T.C.
DÜZCE ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

SALDIRI TESPİTİNDE MAKİNE ÖĞRENMESİ VE ÖZELLİK SEÇİMİNİN PERFORMANSA ETKİSİ

YASİN TÜRKYILMAZ

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

DANIŞMAN
DR. ÖĞR. ÜYESİ ARAFAT ŞENTÜRK

DÜZCE, 2021

T.C.
DÜZCE ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

SALDIRI TESPİTİNDE MAKİNE ÖĞRENMESİ VE ÖZELLİK SEÇİMİNİN PERFORMANSA ETKİSİ

Yasin TÜRKYILMAZ tarafından hazırlanan tez çalışması aşağıdaki jüri tarafından Düzce Üniversitesi Lisansüstü Eğitim Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Dr. Öğr. Üyesi Arafat ŞENTÜRK

Düzce Üniversitesi

Jüri Üyeleri

Dr. Öğr. Üyesi Arafat ŞENTÜRK
Düzce Üniversitesi _____

Doç. Dr. Devrim AKGÜN
Sakarya Üniversitesi _____

Dr. Öğr. Üyesi Enver KÜÇÜKKÜLAHLI
Düzce Üniversitesi _____

Tez Savunma Tarihi: 10/12/2021

BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar bütün aşamalarda etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve etik kurallar içinde elde ettiğimi, bu tez çalışmasıyla elde edilmeyen bütün bilgi ve yorumlara kaynak gösterdiğimi ve bu kaynakları da kaynaklar listesine aldığımı, yine bu tezin çalışılması ve yazımı sırasında patent ve telif haklarını ihlal edici bir davranışımın olmadığını beyan ederim.

10 Aralık 2021

Yasin TÜRKYILMAZ

TEŞEKKÜR

Yüksek lisans öğrenimimde ve bu tezin hazırlanmasında gösterdiği her türlü destek ve yardımdan dolayı çok değerli hocam Dr. Öğr. Üyesi. Arafat ŞENTÜRK'e en içten dileklerimle teşekkür ederim.

Bu çalışma boyunca yardımlarını ve desteklerini esirgemeyen sevgili eşim Hayrunnisa'ya, kızım Hafsa'ya, babama, anneme ve kardeşlerime sonsuz teşekkürlerimi sunarım.

10 Aralık 2021 **Yasin TÜRKYILMAZ**

İÇİNDEKİLER

Sayfa No

ŞEKİL LİSTESİ

Sayfa No

ÇİZELGE LİSTESİ

Sayfa No

KISALTMALAR

AÖM	Aşırı öğrenim makinesi
ASTS	Anomali tabanlı saldırı tespit sistemleri
DoS	Denial of service
DVM	Destek vektör makineleri
IDS	Intrusion detection systems
İSTS	İmza tabanlı saldırı tespit sistemleri
KAA	Kablosuz algılayıcı ağlar
KNN	K-En yakın komşu
MÖ	Makine öğrenmesi
NB	Naive bayes
Nİ	Nesnelerin interneti
ÖS	Özellik seçimi
RO	Rassal orman
SA	Sinir ağları
STS	Saldırı tespit sistemleri
TÖ	Topluluk öğrenimi
YSA	Yapay sinir ağı

ÖZET

SALDIRI TESPİTİNDE MAKİNE ÖĞRENMESİ VE ÖZELLİK SEÇİMİNİN PERFORMANSA ETKİSİ

Yasin TÜRKYILMAZ
Düzce Üniversitesi
Lisansüstü Eğitim Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı
Yüksek Lisans Tezi
Danışman: Dr. Öğr. Üyesi Arafat ŞENTÜRK
Aralık 2021, 48 sayfa

İnternete olan ilgi son yıllarda artmış ve artmaya devam etmektedir. Bu artışa birde salgın hastalık koşulları eklenince insan, hayatını etkileyen her şeyi internet vasıtasıyla yapmaya odaklanılmıştır. İnternete olan ilginin artmasıyla birlikte, internet üzerinden gerçekleştirilen saldırı sayılarındaki ve suç ifa edebilecek olan durumdaki faaliyetler de artmış ve istikrarlı şekilde artmaya devam etmektedir. Bu sebepten, organizasyonların ağ güvenliğini sağlaması çok daha zor hale gelmektedir. Saldırı ve suçlulara karşı ağ güvenliğini sağlamak için birçok farklı güvenlik sistemi kullanılmaktadır. Saldırı Tespit Sistemleri (STS) ağ güvenliği için kullanılan güvenlik sistemlerinden bir tanesidir. Son yıllarda araştırmacılar daha verimli ve etkin bir STS ortaya koymak için birçok çalışma gerçekleştirmişlerdir. Yapılan çalışmalarda kıyaslama veri seti olarak kullanılan veri setlerinin artan ağ trafiğinden dolayı günümüz şartlarına uygun olmadığı ve değerlendirmelerde doğru sonuçları vermediği görülmüştür. Bu soruna çözüm olması için 2015 yılında yayınlanan UNSW-NB15 veri seti oluşturulmuştur. UNSW-NB15 veri seti ReliefF puanlama yöntemi kullanılarak özellik seçimine tabi tutulmuştur. Orijinal halinde 42 olan özellik sayısı 29'a düşürülmüştür. Bu tez çalışmanın amacı STS'yi daha verimli ve etkin hale getirmek için kullanılan makine öğrenmesi yöntemlerini UNSW-NB15 veri seti kullanılarak dört farklı senaryoda performanslarını incelemek ve karşılaştırmaktır. Tez çalışması kapsamında, yeni kıyaslama veri seti olarak literatürde yerini alan UNSW-NB15 veri seti için Orange benzetim aracı kullanılarak makine öğrenmesi yöntemlerinin performansları karşılaştırılmıştır. Gerçekleştirilen benzetimler sonucunda, elde edilen değerler ile daha önce yapılmış çalışmalar karşılaştırılarak performans değerlendirmesi yapılmıştır. Sonuçlara göre özellik seçiminin yapılması test veri setinin bağımsız oluşturulduğu senaryolarda doğruluk performansını arttırmıştır. Özellik Seçimi (ÖS) uygulanarak elde edilen sonuçlardan en yüksek doğruluk oranına "Rassal Orman" yöntemi ulaşmıştır.

Anahtar sözcükler: Makine Öğrenmesi, Saldırı Tespit Sistemleri, UNSW-NB15.

ABSTRACT

THE EFFECT OF MACHINE LEARNING AND FEATURE SELECTION ON PERFORMANCE IN ATTACK DETECTION

Yasin TÜRKYILMAZ
Düzce University
Institue of Graduate Studies, Department of Computer Engineering
Master's Thesis
Supervisor: Assist. Prof. Dr. Arafat ŞENTÜRK
December 2021, 48 pages

Interest in the Internet has grown tremendously in recent years and increasing continuously. When epidemic disease conditions are added to this increase, it is focused on doing everything that affects human life via the internet. Just as the interest in the Internet has increased, the number of people who want to abuse this interest has also increased in the number of attacks carried out over the Internet and in activities capable of committing crimes, and it has continued to increase steadily. It has become much more difficult for organizations to maintain network security. Many different security systems are used to provide network security against attacks and criminals. Intrusion Detection Systems (IDS) is one of the security systems used for network security. IDS is also a subject of great interest in the academic world. In recent years, researchers have done many studies to reveal a more efficient and effective IDS. In the studies, it has been seen that the data sets used as the benchmark data set do not meet today's conditions and do not give the correct results in the evaluations. The UNSW-NB15 dataset, published in 2015, was created to solve this problem. The aim of this study is to examine and compare the machine learning methods used to make IDS more efficient and effective using the UNSW-NB15 data set. Within the scope of the study, the performances of machine learning methods were compared using the Orange tool for the UNSW-NB15 dataset, which took its place in the literature as a new benchmark dataset. In addition, performance evaluation was made with the results obtained and previous studies. Feature selection according to the results increased the accuracy performance in scenarios where the test data set was created independently. The "Random Forest" method reached the highest accuracy rate among the results obtained by applying Feature Selection (PS).

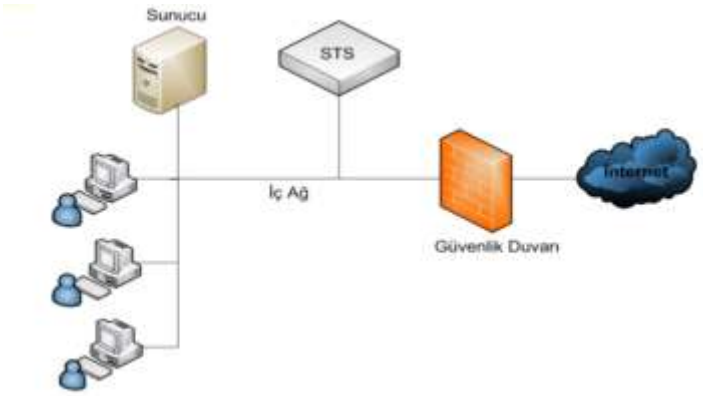
Keywords: Intrusion Detection System, Machine Learning, UNSW-NB15.

1. GİRİŞ

1.1. GİRİŞ

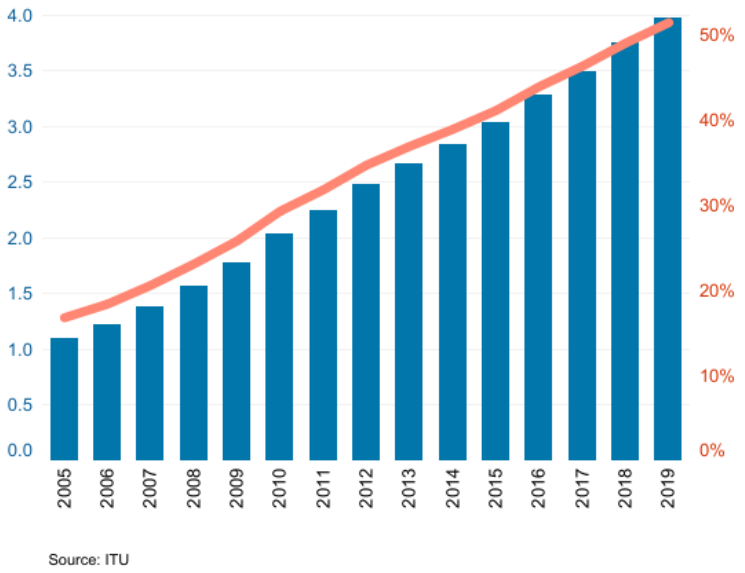
İnternet, uygun internet protokolü (TCP/IP) kullanarak, cihazları küresel bir şekilde bağlayan bilgisayar ağlarının birbiriyle bağlı olduğu evrensel bir sistemdir [1]. İnternetin sağladığı en büyük avantaj bütün dünyanın bağlı olduğu ağ olma özelliğidir. Fakat bu özellik aynı zamanda güvenlik zafiyeti oluşturmaktadır. İnternet ağında var olan hiçbir veri gerekli önlemler alınmadığı takdirde güvende değildir. Bu duruma ek olarak internet ağı ile bağlantılı olan hiçbir ağ da gerekli güvenlik önlemleri alınmadığı taktirde güvenli sayılmaz [2].

İnternetin keşfinden sonra toplumların iletişim yapısı çok büyük bir değişime uğrayarak gelişmiştir. İki önemli güç olan iletişim ve bilişim, internet üzerinde buluşmuştur. Bu durum da kaçınılmaz olarak çok büyük ilgi görmüştür. Günümüzde iletişim ve haberleşme çok büyük oranda internet üzerinden gerçekleşmektedir. Sosyal medya, ana akım medyayı yakalamış ve neredeyse geçmiş vaziyettedir. Bu duruma ek olarak elektronik ticaret ve para transferleri gibi finansal konular eklenince internet ağı üzerinden hizmet alan veren veya internet ağına bir şekilde temas eden bütün ağlarda güvenlik tedbirlerinin alınması kaçınılmaz olmuştur. Nesnelerin İnterneti (Nİ) gömülü cihazları, bilgisayarları ve algılayıcıları kablolu veya kablosuz ağ vasıtasıyla internete bağlayan bir iletişim ağıdır [1]. Milyarlarca sayılara ulaşan Nİ cihazları izlenebilir ve kontrol edilebilirdir yapıya sahiptir. Cihazlar kendi aralarında iletişime veya etkileşime geçerek veri alışverişi yapabilirler. Nİ cihazlarını akıllı telefonlar, ev güvenliği (kamera vb.) cihazları, akıllı televizyon vb. cihazlar olarak örneklendirilebilir [3]. 1995 yılında dünya nüfusunun sadece %0.4 internete erişebilirken 2020 yılında bu oran %53' e ulaşmıştır [4]. Şekil 1.1 de normal bir ağ topolojisi gösterilmiştir. Şekil 1.2 de ise yıllara göre dünya nüfusunun internete olan erişim oranları ve sayısını gösterilmiştir. 21.yy 'da en önemli teknolojik gelişmeyi internetin sağladığı düşünülmektedir.



Şekil 1.1. STS'nin ağ topolojisindeki konumlandırılması.

İnternet teknolojisinin bu kadar büyümesinin olumsuz yönleri de ortaya çıkmıştır. Bunlardan en önemlileri arasında güvenlik problemleri vardır. Günümüzde, mahrem verileri saldırganlara karşı güvende tutmak gittikçe zorlaşan bir görev haline gelmektedir. Güvenlik Duvarı (Firewall) ve virüs önler programlar (anti-virus) gibi geleneksel güvenlik önlemleri tüm atak tiplerine karşı yeterli değildir. Ayrıca alan bazlı (zone-based) Firewall gibi geleneksel güvenlik önlemlerini kullanırken güvenli ve güvensiz bölgeler oluşturulmaktadır. Bir erişim isteği güvenli olmayan bölgeden geliyorsa o isteğe detaylı bir güvenlik taraması uygulanırken, eğer o istek güvenli bölgeden geliyorsa, o isteğe detaylı güvenlik tedbirleri uygulanmaz ve güvenli olmayan bölgeye kıyasla daha kolay şekilde istediği yere erişme imkânı tanınır. Yaşadığımız güvenlik problemlerinin çoğu da güvenli bölge olarak adlandırdığımız iç taraftan gelebilecek olan saldırılardır. Bu nedenle geleneksel güvenlik önlemlerinin yanına ek güvenlik önlemleri gerekmektedir. Saldırı Tespit Sistemleri (STS) ek güvenlik önlemleri açısından önemli bir rol oynamaktadır. STS hedef sistemdeki, ister dışarıda ister de içeride meydana gelmiş olan normal olmayan veya yetkilendirilmemiş aktiviteleri tespit eden, tanımlayan ve cevap veren fonksiyonlara sahip bir yazılım veya donanımdır [5]. STS'ler geleneksel güvenlik çözümlerinden farklı olarak hem dışarıdan gelebilecek hem de içeriden gelebilecek saldırılara karşı her zaman teyakkuzdadır. STS ağ trafiği verilerini dikkatli şekilde takip eder ve verilerin normal mi yoksa saldırı mı olduğuna karar verir [6].



Şekil 1.2. Dünya nüfusunun yıllara sarih internete erişim oranı [8].

