bir kaba kuvvet saldırı senaryosu.

Şekilde gösterildiği üzere Kali Linux bilgisayarına sahip bir saldırgan, internet ağı üzerinden IDS'yi geçerek yerel ağda bulunan web sunucuna ait web sayfası yönetim paneli kullanıcı adı ve şifresi için algoritmik kombinasyonlar deneyerek bilgileri ele geçirmiştir. Bu bilgiler ele geçirildikten sonra sunucu üzerinde yönetici yetkisine sahip olan saldırgan sunucuda bulunan verileri farklı bir sisteme aktarabilir ve sunucuyu kötü niyetleri için kullanabilir.

2.4.5. Port Tarama Saldırısı

Port tarama saldırısı gerçekleştirmek isteyen saldırgan, internet ağı üzerinden istemci bir bilgisayarın web sayfası aracılığı ile açık olan bir portu kullanarak ağa girer. Ardından ağ içerisinde istemci bilgisayarlar veya hizmet veren sunucuların içerisinde port taraması yaparak açık olan portları tespit eder. Genellikle bilgisayar sistemlerinde bilgisayar portları açık, kapalı ya da filtrelenmiş olarak gruplandırılırlar. Port tarama saldırısı yaygın olarak web tarayıcılarında taşıma katmanı güvenliğinde kullanılan güvenli şifreleme yöntemi olan OpenSSL şifreleme uygulaması açıklıklarından gerçekleştirilmektedir (Jacob et al., 2022). Şekil 2.5'te örnek bir port tarama saldırısı gösterilmiştir.



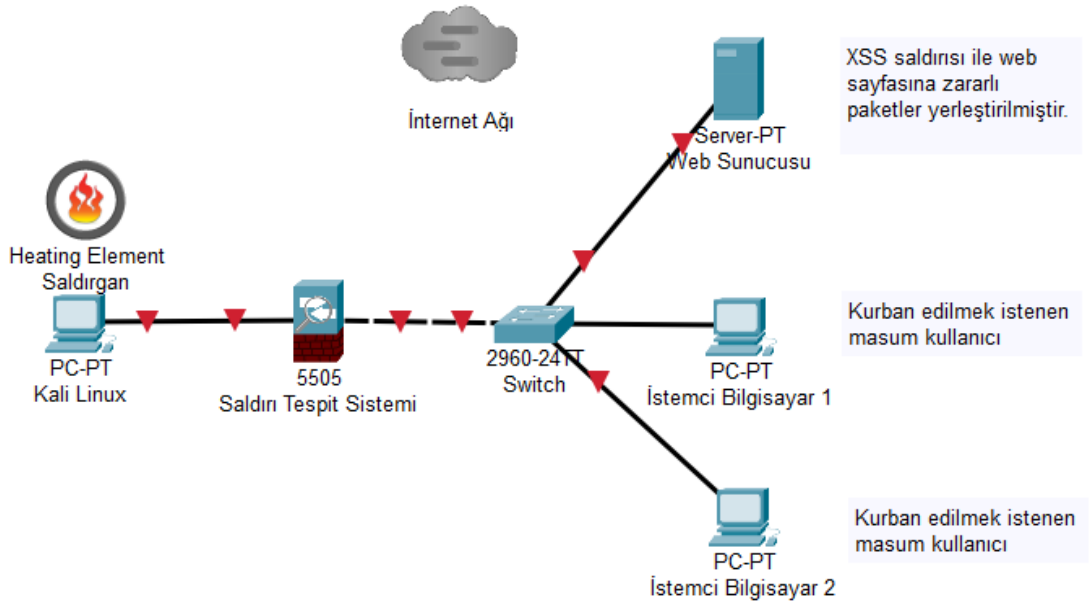
Şekil 2.5: Örnek bir port tarama saldırı senaryosu.

Şekilde gösterildiği gibi Kali Linux bilgisayarına sahip bir saldırgan internet ağı üzerinden IDS'yi geçerek yerel ağda bulunan istemci bilgisayar veya web sunucusuna ait açık portları bulmaktadır. İstemci bilgisayar veya web sunucusu içerisine girip kendisine yönetici yetkileri vererek istemci bilgisayar veya web sunucusunda bulunan verileri farklı bir sisteme aktarabilir ve bu sistemleri kötü amaçları için kullanabilir.

2.4.6. Web Uygulama Saldırısı

OWASP (Open Web Application Security Project) web uygulamalarındaki güvenlik açıklarının tespit edilerek kapatılması ve web uygulamaların güvenli bir şekilde korunmasını sağlamak için çalışmalar yapan bağımsız bir kuruluştur. OWASP 2018 yılında yayınladığı OWASP Top 10 raporunda yer alan bilgilere göre SQL enjeksiyon (SQL Injection) ve komut dosyası çalıştırma (Cross Site Scripting-XSS) saldırısı, en riskli güvenlik açıklıklarıdır (https://owasp.org).

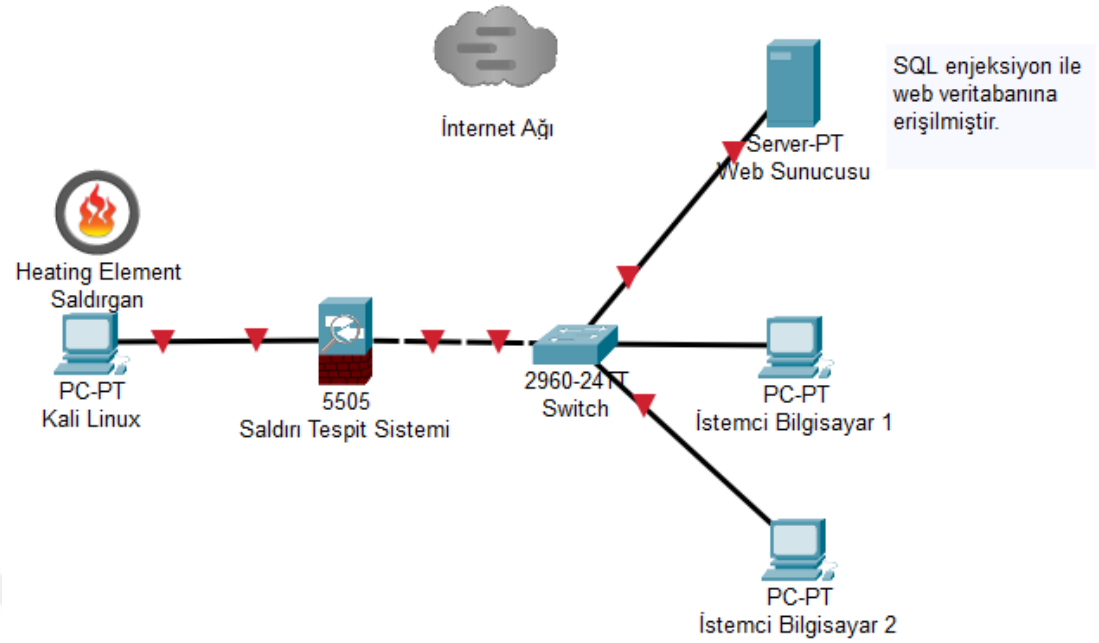
XSS saldırısında, saldırgan yoğun olarak kullanılan bir web sayfasına kötü amaçlı kod ilave eder ve kurbanın web tarayıcısında farkında olmadan kötü amaçlı komut dosyaları çalıştırmasına neden olur (Tariq et al., 2021). Saldırı, kurbanın kötü amaçlı kodu yürüten web sayfasını ziyaret etmesi ile gerçekleşir. Böylece web sayfası kötü amaçlı komut dosyasını kullanıcının tarayıcısına iletmek için bir araç haline gelmiş olur. Forumlar, mesaj panoları ve yorumlara izin veren web sayfaları XSS saldırıları için kullanılan savunmasız araçlara örnek olarak verilebilir. Şekil 2.6'da örnek bir XSS saldırısı gösterilmektedir.



Şekil 2.6: Örnek bir XSS saldırı senaryosu.

Şekilde görüldüğü üzere Kali Linux bilgisayarına sahip bir saldırgan internet ağı üzerinden IDS'yi geçmektedir. Ağda bulunan web sunucusu üzerinde hizmet veren web sayfasında saldırgan tarafından yerleştirilmiş zararlı kodlar bulunmaktadır. Masum olan bilgisayar kullanıcısı web sayfasından hizmet almak istediğinde sayfa içerisine gizlenmiş zararlı kodu çalıştırır ve zararlı kodlarda bulunan virüsü kendi bilgisayarına enjekte etmiş olur. Böylece kullanıcı, bilgisayarında bulunan verileri kendi rızası ve bilgisi olmadan dışarıya aktarmış olmaktadır.

SQL enjeksiyon, web uygulamalarında bulunan veri tabanlarını hedefleyen bir saldırı türüdür (Kasim, 2021). Bu saldırı türü SQL komutlarını kullanılarak gerçekleştirilmektedir. SQL sorguları ile web uygulamalarının arkasındaki veri tabanı sunucuları kontrol edilmektedir. Genellikle saldırganlar, web sunucusu veri tabanında yer alan verileri değiştirebilir veya silebilir, bu da uygulamanın içeriğinde veya davranışında kalıcı değişikliklere sebep olur. Sonuç olarak devlet kurumları ve kurumsal işletmeler itibar kaybına ve finansal kayıplara uğrayabilir (Crespo-Martínez et al., 2023). Şekil 2.7'de örnek bir SQL enjeksiyon saldırısı gösterilmiştir.



Şekil 2.7: Örnek bir SQL enjeksiyon saldırı senaryosu.

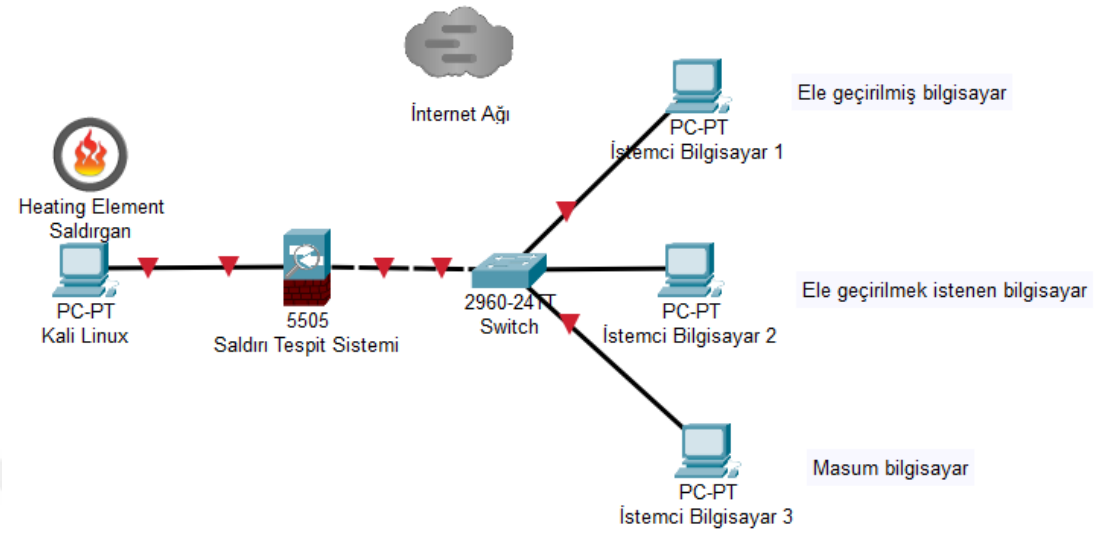
Şekilde gösterildiği gibi Kali Linux bilgisayarına sahip bir saldırgan internet ağı üzerinden IDS'yi geçerek yerel ağda bulunan web sunucusu üzerinde bulunan web veri tabanına sızmaktadır. Saldırgan kendisine yönetici yetkilerini vererek veri tabanında bulunan verileri değiştirebilir ve silebilir. Bunun sonucunda hizmet alan istemci bilgisayarlar veri tabanından hizmet almak istediğinde değişmiş veya silinmiş bilgilerle karşılaşarak hizmet eksikliğine yol açılmış olur.

XSS, web uygulamalarını kullanan kullanıcıları hedefleyen güvenlik açığı iken SQL enjeksiyon, web uygulamaları tarafından kullanılan veri tabanlarındaki güvenlik açıklıklarını hedeflemektedir.

2.4.7. Sızma Saldırısı

Sızma saldırısı (infiltration), ağa sızma olarak bilinen ve savunmasız bir yazılımdan yararlanılarak gerçekleştirilen bir saldırı türüdür. Örneğin saldırganlar tarafından adobe acrobat reader veya dropbox gibi yaygın olarak kullanılan programların kullandığı portlar üzerinden sızma gerçekleştirilir. Saldırganlar sızma gerçekleştikten sonra bilgisayarın tespit edilen portlarından kolaylıkla önce bilgisayara daha sonra yerel ağa giriş ve çıkış yapabilir. Bu portlar aracılığı ile bilgisayar üzerinden farklı saldırılar gerçekleştirebilir. Ayrıca saldırganlar, NMap kullanarak yerel ağ üzerinde IP taraması yapabilir, ağ içerisindeki diğer açıklıkları tespit edebilir ve ağ

cihazlarına/sunuculara ataklar gerçekleştirebilir. Şekil 2.8'de örnek bir sızma saldırısı sunulmaktadır.



Şekil 2.8: Örnek bir sızma saldırı senaryosu.

Şekilde gösterildiği gibi Kali Linux bilgisayarına sahip bir saldırgan, internet ağı üzerinden IDS'yi geçerek yerel ağda bulunan istemci bilgisayarlardan bir tanesine üçüncü paket programların kullandığı port ile sızmış olup, daha sonra ağda bulunan diğer masum bilgisayarları ele geçirmek istemektedir.

2.5. Güvenlik Araçları ve Yöntemleri

IDS, Kullanıcı Tabanlı Saldırı Tespit Sistemi (Host Intrusion Detection System-HIDS) ve Ağ Tabanlı Saldırı Tespit Sistemi (Network Intrusion Detection System-NIDS) olmak üzere iki türlüdür. Yani istenen sonucun tipine göre sisteme farklı şekilde yerleştirilebilir. HIDS ve NIDS için farklı sonuçlar mevcuttur ve buradan şu sonuca varılabilir: sadece bir IDS aracının konumunu değiştirerek çeşitli verimli sonuçlar elde edilebilir (Singh & Singh, 2014). Bu bölümde, izinsiz giriş tespit sistemlerinin algılama açısından sınıflandırılması sunulmuştur. Bunlar, yaklaşım ve veri kaynaklarına göre alt kategorilere ayrılırlar.

2.5.1. Saldırı Tespit Yaklaşımları

Tespit yaklaşımı açısından IDS, temel olarak kategorize edilebilir. Bunlar, imza tabanlı ve anormallik tabanlı izinsiz giriş olarak ikiye ayrılmaktadır. Bununla birlikte

hibrit bir yaklaşım da ortaya çıkmıştır. Bu yaklaşım, imza tabanlı ve anormallik tabanlı yaklaşımların birleşimidir.

Saldırı tespit yaklaşımlarından olan imza tabanlı teknikler, trafiği iyi huylu veya kötü niyetli olarak sınıflandırmak için mevcut tehdit bilgisine dayanırken; anomali tabanlı sistemler, saldırıları tespit etmek için trafik modellerine güvenir (Ahmad & Alsmadi, 2021).

Saldırı tespit yaklaşımları, iki grup açısından karakterize edilebilir (Singh & Singh, 2014):

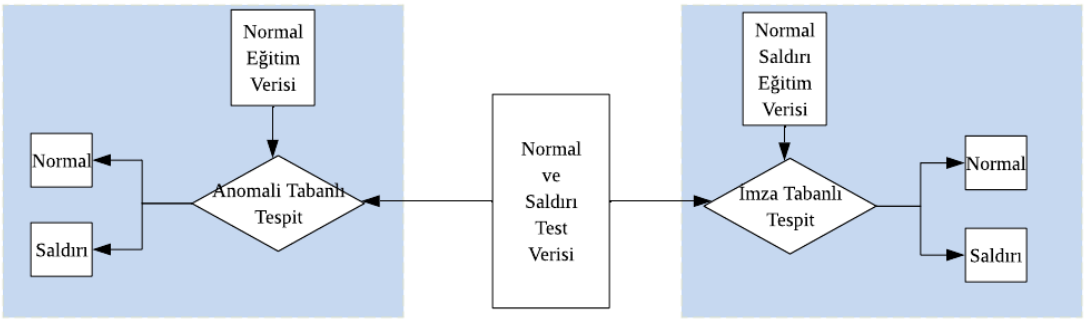
A. İmza (Kural) tabanlı izinsiz giriş saldırı tespit sistemi

B. Anomali tabanlı izinsiz giriş saldırı tespit sistemi

2.5.1.1. İmza Tabanlı Saldırı Tespit Sistemi

Kural Tabanlı IDS, yerel ağdaki paketleri arar ve veri tabanında tanımlanan önceden tanımlanmış kurallar veya imzalarla bunları karşılaştırır. Uyarılar, karşılaştırmanın sonucuna göre oluşturulur. Kurallar, uygulama yazılımının web sitesinden indirilebilir ve dinamik olarak güncellenebilir (Singh & Singh, 2014).

Bazen imza tabanlı algılama olarak da adlandırılan kural tabanlı algılama yaklaşımları, saldırı tespitleri için bilinen saldırıların veri tabanına tanımlanmış kurallara dayanır. Aşağıda görüldüğü gibi test verileri, kural tabanlı karar motorundan akar ve veri tabanından olası bir eşleşmenin tespiti yapılmış olup Şekil 2.9 gösterilmiştir. Hâlihazırda yakalanan saldırılara karşı iyi performans gösterme eğilimindedirler. Tespit edildiğinde ya çok az yanlış alarm vardır ya da yoktur. İyi performans göstermeye devam etmelerini sağlamak için imza veri tabanına yeni kuralların manuel olarak eklenmesi gerekmektedir. Veri tabanında tanımlanması yapılmamış kurallara karşı yapılan saldırılara karşı güçsüzdürler.



Şekil 2.9: Anomali ve imza tabanlı test veri setinin diyagram üzerinde gösterilmesi.

