



**BASİTLEŞTİRİLMİŞ MAHALANOBİS MESAFESİ VE DOĞRUSAL
KORELASYONA DAYALI ÖZNİTELİK SEÇİMİ KULLANARAK
AĞ ANOMALİ TESPİTİ**

Furkan ALAYBEG

**YÜKSEK LİSANS TEZİ
BİLİŞİM SİSTEMLERİ ANA BİLİM DALI**

**GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ**

ARALIK 2021

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmada;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmada yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Furkan ALAYBEG

08/12/ 2021

BASİTLEŞTİRİLMİŞ MAHALANOBİS MESAFESİ VE DOĞRUSAL
KORELASYONA DAYALI ÖZNİTELİK SEÇİMİ KULLANARAK
AĞ ANOMALİ TESPİTİ
(Yüksek Lisans Tezi)

Furkan ALAYBEG

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

Aralık 2021

ÖZET

Güvenlik, ağ saldırılarına ve izinsiz girişlere karşı sistemi korumak ve tedbirler almak açısından önemli bir rol oynamaktadır. Gelişen nesnelerin interneti ile birlikte güvenlik konusu daha da önem kazanmaktadır. Saldırı tespit sistemleri, güvenlik araştırmalarında yaygın olarak tercih edilmekte olup makine öğrenimi ve istatistiksel yöntemlere dayalı saldırı tespit sistemleri olmak üzere sınıflandırılmaktadır. İzinsiz girişleri tespit etmek için imzaya ve anomaliye dayalı olacak şekilde birçok teknik geliştirilmiştir. Saldırı tespit sistemlerinde anomalileri tespit etmede en büyük engel, sistemin karmaşıklığını artıran ve anomalilerin tespit oranını azaltan veri setinin yüksek boyutluluğa ve gereksiz özniteliklere sahip olmasıdır. Karmaşıklıkta bu artış, ağ saldırılarını tespit etmek ve önlemek amacıyla yeni yaklaşımların geliştirilmesini gerekli hale getirmektedir. Bu çalışmanın temel amacı, geleneksel Mahalanobis mesafesi yerine daha az hesaplama karmaşıklığına sahip olan basitleştirilmiş Mahalanobis mesafesinin (SMD) uygulanması ve anomali tespiti için istatistiksel tabanlı yöntemlerin etkinliğinin araştırılmasıdır. Tüm deneyler büyük veri ölçeğinde yaklaşık 2,5 milyon kayıt sayısının mevcut bulunduğu UNSW-NB15 ağ veri seti üzerinde doğrusal korelasyona dayalı öznitelik seçimi (LCFS) ile SMD'yi birleştiren bir yaklaşım kullanılarak uygulanmıştır. Önerilen yaklaşımın deney bulguları incelendiğinde, saldırı tespit sistemleri için kritik öneme sahip düşük yanlış alarm oranının %0,88 ila %1,04 arasında olduğu ve en yüksek tespit oranının %99,94 olarak elde edildiği gözlemlenmiştir. Bununla birlikte, makine öğrenimine dayalı literatür çalışmalarıyla karşılaştırıldığında birbirine yakın sonuçlar elde edildiği görülmektedir. Literatüre katkısı bakımından incelendiğinde ise nesnelerin interneti alanına LCFS ve SMD'yi birleştiren anomali tabanlı bir yaklaşım sunulmuştur.

Bilim Kodu : 92429

Anahtar Kelimeler : Anomali tespiti, ağ saldırı tespiti, doğrusal korelasyon tabanlı öznitelik seçimi, nesnelerin interneti, büyük veri

Sayfa Adedi : 85

Danışman : Dr. Öğr. Üyesi Uraz YAVANOĞLU

NETWORK ANOMALY DETECTION USING LINEAR CORRELATION BASED FEATURE SELECTION AND SIMPLIFIED MAHALANOBIS DISTANCE

(M. Sc. Thesis)

Furkan ALAYBEG

GAZİ UNIVERSITY
INFORMATICS INSTITUTE

December 2021

ABSTRACT

Network security plays a crucial role in protecting the system and taking precautions against network attacks and security breaches. The issue of security has gained even more importance with the emergence of new technologies such as the Internet of Things (IoT). Intrusion detection systems are widely used in security research and classified into two categories such as machine learning and statistical-based techniques. Many techniques have been developed based on signature and profile to detect network breaches. The main obstacle of detecting anomalies in intrusion detection systems is the high dimensionality and redundant features of the dataset, which increases the complexity of the systems and reduces the detection rate of anomalies. This increase in complexity requires new and different techniques to detect and prevent network attacks. The purpose of this study is to apply the simplified Mahalanobis distance (SMD) instead of the traditional Mahalanobis distance, which requires less computational complexity, and to investigate the effectiveness of statistical-based methods for anomaly detection. The experiments were applied using an approach consolidating linear correlation-based feature selection (LCFS) and SMD techniques at the big data scale using the UNSW-NB15 dataset, which includes 2.5 million rows. The findings showed that our model obtained the lowest false alarm rate between 0.88% and 1.04% and the highest detection rate of 99.94%, which are significant for intrusion detection systems. Furthermore, it showed that our approach could obtain results close to each other compared to literature studies based on machine learning models. Consequently, this study proposes an anomaly-based approach that combines LCFS and SMD for IoT environments in terms of literature contribution.

Science Code : 92429

Key Words : Anomaly detection, network intrusion detection, linear correlation based feature selection, internet of things, big data

Page Number : 85

Supervisor : Assist. Prof. Dr. Uraz YAVANOĞLU

TEŞEKKÜR

Bu tez kapsamında, hayatım boyunca maddi ve manevi desteklerinin yanı sıra beni yetiştiren ve desteğini esirgemeyen başta ailem olmak üzere bilgi ve tecrübesiyle çalışmamı yönlendiren değerli danışman hocam Dr. Öğr. Üyesi Uraz YAVANOĞLU'na sonsuz teşekkür eder ve saygılarımı sunarım. Ayrıca yüksek lisans eğitimim boyunca Gazi Üniversitesi'nden ders aldığım, çalışmalarına katkı sağlayan hocalarıma ve bu süreçte desteklerini esirgemeyen arkadaşlarıma teşekkürü bir borç bilirim.



İÇİNDEKİLER

	Sayfa
ÖZET	iv
ABSTRACT.....	v
TEŞEKKÜR.....	vi
İÇİNDEKİLER	vii
ÇİZELGELERİN LİSTESİ.....	ix
ŞEKİLLERİN LİSTESİ.....	x
SİMGELER VE KISALTMALAR.....	xi
1. GİRİŞ	1
2. TANIMLAR VE KAVRAMLAR.....	7
2.1. Saldırı Tespit Sistemleri	7
2.1.1. İmzaya dayalı saldırı tespiti.....	8
2.1.2. Anomali (Profil) tabanlı saldırı tespiti.....	8
2.2. Büyük Veri.....	9
2.3. Öznitelik Seçimi	12
2.3.1. Filtre tabanlı yöntemler.....	13
2.3.2. Sarmalayıcı yöntemler	13
2.4. Makine Öğrenimi.....	13
2.4.1. Gözetimli öğrenme.....	14
2.4.2. Gözetimsiz öğrenme	14
2.5. Nesnelerin İnterneti	15
3. LİTERATÜR ÇALIŞMALARI	17
3.1. Makine Öğrenimine Dayalı Çalışmalar	18
3.2. İstatistik Tabanlı Çalışmalar	26
3.3. Öznitelik Seçimine Dayalı Çalışmalar	33

	Sayfa
4. YÖNTEM	41
4.1. UNSW-NB15 Veri Seti.....	41
4.2. Min-Max Öznitelik Normalizasyonu	46
4.3. Doğrusal Korelasyona Dayalı Öznitelik Seçimi.....	47
4.4. Basitleştirilmiş Mahalanobis Mesafesi	48
4.5. Eşik Değeri ve Anomali Tespiti	50
5. ÖNERİLEN SİSTEMİN UYGULANMASI.....	51
5.1. Deney Ortamı.....	51
5.2. Veri Ön İşleme.....	53
5.2.1. Veri Temizleme.....	55
5.2.2. Öznitelik dönüşümü ve normalizasyon	55
5.3. Deneyin Uygulanması.....	57
5.4. Performans Değerlendirilmesi	61
5.4.1. LCFS ve basitleştirilmiş Mahalanobis mesafesi deney sonuçları.....	63
5.4.2. LCFS kullanılmadan basitleştirilmiş Mahalanobis mesafesi deney sonuçları	64
5.4.3. Diğer çalışmalarla karşılaştırma sonuçları	65
5.4.4. Dengeli veri seti üzerinde deney sonuçları.....	67
6. DEĞERLENDİRME VE SONUÇ.....	71
KAYNAKLAR	75
EKLER.....	82
EK-1. Veri ön işleme ve öznitelik seçimi sonrası veri setindeki öznitelikler	83
EK-2. Google Colab ortamında projenin notebookları.....	84
EK-3. Özniteliklerin korelasyon katsayılarına ait sıcaklık haritası.....	84
ÖZGEÇMİŞ	85

ÇİZELGELERİN LİSTESİ

Çizelge	Sayfa
Çizelge 2.1. Anomali tabanlı saldırı tespit yöntemlerine genel bakış [26]	7
Çizelge 3.1. Literatür çalışmalarına ait karşılaştırmalı sonuç tablosu	17
Çizelge 4.1. Veri setine ait öznitelikler	43
Çizelge 4.2. Veri Setine ait saldırı türleri ve saldırı sayıları	45
Çizelge 4.3. Korelasyon katsayısı ve ilişkinin yorumlanması [88].....	48
Çizelge 5.1. Google Colab ortamında notebook türleri [92].....	51
Çizelge 5.2. Dosya boyutu, kayıt sayısı ve öznitelik sayısı bakımından veri seti.....	53
Çizelge 5.3. UNSW-NB15 veri setine ait karakteristik özellikler	54
Çizelge 5.4. Karmaşıklık matrisi	61
Çizelge 5.5. LCFS ve SMD performansı (ilk üç öznitelik kullanarak).....	63
Çizelge 5.6. LCFS öznitelik seçimi kullanılmadan SMD performansı (ilk üç öznitelik kullanılarak)	64
Çizelge 5.7. UNSW-NB15 veri seti üzerinde farklı istatistiksel tabanlı öznitelik seçim yöntemlerinin karşılaştırılması.....	66
Çizelge 5.8. Aynı LCFS öznitelik seçimini kullanan çalışmanın mevcut yöntemle karşılaştırılması	66
Çizelge 5.9. UNSW-NB15 veri setini kullanan makine öğrenimine dayalı yöntemlerin karşılaştırılması.....	67
Çizelge 5.10. İlk üç öznitelik ve 10 kat çapraz doğrulama kullanılarak 50.000 normal ve 50.000 anomali dengeli test veri setinin performansı	68
Çizelge 5.11. İlk üç öznitelik ve 10 kat çapraz doğrulama kullanılarak 100.000 normal ve 100.000 anomali dengeli test veri setinin performansı	69

ŞEKİLLERİN LİSTESİ

Şekil	Sayfa
Şekil 2.1. Nİ’de büyük veri kaynakları	11
Şekil 2.2. Nİ mimarisi [5]	16
Şekil 4.1. UNSW-NB15 veri setinin elde edildiği ağ sisteminin mimarisi [8].....	42
Şekil 4.2. Veri setinin sınıfı etiketi bakımından dağılımı	46
Şekil 5.1. Google Colab giriş ekranı	52
Şekil 5.2. Google Colab notebook ortamında ilgili python kütüphanelerinin yüklenmesi	52
Şekil 5.3. Veri ön işleme kodlama ekranı	54
Şekil 5.4. Saldırı dağılımları bakımından veri setinin dağılımı	56
Şekil 5.5. İki katmanlı doğrusal korelasyona dayalı öznitelik seçimi (LCFS)	57
Şekil 5.6. Büyükten küçüğe doğru hedef değişkeniyle ilgili ilk on öznitelik sıralaması	58
Şekil 5.7. Önerilen modelin mimarisi	60
Şekil 5.8. Farklı öznitelik sayılarının artan eşik değeri ile tespit oranına etkisi	64
Şekil 5.9. Tüm öznitelikler kullanılarak farklı eşik değerleri üzerinde değerlendirme ölçütleri.....	65
Şekil 5.10. Dengeli veri setlerine ait mesafe değerlerinin dağılımı	69

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler

Açıklamalar

GB

Gigabyte

α

Alfa Sembolü

μ

Ortalama Değer Sembolü

MB

Megabyte

PB

Petabyte

σ

Standart Sapma Sembolü

TB

Terabyte

Kısaltmalar

Açıklamalar

FPR

Yanlış alarm oranı (False positive rate)

IDS

Saldırı tespit sistemi

LCFS

Doğrusal korelasyona dayalı öznitelik seçimi

MCA

Çok değişkenli korelasyon analizi

MD

Mahalanobis mesafesi (Mahalanobis distance)

ML

Makine öğrenimi (Machine learning)

NI

Nesnelerin interneti (IoT- Internet of things)

SMD

Basitleştirilmiş mahalanobis mesafesi

1. GİRİŞ

Hayatımızın vazgeçilmez bir parçası olan akıllı cihazların kullanımı her geçen gün giderek artmaktadır. Donanım, yazılım ve internet protokolleri gibi iletişim teknolojilerindeki gelişmeler farklı cihazlar arasında iletişimi önemli ölçüde kolaylaştırmıştır. Nesnelerin interneti (Nİ) olarak adlandırılan internet bağlantılı cihazların teknolojisi, farklı uygulama alanlarına ait fiziksel nesneleri entegre eden ve siber dünya arasında bir entegrasyon oluşturan yeni bir paradigma olarak tanımlanmaktadır [1], [2]. Bugün bu cihazlar; evlerde, ofislerde, ulaşımda, sağlıkta, telekomünikasyonda, tarımda ve hemen hemen her alanda yer almaktadır. Cisco raporuna göre internete bağlanan nesnelerin sayısının dünyadaki insan sayısını aştığı görülmektedir [3]. Ayrıca Cisco System'in diğer bir raporunda 2013'ten 2022'ye kadar şirketler için sağladığı artan gelirler ve düşük maliyetler sonucunda Nİ'nin 14,4 trilyon dolar değere ulaşacağı tahmin edilmektedir [2]. Bununla birlikte, 2019 yılında 8 milyar olan Nİ cihaz sayısının 2027 yılına kadar 41 milyara ulaşması öngörülmektedir [4]. İnternete erişim oranlarının artışı ve Nİ gibi yeni teknolojiler, bilgisayar sistemlerini ve ağlarını işgal etmeye yönelik yeni ve modern güvenlik tehditlerini de beraberinde getirmektedir [5]. Hızla büyüyen ve sürekli genişleyen bu ağ yapısında büyük veri yönetimi, veri işleme, analitik ve güvenlik gibi konularda kayda değer endişelerin ortaya çıkmasına neden olmaktadır. Böyle bir durumda ağ sistemlerine saldırı yapanlar, kullanıcıların gizliliğini ve güvenliğini tehdit etmenin yeni bir yolu olarak Nİ'nin gelişen ve büyüyen potansiyelinden yararlanmaktadır. Örneğin, 2014 yılında internet ortamında 40 milyondan fazla gerçekleşen güvenlik ihlalinin önemli ekonomik kayıpların yanı sıra kişisel mahremiyetin açığa çıkmasına da yol açtığı görülmüştür [6]. İstatistiksel veriler doğrultusunda, internete bağlı cihaz kullanıcılarının ne kadar büyük bir tehlike ile karşı karşıya olduğu anlaşılmaktadır. Nİ cihazlarının bağlı olduğu ağlara yapılan saldırıların yüksek tespit oranı ile saptanması, bu tehditlerin önüne geçebilmek açısından önem arz etmektedir. Saldırılar tespit edilemediği takdirde, kişisel veri güvenliği ihlali veya cihazların etkisiz hale getirilmesi gibi istenmeyen sonuçlar ortaya çıkabilmektedir. Bu nedenle, internete bağlı cihazlarda ağ saldırılarının yüksek tespit oranıyla algılanması için güvenlik çözümlerine yatırım yapılması ve yeni yaklaşımların geliştirilmesi gerekmektedir. Özellikle Nİ cihazlarının gelişmesiyle birlikte hem güvenlik ihtiyacının artması hem de veri hacminde karmaşıklığın meydana gelmesi bu çalışmanın temel motivasyonunu belirlemektedir. Saldırı tespit sistemleri, geleneksel ağlarda olduğu gibi Nİ için de önemli güvenlik araçlarından biridir. Bu sistemler, özellikle sistem tehditlerini veya sistemin kötüye kullanımını tespit

etmenin yanı sıra herhangi bir güvenlik ihlali tespit edildiğinde sistem yöneticisini de uarmayı amaçlayan sistemler olarak tanımlanmaktadır [2]. İzinsiz giriş olaylarının sayısının artması ve internet ağlarının yaygın hale gelmesi nedeniyle birçok kuruluş, güvenlik ihlallerini kontrol eden çeşitli sistemlerin giderek daha fazla kullanıldığını belirtmektedir [7]. Ağ saldırılarını tespit eden sistemler incelendiğinde imza ve profil tabanlı olmak üzere ikiye ayrıldığı görülmektedir. İmzaya dayalı saldırı tespit sistemleri, veritabanına kaydedilmiş mevcut saldırıları yeni gelen ağ trafiğiyle eşleştirmeye dayanan yaklaşımdır. Bu yaklaşım, önceden bilinen tehditleri tespit etmede etkili olduğu gibi tespit mekanizmasının anlaşılmasında da kolaylık sağlamaktadır [2]. Anomali tespiti olarak da bilinen profile dayalı yaklaşım ise bir ağ sisteminin faaliyetlerini normal davranış sergileyen bir profile karşılaştırıp normal davranış eşiğinden sapması halinde uyarı vermektedir. Veri setindeki normal verilerin dağılımından önemli ölçüde sapan bu değerler, anomali değerler olarak tanımlanmaktadır. İmza tabanlı yaklaşımla kıyaslandığı zaman, ortaya çıkabilecek yeni saldırıları tespit etme özelliğiyle profile dayalı yaklaşımın daha avantajlı olduğu görülmektedir [2], [8]. Anomali tabanlı saldırı tespit sistemlerinin uygulama adımları, veri setini temsil eden en iyi alt özniteliklerin belirlenmesi ve sınıflandırma algoritması kullanılarak ağ trafiğinin anomali veya normal olarak etiketlenmesi şeklinde uygulanmaktadır. Yeni saldırılar tespit edilmek istendiğinde, literatürde çoğu çalışmanın anomali tabanlı yaklaşımlar üzerine odaklandığı görülmektedir. Ancak, 1980'lerin başından beri saldırı tespit sistemleri üzerinde birçok çalışma yürütülmesine rağmen Nİ cihazlarının artışı ve olgunlaşan teknoloji ile birlikte veri hacminin artması sebebiyle saldırı tespit sistemlerinin Nİ sistemleri için yetersiz kaldığı ifade edilmektedir [2], [9].

Nİ yeni verilerin üretilmesinde en önemli kaynaklar arasında yer almaktadır. Bu cihazlar tarafından üretilen verilerin işlenmesi değerli içgörüler elde etmek açısından önem arz etmektedir [9]. Yüksek miktarda ağ verisinin işlenmesi, ağ tabanlı saldırı tespit sistemleri (IDS) için en büyük zorluklardan biridir. Özellikle büyük ağ veri setlerinde mevcut olan gereksiz öznitelikler, saldırı tespit sistemlerini karmaşıklaştırmakla birlikte sınıflandırma doğruluğunu da olumsuz yönde etkilemektedir [10], [11]. Yüksek miktarda verilerin akıllıca işlenmesi ve analiz edilmesi, akıllı Nİ uygulamaları geliştirmenin anahtarını oluşturmaktadır [9]. Bu nedenle saldırı tespit sistemlerinde birbirleriyle yüksek ilgi düzeyine sahip öznitelikleri belirlemek, en düşük yanlış alarm oranıyla en yüksek tespit oranını elde etmek açısından önemlidir [12]. Saldırı tespit sistemlerinin verimliliğini artırmak için öznitelik seçim yöntemleri aracılığıyla orijinal veri setinden gereksiz özniteliklerin çıkarılmasının

gerektiği belirtilmektedir [13]. Bir özniteliğin diğer özniteliklerle alakasız olması ve çıktı özniteliğiyle yüksek alaka düzeyine sahip olması iyi bir öznitelik olarak ifade edilmektedir [10]. Öznitelik seçimi, büyük veri setlerinde hesaplama süresini ve sistem kaynaklarını kullanmayı kolaylaştıran, makine öğreniminde ise sınıflandırma doğruluğundan ödün vermeden karmaşıklığı azaltan bir tür veri ön işleme aşamasıdır [13], [14]. Öznitelik seçimi; istatistiksel model tanıma, makine öğrenimi, veri madenciliği ve istatistik alanlarında uzun zamandan beri araştırma konusu haline gelmiştir [15]. Uygulama bakımından öznitelik seçimi algoritmaları, filtre tabanlı ve sarmalayıcı olmak üzere iki kategoride sınıflandırılmaktadır [15], [16]. Literatürdeki çalışmalar incelendiğinde, filtre tabanlı yaklaşımların yüksek boyutlu veri setlerinde ölçeklenebilirlik özelliğine sahip olduğundan dolayı tercih edildiği görülmektedir [17]. Filtre tabanlı yaklaşımlar, özniteliklerin ilgi değerine göre en yüksekten en düşüğe doğru sıralanması ve en yüksek değere sahip N tane özniteliğin seçilmesiyle elde edilmektedir [10], [17]. Öznitelikleri seçmek için en önemli iyilik ölçütlerinden biri olarak Pearson korelasyon katsayısı belirtilmektedir [10]. Bu tez çalışması kapsamında istatistikte yaygın olarak kullanılan ve verileri doğrusal ilişkiye göre ele alan iki katmanlı Pearson korelasyon yöntemi, öznitelik seçimi olarak uygulanmıştır. Böylece Nİ cihazlarında daha az hesaplama karmaşıklığıyla yüksek tespit oranını elde edecek özniteliklerin belirlenmesi amaçlanmıştır.