Zararlı yazılım (malicious) aktivitelerini tespit ederken ağ trafiğini izleyebilmek için STS kullanılır. STS Güvenlik Duvarını geçen veya aşan saldırıları normal bir ağ trafiği davranışı dışında olarak değerlendirip kolayca tespit edebilir. STS sürekli ağı izler, ağdaki savunmasız noktaları bulur ve ihlaller hakkında yöneticiyi bilgilendirir. STS ağ trafiğinde aktivitenin normal veya zararlı bir trafik olup olmadığını anlamak için Makine Öğrenmesi (MÖ) algoritmalarından yararlanmaktadır. MÖ algoritmaları öğrenme türüne göre ikiye ayrılmaktadır. Bunlar, Denetimli ve Denetimsiz MÖ yöntemleridir. Bu tez çalışmasında Denetimli MÖ algoritmaları kullanılmış ve değerlendirilmiştir. Bir diğer unsurda kullanılan veri setleridir. Etkili bir STS ortaya çıkarılabilmesi için veri setlerinin güncel saldırı tiplerini içeriyor olmadır. Literatür araştırmasından da anlaşılacağı gibi MÖ algoritmalarını eğiten ve performanslarını ölçen veri setleri oldukça eskidir. Bu tez çalışmasında güncel ve yeni kıyaslama veri seti olarak ortaya çıkmış olan UNSW-NB15 veri seti kullanılarak daha etkili ve verimli STS oluşturmak için adım atılmıştır. Elde edilen MÖ algoritma performansının yükselmesi için eğitim aşamasında kullanılan özelliklerin de önemi vardır. Özelliklerin sayısı ve hangi özelliğin seçileceği ayrı bir çalışma alanıdır. Bu tez çalışmasında ReliefF puanlama yöntemi kullanılarak özellik seçimi yapılmış ve bunun MÖ algoritmaları üzerindeki performansları da tartışılmıştır.

1.2. ÇALIŞMANIN AMACI

Dünya nüfusunun internete erişiminin kolaylaşması, internet ağının çok hızlı bir şekilde gelişmesine olanak sağlamıştır. İnternetin gelişmesi de Nesnelerin İnterneti olarak tanımladığımız Nİ cihazlarının gelişmesi ve kullanılmasının önünü açmıştır. Milyarlarca Nİ cihazının da internet olarak adlandırılan bu ağa dahil olmasıyla beraber çok büyük bir veri ortaya çıkmıştır. Bu veriler içerisinde kişisel ve gizli kalması gereken verilerden, finansal işlemler olarak isimlendirebileceğimiz elektronik ticaret, bankacılık hizmetleri gibi verileri de içermektedir. Oluşan bu büyük veri saldırganların ilgisini çok daha fazla bu alana çekmiştir. Bu noktada bireyler veya organizasyonlar internet üzerinden aldığı veya verdiği hizmetlerin kalitesinin yanında güvenliği sağlamak gayreti içinde de olmaktadır [7]. Güvenlik önlemlerinin içerisinde geleneksel yöntemler olarak Güvenlik Duvarı, anti-virüs vb. yöntemler kullanılmasının yanında artık yaşanan güvenlik sorunlarını en aza indirmek için farklı güvenlik yöntemleri de kullanılmaya başlamıştır. Bunlardan bir tanesi de Saldırı Tespit Sistemleridir. STS'ler iki farklı şekilde sınıflandırılmaktadır. Bunlar, İmza tabanlı STS'ler ve Anomali tabanlı STS'ler (ASTS) dir. İmza tabanlı STS'ler (İSTS) de önceden bilinen saldırılar vasıtasıyla karşılaşılacak herhangi bir saldırıyı önlemeyi amaçlamaktadır. Önceden bilinen saldırıların imzaları oluşturulmuş ve bir veri tabanında saklanmaktadır. Ağ trafiğini tarayan STS'ler bu veri tabanındaki imzalar ile ağ trafiğini karşılaştırır ve eğer eşleşme meydana gelirse saldırı olarak nitelendirir. Bu yöntemde imza veri tabanının belli aralıklarla güncellenmesi gerekmektedir. Sıfır-gün saldırıları olarak bilinen saldırılara karşı yetersizdir. Anomali bazlı STS'ler ise normal bir kullanıcı trafiğinin desenlerini MÖ yöntemleri yardımıyla belirleyerek bir model oluşturur ve bu modelin dışındaki herhangi bir ağ trafiğini anomali olarak nitelendirir. Bu yöntem sayesinde herhangi bir imza veri tabanı oluşturulması gerekmemektedir ve sıfır-gün saldırılarında oldukça başarılı sonuçlar elde edilmektedir. MÖ yöntemleri Anomali tabanlı STS'lerin gelişmesinde çok önemli rol oynamaktadır. Bu anlatılanlardan hareketle çalışmamızı anomali tabanlı STS'lerin performanslarını etkileyen en önemli unsurlardan olan şu iki parametre dikkate alınarak gerçekleştirilmiştir. Birincisi, sağlıklı bir STS geliştirmek için elinizdeki eğitim verisinin güncel ve günün şartlarını sağlamış olmasıdır. İkincisi, saldırı tespiti yaparken kullanılan MÖ algoritmalarıdır. İlgili çalışmalar bölümünde de görüleceği gibi daha önce bu alanda yapılan çalışmalarda kıyaslama veri seti olarak 1999 yılında oluşturulan ve sonraki yıllarda üzerinde iyileştirmeler yapılarak oluşturulan veri setleri kullanılmıştır.

Günümüzde ve o dönemde de var olan saldırı çeşitlerinin bazılarının tespit edilmesinde farklılıklar yaşandığı bilinmektedir. Şöyle ki o dönem "spy" olarak adlandırılan saldırı çeşidinin çok kolay tespit edilebilen bir saldırı olduğu ancak günümüz şartlarında aynı saldırı tipini normal trafikten ayırt etmenin çok daha zor olduğu bilinmektedir. Literatürdeki yeni ve günümüz şartlarını sağlayan kıyaslama veri setleri üzerinden başarım analizlerinin yapılması gerektiği görüşüne katkı sağlayabilmek için bu çalışmada yeni kıyaslama veri seti olarak kabul gören UNSW-NB15 veri seti kullanılmıştır. Bu tez çalışmasında Orange isimli araç üzerinde denetimli MÖ algoritmalarını gerçeklenmiştir. Güncel bir veri seti ve o veri setine uygun MÖ algoritmalarının performans analizleri paylaşılmıştır. Burada veri setinin orijinal hali ile elde edilen sonuçlar ve veri seti üzerinde özellik mühendisliği uygulayarak elde edilen sonuçlar sunulmuştur. Bu çalışmanın amacı STS'lerin çok daha verimli ve etkili çalışması için günümüz saldırı çeşitlerini içinde barındıran ve ReliefF puanlama yöntemi kullanılarak özellik seçimi yapılmış bir veri seti üzerinde var olan Makine Öğrenmesi yöntemlerinden hangisinin daha performanslı olduğunu bulmak ve kullanılan MÖ yöntemlerinin performanslarını literatür ile karşılaştırmaktır. Çalışma veri setinde Özellik Seçimi (ÖS) yapılıp yapılmaması ve test veri setinin elde edilme şekline göre dört farklı senaryo ile gerçekleştirilmiştir.

1.3. TEZ ORGANİZASYONU

Tez çalışmasının organizasyonu beş bölümden oluşmaktadır ve bölümlere aşağıda kısaca değinilmiştir:

1. Bölüm: Çalışma konusu hakkında giriş bilgileri verilmiştir. Aynı zamanda çalışmanın amacını bildirmektedir.
2. Bölüm: Çalışma konusu ile ilgili daha önce yapılan çalışmalar hakkında bilgiler verilmiştir.
3. Bölüm: Çalışmanın materyal ve yönteminden bahsedilmiştir.
4. Bölüm: Çalışmanın araçlar yardımıyla benzetimi yapılmıştır.
5. Bölüm: Çalışmanın sonuçları detaylı incelenmiştir.

2. İLGİLİ ÇALIŞMALAR

Bu bölümde daha önce bu alanda yapılan çalışmalarla ilgili bilgiler verilmiştir. Bölüm sonunda çalışmanın literatüre olan katkısından bahsedilmiştir.

2007-2013 yılları arasında gerçekleştirilen çalışmada alanıyla ilgili 65 çalışma incelemiş ve karşılaştırılmıştır. Bu incelemeler sonucunda araştırmacıların elde ettikleri sonuçlar sırayla şöyledir: Birincisi, STS'lerde en çok KDD 99 veri setinin kullanılmıştır. İkincisi DoS, Bilgi Tarama (proping), R2L (Remote to Local), U2R (User to Root) gibi saldırı çeşitlerinin tespitinde Yapay Sinir Ağı (YSA) yüksek başarı göstermiştir. Üçüncüsü, Destek Vektör Makineleri (DVM) ile DoS, Bilgi Tarama ve U2R tipi saldırılarda etkin çözümlerin üretilebileceğidir. Dördüncüsü, Bayes sınıflandırıcının Bilgi Tarama saldırılarında başarılı sonuçlar verdiğidir [8].

[9]'da yapılan çalışmada NSL-KDD veri seti kullanılmıştır. Bu çalışmada 7 farklı makine öğrenimi algoritması kullanılmış ve çıkan sonuçları başarım, eğitim süresi ve çalıştırma süresi olarak 3 farklı kategoride değerlendirmişlerdir. Adaboost algoritması en yüksek doğruluk oranına ulaştığı ancak gerek eğitim süresi gerekse çalışma zaman performansın göz önüne alındığında Karar Ağacı algoritmasının da yüksek performans gösterdiğini belirtmişlerdir. Gelecek çalışmalar için daha güncel veri seti ile çalışma yapılmasını önermişlerdir.

Yapılan çalışmada saldırı verilerini birleştirerek bir veri seti oluşturmuş ve çalışmada oluşturulan veri setini kullanılmıştır. MÖ sınıflandırıcısı olarak DVM ve Naive Bayes (NB) kullanılmıştır. Çalışmanın sonuçlarında ise DVM 0,71 ve NB'de ise 0,79 başarı seviyesine ulaşılmıştır. DVM'nin eğitim süresi nedeniyle büyük veri setleri için uygun olmadığı da belirtilmiştir. Gelecek çalışmalar için sıfır-gün saldırıları olarak bilinen saldırı tipi için bu tip saldırı verilerini geliştiriciler ile paylaşılmasının çok daha etkili STS geliştirilmesinde katkısı olacağı görüşünü ifade etmişlerdir [10].

[11]'de yapılan çalışmada karar ağaçları ve rastgele orman sınıflandırıcılarını kullanarak bilgisayar ağlarında akan normal ve anormal paketleri sınıflandırmışlardır. Ağ trafiğinin kaydedildiği dosya tipi olan PCAP dosyasında çıkarılan 78 adet değişken kullanılmıştır. Bu çalışmada CICIDS2017 veri seti kullanılmıştır. Rastgele orman sınıflandırıcısı karar ağacı sınıflandırıcısından az da olsa daha iyi bir sonuç verdiğini belirtmişlerdir.

[12]'de yapılan çalışama da veri seti olarak NSL-KDD veri seti kullanılmıştır. Bu çalışmada denetimli MÖ sınıflandırıcısı olarak Lojistik regresyon (LR), Gaussian Naive Bayes, Destek Vektör Makineleri, Rassal Orman (RO) kullanılmıştır. Sonuçlar, Rassal Orman sınıflandırıcısının diğer sınıflandırıcılara göre %99 gibi daha yüksek bir orana ulaştığını göstermektedir.

[13]'de yapılan çalışmada STS'lerin Kablosuz Algılayıcı Ağlar'a (KAA) karşı yapılan saldırılardan başlıca güvenlik mekanizmalarından birisi olduğunu belirtmişlerdir. Bu amaçla KDD 99 veri seti ile beraber 4 farklı saldırı tipi ve normal trafiği tanımlayarak MÖ sınıflandırıcıları kullanılmıştır. Deneysel sonuçlara göre rassal orman yöntemi yüksek tespit ve düşük yanlış alarm oranlarına sahip olmuştur.

Bu çalışmada denetimli MÖ yöntemleri kullanarak gerçek-zamanlı izinsiz-giriş tespit yaklaşımı önermişlerdir. Saldırı tipi olarak DoS ve Probing seçilmiştir. Önerilen bu yaklaşımı bilinen birçok MÖ yöntemiyle değerlendirilmiş ve diğer yöntemlere göre en yüksek toplam tespit oranını karar ağaçları vermiştir. Bunun sonucu olarak karar ağacı yöntemi kullanarak gerçek zamanlı bir STS önermişlerdir [14].

[15]'de yapılan çalışmada saldırı tespitinin verimliliğinin ana etkeninin özellik boyutuna bağlı olduğunu belirtmişlerdir. Çalışmada KDD 99 veri seti kullanılmış ve 41 olan özellik sayısı 19'a düşürülmüştür. MÖ yöntemi olarak DVM kullanışmış ve %98 doğruluk değerine ulaşılmıştır.

Başka bir çalışmada DVM ve aşırı öğrenim makinesi (AÖM) kullanarak bilinen ve bilinmeyen atakların tespitindeki verimliliği arttırmak için çok-seviyeli STM önermişlerdir. Veri seti olarak KDD 99 kullanılmıştır. Düzenlenmiş K-ortalama kümele yöntemi kullanılarak orijinal eğitim setini temsil eden sınıflandırma performansını geliştirmede önemli katkısı olan yüksek kaliteli küçük bir veri seti oluşturulmuştur. Aynı veri setinde diğer yöntemlerle kullanıldığında, önerilen model saldırı tespit etmede yüksek verimlilik göstermiş ve %95 doğruluk oranına sahip olduğu görülmüştür [15].

[16]'da yapılan çalışmada UNSW-NB15 veri setini ve ileri beslemeli yapay sinir ağı algoritmasını kullanarak yeni bir ağ saldırı tespit sistemi modellemişlerdir. Veri seti seçiminde KDD 99 ve NSL-KDD gibi kıyaslama veri setlerinin aksine UNSW-NB15 veri setinin daha kullanışlı olduğunu belirtmişlerdir. Buna ek olarak veri setinin normal ve saldırı ağ trafiğinin modern biçimde yansıttığı, yeni tip saldırıların güncel ayak izlerine sahip olduğunu ve sınıflandırma için çok uygun bir veri seti olduğunu belirtmişlerdir.

Yapmış oldukları çalışmanın deneysel sonuçlarında ise, Lojistik Regresyon %83.15, Naive Bayes %81.2, Yapay Sinir Ağı %81.5 ve önerdikleri yöntemin doğruluk oranı %99.99 olduğunu belirtmişlerdir.

[17]'de yapılan çalışmada 2020 yılında yaptıkları bir çalışmada gerçek zamanlı saldırı tespitine uygun bir yapay sinir ağ tabanlı STS geliştirmişlerdir. Geliştirilen STS'nin değerlendirilmesi için UNSW-NB15 veri seti kullanılmıştır. MÖ yöntemi olarak "Sinir Ağları" kullanılmıştır. Yapılan çalışmadan gerçek zamanlı ağ trafiklerinde saldırı tespiti yaparken karşılaşılan zorluklarının en aza indirilmesi için özellik seçimi "gain oranı" yöntemi kullanılarak yapılmıştır. Orijinal haldeki veri setinde 49 olan özellik sayısı bu yöntemler kullanılarak 30'a düşürülmüştür. Deneysel sonuçlarda doğruluk oranının %76.96 olduğunu göstermiştir. Ayrıca sonuçlar UNSW-NB15 veri setinin STS'lerin değerlendirilmesi için uygun bir veri seti olduğunu da göstermiştir.

[6]'da yapılan çalışmada 2020 yılında yapmış oldukları çalışmada UNSW-NB15 veri setini kullanarak MÖ yöntemlerinin sınıflandırma performanslarını karşılaştırmışlardır. Orijinal halinde 49 olan özellik sayısını MÖ yöntemlerinin sınıflandırma yaparken kullanılamayacak bazı özelliklerden oluşuyor olması sebebiyle bunları çıkartarak özellik sayısını 42'ye indirmişlerdir. Akış özellikleri olarak var olan özelliklerden 4 tanesi tek bir özelliğe indirilmiş ve zaman bildiren iki özellikte tek özelliğe indirgenmiş ve toplam özellik sayısı 45 olmuştur. Daha sonra "id", "dur" ve "attack_cat" özellikleri listeden çıkarılmış ve toplam 42 özellikle uygulamalar yapılmıştır. Elde edilen sonuçlardan en yüksek doğruluk oranına "Rassal Orman" ile %95.43'dir.

Bir diğer çalışmalarında da UNSW-NB15 veri setinde özellik seçimi yaparak var olan özellik sayını azaltarak orijinalde 49 olan ve MÖ yöntemlerinin sınıflandırma yapabilmesi için bazı özelliklerin çıkarılmasıyla 42 ye düşen özellik sayısını 23'e indirerek MÖ yöntemlerinin sınıflandırma performanslarını karşılaştırılmıştır. Elde edilen sonuçlara göre en yüksek doğruluk oranı "Rassal Orman" ile %99.64'dür [18].