İmza tabanlı sistemler, mevcut ve iyi bilinen saldırılarda harika çalışır. Ancak imza tabanlı yaklaşımın sorunlarından biri, imza veri tabanını sürekli güncellemenin zaman alıcı olmasıdır. Veri tabanı boyutu büyüdükçe girdiyi büyük bir veri tabanıyla karşılaştırmak, hesaplama açısından pahalıdır. Bu yaklaşım, önceden bilinen saldırı imzalarına dayandığından sıfır gün veya bilinmeyen saldırıları tespit edemez (Singh & Singh, 2014).

İmza tabanlı saldırı tespit sistemleri (Signature Based Intrusion Detection Systems-SIDS), bilinen bir saldırıyı bulmak için model eşleştirme teknikleri ile bilgi tabanlı tespit veya kötüye kullanım tespiti olarak tanımlamıştır. SIDS'te eşleştirme yöntemi, önceden yapılmış benzer bir saldırıyı bulmak için kullanılır. Başka bir deyişle, saldırı ile izinsiz giriş imzası ile eşleştiğinde, zaten var olan önceki izinsiz girişin imzası veri tabanında olduğunda sistem yöneticisine bir alarm sinyali oluşturur. SIDS, sistem veri tabanında bulunan aşağıdaki dizileri bulmak için incelenir: önceden tanımlanmış komutlar veya eylemler, kötü amaçlı yazılım olarak veri tabanına tanımlanmıştır. SIDS, ayrıca literatürde bilgiye dayalı tespit veya kötüye kullanım olarak tespit olarak da geçmektedir (Khraisat et al., 2018; Khraisat et al., 2019; Modi et al., 2013).

2.5.1.2. Anomali Tabanlı Saldırı Tespit Sistemi

Anomali tabanlı saldırı tespit sistemi (Anomaly Intrusion Detection System-AIDS) geçmişte tanımlanmış olan kullanıcılardan veya kullanıcı gruplarından kalıpları belirleyerek çalışır. Bu tür bir teknik, yerel ağda bulunan farklı ve istenmeyen verilerin davranış değişikliklerini arar. Anomali detektörü tarafından sistemin davranışını denetimlerinden incelemek için kullanılan artan miktarda işlemi içerir (Singh & Singh, 2014).

Anomali tabanlı saldırı tespit modellerinin, zararsız bir yerel ağı vardır ve sistem, yerel ağda bulunan verilerin davranışlarını sınıflandırılarak ağda beklenmeyen farklı bir veri olduğunda anomali olarak bunlardan sapmalar olduğunu tespit eder. Şekil 2.14'teki anomali algılama motoru, yalnızca normal örnekler üzerinde eğitilmiştir. Anomali tabanlı saldırı tespit sisteminin en önemli avantajı, bu yaklaşımın sıfırıncı gün saldırılarını tespit etme yeteneklerine sahip olmasıdır. Ancak yanlış alarmlar üretmeye eğilimlidir. Çünkü bilinmeyen yerel ağda ve sistemde davranışları kolayca sınıflandırılabilir ve anormallikler olarak gösterebilir. Anomali tabanlı saldırı tespit uygulamaları üzerine ufuk açıcı çalışmaların çoğu yaklaşım aslında hibrit bir yaklaşım almıştır (Ahmad & Alsmadi, 2021).

Anomali tabanlı algılama, tercih edilen bir yaklaşımdır. Çünkü iyi huylu trafik modellerine bakar ve anormal bir trafik modeli algılandığında bir alarm üretir veya trafiği bloke eder. Anomali tabanlı sistemler kullanmanın faydalarından biri, sıfır gün ve bilinmeyen saldırıları tespit etmede iyi olmalarıdır. Bununla birlikte yüksek oranda hatalı pozitif sonuçlar üretebilmektedirler. AIDS'ler, büyük ölçekli, sıfırıncı gün ve bilinmeyen saldırılara yönelik güçlü tespit yeteneklerine odaklanan sistemlerden biridir (Singh & Singh, 2014).

AIDS, sahip olduğu özellikler nedeniyle pek çok bilim insanının ilgisini çekmiştir. AIDS'te bir bilgisayar sisteminin davranışının normal modeli çalışılarak makine öğrenimi kullanılarak oluşturulan, istatistiksel tabanlı veya bilgiye dayalı yöntemler kullanılarak yerel ağda herhangi bir önemli sapma gözlenen davranış ve model tespit edildiğinde izinsiz giriş olarak yorumlanıp bir anormallik olduğunu söylemiştir. Bu teknikte yerel ağda varsayım, tipik kullanıcı davranışından farklı davranışın kötü niyetli kabul edilmesidir (Butun et al., 2013; Khraisat et al., 2019).

2.5.1.3. Hibrit Tabanlı Saldırı Tespit Sistemi

Hibrit tabanlı saldırı tespit yaklaşımı, imza tabanlı saldırı tespiti ve anomali tabanlı saldırı tespit sisteminin gücünü birleştiren bir yaklaşımdır. Böylece anomali tabanlı saldırı tespit sisteminin tespit oranı seviyeleri iyileştirilerek yanlış pozitif oranları azaltılmış olur (Ahmad & Alsmadi, 2021).

2.5.2. İzinsiz Giriş Tespiti Veri Kaynakları

Saldırı tespit sistemlerini kategorize etmenin bir başka yolu ise hedef altyapıdan geçmektedir. Tespit etmeye çalışılan saldırıların sayısı önemlidir. Bu bakış açısında iki IDS kategorisi bulunmaktadır: Bunlar NIDS ve HIDS'dir. HIDS'e ek olarak, bir yerel ağ içinde farklı konumlarda dağıtılan NIDS ve güvenlik duvarları, saldırılara karşı sağlam bir koruma sağlayabilir (Ahmad & Alsmadi, 2021).

IDS, saldırıları tespit etmek için kullanılan girdi veri kaynaklarına göre sınıflandırılabilir. Anormal aktiviteler, veri kaynakları açısından genellikle iki tür IDS teknolojisi vardır: Bunlar NIDS ve HIDS olarak ikiye ayrılırlar (Khraisat et al., 2019).

2.5.2.1. Ağ Tabanlı Saldırı Tespit Sistemi

Yaygın olarak kullanılan çoğu IDS, ağ tabanlıdır. Bu IDS'ler, yerel ağda bulunan istenmeyen verileri yakalayıp analiz ederek saldırıları tespit ederler. Ağ tabanlı bir IDS, ağ anahtarlama cihazları katmanlarında bulunan aşamalara göre ağı dinleyip yerel ağda bulunan bilgisayarların veri akış trafiğini izleyebilir ve böylece yerel ağın korunmasını sağlamış olur.

Ağ tabanlı IDS'ler, genellikle bir dizi tek amaçlı sensörlerden oluşurlar veya bir ağda çeşitli noktalara yerleştirilmiş bilgisayarlardır. Bu bilgisayarlar, yerel ağ trafiğini izleyip analiz ederek saldırıları merkezi yönetim konsoluna bildirirler. Sensörler, çalışmakta sınırlı olduğundan IDS ile saldırılara karşı daha kolay bir şekilde emniyete alınabilir. Bu sensörler, gizli modda ağda çalışacak şekilde tasarlanmıştır. Bir saldırganın, yerel ağdaki sensörlerin varlıklarını ve konumlarını belirlemesi zordur.

Ağ Tabanlı IDS'lerinin Avantajları:

- Yerel ağda lokasyonları iyi yerleştirilmiş IDS'ler, büyük bir yerel ağ trafiğini rahat bir şekilde izleyebilir.
- Ağ tabanlı IDS'lerin yerel ağa dâhil edilmesi kolaydır. Yerel ağa dâhil edilirken ağ kesintisine veya aksamasına neden olmazlar. IDS'ler, yerel ağda ilave ağ trafik yükü oluşturmazlar.
- Ağ tabanlı IDS'ler, saldırılara karşı çok güvenli hale getirilebilir ve hatta IDS varlığı, çoğu zaman saldırganlar tarafından bilinemez.

Ağ Tabanlı IDS'lerinin Dezavantajları:

- Ağ tabanlı IDS'ler, yerel ağdaki tüm paketleri işlemekte zorluk yaşayabilirler. Büyük ve yoğun bir yerel ağda, hatta veri trafiğinin yoğun olduğu zamanlarda yapılan bir saldırıyı tespit edemeyebilirler.
- Ağ tabanlı IDS'ler, şifrelenmiş bilgileri analiz edemezler.
- Ağ tabanlı IDS'ler, yerel ağda bir saldırı olup olmadığını bilemezler; sadece bir saldırının başladığını anlayabilirler. Bunun anlamı, ağ tabanlı bir IDS bir saldırıyı tespit ettikten sonra sistem yöneticileri, saldırıya uğrayan her bilgisayarı manuel olarak kontrol etmelidir.
- Ağ tabanlı paketlerin parçalanmasını içeren saldırılar veya hatalı olarak biçimlendirilmiş paketler, IDS'lerin kararsız hale gelmesine ve hizmet dışı kalmasına neden olur.

NIDS, bir sistemi ağ tabanlı tehditlerden korumak için ağ trafiğini izlemek ve analiz etmek için kullanılır. NIDS, gelen tüm veri paketlerini okur ve şüpheli olanları tespit eder. Tehditler tespit edildiğinde ciddiyetine bağlı olarak sistem yöneticilerine bildirimde bulunmak veya kaynak IP adresinin ağa erişimini engellemek gibi önlemler alabilir (Singh & Singh, 2014).

NIDS, ağ trafiğindeki izinsiz girişleri belirlemek için yerel ağın farklı noktalarında bulunur. Yerel ağda paket yakalama, Netflow ve diğer ağ veri kaynaklarını izleyerek saldırı olup olmadığını tespit eder. Bir NIDS'nin avantajları, ağ içindeki harici kötü amaçlı olayların, bu tür tehditler başka bir sisteme yayılmadan önce tespit edilebilmesi ve önlem alınabilmesidir. Ancak NIDS, büyük hacimlerde veri içeren yüksek bant genişliğine sahip ağlarda saldırıları tespit etmekte zorlanabilir (Ahmad & Alsmadi, 2021).

NIDS, ayıklanan ağ trafiğini izleyerek NetFlow aracılığıyla bir ağdan ve diğer ağ veri kaynakları paket yakalamak olarak tanımlamıştır. Ağ tabanlı IDS, yerel bilgisayar ağına bağlı birçok bilgisayarı izlemek için kullanılır. NIDS, harici kötü amaçlı yazılımları izleyebilir ve harici bir tehditten başlatılabilecek faaliyetler daha erken bir aşamada, tehditler bilgisayar sistemine yayılmadan önce tespit edebilir. NIDS, yerel bilgisayar ağında belirli bir ağ topolojisi içinde farklı pozisyonlarda konuşlandırıldığında HIDS güvenlik duvarları hem dış hem de içeriden kaynaklanan dış etkenlere karşı somut, dayanıklı ve çok katmanlı bir koruma sağlayabilirler (Bhuyan et al., 2013; Khraisat et al., 2019).

2.5.2.2. İstemci Tabanlı Saldırı Tespit Sistemi

İstemci tabanlı IDS, öncelikli olarak yerel ağda bulunan sunucu ve bilgisayarlara kurulur. Bu IDS'de yerel ağda bulunan kurulu bilgisayar, kendi veri trafiğini izleyip kendine karşı yapılan saldırıları analiz ederek saldırıları tespit eder. İstemci tabanlı IDS, normalde iki tür bilgi kaynağını kullanır: işletim sistemi denetimi izleri ve sistem günlükleridir. İşletim sistemi denetimi izleri, işletim sisteminin çekirdek yapısında olduğu için anlaşılması daha zordur. Sistem günlükleri ise daha geniştir ama kullanıcılar tarafından anlaşılması daha kolaydır. İstemci tabanlı IDS, bazen tek bir sunucuya izin verilebilen merkezi bir IDS yönetimi ve raporlama altyapısını desteklemek üzere tasarlanmıştır. İstemci tabanlı IDS veri trafiğini izlemek için bir yönetim konsolu bulunmaktadır.

İstemci Tabanlı IDS'lerinin Avantajları:

- Yerel ağda bulunan Ağ tabanlı IDS tarafından tespit edilmeyen bir saldırı, İstemci tabanlı IDS tarafından tespit edebilirler.
- Yerel ağda bulunan istemciler, direkt olarak sunucudan hizmet aldıklarından sunucuya yapılan bir saldırı olduğunda İstemci tabanlı IDS, bunu tespit eder.
- Sunucular anahtarlanmış olan verileri çözdüklerinden dolayı kendisine karşı şifrelenmiş olan bir saldırıyı çözmesinden dolayı saldırıyı tespit ederler.

İstemci Tabanlı IDS'lerinin Dezavantajları:

- İşletilmesi daha zordur. Çünkü yerel ağda bulunan her sunucu veya istemci, bilgisayara kurularak her birinin yapılandırılması ve yönetilmesi gerekmektedir.
- IDS kurulu olan bilgisayar, saldırganlar tarafından tespit edilip devre dışı bırakılabilir.
- Sunucu veya istemci üzerinde kurulu olduğundan sadece kendi ağ paketlerini izleyebilirler; ağdaki veri trafiğini izleyemezler.
- Yerel ağda bulunan sunucu veya istemci, DDoS saldırısı ile devre dışı bırakılabilir.
- Yerel ağda bulunan sunucu veya istemcinin kendi fiziksel kaynaklarını kullanmasından dolayı ilave olarak maliyetin yükselmesine neden olurlar.

HIDS, IDS'nin ilk türüdür ve ilk işlevi, yerel ağda bulunan sunucu ve istemci bilgisayar içinde yerel ağı izlemektir. Ancak günümüzde yerel ağı izlemek için kullanılabilecek birçok HIDS çeşidi geliştirilmiştir. HIDS, bir sunucunun veya istemci

bilgisayarın güvenliğinin ihlal edilip edilmediğini belirler ve buna göre sistem yöneticilerini uyarır (Singh & Singh, 2014).

HIDS, sistemdeki etkinlik verilerini inceleyerek bireysel sunucu ve istemci bilgisayarları izler, kaynakları denetler ve şüpheli faaliyetler tespit edildiğinde kullanıcıyı uyarır. HIDS, kötü amaçlı saldırılar veya izinsiz girişler için tek bir sistem üzerinde uygulanmak üzere oluşturulmuştur. Saldırganlar, genellikle işletim sistemine zarar verebilir veya günlük kayıt defterinde değişiklik yaptığında veriler algılanabilir. HIDS türleri: Denetim verileri işletim sistemi düzeyinde HIDS ve denetim verileri uygulama yazılımı düzeyinde HIDS vardır. İşletim sistemi düzeyinde HIDS, sistem dosyaları, dosya sistemi değişiklikleri ve kullanıcı oturum açma işlemleriyle ilgilidir (Ahmad & Alsmadi, 2021).

HIDS, ana bilgisayar işletim sisteminden kaynaklanan verileri inceler. İşletim sistemi bu süreçte sunucu günlükleri, güvenlik duvarı günlükleri, veri tabanı günlükleri, uygulama yazılımı sistemi denetimlerini sürekli kontrol eder. Ayrıca HIDS, ağ içerisinden gelen saldırıları tespit edebilir (Creech & Hu, 2013; Khraisat et al., 2019).

2.5.2.2.1. Uygulama Tabanlı Saldırı Tespit Sistemi

Uygulama tabanlı IDS'ler, genelde İstemci tabanlı IDS'lerin bir alt kümesi olarak bilinir. Yerel ağda bulunan sunucu veya istemci, bilgisayar üzerinde çalışan yazılım uygulamasında meydana gelen olayları analiz eder. Bu süreçte yazılım uygulamasına ait dosyalarda veya işlem günlüğünde izinsiz olarak yapılan değişiklikler izlenir.

Uygulama Tabanlı IDS'lerinin Avantajları:

- Kullanıcıların yazılım uygulamasında yaptığı değişiklikler, diğer kullanıcılar tarafından görülebilir.

Uygulama Tabanlı IDS'lerin Dezavantajları:

- Uygulama tabanlı IDS, genellikle kullanıcı düzeyinde olaylar izlediğinden soyutlama yapamaz. Genellikle Truva atı veya diğer saldırıları tespit edemez. Bu sebepten dolayı öncelikli olarak Ağ tabanlı IDS'ler daha sonra istemci tabanlı IDS'lerin kullanılması tavsiye edilir.

2.5.2.3. Hibrit Tabanlı Saldırı Tespit Sistemi

Diğer bir tür, hibrit tabanlı saldırı tespitidir. Bu tür sistemlerde daha fazla esneklik ve güvenlik sağlamak için hem istemci tabanlı hem de ağ tabanlı saldırı tespiti birlikte kullanılır. Bu tür sistemler, genellikle trafik, IDS yerleşimi ve uyarı türü açısından gelişmiş özelliklere sahiptir ve bu özellikler ihtiyaca göre değiştirilebilir (Singh & Singh, 2014).

3. MALZEME VE YÖNTEM

3.1. Kullanılan Veri Seti

Siber saldırganlar tarafından yapılan yeni saldırıları tespit etmek, birçok araştırmacının odaklandığı ana nokta olmuştur. Ancak gerçek dünya uygulamalarına uyarlanması, sistemin karmaşıklığı nedeniyle engellenmiştir. Çünkü bu sistemler devreye alınmadan önce önemli miktarda test ve değerlendirmeden geçmesi gerekmektedir. Bu sistemleri izinli ve izinsiz girişler veya normal ve anormal davranışlar içeren gerçek etiketli ağ izleri üzerinde çalıştırmak, test etmek ve değerlendirmek, en iyi yöntemdir.

Araştırmacılar tarafından kullanılan veri setleri, son derece az sayıda olması veya gizlilik sorunları nedeniyle paylaşılamamaktadır. Diğer taraftan internet ağında bulunan veri setleri büyük ölçüde anonimleştirildiği için mevcut durumu yansıtmadığından gerçeklikten uzaklaşmaktadır. Bu nedenle araştırmacılar genellikle yetersiz olan veri setleri ile çalışmak zorunda kalmaktadırlar (Canadian Institute for Cybersecurity, 2018).

Buna çözüm üretme adına, Kanada İletişim Güvenliği Kuruluşu (Canada Communications Security Establishment-CSE) ve Kanada Siber Güvenlik Enstitüsü (Canadian Institute for Cybersecurity-CIC) arasındaki ortak bir proje ile CIC-IDS2017 saldırı tespit sistemi veri seti geliştirilmiştir (Canadian Institute for Cybersecurity, 2018).