Saldırı tespit sistemlerinde başarıyı etkileyen diğer bir etmen uygun sınıflandırıcı yönteminin seçilmesidir. Doğrusal korelasyona dayalı öznitelik seçimi adımından sonra elde edilen yeni veri seti üzerinde anomalileri tespit edebilen sınıflandırıcı bir yaklaşıma ihtiyaç duyulmaktadır. Literatür çalışmaları incelendiğinde ağ saldırı tespitinde kullanılabilecek makine öğrenimine ve istatistiksel temellere dayalı yaklaşımların mevcut olduğu görülmektedir. İstatistiksel tabanlı mesafe yöntemlerinin anomali tespitinde kullanılan ilkel ancak popüler yaklaşımlar arasında olduğu belirtilmektedir [18]. Tez çalışması kapsamında, çok değişkenli veri setini tek boyutlu değişkene dönüştüren ve hesaplama verimliliğini artıran Mahalanobis mesafe ölçütü tercih edilmiştir [19], [20]. Mahalanobis mesafesi, varyans ve ölçülen değerlerin kovaryansı gibi her değişkeni kendi ağırlığına göre hesaba kattığından diğer mesafe tabanlı yöntemlere göre daha duyarlı sonuçlar vermektedir [21].

Ancak verilerin kovaryans matrisinin ters çevirilebilir olma gereksiniminden ve ters çevirilebilir olsa bile yüksek boyutlu verilerde kovaryans matrisinin hesaplama karmaşıklığından dolayı klasik Mahalanobis mesafesi beklenen performansı karşılayamamaktadır [22]. Bu nedenle öznitelik sayısına göre ölçeklenebilen mesafeye dayalı bir yöntemin seçilmesi gerekmektedir. Literatür çalışmalarına istinaden tez çalışmasında, büyük verilerde daha az hesaplama maliyetine sahip ve klasik Mahalanobis mesafesine göre altı öznitelik kısıtı bulunmayan basitleştirilmiş Mahalanobis mesafesi (SMD) kullanılmıştır. SMD, hesaplama maliyetini düşürmek için varyansın standart sapma ile yer değiştirmesi üzerine türetilmiş mesafe tabanlı bir yöntemdir [21], [22]. Önerilen SMD yönteminin daha önce güncel ağ veri setleri üzerinde test edilmediği ve LCFS gibi bir öznitelik seçimiyle birlikte kullanılmadığı görülmektedir.

Bu çalışmanın temel amacı, Nİ cihazlarının oluşturduğu büyük hacimli veri setleri üzerinde basit istatistikler kullanarak ağ tehditlerini daha az hesaplama maliyetiyle ve yüksek başarı oranıyla tespit etmektir. Bu nedenle, istatistikte en yaygın bilinen Pearson korelasyonuna dayalı LCFS ile SMD'ye dayalı sınıflandırıcıdan oluşan bir model önerilmiştir. Böylece klasik Mahalanobis mesafesinin muzdarip olduğu öznitelik sayısına bağlı kalmadan SMD ile modern Nİ cihazlarında anomali tehditlerinin saptanması amaçlanmıştır. Tespit mekanizması olarak da literatürde en çok kabul gören ortalama (μ), standart sapma (σ) ve 1-3 arası değer alan alfaya (α) dayalı bir eşik değeri (üç sigma) yaklaşımı kullanılmıştır [12], [23], [24]. Sonuç olarak, UNSW-NB15 veri seti üzerinde önerilen LCFS ile SMD'ye dayalı sınıflandırıcı kullanılarak testler gerçekleştirilmiştir. Deney sonuçları incelendiğinde, %99,94 en yüksek tespit oranının ve %0,88-1,04 arasında değişen en düşük yanlış alarm oranının elde edildiği görülmüştür. Diğer makine öğrenimine bağlı yöntemlerle karşılaştırıldığında onlara yakın veya daha iyi sonuçlar elde edildiği gözlemlenmiştir. Önerilen yöntemin literatüre katkıları şunlardır:

- Ağ saldırılarını içeren veri seti üzerinde LCFS tekniğinin SMD'yle birleştirildiği ilk çalışmadır.
- Nİ uygulamaları için daha az hesaplama maliyetine sahip istatistiksel bir ağ saldırı tespit yaklaşımı sunmaktadır.
- Klasik Mahalanobis mesafesinden daha az hesaplama karmaşıklığına sahip olan SMD'nin büyük veri ölçeğinde 2,5 milyon satır örneklem içeren UNSW-NB15 veri seti üzerinde uygulandığı ilk çalışmadır.

- Büyük ağ veri setlerinde performans bakımından hem makine öğrenimi hem de istatistiksel yöntemleri karşılaştırmakta ve dengeli veri seti üzerinde önerilen yöntemin performansını değerlendirmektedir.

Tez çalışmasının 2. bölümünde; saldırı tespit sistemleri, büyük veri, makine öğrenmesi, nesnelerin interneti gibi kavramların tanımları açıklanmıştır. 3. bölümdeyse anomali tespitinde kullanılan öznelik seçimi, makine öğrenmesine dayalı yöntemler ve istatistiksel tabanlı yöntemlerle ilgili çalışmalar takdim edilmiştir. 4. bölüm, çalışma kapsamında kullandığımız veri setine ait detaylı bilgileri, yöntemi ve formülleri içermektedir. 5. bölümdeyse önerilen yöntemin uygulanması, deney sonuçlarının değerlendirilmesi ve karşılaştırmalı analizlerin tablo ve grafik halinde sunumu verilmiştir. Son olarak 6. bölümde; çalışmada uygulanan yöntemler özetlenmiş, elde edilen bulgular yorumlanmış ve gelecekteki çalışmalara yönelik önerilerde bulunulmuştur.



2. TANIMLAR VE KAVRAMLAR

Tez çalışmasında kullanılacak yöntem ve kavramlarının doğru anlaşılması önem arz etmektedir. Bu nedenle bu bölümde kavramları daha iyi algılamak için teorik tanımlar yapılacaktır.

2.1. Saldırı Tespit Sistemleri

Saldırı tespiti ile ilgili araştırma çalışmaları 1980'lerin başından beri yürütülmekte olup geleneksel ağların ve bilgi sistemlerinin korunması üzerine kullanılan birincil araçlardandır [2]. Saldırı tespit sistemi, özellikle sistem tehditlerini veya sistemin kötüye kullanımı tespit etmeyi ve bir güvenlik ihlali tespit edildiğinde sistem yöneticisini uyarmayı amaçlayan sistem olarak tanımlanmaktadır [2], [14]. Bu sistemler, bilgi sistemlerinin yetkisiz kullanımını, çoğaltılmasını, değiştirilmesini ve yol edilmesini keşfetmeye, belirlemeye ve tanımlamaya yardımcı olmaktadır [25]. Sistemlerde genellikle dış ve iç saldırganlar olmak üzere iki farklı taraf mevcuttur. Bunlardan birincisi olan dış saldırganlar, saldırdıkları makine veya sistemlerde yetkisi olmayan kullanıcılarıdır. İç saldırganlar ise sistem üzerinde bazı kısıtlamaları mevcut olmasına rağmen belirli erişim izinlerine sahip kullanıcıları temsil etmektedir. Bilgi sistemleri kapsamında, içten veya dıştan gelebilecek saldırılara karşı sistemleri korumak adına saldırı tespit sistemlerini oluşturmak oldukça önem arz etmektedir [26]. Makine öğrenmesine dayalı algoritmalarda izinsiz giriş tespiti, "normal" ile "anomali" davranışları ayırt etmeyi kolaylaştırabilir ve böylece izinsiz girişleri tespit edebilir [26]. Ağ saldırı tespit yaklaşımlarını incelediğimizde, genelde üç başlık altında toplandığı görülmektedir. Çizelge 2.1'de saldırı tespit sistemlerinin yaklaşım ve karakteristik özelliklerine ait detaylar verilmektedir.

Çizelge 2.1. Anomali tabanlı saldırı tespit yöntemlerine genel bakış [26]

Yaklaşım	Karakteristik Özelliği
İstatistik Tabanlı Tespit	- Veriler hakkında ön bir bilgi gerektirmez. - İstatistiksel özellikleri, yani model oluşturma için ortalama ve varyansı kullanır.
Bilgi Tabanlı Tespit	- Sağlam, esnek ve çok düşük yanlış alarm oranına sahiptir. - Bilgi modeli düzenli olarak güncellenmelidir. - Yeterli bir bilgi modeli oluşturmak zordur.
Makine Öğrenmesi Tabanlı Tespit	-Tespit performansı, önceki sonuçları kullanarak iyileşir. - Yeni alınan saldırı bilgilerine göre yürütme stratejisini değiştirmeye uyartılabilir.

2.1.1. İmzaya dayalı saldırı tespiti

İmzaya dayalı saldırı tespiti, veritabanında kaydedilmiş bilinen saldırıları yeni gelen veri trafiğinde belirli imzaları arayarak mevcut bilinen saldırılar ile eşleştirmeye dayanan yaklaşımdır [2]. Depolanan imzalarla herhangi bir sistem veya ağ etkinliği eşleştiğinde, alarm uyarısı tetiklenir [2], [23]. İmza tabanlı algılama, doğru bilinen tehditleri tespit etmede etkili olup saldırı mekanizmalarının anlaşılması kolaydır [2]. Bu yaklaşım, bilinen saldırıları algılamada düşük yanlış pozitif oranına ve yüksek doğruluk oranına sahiptir. Fakat bu saldırı tespit sistemleri, henüz imzaların mevcut olmadığı veya imza tabanına dahil edilmeyen yeni saldırıları (sıfıncı gün veya yeni saldırının varyantları gibi) ve bilinen saldırıların çeşitlerini tespit etmede ne yazık ki başarısız kalmaktadır [2], [8], [23]. Bu gibi durumlarda, varyasyon değişimleri bir saldırı olarak algılanabilir ve değerlendirilebilir [17]. Bu nedenle yeni saldırıları tespit etmede kullanılması gereken yöntem anomali tabanlı sistemler olarak tavsiye edilmektedir [8].

2.1.2. Anomali (Profil) tabanlı saldırı tespiti

Anomali tespiti, aykırı değer tespiti, sapma tespiti, yenilik tespiti ve istisna madenciliği olarak da bilinmekte olup istatistik ve makine öğrenimi alanlarında geniş çapta incelenmektedir. Anomali tespiti, veri madenciliğinin önemli bir araı. Burada ki ana amaç, belirli bir veri setinden anomali veya olağandışı verileri tanımlamaktır [27]. Birçok çalışmada imzaya dayalı sistemlerin anomali sistemlere oranla daha yüksek başarı ve düşük yanlış alarm elde ettiğinden bahsedilmektedir. Ancak bilindiği üzere anomaliye dayalı sistemlerin yeni gelebilecek saldırıları ve özellikle de kaynakların kötüye kullanılmasıyla ilgili saldırıları tespit etme yeteneği bulunmaktadır. Anomali tespiti görevinde, anomalileri ikili görevinden ayıran birçok zorluk bulunmaktadır. Temelde anomali verilerin iki önemli karakteristik özelliği bulunmaktadır. Bunlardan birincisi, anomali veriler özelliklerine göre normal bir sistem verilerinden çok farklı davranışlar sergilemektedir. Diğer önemli karakteristik özelliği ise normal örnekler ile karşılaştırıldığında, veri setinde doğası gereği nadir görülmektedir [9], [28]. Anomali tabanlı saldırı tespit sistemlerinin çalışma prensibine baktığımızda, bir sistemin normal ağ trafiği faaliyetlerini içeren bir profil oluşturulur ve yeni gelen ağ trafiği ile oluşturulan profil trafiği karşılaştırılır. Ardından yeni gelen ağ davranışı ve normal ağ profili arasında herhangi bir sapma olması durumunda, yeni gelen davranış anomali olarak işaretlenip uyarı oluşturulur [2], [29]. Fakat bu yaklaşım, eğitim sürecinde yüksek boyutlu veri setleriyle uğraşılması durumunda, yüksek yanlış pozitif oranı sorunuyla karşı karşıyadır [17].

Anomali tabanlı tespit algoritmalarının uygulama alanlarına baktığımızda, saldırı tespit sistemleri, sahtekarlık tespiti, medikal uygulamalar, sistem sağlığını izleme, kredi kartı dolandırıcılık tespiti, eko-sistem bozukları, endüstriyel hasar ve görüntü işleme gibi birçok gerçek dünya uygulamasında yaygın olarak kullanılmaktadır. Örnek verecek olursak, sahtekarlık tespiti senaryosunda sistemin kötüye kullanılması ve şüpheli olayları tespit etmek için günlük log verilerinin analizi, medikal uygulamalarda hastanın kardiyografi sinyallerinin ve vucüt sensörlerinin izlenmesi, tomografi alanında resim analizi gibi senaryolarda uygulanmaktadır [6], [9], [28]. Ayrıca anomali tespiti, bir veri setinde aykırı değerleri kaldırmak için veri ön işleme algoritması olarak makine öğrenmesi algoritmalarının performansını önemli ölçüde artırmada kullanılabilir [9]. Veri setlerinde görülen anomali değerler aşağıdaki gibi üç kategoride ele alınabilir.

Nokta Anomalisi: Bir veri örneği, veri setinin normal modelinden saptığında nokta anomalisi olarak tanımlanabilir. Örnek olarak bir kişinin günlük normal şartlarda ihtiyacı olan araba yakıtı 5 litre olarak belirlersen, herhangi bir günde bu ihtiyaç 50 litreye çıkarsa bu nokta anomali olarak algılanabilir [27].

Bağlamsal Anomali: Veri örneği bir bağlamda anomali şekilde davranıyor, diğer bir bağlamda davranmıyorsa bağlamsal anomali veya koşullu anomali olarak isimlendirilir. Noel veya yeni yıl bayram dönemlerinde kredi kartı harcamaları genellikle yılın diğer geri kalanından daha yüksek olması, bağlamsal anomali örneği olarak verilebilir [27].

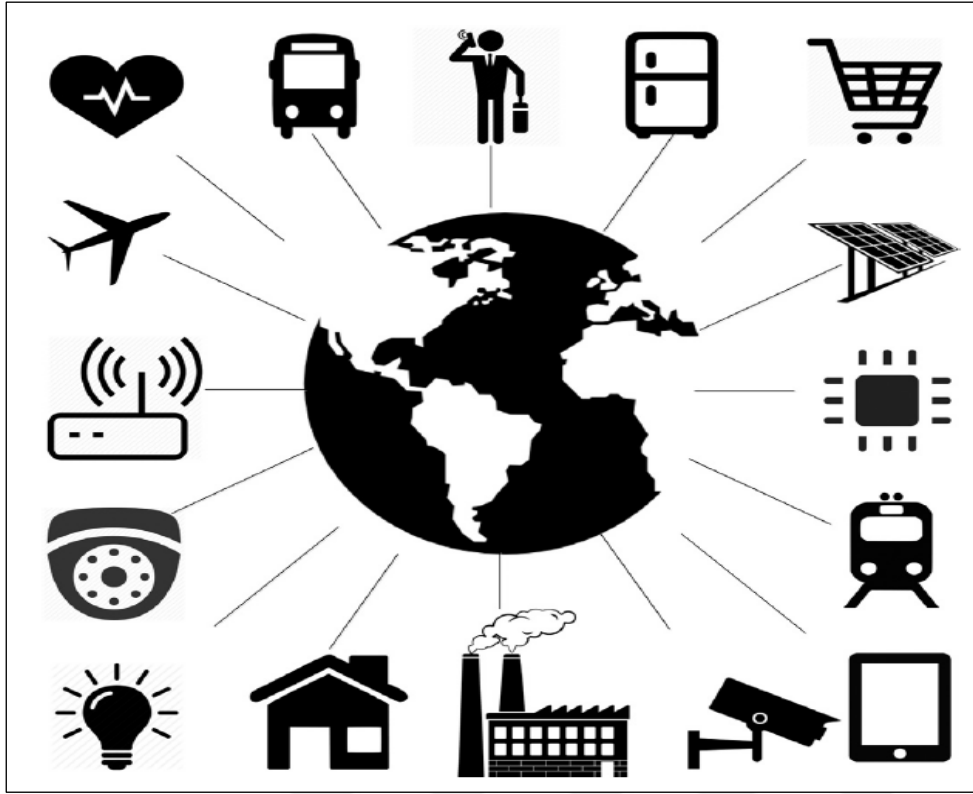
Toplu Anomali: Benzer veri örneklerinden oluşan bir koleksiyon, tüm veri setine göre anomali bir şekilde davrandığında, bu koleksiyon toplu anomali olarak isimlendirilir. Örneğin bireyin elektro kardiyo gram (EKG) çıktısı incelendiğinde, uzun süre boyunca düşük değerlerin olması anomali prematüre kasılmaya karşılık gelen altta yatan fenomeni gösterir. Ancak tek başına düşük bir değer anomali değer olarak kabul edilemez [27].

2.2. Büyük Veri

Veritabanı kavramı, 1970'lerin sonlarında verileri depolamak ve analiz etmek için özel olarak kullanılan bir teknoloji olarak ortaya çıktı. Veri hacminin her geçen gün artmasıyla birlikte tek ana bilgisayar sisteminin depolama ve işleme kapasitesi yetersiz hale gelmeye başladı. Büyük veri çağında hızla artan veri üretimi, veri toplama, depolama, yönetim ve analiz konusunda büyük zorluklar ortaya çıkarmaktadır. Bu kapsamda, hem endüstri hem de akademik alanda büyük veri ile ilgili bir çok tanım bulunmaktadır. META (şu anda Gartner) analisti Doug Laney, bir araştırma raporunda büyük veri 3V modelini ifade eden hacim, hız

ve çeşitlilikte meydana gelen artış ile birlikte verilerin getirdiği zorlukları ve fırsatları belirtmiştir [30]. Genel olarak büyük veri, kabul edilebilir bir süre içinde geleneksel bilgi teknolojileri ve yazılım / donanım araçları tarafından algılanamayan, edinilemeyen, yönetilemeyen ve işlenemeyen veri setleri olarak tanımlanmaktadır [30]. Son 20 yılda gelişen teknoloji ile birlikte, veri üretiminin çeşitli alanlarda büyük ölçüde arttığı söylenebilir. Chen ve arkadaşlarının çalışmasına göre, Google'nin yüzlerce petabyte (PB) veri işlediği, Facebook'un ayda 10 PB'nin üzerinde günlük (log) verisi oluşturduğu, çinli Baidu şirketinin onlarda PB verisini işlediği ve Alibaba'nın bir yan kuruluşu olan Taobao'nun da onlarda PB veri ürettiği belirtilmiştir. [26]. Nİ'nin ortaya çıkışı, mobil algılama teknolojisinin gelişimi ve veri toplama teknolojisinin ilerlemesiyle birlikte, insanlar büyük verinin kullanıcıları ve tüketicileri olmaktan çıkıp aynı zamanda üreticileri ve katılımcıları konumuna da gelmişlerdir. Dolayısıyla Nİ uygulamalarının hayatımızda yer almaya başlamasıyla birlikte büyük verinin önemli kaynağını da oluşturduğu söylenebilmektedir. [3], [26]. Böylesine sürekli genişleyen bir ağda, büyük verilerin yönetimi, veri toplama verimliliği, veri işleme, analitik ve güvenlikle ilgili göz ardı edilemez endişelere yol açmaktadır [3]. Bu nedenle büyük veri teknolojileri, Nİ sistemlerinin kullanım amacını karşılamak, kritik karar vermeyi destekleyebilir hale getirmek ve bilgiyi Nİ altyapılarına ulaştırma amacıyla kritik bir veri analizi aracı olarak ortaya çıkmıştır [1].

Nİ cihazlarında üretilen verilerin büyük ölçekli olması, çeşitli veri toplama cihazlarından dolayı heterojenliği, belirli konuma yerleştirildiğinde ve zaman değeri bulunduğundan güçlü zaman ve mekan korelasyonuna sahip olması ve verilerin iletilme sırasında büyük miktarda gürültünün meydana gelip küçük bir veri bölümünün kullanılabilir veri olması gibi özelliklere sahiptir [30]. Şekil 2.1'de görüldüğü üzere medikal bilgilerin toplanıp analiz edildiği sağlık hizmetleri, elektrik dağıtımını yapan akıllı şebekeler, akıllı ulaşım teknolojileri, yüksek sayıda Nİ cihazı içeren akıllı binalar, akıllı şehirler, ürün üretimini takip eden akıllı tarım uygulamaları ve endüstriyel otomasyon uygulamaları gibi Nİ'nin uygulandığı başlıca alanlardır. Yapılandırılmış ve yapılandırılmamış veriler bakımından büyük veri analitik tekniklerine baktığımızda ise metin madenciliği, ses ve video analitiği, sosyal medya analitiği ve tahmine dayalı analitik gibi alanlarda da yaygın olarak kullanıldığı görülmektedir. [31]. Büyük veriyi tanımlayan V modelinin temel boyutları aşağıda verilmektedir.



Şekil 2.1. Nİ’de büyük veri kaynakları

Hacim (Volume): Veri yığınlarının oluşturulması ve toplanması ile ilgili veri ölçeğinin büyüklüğünü ifade eder. [30], [31]. Büyük veri birkaç terabyte (TB) veya petabyte (PB) olarak rapor edilmektedir. TB ölçü biriminin büyüklüğüne baktığımızda, yaklaşık 16 milyon Facebook fotoğrafının veya 1500 CD’ye ya da 220 DVD’ye sığacak kadar verinin depolanabildiği alanı ifade ettiğini görüyoruz [30], [31]. Bununla birlikte veri hacmi, zamana ve veri türüne bağlı faktörlere göre de değişkenlik göstermektedir. Bu nedenle büyük veri tanımının sektörlere bağlı olduğu söylenebilir [31]. IBM şirketinin 2012 yılının ortalarında 1144 katılımcıyla yaptığı anket sonucuna göre katılımcıların yarısından fazlasının bir terbyte’tan büyük veri setlerini büyük veri olarak kabul ettiği ortaya konmuştur [32].

Hız (Velocity): Verilerin üretilme hızı artarken veri analiz hızının da artmasını ifade etmektedir. Akıllı telefonlar ve sensörler gibi dijital cihazların yaygınlaşmasıyla benzeri görülmemiş veri üretimine yol açılarak gerçek zamanlı analitik ve planlama ihtiyacı da doğal olarak tetiklenmiştir. Geleneksel veri yönetim sistemleri, büyük veri akışlarını gerçek zamanlı işleme kapasitesine sahip olmadığından büyük veri teknolojileri devreye girerek ihtiyacı karşılamaya çalışmaktadır. [31].