Bu tez çalışmasında daha önce bu alanda yapılan çalışmalardan farklı olarak, ilgili çalışmalar bölümünde de görüleceği gibi STS'lerin oluşturulmasında kullanılan veri setlerinin güncel saldırı çeşitleri açısından eksik olmasını göz önünde bulundurularak günümüz şartlarını sağlayan veri seti olan UNSW-NB15 veri seti kullanılmıştır. Kullanılan veri setinde ReliefF puanlama yöntemi kullanılarak Özellik Seçimi yapılmış ve MÖ algoritmalarının performansına olan etkisi değerlendirilmiştir. Kullanılan MÖ

performansları da kendi içerisinde ve literatürdeki çalışmalarla karşılaştırılmış ve tartışılmıştır.

3. MATERYAL VE YÖNTEM

Bu bölümde bilgi güvenliği ve mevcut saldırı tespit sistemleri ile alakalı kısa bir bilgi verildikten sonra kullanılan makine öğrenmesi yöntemleri anlatılacak ve veri seti hakkında ayrıntılı bilgi verilecektir.

3.1. BİLGİ VE BİLGİ GÜVENLİĞİ

Bilgi yaşadığımız çağın en değerli varlıkları arasındadır. Bilginin altın kadar değerli olduğu düşünülen bu çağda, bilgi ile ilgili hususların incelenmesi insanlığın başlangıcından itibaren ileriye dönük gelişmemizin en önemli kilometre taşlarındandır [19]. Bilgi yaşadığımız dönemde ön planda gibi gözükse de aslında insanlığın ortaya çıkışından itibaren toplumların gelişmesinde önemli bir role sahiptir.

Bilgi güvenliği, elektronik ortamlarda bilgilerin veya verilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür. Bilgi güvenliğinin sağlanması için gerekli güvenlik tedbirleri belirlenmeli ve bu tedbirler uygulanmalıdır [20]. Uluslararası standart olan ISO/IEC 27002 bilgi güvenliğini, bilginin erişilebilirliğini, bütünlüğünü ve gizliliğinin korunması olarak tanımlamaktadır. Bu standarda göre bilgi birçok farklı şekilde olabilir. Kâğıda elle yazılmış veya bilgisayar çıktısı olarak alınmış, elektronik olarak depolanmış, posta ile veya elektronik bir şekilde gönderilmiş vb. gibi şekillerde bulunabilir. Whitman ve Mattord ISO/IEC 27002 standardında bahsedilen üç özelliğin bilgisayar endüstrisinin sürekli değişen ortamı göz önüne alındığında yeterli olmadığını belirtmiş, bu özelliklere ek olarak doğruluk, özgünlük, yararlılık ve sahipliğinde korunması gerektiğini eklemişlerdir [7].

3.2. SALDIRI ÇEŞİTLERİ

Ağ güvenliğinin görevi verinin gizliliğini ve bütünlüğünü devam ettirerek, kaynağın erişilebilirliğini garanti altına almaktır. Basit bir tabirle, bir ağda taviz vermeyi amaçlayan zararlı özelliklere sahip her şey bir saldırı/tehdit olarak tanımlanır. Ağdaki zayıf tasarım, kullanıcı dikkatsizliği ve donanımsal veya yazılımsal yanlış yapılandırma saldırılara karşı

ağı savunmasız hale getirir [21]. Saldırı çeşitleri dört farklı kategoriye ayrılmıştır. Bunlar sırayla aşağıda bahsedilmiştir.

3.2.1. Hizmet Engelleme (Denial of Service DoS)

DoS, saldırganın verilen bir hizmetin meşru kullanıcıları tarafından istenen kaynakları kullanmasını engellemesi veya engellemeye yönelik açık bir girişimde bulunmasından ortaya çıkan ve yaygın olarak görülen bir saldırıdır [22]. Böyle bir saldırı hem merkezi hem de dağıtılmış olarak gerçekleştirilebilir. Bu saldırı çeşidine örnek olarak şunlar verilebilir;

- SYN flooding
- Smurf
- Fraggle
- Jolt
- Land
- ping-of-death

Bir DoS saldırı örneği olarak; sunucu çok sayıda bağlantı isteğiyle dolup taştığında meşru bir kullanıcının web sunucusuna erişiminin reddedilmesi olarak verilebilir. DoS saldırısını gerçekleştirmek, herhangi bir ön erişim gerekmediği için çok sık karşılaşılan bir saldırı tipidir [22], [23].

3.2.2. Bilgi Toplama (Probe)

Bilgi toplama saldırısının amacı keşif yapmak amacıyla hedeflenen ağ veya ana bilgisayar hakkında bilgi toplayabilmektir. Keşif amaçlı yapılan bu saldırılar ağa bağlı makinelerin sayısı ve tipi hakkında bilgi almak için kullanılan oldukça yaygın saldırı türleridir. Ana bilgisayara yüklü yazılımları veya kullanılan uygulamaları belirlemek amacıyla da kullanılır. Probe saldırıları ağın açık vermesi için gerçek bir saldırıdaki ilk adım olarak düşünülmektedir. Her ne kadar bu tip saldırılar bir hasara neden olmasa da şirketler için oldukça ciddi tehditler barındırdığı düşünülmektedir. Çünkü ölümcül bir saldırı için yararlı bilgileri elde etmek için yapılan bir saldırı olabilir [23].

3.2.3. Yönetici Hesabı ile Yerel Oturum Açma (R2L)

Bilgisayar ağ saldırılarından bir tanesidir. Bir saldırgan bilgisayar veya sunucuya yerel bir kullanıcı olarak erişme yetkisi olmadığı bir ağ üzerinden paketler yollayarak o ağda yerel kullanıcı yetkisi elde etmeye çalışır. Başarılı olursa da makineden aktarılan verilerde değişiklik yapar ve makinedeki dosyalara erişilebilir [24].

3.2.4. Kullanıcı Hesabının Yönetici Hesabı olarak Davranmaya Çalışması (U2R)

Saldırganlar önemli kaynakları kötüye kullanmak veya manipüle etmek için yasal olmayan bir şekilde yönetici hesabına erişim sağlamak amacıyla bu saldırıyı yaparlar. Saldırganlar, sosyal mühendislik veya şifre yakalama gibi teknikleri kullanarak, normal bir kullanıcıya erişim sağlarlar ve bir veya daha fazla savunmasızlığı istismar ederek süper kullanıcı ayrıcalıklarına erişmeye çalışırlar [23].

3.3. SALDIRI TESPİT SİSTEMLERİ

Saldırı Tespit Sistemleri (STS), hedef sistemin güvenliğinin sürdürülebilmesine olanak sağlamak için bilgisayar sistemlerindeki zararlı yazılımları tanımlayan yazılımsal veya donanımsal sistemlerdir [25]. Karşılaşılan saldırılar, bilgi sistemlerinin yetkisiz kullanımına, değiştirilmesine veya tamamen ortadan kaldırılmasına sebep olarak bilgilerin gizlilik, bütünlük ve erişilebilirliğine yönelik tehdit oluşturur. Saldırı Tespit Sistemleri bilgisayar güvenliğini sürdürmek için zararlı yazılım aktivitelerini tanımlamayı amaçlayan bir yapıdır. Bilgisayar servislerinin meşru kullanıcıların isteklerine cevap veremeyecek hale getiren aktiviteler saldırı olarak düşünülmektedir. STS'nin hedefi geleneksel güvenlik duvarları tarafından tanımlanamayan ağ trafiğindeki farklı zararlı yazılım türlerini tanımlamaktır. Bunun yapılması bilgisayar sistemlerinin gizlilik, bütünlük ve erişilebilirliğini tehlikeye atan olaylar karşısında yüksek koruma sağladığı için hayati öneme sahiptir. STS'ler genel olarak iki gruba ayrılmaktadır: İmza Tabanlı STS (signature-based IDS) ve anomali tabanlı STS (anomaly-based IDS) [26].

3.3.1. İmza Tabanlı Saldırı Tespit Sistemleri (İSTS)

İmza tabanlı STS'ler bilinen bir saldırıyı bulmak için desen eşleştirme tekniğine dayalıdır. Ayrıca bilgi-tabanlı tespit veya misuse-tabanlı tespit olarakta bilinir [27]. İSTS'de daha önceki bir saldırıyı bulmak için eşleştirme yöntemi kullanılır. Bir diğer deyişle bir saldırı, imza veri tabanında var olan önceki saldırının imzasıyla eşleştiğinde alarm tetiklenir.

İSTS'ler ana bilgisayarın sistem günlüklerini daha önceden zararlı yazılım olarak tanımlanan bir komut veya aktivite dizisini bulmak için araştırır [28].

İSTS önceden bilinen saldırılarda, saldırı tespit oranında mükemmel doğruluk oranına sahiptir [29]. Fakat, İSTS yeni saldırı imzasının çıkarılıp veri tabanına depolanmasına kadar imza veri tabanında eşleşen imza olmaması nedeniyle sıfır-gün saldırılarının tespitinde çok zorlanmaktadır.

Sıfır-gün saldırılarının oranının artması İSTS tekniğinin giderek daha verimsiz hale getirmektedir, çünkü bu tip atakların var olan bir imzasının olmaması eşleştirme yapılamaması anlamına gelmektedir [30]. Zararlı yazılımların çok biçimli değişkenlikleri hedeflenen saldırıların miktarının artması geleneksel paradigmaların yeterliliğinin azalmasına neden olabilmektedir. Bu sorunun potansiyel çözümü neyin zararlı olduğundan ziyade kabul edilebilir davranışların ne olduğunu sınıflandırmaya uygun hale getirerek (profilleyerek) işlem yapan Anomali-Tabanlı tekniklerin kullanılmasıdır [26].

3.3.2. Anomali Tabanlı Saldırı Tespit Sistemleri (ASTS)

ASTS, İSTS'nin sınırlamalarını aşabilecek kapasiteye sahip olmasından dolayı birçok bilim insanının dikkatini üzerine çekmiştir. ASTS'de bilgisayar sisteminin davranışlarının normal bir modeli MÖ, istatistik tabanlı veya bilgi tabanlı yöntemler kullanılarak oluşturulmaktadır. Oluşturulan model ve gözlenen davranışlar arasındaki herhangi bir sapma saldırı olarak da nitelendirilebilecek olan anomali olarak değerlendirilmektedir. Bu tür teknikler için tipik bir kullanıcı davranışı ile kötü amaçlı davranış arasında farklılıklar olduğu varsayımı savunulmaktadır. Standart bir kullanıcının davranışına benzer olmayan normal dışı kullanıcının davranışı saldırı girişimi olarak nitelendirilir. ASTS iki farklı grupta incelenmektedir. Bunlar: eğitim ve test aşamasıdır. Eğitim aşamasında, normal trafik profili normal davranışın modelini oluşturmak için kullanılmaktadır. Test aşamasında ise yeni bir veri seti daha önceden görülmemiş saldırılara genelleme kapasitesini belirlemek için kullanılmaktadır [31].

ASTS'nin en önemli avantajı imza veri tabanı kullanmaksızın normal kullanıcı trafiğini tanımlayabilme yeteneğinden dolayı sıfır-gün saldırılarının tanımlayabilme yeteneğidir. ASTS sıradan davranışların dışında bir davranış sezdiği zaman tehlike sinyalini tetikler ve böylece, ASTS sistemin korunması için birçok fayda sağlar. Bunlardan bir tanesi, iç taraftan gelebilecek saldırıları da keşfetme yeteneğine sahip olmasıdır. Eğer saldırgan çalınmış bir hesaptan olağan bir hareket olarak tanımlanamayan bir transfer yapmaya

çalışırsa bir alarm üretilir ve bu da sistemin güvenliğini sağlar [32].

3.4. MAKİNE ÖĞRENMESİ

Makine Öğrenmesi, örnek veri veya deneyimlerden öğrenerek elde olan performans kriterlerini en uygun durumuna getirmek (optimize) için bilgisayarların programlanması bilimi veya sanatıdır [33]. MÖ işlemlerinde, bilgisayarlar kendilerini besleyebilmek için eğitim veri seti olarak da bilinen veri örnekleriyle eğitilirler. Eğitim aşamasından sonra Algoritmaların öğrenim performanslarını test veri seti üzerinden test edilmektedir. MÖ genellikle klasik tekniklerin yetersiz olduğu durumlarda kullanılmaktadır [34].

MÖ eğitim ve denetim yöntemlerine göre dört farklı gruba ayrılmaktadır: denetimli öğrenme, denetimsiz öğrenme, yarı denetimli öğrenme, pekiştirmeli öğrenme [35]. MÖ'nün ayrıldığı dört farklı grup ve bu tez çalışmasında kullanılan MÖ algoritmaları ilgili bölümlerde açıklanacaktır.

3.4.1. Gözetimli Öğrenme

Denetimli öğrenme algoritmaları eldeki verinin etiketlenmiş olması durumunda kullanılmaktadır. Algoritmalar eğitim aşamasında farklı örneklere maruz kalır ve veri örneklerinin içindeki bilgiden istatistiksel bilgi çıkartır. Eğitim aşamasında kazanılan deneyimle beraber algoritmalar, yeni veriyi sınıflandırır ve tahmin edilebilir. Beklenen sonuçlarla elde edilen sonuçlar karşılaştırıldığında net bir şekilde modelin ne kadar iyi eğitildiği gözlemlenebilmektedir [36].

3.4.2. Gözetimsiz Öğrenme

Makine Öğrenmesi algoritmaları öğrenme için etiketlenmiş veri örneklerine dayalı değildir, fakat etiketsiz veriler içerisindeki gizli karakteristik özellikleri bulmak için çabalamaktadır. Bu algoritmaların sadece giriş verisine erişimi vardır ve hedef değerle alakalı herhangi bir veriye sahip değildir [37].

3.4.3. Yarı Gözetimli Öğrenme

Veri etiketleme işlemi yorucu ve maliyetlidir. Özellikle veri seti büyük ve etiketlenmemiş verinin sayısı çok olduğunda, bu tip veri setleri ile başa çıkabilmek için tasarlanan algoritmalara yarı denetimli öğrenim algoritmaları denmektedir. Yarı-denetimli öğrenimin amacı etiketli ve etiketsiz verilerin birleştirilmesinin öğrenme performansını

nasıl değiştirebileceğini anlamaktır [36].

3.4.4. Pekiştirmeli Öğrenme

Pekiştirmeli öğrenme özel durumlarda en mümkün yolu veya davranışı bulmak için kullanılan MÖ yöntemlerinden birisidir. Denetimli MÖ yönteminden farklıdır. Denetimli MÖ yöntemlerinde anahtar rol, eğitim veri setidir. Eğitim veri seti doğru sonuçlarla algoritmaları eğitir ve buna göre bir çıktı oluşturulur. Pekiştirmeli öğrenmede ise eğitim veri seti yoktur. Pekiştirmeli öğrenme ajanları verilen görevi yerine getirmek için ne yapacaklarına karar verirler. Eğitim veri seti yokluğunda bu yöntemin deneyimlerinin kullanılması kaçınılmazdır [34].

3.4.5. Çalışmada Kullanılan Makine Öğrenmesi Algoritmaları

Bu tez çalışmasında, denetimli MÖ algoritmaları kullanılmıştır. Denetimli MÖ algoritmalarında, hedefin belirlenmesi için etiketli eğitim verisi kullanılmaktadır. Etiketli veri ile eğitim aşaması tamamlandıktan sonra test veri seti ile performans ölçümleri yapılmaktadır. Saldırı tespitinin belirlenmesinde kullanılan bu algoritmalar hakkındaki bilgiler bölümün devamında verilmiştir.