2016 yılında McAfee raporunda yer alan ve siber saldırganlar tarafından yaygın olarak kullanılan hizmet reddi saldırısı (DoS), dağıtık hizmet reddi saldırısı (DDoS), botnet, kaba kuvvet, port tarama, web uygulama ve sızma saldırılarına, CIC-IDS2017 veri setinde yer verilmiştir (Canadian Institute for Cybersecurity, 2018).

CIC-IDS2017 veri seti, gerçek dünya verilerinden yakalanmış veri paketlerine (Packet Capture-PCAP) benzeyen zararsız ve en güncel yaygın saldırıları içerir. Ayrıca zaman bilgisi, kaynak ve hedef IP adresleri, kaynak ve hedef bağlantı noktaları, protokoller ve saldırı temelinde etiketlenmiş akışlarla birçok veriyi gerçek zamanda akan ağ trafiği

(CICFlowMeter) kullanılarak ağ trafiği analizinin sonuçlarını içermektedir (Canadian Institute for Cybersecurity, 2018).

Bu veri seti oluşturulurken araştırmacıların en büyük önceliği, gerçekçi zararsız arka plan veri trafiğini oluşturmak olmuştur. Bu yöntem, bir grup insan kullanıcının soyut davranışını ayıklamak üzere tasarlanmıştır. Makine öğrenimi ve istatistiksel analiz teknikleri ile kullanıcılar tarafından üretilen ağ olayları kapsanmaya çalışılmıştır. Bu özellikler, bir protokolün paket boyutlarının dağılımı, akış başına paketin sayısı, yükteki belirli modeller, yükün boyutu ve protokollerin istek zamanı dağılımıdır. Kuruluşlar ve araştırmacılar, bu yaklaşımı kolayca gerçekçi veri setleri oluşturmak için kullanabilir; bu nedenle veri kümelerini anonimleştirmeye gerek yoktur. Bu veri seti için HTTP, HTTPS, FTP, SSH ve e-posta protokollerine dayalı olarak 25 kullanıcının soyut davranışı gözlemlenmiştir (Canadian Institute for Cybersecurity, 2018).

Bu süreçte veri toplama süresi, 3 Temmuz 2017 Pazartesi sabah 09.00'da başlayıp 7 Temmuz 2017 Cuma günü saat 17.00'de bitmiş ve toplamda 5 gün sürmüştür. Uygulanan saldırılar günlere göre şöyledir:

- Pazartesi: Normal gün olup sadece iyi huylu veri trafiği içermektedir.
- Salı: Kaba kuvvet ataklarından olan FTP ve SSH saldırıları yapılmıştır.
- Çarşamba: Sadece DoS atakları yapılmıştır.
- Perşembe: Sabahtan web saldırılarından olan web kaba kuvvet, SSH ve Sql enjeksiyon yapılmış; öğleden sonra sızma saldırıları yapılmıştır.
- Cuma: Sabahtan botnet saldırıları yapılmış iken öğleden sonra DDoS ve portscan atakları yapılmıştır (Canadian Institute for Cybersecurity, 2018).

Araştırmacılar, bu veri setinde güvenilir bir kıyaslama veri seti oluşturmak için gerekli kriterler belirlemişlerdir. Bu kriterleri kısaca özetlemek gerekirse(Canadian Institute for Cybersecurity, 2018):

- Eksiksiz bir ağ yapılandırması: Eksiksiz bir ağ mimarisi, bu mimaride modem, güvenlik duvarı, yönlendiriciler, anahtarlama cihazları ve Windows, Ubuntu ve Macintosh gibi çeşitli işletim sistemlerinin varlığı olmuştur.
- Eksiksiz trafik: Saldırgan ve kurban ağda bulunan tüm veri akışı kullanılmıştır.

- Etiketli veri kümesi: Her gün için iyi huylu veya kötü huylu saldırı etiketleri ile gösterilmiştir. Ayrıca, saldırı zamanlamasının bilgi detayları da veri setinde yer almıştır.
- Eksiksiz etkileşim: İki farklı ağa ve internet iletişimine sahip olarak geniş bir ağda hazır bulunulmuştur.
- Eksiksiz yakalama: Yerel ağda dinleme sistemi gibi ikiz bağlantı noktası kullanıldığı için tüm trafikler yakalanmış ve depolama sunucusuna kaydedilmiştir.
- Kullanılabilir protokoller: HTTP, HTTPS, FTP, SSH ve e-posta protokolleri gibi tüm yaygın kullanılabilir protokollerin varlığı sağlanmıştır.
- Saldırı çeşitliliği: Bu veri seti, web tabanlı kaba kuvvet, DoS, DDoS, Sızma, botnet ve portscan gibi 2016 McAfee raporuna dayalı en yaygın saldırıları içermektedir.
- Heterojenlik: Ana anahtarlama cihazı, saldırıların yürütülmesi sırasında ağ trafiğindeki tüm kurban makinelerden gelen bellek dökümünü ve sistem çağrılarını yakalamıştır.
- Özellik seti: CICFlowMeter kullanılarak oluşturulan ağ trafiğinden 80'den fazla ağ akışı özelliği çıkarılmış ve ağ akışı veri kümesinin CSV uzantılı bir veri dosyası oluşturulmuştur.
- Veri bilgileri: Yayımlanan veri setinde veri ile ilgili elde edilen saldırıları, akışları ve etiketleri içeren veri seti, hiçbir değişiklik yapılmadan tamamen açıklanmıştır.

Bu veriseti ile ilgili günlerde elde edilen bilgilerin boyutları Tablo 3.1'de sunulmuştur.

Tablo 3.1:CIC-IDS2017 veri setinde elde edilen verilerin gün ve boyutları

Gün	Saldırı Durumu	Boyut
Pazartesi	Normal	11 GB
Salı	Saldırılar	11 GB
Çarşamba	Saldırılar	13 GB
Perşembe	Saldırılar	7,8 GB
Cuma	Saldırılar	8,3 GB

3.2. Makine Öğrenme Yöntemleri

3.2.1. Bayes Sınıflandırıcısı

Bayes sınıflandırıcıları nedir? Bayes sınıflandırıcıları, istatistiksel sınıflandırıcılardır. Belirli bir sınıfa ait demetin, ait olma olasılığı gibi sınıf üyeliği olasılıklarını tahmin edebilirler.

Bayes sınıflandırması, aşağıda açıklanan Bayes teoremine dayanmaktadır. Karşılaştıran çalışmalar sınıflandırma algoritmaları, Naive olarak bilinen basit bir Bayesci sınıflandırıcı bulmuştur. Bayes sınıflandırıcısı, performans açısından karar ağacı ve seçilen nöral ile karşılaştırılabilir. Ağ sınıflandırıcıları, Bayes sınıflandırıcıları büyük veritabanlarına uygulandığında yüksek doğruluk ve hız sergilemiştir (Han et al., 2012).

Naive Bayesci sınıflandırıcılar, bir öznitelik değerinin verilen bir sınıf üzerindeki etkisinin diğer niteliklerin değerlerinden bağımsızdır. Bu varsayıma bağımsızlık sınıf koşulu da denir. İlgili hesaplamaları basitleştirmek için kullanılır (Han et al., 2012). Bayes teoremi, adını konformist olmayan bir İngiliz din adamı olan Thomas Bayes'ten almıştır. Kendisi 18. yüzyılda olasılık ve karar teorisi üzerine çalışmalar yapmıştır.

Bu çalışmalarda veri grubundaki X, Bayes terimlerinde "kanıt" olarak kabul edilir. Her zamanki gibi n, öznitelik kümesi üzerinde yapılan ölçümler tarafından tarif edilir. H veri grubu X, belirtilen bir C sınıfına aittir. Böyle bir hipotez olsun. Sınıflandırma problemleri için P(H\X) "kanıt" verildiğinde H hipotezinin tutma olasılığı veya gözlemlenen veri kümesi X olarak kabul edilir. Diğer bir deyişle, X kümesinin olma olasılığı aranır. X'in öznitelik tanımı bilindiğine göre, C sınıfına aittir (Han et al., 2012).

P(H\X), H koşullunun sonsal olasılığı veya X'te bir posteriori olasılığıdır. Örneğin, veri grupları dünyamızın açıklanan müşterilerle sınırlı olduğunu varsayalım. Sırasıyla yaş ve gelir özelliklerine ve X'in 35 yaşında bir müşteri olduğuna göre 40.000 $ geliri olduğunu ve H'nin, müşterimizin bilgisayar satın alacağı hipotezi olduğunu varsayalım. Ardından P(H\X), X müşterisinin bir bilgisayar satın alma olasılığı, müşterinin yaşını ve gelirini bildiğimiz için alma olasılığını yansıtır (Han et al., 2012).

Buna karşılık, P(H), H'nin önceki olasılığı veya öncelik olasılığıdır. Örneğimiz için bu herhangi bir müşterinin gelir ve yaşına bakmaksızın, bu konuda başka herhangi bir

bilgi olmadan bir bilgisayar satın alma olasılığıdır. Son olasılık, P(H\X) önceki olasılıktan daha fazla bilgiye yani X'ten bağımsız olan P(H)'ye dayanmaktadır (Han et al., 2012).

Benzer şekilde, P(X\H), X'in H üzerinde şartlandırılmış son olasılığıdır. Bir müşterinin, X'in, 35 yaşında olması ve 40.000 $ kazanması olasılığı, müşterinin bir bilgisayar satın alma olasılığıdır (Han et al., 2012).

P(X), X'in önceki olasılığıdır. Örneğimizi kullanırsak, bir müşteri grubumuzdan bir kişi 35 yaşındaydı ve 40.000 $ kazanıyordu (Han et al., 2012).

"Bu olasılıklar nasıl tahmin ediliyor?" P(H), P(X\H) ve P(X) tahmin edilebilir. Daha sonra göreceğimiz gibi, verilen verilerden, Bayes teoremi sağladığı için yararlıdır. P(H), P(X\H) ve P(X)'ten sonsal olasılık P(H\X)'yi hesaplamanın bir yoludur. Aşağıda Bayes teoremi formülü gösterilmektedir (Han et al., 2012).

$$P(\mathrm{H}\backslash\mathrm{X}) = \frac{\mathrm{P}(\mathrm{X}\backslash\mathrm{H})\mathrm{P}(\mathrm{H})}{\mathrm{P}(\mathrm{X})} \tag{3.1}$$

3.2.2. Destek Vektör Makinesi

Bu bölümde, sınıflandırma için bir yöntem olan destek vektör makineleri (Support Vector Machine-SVM) incelenecektir. Özetle hem doğrusal hem de doğrusal olmayan verilerin incelendiği bir algoritmadır. Orijinal eğitim verilerini dönüştürmek için daha yüksek bir boyuta doğrusal olmayan bir haritalama kullanır. Bu yeni boyutta doğrusal optimali arayarak ayırıcı hiper düzlemdir (yani bir sınıfın demetlerini ayıran bir "karar sınırı"). Yeterince yüksek bir boyuta uygun bir doğrusal olmayan eşleme ile iki sınıftan gelen veriler her zaman bir hiper düzlemle ayrılabilir. SVM destek vektörlerini (temel eğitim demetleri) ve kenar boşluklarını (tarafından tanımlanan) kullanan hiper düzlem destek vektörleri bulur. Son zamanlarda DVM'ler büyük ilgi görmektedir. Peki ama neden? diye soracak olursak; destek vektör makineleri hakkındaki ilk makale 1992'de Vladimir Vapnik ve meslektaşları Bernhard Boser ve Isabelle Guyon tarafından sunulmuştur. Ancak SVM'nin temeli olan istatistiksel öğrenme teorisi 1960'lara kadar dayanmaktadır. En hızlı SVM'lerin bile eğitim süresi son derece yavaş olabilir. Doğrusal olmayan karar sınırlarından dolayı, karmaşık modelleme yetenekleri sayesinde oldukça hassastırlar. Bulunan destek vektörleri ayrıca öğrenilenlerin kompakt bir tanımını sağlar. SVM'ler, sınıflandırmanın yanı sıra genellikle sayısal tahmin için de kullanılabilir. El yazısı rakam tanıma, nesne tanıma ve konuşmacı

tanımlamanın testlerinin yanı sıra kıyaslama zaman serisi tahmini dahil olmak üzere bir dizi alana uygulanmışlardır (Han et al., 2012).

3.2.3. Lojistik Regresyon

Lojistik Regresyon istatistiksel model (logit modeli olarak da bilinir), genellikle sınıflandırma ve tahmine dayalı analitik için kullanılır. Lojistik regresyon, belirli bir bağımsız değişken veri kümesine dayalı olarak, oy verilmiş veya verilmemiş gibi bir olayın meydana gelme olasılığını tahmin eder. Sonuç bir olasılık olduğu için bağımlı değişken, 0 ile 1 arasında sınırlanır. Lojistik regresyonda olasılıklara bir logit dönüşümü uygulanır. Yani başarı olasılığının başarısızlık olasılığına bölümüdür. Bu aynı zamanda günlük olasılıklar veya olasılıkların doğal logaritması olarak da bilinir ve bu lojistik fonksiyon aşağıdaki formüllerle temsil edilir:

$$\text{Logit}(p_i) = 1/(1+ \exp(-p_i))$$

$$\ln(p_i/(1-p_i)) = \text{Beta\_0} + \text{Beta\_1}*X\_1 + \ldots + B\_k*K\_k \qquad (3.2)$$

Bu lojistik regresyon denkleminde logit(pi), bağımlı veya yanıt değişkeni; x ise bağımsız değişkendir. Bu modeldeki beta parametresi veya katsayısı, genellikle maksimum olasılık tahmini (MLE) aracılığıyla tahmin edilir. Bu yöntem, günlük oranlarının en iyi şekilde uyması için optimize etmek üzere birden fazla yineleme yoluyla farklı beta değerlerini test eder. Tüm bu iterasyonlar, log olabilirlik fonksiyonunu üretir ve lojistik regresyon, en iyi parametre tahminini bulmak için bu fonksiyonu maksimize etmeye çalışır. Optimal katsayı bulunduğunda her gözlem için koşullu olasılıklar hesaplanabilir, günlüğe kaydedilebilir ve tahmini bir olasılık elde etmek için birlikte toplanabilir. İkili sınıflandırma için 0,5'ten küçük bir olasılık 0'ı tahmin ederken; 0'dan büyük bir olasılık 1'i tahmin etmektedir. Model hesaplandıktan sonra modelin bağımlı değişkeni ne kadar iyi tahmin ettiğini değerlendirmek, en iyi uygulamadır.

3.2.4. k-En Yakın Komşu Algoritması

Yöntem, büyük eğitim veri setleri verildiğinde yavaş çalıştığından popülerlik kazanamamıştır. 1960'lardan sonra artan bilgi işlem cihazlarının gücü sayesinde tekrar kullanılmaya başlanmıştır. 1960'lardan günümüze kadar genellikle örüntü tanıma alanında yaygın olarak kullanılmaktadır (Han et al., 2012).

En yakın komşu sınıflandırıcılar, analoji yolunu kullanır. Yani kendisine benzer eğitim grupları olan belirli bir test grubunu karşılaştırarak öğrenmeye dayanır. Eğitim demetleri n nitelikle tanımlanır. Her demet, n boyutlu uzayda bir noktayı temsil eder. İçinde bu şekilde, tüm eğitim demetleri n boyutlu bir desen uzayında saklanır. Bilinmeyen bir demet, bir k-en yakın komşu sınıflandırıcı, k için örüntü uzayını arar. Bilinmeyen demete en yakın eğitim demetleri, bu k eğitim grubu, k bilinmeyen demetin en yakın komşularıdır (Han et al., 2012).

"Yakınlık", Öklid mesafesi gibi bir mesafe ölçüsü cinsinden tanımlanır [99]. Bu İki nokta veya demet arasındaki Öklid mesafesidir. Bir örnek verecek olursak;

X_1 D .x_{11}, x_{12}, : : : , x_{1n}/ ve

X_2 D .x_{21}, x_{22}, : : : , x_{2n}/, gibidir.

$$dist(X_1, X_2) = \sqrt{\sum_{i=1}^{n} (x_{1i} - x_{2i})^2} \quad (3.3)$$

Başka bir deyişle, her bir sayısal özellik için karşılık gelen özellikler arasındaki fark alınır. X_1 demetindeki ve X_2 demetindeki bu özniteliğin değerleri, bu farkın karesini alır ve biriktirir. Toplam birikmiş mesafe sayısının karekökü alınır. Tipik olarak, eşitliği kullanmadan önce her özelliğin değerleri normalleştirilir (Han et al., 2012).

Başlangıçta geniş aralıklara sahip niteliklerin (ör. gelir) niteliklere ağır basmasını önleme başlangıçta daha küçük aralıklarla (ör. ikili nitelikler). Min-maks normalleştirme, örneğin, A sayısal özniteliğinin v değerini [0, 1] aralığında v 0'a dönüştürmek için hesaplama ile kullanılabilir (Han et al., 2012).

$$v^1 = \frac{v - min_A}{max_A - min_A} \quad 3.4)$$

Burada minA ve maxA, A özelliğinin minimum ve maksimum değerleridir. Bir veri dönüştürme biçimi olarak veri normalleştirme için diğer yöntemleri açıklar [99].

k-en yakın komşu sınıflandırması için, bilinmeyen demet k-en yakın komşuları arasında sınıfta en yaygın olarak atanır. k D 1 olduğunda, bilinmeyen demet r desen uzayında kendisine en yakın olan eğitim demetinin sınıfına atanır. En yakın komşu sınıflandırıcılar sayısal tahmin için, yani gerçek değerli bir tahmin döndürmek için belirli bir bilinmeyen demet için de kullanılabilir. Bu durumda, bilinmeyen demetin k-en yakın komşusuyla ilişkili gerçek değerli etiketler sınıflandırıcı ortalama değeri döndürür (Han et al., 2012).