Çeşitlilik (Variety): Teknolojik gelişmeler, firmaların çeşitli yapılandırılmış, yarı yapılandırılmış ve yapılandırılmamış veri türlerini kendi bünyelerinde kullanmalarına olanak tanımaktadır. Çeşitlilik, veri setindeki verilerin yapısal bakımdan (ses, video, web sayfası ve metin gibi) heterojenliğini ifade etmektedir [31]. Elektronik tablolarda veya ilişkisel veritabanlarında tablo halinde yapılandırılmış veriler, mevcut verilerin %5'ini oluşturur [31].

Doğruluk/Gerçeklik (Veracity): IBM, gerçekliği bazı veri kaynaklarının doğasında bulunan güvenilmezliği temsil eden dördüncü V olarak belirlemiştir [31]. Veri gerçekliği veya doğruluğu, genel olarak bir veri setinin ne kadar doğru veya gerçek veriler içerdiği ile ilgili bir kavramdır. Kesin olmayan ve belirsiz verilerle başa çıkma ihtiyacı, belirsiz verilerin yönetimi ve madenciliği için geliştirilen araçların ve analitiğin kullanılmasıyla ele alınan veri kaynağının, türünün ve işlenmesinin ne kadar güvenilir olduğunu ifade etmektedir. [31].

Değişkenlik (Variability): SAS, büyük verinin iki ek boyutu olarak değişkenlik ve karmaşıklık kavramlarını tanıtmıştır [31]. Değişkenlik, büyük verinin veritabanına yüklendiği hızı ve veri akış hızlarındaki değişimi ifade etmektedir. Çoğu zaman büyük veri hızı tutarlı olmamakla birlikte periyodik zirve veya dip noktalara sahip olmaktadır. Diğer kavram olan karmaşıklık ise büyük verilerin sayısız kaynak aracılığıyla üretildiğini ifade etmektedir. Farklı kaynaklardan alınan verilerin bağlanması, eşleştirilmesi, temizlenmesi ve dönüştürülmesi gibi kritik zorlukları da beraberinde getirmektedir. [31].

Değer (Value): Oracle büyük verinin “düşük değer yoğunluğu” ile karakterize edildiğini belirtmiştir [31]. Orijinal formdan alınan ham veriler, genellikle hacmine göre düşük bir değere sahiptir. Verilerden iş değeri üretilmezse büyük verinin diğer özellikleri anlamsız kalmaktadır. Bu nedenle büyük hacimli verilerin analiz edilerek yüksek bir değer elde edilmesi gerekmektedir. Müşterileri daha iyi anlamak, süreçleri optimize etmek ve makine veya iş performansını iyileştirmek de dahil olmak üzere büyük verilerden önemli değerler üretilir [31].

2.3. Öznitelik Seçimi

Büyük miktarda ağ verisinin işlenmesi, ağ tabanlı saldırı tespit sistemleri için büyük zorluk teşkil etmektedir. Çoğunlukla bu veriler ilgisiz ve gereksiz öznitelikler içermektedir [11]. Öznitelik seçimi, büyük veri setlerinde hesaplama süresini azaltan ve kaynakları kullanmayı kolaylaştıran, makine öğrenmesinde sınıflandırma doğruluğundan ödün vermeden

karmaşıklığı azaltan bir veri ön işleme aşaması olarak tanımlanmaktadır [13], [14]. Veri setinde ilgisiz ve gereksiz özniteliklerin kaldırılması, hedef değişkenini daha yüksek doğruluk oranıyla tespit etmeyi amaçlamaktadır [33], [34]. Bir özneliğin güçlü ilgi düzeyine sahip olması, optimum alt veri setinde her zaman gerekli olduğu anlamına gelmektedir. Özellikle veri seti boyutunu azaltmada kullanılan öznitelik seçimi yöntemleri; istatistiksel model tanıma, makine öğrenimi, veri madenciliği ve istatistiğin diğer alanlarında uzun yıllar araştırma konusu olarak karşımıza çıkmaktadır [15]. Öznitelik seçimi algoritmalarını teknik bakımından incelediğimizde ise filtre ve sarmal olmak üzere iki kategoride ele alındığı görülmektedir [15], [16].

2.3.1. Filtre tabanlı yöntemler

Bu yöntemleri araştırdığımızda, herhangi bir öğrenme algoritmasından bağımsız olarak verilerin iç özelliklerine bağlı öznitelikleri puanlamak ve sıralamak üzere istatistiksel bir model kullanıldığı görülmektedir [15], [17]. Filtre tabanlı yaklaşımların, yeni öznitelik kümesini seçmek ve bir dizi özneliğin ilişkisini tespit etmek için verilerin mesafe, bilgi, bağımlılık ve tutarlılık gibi genel ölçüm özelliklerine bağlı olduğu belirtilmiştir [15], [33]. Veri seti öznitelikleri en yüksekten en düşüğe doğru sıralanır ve en yüksek ilgi değerlerine sahip özniteliklerin seçilmesiyle yeni bir alt öznitelik kümesi elde edilmektedir. [10], [17]. Bu yöntemler, sınıflandırma algoritmasından bağımsız ve yüksek boyutlu verilerde ölçeklenebilir olmalarından dolayı tercih edilmektedir [17]. Pearson korelasyon katsayısı, ki-kare ve bilgi kazancı gibi yöntemler filtre tabanlı yaklaşımlar arasında en çok kullanılan yöntemlerdir [35].

2.3.2. Sarmalayıcı yöntemler

Sarmalayıcı yöntemler, en uygun alt kümeyi seçmek için önceden belirlenmiş bir makine öğrenimi algoritmasının tahmin doğruluğunu kullanmaktadır [10], [15]. Özniteliklerin önem derecesini değerlendirmek adına sınıflandırma algoritmasının performansı kullanıldığından, çok sayıda özneliğe sahip veri setleri üzerinde hesaplama açısından pahalı olduğu belirtilmiştir [15]. Genetik algoritmalar, karar ağaçları ve Bayes ağları gibi algoritmalar sarmalayıcı öznitelik seçiminde yaygın olarak kullanılan sınıflandırıcılardır [34].

2.4. Makine Öğrenimi

Bilgisayar bilimi bilgisayarların manuel olarak nasıl programlanacağı üzerine odaklanırken, makine öğrenimi bilgisayarların kendilerini deneyimle ve bazı başlangıç yapılarla nasıl programlayacağı sorusuna odakladığı bir alan olarak ifade edilmektedir [36]. İstatistikle

karşılaştırıldığında istatistiğin verilerden hangi sonuçların çıkarılabileceği üzerine odaklandığı belirtilirken, makine öğrenmesinin bu verilerin en etkili şekilde nasıl yakalanacağı, depolanacağı, indeksleneceği, birleştirmek için hangi hesaplama mimarilerinin ve algoritmaların kullanılabileceği, birden fazla öğrenim alt görevinin nasıl düzenlenebileceği ve sistemin izlenebilirliği ile ilgili soruları içerdiği belirtilmiştir [36]. Makine öğrenmesi, karmaşık kalıpları ayırt etmek ve veriye dayalı kararları vermek üzere istatistik, olasılık teorisi, veri madenciliği, örüntü tanıma, yapay zeka, uyarlamalı kontrol ve teorik bilgisayar bilimi alanlarının bir araya getirilmesi şeklinde tanımlanmaktadır [26]. Görüldüğü üzere makine öğrenimi, bilgisayar biliminin bir alt alanı olmakla beraber makinelere açık programlama gerektirmeden öğrenme yeteneği sağlayan yapay zekanın bir alt türü olarak bilgisayar bilimi dünyasında önemli rol oynamaktadır [9]. Makine öğrenmesi alanını öğrenme teknikleri bakımından incelediğimizde ise gözetimli öğrenme, gözetimsiz öğrenme ve yarı gözetimli olmak üzere üç kategoride toplandığı görülmektedir [9], [26]. Bu alan ile ilgili birçok öğrenme algoritması farklı uygulama alanlarında deneysel olarak önerilmiş ve değerlendirilmiştir. Bu algoritmalar; k-en yakın komşu, naive bayes, destek vektör makinesi, lineer regresyon, rastgele orman ağacı, temel bileşen analizi, geri beslemeli sinir ağları, k-means ve regresyon ağaçları en sık kullanılan makine öğrenmesi algoritmalarıdır [9].

2.4.1. Gözetimli öğrenme

Gözetimli öğrenme tekniğinin amacı, belirli bir girdi vektörünün ve ona uygun çıktı (hedef değişkeni) vektörünün nasıl tahmin edileceğinin öğrenilmesidir [9]. Hedef etiketlerinin sınırlı sayıda ayrık değişkenden oluştuğu uygulamalar, sınıflandırma görevleri olarak tanımlanmaktadır. Ancak hedef değişkenlerinin bir veya daha fazla sürekli değişkenden oluştuğu durumlar ise regresyon problemleri olarak ifade edilmektedir. Karar destek makinesi, k-en yakın komşu, naive bayes ve karar ağaçları gözetimli öğrenmede en sık kullanılan sınıflandırma algoritmalarıdır [9].

2.4.2. Gözetimsiz öğrenme

Gözetimsiz öğrenme amacının tanımlanması zor olmakla birlikte eğitim veri setinde hedef değişkenine sahip olması gerekli değildir. Bu yöntemin ana hedeflerinden biri, kümeleme analizi olup bilinen girdi verileri üzerinde benzer örneklemelerden oluşan mantıklı kümeleri oluşturmaktır. K-means kümeleme, birliktelik kuralı öğrenmesi, saklı markov modeli, genetik algoritmalar, bulanık mantık ve yoğunluk tabanlı kümeleme başlıca gözetimsiz öğrenme algoritmalarıdır [9], [26].

2.5. Nesnelerin İnterneti

Kablosuz iletişim, dijital elektronik ve mikro-elektro-mekanik sistemlerdeki (MEMS) teknolojik ilerlemelerin ve hızlı yakınsamanın Nİ'nin ortaya çıkmasına neden olduğu belirtilmektedir [3]. Cisco'nun raporuna¹ göre internete bağlanan nesnelerin sayısının dünyadaki insan sayısını aştığı görülmektedir [3]. Ayrıca Cisco System, 2013'ten 2022'ye kadar şirketler için artan gelirler ve düşük maliyetler sonucunda Nİ'nin 14,4 trilyon dolarlık bir değer oluşturacağını tahmin etmektedir [2].

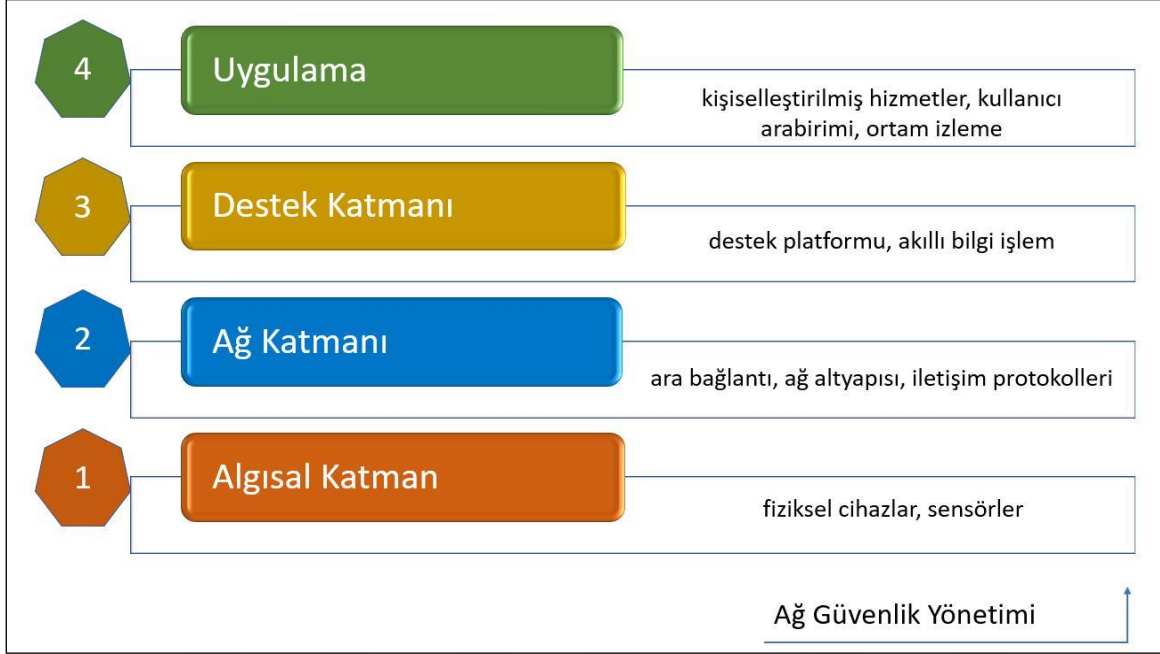
Nesnelerin interneti, akıllı nesnelerin küresel ağ altyapısı aracılığıyla etkileşime girebilen farklı alanlara ait fiziksel nesneleri entegre eden ve siber dünya arasında bir entegrasyon oluşturan yeni bir paradigma olarak tanımlanmaktadır [1], [2]. Altyapı bakımından Nİ, birbirine bağlı ve büyük miktarda veri ileten çok sayıda farklı cihazdan oluşup zamandan, enerjiden ve paradan tasarruf ederek daha akıllı bir ortam sunmayı amaçlamaktadır. Bu sayede basitleştirilmiş bir yaşam tarzı geliştirerek farklı sektörlerdeki harcamaları minimum seviyeye indirgemektedir [9]. Şekil 2.1'de görüldüğü üzere bilgisayarlar, akıllı telefonlar, tabletler, wifi özellikli sensörler, giyilebilir cihazlar ve ev aletleri gibi aygıtların oluşturduğu Nİ kavramı verilmektedir [3]. Nİ, sensörler ve diğer cihazlar arasında internet bağlantısı sağladığından ve akıllı hizmetlerin gelişmesini desteklediğinden dolayı önemli rol oynamaktadır [1]. Cihazlarda kullanılan sensörler; otomatik tanımlama ve izleme, gömülü bilgi işlem, kablosuz iletişim, geniş bant internet erişimi ve dağıtılmış hizmetler gibi farklı teknoloji alanlarının gelişimini sağlamakta olup akıllı nesnelerin internet aracılığıyla günlük faaliyetlerimize entegrasyon potansiyelini de artırdığı görülmüştür [2].

Genel olarak Nİ altyapısını oluşturan mekanizmanın algılama, iletim ve uygulama olmak üzere üç katmandan oluştuğu görülmektedir [13]. Algılama ya da toplama katmanı, cihazların fiziksel çevreden veri toplamak üzere iletişim kurduğu ve algılama düğümleri olarak adlandırılan sensörlerden oluştuğu katmandır. Bu katmanda mevcut olan iletişim protokolleri ve teknolojileri, sınırlı veri hızlarında ve kısa mesafelerde olup sınırlı bellek kapasitesi ve düşük enerji tüketimi ile çalışmak üzere tasarlanmıştır [2]. İletişim katmanı ise algılama katmanından toplanan verilerin uygulamalara ve kullanıcılara iletilmesini sağlamaktadır [2]. Bu katman kapsamında, Ethernet, WiFi, Hibrit Fiber Koaskiyel (HFC) ve Dijital Abone Hattı (DSL) gibi teknolojiler aracılığıyla daha uzun mesafelerdeki nesneleri ve kullanıcıları birbirine bağlayan ağı oluşturmak üzere TCP/IP protokollerini

¹ "The Internet of Things", Cisco, Erişim Tarihi: 30 Nisan, 2021.

https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

birleştirmektedir [2]. Son olarak, uygulama katmanında çevre hakkında yararlı bilgiler elde etmek üzere veriler toplanmaktadır. Bu katmanda bulunan uygulamalar, belirli fiziksel nesnelerin fiziksel ortama göre hareketlerini kontrol ederek bu bilgilere dayalı karar almayı sağlamaktadır [2], [30].



Şekil 2.2. Nİ mimarisi [5]

Şekil 2.2’de görüldüğü üzere Nİ için önerilen genel mimari katmanları verilmiştir [5]. Bununla birlikte, Nİ cihazları çeşitli teknolojilerle entegre edilmiş olup bu cihazlar arasında iletişim türleri bakımından üçe ayrılmaktadır [9]:

- (1) **Aygıttan Aygıt (D2D):** Yakındaki cep telefonları arasında iletişimi sağlamaktadır. Yeni nesil hücresel ağları temsil etmektedir.
- (2) **Aygıttan Sunucuya (D2S):** Bu tür iletişim aygıtlarında tüm veriler yakın veya uzak olan sunuculara gönderilmektedir. Bulut bilişim alanında uygulanmaktadır.
- (3) **Sunucudan Sunucuya (S2S):** Sunucular arasında verilerin iletildiği iletişim türüdür. Bu tür iletişim türü çoğunlukla hücresel ağlar için uygulanmaktadır.

3. LİTERATÜR ÇALIŞMALARI

Bu bölümde saldırı tespit sistemlerinde kullanılan makine öğrenmesine dayalı, istatistiksel tabanlı ve öznitelik seçimi ile ilgili yer alan literatür çalışmalarına yer verilmektedir. Çizelge 3.1’de tez çalışmasında referans olarak aldığımız çalışmalar gösterilmiştir.

Çizelge 3.1. Literatür çalışmalarına ait karşılaştırmalı sonuç tablosu

Yazar	Algoritma	Öznitelik Seçimi	Veri Seti	Doğruluk	Tespit Oranı	Yanlış Alarm (FPR)	F1 Skor
[10]	C4.5	LCFS	NSL-KDD	/	/	/	%99,1
[12]	MD	CorrCorr	UNSW-NB15	%93,27	%56,80	%1,12	/
[22]	SMD	/	Pittsburgh Üniversitesi DNS trafiği	/	/	/	/
[21]	SMD	Payload n-Gram	DARPA 1999	/	%60	< %1	/
[23]	MD	Polynomial Korelasyon	KDD Cup 99	%99,94	%99,99	%0,13	/
[37]	MD	Faktör Analizi	DARPA 1999	/	%84,4	%1	/
[24]	MD	MCA	KDD Cup 99	%99,95	%99,99	%2,03	/
[38]	Rastgele Orman	/	UNSW-NB15	%95,5	/	%7,22	/
[39]	K-Means + C4.5	/	KDD Cup 99	%95,8	%99,6	%0,1	%94

Çizelge 3.2. (devam) Literatür çalışmalarına ait karşılaştırmalı sonuç tablosu

[40]	MPCK-means	/	KDD Cup 99		%96	/	%94
[41]	Enhanced SVM	Genetik Algoritma	DARPA 99	/	%89,39	%0,30	/
[42]	K-Means ve SMO	Genetik Algoritma	NSL-KDD	%97,36	%94,48	%1,2	/
[43]	Rastgele Orman	RF-FST & RF-BER	KDD Cup 99	%99,90	%99,8	%0,001	/
[44]	Finite Dirichlet Mixture Model	PCA	UNSW-NB15	%94,3	%93,9	%5,8	/
Mevcut Çalışma	SMD	LCFS	UNSW-NB15	%98,38	%99,82	%1,82	%93,98

3.1. Makine Öğrenimine Dayalı Çalışmalar

Eid ve arkadaşları, Pearson korelasyon katsayılarının analizine dayalı olarak veri setinden optimal alt kümesinin seçilmesine yönelik bir yöntem önermişlerdir [10]. NSL-KDD veri setinden seçilen optimal öznitelikler üzerinde C4.5 karar ağacı sınıflandırma algoritması olarak kullanılmıştır. C4.5 sınıflandırıcısı üzerinde IDS tasarımı için önerilen doğrusal ilişki tabanlı öznitelik seçiminin performansı değerlendirilmiştir. Deneyler 10 kat çapraz doğrulama yöntemi uygulanarak gerçekleştirilmiş ve sonucunda %99,1 doğruluk oranı elde edilmiştir.

Primartha ve Tama yaptığı çalışmada [38], nesnelerin interneti (Nİ) ağlarında anomali tespit performansını iyileştirmek için parametre ayarlı etkili bir rastgele orman sınıflandırıcısı önerilmiştir. Rastgele orman algoritması, modelde optimum eğitim parametrelerini elde

etmek için kapsamlı bir arama yöntemi olan ızgara araması kullanmaktadır. Önerilen modelin Nİ ağına uygun olduğunu kanıtlamak için sınıflandırıcının performansı; NSL-KDD, UNSW-NB15 ve GPRS olmak üzere üç veri seti üzerinde doğruluk ve yanlış alarm metrikleri karşılaştırılarak değerlendirilmiştir. NSL-KDD veri seti üzerinde deney sonuçları incelendiğinde %99,57 doğruluk oranı ve %0,34 yanlış alarm oranıyla diğer algoritmalara göre daha iyi performans göstermiştir. UNSW-NB15 veri seti üzerinde gerçekleştirilen RF-800 modeli ve geleneksel karar ağacı deneyleri karşılaştırıldığında sırasıyla %95,5 ve 95,7 doğruluk oranı elde edilirken, yanlış alarm oranı bakımından ise sırasıyla %7,22 ve %7,64 sonuçlar elde edilmiştir.

Verma ve Ranga, Nİ cihazlarını DoS saldırılarına karşı güvence altına almaya yönelik anomali tabanlı saldırı tespit sistemlerinin gelişimi ilerletebilecek kapsamlı bir çalışma yürütmüşlerdir [45]. Çalışma kapsamında özellikle Nİ ve IDS için makine öğrenmesi sınıflandırıcılarının performansı değerlendirilmiştir. Ayrıca sınıflandırıcılar arasında önemli farklılıkların tespit edilmesi Friedman ve Nemenyi post host testleri kullanılarak sağlanmıştır. Sınıflandırma algoritmalarını karşılaştırmak için CIDDS-001, UNSW-NB15 ve NSL-KDD gibi popüler ağ veri setleri üzerinde deneyler gerçekleştirilmiştir. Doğruluk ölçütü bakımından deney sonuçları incelendiğinde %96,74 doğruluk oranıyla CART karar ağacı en iyi sonucu elde ederken, tespit oranı bakımından ise %97,31 değerle rastgele orman ve XGB algoritmalarının en yüksek sonucu elde ettiği gözlemlenmiştir. AUC performans ölçütü bakımından %98,77 başarı oranıyla XGB algoritmasının en iyi sonucu elde ettiği görülmüştür.