3.4.5.1. *K-En Yakın Komşu (KNN)*

KNN en eski, parametrik olmayan ve ilk sınıflandırma tekniklerinden birisidir. KNN sadece sınıflandırma problemlerinde değil aynı zamanda regresyon ve tahmin problemlerinde de oldukça verimli şekilde kullanılmaktadır. Yorumlanması kolay ve düşük işletim zamanına sahip olduğu için oldukça fazla kullanılmaktadır [35]. KNN algoritmasının çalışma prensibi şu şekildedir: KNN, eğitim veri seti olarak kullandığımız veri seti yoğunluğuna göre gruplara ayırır. Yeni bir veri geldiğinde daha önceden seçilmiş olan K referans değeri en yakın kaç tane komşusuna göre sınıflandırma yapılacağını gösterir. K referans değeri 3 olarak seçildiyse, sınıflandırılması için bir veri geldiğinde o verinin en yakın 3 komşusunun hangi sınıfta olduğuna bakar ve ona göre yeni gelen veriyi sınıflandırır.

3.4.5.2. *Rassal Orman (RO)*

Rassal Orman (RO), Karar Ağaçlarına dayalı Topluluk Öğrenimi (TÖ) yöntemlerinden biri olarak sınıflandırma için kullanılan bir MÖ algoritmasıdır [38]. Eğitim aşamasındayken, çok sayıda karar ağacı ile beraber bir karar ağacı ormanı oluşturur [39]. Karar Ağacı ormanı üyesi her bir ağaç verilen örnek için sınıf etiketini tahmin eder. Sınıf

etiketi her bir ağaç tarafından tahmin edildiğinde, son kararı vermek için çoğunluk oylaması yapılır. En fazla oyu alan sınıf etiketi, test verilerine uygulanan en uygun etiket olarak kabul edilir. Elimizdeki veri setindeki her bir değer için bu döngü tekrar edilir [40]. Bu algoritma bu tez çalışmada en iyi sonucu elde etmiştir.

3.4.5.3. *AdaBoost*

AdaBoost, yaygın olarak kullanılan Topluluk Öğrenimi (TÖ) tabanlı denetimli MÖ sınıflandırıcısıdır. Birden çok zayıf sınıflandırıcıyı güçlü bir sınıflandırıcıya entegre ederek gelişmiş sınıflandırma sonuçları üretir [41]. Başlangıçta, bütün gözlemlere aynı ağırlık verilir. Gözlemin ağırlığı zayıf sınıflandırıcının katsayı ile değişir, uygulanan sınıflandırıcının katsayısı hata tahmini değeri kullanılarak tahmin edilir. Böylece, sınıflandırıcı tarafından oluşturulan hata değeri, sınıflandırıcının katsayısı olarak düşünülebilir. Sonuç olarak, yanlış sınıflandırılmış gözlemin katsayısı AdaBoost algoritması tarafından arttırılabilir ve doğru tanımlanmış gözlemin ağırlığı düşürülebilir. Sonraki yinelemelerde, yanlış sınıflandırılmış gözlemelerin ağırlıklara daha da yükselecektir. Sonunda geliştirilen tüm zayıf sınıflandırıcılar doğrusal birleştirme yöntemi kullanılarak daha güçlü bir sınıflandırıcı oluşturmak için birleştirilir [42].

3.4.5.4. *Lojistik Regresyon (LR)*

Lojistik Regresyon (LR) denetimli MÖ algoritmaları arasında güçlü bir sınıflandırıcıdır. LR yeni gözlemlerin belirli bir sınıfa ait olma olasılığını belirler. Olasılık olduğu içinde sonuçları 1-0 arasında değişir [43]. LR ikili sınıflandırma için uygulanacaksa iki sınıf arasındaki ayrımı tanımlayabilsin diye bir eşik değer atanır. Örneğin, bir değerin ihtimali 0,5'den büyükse "A sınıfı" değilse "B Sınıfı" olarak tasarlanır [44].

3.4.5.5. *Naive Bayes (NB)*

Naive Bayes sınıflandırıcısı, Basitliği ile bilinen yaygın olarak kullanılan denetimli MÖ yöntemlerinden birisidir. Önceki bilgilerin ışığında ihtimalleri hesaplayarak geleceği tahmin etmek üzerine kuruludur. Örneğin, saldırı tespitinde NB trafiği normal veya saldırı olarak sınıflandıracaktır. Bağlantı süresi, bağlantı protokolü vb. özellikler trafiğin sınıflandırılması için kullanılacaktır ve bu özellikler birbiriyle ilişkili olmasına rağmen NB bu özellikler bağımsız olarak ele alır. NB sınıflandırmasında, tüm özellikler, trafiğin normal veya anormal olma olasılığına ayrı ayrı katkıda bulunur. Ancak NB sınıflandırıcısı özellikler arasındaki ilişkilerden ve aksiyonlardan herhangi bir ip ucu çıkartamaz ve kullanamaz. Örneğin; Sınıflandırıcının, sınıflar arasındaki ayrım gücünü arttırmaya

yardımcı olduğu karmaşık durumlarda özellikler arasındaki ilişkiler doğru sınıflandırma için önemlidir [45].

3.4.5.6. *Destek Vektör Makineleri (DVM)*

DVM, iki veya daha fazla sınıf arasındaki veri özelliklerinde ayırıcı bir köprü oluşturarak sınıflandırma yapmak için kullanılır. Köprü ile her bir sınıfın en yakın komşusu arasındaki mesafeyi en yüksek seviyeye çıkarmaya çalışır. DVM genelleştirebilme yeteneği ile tanınmıştır. Özellikle büyük miktarda özellik içeren ama az sayıda kayıt sahibi olan veri setleri için uygundur. DVM avantajları, ölçeklenebilirliği, gerçek-zaman saldırı tespiti yapabilme yeteneği ve eğitim desenlerini dinamik bir şekilde güncelleyebilmesidir [46].

3.4.5.7. *Sinir Ağları (SA)*

Bir Sinir Ağı başlangıçta hiçbir alan bilgisi içermez, ancak örnek girdi verisi çiftlerini çıktı vektör örnekleri ile eşleyerek karar verme için eğitilebilirler. Her bir girdi örnek vektörlerinin uygun bir çıktı vektörü temsil etmesi için ağırlıklar ayarlanır. Sinir ağları insan beyninde kullanılan sistem gibi çalışır. İnsan beynindeki öğrenme fonksiyonunu gerçekleştiren bilgisayar sistemleridir. Öğrenme işlemini gerçekleştirirken örnekler kullanılır. Her bir ağın kendine uygun bir ağırlığı vardır. Sinir ağlarının sahip oldukları bu ağırlıkta sahip oldukları bilgi saklıdır ve ağa yayılmıştır [5].

3.5. KULLANILAN VERİ SETİ

Son yıllarda Saldırı Tespit Sistemleri, var olan geleneksel güvenlik çözümlerinin yeterli olmadığı noktalarda MÖ yöntemlerini kullanarak başarılı işler çıkarmıştır. Özellikle de anomali bazlı STS'ler sıfır-gün atakları olarak bilinen saldırıların tespitinde çok önemli rol oynamaktadır. STS'lerin performanslarını değerlendirirken ve daha etkili ve verimli STS'ler oluşturmaya çalışırken hiç kuşkusuz en önemli etkenlerden birisi de kullanılan veri setleridir. STS'lerin performanslarını ölçerken en çok kullanılan kıyaslama veri setleri; KDD 99 ve NSL-KDD'dir [47]. STS'lerin geliştirilmesi ve performanslarının ölçülmesinde veri setlerinin önemi çok büyüktür. Kullanılan veri seti çağın gereklerine uygun olmalı ve güncel saldırı tiplerini barındırmalıdır. Çalışmalarda en çok kullanılan KDD 99 ve NSL-KDD veri setlerinin atak tipleri çeşitliliğinde günümüz şartlarını taşımaması, normal trafik senaryolarının çağımız şartlarından uzak olması ve eğitim ve test veri setlerinde dağılımlarının farklı olması bu veri setlerinin olumsuz yönleri olarak

sayılmaktadır. Literatürde de STS'lerin geliştirilmesinde güncel veri setlerinin kullanılması gerektiğinden bahsedilmektedir [48]. Bahsedilen bu sorunlara çözüm olması için son zamanlarda geliştirilen ve güncel atak tiplerini içeren UNSW-NB15 veri seti ortaya çıkmıştır.

Bu çalışmadaki amacımız ortaya çıkan bu veri setini, "Özellik Mühendisliği" tekniğini kullanarak MÖ yöntemlerinin performanslarının karşılaştırılmasını ve arttırılmasını sağlamaktır. Yukarıda bahsedilen veri setleri ve çalışmada kullanılan UNSW-NB15 veri seti bölümün devamında detaylı şekilde açıklanmıştır.

3.5.1. DARPA Veri Seti

DARPA veri seti 1998'de MT Lincoln laboratuvarlarında ağ-tabanlı bir veri seti olarak üretilmiştir. Eğitim verisi yedi haftalık ağ-tabanlı saldırıları içerirken test verisi iki haftalık ağ-tabanlı saldırıları içermektedir. Saldırı tipi olarak DoS, Probe, R2L ve U2R saldırı tiplerini içermektedir [49]. [48]'de yapmış oldukları çalışmada DARPA veri setinin gerçek dünya ağ trafiğini temsil etmediğini belirtmişlerdir.

3.5.2. KDD 99 Veri Seti

Bu veri seti DARPA veri seti temelli bir veri setidir. DoS, R2L, U2R ve probing saldırılarını benzetimi yapılmıştır. Veri seti yaklaşık 5 milyon satırdan oluşan ve yedi haftalık ağ trafiğinden oluşmaktadır. 41 özellik barındırmaktadır ve bu özellikler 3 farklı grupta; basit özellikler, trafik özellikleri ve içerik özellikleri olmak üzere sınıflandırılmışlardır. Basit özellikler TCP/IP bağlantılarından çıkarılmıştır. Trafik özellikleri iki farklı gruba ayrılmaktadır. Bunlar "same host" ve "same service" dir. İçerik özellikleri veri bölümündeki şüpheli davranışlarla ilgilenir. Bu veri seti saldırı tespit sistemlerinin değerlendirmesinde en çok kullanılan veri setlerinden birisidir [50], [51]. [52]'de yapmış oldukları çalışmada KDD 99 veri setinin anomali tespitinde düşük başarı oranları verdiğini ve bu nedenle KDD 99 veri setinin yerine güncellenmiş hali olarak bilinen NSL-KDD veri setini önermişlerdir.

3.5.3. NSL-KDD Veri Seti

NSL-KDD veri seti [48]'tarafından önerilmiştir. KDD 99 veri setindeki problemleri çözmek için oluşturulmuş bir veri setidir. Orijinal KDD 99 veri setine göre tekrarlayan ve gereksiz veri içermemektedir. KDD 99 veri setindeki mükerrer ve gereksiz kayıtlar çıkarıldığında veri sayısı 5 milyondan 150 bine kayıta kadar düşmüştür. Gelişmiş bir veri

seti oluşturulmuştur. Unutulmamalıdır ki NSL-KDD veri setindeki ağ trafik 1998 yılı öncesine aittir. Kayıtlarda düzenlemeden sonra STS'ler için daha önceden tanımlanan eğitim ve test alt setlerine bölünmüştür. NSL-KDD veri seti KDD 99 veri seti ile aynı özellik ve sınıfları barındırır. Saldırı tipi olarak DoS, R2L, U2R ve probing saldırı tiplerini hem KDD 99 veri setinde hem de bu veri setinde benzetimi yapılmıştır [50], [51], [53].

3.6. UNSW-NB15 VERİ SETİ

Var olan mevcut veri setleri ağ trafiği modern yöneliminin ve saldırı senaryolarının geniş kapsamlı bir şekilde temsil edememektedir [54]. Saldırı tespit sistemlerinin verimliliğinin arttırılması için modern, kapsamlı, günümüz şartlarına uygun, normal ve saldırı aktivitelerini içeren bir veri setine ihtiyaç vardır. Yaşanan sorunlara çözüm olması için Moustafa & Slay tarafından UNSW-NB15 veri seti yayınlanmıştır [55]. Bu çalışmada veri seti olarak UNSW-NB15 veri setini kullanıldı. Bu veri seti değişen zamanlarda yakalanan normal (saldırı içermeyen) trafik verilerinde gerçekçi aktiviteler barındırmaktadır. Veri seti 9 modern saldırı çeşidinden oluşmaktadır. Bunlara ek olarak ağ trafiğinin derinlemesine özelliklerini kapsayan paket başlığını içeren 49 özellik içermektedir. UNSW-NB15 veri seti eğitim ve test veri setleri olarak iki parçaya ayrılmıştır.

3.6.1. UNSW-NB15 Veri Seti Özellikleri ve Açıklamaları

UNSW-NB15 veri seti IXIA PerfectStorm aracı kullanılarak Avustralya siber güvenlik merkezi laboratuvarlarında hem gerçek, modern normal aktivite hem de yapay, günümüz şartlarına uygun ağ trafiği saldırı hareketlerini içeren hibrit bir model oluşturulmuştur. Tcpdump aracı ile 100 GB işlenmemiş ağ trafiği yakalanmış ve ARgus ve Bro-IDS vb. 12 araç yardımıyla model veri setindeki özellikleri çıkarmak için geliştirilmiştir [47]. Veri setinde bulunan özellikler beş gruba ayrılmış ve aşağıda sırasıyla açıklanmıştır. Akış özellikleri ve tanımları Çizelge 3.1'de, basit özellikleri ve tanımları Çizelge 3.2'de, içerik özellikleri ve tanımları Çizelge 3.3'de, zaman özellikleri ve tanımları Çizelge 3.4'de ve ek oluşturulan özellikleri ve tanımları Çizelge 3.5'de sunulmuştur.

- Akış özellikleri: Ana bilgisayarlar arasındaki (client to server, server to client) özellikleri tanımlar.
- Basit özellikler: Protokollerin bağlantılarını temsil eden özellikleri içerir.

- İçerik özellikleri: TCP/IP'nin özelliklerini içerir, ayrıca http servislerinin bazı özelliklerini de içerir.
- Zaman özellikleri: zaman özelliklerini içerir, örneğin, paketler arasındaki varış süresi, paketin başlangıç ve bitiş zamanı ve TCP protokolünün gidiş dönüş süresi.
- Ek oluşturulan özellikler: iki gruba ayrılır; (1) Protokollerin hizmetini korumak için her özelliğin kendi amacına sahip olduğu genel amaçlı özellikler. (2) Bağlantı özellikleri, son zaman özelliğinin sırasına göre 100 kayıt bağlantısının akışından oluşturulur.

Çizelge 3.1. Akış özellikleri.

NO	İSİM	TANIM
1	Srcip	Kaynak IP adres
2	Sport	Kaynak port numarası
3	Dstip	Hedef IP adres
4	Dsport	Hedef port numarası
5	proto	Protokol tipi (TCP, UDP vs)

Çizelge 3.2. Basit özellikleri.

NO	İSİM	TANIM
6	state	Durumu ve bağlı protokolleri(ACC,CLO Ve CON) gösterir.
7	dur	Kayıtlı toplam süre (duration)
8	sbytes	Kaynaktan hedef baytlara
9	Dbytes	Hedeften kaynak baytlara
10	Sttl	Kaynaktan hedefe yaşam süresi
11	Dttl	Hedeften kaynağa yaşam süresi
12	Sloss	Kaynak paketleri yeniden taransfer edildi veya drop edildi
13	Dloss	Hedef paketleri yeniden transfer edildi veya drop edildi
14	Service	http, ftp, smtp, ssh, dns gibi protokoller
15	Sload	Saniye başına kaynak bitleri
16	Dload	Saniye başına hedef bitleri
17	Spkts	Kaynaktan hedefe paket sayısı
18	Dpkts	Hedeften kaynağa paket saysı

Çizelge 3.3. İçerik özellikleri.

NO	İSİM	TANIM
19	Swin	Kaynak TPC pencere duyuru değeri
20	Driw	Hedef TPC pencere duyuru değeri
21	Stcpb	Kaynak TPC bazlı sıra numarası
22	Dtcpb	Hedef TPC bazlı sıra numarası
23	Smeanz	Kaynak tarafından iletilen akış paketi boyutunun ort.
24	Dmeanz	Hedef tarafından iletilen akış paketi boyunun ort.
25	Trans_depth	http istek/cevap işleminin bağlantısını temsil eder
26	Res_bfy_len	Sunucunun http servisinden transfer edilen verinin gerçek sıkıştırılmamış veri boyutu

Çizelge 3.4. Zaman özellikleri.