"Fakat sayısal olmayan, ancak nominal olan nitelikler için veya kategorik olan renk için mesafe nasıl hesaplanabilir?" Önceki tartışma, kullanılan özniteliklerin demetleri tanımlamak için hepsi sayısaldır. Nominal nitelikler için basit bir yöntem, X_1 demetindeki özniteliğin ilgili değeri X_2 demetindeki değerle karşılaştırılır. Eğer ikisi aynı ise (örneğin, X_1 ve X_2 demetlerinin her ikisi de mavi renge sahiptir) o zaman fark ikisi arasındaki değer 0 olarak alınır. İkisi farklı ise (örneğin, X_1 demeti mavi, ancak X_2 demeti kırmızı) o zaman fark 1 olarak kabul edilir. Diğer yöntemler daha fazlasını içerebilir. Diferansiyel derecelendirme için karmaşık şemalar da kullanılır. Örneğin, daha büyük bir fark puanının örneğin mavi ve beyaz yerine mavi ve siyah olarak atanmıştır (Han et al., 2012).

"Kayıp değerler ne olacak?" Genel olarak, belirli bir A özelliğinin değeri eksikse X_1 demetinde ve/veya X_2 demetinde olası maksimum fark varsayılır. Özniteliklerin her birinin [0, 1] aralığına eşlendiği ve nominal nitelikler için A'nın karşılık gelen değerlerinden biri veya her ikisi birden ise fark değeri 1 olarak alınır. A sayısal ise ve hem X_1 hem de X_2 demetlerinde eksikse o zaman fark değeri de 1 olarak alınır (Han et al., 2012).

Bu, deneysel olarak belirlenebilir. K=1 ile başlayarak, hata oranını tahmin etmek için bir test seti kullanılır. Sınıflandırıcının bu işlem, izin vermek için k artırılarak her seferinde tekrarlanabilir ve bir komşu daha minimum hata oranını veren k değeri seçilebilir. İçinde genel olarak eğitim demetlerinin sayısı ne kadar fazlaysa k'nin değeri de o kadar büyük olacaktır. Yani sınıflandırma ve sayısal tahmin kararlarının daha büyük bir kısmına dayandırılabileceği saklanan demetlerdir. Eğitim demetlerinin sayısı sonsuza ve k=1'e yaklaştığında hata oranı, Bayes hata oranının iki katından daha kötü olamaz. Eğer k de sonsuza yaklaşırsa hata oranı, Bayes hata oranına yaklaşır (Han et al., 2012).

En yakın komşu sınıflandırıcılar, özünde atayan her özelliğe eşit ağırlık mesafeye dayalı karşılaştırmalar kullanır. Bu nedenle, verildiğinde zayıf doğruluktan gürültülü veya alakasız özellikler muzdarip olabilirler. Bununla birlikte, yöntem, dahil etmek için öznitelik ağırlıklandırma ve gürültülü veri demetlerinin budanması değiştirilmiştir. Bir mesafe metriği seçimi kritik olabilir. Manhattan (şehir bloğu) mesafesi veya diğer mesafe ölçümler de kullanılabilir (Han et al., 2012).

En yakın komşu sınıflandırıcılar, test gruplarını sınıflandırırken aşırı derecede yavaş olabilir. Eğer D lDl demetlerinin bir eğitim veri tabanıdır ve D 1, sonra O (lDl) karşılaştırmaları gereklidir. Belirli bir test grubunu sınıflandırın ve saklanan demetleri önceden sıralayarak ve arama ağaçlarına yerleştirerek karşılaştırma sayısı O(log(lDl)'ye düşürülebilir. Paralel uygulama şunları yapabilir: çalışma süresini bir sabite, yani lDl'den bağımsız O(1)'ye düşürün (Han et al., 2012).

Sınıflandırma süresini hızlandırmak için diğer teknikler, hesaplamalar ve saklanan demetleri düzenleme kısmi mesafe kullanımını içerir. Kısmi mesafe yönteminde n özelliğin bir alt kümesine dayalı mesafe hesaplanır. Bu mesafe bir eşiği aşarsa daha sonra verilen depolanan demet için daha fazla hesaplama ve işlem devam eder; bir sonraki saklanan kayıt grubuna durdurulur. Düzenleme yöntemi, yararsız olduğu kanıtlanan eğitim demetlerini kaldırır. Bu yöntem, toplam depolanan demet sayısından dolayı aynı zamanda budama veya yoğunlaştırma olarak da adlandırılır (Han et al., 2012).

3.2.5. AdaBoost

Adaptive Boosting (AdaBoost), popüler bir boost algoritmasıdır. Örneğin bir öğrenme yönteminin doğruluğunu artırmak istiyoruz. Bize bir veri seti olan D verildi, d sınıfı etiketli demetler, (X_1, y_1), (X_2, y_2), : : : , (X_d, y_d), burada ki Xi demetin sınıf etiketidir. AdaBoost, başlangıçta her eğitim grubuna 1/d'lik eşit bir ağırlık atar. Oluşturma topluluk için k sınıflandırıcı, algoritmanın geri kalanında k tur gerektirir. İçinde i turunda, D'deki demetler, d boyutunda bir eğitim seti Di oluşturmak için örneklenir. Değiştirmeli örnekleme kullanılır. Aynı demet birden fazla seçilebilir. Her demet seçilme şansı ağırlığına bağlıdır. Bir sınıflandırıcı model olan M_i türetilmiştir. D_i'nin eğitim demetleri, hatası daha sonra test seti olarak D_i kullanılarak hesaplanır. Ağırlıkları eğitim demetleri daha sonra nasıl sınıflandırıldıklarına göre ayarlanır (Han et al., 2012).

Bir demet yanlış sınıflandırılmışsa ağırlığı artar; bir demet doğru sınıflandırılmışsa ağırlığı azalır. Bir demetin ağırlığı, sınıflandırmanın ne kadar zor olduğunu yansıtır. Ağırlık ne kadar yüksekse o kadar sıklıkla yanlış sınıflandırılır. Bu ağırlıklar olacak sonraki turun sınıflandırıcısı için eğitim örnekleri oluşturmak için kullanılır. Temel fikir bir sınıflandırıcı oluşturulduğunda, onun yanlış sınıflandırılmış demetlerine daha fazla odaklanması istenir. Önceki tur bazı sınıflandırıcılar, bazı zor demetleri

sınıflandırmada daha iyi olabilir. Bu şekilde birbirini tamamlayan bir dizi sınıflandırı oluşturulur (Han et al., 2012). Algoritmada yer alan bazı matematik işlemlerine bakıldığında;

Hesaplamak M_i modelinin hata oranı, M_i'deki D_i'deki demetlerin her birinin ağırlıklarını toplanır yanlış sınıflandırılmış. Yani,

$$error(M_i) = \sum_{j=1}^{d} W_j \; x \; err(X_j) \tag{3.5}$$

burada hata (X_j), X_j demetinin yanlış sınıflandırma hatasıdır: Eğer demet yanlış sınıflandırılmışsa o zaman hata (X_j)=1'dir; aksi takdirde, 0'dır. M_i sınıflandırıcısının performansı o kadar zayıfsa hatası 0,5'i geçerse o terk edilir. Bunun yerine, yeni bir Di eğitimi oluşturarak tekrar denenir ve buradan yeni bir M_i türetilir (Han et al., 2012).

Mi'nin hata oranı, eğitim demetlerinin ağırlıklarının nasıl güncellendiğini etkiler. i turundaki bir demet doğru bir şekilde sınıflandırıldıysa ağırlığı hatayla çarpılır. Hata (M_i)/(1- Hata (M_i)) olur. Tüm doğru sınıflandırılmış demetlerin ağırlıkları güncellendikten sonra yanlış sınıflandırılmış olanlar dahil tüm demetler için ağırlıklar normalleştirilir. Böylece toplamları daha önce olduğu gibi kalır. Bir ağırlığı normalleştirmek için toplamıyla çarpılır. Yani eski ağırlıkların yeni ağırlıkların toplamına bölümüdür. Sonuç olarak, daha önce açıklandığı gibi yanlış sınıflandırılan ağırlıklar demetler artırılır ve doğru sınıflandırılan demetlerin ağırlıkları azaltılır (Han et al., 2012).

Yükseltme tamamlandığında sınıflandırıcılar topluluğu sınıf etiketini tahmin etmek için nasıl kullanılır? Her sınıflandırıcıya eşit oy atanan torbalamanın aksine, sınıflandırıcının ne kadar iyi performans gösterdiğine bağlı olarak her sınıflandırıcının oyu için bir ağırlık atanır. Bir sınıflandırıcının hata oranı ne kadar düşükse o kadar doğru olur ve dolayısıyla ağırlığı oylama için sınıflandırıcı Mi'nin oylarının ağırlığı o kadar yüksek olmalıdır (Han et al., 2012).

$$\log \frac{1-error(M_i)}{error(M_i)} \tag{3.6}$$

Her c sınıfı için, c sınıfını X'e atayan her sınıflandırıcının ağırlıkları toplanır. Yani en yüksek toplam kazanan olur ve X grubu için sınıf tahmini olarak döndürülür. Yükseltme, torbalamayla nasıl karşılaştırılır? diye düşünülürse, Boosting'in odaklandığı yol nedeniyle yanlış sınıflandırılmış demetler, ortaya çıkan bileşik modeli bu tür verilere fazla uydurma riskini taşır (Han et al., 2012).

Algoritma: AdaBoost, yükseltme algoritması bir sınıflandırıcı grubu oluşturun [99]. Her biri ağırlıklı oy verir.

Girdi:

- D, bir dizi d sınıfı etiketli eğitim demetleri;
- *k*, tur sayısı (her turda bir sınıflandırıcı üretilir);
- bir sınıflandırma öğrenme şeması.

Çıktı:

Metot

(1) D'deki her demetin ağırlığını 1=d olarak sıfırlayın;

(2) for i D 1 to *k* do // her tur için:

(3) Di elde etmek için demet ağırlıklarına göre değiştirilerek örnek D;

(4) bir M_i modeli türetmek için D_i eğitim setini kullanın;

(5) hesaplama hatası(M_i), M_i'nin hata oranı

(6) eğer hata (M_i) > 0,5 ise o zaman

(7) 3. adıma geri dönün ve tekrar deneyin;

(8) son

(9) D_i'de doğru şekilde sınıflandırılan her demet için

(10) demetin ağırlığını error ile çarpın (M_i)/(1 hata(M_i)); // ağırlıkları güncelle

(11) her demetin ağırlığını normalize edin;

(12) son

Topluluğu, X grubunu sınıflandırmak üzere kullanmak için:

(1) her sınıfın ağırlığını 0 olarak başlat;

(2) for i = 1 to k do // her sınıflandırıcı için:

(3) wi = log 1 - hata(M_i) / hata(M_i) ; // sınıflandırıcının oy ağırlığı

(4) c = M_i(X); // M_i'den X için sınıf tahmini alın

(5) c sınıfı için ağırlığa M_i ekleyin

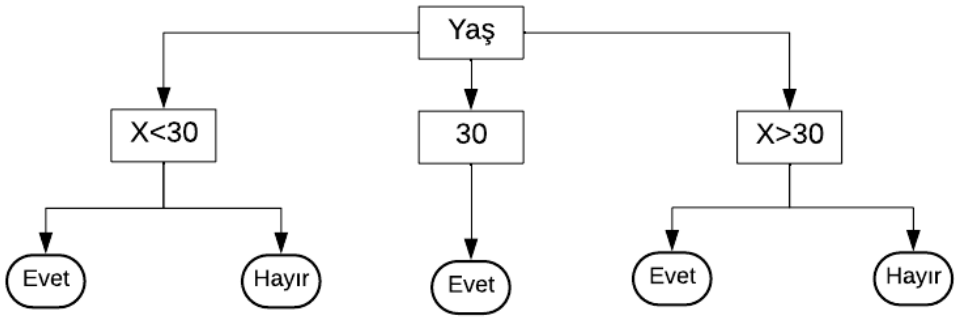
(6) sonu

(7) en büyük ağırlığa sahip sınıfı döndürür;

* AdaBoost, bir artırma algoritmasıdır.*

3.2.6. Karar Ağacı

Karar ağacı indüksiyonu, sınıf etiketli demetler eğitiminden karar ağaçlarının öğrenilmesidir. Karar ağacı, akış şeması benzeri bir ağaç yapısıdır. Burada her bir dahili düğüm (yaprak olmayan düğüm), bir öznitelik üzerinde bir testi belirtir; her dal bir sonucu temsil eder. Test ve her yaprak düğüm (veya terminal düğüm), bir sınıf etiketine sahiptir. En üstteki düğüm, ağaç kök düğümdür. Tipik bir karar ağacı aşağıda gösterilmiştir. Örneğin bilgisayar satın alması, yani elektronik firmasındaki bir müşterinin bilgisayar satın alıp almayacağını tahmin eder. Dahili düğümler dikdörtgenler ve yaprak düğümlerle, ovallerle gösterilir. Bazı karar ağacı algoritmaları yalnızca ikili ağaçlar üretir iken; diğerleri, ikili olmayan ağaçlar üretebilir Örnek bir karar ağacı Şekil 3.1'de gösterilmektedir. (Han et al., 2012).



Şekil 3.1: Karar ağacı diyagramının şekil üzerinde gösterilmesi.

İlişkili olduğu X demeti verildiğinde sınıf etiketi bilinmiyorsa, demetin öznitelik değerleri karar ağacına karşı test edilir; kökten, sınıfı tutan yaprak düğüme giden bir yol izlenir. Karar ağaçları, kolayca sınıflandırma kurallarına dönüştürülebilir (Han et al., 2012).

"Karar ağacı sınıflandırıcıları neden bu kadar popüler?" Karar ağacı sınıflandırıcılarının yapısı herhangi bir alan bilgisi veya parametre ayarı gerektirmez ve bu nedenle keşfedici bilgi keşfi için uygundur. Sonuç olarak karar ağaçları verileri çok boyutlu işleyebilir. Edinilen bilgiyi ağaç biçiminde temsil etmeleri sezgiseldir ve genellikle insanlar tarafından asimile edilmesi kolaydır. Karar ağaçları öğrenme ve

sınıflandırma adımları ağaç indüksiyonu basit ve hızlıdır. Genel olarak, karar ağacı sınıflandırıcıları iyi bir doğruluğa sahiptir. Ancak başarılı kullanım eldeki verilere bağlı olabilir. Karar ağacı indüksiyonu, algoritmalar, imalat ve üretim, finansal analiz, astronomi ve moleküler biyoloji ve tıp gibi birçok uygulama alanında sınıflandırma için kullanılmıştır (Han et al., 2012).

3.2.7. Rastgele Orman

Rastgele ormanlar adı verilen başka bir topluluk yöntemi daha vardır. Her bir topluluktaki sınıflandırıcılar, bir karar ağacı sınıflandırıcısıdır; sınıflandırıcılar topluluğu ise bir "orman"dır. Bireysel karar ağaçları, bölünmeyi belirlemek için her düğümdeki öznitelikler rastgele bir seçim kullanılarak oluşturulur. Daha resmi olarak, her ağaç bağımsız olarak ve aynı dağılımla örneklenmiş rastgele bir vektörün değerleri, ormandaki tüm ağaçlardır. Sınıflandırma sırasında her ağaç oy verir ve en popüler sınıfa geri döner (Han et al., 2012).

Rastgele ormanlar, rastgele ormanlarla birlikte torbalama öznitelik seçimi kullanılarak oluşturulabilir. D demetlerinden oluşan bir eğitim seti verilir ve oluşturmak için genel prosedür topluluk için k tane karar ağacı aşağıdaki gibidir. Her yineleme için, *i* (*i*= 1, 2, : : : , *k*), d demetlerinden oluşan bir eğitim seti D_i , D'den değiştirilerek örneklenir. Yani, her D_i bir D'nin önyükleme örneği, böylece bazı demetler bir defadan fazla oluşabilir Di'de, diğerleri hariç tutulabilir. Kullanılacak özelliklerin sayısı F olsun. F'nin mevcut sayıdan çok daha küçük olduğu her düğümdeki bölünmeyi öznitellikler belirleyin. Bir karar ağacı sınıflandırıcısı Mi oluşturmak için her düğümde rasgele seçim yapın. F düğümdeki bölme için aday olarak nitelik gösterir. CART metodolojisi, ağaçların büyütülmesi için kullanılır. Ağaçlar maksimum boyuta büyütülür ve azaltılmaz. Rastgele giriş seçimi ile bu şekilde oluşturulan ormanlara Forest-RI denir (Han et al., 2012).

Forest-RC adı verilen başka bir rastgele orman biçimi, giriş özniteliklerinden rastgele doğrusal kombinasyonlar kullanır. Niteliklerin bir alt kümesini rastgele seçmek yerine mevcut niteliklerin doğrusal bir kombinasyonu olan yeni nitelikler seçilir. Yani bir öznitelik, kullanılacak orijinal özniteliklerin sayısı olan L belirtilerek oluşturulur. Kombine belirli bir düğümde L nitelikleri rastgele seçilir ve şunlarla birlikte eklenir: [-1, 1] üzerinde tekdüze rastgele sayılar olan katsayılardır. F doğrusal kombinasyonları oluşturulur ve bunlar üzerinden en iyi dağılım için arama yapılır. Bu rastgele orman

biçimi, korelasyonu azaltmak için yalnızca birkaç özellik mevcut olduğunda bireysel sınıflandırıcılar arasında kullanışlıdır (Han et al., 2012).

Rastgele ormanlar, doğruluk açısından AdaBoost ile karşılaştırılabilir ancak, hatalar ve aykırı değerler olabilir. Bir orman için genelleme hatası, sayı olduğu sürece yakınsayarak ormandaki ağaçların sayısı büyüktür. Bu nedenle, aşırı uyum bir sorun değildir. Doğruluğu bir rastgele orman, bireysel sınıflandırıcıların gücüne ve arasındaki bağımlılık ile ilgilidir. İdeal olan, bireysel sınıflandırıcıların korelasyonlarını arttırmadan gücünü korumaktır. Rastgele ormanlar, sayıya duyarsızdır ve her bölmede dikkate alınmak üzere seçilen niteliklerdir. Tipik olarak, $\log_2 d'+1$ seçilir. İlginç bir ampirik gözlem, tek bir rastgele girdi özelliği kullanmanın genellikle birkaç özellik kullanıldığında daha yüksek olan iyi bir doğrulukla sonuçlanabilir. Rastgele ormanlar her bölme için çok daha az özniteliği dikkate aldığından çok büyük veritabanlarında verimlidirler. Torbalama veya güçlendirmeden daha hızlı olabilirler. Rastgele ormanlar, değişken öneme sahip dahili tahminler verirler (Han et al., 2012).