Timcenko ve Gajin, Nİ ve benzeri ortamlarda ağ anomalilerini doğru bir şekilde tespit etmek amaçlı makine öğrenmesi sınıflandırma algoritmalarını karşılaştıran bir çalışma yürütmüşlerdir [46]. Çalışmanın odak noktası; SVM, torbalama (bagging) ve güçlendirme (boosting) algoritmalarının performanslarını analiz edip, UNSW-NB15 veri üzerinde Nİ ve benzeri ortamlar için güçlü bir savunma mekanizması oluşturacak uygun makine öğrenmesi tekniğinin rolünü analiz etmek olarak belirtilmiştir. SVM algoritmasının bir benzeri olan SMO ve C-SVM algoritmalarıyla birlikte LADTree, REPTree, rastgele orman ve MultiBoost gibi sık kullanılan sınıflandırıcıların karşılaştırması ele alınmıştır. Deney sonuçları incelendiğinde SVM grubuna ait SMO ve LibSVM algoritmalarının sınıflandırmada çok yavaş kaldığı görülmüştür. Bunların arasında rastgele orman algoritması kesinlik, tespit oranı ve ROC ölçütleri bakımında karşılaştırıldığında sırasıyla

%98, %99 ve %99 değerler ile en yüksek başarıyı elde ettiği gözlemlenmiştir. Sınıflandırma hızı bakımından ele alındığında ise REPTree ve MultiBoost en iyi sonuçları göstermiştir.

Chen ve arkadaşları, bilinmeyen saldırıları tespit etmek için iki yarı denetimli sınıflandırma yöntemi ve geleneksel gözetimsiz kümeleme yöntemlerinin performansını iyileştirmek üzere yarı denetimli kümeleme önermişlerdir [40]. İlk olarak bilinmeyen saldırıları tespit etme görevini üstlenen iki yarı gözetimli sınıflandırma yöntemi olan Spektral Grafik Dönüştürücü ve Gauss Alan Yaklaşımı sunulmuştur . İkinci olarak denetlenmemiş kümeleme yöntemlerini iyileştirmek için MPCKmeans yarı denetimli kümeleme yöntemi tanıtılmıştır. Son olarak deney sonuçlarını derinlemesine analiz ettikten sonra biriken saldırıları kayıtları yardımıyla bilinmeyen saldırıları tespit etmede daha başarılı olan transfer öğrenim yöntemi sunulmuştur. Sonuç olarak, yarı gözetimli sınıflandırma yöntemlerinin performanslarının gözetimli sınıflandırıcılardan daha iyi olduğu ve yarı gözetimli kümeleme yönteminin gözetimsiz kümeleme yöntemlerini önemli ölçüde iyileştirebileceği gösterilmiştir.

Muniyandi ve arkadaşları, bilgisayar ağındaki anomali ve normal trafiği sınıflandırmak için kümeleme algoritması olan k-means ve C4.5 karar ağacı yöntemlerini kullanan kademeli bir algoritma önermişlerdir [39]. K-Means kümeleme yöntemi, ilk olarak eğitim veri seti üzerinde Öklid mesafe benzerliği kullanılarak k kümelerine bölmek için kullanılmıştır. Ardından normal veya anomali durumların yoğunluk bölgesini temsil eden her kümede, C4.5 karar ağacı algoritmasını kullanarak karar ağaçları oluşturulup her kümedeki karar ağacı, küme içindeki alt grupları öğrenerek karar sınırlarını iyileştirmektedir. Önerilen yöntem K-Means, ID3, Naive Bayes, K-NN, SVM ve TCM-KNN gibi makine öğrenmesi algoritmalarıyla algılama doğruluğu, yanlış pozitif oranı, kesinlik, toplam doğruluk ve f-ölçümleri olmak üzere beş metrik kullanılarak karşılaştırılmıştır. Deneyler KDD Cup1999 veri seti kullanılarak gerçekleştirilmiştir. Sonuç olarak önerilen yöntemin TCM-KNN'nin elde ettiği %99,7 tespit oranından sonra %99,6 tespit oranla ikinci en iyi performansı elde ettiği görülmüştür. Yanlış alarm bakımından incelendiğinde ise TCM-KNN'den sonra %0,1 oranla ikinci en düşük yanlış alarm başarısını elde etmiştir. Doğruluk ve f1-skor metriği bakımından sırasıyla %95,8 ve %94'lük oranla en iyi sonucu elde ettiği gözlemlenmiştir.

Abdulhammed ve arkadaşları, güncel CIDDs-001 veri setini kullanarak etkili bir saldırı tespit sistemini oluşturmak ve dengesiz sınıf yaklaşımlarını işlemenin etkinliğini araştıran bir çalışma yürütmüşlerdir [47]. Deneyler Derin Sinir Ağları (DNN), Rastgele Orman,

Oylama, Varyasyonel Otomatik Kodlayıcı (VAE) ve Yığınlama makine öğrenimi sınıflandırıcıları kullanılarak CIDD-001 veri seti üzerinde orijinal veri dağılımı, down-sampling ve up-sampling gibi senaryolar üzerinde gerçekleştirilmiştir. Performans sonuçları incelendiğinde yığınlama tekniğinde [45] en yüksek doğruluk oranının %99,80 yukarı örnekleme elde edildiği, VAE yönteminin orijinal dağılımında en yüksek doğruluk oranının %97,59 ve DNN yönteminde ise alt örnekleme %99,30'luk en yüksek doğruluk oranı elde edilmiştir. Rastgele orman yöntemi; orijinal dağılım, alt örnekleme ve sınıf dengeleyi senaryolarında %99,99 doğruluk oranıyla en yüksek başarıyı göstermiştir.

Pajouh ve arkadaşları, makine öğrenmesine dayalı Naive Bayes ve k-en yakın komşu (KNN) kesinlik faktörü oylama versiyonundan oluşan sınıflandırıcı ve boyut azaltmada daha iyi sınıflandırma gerçekleştirmek ve hesaplama süresi karmaşıklığını azaltmak için çok sınıflı Doğrusal Ayrım analizi (LDA) modülünü kullanan iki katmanlı bir ağ anomali tespit modeli önerilmiştir [48]. İki katmanlı benzerlik ölçüsünü değerlendirmek için SMOTE yöntemi kullanılarak dengesiz dağılım gösteren NSL-KDD ağ veri seti üzerinde dengeli dağılmış iki eğitim seti oluşturulmuştur. Naive Bayes ve CF-KNN tabanlı iki seviyeli sınıflandırma yaklaşımının nadir ve tehlikeli saldırı türlerinde diğer modellere göre daha yüksek tespit oranı elde ettiği görülmüştür. Deney sonuçları incelendiğinde önerilen yöntemin %83,24 tespit oranı ve %4,83 yanlış alarm oranıyla Naive Bayes, Random Forest, SVM ve Karar ağacı algoritmalarından daha iyi sonuçlar elde etmiştir.

Ravale ve arkadaşları, K-Means kümeleme algoritması ve Destek Vektör Makinesinin RBF çekirdek işlevi gibi yaklaşımları bir sınıflandırma modülü olarak birleştiren KMSVM karma öğrenme yaklaşımını önermişlerdir [49]. Önerilen sistem, büyük heterojen veri setlerini bir dizi küçük homojen alt kümeye düşürmek için K-Means kümeleme kullanılırken, hibrit sınıflandırma amacıyla SVM'nin RBF çekirdek fonksiyonu kullanılmıştır. Önerilen yaklaşım, KDD CUP99 veri seti kullanılarak yürütülen deney sonuçları incelendiğinde önerilen KMSVM yaklaşımının öznelilik çıkarımı kullanılarak DOS, Probe ve U2R saldırı tiplerinde %100 tespit oranı elde ederken R2L saldırı tipinde %93,33 tespit oranı elde etmiştir. Tüm saldırı tiplerini içeren genel başarımlar incelendiğinde ise %88,71 tespit oranı elde ettiği görülmüştür. Önerilen yöntemin simülasyon sonuçları DOS, PROBE, U2R ve R2L saldırı türlerinde doğruluk oranını ve tespit oranını artırdığı kanıtlanmıştır.

Shon ve arkadaşları, denetimli SVM yaklaşımına benzer şekilde gözetimsiz öğrenme ve düşük yanlış alarm kapasitesi sağlamak için gelişmiş SVM adlı yeni bir çerçeve

önermişlerdir [41]. Önerilen çerçeve performansını iyileştirmek üzere önceden mevcut bilgi olmadan SVM öğrenimi için kendi kendine düzenlenmiş özellik haritası (SOFM) yöntemi kullanılarak normal paketlerin bir profili oluşturulmuştur. İkinci olarak eksik ağ trafiğini reddetmek için pasif TCP/IP Parmak İzi (PTF) tabanlı bir paket şifreleme şeması ve ham internet paketlerinden optimize edilmiş bilgileri çıkarmak için Genetik Algoritma (GA) kullanan öznelik seçim tekniği kullanılmıştır. Son aşamada ise SVM öğrenmesinde girdiler arasındaki zamansal ilişkileri göz önünde bulundurmak için zaman ilişkilerine dayalı paket akışı uygulanmıştır. Geliştirilmiş SVM yaklaşımının amacı, her iki SVM yaklaşımının yüksek performans ve etiketsiz yetenekleri gibi avantajlarını miras alarak ağ trafiğindeki yeni saldırıları tespit etmek ve sınıflandırmak için genel bir çerçeve önermektir. Önerilen yaklaşım MIT Lincoln Lab veri setleri ve gerçek bir ağdan yakalanan canlı veri seti kullanarak değerlendirilmiştir. Deney sonuçları kapsamında sentetik veri seti üzerinde %65,76-66,60 arası tespit oranı elde edilirken, gerçek veri setinde %99,90 oranında anomali tespit oranı elde edilmiştir. Yanlış alarm bakımından ise %0,09 oranı elde edildiği görülmüştür.

Saeedi Emadi ve Mazinani, kablosuz sensör ağlarında verilerin bütünlüğünü etkileyen anomali sorununa, katsayı korelasyonun yararlanarak DBSCAN'ın girdi parametreleri problemini çözem HSE algoritmasını önermişlerdir [50]. Bu yöntem, çeşitli boyutlarda sıcaklık, nem ve voltajı aynı anda karşılaştırarak önceki yöntemlere kıyasla algılama doğruluğunu artırmaktadır. İlk olarak, ağ trafiğinden sıcaklık, nem ve voltajın üç özelliği çıkarılır. Ardından ağ verileri, gürültülü (DBSCAN) algoritmasıyla yoğunluk tabanlı uzamsal kümelenmesi kullanılarak kümelenmiştir. Ayrıca yoğunluk tabanlı algılama teknikleri yardımıyla DBSCAN algoritması giriş verilerinin doğruluğunu analiz eder ve bölgelerde düşük yoğunluklu noktaları anomali olarak algılamaktadır. Deney sonuçları Intel Berkeley Araştırma laboratuvarının standart ve genel veri seti üzerinde değerlendirildiğinde, HSE algoritmasının %96,8 doğruluk oranı elde ettiği görülmüştür.

Gadal ve arkadaşları, saldırı tespit sistemi parametrelerinin performansını artırmak, yanlış pozitif alarm oranını azaltarak yeni saldırıları keşfetmek ve doğru bir şekilde tanımlamak için K-means kümeleme ve Sıralı Minimum Optimizasyon (SMO) algoritmalarının kombinasyonuna dayalı bir hibrit makine öğrenimi tekniği önermişlerdir [42]. Önerilen yöntem özellikle büyük veri setleri üzerinde ortaya çıkan sorunları ele almıştır. Veri setinin sayısını azaltmak ve belirli öznelikleri seçmek için Tutarlılık SebsetEvel ve Genetik arama algoritmaları uygulanmıştır. NSL-KDD üzerinde deney sonuçları incelendiğinde hibrit

makine öğrenmesi tekniğinin %94,48 pozitif tespit oranı, %1,2 yanlış alarm oranı ve %97,369 doğruluk oranı elde ettiği görülmüştür.

Tonejc ve arkadaşları, BACnet ağ trafiğinde anomalilerini tespit etmede etkili olan gözetimsiz makine öğrenmesi teknikleri aracılığıyla karakterizasyonuna izin veren bir çerçeve sunmuşlardır [51]. Boyut azaltma aşamasında temel bileşen analizini (PCA) içeren bir ön işleme adımından sonra kümeleme, rastgele orman, tek sınıf destek vektör makineleri ve destek vektör sınıflandırıcı gibi makine öğrenmesi yöntemleri kullanılmıştır. Çeşitli kaynaklardan BACnet ağ trafiği verileri üzerinde yöntemlerin tespit etkinliği karşılaştırılıp yeni anomali türlerini tespit etmek için hangi yöntemin en uygun olduğunu veya hangi yöntemin daha önce verilerde yakalanmış bir türden yeni saldırıları en güvenilir ve verimli bir şekilde tespit ettiği tartışılmıştır. Çalışma kapsamında deneyler Weka ve scikit-learn kütüphanesi kullanılarak gerçekleştirilmiştir. Deney sonucunda özgüllük ve f1-skor bakımından %100 oranla rastgele orman ağacının diğerlerine göre en iyi sonucu elde ettiği görülmüştür.

Zhang ve arkadaşları, perfSONAR sunucularını kullanarak Open Science Grid tarafından toplanan ağ performans veri seti üzerinde bölünmüş örneklem sınıflandırmasına ve yeniden yapılandırmaya dayalı iki yeni yöntem sunmuşlardır [52]. Çalışma kapsamında güçlendirilmiş (boosted) karar ağacı olan AdaBoost ve basit bir ileri beslemeli sinir ağı olmak üzere iki makine öğrenmesi algoritması kullanılmıştır. Deneyler simüle edilmiş ve gerçek CERN olmak üzere iki veri seti üzerinde gerçekleştirilmiştir. Sonuçlar incelendiğinde güçlendirilmiş karar ağacı yönteminin çok hızlı olduğu ve simüle edilmiş veri setinde tüm anomalileri tespit ettiği kanıtlanmaktadır. Ancak test edilen verinin saat başına 20 saniyeden daha yavaş olduğu ve veri işlenmesi için GPU gerektirse bile pratik kullanım için yeterince hızlı olduğu söylenebilmektedir. Sonuç olarak simüle veri seti üzerinde %92,3 doğruluk oranı elde edilirken gerçek veri seti deneyinde %96 oranında doğruluk oranı elde edilmiştir.

Doshi ve arkadaşları, Nİ cihazlarında paket düzeyinde çeşitli makine öğrenimi algoritmaları ile normal ve DDoS ağ trafiğinin yüksek doğrulukta tespit edilebileceğini gösteren bir çalışma yürütmüşlerdir [53]. Bununla birlikte gerçekçi iyi huylu ve kötü huylu Nİ ağ trafiğini toplamak için Raspberry Pi v3'ün ara kutu görevi göreceği şekilde bir WiFi erişim noktası olarak yapılandırıldığı, deneysel yerel bir tüketici Nİ cihaz ağı kurulmuştur. Böylece açık kaynak veri setlerindeki eksiklik göz önüne alınarak tüketici Nİ cihaz ağından toplanan normal ve DoS ağ trafiğini içeren veri seti; KNN, lineer SVM, karar ağacı, rastgele orman

ve sinir ağıları olmak üzere beş farklı makine öğrenmesi algoritması uygulanarak test edilmiştir. Deney sonuçları incelendiğinde tüm sınıflandırıcıların %99.9 tespit oranıyla saldırı trafiğini tespit ettiği görülmüştür. F1-skor ölçütü bakımından KNN, LSVM, karar ağacı, rastgele orman ağacı ve sinir ağıları anomali tespit sonuçları incelendiğinde sırasıyla %99,5, %92,1, %99,5, %99,8 ve %98,9 başarı oranı elde etmiştir. Sonuç olarak rastgele orman, k-NN ve sinir ağıları sınıflandırıcıların saldırı tespitinde etkili olduğu görülmüştür.

Casas ve arkadaşlarının yürüttüğü çalışmada [54], İnternet Servis Sağlayıcılarının (ISP) günlük işlerinde karşılaştıkları ve giderek artan büyük ölçekli ağ trafiği anomalilerini yönetmek üzere bir teknik sunmuşlardır. Hücresel ağ ölçümlerinde gözlenen anomalilerin tespiti, gözetimli makine öğrenmesi tekniği olan C4.5 karar ağacı algoritması kullanılarak gerçekleştirilmiştir. Önerilen çözüm gerçek hücresel ağ trafiğine benzemek için gerçek trafik istatistiklerinden alınan operasyonel bir hücresel ISP'den yarı sentetik olarak oluşturulmuştur. Ardından veriler iki istatistiksel tabanlı (dağılım tabanlı anomali algılama ve entropi tabanlı algılama) ve literatürde kullanılan beş denetimli makine öğrenmesi (rastgele orman, karar destek vektörü, çok katmanlı algılayıcılar, naive bayes, yerel ağırlıklı öğrenme) tarafından değerlendirilmiştir. Deney sonuçları incelendiğinde tüm modellerin %90 üzeri doğruluk oranı elde ettiği görülmüştür.

Domb ve arkadaşları, literatürde diğer çalışmalardan farklı olarak bir makine öğrenimi tabanlı kural keşfi, bir tehdit tahmin model oluşturucusu ve kural ihlaline ve trafik davranışındaki değişikliklere zamanında tepki verilmesini sağlayan araçlardan olmak üzere üç bileşenden oluşan hafif, basit ve kullanışlı bir çerçeve sunmuşlardır [55]. Kural keşfi ve gerçek zamanlı anomali tespiti için makine öğrenimi platformu olarak rastgele orman (RF) algoritması kullanılmıştır. Deneyler 30 test döngüsü olacak şekilde 10, 100, 250, 500, 750 ve 1000 orman başına ağaç sayısı ile çalışan sekiz işlemcili bir bilgisayar ortamında gerçekleştirilmiştir. İki işlemci kullanılarak genel olarak doğruluk seviyesinin iyi olmadığı görülürken sekiz ve diğer herhangi bir sayıdaki işlemci için ormandaki ağaç sayısına bakılmaksızın yaklaşık %95 doğruluk oranı elde edilmiştir. Sonuç olarak önerilen çerçevenin uygulanabilirliği ve etkinliği deneysel olarak kanıtlandığı görülmüştür.

Dromard ve arkadaşları, kümeleme adımını hızlandırmak için her bölümü yeniden hesaplamak yerine güncellenen bir ızgara ve artırılmış kümeleme algoritmasına dayalı ölçeklenebilir ve gerçek zamanlı kayan pencere kullanan denetimsiz ORUNADA ağ anomali dedektörünü önermişlerdir [56]. Izgara kümeleme algoritmalarına dayanan yöntem, alanı

ardışık dikdörtgen birimlere veya hücelere bölüp elde edilen ızgaraya noktaları yerleştirmektedir. Olağan kümeleme algoritmaları bir öznitellik alanına birkaç nokta eklendiğinde veya çıkarıldığında tüm alanı yeniden bölümlerken, artırımlı kümeleme sadece önceki alanın bölümünü güncellemiştir. Böylece hücre sayısı nokta sayısından önemli ölçüde düşük olduğundan DBSCAN ve Means gibi noktaları gruplayan normal kümeleme algoritmalarına göre daha az karmaşıklığa sahiptir. ONTS ve 2001'den beri toplanan MAWILab veri setleri üzerinde yürütülen deney sonuçları incelendiğinde ise %99,5'e yakın bir tespit oranı ve %0,002 oranında yanlış alarm elde edildiği görülmüştür.

Kaya tarafından saldırı tespit sistemlerinde hangi tekniğin daha başarılı olduğuna yönelik bir çalışma sunulmuştur [57]. Çalışma kapsamında, karar ağaçları, Bayes ağlar, destek vektör makinesi, yapay sinir ağları ve k en yakın komşu olmak üzere en çok kullanılan makine öğrenmesi algoritmaları üzerinde performans analizi gerçekleştirilmiştir. Böylece gelecekte makine öğrenmesine dayalı yapılacak saldırı tespit uygulamalarına bir bakış açısı kazandırılması hedeflenmiştir. KDD CUP99 ve NSL-KDD veri setleri üzerine yürütülen deney sonuçları değerlendirildiğinde, normal ağ trafiğini sınıflandırmada doğruluk, duyarlılık, seçicilik, kesinlik ve f-ölçütü bakımından karar ağaçlarının en yüksek başarıyı elde ettiği görülmüştür. KNN, karar ağaçları ve yapay sinir ağlarının DOS saldırılarını tespit etmede %100'e yakın doğruluk oranına ulaştığı gözlemlenmiştir. İşlem zamanına göre Bayes ağları ve karar ağaçlarının diğer gözetimli sınıflandırıcılara göre daha hızlı sonuç verdiği görülmüştür.

Mahamat ve Çeken yaptığı çalışmada [58], Yazılım Tanımlı Ağlarda (SDN) makine öğrenmesine dayalı ping flood saldırılarını tespit eden bir anomali algılama stratejisi önermişlerdir. Çalışma kapsamında, POX denetleyicisi kullanılarak, saldırıları tespit etmek ve engellemek için bir saldırı tespit modülü geliştirilmiştir. Geliştirilen sistem OpenFlow destekli anahtardan geçen ağ trafiği akışını analiz ederek makine öğrenmesine dayalı karar ağacı kullanılarak anomali durumları tespit etmeye çalıştığı belirtilmiştir. Deneylerde eski ağ trafik verilerini içeren KDD CUP 99 veri seti yerine anahtarlar tarafından gönderilen süre, paket sayısı ve bayt sayısı olmak üzere üç öznitelliğin çıkarılmasıyla oluşturulan bir ağ simülasyon veri seti kullanılmıştır. Sonuçlar karar ağacı algoritması kullanılarak oluşturulan sistemin DDoS saldırılarına karşı başarılı bir şekilde çalıştığını göstermiştir.

3.2. İstatistik Tabanlı Çalışmalar

Tian-yi ve arkadaşları, anomali tespiti için istatistiksel Mahalanobis mesafesine dayalı Artırımlı Olasılık Kümeleme (IPC) algoritmasını önermişlerdir [59]. IPC kademeli olarak aykırı değerleri yeni kümeleme merkezleri olarak algılayıp, küme merkezlerini ayarlamak ve birleştirmek için olasılık kümelemesini kullanmaktadır. İlk olarak bellek tüketimini azaltmak adına şebeke akışının öznelilikleri, pencereyi kaydırmak yerine sönümlü artımlı istatistiklerle çıkarılır. Ardından IPC algoritmasıyla normal ağ trafiğinin modeli oluşturulup önceden bilinen sayıda küme merkezi olmadan yüksek boyutlu veri modelini çıkarmak için aykırı değerlerin yeni kümeleme merkezleri olacak seçilip, örtüşen küme merkezleri birleştirilmiştir. Herhangi bir normal modele ait olmayan veriler ise anomali veri olarak kabul edilmiştir. Deney sonuçları değerlendirildiğinde modelin %98,8 anomali paketleri tespit edebildiği ve hata oranının ise %0,86 oranına ulaştığını görülmüştür.