NO	İSİM	TANIM
27	Sjit	Kaynak jitter (sapma)-milisaniye
28	Djit	Hedef jitter (sapma)-milisaniye
29	Stime	Kayıt başlangıç zamanı
30	Ltime	Kayıt son zamanı
31	Sintpkt	Kaynak paketler arası varış zamanı-milisaniye
32	Dintpkt	Hedef paketler arası varış zamanı-milisaniye
33	Pcprtt	TPC bağlantı gidiş geliş zamanı kurulumu, “synack” ve “syndat” toplamı
34	Synack	TPC bağlantı kurulum zamanı, SYN ve SYN_ACK paketleri arasındaki zaman
35	Ackdat	TPC kurulum zamanı, SYN_ACK ve ACK paketleri arasındaki zaman

Çizelge 3.5. Ek Oluşturulan özellikleri.

NO	İSİM	TANIM
36	İs_am_ips_port	Eğer srcip(1) dstip'e (3) eşitse ve sport(2) dsport2qa(4) eşitse değeri 1 olarak atanır aksi halde 02dır
37	Ct_state_ttl	Sttl(10) ve dttl(11) değerlerinin belirli aralığına göre her durum (6) için numara
38	Ct_flw_http_mtld	http servisindeki"get" ve "post" gibi yöntemlere sahip akışların numarası
39	İs_ftp_login	ftp oturumuna (session) kullanıcı veya şifre tarafından erişildiyse değeri 1 değilse 101dur
40	Cy_ftp_cmd	ftp oturumunda komutu olan akış sayısı
41	Ct_srv_src	L time'a (26) göre 100 kayıt içerisinde aynı service(14) ve srcip(1) içeren kayıtların sayısı
42	Ct_srv_dts	L time'a (26) göre 100 kayıt içerisinde aynı service(14) ve dstip(3) içeren kayıtların sayısı
43	Ct_dst_ltm	L time'a (26) göre 100 kayıt içerisinde dstip(3) içeren kayıtların sayısı
44	Ct_src_ltm	L time'a (26) göre 100 kayıt içerisinde srcip(1) içeren kayıtların sayısı
45	Ct_src_sport_ltm	L time'a (26) göre 100 kayıt içerisinde aynı dsport(4) ve srcip(1) içeren kayıtların sayısı
46	Ct_dst_sport_ltm	L time'a (26) göre 100 kayıt içerisinde aynı dstip(3) ve sport(2) içeren kayıtların sayısı
47	Ct_dst_src_ltm	L time'a (26) göre 100 kayıt içerisinde aynı dstip(3) ve srcip(1) içeren kayıtların sayısı

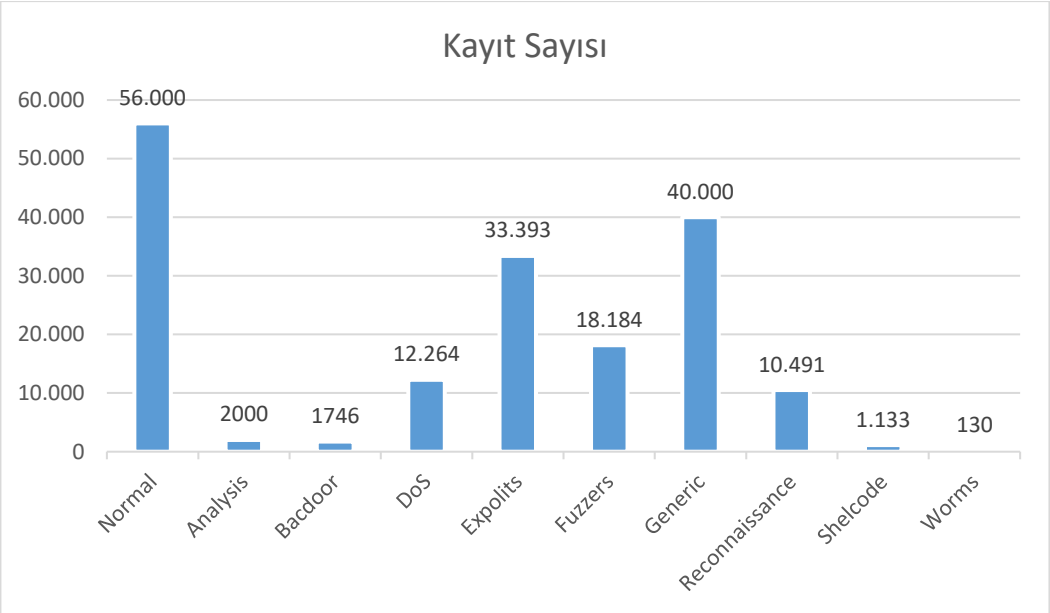
Veri setinin geliştiricileri ayrıca veri setini eğitim veri seti ve test veri seti olarak iki gruba da ayırmıştır. Bu veri seti daha sonra birçok araştırmacı tarafından da kullanılmıştır [47]. Alt örnek olarak verilen eğitim ve test veri seti Çizelge 3.6 da saldırı tiplerindeki dağılımları ile birlikte verilmiştir. Eğitim ve test veri setinin içerdikleri kayıt sayıları Şekil 3.1 ve 3.2'de gösterilmiştir. Eğitim veri seti 175,341 kayıttan, test veri seti 82,332 kayıttan oluşmaktadır. Orijinal veri seti 2,540,044 kayıttan oluşmaktadır [54]. Bu tez çalışmasında orijinal veri setinin geliştiricileri tarafından oluşturulan ve birçok araştırmacının da

çalışmalarında kullandığı eğitim ve test veri seti olarak ikiye ayrılan alt örnek veri seti kullanılmıştır. Kullanılan veri seti herhangi bir gereksiz kayıt içermemektedir.

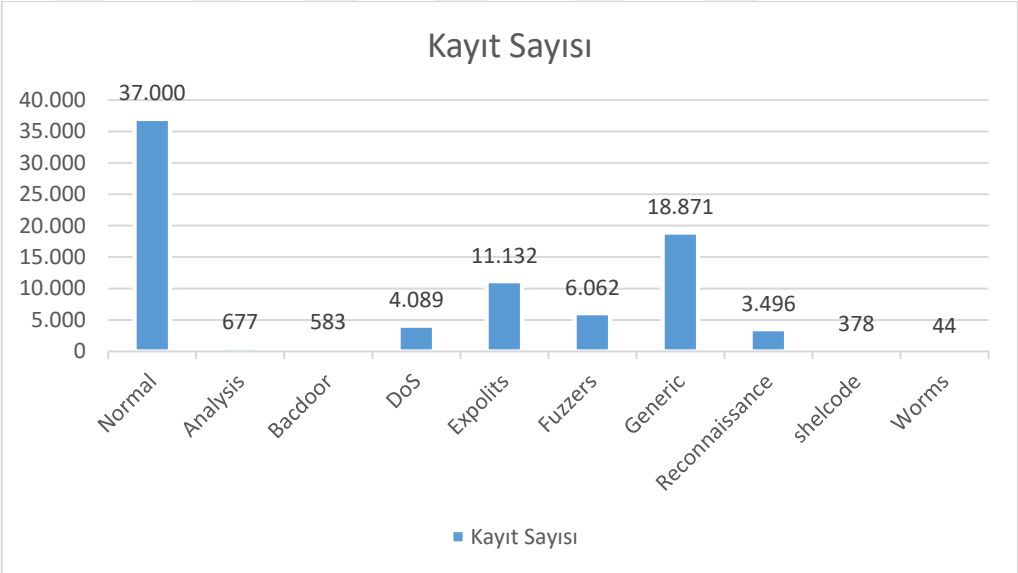
Eğitim veri seti toplam 175,342 kayıttan ve test veri seti 82,332 kayıttan oluşmaktadır. Bu iki veri setinin bölümün başında anlatılan saldırı tiplerine göre dağılımları aşağıdaki Çizelgelerde sunulmuştur.

Çizelge 3.6. Eğitim ve test veri seti saldırı tiplerine göre kayıt sayısı.

Sınıf	Eğitim Seti	Test Seti
Normal	56,000	37,000
Analysis	2,000	677
Backdoor	1,746	583
DoS	12,264	4,089
Exploits	33,393	11,132
Fuzzers	18,184	6,062
Generic	40,000	18,871
Reconnaissance	10,491	3,496
Shellcode	1,133	378
Worms	130	44
Toplam Kayıt Sayısı	175,341	82,332



Şekil 3.1. Eğitim veri seti kayıt sayısı.



Şekil 3.2. Test veri seti kayıt sayısı.

Veri setindeki saldırı tipleri dokuz farklı grupta sınıflandırılmaktadır. Bunlar;

3.6.1.1. *Fuzzers*

Saldırganın bir program, işletim sistemi veya ağdaki güvenlik boşluklarını, onu çökmesini sağlamak için büyük miktarda rastgele veri girişiyle besleyerek keşfetmeye çalıştığı bir saldırı tipidir.

3.6.1.2. *Analysis*

Bağlantı noktaları (ör., bağlantı noktası taramaları), e-postalar (ör., spam) ve web komut

dosyaları (ör., HTML dosyaları) aracılığıyla web uygulamalarına sızan bir tür saldırı tipidir.

3.6.1.3. *Backdoor*

Gizlice, normal bir kimlik yetkilendirmesini atlatma, bir cihaza uzaktan ve yetkisiz bir şekilde erişme gibi saldırıları içinde barındıran bir saldırı tipidir.

3.6.1.4. *DoS*

Meşru kullanıcıların isteklerine cevap verememesi için sunucunun kaynaklarının gereksiz yere meşgul edilmesi olayıdır. En çok görülen saldırı tipleri arasında bulunmaktadır.

3.6.1.5. *Exploit*

Ana bilgisayar veya ağ üzerinde şüphelenilmeyen bir davranışın neden olduğu aksaklık, hata ve güvenlik açıklarından yararlanan bir dizi talimatlar olarak tanımlanmaktadır.

3.6.1.6. *Generic*

Bu saldırı bir kriptografik sisteme karşı hareket eder ve güvenlik sisteminin anahtarını kırmaya çalışır.

3.6.1.7. *Reconnaissance*

Probe olarak tanımlanabilir. Güvenlik kontrollerinden kaçınmak için bilgisayar ağı hakkında bilgi toplayan saldırı tipidir.

3.6.1.8. *Shellcode*

Saldırganın, güvenliği ihlal edilmiş makineyi kontrol etmek için kabuktan (Shell) başlayarak küçük bir kod parçasına girmesiyle oluşan saldırı tipidir.

3.6.1.9. *Worm*

Saldırganın diğer bilgisayarlara yayılmak için kendini kopyaladığı bir saldırı. Genellikle, bilgisayara erişmek için hedef bilgisayardaki güvenlik hatalarına dayalı olarak kendini yaymak için bilgisayar ağını kullanır.

3.7. UYGULAMA ARAÇLARI

Veri setindeki kayıtların normal veya anormal olarak sınıflandırmasını yapan MÖ algoritmalarının benzetiminde gelişmiş bir ara yüze sahip Orange aracı kullanılmıştır. Bölümün devamında kullanılan araç tanıtılacaktır.

3.7.1. Orange

Orange, Python ile yazılmış açık kaynak, MÖ ve veri madenciliği benzetim aracıdır. Veriyi analiz edebilmek ve görselleştirmek için baştan-sona görsel programlamaya sahiptir. Bu benzetim aracı Ljubljana Üniversitesi Bilgisayar Fakültesi laboratuvarlarında geliştirilmiştir. Orange veri madenciliği veri analizi ve MÖ için bileşen-tabanlı bir görselleştirme programıdır. Bileşenleri, öğrenme algoritmalarının ve tahmin modellemenin değerlendirilmesini yapabilmek için widget olarak adlandırılan ve veri görselleştirme veri alt küme seçimi ve veri ön işleme widget'larını içinde barındırır [56], [57]. Yapılan çalışmanın benzetim aracı olarak seçilen Orange'ın ara yüzünün gelişmiş olması, MÖ algoritmalarının sınıflandırmada kullanımın kolay ve hızlı olması verinin görselleştirilmesine olanak sağlaması tercih edilmede en önemli nedenlerdendir.

3.8. VERİ ÖN İŞLEME

Saldırı tespiti yapılabilmesi için bir model oluşturulması gerekmektedir. Model oluşturulabilmesi için verinin hazırlanması gerekmektedir. Veri hazırlığının ilk adımı verilerin toplanmasıdır. Birçok MÖ yöntemi sadece sayısal veriler kullanmaktadır, ancak birçok farklı veri tipileri de mevcuttur. Bunlara kategorik veriler örnek verilebilir. Verinin kullanılan MÖ yöntemlerine uygun hale getirilmesi performans artışını beraberinde getirmektedir.

3.8.1. Kategorik Özellikler

Veri tipi olarak sayısal olmayan en yaygın tip kategorik verilerdir. Eğer yer değiştirebiliyorsa ve sırasının bir önemi yoksa bu veri kategorik veri olarak tanımlanmaktadır. Veri hem kategorik hem de sayısal olarak tercih edilebilmektedir. Haftanın günleri pazartesiden itibaren sayı ile yazılabilirken aynı zamanda haftanın günlerinin isimleri de kullanılabilir. Bu ikisi arasında seçim yapmak algoritmaların performansını etkileyebilmektedir. Elimizdeki orijinal veri setindeki kategorik olan özellikleri sayısal veri tipine dönüştürülmüştür. Yapılan değişiklikler Çizelge 3.7'de sunulmuştur.

Çizelge 3.7. Sayısala dönüştürülen ve silinen kategorik veriler.

Özellik	Tanımı	Güncellenmiş hali
Proto	Transfer protokolleri	0-4
State	Bağlı olduğu protokol	0-6
Service	http, ftp, ssh gibi protokoller	0-13
Srcip	Kaynak IP adresi	Silinmiştir
dstip	Hedef IP adresi	Silinmiştir

Bazı makine öğrenmesi algoritmaları kategorik veriyi işleyebilir ama genellikle sayısal değerlere çevrilmesine ihtiyaç vardır. Sırasının değiştiğinde herhangi bir bilgi kaybına neden olmadığı sürece kategorik veriler sayısal hale dönüştürülebilir fakat sıralama değiştiğinde farklı bir anlam ifade ederse sayısal veri şekline dönüştürülemez.

Kategorik verinin sayısal veriye dönüştürülmesi birçok MÖ yöntemi ile sağlanabilmektedir. Bunun yanı sıra karar ağaçları ve buna benzer Rassal Orman gibi bazı algoritmalar, doğal olarak kategorik verileri işleyebilmektedir. Bu algoritmaları kullanarak büyük miktarda kategorik veriyle çok daha iyi sonuçlar elde edilebilir.

3.8.2. Kayıp Veriyle Başa Çıkmak

Kayıp veri verilerin toplanması aşamasında meydana gelen ve bazı nedenlerle örneklerin ölçülememesinden kaynaklanmaktadır. İki tip kayıp veri vardır. Birincisi verinin eksik olarak ölçülmesi ki bunlar anlamlı bilgi taşıyabilir. İkincisi, ölçülmesi imkânsız olan kayıp veridir. İlk olarak bilgilendirici kayıp veriyi ele alalım. Bir sütunda kayıp verilerin olduğu gördüğünde bu sütunun da tahmin doğruluğunun arttırılması için kullanılması istenmektedir. Fakat bunun yapılabilmesi için bütün kayıp verilerin -1 veya -999 değerlerine eşitlenmesi gerekmektedir. Tabi seçilen bu değer sayısal verilerin arasındaki en uzak veri olmalıdır çünkü unutulmamalıdır ki sayısal veri için sıralama önemlidir [37].