3.2.8. Bagging

Doğruluğu artırmanın bir yöntemi olarak torbalamanın (bagging) nasıl çalıştığına sezgisel bir bakış için aşağıdaki senaryo kullanılabilir.

Farz edin ki bir hastanızın belirtilerine ve durumuna göre bir teşhis konulmasını istiyorsunuz. Bir doktora sormak yerine birkaç doktora sormayı seçebilirsiniz. Eğer belirli teşhis, diğerlerinden daha fazla gerçekleşirse bunu nihai veya en iyi teşhis olarak seçebilirsiniz. Yani nihai teşhis, her doktorun aldığı oy çokluğuna göre yapılır. Sezgisel olarak, büyük bir doktor grubu tarafından verilen çoğunluk oyu, küçük bir grup tarafından yapılan çoğunluk oylamasından daha güvenilirdir (Han et al., 2012).

D demetlerinden oluşan bir D kümesi verildiğinde torbalama şu şekilde çalışır. Yineleme için i ($i = 1, 2, : : : , k$), d demetlerinden oluşan bir eğitim seti, D_i orijinal setten değiştirilerek örneklenir. D torbalama teriminin önyükleme toplaması anlamına geldiğini unutmayın. Çünkü değiştirme ile örnekleme kullanıldığında D'nin orijinal demetlerinden bazıları D_i'ye dahil edilmeyebilir. Oysa diğerleri birden fazla meydana gelebilir. Her eğitim seti D_i için bir sınıflandırıcı modeli M_i öğrenilir. Bilinmeyen bir grup X'i sınıflandırmak için her sınıflandırıcı M_i, kendi sınıf tahminini döndürerek bir oy olarak sayılır. Torbalı sınıflandırıcı M, oyları sayar ve sınıfı atar; en çok oyu X'e

verir. Torbalama, sürekli değerlerin tahminine uygulanabilir belirli bir test demeti için her tahminin ortalama değerini alır (Han et al., 2012).

Torbalı sınıflandırıcı, genellikle tek bir sınıflandırıcıdan önemli ölçüde daha fazla doğruluğa sahiptir. Orijinal eğitim verileri olan D'den türetilmiş ve önemli ölçüde daha kötü olmayacak ve gürültülü verilerin ve fazla uydurmanın etkilerine karşı daha sağlam olacaktır. Artan doğruluk oluşur çünkü bileşik model, bireysel sınıflandırıcıların varyansını azaltır (Han et al., 2012).

Girdi:

- D, bir dizi d eğitim demeti,
- *k*, topluluktaki model sayısı,
- bir sınıflandırma öğrenme şeması (karar ağacı algoritması, Naive Bayes, vb.).

Çıktı:

Metot

(1) for i = 1 ila k yapmak // k model oluşturmak için;

(2) değiştirme ile D'yi örnekleyerek önyükleme örneği D_i oluşturun;

(3) bir model, M_i türetmek için D_i ve öğrenme şemasını kullanın;

(4) bitiş;

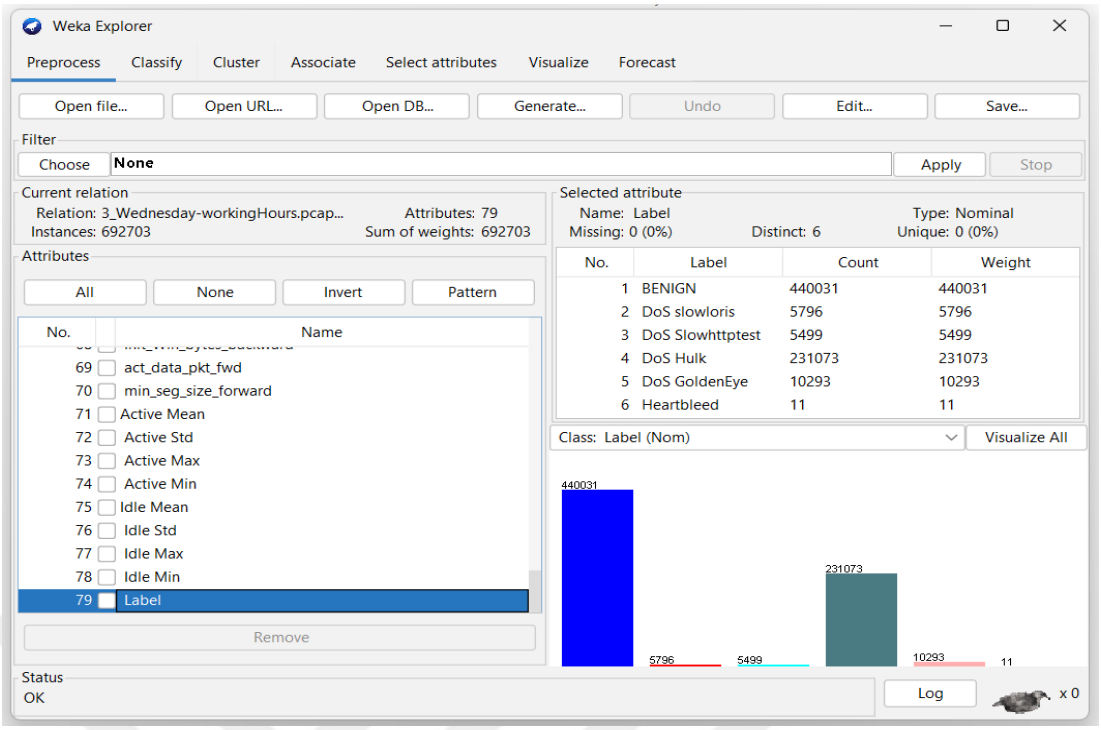
Bir demet X'i sınıflandırmak üzere grubu kullanmak için:

k modelin her birinin X'i sınıflandırmasına ve çoğunluk oyu vermesine izin verin;

3.3. Yöntem

3.3.1. Kullanılan Yazılım

WEKA, veri madenciliğinde yaygın olarak kullanılan Waikito Üniversitesi tarafından geliştirilen bir uygulama programıdır. Aşağıda WEKA uygulaması ekranına ait bir ekran görüntüsü Şekil 3.2'te sunulmuştur. Bu tez çalışmasında tamamen WEKA uygulaması kullanılarak sonuçlara ulaşılmıştır.



Şekil 3.2: WEKA uygulamasının keşif ekran görüntüsü.

3.3.2. Gerçekleme Ortamının Özellikleri

WEKA uygulamasının çalışması için donanım özellikleri, HP Gen 10 model Vsphere sanallaştırma programı üzerinde çalışan Windows 10 Pro işletim sistemine sahip, donanım bilgileri Intel ® Xeon ® Gold 5218R CPU @ 2,10Ghz işlemci, 128 GB Ram ve 512 GB disk sürücüye sahip bilgiler ile uygulama programı çalıştırılmıştır.

3.3.3. Veri Bölme Yöntemi

Bu tez çalışmasında üç test yöntemi kullanılmıştır. Birincisinde bölme yöntemi kullanılarak veri seti %80 eğitim-%20 test oranında bölünmüş; ikincisinde 5-kat çapraz doğrulama; üçüncüsünde ise 10-kat çapraz doğrulama yöntemi kullanılmıştır.

Bölme yönteminde veri setinin tamamı %80 eğitim ve %20 test veri seti olarak modellenmiştir. CIC-IDS2017 Çarşamba günü olan DoS veri setinde toplam 692703 adet verinin 554162 tanesi, modelin eğitilmesi için kullanılırken; 138540 tanesi, test verisi olarak kullanılmıştır.

5-kat çapraz doğrulama tekniğinde her bir adımda 692703 adet verinin 554162 tanesi modelin eğitilmesi için kullanılırken; 138540 tanesi test verisi olarak kullanılmıştır.

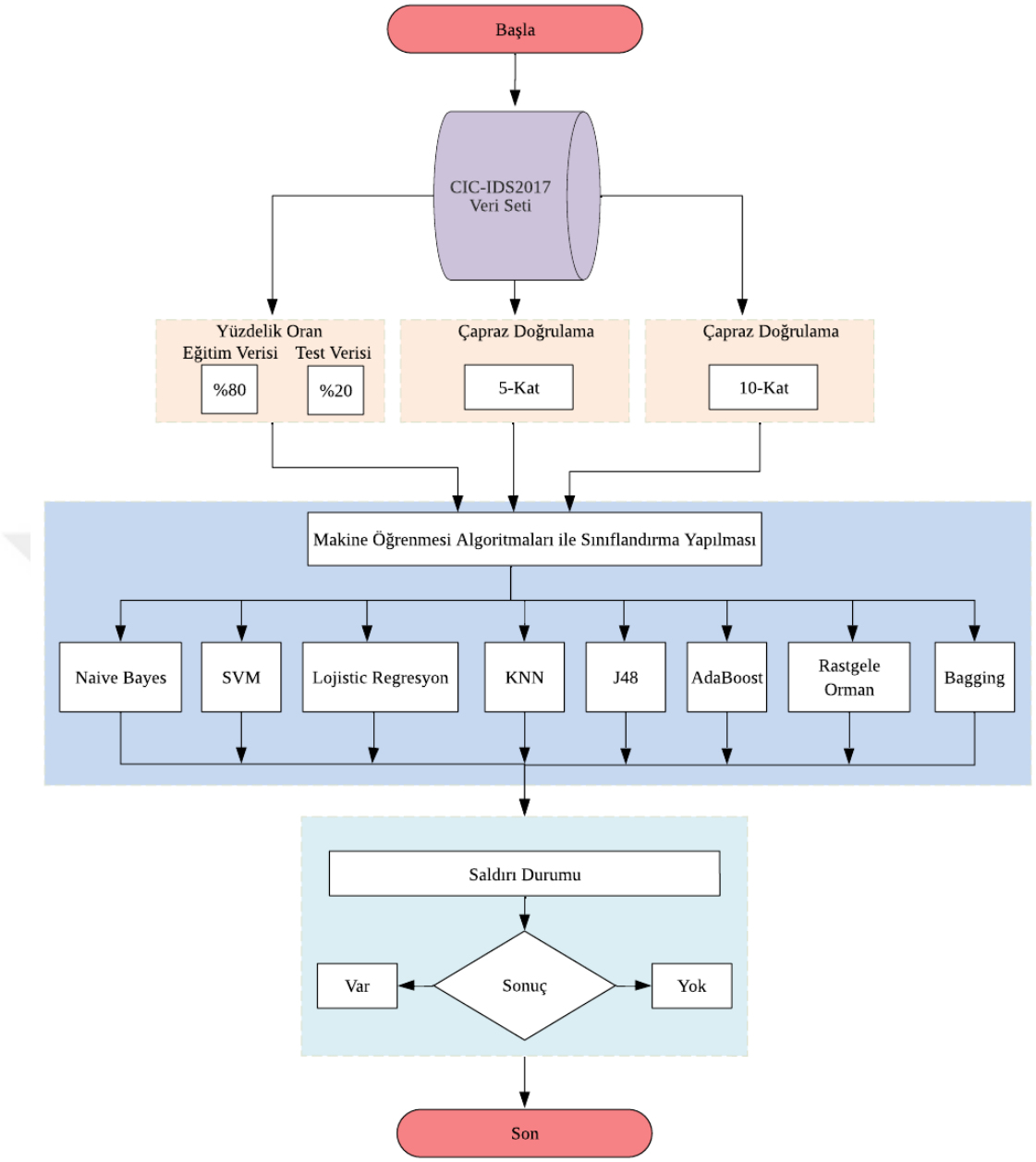
10-kat çapraz doğrulama tekniğinde ise her bir adımda 692703 adet verinin 623432 tanesi modelin eğitilmesi için kullanılırken; 69270 tanesi test verisi olarak kullanılmıştır.

3.3.4. Tez Kapsamında Kullanılan Metotlar

Bu tez çalışmasında, CIC-IDS2017 Çarşamba günü olan DoS veri setinin tamamında hiçbir değişiklik yapılmadan ilk olarak orijinal hali ile bir sonuca ulaşılmış ve tabloda sunulmuştur. İkincisinde temel bileşen analizinden özellik çıkarımı yapılarak bir sonuca ulaşılmış ve tabloda sunulmuştur. Üçüncüsünde ise yedi adet özellik seçimi yapılarak yedi sonuca ulaşılmış ve bunlar tablolarda sunulmuştur.

3.3.4.1. Orijinal Veri Setinin Kullanımına Dayalı Metot

Bu tez çalışmasında CIC-IDS2017 orijinal veri setinde hiçbir değişiklik yapılmadan %80 eğitim-%20 test yüzdelik oranı ve 5-kat veya 10-kat çapraz doğrulama modeli olmak üzere 3 farklı metot kullanılmıştır. Bu metotlar Naive Bayes, destek vektör makinesi, lojistik regresyon, k-en yakın komşu, karar ağacı (J48), AdaBoost, rastgele orman ve bagging makine öğrenme yöntemleri kullanılarak, saldırının var veya yok şeklinde gösterildiği orijinal veri setinin kullanımına dayalı metodun akış diyagramı Şekil 3.3'te gösterilmektedir.

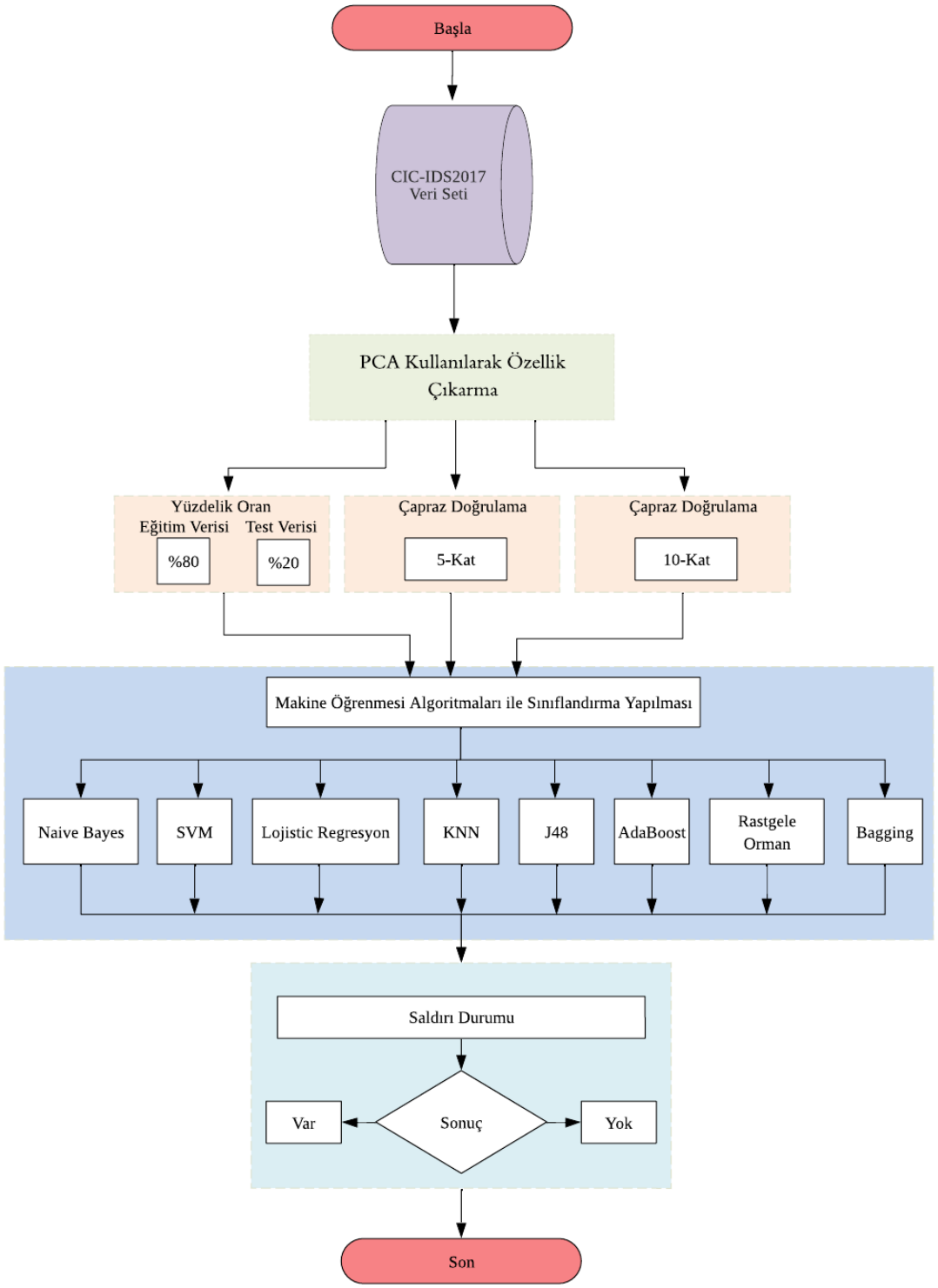


Şekil 3.3: Orijinal veri setinin kullanımına dayalı metodun akış diyagramı.