Wang ve Stolfo tarafından izinsiz girişleri tespit etmeye yarayan PAYL adı verilen yük tabanlı bir anomali detektörü önerilmiştir [21]. PAYL, ağ trafiğinin normal uygulama yükünü tam otomatik, gözetimsiz ve verimli bir şekilde modellediği belirtilmiştir. Yeni verilerin önceden hesaplanmış profile benzerliğini hesaplamak için algılama aşamasında Mahalanobis mesafesi kullanılmıştır. Ancak Mahalanobis mesafesi hesaplanırken bayt frekansları arasında farkları topladıktan sonra çarpımları ve karekökleri hesaplama zorunluluğu karmaşıklığı arttırdığı görülmüş ve bu süreci daha da hızlandırmak için varyansın standart sapmayla değiştirildiği basitleştirilmiş Mahalanobis mesafesi (SMD) tanıtılmıştır. Deneyler, DARPA 1999 ve Columbia CS departman ağında toplanan canlı veri setleri üzerinde gerçekleştirilmiştir. Sonuç olarak 80 numaralı bağlantı noktası trafiğinde %0,1 yanlış pozitif oranı ve neredeyse %100'e yakın doğruluk oranı elde edilmiştir.

Villamarin-Salomon ve Brustoloni tarafından kurumsal ve erişim sağlayıcı ağlarında DDNS trafiğine dayalı olarak botnet komuta ve kontrol saldırılarını tespit etmek üzer iki yaklaşım önermişlerdir [22]. İlk yaklaşımda, sorgu oranları anormal derecede yüksek veya geçici olarak yoğunlaşmış olan DDNS adlarının tespit edilmesi çalışılmıştır. İkinci yaklaşımda ise anormal şekilde tekrar eden NXDOMAIN yanıtlarına sahip DDNS adlarını tespit etmeye yönelik çalışılmıştır. Bununla birlikte iki ağ trafiği arasında benzerlikleri karşılaştırmak adına veri dağılımını göz önünde bulunduran basitleştirilmiş Mahalanobis mesafesi benzerlik ölçütü olarak kullanılmıştır. Deneyler sonucunda anormal derecede yüksek veya geçici olarak yoğunlaştırılmış sorgu oranlarına dayalı olan ilk yaklaşımın bir çok yanlış

pozitif ürettiği görülürken, anomal şekilde tekrar eden NXDOMAIN yanıtlarına dayanan yaklaşımın daha etkili olduğu görülmüştür.

Li ve arkadaşları, mesafeye dayalı bir sınıflandırıcı kullanarak anomali ağ trafiğini tespit eden anomali tabanlı bir saldırı tespit sistemi önermişlerdir [23]. Çalışma kapsamında, tespit doğruluğunu artırmak amaçlı ilgili istatistiklerden gizli korelasyonları çıkarmak için polinom öznitelik yaklaşımı ve iki vektör arasında benzerliği ölçmek için Mahalanobis mesafesi kullanılmıştır. Ardından anomali değerleri tespit etmek için ortalama, standard sapma ve 1-3 arası değişen alfa parametlerinden oluşan üst ve alt eşik değerleri ($\mu - \alpha\sigma$, $\mu + \alpha\sigma$) oluşturulmuştur. KDD Cup 1999 veri seti üzerinde deney sonuçları incelendiğinde %99,99 tespit oranı, %99,94 doğruluk ve %0,13 yanlış alarm oranı elde edildiği görülmüştür.

Hu ve arkadaşları, karmaşık mimari yapısı ve birden fazla bileşenin toleranslarından dolayı analog filtrelerin anomaliliğini tespit etmek üzere frekans özelliklerini kullanan Mahalanobis mesafesine (MD) dayalı bir yaklaşım önermişlerdir [20]. Frekans özellikleri, giriş sinyali olarak bir tarama sinyali kullanılarak CUT çıkışlarından elde edilmiştir. Ardından sağlıklı öznitelik örnekleri Mahalanobis mesafesi kullanılarak tek boyutlu mesafe verilerine dönüştürülmüştür. Normal profili temsil eden MD veri setinin olasılık yoğunluğunu tahmin etmek için Parzen pencere yoğunluğu yöntemi kullanılmıştır. Bununla birlikte belirlenen eşik değeriyle her test örnekleme ve sağlıklı mesafe veri seti arasında Mahalanobis değerinin eşik değeriyle karşılaştırılıp anomalilerin tespiti sağlanmıştır. Deneyler Sallen-Key bant geçiren filtre ve biquad alçak geçiren filtre olmak üzere iki vaka çalışması olarak gerçekleştirilmiştir. Sonuçlar önerilen Mahalanobis mesafesine dayalı yaklaşımın, analog filtrelerdeki anomalileri OCSVM tabanlı yöntemle göre daha yüksek doğrulukta ve daha erken bir zamanda tespit ettiği görülmüştür.

Christensen ve arkadaşları, moment temelli bir yaklaşım kullanarak soğutma sistemlerinde uygulanabilirlik açısından hataları tespit eden bir çalışma gerçekleştirmişlerdir [60]. Çalışma kapsamında diğer literatür çalışmalarından farklı olarak Mahalanobis mesafesinde kovaryans matrisi yerine moment matrisiyle yer değiştirildiği ve hesaplanan değere uygun bir eşik değeri belirlenmiştir. Moment matrisinin, veri örneklerinin dağılımını tahmin etmek ve ters moment matris polinomunu genişletmek gibi temel bir işlevin mevcut olduğu ifade edilmiştir. Sonuç olarak önerilen yöntem, soğutma kaplarında $d \leq 3$ için hesaplama açısından uygulanabilir olup doğruluğu koruyan ve mevcut yöntemlerden daha iyi performans elde

ettiği görülmüştür. Ancak $D = 4$ olduğunda moment matrisinin beklenen sonuçlara daha yakınsandığı ve dağılımın şeklini daha doğru yakalayabildiği gözlemlenmiştir.

Salem ve arkadaşları, tıbbi kablosuz sensör ağlardan (WSN) toplanan verilerdeki anomali ölçümleri doğru bir şekilde tespit etmeyi ve tutarsız sensörler okumaları tarafından tetiklenen yanlış alarmları azaltmak için hatalı ölçümler ve klinik acil durumlar arasında ayırım yapan bir model önermişlerdir [61]. Çalışma kapsamında, bazı fizyolojik parametreleri izlemek ve toplanan verileri analiz etmek üzere bir akıllı telefona iletmesi ve hasta sağlığı kötüleştiğinde bakıcıya alarm verecek birçok sensörün hastaya eklendiği bir senaryo geliştirilmiştir. Uzamsal analiz için Mahalanobis mesafesine ve anomali zamansal modellerin belirlenmesi için çekirdek yoğunluğu tahmin edicisine (KDE) dayalı bir yaklaşım kullanılmıştır. Sapmaları tespit etmek için eşik değeri kullanılmakta olup önceden tanımlanmış bir eşikten daha büyük değere sahip olduğunda, aykırı değerleri tespit etmek üzere KDE etkinleştirilmektedir. Önerilen yaklaşım deneyleri, hem sentetik hem de anomali verileri içeren gerçek fizyolojik veri setleri üzerinde gerçekleştirilmektedir. Sonuçlar değerlendirildiğinde, %100 tespit oranı ve %5,5 yanlış alarm oranı elde edildiği görülmüştür.

Dai'nin yürüttüğü çalışmada [62], yüksek boyutlu veri setlerinde ters kovaryans matrisinin tahmin etmede kötü performans gösteren Mahalanobis mesafesi için farklı koşullarda çeşitli Mahalanobis özniteliklerini içeren bir çalışma gerçekleştirilmiştir. Bununla birlikte Mahalanobis mesafelerinin açık dağılımlarını ve normal varsayım olmaksızın MD'lerin asimptotik dağılımlarını bulmak üzere iki çözüm önerilmiştir. Ayrıca kovaryans matrisini oluşturmak için faktör modeli kullanılarak değişkenleri daha az sayıda gruba sınıflandırarak yapılandırılmış veri setleri için ters matris tahminini basitleştiren faktör modeli ve Mahalanobis mesafesini birleştiren bir yaklaşım da geliştirilmiştir. Sonuç olarak yapılandırılmış veri seti değişkenlerinden aykırı değerlerin tespit edilmesine katkı sağlanmıştır.

Patil ve arkadaşları, yalıtımlı kapılı bipolar transistörlerde (IGBT) anomalileri tespit etmek için Mahalanobis mesafesine dayalı bir arıza tespit yaklaşımı önermişlerdir [18]. Anomalileri tespit etmek için sağlıklı verilerde elde edilen Mahalanobis mesafesi değerleri Box-Cox dönüşümü kullanılarak dönüştürülmüştür. Ardından dönüştürülen verilerden anomalilik tespitini gerçekleştirecek üç standart sapma sınırından oluşan eşik değeri elde edilmiştir. Elektrik-termal stres deneylerinden elde edilen veriler üzerinde deney sonuçları incelendiğinde, VCE'de %5'lik değişime dayalı tek parametre eşiği kullanılarak anomali

süreleri karşılaştırılmıştır. Tek parametre yerine birden çok parametre kullanılarak gerçekleştirilen deneylerde ise Mahalanobis mesafesine dayalı yaklaşımın tüm cihazlarda anomalileri arızadan önce tespit edebileceği gözlemlenmiştir.

Tian-yi ve arkadaşları tarafından kademeli olarak aykırı değerleri yeni kümeleme merkezleri olarak algılayan ve küme merkezlerini ayarlamak ve birleştirmek için olasılık kümelemesini kullanan Artırmalı Olasılık Kümeleme algoritması önerilmiştir [59]. İlk olarak bellek yükünü azaltmak için kayan istatistikler yerine sönümlü artımlı istatistikler yoluyla ağ akışının çok boyutlu öznelikleri çıkarılmıştır. Ardından IPC algoritması ile normal trafik modeli oluşturulmuş ve Mahalanobis mesafesine dayalı anomali paketlerin tespiti gerçekleştirilmiştir. Deney sonuçları değerlendirildiğinde %98,8 anomali paket tespit oranı ve %1 hata oranı elde edilmiştir.

Nguyen ve Vu; Robust Mahalanobis mesafesi, uzamsal otokorelasyon analizi ve sağlam istatistiklerin kombinasyonuna dayalı jeokimyasal anomalileri tanımlamak için yeni bir yaklaşım önermişlerdir [63]. Jeokimyasal veri setlerinin boyutunu azaltmak için minimum kovaryans belirleyici (MCD) tahmin ediciye dayalı sağlam Mahalanobis mesafesi kullanılmıştır. Daha sonra uzamsal korelogram ve yerel Moran istatistikleri sırasıyla küresel ve farklı yerel ölçeklerde uzamsal değişkenliği belirlemek ve uzamsal otokorelasyon derecesini ölçmek için uygulanmıştır. Son olarak sağlam istatistik temelli MEDYAN $\pm 1.5 \cdot IQR$ kuralı pozitif ve negatif anomalileri tespit etmek üzere eşik değeri olarak kullanılmıştır. Dere çökeltisi verileri kullanılarak elde edilen bulgular değerlendirildiğinde, uzamsal otokorelasyon analizi ve sağlam istatistiklere dayalı kombinasyonun çok değişkenli veriler üzerinde jeokimyasal anomalileri tespit etmede etkili bir yöntem olduğu gözlemlenmiştir.

Srinivasan ve Vaidehi, diğer dedektörlere entegre edilmek üzere Mahalanobis mesafesi ve benzerlik ölçüsüne dayalı geleneksel saldırı tespit sistemleri tarafından üretilen yanlış alarmların sayısını büyük ölçüde azaltan bir öneri sunmuşlardır [7]. Ağ etkinliklerinin istatistiksel bir modeli yük kullanılarak oluşturulup belirli bir süre boyunca ağdaki kullanıcıların normal davranışlarıyla eğitilmiştir. Uygulama yükünün bayt frekansı, yük uzunluğu ve bağlantı numarasına bağlı olarak her normal paket için hesaplanmıştır. Ardından Mahalanobis mesafesi ve benzerlik ölçüsü kullanılarak gelen yeni verilerin önceden hesaplanmış değerlerle benzerliğini ölçülmüştür. Hesaplanan mesafe bir eşik değeriyle karşılaştırılır ve eşik değeri aşırsa uyarı oluşturulmuştur. Sonuç olarak önerilen

yöntemin ağ paketlerini tamamen veya belirli bir süre boyunca analiz ederek yeni saldırıları erken tespit etme yeteneğine sahip olduğu ve sistem performansını minimum kaynak tüketimi ile büyük ölçüde artırdığını göstermiştir.

Khalastchi ve arkadaşları, Mahalanobis mesafesi ve gerçek zamanlı otonom robotlardan toplanan verilere dayalı anomalileri algılamak için ODDAD adlı yeni bir yaklaşım sunmuşlardır [64]. ODDAD; veri filtreleme, öznitelikler arası bağımlılığa dayalı öznitelik gruplaması ve her grup için aykırı tespit olmak üzere üç adımdan oluştuğu anlatılmıştır. Ayrıca çalışma kapsamında nokta, bağlamsal ve toplu olmak üzere üç genel anomali kategorisini tespit edebilen Mahalanobis mesafesinin otonom sistemler alanında kullanılması sağlanmıştır. Önerilen ODDAD yaklaşımının, insansız hava araçları (İHA), bir vakumlu temizleme robotu, yüksek kaliteli bir uçuş simülatörü ve bir uzay aracının elektrik güç sistemi gibi farklı alanlardaki veri setleri üzerinde deneyleri gerçekleştirilmiştir. İnsansız hava araçları (İHA), bir vakumlu temizleme robotu, yüksek kaliteli uçuş simülatörü ve bir uzay aracının elektrik güç sistemi üzerinde yürütülen deney sonuçları değerlendirildiğinde, gerçek dünya anomalilerini %0,06'lık yanlış alarm oranıyla tespit edebildiği görülmüştür.

Park ve arkadaşları, özellikle DDoS tipi saldırıları tespit edebilecek olasılıklı analize dayalı yeni bir ağ saldırı tespit sistemi önermişlerdir [65]. Ağ trafiğindeki anomalileri tespit etmek için Mahalanobis mesafesi hesaplanmakta olup bu mesafe göre sezgisel bir eşik değeri belirlenmiştir. Belirli ortalama ve varyans ile çok değişkenli normal dağılımla modellenebileceği varsayılan 2-D özellik alanında, iki anomali belirtisi olan TCP çıkışı ve CPU kullanımı özellik olarak kullanılmıştır. Normal dağılım gösteren Mahalanobis mesafe verilerinin eşik değeriyle karşılaştırılması sonucunda saldırı tespiti gerçekleştirilmiştir. Simüle veri seti üzerinde deney sonuçları değerlendirildiğinde ise Mahalanobis mesafe eşiklerinin anomali tespiti için oldukça iyi bir kriter olduğu görülmüştür.

Cerquitelli diğer literatür çalışmalarından farklı olarak binalarda termal enerji tüketim sensörlerinden sağlanan ölçümlerde anomali değerleri tespit etmek üzere veri madenciliği odaklı bir motor olan SPEC'i (Enerji Tüketiminin Ölçeklenebilir Tahmini) önermiştir [66]. SPEC enerji tüketim tahmininde anomali değerleri tespit etmek için iki stratejiden yararlanmaktadır. Birinci olarak çeyrekler arası aralık, medyan, çeyrekler, minimum ve maksimum değerlerin hesaplanmasıyla frekans dağılımı modellenir. İkinci ise Mahalanobis mesafesine dayalı enerji verileri üzerinde enerji tüketiminin diğerlerinden farklı olup olmadığını tespit eden ve belirlenen eşik değerine göre ileri bir analitik adıma gerek olup

olmadığını belirleyen stratejidir. Büyük bir şehrin termal enerji tüketim verileri üzerinde SPEC değerlendirildiğinde, oldukça doğru bir tahmin modeli oluşturma potansiyeli gösterdiği görülmüştür.

Vilaca ve arkadaşları, sağlam temel bileşen analizi (RPCA) ve Mahalanobis mesafesi yaklaşımlarından oluşan ve botnetler tarafından oluşturulan anomali ağ trafiğinin otomatik tespit edilmesini amaçlayan RPCA-MD yöntemini önermişlerdir [67]. RPCA-MD yaklaşımı, Çek Cumhuriyeti CTU Üniversitesi'nde 2011 yılında yakalan botnet trafiğinden oluşan CTU-13 veri seti üzerinde değerlendirilmiştir. Sonuçlar duyarlılık, tespit oranı ve f1-skor bakımından değerlendirildiğinde sırasıyla %81,2, %81,5 ve %81,8 başarı elde edildiği gözlemlenmiştir.

Hou ve arkadaşlarının yaptığı çalışmada [68], Çekişmeli Üretici Ağlar (GAN) uygulanarak verileri modelleyen ve Mahalanobis mesafesi kullanılarak anomalileri tespit eden MDAN olarak bilinen etkili bir yöntem önerilmiştir. MDAN yöntemi, geleneksel GAN tabanlı yöntemlerden daha iyi performans gösterdiği ve görüntü veri setlerine uygulandığında daha yüksek bir çıkarım hızına sahip olduğu belirtilmiştir. Deneyler ağ veri seti olan KDD CUP99, görüntü veri setlerini içeren SVHN ve 6 tür hayvan ve 4 tür taşıma içeren CIFAR-10 veri setleri üzerinde yürütülmüştür. KDD Cup99 veri seti üzerinde yürütülen deneylerde %96,23 tespit oranı ve %95,47 f1-skor oranı elde edildiği görülmüştür. SVHN resim veri seti deneylerinde %61,85 AUROC değeri elde edilirken, CIFAR-10 veri seti üzerinde ise %60,35 elde edilmiştir.

Daneshgadeh Çakmakçı ve arkadaşları; Shannon entropi, KOAD, Mahalanobis mesafesi ve ki-kare testine dayalı protokol tabanlı (TCP, UDP, DNS, ICMP) flooding saldırını tespit eden çevrimiçi bir DDoS algılama çerçevesi önermişlerdir [69]. Başlangıçta algılama ölçümleri kullanılarak dakika başına ağ akışlarından dört entropi tabanlı ve dört istatistiksel öznitelik çıkarılmaktadır. Ardından DDoS olduğundan şüphelenilen giriş vektörlerini tespit etmek için entropi özelliklerini kullanan çekirdek tabanlı öğrenme algoritması kullanılmıştır. Son olarak normal davranışın alt uzayını kapsayan bir öznitellik sözlüğü oluşturulup her T dakikada şüpheli vektörler arasında mesafe ve sözlük üyelerinin dağılımı ölçülmüştür. Mahalanobis mesafe değerlendirmesi de ki-kare testi kullanarak gerçekleştirilmektedir. CICIDS2017 veri seti kullanılarak yürütülen deneyler sonuçları incelendiğinde %95,23 anomali tespit oranı ve %0,9 yanlış alarm oranı elde edildiği belirtilmiştir.

Hoque ve arkadaşları tarafından DDoS saldırılarını tespit etmek için örnekler arasında korelasyonların hem kaymasını hem de ölçeklenmesini yönetebilen gerçek zamanlı bir korelasyon ölçüsü olan NaHiD yöntemi önerilmiştir [70]. Yöntem kapsamında dinamik olarak tüm öznitelikler arasında korelasyon değerleri hesaplanıp normal ağ trafiğini içeren profil oluşturulmuştur. Ardından normal ve gözlenen trafik arasında hesaplanan korelasyon değeri belirli bir eşik değerinden büyük olması durumunda, sistemde bir saldırının meydana geldiğini belirten alarm üretilmiştir. Yöntemin etkinliği; CAIDA DDoS 2007, MIT DARPA 2000 ve TUIDS olmak üzere üç ağ veri seti ve FPGA kartlar kullanılarak değerlendirilmiştir. FPGA donanımlarında, bir saldırıyı 354 nano saniyede tespit edebildiği görülmüştür. Diğer sonuçları değerlendirildiğinde CAIDA veri setinde %99,95 tespit oranı ve %0 yanlış alarm oranı elde edildiği, DARPA 200 veri setinde ise %100 tespit oranı ve %0 yanlış alarm oranı elde edildiği ifade edilmiştir.

Shukla ve Maurya'nın yürüttüğü çalışmada [71], açık kaynaklı saldırı tespit sistemi Snort aracılığıyla tüm ağ trafiğini toplayan entropi tabanlı ağ anomalilerini algılayan bir yöntem önermişlerdir. Veriler toplandıktan sonra oluşturulan çok sayıda öznitelikten alt özniteliklerin seçilmesi için Snort uyarısı işlenmiştir. Ardından mevcut ağın normal davranışını ölçmek için Shannon entropileri hesaplanmakta olup şebeke saldırısını tespit etmek için hesaplanan Shannon vektörüne Renyi çapraz entropi yöntemi uygulanmıştır. Deney sonuçları değerlendirildiğinde yaklaşık %90 saldırı tespit oranı elde edildiği görülmüştür.

Gottwalt ve arkadaşları, çok değişkenli korelasyon (CorrCorr) tabanlı öznitelik seçim yöntemi ve Mahalanobis mesafesine dayalı ağ trafiğindeki anomalileri tespit eden bir yöntem önermişlerdir [12]. CorrCorr öznitelik seçim algoritmasından elde edilen alt öznitelik kümesinden yasal ağ trafiği kullanılarak normal bir ağ profili oluşturulmuştur. Ardından yeni gelen bir ağ örneğiyle oluşturulan normal ağ profilinin benzerliğini ölçmek için istatistiksel tabanlı Mahalanobis mesafesi kullanılmıştır. Son olarak, elde edilen mesafe değerleri üzerinde standart sapmaya dayalı 1-3 arası değişen eşik değeriyle karşılaştırılarak anomali ağ trafiği tespit edilmiştir. UNSW-NB15 veri kullanılarak gerçekleştirilen deney sonuçları incelendiğinde sıfırıncı eşik seviyesinde %100 tespit oranı ve %7,88 yanlış alarm oranı elde edildiği belirtilmiştir. Eşik seviyesi arttıkça anomali tespit oranının %100'den %56,80'e düştüğü gözlemlenmiştir.