Veri unsurunun değer yokluğu yaşandığında kendisi için herhangi bir öğreticiliği yoktur. Bunu farklı yollarla aşmanız gerekmektedir. Veri unsuru içinde değerin yokluğu durumunda, siz özel bir numara veya kategori ortaya çıkartamazsınız, çünkü sizin ortaya süreceğiniz veri tamamen yanlış olabilir. Bazı MÖ yöntemleri bilgilendirici kayıp veriyi yok sayabilmektedir. Fakat bazıları için ön işlem gerekmektedir. Bu ön işlemde ya veriyi

tamamen yok etmek ya da yerine uygun bir değer atamaktır. Eğer büyük bir veri setiniz varsa ve kayıp değerleriniz küçük miktarda ise onları elimine etmek en basit yaklaşımdır. Fakat elinizdeki veri setinin büyük bir kısmını kayıp veriler oluşturmakta ise bunların elimine edilmesi modelinizin tahmin oranını düşürebilecektir [37].

Bu çalışmada kullanılan veri setinde kayıp veriler bulunmaktadır. Kayıp verilerin bulunduğu özellikler Çizelge 3.18'de sunulmuştur. Kayıp verilerle başa çıkabilmek için iki yöntem önerilmektedir. Birincisi, kayıp verilerin olduğu özelliği veri setinden çıkarmak. İkincisi, kayıp verileri tamamlayarak, bulunduğu özelliği veri seti içerisinde tutmak. Bu iki çözümün hangisinin algoritma performanslarını arttırdığını bulmak için iki yöntem de denenmiştir. Elimizdeki kayıp veri sayısının fazla olduğu bir özellik veri setinden silinmiş ve performans sonuçlarını kaydedilmiştir. Bu sütundaki kayıp verilere uygun değerler atayarak performans sonuçları kaydedilmiştir. İki farklı çalışmada kayıt altına alınan sonuçlar karşılaştırılmış ve kayıp verilerin tamamlanması ile kayıp verilerin olduğu özelliğin silinmesi arasında %0,2'lik bir doğruluk performans yükselişi elde edilmiştir. Bu nedenlerle çalışmada, kayıp verilerin olduğu özellikleri tamamlama yöntemi kullanılmıştır.

Çizelge 3.8. Kayıp veri bulunan özellikler.

Service (80.000 ad.)
Proto (15 ad.)
State (15.)

3.8.3. Özellik Mühendisliği

UNSW-NB15 veri seti toplam 49 özellik ve 1 hedef değere sahiptir. UNSW-NB15 veri setinden oluşturulan alt veri setinden 7 özellik çıkarılmıştır. Bu 7 özelliğin tanımları ve veri setinden çıkarılma nedenleri Çizelge 3.9'da sunulmuştur.

Çizelge 3.9. Orijinal veri setinden çıkarılan özellikler.

Özellik	Tanımı	Neden çıkarıldığı
Srcip	Kaynak IP adresi	Küresel bir değer değil
Sport	Kaynak port numarası	Her defasında değişebilir
Dstip	Hedef IP adresi	Küresel bir değer değil
Sdport	Hedef port numarası	Her defasında değişebilir

Çizelge 3.9. (devam) Orijinal veri setinden çıkarılan özellikler.

Stime	Başlama zaman kayıt	MÖ için bir anlam ifade etmez
ltime	Bitiş zaman kayıt	MÖ için bir anlam ifade etmez
Attack_cat	Saldırı tiplerinin isimleri	Hedef etiket ile aynıdır

Bu çalışmada veri setinin 42 özelliğinin tamamının bulunduğu durum Orijinal veri seti olarak adlandırılmıştır. Literatürde puanlama yöntemi (scoring method) olarak bilinen ReliefF yöntemi kullanılarak orijinal veri setinde 42 olan özellik sayısı 29'a düşürülmüştür. Özellik sayısının azaltılmış olduğu veri setin özellik seçimi yapılmış veri seti olarak adlandırılmıştır. 42 özellik içinden seçilen 29 özellik ve ReliefF puanlama yöntemine göre sıralaması Şekil 3.3'de sunulmuştur.

	#	ReliefF
xServ		0.255
dttl		0.127
ct_dst_sport_ltm		0.071
dload		0.049
ct_state_ttl		0.043
is_sm_ips_ports	2	0.040
sinpkt		0.038
smean		0.037
dur		0.025
dmean		0.022
sttl		0.022
ct_srv_dst		0.020
ct_srv_src		0.019
rate		0.019
ct_dst_src_ltm		0.018
ct_dst_ltm		0.016
ct_src_ltm		0.016
ct_src_dport_ltm		0.014
dinpkt		0.014
sload		0.011
dtcpb		0.011
stcpb		0.009
xProt		0.009
ct_ftp_cmd		0.008
is_ftp_loqin		0.008
tcprtt		0.005
ackdat		0.005
synack		0.003
ct_flw_http_mthd		0.003

Şekil 3.3. RelieF puanlama yöntemine göre seçilen 29 özellik.

3.9. PERFORMANS DEĞERLENDİRME METRİKLERİ

Sınıflandırma Algoritmaları ikili (binary) veya ikiden fazla (multiclass) değeri sınıflandırmayı amaçlamaktadır. Bu sınıflandırmanın doğruluk oranları ve hataların çıktılarının değerlendirilmesi için bazı metrikler kullanılmaktadır. Bunların arasında ön planda olan doğruluk (accuracy) değerlendirme metriğidir [58]. Bu tez çalışmasında doğrulukla beraber duyarlılık, hassasiyet ve F-1 skor değerlendirme metriği olarak kullanılmıştır.

3.9.1. Karmaşıklık Matrisi

Sınıflandırma modelinin sonuçlarını değerlendirmek için kullanılır. Olması gereken ve tahmin edilen değerler arasındaki hataların incelenmesine olanak sağlar. Çizelge 3.10'da gösterilen ikili sınıflandırma için kurulmuş bir modelin karmaşıklık matrisidir.

Çizelge 3.10. Karmaşıklık matrisi.

<table>
<tr><td colspan="2" rowspan="2"></td><td colspan="2">Gerçek Sonuçlar</td></tr>
<tr><td>Pozitif (1)</td><td>Negatif (0)</td></tr>
<tr><td rowspan="2">Tahminlenen Sonuçlar</td><td>Pozitif (1)</td><td>TP [1,1]
Gerçek Pozitif</td><td>FP [1,0]
Yanlış Pozitif</td></tr>
<tr><td>Negatif (0)</td><td>FN [0,1]
Yanlış Negatif</td><td>TN [0,0]
Gerçek Negatif</td></tr>
</table>

Bir örnek; elimizdeki veri setine göre 10 tane sınıflandırılmayı bekleyen ağ trafiği vardır. Veri setine göre bu 10 tane ağ trafiğinin 5 tanesi saldırı yani 1 olarak, 5 tanesi de normal trafik yani 0 olarak temsil edilmektedir. Yapılan sınıflandırma sonucunda saldırı olarak 6 adet, normal trafik olarak da 4 adet sonuç bulduğumuzu düşünürsek burada TP: 5, FN:0 FP:1, TN:4 olarak karmaşıklık matrisimizde elde edeceğiz.

TP ve TN: Sınıfların doğru tahmin edildiği rakamı verir.
FN ve FP: Sınıfların birbiri ile olan yanlış tahmin adetlerini verir [58].

3.9.2. Doğruluk

Doğruluğun skoru aşağıdaki gibi hesaplanmaktadır. Doğruluk skoru 0-1 arasında bir değer almaktadır ve 1'e yaklaşan skorlar başarılı kabul edilmektedir [58].

Doğruluk metriği kullanılırken doğru sonuçlar alınabilmesi için veri setinin dengeli bir dağıtıma sahip olması gerekmektedir. Örneğin %90 saldırı verisi içeren bir veri setinde %10 olan normal olan trafik yanlış ölçülse bile doğruluk oranımız %90 olacaktır. Bu nedenle dengesiz veri setlerine bölümün devamında açıklayacağımız değerlendirme metrikleri kullanılmalıdır. Denklem 3.1'de Doğruluk metriği hesaplama biçimi gösterilmiştir.

3.9.3. Duyarlılık - Hassasiyet ve F-1 Skor

Uygulamada kullanılan diğer performans değerlendirme metrikleri ve hesaplanma biçimleri aşağıda gösterilmiştir. Denklem 3.2'de Duyarlılık, Denklem 3.3'de Hassasiyet, Denklem 3.4'de F1-Skor hesaplama formülleri yer almaktadır.

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

$$Duyarlılık: \frac{TP}{TP + FN} \tag{3.2}$$

$$Hassasiyet: \frac{TP}{TP + Fp} \tag{3.3}$$

$$F1 - Skoru: \frac{2(Hassasiyet * Duyarlılık)}{(Hassasiyet + Duyarlılık)} \tag{3.4}$$

4. DENEYSEL ÇALIŞMA

Bu çalışmada kullanılan algoritmalar Intel(R) Core (TM) i5-9400 CPU @ 2.90GHz, 8 GB RAM özelliklere sahip bilgisayarda test edilmiştir. Algoritmaların benzetimi Orange aracı ile gerçekleştirilmiştir.

4.1. ÇALIŞMADA KULLANILAN MAKİNE ÖĞRENMESİ ALGORİTMALARI

Bu tez çalışmasında, denetimli MÖ algoritmaları kullanılmıştır. Denetimli MÖ algoritmalarında, hedefin belirlenmesi için etiketli eğitim verisi kullanılmaktadır. Etiketli veri ile eğitim aşaması tamamlandıktan sonra test veri seti ile performans ölçümleri yapılmaktadır. Saldırı tespitinin belirlenmesinde kullanılan bu algoritmalar aşağıda sırayla verilmiştir.

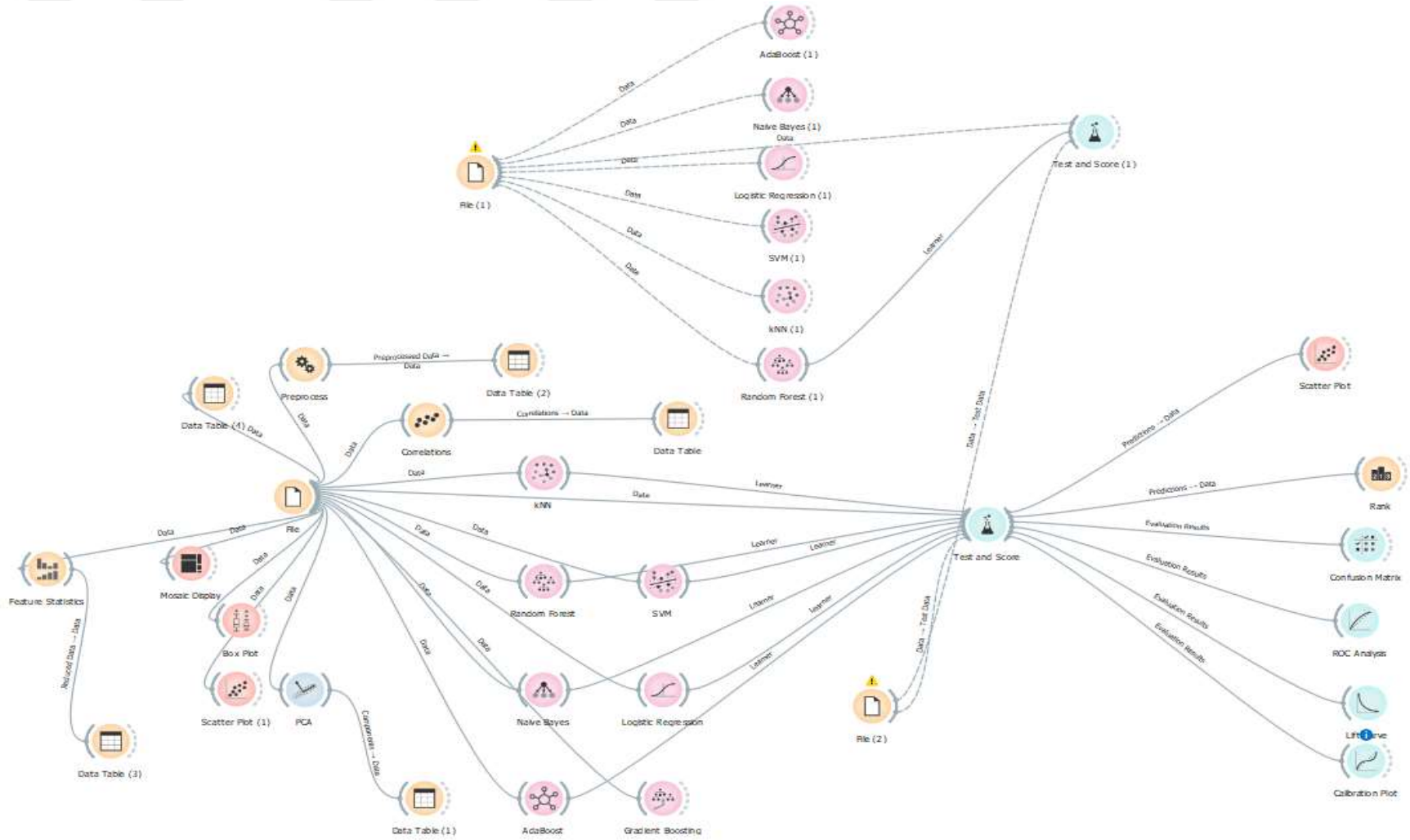
- K-En Yakın Komşu
- Rassal Orman
- Adaboost
- Lojistik Regresyon
- Naive Bayes
- Destek Vektör Makineleri
- Sinir Ağları

4.2. UYGULAMA

Bu çalışmada dört farklı senaryo gerçekleştirilmiştir. Senaryolar kullanılan veri setindeki özellik sayısı ve test veri setinin oluşturulması farklarına dayanarak dört farklı şekilde gerçekleştirilmiştir. Kullanılan veri setinde, hedef etiketi ve 42 özellik bulunmaktadır. Veri setinin orijinal hali ve ReliefF puanlama yöntemi kullanılarak özellik seçimi yapıldıktan sonraki hali olmak üzere iki farklı senaryo kullanılmıştır. Test veri seti seçiminde iki farklı yöntem olmak üzere iki farklı senaryo kullanılmıştır. Birincisi, eğitim veri seti ve test veri seti bağımsız oluşturulmuştur. İkincisi, eğitim veri setinin %20'si test veri seti olarak ayrılmıştır. Orange aracı kullanılarak MÖ algoritmalarının benzetimi yapılmış ve elde edilen sonuçlar bölümün devamında sunulmuştur. Orange aracı

kullanılarak oluşturulan çalışmanın ana görünümü Şekil 4.1'de sunulmuştur.

UNSW-NB15 veri seti eğitim ve test veri seti olarak iki farklı kategoriye ayrılmıştır. Eğitim veri setinin tamamı eğitim için, test veri setinin tamamı da modeli test etmek için kullanılmaktadır. Test veri seti iki farklı şekilde oluşturulabilir. Birincisi, eğitim veri setinin belli bir oranının test veri setini oluşturmak için kullanılması. İkincisi, eğitim veri setinden bağımsız bir veri seti oluşturulmasıdır. Test veri setinin bağımlı (eğitim veri seti içerisinden belli oranda) oluşturulması durumlarında elde edilen sonuçların bağımsız (eğitim veri setinden bağımsız) olarak oluşturulan test veri setlerine göre değerlendirme metriklerinde daha yüksek sonuçlar vermektedir. Bu durum bağımlı veri setlerinin test aşamalarında daha iyi bir seçenek olarak algılanmamalıdır. Bağımlı oluşturulan test veri setlerinde aşırı uyma (over-fitting) meydana gelebilmektedir. Bu çalışmada, test veri seti oluşturulurken, bağımlı ve bağımsız olmak üzere iki yöntem de kullanılmıştır.



Şekil 4.1. Çalışmanın ana şablonu.

4.2.1. Senaryo 1: Orijinal Veri Seti – Test Veri Seti Bağımlı

Senaryo 1'de özellik seçimi yapılmaksızın 42 özelliğe sahip orijinal veri seti kullanılmıştır. Kullanılan MÖ yöntemlerine dört farklı kategoride performans değerlendirilmesi yapılmıştır. Senaryo 1'in sonuçları değerlendirilirken test veri setinin seçiminde, eğitim veri setinin %20'si test veri seti olarak ayrılmıştır. Elde edilen sonuçlar Çizelge 4.1'de verilmiştir. Elde edilen sonuçlar doğruluk oranı açısından çalışmadaki en yüksek seviyeye ulaşmıştır. Bunun ana nedeni test veri setinin eğitim veri seti içerisinden oluşturulmuş olması aşırı uyma meydana gelmiş olabileceği düşündürmektedir.