3.3.4.2. Temel Bileşen Analizine Dayalı Metot

Bu tez çalışmasında CIC-IDS2017 orijinal veri seti üzerinde temel bileşen analizi (Principal Component Analysis-PCA) yöntemi uygulanarak veri setinde bulunan en değerli 21 tane özellik çıkarımı elde edilmiştir. Bu veriler üzerinde %80 eğitim-%20 test yüzdelik oranı ve 5-kat veya 10-kat çapraz doğrulama olmak üzere 3 farklı metot kullanılmıştır. Bu metotlar Naive Bayes, destek vektör makinesi, lojistik regresyon, k-en yakın komşu, karar ağacı (J48), AdaBoost, rastgele orman ve bagging makine

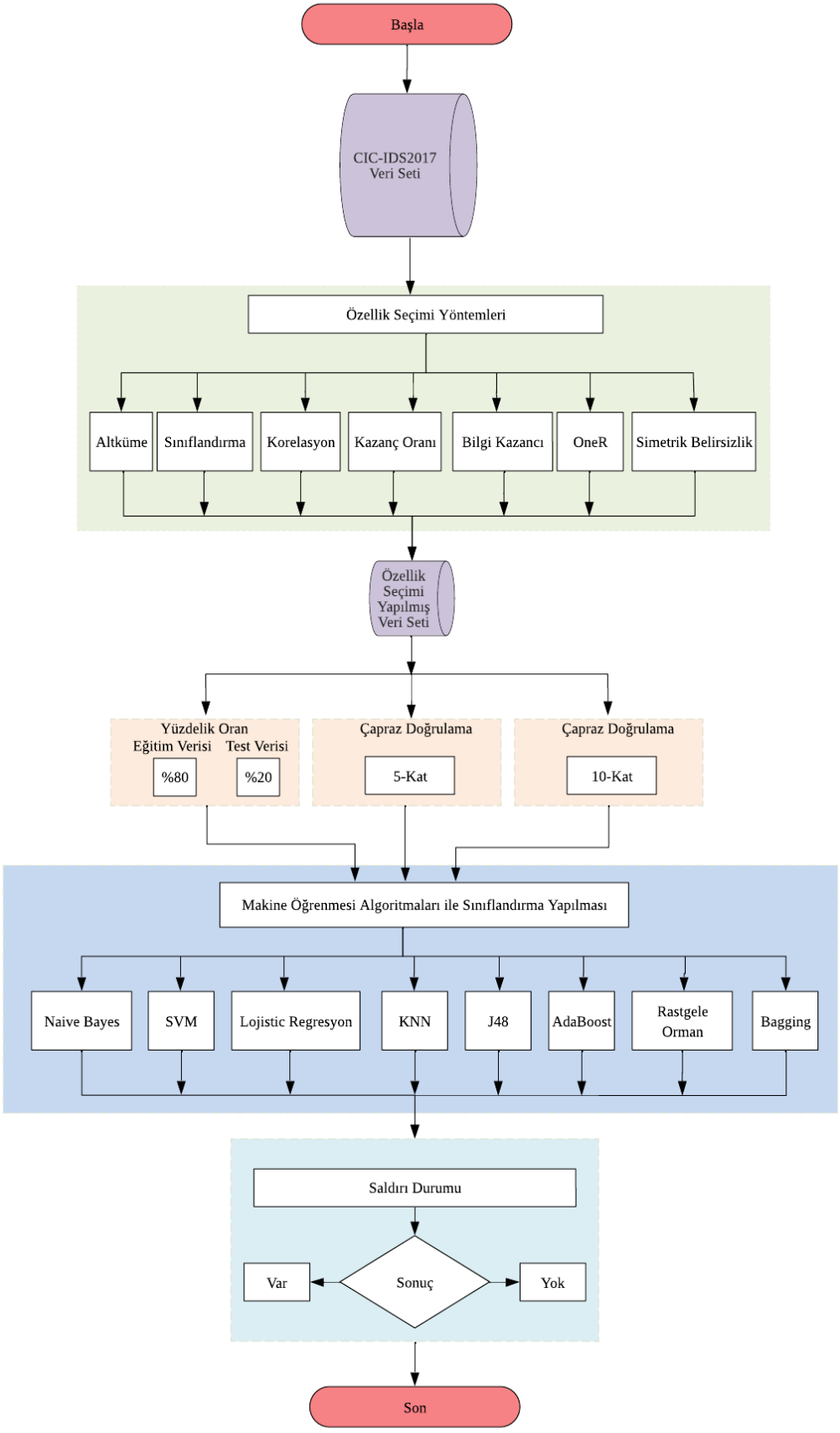
öğrenme yöntemleri kullanılarak, saldırının var veya yok şeklinde gösterildiği temel bileşen analizine dayalı metodun akış diyagramı Şekil 3.4'te gösterilmektedir.



Şekil 3.4: Temel bileşen analizine dayalı metodun akış diyagramı.

3.3.4.3. Özellik Seçimine Dayalı Metot

Bu tez çalışmasında, CIC-IDS2017 orijinal veri seti üzerinde WEKA uygulamasında yaygın olarak kullanılan yedi adet özellik seçimi yöntemlerinden olan altküme, sınıflandırma, korelasyon, kazanç oranı, bilgi kazancı, OneR ve simetrik belirsizlik yöntemleri uygulanarak veri setinde bulunan en değerli 10 tane özellik seçimi elde edilmiştir. Bu veriler üzerinde %80 eğitim-%20 test yüzdelik oranı ve 5-kat veya 10-kat çapraz doğrulama olmak üzere 3 farklı metot kullanılmıştır. Bu metotlar Naive Bayes, destek vektör makinesi, lojistik regresyon, k-en yakın komşu, karar ağacı (J48), AdaBoost, rastgele orman ve bagging makine öğrenme yöntemleri kullanılarak, saldırının var veya yok şeklinde gösterildiği özellik seçimine dayalı metodun akış diyagramı Şekil 3.5'te gösterilmektedir.



Şekil 3.5: Özellik seçimine dayalı metodun akış diyagramı.

4. BULGULAR

4.1. Orijinal Veri Setinin Kullanılımına Dayalı Metodun Sonuçları

Bu tez çalışmasında, CIC-IDS2017 orijinal veri setinde hiçbir değişiklik yapılmadan veri setinin tamamı kullanılmıştır.

Veri bölme %80 eğitim-%20 test yüzdelik oranı, 5-kat ve 10-kat çapraz doğrulama modeli olmak üzere 3 farklı metot kullanılmıştır. Makine öğrenme yöntemlerinden olan Naive Bayes, destek vektör makinesi, lojistik regresyon, k-en yakın komşu, karar ağacı (J48), AdaBoost, rastgele orman ve bagging üzerinde WEKA uygulaması üzerinde çalıştırılmıştır.

Sonuç olarak bu tez çalışmasında orijinal veri setinin kullanılımına dayalı metot kullanılarak makine öğrenme yöntemlerinden olan karar ağacı (J48) yöntemi ile 10-kat çapraz doğrulama tekniği, saldırının var olup olmadığına dair en iyi sonucu veren yöntem olmuşlardır. İkinci ve üçüncü sırada ise makine öğrenme yöntemlerinden birisi olan bagging yöntemi ile 10-kat çapraz doğrulama ve %80-%20 bölme yöntemi ile en iyi sonuçlara ulaşılmıştır.

Orijinal veri setinin kullanılımına dayalı metodun kullanılması sonucunda elde edilen bilgiler, Tablo 4.1'de sunulmuştur.

Tablo 4.1: Orijinal veri setinin kullanımına dayalı metodun sonuçları.

Sınıflandırıcı	Veri Bölme Yöntemi	Kesinlik	Duyarlılık	F-Ölçütü	Doğruluk (%)
Naive Bayes	%80 - %20	0,950	0,916	0,927	91,6075
	5-Kat	0,949	0,914	0,926	91,4415
	10-Kat	0,949	0,915	0,926	91,4552
SVM	%80 - %20	0,977	0,977	0,977	97,6837
	5-Kat	0,977	0,977	0,977	97,6657
	10-Kat	0,977	0,977	0,977	97,6837
Lojistik Regresyon	%80 - %20	0,997	0,997	0,997	99,668
	5-Kat	0,997	0,997	0,997	99,6573
	10-Kat	0,997	0,997	0,997	99,6602
KNN	%80 - %20	1,000	1,000	1,000	99,9509
	5-Kat	0,999	0,999	0,999	99,9477
	10-Kat	0,999	0,999	0,999	99,9485
AdaBoost	%80 - %20	0,930	0,936	0,952	93,5824
	5-Kat	0,930	0,947	0,894	93,6033
	10-Kat	0,930	0,965	0,894	93,6035
Karar Ağacı (J48)	%80 - %20	0,999	0,999	0,999	99,9437
	5-Kat	1,000	1,000	1,000	99,9526
	10-Kat	1,000	1,000	1,000	99,9558
Rastgele Orman	%80 - %20	0,999	0,999	0,999	99,9444
	5-Kat	0,999	0,999	0,999	99,9391
	10-Kat	0,999	0,999	0,999	99,9415
Bagging	%80 - %20	1,000	1,000	1,000	99,9545
	5-Kat	1,000	1,000	1,000	99,9526
	10-Kat	1,000	1,000	1,000	99,9551

4.2. Temel Bileşen Analizine Dayalı Metodun Sonuçları

Bu tez çalışmasında, CIC-IDS2017 orijinal veri setinde temel bileşen analizi (Principal Component Analysis-PCA) yöntemi kullanılarak 21 tane özellik çıkarım yapılmıştır.

Veri bölme %80 eğitim - %20 test yüzdelik oranı, 5-kat ve 10-kat çapraz doğrulama modeli olmak üzere 3 farklı metot kullanılmıştır. Makine öğrenme yöntemlerinden olan Naive Bayes, destek vektör makinesi, lojistik regresyon, k-en yakın komşu, karar ağacı (J48), AdaBoost, rastgele orman ve bagging üzerinde WEKA uygulaması üzerinde çalıştırılmıştır.

Sonuç olarak bu tez çalışmasında temel bileşen analizine dayalı metot kullanılarak makine öğrenme yöntemlerinden olan k-en yakın komşu yöntemi ile 10-kat çapraz doğrulama tekniği, saldırının var olup olmadığına dair en iyi sonucu veren yöntem olarak ortaya çıkmıştır. İkinci ve üçüncü sırada aynı makine öğrenme yöntemi %80-%20 bölme yöntemi ve 5-kat çapraz doğrulama metodu ile en iyi sonuçlara ulaşılmıştır.

Temel bileşen analizine dayalı metodun kullanılması sonucunda elde edilen bilgiler Tablo 4.2'de sunulmuştur.

Tablo 4.2: Temel bileşen analizine dayalı metodun sonuçları.

Sınıflandırıcı	Veri Bölme Yöntemi	Kesinlik	Duyarlılık	F-Ölçütü	Doğruluk (%)
Naive Bayes	%80 - %20	0,783	0,600	0,601	60,0328
	5-Kat	0,782	0,596	0,598	59,7999
	10-Kat	0,782	0,598	0,597	59,7848
SVM	%80 - %20	0,938	0,968	0,836	96,7952
	5-Kat	0,940	0,968	0,839	96,797
	10-Kat	0,940	0,968	0,839	96,8034
Lojistik Regresyon	%80 - %20	0,978	0,978	0,978	97,8346
	5-Kat	0,978	0,978	0,978	97,8188
	10-Kat	0,978	0,978	0,978	97,817
KNN	%80 - %20	0,999	0,999	0,999	99,9271
	5-Kat	0,999	0,999	0,999	99,9219
	10-Kat	0,999	0,999	0,999	99,9267
AdaBoost	%80 - %20	0,891	0,902	0,909	90,2296
	5-Kat	0,891	0,902	0,908	90,1916
	10-Kat	0,902	0,902	0,820	90,1916
Karar Ağacı (J48)	%80 - %20	0,999	0,999	0,999	99,8838
	5-Kat	0,999	0,999	0,999	99,8979
	10-Kat	0,999	0,999	0,999	99,9000
Rastgele Orman	%80 - %20	0,999	0,999	0,999	99,9401
	5-Kat	0,999	0,999	0,999	99,9438
	10-Kat	0,999	0,999	0,999	99,9467
Bagging	%80 - %20	0,999	0,999	0,999	99,8925
	5-Kat	0,999	0,999	0,999	99,9018
	10-Kat	0,999	0,999	0,999	99,9075

4.3. Özellik Seçimine Dayalı Metodun Sonuçları

4.3.1. Altküme Tekniğinin Kullanılması

Bu tez çalışmasında, CIC-IDS2017 orijinal veri setinde WEKA uygulaması ile özellik seçimi yöntemlerinden birisi olan altküme (CfsSubsetval) tekniği kullanılarak özellik seçimi yapılmış olup 4 tanesi seçilmiştir. Özellik seçimi sonucunda elde edilen bilgiler, "Destination Port, Total Length of Bwd Packets, Init_Win_bytes_forward, Idle Max, Label" bilgileridir.

Veri bölme %80 eğitim - %20 test yüzdelik oranı, 5-kat ve 10-kat çapraz doğrulama modeli olmak üzere 3 farklı metot kullanılmıştır. Makine öğrenme yöntemlerinden olan Naive Bayes, destek vektör makinesi, lojistik regresyon, k-en yakın komşu, karar ağacı (J48), AdaBoost, rastgele orman ve bagging üzerinde WEKA uygulaması üzerinde çalıştırılmıştır.

Sonuç olarak bu tez çalışmasında altküme özellik seçimi metodu kullanılarak makine öğrenme yöntemlerinden olan rastgele orman ile 10-kat çapraz doğrulama tekniği, saldırının var olup olmadığına dair en iyi sonucu veren yöntem olarak ortaya çıkmıştır. İkinci ve üçüncü sırada aynı makine öğrenme yöntemi 5-kat çapraz doğrulama ve %80-%20 bölme yöntemi ile en iyi sonuçlara ulaşılmıştır.

Altküme özellik seçimine dayalı metodun kullanılması sonucunda elde edilen bilgiler Tablo 4.3'te sunulmuştur.

Tablo 4.3: Altküme özellik seçimine dayalı metodun sonuçları.

Sınıflandırıcı	Veri Bölme Yöntemi	Kesinlik	Duyarlılık	F-Ölçütü	Doğruluk (%)
Naive Bayes	%80 - %20	0,922	0,873	0,891	87,2637
	5-Kat	0,926	0,887	0,889	88,7149
	10-Kat	0,923	0,888	0,900	88,8353
SVM	%80 - %20	0,853	0,822	0,802	82,1533
	5-Kat	0,853	0,822	0,802	82,1885
	10-Kat	0,853	0,822	0,802	82,1885
Lojistik Regresyon	%80 - %20	0,682	0,827	0,645	82,7011
	5-Kat	0,535	0,828	0,496	82,7697
	10-Kat	0,685	0,828	0,648	82,751
KNN	%80 - %20	0,994	0,994	0,994	99,4045
	5-Kat	0,994	0,994	0,994	99,4091
	10-Kat	0,994	0,994	0,994	99,4153
AdaBoost	%80 - %20	0,849	0,835	0,822	83,4829
	5-Kat	0,850	0,835	0,823	83,5489
	10-Kat	0,850	0,835	0,823	83,5489
Karar Ağacı (J48)	%80 - %20	0,994	0,994	0,994	99,4269
	5-Kat	0,994	0,994	0,994	99,4413
	10-Kat	0,994	0,994	0,994	99,4422
Rastgele Orman	%80 - %20	0,994	0,994	0,994	99,4413
	5-Kat	0,994	0,995	0,994	99,4513
	10-Kat	0,994	0,995	0,994	99,4519
Bagging	%80 - %20	0,994	0,994	0,994	99,4319
	5-Kat	0,994	0,994	0,994	99,4467
	10-Kat	0,994	0,994	0,994	99,4431

4.3.2. SınıflandırmaTekniğinin Kullanılması

Bu tez çalışmasında, CIC-IDS2017 orijinal veri setinde WEKA uygulaması ile özellik seçimi yöntemlerinden birisi olan sınıflandırma (ClassifierAttributeEval) tekniği kullanılarak özellik seçimi yapılmış olup ilk 10 tanesi seçilmiştir. Özellik seçimi sonucunda elde edilen bilgiler, "Fwd IAT Std, Fwd IAT Max, Fwd IAT Min, Bwd

IAT Total, Bwd IAT Mean, Bwd IAT Std, Bwd IAT Max, Bwd IAT Min, Bwd PSH Flags, Idle Min, Label" bilgileridir.

Veri bölme %80 eğitim - %20 test yüzdelik oranı, 5-kat ve 10-kat çapraz doğrulama modeli olmak üzere 3 farklı metot kullanılmıştır. Makine öğrenme yöntemlerinden olan Naive Bayes, destek vektör makinesi, lojistik regresyon, k-en yakın komşu, karar ağacı (J48), AdaBoost, rastgele orman ve bagging üzerinde WEKA uygulaması üzerinde çalıştırılmıştır.

Sonuç olarak bu tez çalışmasında sınıflandırma özellik seçimi metodu kullanılarak makine öğrenme yöntemlerinden olan rastgele orman ile 10-kat çapraz doğrulama tekniği, saldırının var olup olmadığına dair en iyi sonucu veren yöntem olarak ortaya çıkmıştır. İkinci sırada aynı makine öğrenme yöntemi 5-kat çapraz doğrulama tekniği ile üçüncü sırada ise bagging makine öğrenme yöntemi 5-kat çapraz doğrulama tekniği ile en iyi sonuçlara ulaşılmıştır.

Sınıflandırma özellik seçimine dayalı metodun kullanılması sonucunda elde edilen bilgiler Tablo 4.4'te sunulmuştur.

Tablo 4.4: Sınıflandırma özellik seçimine dayalı metodun sonuçları.

Sınıflandırıcı	Veri Bölme Yöntemi	Kesinlik	Duyarlılık	F-Ölçütü	Doğruluk (%)
Naive Bayes	%80 - %20	0,788	0,778	0,775	77,7791
	5-Kat	0,784	0,774	0,771	77,3773
	10-Kat	0,786	0,777	0,774	77,6717
SVM	%80 - %20	0,901	0,837	0,537	83,7117
	5-Kat	0,904	0,838	0,545	83,7841
	10-Kat	0,904	0,838	0,545	83,7948
Lojistik Regresyon	%80 - %20	0,857	0,838	0,824	83,8019
	5-Kat	0,857	0,839	0,825	83,8823
	10-Kat	0,857	0,839	0,825	83,8808
KNN	%80 - %20	0,961	0,960	0,961	96,0337
	5-Kat	0,961	0,960	0,960	96,0163
	10-Kat	0,961	0,960	0,961	96,035
AdaBoost	%80 - %20	0,876	0,829	0,811	82,9372
	5-Kat	0,876	0,830	0,812	82,9797
	10-Kat	0,876	0,830	0,664	82,9797
Karar Ağacı (J48)	%80 - %20	0,963	0,962	0,962	96,1744
	5-Kat	0,963	0,962	0,962	96,1878
	10-Kat	0,963	0,962	0,962	96,2102
Rastgele Orman	%80 - %20	0,963	0,962	0,962	96,2242
	5-Kat	0,963	0,962	0,963	96,2347
	10-Kat	0,964	0,962	0,963	96,2451
Bagging	%80 - %20	0,963	0,962	0,962	96,2177
	5-Kat	0,963	0,962	0,962	96,2262
	10-Kat	0,963	0,962	0,963	96,2346

4.3.3. Korelasyon Tekniğinin Kullanılması

Bu tez çalışmasında, CIC-IDS2017 orijinal veri setinde WEKA uygulaması ile özellik seçimi yöntemlerinden birisi olan korelasyon (CorrelationAttributeEval) tekniği kullanılarak özellik seçimi yapılmış olup ilk 10 tanesi seçilmiştir. Özellik seçimi sonucunda elde edilen bilgiler, "Bwd Packet Length Max, Bwd Packet, Length Mean, Bwd Packet Length Std, Flow IAT Max, Fwd IAT Std, Fwd IAT Max, Packet Length Std, Avg Bwd Segment Size, Idle Mean, Idle Max, Label" bilgileridir.