3.3. Öznitelik Seçimine Dayalı Çalışmalar

Wu ve Zhang ve arkadaşları tarafından faktör analizine dayalı öznitelik çıkarımı ve Mahalanobis mesafesi kullanılarak yeni bir anomali algılama ve kümeleme algoritması sunulmuştur [37]. Faktör analizi çok sayıda değişken arasında karşılıklı ilişkileri analiz edip orijinal değişkenlerin içerdiği bilgileri minimum bilgi kaybıyla daha küçük boyutlu veri kümesine yoğunlaştırmak için kullanılmıştır. Önerilen yöntemde, faktör analizi ile eğitim veri setinin boyutu azaltılıp Mahalanobis mesafesi ile anomali olup olmadığı incelenmiştir. Anormal bir durum tespit edildiğinde ise anomali değerlere sahip faktörler, saldırı mekanizmalarına için ilişkin içgörüler sağlamak ve saldırı-yanıt sistemine yardımcı olmak adına kümeler halinde sınıflandırılmıştır. DARPA veri seti üzerinde gerçekleştirilen deney sonuçları incelendiğinde %84,4 tespit oranı ve %1 yanlış alarm oranı elde edildiği belirtilmiştir.

Gottwalt ve arkadaşları [12], hedef değişkeniyle en yüksek korelasyona sahip özniteliklerin anomali tespit sistemlerinin performansını artırmada daha kullanışlı olduğunu varsayan CorrCorr (çok değişkenli korelasyon analizine dayalı) öznitelik seçim yöntemini önermişlerdir. İlk aşamada, iki öznitelik arasında korelasyonu temsil eden matris oluşturulmuştur. Ardından sınıf etiketini tahmin etmede kullanılacak en ilgili öznitelik çiftini belirlemek için simetrik tau korelasyon ölçüsü uygulanmıştır. Son olarak, anomali ağ trafiğini tespit etmek ve normal ile gelecekteki gelen olaylar arasında benzerliği ölçmek için Mahalanobis mesafesi kullanılmıştır. UNSW-NB15 ve NSL-KDD veri setleri üzerinde gerçekleştirilen deneyler incelendiğinde, sıfıncı eşik seviyesinde en yüksek %100 tespit oranı ve %7,88 yanlış alarm oranı elde edildiği gözlemlenmiştir. Eşik değeri seviyesi arttıkça anomali tespit oranının %100'den %56,80'e doğru aniden düştüğü görülmüştür.

Eid ve arkadaşlarının önerdiği [10] ve tez çalışmamızda da kullandığımız doğrusal korelasyon katsayılarının analizine dayalı optimal öznitelik alt kümesini seçen yeni bir yöntem önermişlerdir. Pearson korelasyona dayalı öznitelik seçimi, birinci katmanda öznitelikler arasında gereksiz özniteliklerin çıkarılması ve ikinci katmanda sınıf etiketiyle en yüksek korelasyon ilgi düzeyine sahip öznitelikleri belirleyecek şekilde uygulanmıştır. KDD CUP99 veri seti üzerinde yapılan deneylerde öznitelik sayısı 41'den 17'ye düşürüldüğünü ve bunun da sınıflandırma doğruluğunu %99,1 oranına yükselttiği görülmüştür. Deney sonuçları PCA, bilgi kazancı ve önerilen LCFS öznitelik seçimi bakımından değerlendirildiğinde sırasıyla %97,6, %98,6 ve %99,1 f1 skor değerleri elde edildiği belirtilmiştir.

Zhiyuan Tan ve arkadaşları tarafından yürütölem alıřmada [24], ađ trafiđi öznitelikleri arasında geometrik korelasyonların ıkarılmasıyla dođru ađ trafiđi karakterizasyonu iin ügen alan tabanlı ok Deđiřkenli Korelasyon Analizini (MCA) kullanan bir DoS saldırı tespit sistemi sunulmuřtur. İlk teknik, her ađ trafiđi kaydında iki farklı özniteliđin ayrı iftlerinde gizlenen geometrik korelasyonları ıkarırken ikinci teknik, sistemde hem bilinen hem de bilinmeyen DoS saldırılarının meřru ađ trafiđinden ayırt edebilmesini kolaylařtırılmıřtır. KDD Cup 99 veri seti üzerinde deney sonuçları deđerlendirildiđinde normalize edilmemiř veriler üzerinde %95,11 tespit oranı, %95,20 dođruluk ve en düřük %1,26 yanlış alarm elde edilmiřtir. Normalize veriler üzerinde ise %99,97 tespit oranı ve %1,68 yanlış alarm oranına ulařıldıđı gözlemlenmiřtir.

Hoang ve arkadaşları, diđer öznitelik alıřmalarından farklı olarak Nİ ađlarında anomali tespiti iin kullanılan PCA tekniklerini arařtırıp mesafe hesaplaması iin yeni bir uzaklık formölüne dayalı PCA-NTAD řemasını önermiřlerdir [72]. Önerilen yeni yöntemin, düřük karmařıklıkla ađ trafiđi anomalilerinin hızlı tespit edebilmesi iin sadece birkaç bilgisayara ihtiya bulunduđu belirtilmiřtir. Deneyler, gerek veri seti olan Kyoto 2006+ üzerinde ađ katmanının ve taşıma katmanının trafik verilerden en önemli öznitelikler dahil olmak üzere ön dört temel öznitelik kullanılarak gerekleřtirilmiřtir. Deney sonuçları deđerlendirildiđinde %91,3 ile %94,4 arası en yüksek anomali tespit oranı elde edilirken, en düřük yanlış alarm oranının da %4,7 ile %5,6 arası elde edildiđi belirtilmiřtir.

Li ve arkadaşlarının yürüttüđu alıřma [23] kapsamında, farklı polinom formlarını kullanarak ađ trafiđinde ayırt edici öznitelikleri sađlamak ve gizli korelasyonları ortaya ıkarmak iin polinom öznitelik korelasyon tekniđini kullanan anomali tabanlı bir tespit mekanizması önerilmiřtir. Önerilen sistemin korelasyon üzerinde uyguladıđı deđerlemlerle hesaplama karmařıklıđı azaltılırken, tespit performansı üzerinde hiçbir etkiye neden olmadıđı gözlemlenmiřtir. KDD Cup 99 veri seti üzerinde gerekleřtirilen deneyler sonucunda, %100'e yakın anomali tespit oranı ve %0,13 en düřük yanlış alarm oranı elde edilmiřtir.

Wang ve arkadaşları, sabit diskler üzerinde kritik parameterleri seçmek iin FMMEA (arıza modları, mekanizma ve etki analizi) ve mRMR (minimum artıklık maksimum ilgililik) dahil olmak üzere iki ařamalı bir öznitelik seçim yaklařımı geliřtirmiřlerdir [19]. FMMEA, olası arıza mekanizmalarıyla ilgili bir dizi özniteliđi seçmek iin kullanılmıřtır. Ancak FMMEA parametreler arasında korelasyonu hesaba katmadıđından seçilen parametrelerin gereksiz olma durumu bulunmaktadır. Bu nedenle ikinci ařamada, öznitelikleri hedef deđerlemlerle

alaka düzeyine göre sıralayabilen ve gereksiz öznitelikleri hariç tutan mRMR yöntemi uygulanmıştır. Geliştirilen yaklaşımın performansını değerlendirmek adına kendi kendini izleme, analiz etme ve raporlama teknolojisinin (SMART) veri seti kullanılmıştır. Yürütülen deneyler sonucunda, %67 tespit oranı ve %0 yanlış alarm oranı elde edildiği gözlemlenmiştir.

Gottwalt ve arkadaşları, diğer çalışmalardan farklı olarak korelasyon tekniklerinde öznitelikler arasındaki zamansal korelasyon değişikliklerinin seçim sürecinde dikkate alınması durumunda tespit performansının iyileştirilebileceği varsayımını değerlendirmek üzere çok değişkenli korelasyona dayalı tekniklerin özelliklerini ve yaygın kullanılan iki öznitelik seçim yöntemini niteliksel olarak analiz eden bir çalışma gerçekleştirmişlerdir [73]. UNSW-NB15 veri seti üzerinde gerçekleştirilen deney sonuçları değerlendirildiğinde Pearson korelasyonu tarafından seçilen özniteliklerin 50 bin numune için 0,975 AUC skoruyla diğer tüm farklı numune boyutları arasında en iyi sonucu verdiği belirtilmiştir. Ortalama olarak Pearson korelasyon öznitelikleri, orijinal özniteliklere göre ~% 9'luk bir performans artışı sağlarken, PCA bileşenleri ise orijinal özniteliklere kıyasla yaklaşık %3'lük bir performans kaybına neden olduğu görülmüştür.

Al-Jarrah ve arkadaşları, ileriye seçim ve geri doğru eleme tekniklerine dayalı saldırı tespit sistemlerinin performansını artırmaya yardımcı olabilecek RFFSR (RandomForest-Forward Selection Ranking) ve RF-BER (RandomForest Backward Elimination Ranking) gibi iki farklı yeni öznitelik seçim yöntemlerini önermişlerdir [43]. Önerilen yöntemler yaygın olarak bilinen KDD Cup 99 ve NSL-KDD veri kümeleri üzerinde değerlendirilmiştir. Deney sonuçları değerlendirildiğinde, önerilen yöntemler ile seçilen özelliklerin tespit oranı ve yanlış alarm oranını etki bir şekilde iyileştirdiği görülmüştür. Sonuç olarak KDD Cup 99 veri setinde %99,8 tespit oranı ve %0,001'e yakın yanlış alarm oranı elde edilmiştir.

Jin ve arkadaşları, soğutma fanlarının sağlığının izlenmek için mRMR (Minimum artıklık maksimum uygunluk) öznitelik seçimine ve Mahalanobis mesafesine dayalı bir anomali tespit yöntemi önermişlerdir [74]. MRMR kriterlerine dayalı öznitelik seçimi, veri kümesinin boyutsallık ve fazlalık sorunlarını çözmek ve soğutma fanlarının özniteliklerini etkili bir şekilde temsil etmek için kullanılmıştır. Deneyler, bilyeli rulmanlarda yağlayıcı bulunmayan soğutma fanlarından veri setinin toplanması ve bilyalı rulmanlara herhangi bir yağ eklenmeyerek yağlayıcı kaybının simüle edilmesiyle gerçekleştirilmiştir. Eşik değeri iki olarak ayarlandığında eğitim veri seti doğrulununun %100 olduğu ve test sınıflandırma

doğruluğunun %98 olduğu görülmüştür. Sonuç olarak önerilen yöntemin soğutma fanlarının sağlığını izlemede uygulanabilir olduğu ve kalan faydalı ömrü (RUL) ve değişimin tahmin edilmesine yardımcı olduğundan üreticilere katkı sağlayan bir çalışma olduğu bahsedilmiştir.

Biesiada ve arkadaşları, Pearson χ^2 testine dayalı ikili ikili rastgele değişkenin olasılık dağılımı arasında farkı ölçen ve gereksiz olmayan gruplanmış öznitelik alt kümelerini bulmak için PRBF isminde yeni bir algoritma tanıtmışlardır [35]. İlk aşamada, alaka düzeylerinin azalan değerine göre sıralı bir öznitelik listesi oluşturulmuştur. Ardından Pearson χ^2 göre gereksiz öznitelikler denetimsiz bir şekilde kaldırılmıştır. Medikal yapay veri setleri olan Gauss4 ve Gauss8 üzerinde yürütülen sonuçlar incelendiğinde PRBF öznitelik seçim algoritması %79,07 doğruluk oranıyla diğer FCBF, CorrSF, ReliefF ve ConnSF algoritmalarıyla benzer bir başarıya ulaştığı görülmüştür. Dengeli veri seti üzerinde yapılan sonuçlarda ise %82,69 doğruluk oranı elde edilmiştir.

Zhang ve Wang, ağ saldırı tespitinde uygulanabilen Bayes Ağları sınıflandırıcısına dayalı etkili bir sarmalayıcı öznitelik seçim yaklaşımını önermişlerdir [11]. Yaklaşım tarafından seçilen öznitelikler hem saldırıları tespit etme süresini kısalttığı hem de sınıflandırma doğruluğu ve gerçek pozitif oranlarını önemli ölçüde arttırdığı belirtilmiştir. WEKA açık kaynak projesi kullanılarak NSL-KDD veri seti üzerinde uygulanan model sonuçlarının; IG, GR, ReliefF ve Ki-Kare yöntemleriyle karşılaştırıldığında diğerlerine göre %2,5 farkla %98,98 doğruluk oranı elde ettiği gözlemlenmiştir.

Dash ve arkadaşları tarafından yürütülen çalışmada [75], daha önce kullanılan sarmalayıcı yöntemlerden farklı olarak herhangi bir kümeleme algoritmasından bağımsız en iyi alt kümeyi seçmek için bir filtre yöntemi önerilmiştir. Çalışma kapsamında en önemli öznitelik alt kümesini seçmek için boyut sayısı ile değişmeyen, yalnızca küme kalitesinden etkilenen bir entropi ölçüsü de sunulmuştur. Sentetik ve gerçek veri kümeleri üzerinde yürütülen kapsamlı performans değerlendirmesinde, önerilen yöntemin kümeleme yapmadan önce kümeler hakkında herhangi bir ön bilgi mevcut olmasa bile en önemli alt kümeyi doğru bir şekilde keşfettiği görülmüştür.

Yu ve arkadaşları, alaka analizi için C-korelasyonu ve artıklık analizi için hem C hem de F-korelasyonlarını kullanan korelasyon tabanlı bir öznitelik seçim yöntemi önermişlerdir [15]. Çalışma kapsamında diğer literatür çalışmalarından farklı olarak yüksek boyutlu veriler üzerinde tek başına öznitelik ilişkisinin yetersiz olduğu gösterilmiştir. UCI Benchmark ve

NIPS 2003 veri setleri üzerinde gerçekleştirilen kapsamlı deneylerde önerilen FCBF algoritması, gözetimli öğrenmede öznitelik seçimi verimliliğini ve etkinliğini göstermiştir. Sonuç olarak UCI sentetik veri seti ve C4.5 gözetimli öğrenme algoritması kullanılarak diğer ReliefF, CFS-SF ve FOCUS-SF öznitelik seçim algoritmalarıyla karşılaştırıldığında %93,65 doğruluk oranı elde ettiği belirtilmiştir.

Anwer ve arkadaşlarının çalışmasında ise diğer öznitelik seçim algoritmalarından farklı olarak filtre ve sarma yöntemleri kullanılarak öznitelik seçimi için farklı stratejilerin uygulandığı bir çerçeve sunulmuştur [17]. Çalışma kapsamında en yüksek doğruluğu sağlayan minimum sayıda özneliğin elde edilmesi amaçlanmıştır. Önerilen yöntem, UNSW-NB15 veri kümesi üzerinde J48 ve Naïve Bayes olmak üzere iki makine öğrenimi sınıflandırıcısıyla filtre ve sarmalayıcı yöntemler kullanılarak beş ana strateji kullanan bir vaka çalışmasında uygulanmıştır. Deneyler sonucunda, GR filtre sıralama yönteminde 18 öznitelik kullanılarak ve J48 sınıflandırıcı uygulanarak %88 doğruluk oranının elde edildiği gözlemlenmiştir.

Dy ve arkadaşları, gözetimsiz öğrenmenin öznitelik seçimi sorunlarını ele almak ve önyargınlığı kaldırmak üzere sarmalayıcı yöntem olan Beklenti-Makzimizasyonu (EM) kümelemesi ve Öznitelik Alt Küme Seçimi (FSSEM) yöntemine dayalı çapraz projeksiyon kriter normalleştirme şeması önermişlerdir [16]. Iris, şarap, iyonosfer yüksek çözünürlüklü bilgisayarlı akciğer tomografi (HRCT) görüntü verileri üzerinde deney sonuçları değerlendirildiğinde, önerilen yöntemin ilginç kalıpları bulmada kümeleme algoritmalarının performansını artırdığını göstermiştir.

Ambusaidi ve arkadaşlarının yürüttüğü çalışma [33] kapsamında, öznitelikler ve çıktı arasında bağımlılığı değerlendirmek için Esnek Karşılıklı Bilgi Öznitelik Seçimi (FMIFS) adı verilen yeni bir filtre tabanlı öznitelik seçme yöntemi sunulmuştur. Önerilen FMIFS öznitelik seçimi gözetimli LS-SVM yönemiyle saldırı tespit sistemi oluşturmak için birleştirilmiştir. Yöntemin etkinliğini ve uygulanabilirliğini göstermek adına KDD Cup 1999, NSL-KDD ve Kyoto 2006+ veri setleri üzerinde deneyler gerçekleştirilmiştir. Deney sonuçları değerlendirildiğinde, KDD Cup 99 veri setinde %99,46 tespit oranı ve %0,13 yanlış alarm oranı; NSL-KDD veri setinde %99,76 tespit oranı ve %0,28 yanlış alarm oranı ve son olarak güncel veri seti olan Kyoto 2006+ deneylerinde ise %99,64 tespit oranı ve %0,13 yanlış alarm oranı elde edildiği görülmüştür. Doğruluk ölçütü bakımından KDD Cup

99, NSL-KDD ve Kyoto 2006+ veri setleri incelendiğinde sırasıyla %99,79, %99,91 ve %99,77 başarı oranlarına ulaştığı gözlemlenmiştir.

Z. Chen ve arkadaşları, Maksimal Bilgi Katsayısı (MIC) tabanlı öznitelik seçim algoritması ve anomali bilgileri daha verimli bir şekilde ayırabilen öznitelik tabanlı bir MSPCA tespit algoritmasından oluşan anomali tespit sistemi önermişlerdir [76]. Önerilen MIC yöntemi, öznitelikler ve etiketler arasında bağımlılığı yakalayabilen bir bilgi ölçümüdür. DARPA 1999 veri seti üzerinde tüm öznitelikler kullanılarak yürütülen deneylerde %80 anomali tespit oranı elde edilirken, seçilen öznitelikler kullanıldığında ise gerçek pozitif oranının %89,4'e yükseldiği görülmüştür.

Aghdam ve arkadaşları yürüttüğü çalışma kapsamında, saldırı tespit sistemlerinin performansını artırmak için kolayca uygulanabilen ve düşük hesap karmaşıklığına sahip Karınca Kolonisi Optimizasyonuna (ACO) dayalı öznitelik seçim algoritması önermişlerdir. Önerilen yöntemin, seçilen alt kümenin uzunluğunu sezgisel bir bilgi olarak benimsediğinden özniteliklerle ilgili ön bilgiye sahip olma gereksinimi bulunmadığı belirtilmiştir. Bununla birlikte problem alanında güçlü bir arama kabiliyetine sahip olduğundan minimum öznitelik alt kümesini verimli bir şekilde tespit edebilmektedir. KDD Cup 99 ve NSL-KDD veri setleri üzerinde deney sonuçları değerlendirildiğinde %98,9 doğruluk oranı ve %2,59 yanlış alarm oranı elde edilmiştir. Öznitelik sayına dayalı deney grafiklerinde dört öznitelikle en düşük yanlış alarm oranına ulaşılrken, beş öznitelik kullanıldığında en yüksek tespit oranına ulaşıldığı görülmüştür [13].

Diğer bir çalışma kapsamında Iglesias ve arkadaşları tarafından filtreler ve aşamalı regresyon sarmalayıcılarının kullanıldığı çok aşamalı bir öznitelik seçim yöntemi önerilmiştir. Diğer literatür çalışmalarından farklı olarak anomali tespitinde güçlü katkısı olan 16 öznitelik, düşük katkı sağlayan 14 öznitelik ve önemsiz olan 11 öznitelik de filtreler ve sarmalayıcıların bir kombinasyonuna göre sıralanmıştır. Ardından önerilen yöntemin performansını değerlendirmek adına karar ağacı, k-en yakın komşu (k-NN), naïve bayes, en küçük mutlak seçim ve en küçük aç regresyonlu büzülme operatörü, yapay sinir ağları ve destek vektör makineleri kullanılmıştır. Deneyler 41 öznitelik, 30 öznitelik ve 16 öznitelik olmak üzere NSL-KDD veri seti üzerinde 5-kat çapraz doğrulama yöntemi kullanılarak gerçekleştirilmiştir. Yürütülen deney sonuçları incelendiğinde, 41 öznitelik kullanılarak en yüksek başarıya %99,66 tespit oranıyla Naïve Bayes'in ulaştığı görülmüştür. Diğer 30 ve 16

öznitelik grubu kullanılarak yürütülen deneylerde ise karar ağacı, en yüksek tespit başarısını sırasıyla %85,53 ve %82,65 oranla elde ettiği gözlemlenmiştir [77].

Haq ve arkadaşları, saldırı tespit sistemlerinde sarmalayıcı arama olarak en iyi ilk (best first), genetik arama ve sıralayıcı arama yaklaşımlarını kullanan HFSA adlı hibrit bir öznitelik seçim yöntemi önermişlerdir [78]. Çalışma kapsamında, iyi bilinen NSL-KDD veri kümesinde 3 sarmalayıcı aramayla seçilen minimum miktarda özniteliği kullanan ve aralarındaki karşılaştırmaları gösteren bayes ağlar, naïve bayes ve J48 sınıflandırıcılarının sınıflandırma kesinliğine odaklanılmıştır. Sonuç olarak hibrit öznitelik seçme yöntemi kullanılarak 12 kritik öznitelik seçilerek normal ve anomali değerleri ayırt etmek için güvenilir bir model geliştirilmiştir. HFSA deney sonuçları değerlendirildiğinde, %98 tespit oranı ve %0,021 yanlış alarm oranı elde edildiği belirtilmiştir.

Jyothsna ve arkadaşlarının yürüttüğü çalışmada [79], anomali tabanlı saldırı tespit sistemlerinde uygulanmasını amaçlayan öznitelik korelasyon analizi ve ilişkilendirme etki ölçeği (FCAAIS) adı verilen bir meta-sezgisel değerlendirme modeli önerilmiştir. Önerilen stratejide yüksek sınıflandırma doğruluğuyla izinsiz girişleri tespit etmek ve eğitim verilerinden çıkarılan kuralların karmaşıklığının azaltılmasına yönelik öznitelikleri optimize etmek için doğrusal kanonik korelasyon ve seçilen optimum özniteliklerden öznitelik ilişkilendirme etki ölçeği araştırılmıştır. Deneyler kapsamında FCAAIS modelinin, işlem karmaşıklığını ve tamamlanma süresini en aza indirdiği ve maksimum tahmin doğruluğunu koruduğu belirtilmiştir. Performans sonuçları değerlendirildiğinde ise %98,5 tespit oranı elde edildiği gözlemlenmiştir.



4. YÖNTEM

Bu bölümde önerilen anomali tespit sisteminde kullanılan yöntemler hakkında bilgi verilecektir.