Çizelge 4.1. Orijinal veri seti-test veri seti bağımlı.

MÖ Algoritması	Doğruluk	Hassasiyet	Duyarlılık	F-1 Skor
Adaboost	0.957	0.957	0.957	0.957
Rassal Orman	0.956	0.956	0.956	0.956
Sinir Ağları	0.948	0.948	0.948	0.948
K-En Yakın Komşu	0.893	0.892	0.892	0.893
Lojistik Regresyon	0.851	0.842	0.858	0.851
Naive Bayes	0.760	0.768	0.830	0.760
DVM	0.514	0.510	0.682	0.514

4.2.2. Senaryo 2: Orijinal Veri Seti – Test Veri Seti Bağımsız

Senaryo 2'de özellik seçimi yapılmaksızın 42 özelliğe sahip orijinal veri seti kullanılmıştır. Kullanılan MÖ yöntemleri dört farklı kategoride performans değerlendirilmesine tabi tutulmuştur. Senaryo 2'nin sonuçlarını değerlendirilirken test veri seti seçiminde, 175 bin kayıta sahip eğitim veri seti ve 82 bin kayıta sahip test veri seti bağımsız şekilde kullanılmıştır. Elde edilen sonuçlar Çizelge 4.2'de verilmiştir. Elde edilen sonuçlara göre en yüksek doğruluk oranına Rassal Orman ulaşmıştır. Senaryo 1'e göre sonuçlardaki değişimin ana nedeni test veri setinin eğitim veri setinden bağımsız bir şekilde elde edilmesidir.

Çizelge 4.2. Orijinal veri seti-test veri seti bağımsız.

MÖ Algoritması	Doğruluk	Hassasiyet	Duyarlılık	F-1 Skor
Rassal Orman	0.867	0.864	0.883	0.867
Sinir Ağları	0.856	0.852	0.872	0.856
Adaboost	0.856	0.851	0.876	0.856
K-En Yakın Komşu	0.783	0.773	0.808	0.783
Naive Bayes	0.751	0.751	0.766	0.751
Lojistik Regresyon	0.706	0.676	0.765	0.706
DVM	0.449	0.297	0.474	0.449

4.2.3. Senaryo 3: Özellik Seçimi – Test Veri Seti Bağımlı

Senaryo 3'de ReliefF puanlama yöntemi kullanılarak özellik seçimi yapılmıştır. Orijinal hali 42 olan özellik sayısı 29'a indirilmiştir. Senaryo 3'de özellik seçimi yapılmış olan veri seti kullanılmıştır. Kullanılan MÖ yöntemlerine dört farklı kategoride performans değerlendirmesi yapılmıştır. Senaryo 3'ün sonuçları değerlendirilirken test veri setinin seçiminde, eğitim veri setinin %20'si test veri seti olarak ayrılmıştır. Elde edilen sonuçlar Çizelge 4.3'de verilmiştir. Senaryo 3 ile Senaryo 1 arasındaki tek fark kullanılan özellik sayısıdır. Senaryo 1'de 42 olan özellik sayısı 29'a düşürülmüştür. Test veri seti oluşturulma şekli aynıdır. Senaryo 1 ile kıyaslandığında elde edilen sonuçlara göre her bir performans değerlendirme kriterinde de artış olmuştur. Algoritmaların sınıflandırma zamanlarında azalma meydana gelmiştir. Bunun ana sebebi özellik sayısının 42'den 29'a düşürülmesidir. Performanstaki artışın bir diğer nedeni Özellik seçimi yaparken kullanılan ReliefF yönteminin özellik seçimindeki başarısıdır.

Çizelge 4.3. Orange-özellik seçimi -test veri seti bağımlı.

MÖ Algoritması	Doğruluk	Hassasiyet	Duyarlılık	F-1 Skor
Rassal Orman	0.955	0.955	0.955	0.955
Adaboost	0.955	0.955	0.955	0.955
Sinir Ağları	0.947	0.947	0.947	0.947
K-En Yakın Komşu	0.893	0.892	0.892	0.893

Çizelge 4.3. (devam) Orange-özellik seçimi -test veri seti bağımlı.

Lojistik Regresyon	0.842	0.834	0.843	0.842
Naïve Bayes	0.815	0.820	0.846	0.815
DVM	0.458	0.431	0.676	0.458

4.2.4. Senaryo 4: Özellik Seçimi – Test Veri Seti Bağımsız

Senaryo 4'de ReliefF puanlama yöntemi kullanılarak özellik seçimi yapılmıştır. Orijinal hali 42 olan özellik sayısı 29'a indirilmiştir. Senaryo 4'de özellik seçimi yapılan bu veri seti kullanılmıştır. Kullanılan MÖ yöntemlerine dört farklı kategoride performans değerlendirilmesi uygulanmıştır. Senaryo 4'ün sonuçları değerlendirilirken test veri setinin seçiminde, 175 bin kayıta sahip eğitim veri seti ve 82 bin kayıta sahip test veri seti bağımsız şekilde kullanılmıştır. Elde edilen sonuçlar Çizelge 4.4'de verilmiştir. Senaryo 4 ile Senaryo 2 arasındaki tek fark kullanılan özellik sayısıdır. Senaryo 1'de 42 olan özellik sayısı 29'a düşürülmüştür. Test veri seti oluşturma şekli aynıdır. Senaryo 2 ile kıyaslandığında elde edilen sonuçlara göre her bir performans değerlendirme kriterinde artış olmuştur. Bunun ana sebebi özellik sayısının 42'den 29'a düşürülmesidir. Performanstaki artışın bir diğer nedeni Özellik seçimi yaparken kullanılan ReliefF yönteminin özellik seçimindeki başarısıdır.

Çizelge 4.4. Orange-özellik seçimi yapılmış-test veri seti bağımsız.

MÖ Algoritması	Doğruluk	Hassasiet	Duyarlılık	F-1 Skor
Sinir Ağları	0.948	0.856	0.877	0.862
Rassal Orman	0.873	0.870	0.889	0.873
Adaboost	0.862	0.858	0.880	0.862
K-En Yakın Komşu	0.783	0.774	0.808	0.783
Naive Bayes	0.751	0.751	0.766	0.751
Lojistik Regresyon	0.706	0.676	0.765	0.706
DVM	0.449	0.297	0.474	0.449

4.3. SONUÇLARIN KARŞILAŞTIRILMASI

Senaryoların uygulanması sonrasında elde edilen sonuçların doğruluk performans karşılaştırmaları Çizelge 4.5'de sunulmuştur. Sonuçlara göre özellik seçiminin yapılması test veri setinin bağımsız oluşturulduğu senaryolarda doğruluk performansını arttırmıştır. Test veri setinin bağımsız olarak kullanılması doğruluk performansını düşürmüştür.

Çizelge 4.5. Senaryoların doğruluk performanslarının karşılaştırılması.

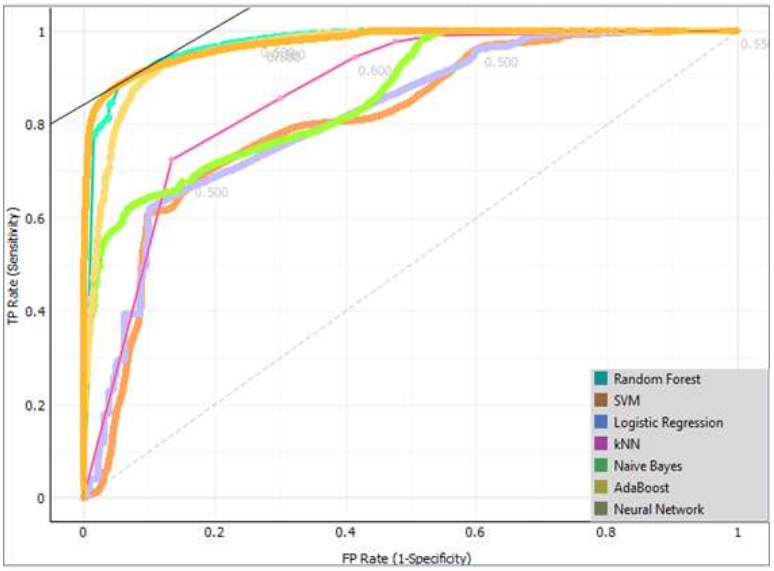
MÖ Algoritması	Senaryo-1	Senaryo-2	Senaryo-3	Senaryo-4
Rassal Orman	0.956	0.867	0.955	0.873
Adaboost	0.957	0.856	0.955	0.862
Sinir Ağları	0.948	0.947	0.947	0.862
K-En Yakın Komşu	0.893	0.783	0.893	0.783
Naive Bayes	0.760	0.751	0.815	0.751
Lojistik Regresyon	0.851	0.706	0.842	0.706
DVM	0.514	0.449	0.458	0.449

Özellik seçimi yaparak elde ettiğimiz sonuçlarda en yüksek doğruluk oranına ulaşan Rassal Orman (Random Forest) yönteminin karmaşıklık matrisi Şekil 4.2'de gösterilmiştir.

	0	1	∑
0	27412	9588	37000
1	870	44462	45332
∑	28282	54050	82332

Şekil 4.2. Rassal Orman karmaşıklık matrisi.

Özellik seçimi yaparak elde edilen sonuçların ROC grafiği Şekil 4.3'de gösterilmiştir. ROC, işlem karekteristik eğrisi (Receiver Operating Characteristics) olup AUC (Area Under Curve) ise bu eğrinin altında kalan alan anlamına gelmektedir. ROC grafiği MÖ modellerinin performanslarının değerlendirilmesinde etkili bir yöntemdir.



Şekil 4.3. ROC grafiği.

4.4. SONUÇLARIN GÜNCEL ÇALIŞMALAR İLE KARŞILAŞTIRILMASI

Elde edilen sonuçlar ve literatürde elde edilen sonuçlar bu bölümün devamında tartışılmıştır.

[17]'de yapılan çalışmada UNSW-NB15 veri setini kullanmışlardır. Ön işleme tekniği ile beraber Özellik Seçimi yapmışlardır. Çalışmalarında MÖ yöntemlerinden "Sinir Ağları" algoritmasını kullanılmıştır. Elde ettikleri sonuçlar ve bu tez çalışmasındaki sonuçlar Çizelge 4.6'de sunulmuştur. [17]'de yapmış oldukları çalışma ile bu çalışmada arasındaki fark özellik Seçimi yaparken kullanılan puanlama yönteminin farklı olmasıdır. Bu tez çalışmasında puanlama yöntemi olarak ReliefF yöntemi kullanılmış ve özellik sayısı 29'a düşürülmüştür. [17]'de yapmış oldukları çalışmada ise Gain Ratio puanlama yöntemi kullanılmış ve özellik sayısı 30'a düşürülmüştür. Senaryo 4 ile karşılaştırıldığında daha düşük doğruluk ve hassasiyet değerine ulaşmıştır. ReliefF yönteminin seçtiği özelliklerin algoritma performanslarını yükseltici etkisinin olduğu görülmüştür.

Çizelge 4.6. Önerilen yöntem ve [17]'deki çalışmanın karşılaştırılması.

	Doğruluk (%)	Hassasiyet
[17]	76.96	0.798
Önerilen yöntem	94.8	0.856

[6]'da 2020 yılında yapılan çalışmada UNSW-NB15 veri setini kullanarak MÖ algoritmalarının sınıflandırma performanslarını analiz etmişlerdir. Test veri setini oluştururken eğitim veri setinin %20'si kullanılmıştır. Yapılan çalışmada 42 özellik sayısına sahip orijinal veri seti kullanılmıştır. Bu tez çalışmasındaki sonuçlar ve [6]'da yapmış oldukları çalışmanın sonuçlarının performanslarının karşılaştırmaları Çizelge 4.7'de sunulmuştur. Senaryo 1 ile karşılaştırıldığında, Senaryo 1 Rassal Orman ve Naive Bayes algoritmalarında daha yüksek sonuçlar elde etmiş fakat diğer algoritmalarda daha düşük sonuçlar elde etmiştir. iki çalışma arasındaki fark 49 olan özellik sayısının MÖ algoritmaları tarafından kullanılabilecek olan özelliklerin seçilmesi ve dönüştürülmesi sırasında farklı özelliklerin oluşmasıdır.

Çizelge 4.7. Önerilen yöntem ve [6]'daki çalışmanın karşılaştırılması.

	MÖ Yöntemi	Doğruluk	Hassasiyet	Recall	F1-Skoru
[6]	LR	93.23	0.92	0.99	0.95
Önerilen Yöntem		84.20	0.843	0.842	0.834
[6]	NB	48.03	1.00	0.23	0.38
Önerilen Yöntem		81.50	0.846	0.815	0.820
[6]	RO	95.43	0.96	0.97	0.97
Önerilen Yöntem		95.60	0.955	95.50	95.50
[6]	KNN	93.71	0.94	0.96	0.95
Önerilen Yöntem		83.9	0.892	0.893	0.892

[16]'da yapmış oldukları çalışmada UNSW-NB15 veri seti kullanılmıştır. Yaptıkları çalışmadan yeni bir Ağ STS modellemişlerdir. Çalışmalarının deneysel sonuçlarında ise, Lojistik Regresyon %83.15, Naive Bayes %81.2, Yapay Sinir Ağı %81.5. [16]'da yapmış oldukları çalışmanın sonuçlarının performanslarının karşılaştırmaları Çizelge 4.8'de

sunulmuştur Hazır olarak sunulan eğitim/test veri setlerini kullanmak yerine veri setinin tamamı kullanılmıştır. Tam veri seti dört farklı CSV dosyası olarak bulunmaktadır. Tam veri seti ve eğitim/test veri seti olarak hazırlanan veri setleri arasında bazı farklılıklar vardır. Bunlar gereksiz kayıtsızların varlığı ve lokal IP adreslerinin bulunması olarak örneklendirilebilir.

Çizelge 4.8. Önerilen yöntem ve [16]'daki çalışmanın doğruluk performans karşılaştırılması.

Algoritmalar	Önerilen Yöntem	[16]
LR	0.842	0.8315
NB	0.815	0.812
SA	0.856	0.815

5. SONUÇLAR VE ÖNERİLER

5.1. SONUÇ

İnternet 21.yy'ın en hızlı gelişen teknolojisi olarak kabul edilmektedir. Özellikle salgın hastalık (pandemi) koşullarında fiziksel temasın minimuma indirilmesi bu gelişimi hızlandırmıştır. İnternetin yaygınlaşması bazı sorunları da beraberinde getirmiştir. Bunlardan en önemlisi güvenlik sorunlarıdır. Geleneksel güvenlik önlemlerinin yanında Saldırı Tespit Sistemleri (STS) gibi gelişmiş güvenlik önlemleri kullanılmaya başlamıştır. STS'ler ağ trafiğinde bir aktivitenin anomali mi yoksa normal bir trafik mi olduğuna karar veren yapılardır. Aktivitenin anomali olup olmadığına karar vermesinde MÖ algoritmaları ve algoritmaları eğiten veri setleri çok etkindir.

Bu çalışmada etkili ve verimli bir STS geliştirmek için kullanılan, güncel bir veri seti olan UNSW_NB15 veri setiyle eğitilen MÖ algoritmalarının performans değerlendirmesini yapılmıştır. Önerilen yöntem diğer yöntemlerde ReliefF puanlama yöntemi kullanarak özellik sayısı azaltılması yönünden ayrılmaktadır. Karşılaştırma yapılan diğer çalışmalara göre özelliklerin belirlenmesinde kullanılan yöntem farklılığı sağlamış ve daha iyi performans değerleri elde edilmiştir.