Veri bölme %80 eğitim - %20 test yüzdelik oranı, 5-kat ve 10-kat çapraz doğrulama modeli olmak üzere 3 farklı metot kullanılmıştır. Makine öğrenme yöntemlerinden olan Naive Bayes, destek vektör makinesi, lojistik regresyon, k-en yakın komşu, karar ağacı (J48), AdaBoost, rastgele orman ve bagging üzerinde WEKA uygulaması üzerinde çalıştırılmıştır.

Sonuç olarak bu tez çalışmasında korelasyon özellik seçimi metodu kullanılarak makine öğrenme yöntemlerinden olan bagging ile 10-kat çapraz doğrulama tekniği, saldırının var olup olmadığına dair en iyi sonucu veren yöntem olarak ortaya çıkmıştır. İkinci ve üçüncü sırada aynı makine öğrenme yöntemi %80-%20 bölme yöntemi ve 5-kat çapraz doğrulama tekniği ile en iyi sonuçlara ulaşılmıştır.

Korelasyon özellik seçimine dayalı metodun kullanılması sonucunda elde edilen bilgiler Tablo 4.5'de sunulmuştur.

Tablo 4.5: Korelasyon özellik seçimine dayalı metodun sonuçları.

Sınıflandırıcı	Veri Bölme Yöntemi	Kesinlik	Duyarlılık	F-Ölçütü	Doğruluk (%)
Naive Bayes	%80 - %20	0,843	0,801	0,807	80,0803
	5-Kat	0,844	0,802	0,809	80,2026
	10-Kat	0,844	0,802	0,809	80,201
SVM	%80 - %20	0,871	0,860	0,848	86,0179
	5-Kat	0,874	0,861	0,850	86,1209
	10-Kat	0,877	0,863	0,853	86,292
Lojistik Regresyon	%80 - %20	0,851	0,847	0,837	84,6515
	5-Kat	0,853	0,848	0,839	84,7987
	10-Kat	0,853	0,848	0,839	84,8019
KNN	%80 - %20	0,971	0,970	0,971	97,05
	5-Kat	0,971	0,970	0,971	97,0397
	10-Kat	0,971	0,970	0,971	97,0464
AdaBoost	%80 - %20	0,890	0,857	0,844	85,6548
	5-Kat	0,891	0,857	0,845	85,7092
	10-Kat	0,891	0,857	0,845	85,7092
Karar Ağacı (J48)	%80 - %20	0,971	0,971	0,971	97,0579
	5-Kat	0,971	0,971	0,971	97,0563
	10-Kat	0,972	0,971	0,971	97,0641
Rastgele Orman	%80 - %20	0,972	0,971	0,971	97,0673
	5-Kat	0,972	0,971	0,971	97,0628
	10-Kat	0,972	0,971	0,971	97,0705
Bagging	%80 - %20	0,972	0,971	0,971	97,0796
	5-Kat	0,972	0,971	0,971	97,0774
	10-Kat	0,972	0,971	0,971	97,0823

4.3.4. Kazanç Oranı Tekniğinin Kullanılması

Bu tez çalışmasında, CIC-IDS2017 orijinal veri setinde WEKA uygulaması ile özellik seçimi yöntemlerinden birisi olan kazanç oranı (GainRatioAttributeEval) tekniği kullanılarak özellik seçimimyapılmış olup ilk 10 tanesi seçilmiştir. Özellik seçimi sonucunda elde edilen bilgiler, "Destination Port, Total Length of Bwd Packets, Fwd Packet Length Min, Bwd Packet Length Min, Bwd Packet Length Mean, Min Packet Length, Avg Bwd Segment Size, Subflow Bwd Bytes, Init_Win_bytes_forward, Init Win bytes backward, Label" bilgileridir.

Veri bölme %80 eğitim - %20 test yüzdelik oranı, 5-kat ve 10-kat çapraz doğrulama modeli olmak üzere 3 farklı metot kullanılmıştır. Makine öğrenme yöntemlerinden olan Naive Bayes, destek vektör makinesi, lojistik regresyon, k-en yakın komşu, karar ağacı (J48), AdaBoost, rastgele orman ve bagging üzerinde WEKA uygulaması üzerinde çalıştırılmıştır.

Sonuç olarak bu tez çalışmasında kazanç oranı özellik seçimi metodu kullanılarak makine öğrenme yöntemlerinden olan rastgele orman ile 10-kat çapraz doğrulama tekniği, saldırının var olup olmadığına dair en iyi sonucu veren yöntem olarak ortaya

çıkmıştır. İkinci sırada aynı makine öğrenme yöntemi ile 5-kat çapraz doğrulama tekniği ile üçüncü sırada ise bagging makine öğrenme yöntemi 10-kat çapraz doğrulama tekniği ile en iyi sonuçlara ulaşılmıştır

Kazanç oranı özellik seçimine dayalı metodun kullanılması sonucunda elde edilen bilgiler Tablo 4.6'da sunulmuştur.

Tablo 4.6: Kazanç oranı özellik seçimine dayalı metodun sonuçları.

Sınıflandırıcı	Veri Bölme Yöntemi	Kesinlik	Duyarlılık	F-Ölçütü	Doğruluk (%)
Naive Bayes	%80 - %20	0,948	0,792	0,853	79,2199
	5-Kat	0,949	0,811	0,866	81,0892
	10-Kat	0,949	0,801	0,860	80,1011
SVM	%80 - %20	0,937	0,926	0,663	92,6311
	5-Kat	0,733	0,926	0,656	92,6211
	10-Kat	0,934	0,927	0,657	92,7416
Lojistik Regresyon	%80 - %20	0,942	0,953	0,945	95,3415
	5-Kat	0,942	0,954	0,945	95,3884
	10-Kat	0,942	0,954	0,945	95,3811
KNN	%80 - %20	0,995	0,995	0,994	99,4666
	5-Kat	0,995	0,995	0,995	99,4802
	10-Kat	0,995	0,995	0,995	99,481
AdaBoost	%80 - %20	0,882	0,851	0,840	85,1228
	5-Kat	0,882	0,852	0,835	85,1636
	10-Kat	0,882	0,852	0,840	85,1636
Karar Ağacı (J48)	%80 - %20	0,995	0,995	0,994	99,4673
	5-Kat	0,995	0,995	0,995	99,4755
	10-Kat	0,995	0,995	0,995	99,4761
Rastgele Orman	%80 - %20	0,995	0,995	0,995	99,4738
	5-Kat	0,996	0,995	0,995	99,4861
	10-Kat	0,996	0,995	0,995	99,4871
Bagging	%80 - %20	0,995	0,995	0,994	99,4623
	5-Kat	0,995	0,995	0,995	99,4809
	10-Kat	0,995	0,995	0,995	99,4815

4.3.5. Bilgi Kazancı Tekniğinin Kullanılması

Bu tez çalışmasında, CIC-IDS2017 orijinal veri setinde WEKA uygulaması ile özellik seçimi yöntemlerinden birisi olan bilgi kazancı (InfoGainAttributeEval) tekniği kullanılarak özellik seçimi yapılmış olup ilk 10 tanesi seçilmiştir. Özellik seçimi sonucunda elde edilen bilgiler, "Flow Duration, Total Length of Bwd Packets, Bwd Packet Length Mean, Flow IAT Max, Max Packet Length, Packet Length Mean, Average Packet Size, Avg Bwd Segment Size, Subflow Bwd Bytes, Init_Win_bytes_forward, Label" bilgileridir.

Veri bölme %80 eğitim - %20 test yüzdelik oranı, 5-kat ve 10-kat çapraz doğrulama modeli olmak üzere 3 farklı metot kullanılmıştır. Makine öğrenme yöntemlerinden olan Naive Bayes, destek vektör makinesi, lojistik regresyon, k-en yakın komşu, karar ağacı (J48), AdaBoost, rastgele orman ve bagging üzerinde WEKA uygulaması üzerinde çalıştırılmıştır.

Sonuç olarak bu tez çalışmasında bilgi kazancı özellik seçimi metodu kullanılarak makine öğrenme yöntemlerinden olan bagging ile 10-kat çapraz doğrulama tekniği, saldırının var olup olmadığına dair en iyi sonucu veren yöntem olarak ortaya çıkmıştır. İkinci sırada aynı makine öğrenme yöntemi ile 5-kat çapraz doğrulama tekniği ile üçüncü sırada ise rastgele orman makine öğrenme yöntemi 10-kat çapraz doğrulama tekniği ile en iyi sonuçlara ulaşılmıştır.

Bilgi kazancı özellik seçimine dayalı metodun kullanılması sonucunda elde edilen bilgiler Tablo 4.7'de sunulmuştur.

Tablo 4.7: Bilgi kazancı özellik seçimine dayalı metodun sonuçları.

Sınıflandırıcı	Veri Bölme Yöntemi	Kesinlik	Duyarlılık	F-Ölçütü	Doğruluk (%)
Naive Bayes	%80 - %20	0,899	0,234	0,256	23,3743
	5-Kat	0,900	0,235	0,258	23,499
	10-Kat	0,900	0,236	0,259	23,5651
SVM	%80 - %20	0,941	0,852	0,824	85,2296
	5-Kat	0,919	0,853	0,803	85,3432
	10-Kat	0,919	0,853	0,804	85,3441
Lojistik Regresyon	%80 - %20	0,833	0,829	0,817	82,8715
	5-Kat	0,834	0,830	0,819	82,9738
	10-Kat	0,834	0,830	0,819	82,9803
KNN	%80 - %20	0,998	0,998	0,998	99,8232
	5-Kat	0,998	0,998	0,998	99,8256
	10-Kat	0,998	0,998	0,998	99,8286
AdaBoost	%80 - %20	0,882	0,851	0,840	85,1228
	5-Kat	0,882	0,852	0,840	85,1636
	10-Kat	0,882	0,852	0,840	85,1636
Karar Ağacı (J48)	%80 - %20	0,999	0,999	0,999	99,86
	5-Kat	0,999	0,999	0,999	99,875
	10-Kat	0,999	0,999	0,999	99,8735
Rastgele Orman	%80 - %20	0,999	0,999	0,999	99,8708
	5-Kat	0,999	0,999	0,999	99,8743
	10-Kat	0,999	0,999	0,999	99,875
Bagging	%80 - %20	0,999	0,999	0,999	99,8708
	5-Kat	0,999	0,999	0,999	99,8796
	10-Kat	0,999	0,999	0,999	99,8803

4.3.6. OneR Tekniğinin Kullanılması

Bu tez çalışmasında, CIC-IDS2017 orijinal veri setinde WEKA uygulaması ile özellik seçimi yöntemlerinden birisi olan OneR (OneRAttributeEval) tekniği kullanılarak özellik seçimi yapılmış olup ilk 10 tanesi seçilmiştir. Özellik seçimi sonucunda elde edilen bilgiler, "Destination Port, Flow Duration, Flow IAT Mean, Flow IAT Max, Fwd IAT Max, Fwd Packets/s, Max Packet Length, Packet Length Mean, Average Packet Size, Init_Win_bytes_forward, Label" bilgileridir.

Veri bölme %80 eğitim - %20 test yüzdelik oranı, 5-kat ve 10-kat çapraz doğrulama modeli olmak üzere 3 farklı metot kullanılmıştır. Makine öğrenme yöntemlerinden olan Naive Bayes, destek vektör makinesi, lojistik regresyon, k-en yakın komşu, karar ağacı (J48), AdaBoost, rastgele orman ve bagging üzerinde WEKA uygulaması üzerinde çalıştırılmıştır.

Sonuç olarak bu tez çalışmasında OneR özellik seçimi metodu kullanılarak makine öğrenme yöntemlerinden olan rastgele orman ile %80-%20 bölme yöntemi saldırının var olup olmadığına dair en iyi sonucu veren yöntem olarak ortaya çıkmıştır. İkinci ve üçüncü sırada aynı makine öğrenme yöntemi ile 10-kat ve 5-kat çapraz doğrulama tekniği ile en iyi sonuçlara ulaşılmıştır.

OneR özellik seçimine dayalı metodun kullanılması sonucunda elde edilen bilgiler Tablo 4.8'de sunulmuştur.

Tablo 4.8: OneR özellik seçimine dayalı metodun sonuçları.

Sınıflandırıcı	Veri Bölme Yöntemi	Kesinlik	Duyarlılık	F-Ölçütü	Doğruluk(%)
Naive Bayes	%80 - %20	0,962	0,846	0,893	84,6233
	5-Kat	0,963	0,847	0,894	84,6872
	10-Kat	0,963	0,847	0,893	84,6719
SVM	%80 - %20	0,915	0,920	0,861	91,9901
	5-Kat	0,916	0,920	0,860	92,0073
	10-Kat	0,915	0,920	0,859	92,0041
Lojistik Regresyon	%80 - %20	0,924	0,924	0,921	92,416
	5-Kat	0,925	0,925	0,922	92,5034
	10-Kat	0,925	0,925	0,922	92,4978
KNN	%80 - %20	0,999	0,999	0,999	99,9285
	5-Kat	0,999	0,999	0,999	99,9153
	10-Kat	0,999	0,999	0,999	99,9174
AdaBoost	%80 - %20	0,867	0,843	0,830	84,2819
	5-Kat	0,868	0,844	0,831	84,3523
	10-Kat	0,868	0,844	0,831	84,3523
Karar Ağacı (J48)	%80 - %20	0,999	0,999	0,999	99,9365
	5-Kat	0,999	0,999	0,999	99,941
	10-Kat	0,999	0,999	0,999	99,9423
Rastgele Orman	%80 - %20	1,000	1,000	1,000	99,9617
	5-Kat	1,000	1,000	1,000	99,9577
	10-Kat	1,000	1,000	1,000	99,959
Bagging	%80 - %20	0,999	0,999	0,999	99,948
	5-Kat	0,999	0,999	0,999	99,9434
	10-Kat	0,999	0,999	0,999	99,9453

4.3.7. Simetrik Belirsizlik Tekniğinin Kullanılması

Bu tez çalışmasında, CIC-IDS2017 orijinal veri setinde WEKA uygulaması ile özellik seçimi yöntemlerinden birisi olan Simetrik Belirsizlik (Symmetrical Uncert Attribute Eval) tekniği kullanılarak özellik seçimi yapılmış olup ilk 10 tanesi seçilmiştir. Özellik seçimi sonucunda elde edilen bilgiler, "Destination Port, Total Length of Bwd Packets, Bwd Packet Length Max, Bwd Packet Length Mean, Min Packet Length, Max Packet Length, Avg Bwd Segment Size, Subflow Bwd Bytes, Init_Win_bytes_forward, Init_Win_bytes_backward, Label" bilgileridir.

Veri bölme %80 eğitim - %20 test yüzdelik oranı, 5-kat ve 10-kat çapraz doğrulama modeli olmak üzere 3 farklı metot kullanılmıştır. Makine öğrenme yöntemlerinden olan Naive Bayes, destek vektör makinesi, lojistik regresyon, k-en yakın komşu, karar ağacı (J48), AdaBoost, rastgele orman ve bagging üzerinde WEKA uygulaması üzerinde çalıştırılmıştır.

Sonuç olarak bu tez çalışmasında simetrik belirsizlik özellik seçimi metodu kullanılarak makine öğrenme yöntemlerinden olan rastgele orman 10-kat çapraz doğrulama tekniği ile saldırının var olup olmadığına dair en iyi sonucu veren yöntem olarak ortaya çıkmıştır. İkinci sırada aynı makine öğrenme yöntemi ile 5-kat çapraz doğrulama tekniği ile üçüncü sırada ise bagging 10-kat çapraz doğrulama tekniği ile en iyi sonuçlara ulaşılmıştır.

Simetrik belirsizlik özellik seçimine dayalı metodun kullanılması sonucunda elde edilen bilgiler Tablo 4.9'da sunulmuştur.

Tablo 4.9: Simetrik belirsizlik özellik seçimine dayalı metodun sonuçları.

Sınıflandırıcı	Veri Bölme Yöntemi	Kesinlik	Duyarlılık	F-Ölçütü	Doğruluk (%)
Naive Bayes	%80 - %20	0,947	0,791	0,852	79,0863
	5-Kat	0,949	0,791	0,853	79,1355
	10-Kat	0,949	0,791	0,853	79,1328
SVM	%80 - %20	0,803	0,928	0,641	92,8303
	5-Kat	0,746	0,928	0,636	92,8011
	10-Kat	0,743	0,929	0,636	92,9101
Lojistik Regresyon	%80 - %20	0,940	0,953	0,944	95,2678
	5-Kat	0,939	0,953	0,944	95,2521
	10-Kat	0,939	0,953	0,944	95,2519
KNN	%80 - %20	0,997	0,996	0,996	99,6247
	5-Kat	0,997	0,996	0,996	99,646
	10-Kat	0,997	0,996	0,996	99,6482
AdaBoost	%80 - %20	0,882	0,851	0,840	85,1228
	5-Kat	0,882	0,852	0,840	85,1636
	10-Kat	0,882	0,852	0,835	85,1636
Karar Ağacı (J48)	%80 - %20	0,997	0,996	0,996	99,6312
	5-Kat	0,997	0,997	0,996	99,6501
	10-Kat	0,997	0,997	0,996	99,6524
Rastgele Orman	%80 - %20	0,997	0,996	0,996	99,6398
	5-Kat	0,997	0,997	0,997	99,6586
	10-Kat	0,997	0,997	0,997	99,6605
Bagging	%80 - %20	0,997	0,996	0,996	99,6297
	5-Kat	0,997	0,997	0,996	99,6521
	10-Kat	0,997	0,997	0,996	99,6524

5. SONUÇ

Bu tez çalışması için yapılan literatür taramasında, son yıllarda siber saldırıların sayısında ve çeşitliliğinde önemli bir artış olduğu görülmüştür. Bu nedenle siber ataklar üzerinde çalışmalar yapılmaya devam edilmektedir. Araştırmalarda siber saldırıların daha çok kritik alt yapılar, devlet kurumları ve kurumsal işletmelerin bilgisayar ağlarına karşı yapıldığı görülmüştür. Bu siber saldırıları, ağlara ciddi zararlar vermeden önce tespit etmek çok önemlidir. Bu amaçla siber güvenlik araştırmacıları ve profesyonelleri tarafından gerçek zamanlı savunma araçlarından olan IDS ve IPS sistemleri geliştirilmektedir.