4.1. UNSW-NB15 Veri Seti

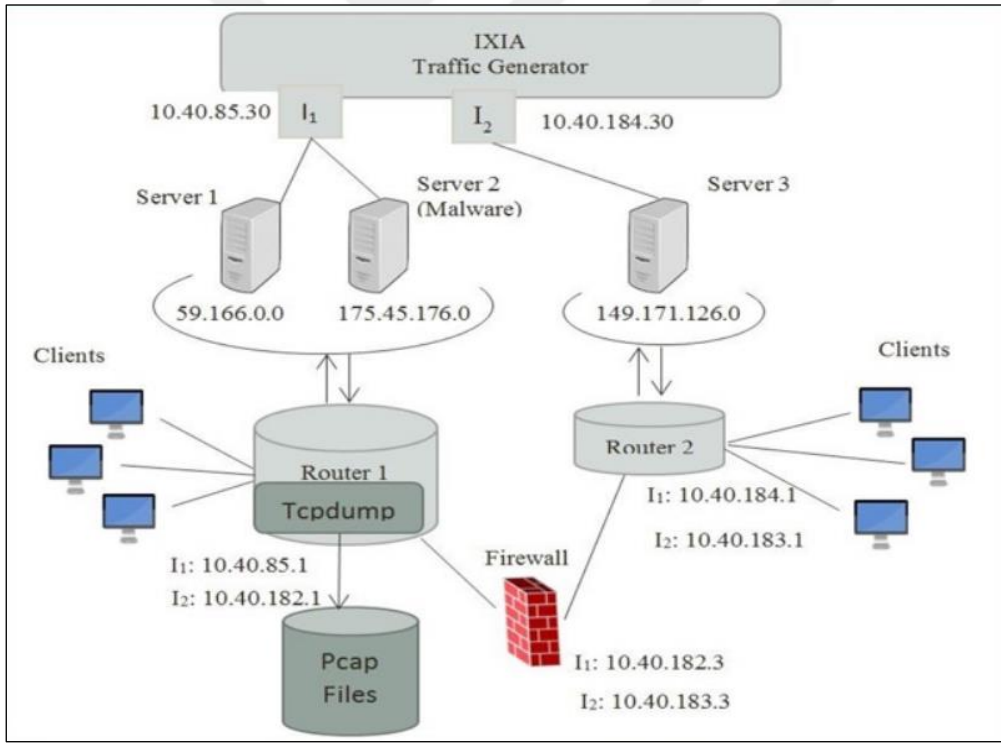
Saldırı tespit alanında yapılan çalışmalarda en büyük araştırma zorluklarından biri, modern ağ trafiği senaryolarını ve çeşitli saldırı izlerini içeren kapsamlı bir ağ veri setinin eksikliğidir. Saldırı tespit sistemleri için KDD Cup 1999 ve NSL-KDD gibi birçok veri seti önerilmiş ve bu veri setleri kullanılarak çok fazla araştırma yapılmıştır. Saldırı tespit sistemleri için uygun olan NSL-KDD ve KDDCUP99 veri setlerini incelediğimizde, araştırmacılar tarafından belirlenen üç dezavantajı olduğu görülmektedir [8]. İlk olarak, zaman geçtikçe saldırı tipleri normal davranışa benzer hale gelmiştir. Bu nedenle, belirtilen ağ veri setlerinin güncel olanlara göre eski kalmaktadır. İkinci olarak, veri seti 20 yıl önce önerildiğinden bugünkü ağ trafiğiyle kıyasladığımızda ağ hızı ve uygulamaları bakımından değişkenlik göstermektedir. Diğer bir dezavantajına baktığımızda, eğitim ve test veri setlerinin farkı dağılıma sahip olması sınıflandırma yönteminin çarpık ve yanlış değer üretip yanlış alarmların artmasına neden olduğu görülmektedir. Son olarak, veri paketlerinde yaşam zamanı olarak isimlendirilen (TTL) değer 126-253 arasında olduğu görülürken çoğu trafik paketinde 127-254 arasında olduğu saptanmıştır [8], [29]. Dolayısıyla, saldırı tespit sistemlerinin verimliliğini değerlendirmek üzere normal aktiviteleri ve saldırı aktivitelerini içeren modern kapsamlı bir veri setine ihtiyaç duyulmaktadır [29]. Çünkü veri setinin kalitesi uygulanacak saldırı tespit sisteminin güvenilir sonuç vermesini etkilemektedir [8]. Bu gibi zorlukların üstesinden gelmek üzere Cyber Range Lab of the Australian Center² tarafından hem gerçek modern ağ trafiğini hem de sentetik saldırı tiplerini içeren UNSW-NB15 veri seti önerilmiştir [80], [81].

UNSW-NB15 veri seti, Şekil 4.1’de görüldüğü gibi 3 sanal sunucu ve IXIA PerfectStorm aracı kullanılarak 22 Ocak 2015 tarihinde 16 saat ve 17 Şubat 2015 tarihinde 15 saatlik toplanan 100 GB ham veriden oluşturulmuştur [8], [82]. Bunlardan sunucu 1 ve sunucu 3 normal ağ trafiğini oluştururken sunucu 2 anomali ağ trafiği aktiviteleri için

² Australian Cyber Security Centre Laboratories, Erişim Tarihi: 30.04.2021, <https://unsw.adfa.edu.au/our-research/facilities/cyber-security-labs>

yapılandırılmıştır. Sunucular arasında iletişimi açık ve özel ağ trafiği şeklinde oluşturmak adına iki sanal router arayüzü bulunmaktadır.

Routerler aracılığıyla sunucular ana bilgisayara ve güvenlik duvarına bağlanarak normal trafiği ya da anomali trafiğini geçirecek şekilde konumlandırılmıştır. Ağ trafiğinin hızı ve modern saldırılarının oluşturulması için IXIA aracı, saniyede bir saldırı oluşturacak şekilde yapılandırılmış ve tcdump³ aracı kullanılarak router 1'den pcap simülasyon dosyaları olarak toplanmıştır. İlk simülasyonda 50 GB kadar veri toplanmıştır. İkinci simülasyonda da 50 GB ham veri toplanarak 100 GB ham ağ verisi elde edilmiştir [8]. Simülasyonda tcdump ile toplanan verileri Argus, Bro-IDS ve geliştirilen 12 algoritma aracılığıyla mevcut CSV dosyasına dönüştüren ve 49 özneliğin çıkarım işlemini gerçekleştiren bir mekanizma geliştirilmiştir. Mekanizma sonucunda 4 farklı CSV dosyası halinde oluşturulan veri seti ilk üç dosyada 700000 ve dördüncüde 440044 kayıt içermektedir [8].



Şekil 4.1. UNSW-NB15 veri setinin elde edildiği ağ sisteminin mimarisi [8]

³ <http://www.tcpdump.org/>

Çizelge 4.1. Veri setine ait öznelikler

Sütün No	Özellik İsmi	Veri Tipi	Sütün No	Özellik İsmi	Veri Tipi
1	Srcip	object	26	Res_bdy_len	int
2	Sport	object	27	Sjit	float
3	Dstip	object	28	Djit	float
4	Dsport	object	29	Stime	int
5	Proto	object	30	Ltime	int
6	State	object	31	Sintpkt	float
7	Dur	float	32	Dintpkt	float
8	Sbytes	int	33	Tcprtt	float
9	Dbytes	int	34	Synack	float
10	Sttl	int	35	Ackdat	float
11	Dttl	int	36	Is_sm_ips_ports	int
12	Sloss	int	37	Ct_state_ttl	int
13	Dloss	int	38	Ct_flow_http_mthd	int
14	Service	object	39	Is_ftp_login	int
15	Sload	float	40	Ct_ftp_cmd	int
16	Dload	float	41	Ct_srv_src	int
17	Spkts	int	42	Ct_srv_dst	int
18	Dpkts	int	43	Ct_dst_ltm	int
19	Swin	int	44	Ct_src_ltm	int
20	Dwin	int	45	Ct_src_dport_ltm	int
21	Stcpb	int	46	Ct_dst_sport_ltm	int
22	Dtcpb	int	47	Ct_dst_src_ltm	int
23	Smeansz	int	48	Attack_cat	object
24	Dmeansz	int	49	Label	int
25	Trans_depth	int			

Veri kümesi, dört CSV dosyası halinde belirtilen bağlantı⁴ kullanılarak indirilmiştir. Öznitelik sayısı bakımından veri seti incelendiğinde, Çizelge 4.1’de görüldüğü üzere sınıf etiketi dahil 49 öznitelikten oluşmakta ve öznitelik bakımından 5 farklı kategoride toplanmaktadır [29].

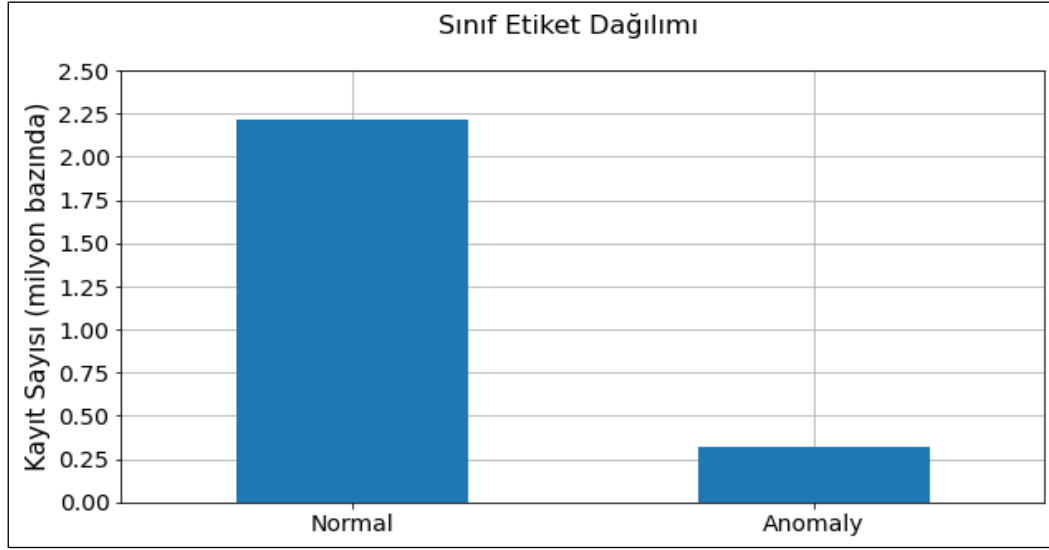
- *Akış Öznitelikleri*: Ana bilgisayarlar arasında sunucudan istemciye veya istemciden sunucuya tanımlayıcı öznitelikleri içerir.
- *Temel Öznitelikler*: Protokol bağlantıları, hedef kaynak arasında dosya boyutu ve paket sayısı gibi öznitelikleri içermektedir.
- *İçerik Öznitelikleri*: TCP/IP gibi özellikleri kapsüllemekle birlikte bazı HTTP servislerini de içerir.
- *Zaman Öznitelikleri*: Gelen paketler arasındaki zaman, başlangıç ve bitiş zamanı ve TCP protokolünün gidiş-dönüş zamanı gibi özellikleri içermektedir.
- *Ek Oluşturulan Öznitelikler*: Genel amaçlı (36-40 arası öznitelikler) ve bağlantı öznitelikleri (41-47 arası özellikler) olmak üzere iki farklı öznitelik grubu içermektedir.

Çizelge 4.2’de veri setinin içerdiği saldırı türleri, satır sayısı ve açıklama bilgileri verilmiştir. Saldırı türleri bakımından ele aldığımızda, Generic, Exploits, Fuzzers, Reconnaissance, DoS, Backdoors, Analysis, Shellcode ve Worms olmak üzere 9 farklı saldırı türü içerdiği görülmektedir [8]. Moustafa’nın ve Slay’ın yaptıkları çalışma göz önünde bulundurulduğunda, yeni saldırı tespit sistemlerini değerlendirmek için çarpıklık, basıklık ve veri seti özniteliklerinin istatistiksel bakımdan korelasyonlu olduğundan UNSW-NB15 veri setinin kullanılabilir olduğunu göstermektedir [29].

⁴ The UNSW-NB15 data set, Erişim Tarihi: 15.01.2021, <https://research.unsw.edu.au/projects/unsw-nb15-data-set>

Çizelge 4.2. Veri setine ait saldırı türleri ve saldırı sayıları

UNSW-NB15 Veri Setine Genel Bakış		
Saldırı Türleri	Satır Sayısı	Açıklama
Normal	2,218,761	Normal trafik verisi
Generic	215,481	Saldırganın bir işletim sistemi veya yazılımda bildiği güvenlik açığından yararlandığı saldırılardır.
Exploits	44,525	Saldırganların bir işletim sistemi veya yazılımdaki güvenlik açığından faydalandığı saldırılardır. bilinmesinen kaynaklanan
Fuzzers	24,246	Bir ağı veya program rastgele oluşturulmuş veriler ile askıya alma girişimidir.
Reconnnaissance	13,987	Bilgi toplayan saldırı simülasyonları içerir
DoS	16,353	İnternete bağlı bir ana bilgisayarın hizmetlerini kesmek veya askıya almak için kullanılır.
Backdoors	2,329	Bir bilgisayara veya verilerine erişmek için bir sistem güvenlik mekanizmasının gizlice atlandığı bir teknik.
Analysis	2,677	Bağlantı noktası taraması, spam ve html dosya girişleri gibi saldırı türleridir.
Shellcode	1,51	Yazılım güvenlik açığından yararlanan küçük bir kod parçası saldırıdır.
Worms	174	Kendini diğer bilgisayarlara yaymak için bir bilgisayar ağını kullanan saldırı türüdür.



Şekil 4.2. Veri setinin sınıfı etiketi bakımından dağılımı

Çizelge 4.1 ve Çizelge 4.2 incelendiğinde, UNSW-NB15 veri setinin 49 sütundan oluştuğu ve sınıf etiketi bakımından 9 farklı saldırı türü içerdiği görülmektedir. Şekil 4.2’de veri setinin sadece normal ve anomali satır sayıları verilmiştir. Satır sayılarını incelediğimizde, normal ağ trafiğinin anomali verilerinden neredeyse yedi kat daha fazla kayıt içerdiği görülmekte ve veri setinin dengesiz bir dağılım gösterdiği anlamına geldiği görülmektedir.

4.2. Min-Max Öznitelik Normalizasyonu

Ağ verilerini ele aldığımızda farklı öznitelik ölçümleri ve ölçekleri değişken olabilir ve bu, özniteliklerin önem oranı bakımından farklılığa yol açabilir. Özniteliklerin büyük değerler alması diğerlerine göre daha büyük katkıya sahip olduğu anlamına gelmektedir. Çeşitli özniteliklerin yüksek sayısal değerlere sahip olması modelin öğrenme sürecini de etkilemektedir [83]. Bu nedenle farklı değerleri belirli bir aralığa getirmek üzere normalleştirme teknikleri kullanılır [12], [66]. Veri normalizasyonu, tüm özniteliklere eşit ağırlık verip benzer ölçekte olduğundan emin olmak ve ham verilerdeki sapmayı/önyargıyı (bias) ortadan kaldırmak için kullanılan istatistiksel bir yöntemdir [12], [24], [84], [84]. Öznitelik verileri, $-1,0$ ile $1,0$ veya $0,0$ ile $1,0$ gibi küçük bir aralığa düşecek şekilde ölçeklendirilir [85]. Bu yöntem veri ön işleme aşamasında en uygun teknikle uygulandığında daha iyi ve daha hızlı sonuçlar elde edilmektedir [84]. Normalleştirme, özellikle sınır ağlarını, en yakın komşu sınıflandırması ve kümeleme gibi mesafe ölçümlerini içeren sınıflandırma algoritmaları için oldukça kullanışlıdır [85]. Literatür çalışmalarını

incelediğimizde min-max ve z-skor gibi çeşitli normalizasyon tekniklerin olduğu görülmektedir [12], [66].

$$\text{Min} - \text{Max}_{\text{normalizasyonu}} = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \quad (4.1)$$

Said ve arkadaşlarının çalışmasında min-max yönteminin, mesafeye dayalı anomali tespitinde z-skor normalizasyonundan daha iyi performans verdiği belirtilmiştir [86]. Bu nedenle tez çalışmasında, pratik uygulamalarda en çok kullanılan ve orijinal veriler üzerinde doğrusal bir dönüşüm gerçekleştiren min-max tekniği kullanılmıştır [28], [84], [85]. Eş. 4.1'de görüldüğü üzere sütunun orijinal değeri ve minimum değerinin farkı, sütunun maksimum ve minimum farkına bölünerek hesaplanır. Böylece öznitelikler arasında orijinal ilişkiler korunup her öznitelik 0 ve 1 aralığında ölçeklendirilir.

4.3. Doğrusal Korelasyona Dayalı Öznitelik Seçimi (LCFS)

Öznitelik seçimi yöntemleri, veri setini en iyi şekilde açıklayan ve yüksek korelasyona sahip gereksiz özniteliklerin kaldırılması veya sınıf etiketi üzerinde en yüksek öneme sahip özniteliklerin belirlenmesini amaçlamaktadır [12], [35]. Korelasyon analizi, makine öğrenmesi ve ilişki analizi için istatistikte yaygın olarak kullanılan, iki sürekli değişken arasındaki doğrusal veya doğrusal olmayan ilişkinin gücünü ve yönünü ölçmeyi amaçlayan yöntemdir [15], [87], [88]. Literatürde korelasyon değişimlerini ölçen birçok doğrusal ve doğrusal olmayan ölçütler önerilmiştir [12], [15].

Doğrusal korelasyon, iki rastgele değişken arasında benzerlik ölçüsü olarak kullanılmaktadır [10]. Bir özneliliğin diğer özneliliklerle alakasız olması ve çıktı özneliliğiyle yüksek alaka düzeyine sahip olması iyi bir öznitelik olduğunu göstermektedir [10]. Öznelilikleri seçmek için de en önemli iyilik ölçütlerinden biri olarak Pearson korelasyon katsayısı belirtilmektedir [10]. Bu tez çalışmasında istatistikte yaygın olarak kullanılan ve doğrusal ilişkiyi analiz eden Pearson korelasyon katsayı yöntemi, öznitelik seçimi olarak uygulanmıştır. Pearson korelasyon katsayısı; örnek korelasyon katsayısı (r), ürün-moment korelasyon katsayısı veya korelasyon katsayısı olarak bilinen iki rastgele değişken arasındaki doğrusal ilişkinin bir ölçüsüdür. İlişkili verilerde, bir değişkenin büyüklüğündeki değişiklik aynı veya ters yönde başka bir değişkenin büyüklüğündeki bir değişiklikle ilişkilendirilir [87]. Pearson korelasyon yöntemi, normal dağılım gösteren veriler için kullanılmakta olup çalışma popülasyonunda ölçülen sonucun aralıklı veya sürekli (ondalıklı) değerler alan veri seti varsayımının karşılanmasını gerektirmektedir [87], [88]. Bununla

birlikte Pearson korelasyon hesabı için veriler rastgele veya en azından bir örneklemeden temsil edildiğinden, verilerin ilgilenilen popülasyonu temsil etmesi beklenmektedir. Temsil etmiyorsa o popülasyon hakkında anlamlı bir sonuç çıkarılamaz [87].

$$r = \frac{\sum(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum(x_i - \bar{x})^2 \sum(y_i - \bar{y})^2}} \quad (4.2)$$

Eş. 4.2’de görüldüğü üzere r olarak belirtilen Pearson korelasyon katsayısı ifade edilmektedir. Korelasyon katsayı değerleri ve ilişki yönü ile ilgili bilgiler de Çizelge 4.3’te verilmiştir.

Çizelge 4.3. Korelasyon katsayısı ve ilişkinin yorumlanması [88]

R	İlişki Yorumu
-1.0	Çok güçlü negatif korelasyon
-0.8	Güçlü negatif korelasyon
-0.50	Orta negatif korelasyon
-0.20	Düşük negatif korelasyon
0.0	İlişki Yok
+0.20	Düşük pozitif korelasyon
+0.50	Orta pozitif korelasyon
+0.80	Güçlü pozitif korelasyon
+1.0	Çok güçlü pozitif korelasyon

Pearson korelasyon katsayısı; negatif korelasyonlu (-1), korelasyonsuz (0) ve pozitif korelasyonlu (+1) arasında değişen değerler almaktadır [88]. X ve Y değişkeni lineer olarak birbirine bağımlıysa korelasyon katsayısı -1 ve +1 arasında birbiriyle ilişkilidir. Ancak korelasyon katsayısı $p=0$ olduğu durumlarda X ve Y değişkenleri birbirinden tamamen bağımsızdır [10]. Bir öznitelik diğer özniteliklerle alakasız ve çıktı sınıflarıyla yüksek alaka seviyesine sahip olması beklenmektedir. Birbiriyle yüksek ilişkili olan öznitelikler birbiriyle bağımlı olup hedef değişkenini tahmin etmede güçlü korelasyona sahip iki değişken aynı bilgiyi içerdiğinden biri gereksiz kabul edilip veri setinden çıkarılır [10], [14].