Bu çalışmada dört farklı senaryo uygulanmıştır. Sonuçlar, senaryoların kendi arasında ve literatürdeki benzer çalışmalarla karşılaştırılmıştır. Senaryoların farklılıklarının nedeni, kullanılan veri setinde özellik seçimi yapılıp yapılmaması ve test veri setinin oluşturulma yöntemidir. Literatürde son zamanlarda kullanılan veri seti UNSW-NB15 kullanılarak MÖ algoritmaları eğitilmiştir. Eğitilen MÖ algoritmaları, senaryolara uygun test veri seti ile değerlendirilip sonuçlar elde edilmiştir. Senaryoları kendi arasında değerlendirildiğinde en yüksek doğruluk performansına sahip algoritma "Rassal Orman" olmuştur. Sonuçların literatürde benzer çalışmalara göre daha yüksek performans değerleri elde ettiği gözlemlenmiştir. Bu durumun sebebi özellik seçimi yaparken ReliefF puanlama yönteminin kullanılmasıdır.

5.2. ÇALIŞMANIN GETİRDİĞİ KATKILAR

STS'ler modellenirken anomali tespitinin yapılması sırasında en uygun algoritmanın bulunması ve algoritmanın güncel saldırı tiplerini içeren bir veri seti ile eğitilmesi gerekmektedir. Literatür 'de STS modellenirken kullanılan veri setlerinin güncel olmadığı ve günümüz şartlarını sağlayan bir veri seti kullanılmasının STS'lerin veriminin yükselmesine katkı sağlamıştır.

Veri setinde, özellik seçimi yaparken kullanılan yöntemlerin algoritmaların performanslarına etkisi vardır. Özellik sayısının doğru oranda azaltılması ve seçilen özelliklerin performansa etkisi göz önüne alınarak seçimler yapılmıştır. Özellik seçiminde ReliefF puanlama yöntemi kullanılması literatüre katkı sağlamıştır.

5.3. TARTIŞMA VE ÖNERİLER

Tez çalışmasında kullanılan veri seti ve MÖ algoritmalarının performans sonuçlarından faydalanarak gelecekte yapılabilecek çalışmalara yol göstermek üzere aşağıdaki öneriler sunulmaktadır:

Bu çalışmada elde edilen sonuçlara göre dört farklı senaryoda da en yüksek doğruluk değerine "Adaboost" algoritması sahip olmuştur. Nİ cihazlarının internet ağına katılımının artması ve Nİ cihazlarının heterojen bir yapıya sahip olması saldırı tiplerine göre algoritmaların performanslarının değişmesine sebep olmaktadır. Her bir saldırı tipi için farklı algoritma daha iyi sonuçlar elde edebilmektedir. İnternetin heterojen yapısından dolayı gelecek çalışmalarda birden fazla algoritmayı bir araya getirip sonuçlar üreten, Birliktelik Kural Çıkarımı (BKÇ) ve Topluluk Öğrenimi (TÖ) gibi makine öğrenmesi yöntemlerinin kullanılarak sınıflandırmada çok daha yüksek doğruluk oranlarına ulaşılabilir.

6. KAYNAKLAR

[1] S. Sarkar, S. Chatterjee ve S. Misra, "Assessment of the suitability of fog computing in the context of ınternet of things," *IEEE Translation Cloud Computer*, c. 6, sayı 1, ss. 46–59, 2018.

[2] T. Fırlar, "AG güvenligi" *Sakarya Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, c. 7, sayı 1, ss. 9-16, 2003.

[3] A. Chowdhury, G. Karmakar ve J. Kamruzzaman, "The Co-evolution of Cloud and IoT Applications," Toronto, Kanada, 2019, ss. 213–234.

[4] İTÜ. (2021, 16 Eylül). *Statistics* [Online]. Erişim: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[5] D. Joo, T. Hong ve I. Han, "The neural network models for IDS based on the asymmetric costs of false negative errors and false positive errors" *Pergamon*, c. 1, sayı 25, ss. 69-75, 2003.

[6] G. Kocher ve G. Kumar, "Performance analysıs of machıne learnıng classıfıers for ıntrusıon detectıon usıng UNSW-NB15 Dataset," *International Conference on Signal and Image Processing (SIGI 2020),* Chennai, Hindistan, ss. 31–40, 2020

[7] R. Von Solms ve J. Van Niekerk, "From information security to cyber security," *Computers & Security*, c. 38, sayı 1, ss. 97–102, 2013.

[8] Ç. Kaya ve O. Yildiz, "Makine öğrenmesi teknikleriyle saldırı tespiti: karşılaştırmalı analiz," *Marmara Fen Bilimleri Dergisi*, c. 3, ss. 89–104, 2014.

[9] C. Kaya, F. S. Bulut, H. Fırat, G. Karataş, Ö. K. Şahingöz , "Saldırı tespit sistemlerinde makine öğrenmesi modellerinin karşılaştırılması," *Journal of Science and Technology*, c. 12, sayı 3, ss. 1513–1525, 2019.

[10] Ç. Özer ve M. Takaoğlu, "Saldırı tespit sistemlerine makine öğrenme etkisi, The effect of machıne learnıng on ıntrusıon detectıon systems," *International Journal of Management Information Systems and Computer Science*, c. 20, sayı 1, ss. 11–22, 2019.

[11] S. Özekes ve E. N. Karakoç, "Makine öğrenmesi yöntemleriyle anormal ağ trafiğinin tespit edilmesi." *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, c. 7, sayı 1, ss. 566-576, 2019.

[12] M. C. Belavagi ve B. Muniyal, "Performance evaluation of supervised machine learning algorithms for ıntrusion detection," *Procedia Computer Sciencei*, c. 89, ss. 117–123, 2016.

[13] Y. El, A. Toumanarı, A. Bouırden ve N. El, "Intrusion detection techniques in wireless sensor network using data mining algorithms: Comparative evaluation based on attacks detection," *International Journal of Advanced Computer Science and Applications*, c. 6, sayı 9, 2015.

[14] P. Sangkatsanee, N. Wattanapongsakorn, and C. Charnsripinyo, "Practical real-time intrusion detection using machine learning approaches," *Computer Communications*, c. 34, sayı 18, ss. 2227–2235, 2011.

[15] W. L. Al-Yaseen, Z. A. Othman ve M. Z. A. Nazri, "Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system," *Expert Systems Applications*, c. 67, ss. 296–303, 2017.

[16] L. Zhiqiang, G. Mohi-Ud-Din, L. Bing, L. Jianchao, Z. Ye ve L. Zhijun, "Modeling network ıntrusion detection system using feed-forward neural network using UNSW-NB15 dataset," *Proceedings of 2019 the 7th International Conference on Smart Energy Grid Engineering*, c. 7, ss. 299–303, 2019.

[17] J. O. Mebawondu, O. D. Alowolodu, J. O. Mebawondu ve A. O. Adetunmbi, "Network intrusion detection system using supervised learning paradigm," *Scientific African*, c. 9, ss. 497-517, 2020.

[18] G. Kocher ve G. Kumar, "Analysis of machine learning algorithms with feature selection for intrusion detection using UNSW-NB15 dataset," *İnternational Journal Of Network Security & Its Applications Impact Factor*, c. 13, sayı 1, 2021.

[19] G. Canberk. (2021, 18 Eylül). *Klavye dinleme ve önleme sistemleri analiz, tasarım ve geliştirme.* [Online]. Erişim: https://tezarsivi.com/klavye-dinleme-ve-onleme-sistemleri-analiz-tasarim-ve-gelistirme.

[20] G. Canbek ve Ş. Sağıroğlu, "Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme," *Politeknk Dergisi*, c. 9, sayı 3, ss. 165–174, 2006.

[21] K. Kristopher ve R. Kendall. (2021,18 Mart). *A database of computer attacks for the evaluation of intrusion detection systems* [Online]. Erişim: https://dspace.mit.edu/handle/1721.1/9459.

[22] N. Hoque, M. H. Bhuyan, R. C. Baishya, D. K. Bhattacharyya ve J. K. Kalita, "Network attacks: Taxonomy, tools and systems," *The Journal of Network and Computer Applications*, c. 40, sayı 1, ss. 307–324, 2014.

[23] M. Ahmed, A. Naser Mahmood ve J. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, c. 60, ss. 19–31, 2016.

[24] J. Mirkovic ve P. Reiher, "D-WARD: A source-end defense against flooding denial-of-service attacks," *IEEE Transactions on Dependable and Secure Computing*, c. 2, sayı 3, ss. 216–232, 2005.

[25] H. J. Liao, C. H. Richard Lin, Y. C. Lin ve K. Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, c. 36, sayı 1, ss. 16–24, 2013.

[26] A. Khraisat, I. Gondal, P. Vamplew ve J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity 2019 21*, c. 2, sayı 1, ss. 1–22, 2019.

[27] A. Khraisat, I. Gondal ve P. Vamplew, "An anomaly ıntrusion detection system using C5 decision tree classifier," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, c. 1, ss. 149–155, 2018.

[28] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel ve M. Rajarajan, "A survey of intrusion detection techniques in Cloud," *Journal of Network and Computer Applications*, c. 36, sayı 1, ss. 42–57, 2013.

[29] K. Christian ve C. Jon, "Honeycomb," *Computer Communication Review*, c. 34, sayı 1, ss. 51–56, 2004.

[30] Internet Security Threat Report ISTR, "Symantec", Amerika, Rap. 22 2017.

[31] I. Butun, S. D. Morgera ve R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, c. 16, sayı 1, ss. 266–282, 2014.

[32] A. Alazab, M. Hobbs, J. Abawajy ve M. Alazab, "Using feature selection for intrusion detection system," *The 12th International Symposium on Communications and Information Technologies*, ss. 296–301, 2012

[33] O. Ata ve K. Kadhim, "Network ıntrusıon detectıon usıng machıne learnıng technıques," *Journal Engineering Systems Architecture Cilt*, c. 2, sayı 1, ss. 115–123, 2018.

[34] A. Ethem, "Introduction to machine learning second edition adaptive computation and machine learning," *Massachusetts Teknoloji Enstitüsü*, c. 5 ss. 41–470, 2015.

[35] C. F. Tsai, Y. F. Hsu, C. Y. Lin ve W. Y. Lin, "Intrusion detection by machine learning: A review," *Expert Systems with Applications*, c. 36, sayı 10, ss. 11994–12000, 2009.

[36] A. Géron, "*Hands-on machine learning with Scikit-Learn, Keras, and TensorFlow : concepts, tools, and techniques to build intelligent systems,*" 2. baskı, Liverpool. İngiltere: Oreilly, s. 819.

[37] H. Brink, J. W. Richards ve M. Fetherolf. (2021, 23 Agustos). *Real-World Machine Learning* [Online]. Erişim: www.allitebooks.com.

[38] L. Breiman, "Random Forests," *Machine Learning*, c. 45, sayı 1, ss. 5–32, 2001

[39] S. M. M. Hasan, M. A. Mamun, M. P. Uddin ve M. A. Hossain, "Comparative analysis of classification approaches for heart disease prediction," *The International Conference on Computer, Communication, Chemical, Material and Electronic Engineering*, c. 8, ss. 76-86, 2018.

[40] J. R. Quinlan, "Induction of decision trees," *Machine. Learning*, c. 1, sayı 1, ss. 81–106, 1986.

[41] K. Li, G. Zhou, J. Zhai, F. Li ve M. Shao, "Improved PSO_AdaBoost Ensemble Algorithm for Imbalanced Data," *Sensors 2019*, c. 19, sayı 6, ss. 1476, 2019.

[42] Z. Cai, C. Youguang. (2021, 16 Şubat), *Improved piecewise nonlinear combinatorial adaboost algorithm based on noise self-detection* [Online]. Erişim: https://en.cnki.com.cn/Article_en/CJFDTotal-JSJC201705027.htm.

[43] S. Uddin, A. Khan, M. E. Hossain ve M. A. Moni, "Comparing different supervised machine learning algorithms for disease prediction," *BMC Medical Informatics and Decision Making*, c. 19, sayı 1, ss. 1–16, 2019.

[44] S. Dreiseitl ve L. Ohno-Machado, "Logistic regression and artificial neural network classification models: a methodology review," *Journal of Biomed Inform*, c. 35, sayı 5–6, ss. 352–359, 2002.

[45] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali ve M. Guizani, "A survey of machine and deep learning methods for ınternet of things (IoT) security," *IEEE Communications Surveys Tutorials*, c. 22, sayı 3, ss. 1646–1685,

2020.

[46] S. Tong ve D. Koller, "Support vector machine active learning with applications to text classification," *Joutnal of Machine Learning,* c. 8, ss. 45–66, 2001.

[47] N. Moustafa ve J. Slay, "The evaluation of network anomaly detection systems: statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set," *Information Security Journal: A Global Perspective,* c. 25, sayı 1–3, ss. 18–31, 2016.

[48] I. Sharafaldin, A. Habibi Lashkari ve A. A. Ghorbani, "A detailed analysis of the CICIDS2017 data set," *Communications in Computer and Information Science,* c. 977, ss. 172–188, 2018.

[49] R. P. Lippmann, M. A. Zissman, R. K. Cunningham, D. Wyschogrod, S. E. Webster, D. Weber, D. McClung, K. R. Kendall, J. W. Haines "Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation," *Information Survivability Conference and Exposition,* c. 2, ss. 12–26, 2000.

[50] I. F. Kilincer, F. Ertam ve A. Sengur, "Machine learning methods for cyber security intrusion detection: Datasets and comparative study," *Computer Networks,* c. 188, ss. 107840, 2021.

[51] M. A. Ferrag, L. Maglaras, S. Moschoyiannis ve H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *Journal of Information Security and Applications,* c. 50, ss. 102419, 2020.

[52] M. Tavallaee, E. Bagheri, W. Lu ve A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," *IEEE Symposium on Computational Intelligence for Security and Defence Applications,* c. 5 , ss. 117-134 , 2009.

[53] M. Ring, S. Wunderlich, D. Scheuring, D. Landes ve A. Hotho, "A survey of network-based intrusion detection data sets," *Computer Security,* c. 86, ss. 147–167, 2019.

[54] A. Sonule, M. Kalla, A. Jain ve d. S. Chouhan, "UNSW-NB15 dataset and machine learning based ıntrusion detection systems," *The International Journal of Engineering and Advanced Technology,* sayı 9, ss. 2249–8958, 2020.

[55] N. Moustafa ve J. Slay. (2021, 27 Ağustos). *The UNSW-NB15 dataset | UNSW research* [Online]. Erişim: https://research.unsw.edu.au/projects/unsw-nb15-dataset.

[56] A. Naik ve L. Samant, "Correlation review of classification algorithm using data mining tool: WEKA, rapidminer, tanagra, orange and knime," *Procedia Computer Science,* c. 85, ss. 662–668, 2016.

[57] P. Bisht, N. Negi, P. Mishra ve P. Chauhan, "A comparative study on various data mining tools for ıntrusion detection," *International Journal of Scientific and Engineering Research,* c. 9, sayı 5, 2018.

[58] M. Hasan, M. M. Islam, M. I. I. Zarif ve M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet of Things,* c. 7, sayı. 10, ss. 100059, 2019.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Yasin TÜRKYILMAZ

Yabancı Dili : İngilizce

ÖĞRENİM DURUMU

Derece	Alan	Okul/Üniversite	Mezuniyet Yılı
Y. Lisans	Bilgisayar Müh.	Düzce Üniversitesi	2021
Lisans	Bilgisayar Müh.	Sakarya Üniversitesi	2018
Lise	Arifiye AÖL	Arifiye AÖ Lisesi	2014

YAYINLAR

[1] Y. Türkyılmaz ve A. Şentürk, *"*Nesnelerin İnternetinde Güvenliği Sağlamada Kullanılan Makine Öğrenmesi Yöntemleri", *EEMGG Elektrik-Elektronik Mühendisliğinde Güncel Gelişmeler Sempozyumu,* Trabzon, Türkiye,2021, ss. 56-63.

[2] Y. Türkyılmaz ve A. Şentürk, "Saldırı Tespitinde Makine Öğrenmesi Yöntemlerinin Performans Analizi," *European Journal of Science and Technology,* sayı 32, ss. 107–112, 2021.