Günümüzde siber güvenlik, toplumda önemli bir endişe kaynağı olmuştur. Devlet kurumları ve kurumsal işletmelere ait bilgiler, hayati derecede önemli olmasından dolayı güvenli bir şekilde muhafaza edilmelidir. Saldırganlar tarafından güvenlik ihlali yapılma riski her zaman olduğundan bu bilgileri muhafaza etmek zordur. Bu riski ortadan kaldırmak için araştırmacılar, kendilerini siber saldırganların yerine koyarak onlar gibi düşünüp önlemler geliştirmek dâhil pek çok çalışma yürütmektedirler. Araştırmacılar, çalışmalarında siber güvenliğin temelini oluşturan üç ilkeyi (gizlilik, bütünlük ve erişilebilirlik) etkin bir şekilde uygulamaya özen göstererek çalışmalarına devam etmektedirler.

Bu tez çalışmasında, CIC-IDS2017 veri setinde ağ güvenliği ve izinsiz giriş tespiti için kullanılan saldırı senaryolarına yer verilmiştir.

İkinci bölümde, genel kısımlar başlığı altında saldırı tespit sistemleri ve saldırı önleme sistemleri ele alınmıştır. Saldırganların amaçları ile kötü amaçlı yazılımların belirtileri incelenmiş; ağ ortamında gerçekleşen saldırı türleri (hizmet reddi saldırısı, dağıtık hizmet reddi saldırısı, botnet saldırısı, kaba kuvvet saldırısı, port tarama saldırısı, web uygulama saldırısı ve sızma saldırısı) hakkında detaylı bir inceleme yapılarak örnek senaryolar ile anlatılmıştır.

Üçüncü bölümde, kapsamlı bir literatür çalışmalarından sonra ulaşılan CIC-IDS2017 veri seti ile ilgili detaylı bir incelemeye yer verilmiştir. Günümüzde yaygın olarak

kullanılan makine öğrenme yöntemlerinden olan Naive Bayes, destek vektör makinesi, lojistik regresyon, k-en yakın komşu, karar ağacı (J48), AdaBoost, rastgele orman ve bagging algoritmaları incelenmiştir. Veri madenciliğinde yaygın olarak kullanılan WEKA uygulaması kısaca tanımlanmış ve WEKA uygulamasının kullanıldığı bilgisayarın teknik özelliklerine yer verilmiştir. Daha sonra CIC-IDS2017 veri seti üzerinde farklı yöntemler ile kullanılan akış diyagramları gösterilmiştir. İlk olarak, orijinal veri setinde hiçbir değişiklik yapılmadan; ikinci olarak, temel bileşen analizi yöntemi kullanılarak özellik çıkarımı yapılarak; üçüncü olarak ise WEKA üzerinde yaygın olarak kullanılan özellik seçimi yöntemlerinden yedi tanesine yer verilmiştir. Bu üç ana yöntemin hepsinde %80 eğitim-%20 test yüzdelik oranı ve 5-kat veya 10-kat çapraz doğrulama modeli olmak üzere 3 farklı metot kullanılmıştır. Bu metotlar Naive Bayes, destek vektör makinesi, lojistik regresyon, k-en yakın komşu, karar ağacı (J48), AdaBoost, rastgele orman ve bagging makine öğrenme yöntemleriyle saldırının olup olmadığını gösteren akış diyagramları sunulmuştur.

Dördüncü bölümde ise yukarıda bahsedilen üç ana yöntemin hepsinde %80 eğitim-%20 test yüzdelik oranı ve 5-kat veya 10-kat çapraz doğrulama modeli olmak üzere 3 farklı metot kullanılmıştır. Bu metotlar Naive Bayes, destek vektör makinesi, lojistik regresyon, k-en yakın komşu, karar ağacı (J48), AdaBoost, rastgele orman ve bagging makine öğrenme yöntemleri sonucunda ulaşılan sonuçlar tablolarda sunulmuştur. Bu tablolarda, yaygın olarak kullanılan makine öğrenme metriklerinden olan kesinlik, duyarlılık, F-Ölçütü ve doğruluk değerlerinin hepsine yer verilmiştir. Sonuç olarak CIC-IDS2017 veri seti Çarşamba günü DoS saldırıları sonucunda elde edilen verilerden WEKA uygulaması üzerinde OneR (OneRAttributeEval) özellik seçiminin en iyi yöntem olduğu ortaya çıkmıştır. Özellik seçimi sonucunda elde edilen bilgiler, "Destination Port, Flow Duration, Flow IAT Mean, Flow IAT Max, Fwd IAT Max, Fwd Packets/s, Max Packet Length, Packet Length Mean, Average Packet Size, Init_Win_bytes_forward, Label" bilgileridir.

Bu tez çalışmasında, makine öğrenme yöntemlerinden olan rastgele orman %80-%20 bölme yöntemi kullanarak saldırının var olup olmadığını doğruluk değeri 99,9614 ile en iyi sonucu veren en iyi yöntem olarak ortaya çıkmıştır. İkinci ve üçüncü sırada ise aynı makine öğrenme yöntemi ile 10-kat çapraz doğrulama ile doğruluk değeri 99,9590'a ve 5-kat çapraz doğrulama ile doğruluk değeri 99,9577 tekniği ile en iyi sonuçlara ulaşılmıştır.

Bu tez çalışması sonucunda elde edilen en iyi sonuçlar Tablo 5.1'de sunulmuştur.

Tablo 5.1: Tez kapsamında elde edilen en iyi sonuçlar (OneR özellik seçimi yöntemi).

Sınıflandırıcı	Veri Bölme Yöntemi	Kesinlik	Duyarlılık	F-Ölçütü	Doğruluk (%)
Rastgele Orman	%80 - %20	1,000	1,000	1,000	99,9617
	5-Kat	1,000	1,000	1,000	99,9577
	10-Kat	1,000	1,000	1,000	99,959

Bu tez çalışması kapsamında, CIC-IDS2017 veri seti Çarşamba günü DoS saldırıları kullanılarak, farklı makine öğrenme yöntemleri kullanılarak başarılı bir IDS geliştirilebileceği öngörülmüştür. Geliştirilen IDS modelinin kesinlik, duyarlılık, F-Ölçütü, doğruluk değerleri ve performansların artırılması için veri madenciliğinde kullanılan farklı algoritmaların da kullanılabileceği görülmüştür.

Bu tezin devamında, CIC-IDS2017 veri seti içerisinde yer alan DDoS, botnet, kaba kuvvet, port tarama, web uygulama ve sızma saldırıları için de aynı makine öğrenme yöntemleri kullanılarak ve aynı bölümleme teknikleri ile aynı özellik seçimleri yapılarak alınan sonuçların değerlendirilmesi yapılacaktır.

6. KAYNAKÇA

Ahmad, R., & Alsmadi, I. (2021). Machine learning approaches to IoT security: A systematic literature review. Internet of Things, 14, 100365.

Ahmad, T., Truscan, D., Vain, J., & Porres, I. (2022, April). Early detection of network attacks using deep learning. In *2022 IEEE International Conference on Software Testing, Verification and Validation Workshops* (ICSTW) (pp. 30-39). IEEE.

Ajayi, O., Gangopadhyay, A., Erbacher, R. F., & Bursat, C. (2022). Developing Cross-Domain Host-Based Intrusion Detection. *Electronics, 11*(21): 3631.

Akgun, D., Hizal, S., & Cavusoglu, U. (2022). A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. *Computers & Security, 118*: 102748.

Albelwi, S. A. (2022, January). An Intrusion Detection System for Identifying Simultaneous Attacks using Multi-Task Learning and Deep Learning. In *2022 2nd International Conference on Computing and Information Technology* (ICCIT) (pp. 349-353). IEEE.

Al-Fawa'reh, M., Al-Fayoumi, M., Nashwan, S., & Fraihat, S. (2022). Cyber threat intelligence using PCA-DNN model to detect abnormal network behavior. *Egyptian Informatics Journal, 23*(2): 173-185.

Alhabshy, A. A., Hameed, B. I., & Eldahshan, K. A. (2022). An Ameliorated Multiattack Network Anomaly Detection in Distributed Big Data System-Based Enhanced Stacking Multiple Binary Classifiers. *IEEE Access, 10*: 52724-52743.

Bhargav, R., Jain, V., & Verma, M. (2022, April). A DDoS Attack Detection on Cloud Framework Using Improved Features Based Machine Learning Approach. In *2022 Second International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies* (ICAECT) (pp. 1-6). IEEE.

Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2013). Network anomaly detection: methods, systems and tools. *IEEE communications surveys & tutorials, 16*(1): 303-336.

Butun, I., Morgera, S. D., & Sankar, R. (2013). A survey of intrusion detection systems in wireless sensor networks. *IEEE communications surveys & tutorials, 16*(1): 266-282.

Canadian Institute for Cybersecurity (2018). Intrusion Detection Evaluation Dataset (CIC-IDS2017). Alındığı yer: https://www.unb.ca/cic/datasets/ids-2017.html

Cisco Ağ Akademisi (t.y.). CCNA1 CCNAv7: Introduction to Networks. Alındığı yer: https://contenthub.netacad.com/itn/16.1.1

Creech, G., & Hu, J. (2013). A semantic approach to host-based intrusion detection systems using contiguousand discontiguous system call patterns. *IEEE Transactions on Computers, 63*(4): 807-819

Crespo-Martínez, I. S., Campazas-Vega, A., Guerrero-Higueras, Á. M., Riego-DelCastillo, V., Álvarez-Aparicio, C., & Fernández-Llamas, C. (2023). SQL injection attack detection in network flow data. *Computers & Security, 127*: 103093.

Dang, X., & Li, Z. (2022, May). Network Intrusion detection approach based on convolutional neural network. In *2022 4th International Conference on Communications, Information System and Computer Engineering* (CISCE) (pp. 247-251). IEEE.

Das, S., Saha, S., Priyoti, A. T., Roy, E. K., Sheldon, F. T., Haque, A., & Shiva, S. (2021). Network intrusion detection and comparative analysis using ensemble machine learning and feature selection. *IEEE Transactions on Network and Service Management.*

Gosai, K., Mehta, H., & Katkar, V. (2022, March). An Intrusion Detection Using Ensemble Classifiers. In *2022 6th International Conference on Computing Methodologies and Communication* (ICCMC) (pp. 163-168). IEEE.

Gupta, S., Singhal, A., & Kapoor, A. (2016, April). A literature survey on social engineering attacks: Phishing attack. In *2016 international conference on computing, communication and automation* (ICCCA) (pp. 537-540). IEEE.

Hai, T. H., & Nam, L. H. (2021, June). A practical comparison of deep learning methods for network intrusion detection. In *2021 International Conference on Electrical, Communication, and Computer Engineering* (ICECCE) (pp. 1-6). IEEE.

Han, J., Kamber, M., & Pei, J. (2012). *Data mining, concepts and techniques* (Third edition). Morgan Kaufmann Publishers (Elsevier*)*.

Hashemi, M. J., Keller, E., & Tizpaz-Niari, S. (2022). Detecting Unseen Anomalies in Network Systems by Leveraging Neural Networks. *IEEE Transactions on Network and Service Management*.

https://owasp.org

Ihekoronye, V. U., Ajakwe, S. O., Kim, D. S., & Lee, J. M. (2022, October). Cyber Edge Intelligent Intrusion Detection Framework For UAV Network Ba2ed on Random Forest Algorithm. In *2022 13th International Conference on Information and Communication Technology Convergence* (ICTC) (pp. 1242-1247). IEEE.

Jacob, S., Qiao, Y., Ye, Y., & Lee, B. (2022). Anomalous distributed traffic: Detecting cyber security attacks amongst microservices using graph convolutional networks. *Computers & Security*, *118*: 102728.

James, F. (2019, October). IoT cybersecurity based smart home intrusion prevention system. In *2019 3rd Cyber Security in Networking Conference* (CSNet) (pp. 107-113). IEEE.

Kasim, Ö. (2021). An ensemble classification-based approach to detect attack level of SQL injections. *Journal of Information Security and Applications*, *59*: 102852.

Katherasala, S. K., Manvith, V. S., Therala, A., & Murala, M. (2022, February). NetMD-Network Traffic Analysis and Malware Detection. In *2022 International Conference on Artificial Intelligence in Information and Communication* (ICAIIC) (pp. 011-016). IEEE.

Kaur, G., Lashkari, A. H., & Rahali, A. (2020, August). Intrusion traffic detection and characterization using deep image learning. In *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress* (DASC/PiCom/CBDCom/CyberSciTech) (pp. 55-62). IEEE.

Khraisat, A., Gondal, I., & Vamplew, P. (2018). An anomaly intrusion detection system using C5 decision tree classifier. In *Trends and Applications in Knowledge Discovery and Data Mining: PAKDD 2018 Workshops, BDASC, BDM, ML4Cyber, PAISI, DaMEMO*, Melbourne, VIC, Australia, June 3, 2018, Revised Selected Papers 22 (pp. 149-155). Springer International Publishing.

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, *2*(1): 1-22.

Kilincer, I. F., Tuncer, T., Ertam, F., & Sengur, A. (2023). SPA-IDS: An intelligent intrusion detection system based on vertical mode decomposition and iterative feature selection in computer networks. *Microprocessors and Microsystems*, *96*: 104752.

Kumari, P., & Jain, A. K. (2023). A Comprehensive Study of DDoS Attacks over IoT Network and Their Countermeasures. *Computers & Security*, 103096.

Leung, T. C., & Lee, C. N. (2022, November). Flow-Based DDoS Detection Using Deep Neural Network with Radial Basis Function Neural Network. In *2022 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference* (APSIPA ASC) (pp. 1774-1779). IEEE.

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. *Journal of network and computer applications*, *36*(1): 42-57.

Nguyen, T. L., Nguyen, X. H., & Le, K. H. (2022, December). Enhancing Explainability of Machine Learning-based Intrusion Detection Systems. In *2022 RIVF International Conference on Computing and Communication Technologies* (RIVF) (pp. 606-611). IEEE.

Rumsey, M. J. (2016). *Cybersecurity: Challenging rhetoric to identify the future of defensive and offensive measures against defined threat actors* (Doctoral dissertation). San Diego State University.

Salamatian, S., Huleihel, W., Beirami, A., Cohen, A., & Médard, M. (2019). Why botnets work: Distributed brute-force attacks need no synchronization. *IEEE Transactions on Information Forensics and Security*, *14*(9): 2288-2299.

Schuartz, F. C., Fonseca, M., & Munaretto, A. (2022, October). A Distributed Platform for Intrusion Detection System Using Data Stream Mining in a Big Data Environment. In *2022 6th Cyber Security in Networking Conference* (CSNet) (pp. 1-7). IEEE.

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSp, 1*: 108-116.

Singh, A. P., & Singh, M. D. (2014). Analysis of host-based and network-based intrusion detection system. *International Journal of Computer Network and Information Security, 6*(8): 41-47.

Singh, K. J., Thongam, K., & De, T. (2018). Detection and differentiation of application layer DDoS attack from flash events using fuzzy-GA computation. *IET Information Security, 12*(6): 502-512.

Singh, R., & Deorari, R. (2022, October). Enhancing Collaborative Intrusion detection networks against insider attack using supervised learning technique. In *2022 IEEE 2nd Mysore Sub Section International Conference* (MysuruCon) (pp. 1-6). IEEE.15

Tams, B., Mihăilescu, P., & Munk, A. (2015). Security considerations in minutiae-based fuzzy vaults. *IEEE Transactions on Information Forensics and Security, 1*0(5): 985-998.

Taner, C. (2019). *Herkes için siber güvenlik.* Abaküs Kitap.

Tariq, I., Sindhu, M. A., Abbasi, R. A., Khattak, A. S., Maqbool, O., & Siddiqui, G. F. (2021). Resolving cross-site scripting attacks through genetic algorithm and reinforcement learning. *Expert Systems with Applications, 168*: 114386.

Toklu, S., & Şimşek, M. (2018). Two-layer approach for mixed high-rate and low-rate distributed denial of service (DDoS) attack detection and filtering. *Arabian Journal for Science and Engineering, 43*(12): 7923-7931.

Vishwakarma, M., & Kesswani, N. (2022). DIDS: A Deep Neural Network based real-time Intrusion detection system for IoT. *Decision Analytics Journal, 5*:100142.

Wu, Z., Zhang, H., Wang, P., & Sun, Z. (2022). RTIDS: A robust transformer-based approach for intrusion detection system. *IEEE Access*, *10*: 64375-64387.

Yang, Y., & Liu, D. (2022, October). mKDNAD: A network flow anomaly detection method based on multi-teacher knowledge distillation. In *2022 16th IEEE International Conference on Signal Processing* (ICSP) (Vol. 1, pp. 314-319). IEEE.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı : KILINÇ, Fırat
Uyruğu : T.C.

Eğitim

Derece	Üniversite ve Bölüm	Mezuniyet Tarihi
Lisans	Hoca Ahmet Yesevi Uluslararası Uluslararası Türk–Kazak Üniversitesi Bilgisayar ve Öğretim Teknolojileri Öğretmenliği	23.06.2015

Yabancı Dil

İngilizce

Tezden Türetilen Yayınlar

Makale (Yayım aşamasında)

Kılınç, F. & Eyüpoğlu, C. (2023). Ağ Ortamındaki Saldırı Türleri: Saldırı Senaryo Örnekleri. *İstanbul Ticaret Üniversitesi Teknoloji ve Uygulamalı Bilimler Dergisi.*