4.4. Basitleştirilmiş Mahalanobis Mesafesi

Mesafeye dayalı yöntemler anomali tespitinde ilkel ancak popüler yaklaşımlardır. Literatürde, değişkenler arasındaki mesafeyi ölçen birçok yöntem önerilmiştir. Örüntü tanımda, benzer nesneleri tespit etmede ve anomali tespiti gibi alanlarda kullanılmaktadır [18], [89]. Mahalanobis mesafesi, ilk olarak 1936 yılında Hintli istatistikçi Mahalanobis

tarafından ortaya konmuştur [20]. Bu mesafe, çok değişkenli veri setini çeşitli performans parametreleriyle tek değişkenli mesafe değerine dönüştüren ve hesaplama verimliliğini artıran ölçüttür [19], [20]. İki veri nesnesi, x ve y arasındaki $d(x,y)$ mesafesinin ne kadar farklı olduğunu ölçmektedir. Mahalanobis mesafesi, bilinmeyen bir örnek veri kümesinin bilinen bir örnek veri kümesine benzerliğini belirlemek ve iki istatistik dağılımını karşılaştırmak için kullanılmaktadır [7], [21]. Bu mesafenin diğer yöntemlere göre avantajı, sadece ortalama değeri değil, aynı zamanda değişkenlerin varyansını ve ölçülen değişkenlerin kovaryansını da hesaba katmasıdır [21]. Bu nedenle, her değişkeni kendi ağırlığına göre hesaba kattığından diğer mesafe tabanlı yöntemlere göre daha duyarlı olup yeni veri örneğinin eğitim örnekleriyle ne kadar iyi eşleştiğine ilişkin istatistiksel bir bilgi vermektedir [20], [21], [72]. Ancak verilerin kovaryans matrisinin ters çevirilebilir olma gereksiniminden ve ters çevirilebilir olsa bile veri boyutu arttıkça kovaryans matrisinin hesaplama karmaşıklığından dolayı klasik Mahalanobis mesafesi beklenen performansı karşılayamamaktadır [22], [62]. Bununla birlikte klasik Mahalanobis mesafesi, kendi başına özniteliklerin sayısı ile ölçeklenemediğinden yalnızca sınırlı sayıda değişkenle kullanılabilir [90]. Bu nedenle hesaplamayı hızlandırmak için varyansın standart sapma ile değiştirildiği basitleştirilmiş Mahalanobis mesafesi (SMD) türetilmiştir [21], [22]. Dolayısıyla, bu tez çalışmasında büyük verilerde daha az hesaplama maliyetiyle klasik Mahalanobis mesafesinin altı öznitelik kısıtına bağlı kalmayan SMD kullanılmaktadır. Böylece tek bir bölme işlemiyle zaman alan kare ve karekök hesaplamalarından kaçınılmış olur.

$$\text{Simplified_Mahalanobis_Distance} = \sum_{i=1}^n \frac{|x_i - x_i|}{\sigma_i + \alpha} \quad (4.3)$$

Eş. 4.3'te basitleştirilmiş Mahalanobis mesafesi formülü verilmiştir. Eğitim örneklerinde bir karakter veya bayt değeri hiçbir zaman görünmediğinde ya da aynı frekansta görüldüğünde standart sapma değerinin sıfıra eşit olması ve mesafenin sonsuz olma olasılığı vardır. Bundan kaçınmak için standart sapmaya bir yumuşatma faktörü (α) eklenir. Bu faktör, örneklenen eğitim verilerinin istatistiksel güvenilirliğini yansıtmaktadır. Eğitim veri setinde daha fazla örneklem gözlemlendikçe α faktörü otomatik olarak azaltılabilir [21]. SMD, vektör elemanlarının istatistiksel olarak bağımsız olduğu “naive” varsayımına dayanmaktadır. Varsayımın doğru olduğu durumlarda, kovaryans matrisi Σ köşegen olup köşegen boyunca bulunan ögeler her bir değişkenin varyansıdır [22]. Sonuç olarak, yukardaki formül kullanılarak önceden tanımlanmış profil ve yeni gelen veriler arasında

benzerlik mesafesi hesaplanabilir. Hesaplanan iki vektör arasındaki Mahalanobis değeri düşükse yüksek benzerliğe sahip olduğu anlamına gelmektedir [19]. Bununla birlikte SMD anomalileri tespit etmek için eşik değerinin nasıl ayarlanacağını da önermektedir [21].

4.5. Eşik Değeri ve Anomali Tespiti

Aykırı değerleri belirlemek üzere normal verilere dayalı bir algılama eşiği belirlenerek anomali tespit sistemleri geliştirilebilir. Eşik değerleri, bilinen arıza koşulları ve yanlış alarmların sayısını azaltma ihtiyacı gibi durumlarda uzman görüşüne dayalı olarak tanımlanmaktadır. Eşik değerine dayalı tespit yaklaşımı, anomalilere ilişkin ön bilgi olmadığı durumlarda anomalileri tespit edemeyebilir [18]. Bu nedenle izinsiz giriş davranışını normal trafikten ayırt etmek için eşik değeri ayarlanır [23]. Anomali tespiti için eşik değerlerini belirlemek üzere genelleştirilmiş bir olasılık yaklaşımı uygulamak faydalı olabilir [18]. Tez çalışması kapsamında literatürde en çok kabul gören ortalama (μ), standard sapma (σ) ve 1-3 arası değer alan alfaya (α) dayalı üç sigma eşik değeri yaklaşımı kullanılmıştır [12], [23], [24]. Üç sigma tekniği, ölçülen değerlerin ortalama ve standart sapma'nın normal dağılımını takip etmesi durumunda, veri değerlerinin %99,7'sinin ($\mu-3\sigma$) ve ($\mu+3\sigma$) aralığına düştüğünü belirten basit ama etkili bir istatistiksel kuraldır [91].

$$W_1 = \mu - \alpha\sigma, W_2 = \mu + \alpha\sigma \quad (4.4)$$

Genel olarak, sağlıklı veri seti normal dağılıma uyuyorsa 3σ yasasına göre ($\mu-3\sigma$) ve ($\mu+3\sigma$) aralığı dışında kalan örnek veri noktaları aykırı değer olarak kabul edilmektedir [20]. Eş. 4.4'te görüldüğü üzere normal bir dağılım için α değeri genellikle 1-3 aralığında değer almaktadır [23], [24]. Anomali tespitinde $\mu+3\sigma$ aralığı genellikle üst sınır olarak kabul edilmektedir. Farklı α değerlerinin seçimine göre gözlemlerin %68,26'sının ilk standart sapma ($\mu \pm \sigma$), %95'inin ilk iki standart sapma ($\mu \pm 2\sigma$) ve %99,7'sinin ilk üç standart sapma ($\mu \pm 3\sigma$) aralığında değiştiği belirtilmektedir [20], [23], [24]. Dolayısıyla, anomali tespitinde Mahalanobis mesafesi kullanılarak normal ağ profiliyle yeni gelen ağ profili arasındaki benzerlik değeri hesaplanır. Yeni gelen verinin mesafe değeri, üst ve alt eşik değerlerinden büyükse anomali tespit uyarısı oluşturulur [7], [24].

5. ÖNERİLEN SİSTEMİN UYGULANMASI

Bu bölümde büyük veriler üzerinde anomali tespiti için önerilen yöntemin nasıl uygulandığına dair bilgi vermektedir.

5.1. Deney Ortamı

Önerilen model 2,5 milyon satırdan oluşan UNSW-NB15 veri seti üzerinde değerlendirilmiştir. Ücretsiz bir bulut hizmeti olan ve aynı şekilde ücretsiz GPU'yu destekleyen Google Colab⁵ ortamında deneyler yürütülmüştür. Google Colab, GPU ve TPU gibi güçlü donanım seçeneklerini ve makine öğrenmesi modellerinin prototipini oluşturmaya yönelik bir bilgi işlem altyapısını sağlayan, sunucusuz (serverless) Jupyter notebook ortamı sunmaktadır. Aynı anda birden fazla CPU, GPU ve TPU örneğini çalıştırmaya olanak sağlamaktadır. Çizelge 5.1'de Google Colab'ın sağlamış olduğu CPU, GPU ve TPU çalışma ortamlarının teknik özelliklerine yer verilmiştir.

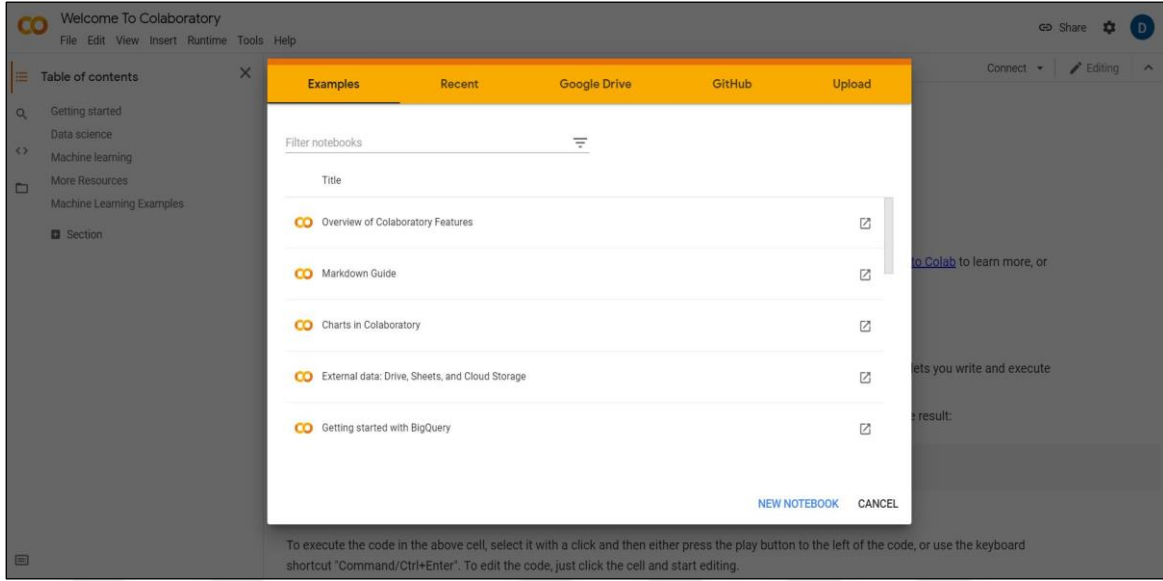
Çizelge 5.1. Google Colab ortamında notebook türleri [92]

CPU	GPU	TPU
İki çekirdekli 2.3 Ghz Intel Xeon işlemci ve 13 GB RAM	İki çekirdekli 2.3 Ghz Intel Xeon işlemci ve 13 GB RAM, 12 GB GDDR5 VRAM ile Tesla K80'e kadar yükseltilebilir	180 teraflops bulut TPU hesaplama, iki çekirdekli 2.3 Ghz Intel Xeon işlemci ve 13 GB RAM

Google Colab'ın geliştiricilere sağladığı özellikler [93] aşağıda maddeler halinde belirtilmiştir:

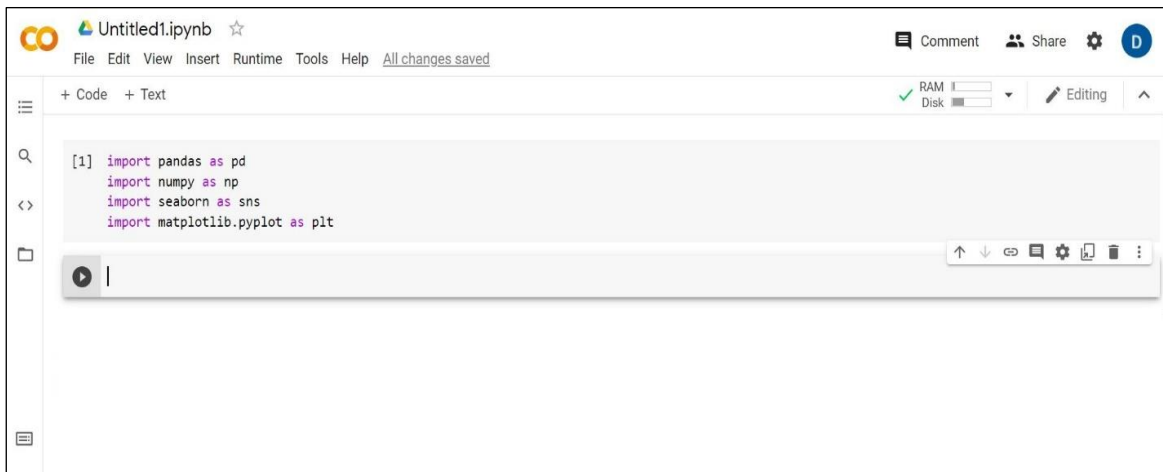
- Python programlama dili ile kod yazıp yürütme,
- Ücretsiz GPU ile bulut hizmeti,
- Notebooklar oluşturma, yükleme ve paylaşma,
- Kaggle gibi harici veri kümelerini içe aktarma,
- PyTorch, Tensorflow, Keras, OpenCV kütüphaneleri entegre etme,
- Not defterlerini Github'dan içe aktarma ve yayınlama.

⁵ Welcome to Colaboraty, Erişim Tarihi: 30.04.2021, <https://colab.research.google.com>



Şekil 5.1. Google Colab giriş ekranı

Şekil 5.1’de görüldüğü üzere Google Colab ortamında oluşturulan notebooklar, Google Drive ortamında depolanmaktadır. Aynı şekilde oluşturulan notebookları Github ortamında da depolama imkanı bulunmaktadır. Ayrıca bize yerel bilgisayarımızdan veya github ortamından jupyter notebook çalışmalarımızı Colab ortamına aktarma imkanı da sunmaktadır. EK-2’de tez çalışmasında oluşturduğumuz notebooklara ait görsel verilmiştir. Google Colab; veri bilimi, makine öğrenmesi ve derin öğrenme projelerini prototipleme söz konusu olduğunda bilgi işleme maliyeti bakımından kullanıcılara tasarruf sağladığından dolayı modelleme işlemlerinde iyi bir alternatiftir [94]. Herhangi bir kurulum gerektirmeden birçok popüler python kütüphanesini içermesi ve oluşturduğumuz notebookların ekip üyeleri tarafından eş zamanlı düzenlenebilmesi en önemli avantajdır.



Şekil 5.2. Google Colab notebook ortamında ilgili python kütüphanelerinin yüklenmesi

Şekilde 5.2’de görüldüğü üzere Google Colab, python geliştiricileri için etkileşimli bir notebook ortamı sunmaktadır. Kullanılan ortam, 12,72 GB RAM ve 107,77 GB depolama kapasitesi sağlamaktadır. Deneyler Python 3.6.9 sürümü kullanılarak yürütülmüştür. Çalışma kapsamında, Google Colab notebook ortamından Google Drive bulut ortamına bağlanarak veriler okunmuştur. Ardından uygulama kısmı için pandas, numpy ve scikit-learn kütüphaneleri kullanılırken görselleştirme için seaborn ve matplotlib kütüphaneleri kullanılmıştır.

5.2. Veri Ön İşleme

Makine öğrenimi ve veri madenciliğinin uygulama aşamasında veri ön işleme süreci önemli rol oynamaktadır. Veri setinde bazı öznitelikler gereksiz bilgiler ve birbiriyle düşük ilişki düzeyine sahip değerler içermektedir [82]. Verilerden eyleme dönüştürülebilir bilgilerin çıkarılması, veri ön işleme aşamasını içeren çok adımlı bir süreçtir [66]. Bu nedenle, kullanılacak veri setinin algoritmaya hazır hale getirilebilmesi için öznitelik seçimi, kategorik sayısal dönüşüm ve öznitelik ölçeklendirme işlemleri uygulanmalıdır.

Çizelge 5.2. Dosya boyutu, kayıt sayısı ve öznitelik sayısı bakımından veri seti

Dosya İsmi	Dosya Boyutu	Kayıt Sayısı	Öznitelik Sayısı
UNSW-NB15_1	161,2 MB	700000	49
UNSW-NB15_2	157,6 MB	700000	49
UNSW-NB15_3	147,4 MB	700000	49
UNSW-NB15_4	91,3 MB	440044	49

Çizelge 5.2’de görüldüğü üzere dört farklı UNSW-NB15 veri dosyasının; dosya boyutu, kayıt sayısı ve öznitelik sayısına ait istatistiksel bilgiler verilmiştir. Veri seti öznitelikleri incelendiğinde karşımıza; kategorik, ikili ve sürekli olmak üzere üç farklı öznitelik veri türü çıkmaktadır. Bu nedenle UNSW-ADFA web sitesinden⁶ dört farklı CSV dosyası halinde indirilen ağ verilerinin, tek dosyada birleştirilmesi ve gereksiz özniteliklerinin çıkarılması gerekmektedir.

Şekil 5.3’te görüldüğü üzere Google Colab ortamında veri ön işleme aşamasının ilk adımı olan, dört farklı CSV dosyasının birleştirme sürecine ait kodlama görseli verilmiştir.

⁶ The UNSW-NB15 Dataset, Erişim Tarihi: 10.12.2020, <https://research.unsw.edu.au/projects/unsw-nb15-dataset>

```

import pandas as pd
import numpy as np
from sklearn import preprocessing

[ ] uns1 = pd.read_csv("/content/drive/My Drive/UNSW-NB15 Dataset/UNSW-NB15_1.csv")

/usr/local/lib/python3.6/dist-packages/IPython/core/interactiveshell.py:2718: DtypeWarning: Columns (1,3) have mixed types.Specify dtype option on import or set low_memory=False.
interactivity=interactivity, compiler=compiler, result=result)

[ ] uns2 = pd.read_csv("/content/drive/My Drive/UNSW-NB15 Dataset/UNSW-NB15_2.csv")

/usr/local/lib/python3.6/dist-packages/IPython/core/interactiveshell.py:2718: DtypeWarning: Columns (3,39,47) have mixed types.Specify dtype option on import or set low_memory=False.
interactivity=interactivity, compiler=compiler, result=result)

[ ] uns3 = pd.read_csv("/content/drive/My Drive/UNSW-NB15 Dataset/UNSW-NB15_3.csv")

[ ] uns4 = pd.read_csv("/content/drive/My Drive/UNSW-NB15 Dataset/UNSW-NB15_4.csv")

```

Şekil 5.3. Veri ön işleme kodlama ekranı

Her bir CSV dosyası python’ın pandas kütüphanesi kullanılarak dört farklı değişkene atanacak şekilde okunur. Son olarak dört farklı CSV verisi tek değişkende birleştirilir. Çizelge 5.3’te veri kümesine ait istatistiksel bilgileri içeren tablo verilmektedir. Verilen tabloda veri kümesinin %87,35 oranında normal ve %12,65 oranında anomali verilerden oluştuğu görülmektedir. Ardından tekrarlı, eksik ve gürültülü veriler kontrol edilerek herhangi bir temizleme işlemine gerek duyulup duyulmadığına dair karar verilmektedir.

Çizelge 5.3. UNSW-NB15 veri setine ait karakteristik özellikler

Karakteristik	Değer
Toplam Satır Sayısı	2.540.044
Öznitelik Sayısı	49
Saldırı Etiket Sayısı	9
Normal Veri Yüzdesi	%87,35
Anomali Veri Yüzdesi	%12,65

Bazı durumlarda veri setleri istenildiği gibi dengeli bir dağılım göstermemektedir. Bu nedenle modelin eğitiminde önyargılı (bias) sonuçlar oluşabilmektedir. Şekil 4.2 incelendiğinde, hedef değişkeni bakımından veri setinin dengesiz bir dağılım gösterdiği görülmektedir. Bu nedenle dengeli veri dağılımını sağlamak için alt örnekleme (down-sampling) yöntemi uygulanmıştır. Diğerine sayıca üstün olan sınıfın kayıt sayısı azaltılmış ve bunun sonucunda veri setinde normal ve anomali sınıf sayıları dengeli hale getirilmiştir. Böylelikle yüksek sayıya sahip olan sınıf etiketinin öğrenme algoritmasına üstün gelmesi engellenmiştir [47].

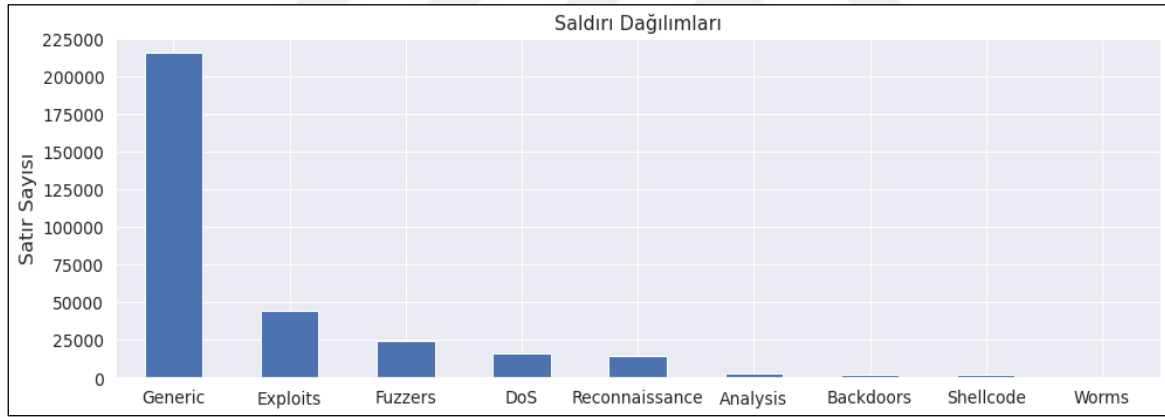
5.2.1. Veri temizleme

Veri temizleme sürecinde; verilerin kalitesini artırmak için verilerde eksik değerler, yazım hataları, gömülü değerler, tekrarlı veriler ve çelişen kayıtlar gibi işlemler ele alınmaktadır. Verilerin tutarsız olması ve veri hacminin büyük olması nedeniyle bu süreç büyük bir sorun teşkil etmektedir [95]. Gürültüsüz ve temiz bir veri kümesi elde etmek için veri temizleme yöntemleri uygulanmıştır. Veri seti üzerinde 49 özniteliğin hepsi hedef değişkeniyle alakalı değildir. Toplam süre (dur) özniteliği, Stime ve Ltime öznitelik değerlerinin farkından elde edildiğinden dolayı gereksiz olarak değerlendirilmektedir. Bununla birlikte, kaynak ip adresi (Srcip), kaynak bağlantı nokta numarası (Sport), hedef IP adresi (Dstip) ve hedef bağlantı nokta numarası (Dsport) gibi öznitelikler bilgi işlem altyapısına özgü değerlere sahip olduğundan dolayı, anomali tespitinde fayda sağlayacak bilgileri içermemektedir [96]. Ayrıca bu değişkenler hem on altılı hem de tam sayı gibi değerler içerdiğinden kapsamlı veri ön işleme adımlarını gerektirmekle birlikte veri kümesiyle çalışmayı zorlaştırmaktadır. Bu nedenle ilk olarak UNSW ADFA sitesinde yayınlanan küçük ölçekli UNSW-NB15'e ait eğitim ve test veri setlerinde Srcip, Sport, Dstip, Dsport, Stime ve Ltime özniteliklerinin yer almadığından dolayı veri setimizden çıkarılmıştır. Ardından hedef değişkeninin boşluk ve nokta gibi gürültülü karakterler içerdiği görülmüştür. Bu kapsamda hedef değişkeninin içerdiği gürültülü karakterler temizlenip orijinal isimleri kullanılarak düzeltilmiştir. Diğer bir adım olarak büyük veri ölçeğinde 2,5 milyon satır içeren veri seti üzerinde, eksik veriler kontrol edildiğinde is_ftp_login ve ct_flw_http_mthd özniteliklerinin %50'den fazla eksik değer içerdiği görülmüştür. Yüksek oranda eksik değerlere sahip öznitelikler, veri temizleme yaklaşımının en basit tekniğine göre veri setimizden çıkarılmıştır. Son olarak veri seti üzerinde Gottwalt ve arkadaşlarının [12] yaptığı çalışmaya göre is_ftp_cmd ve ct_ftp_cmd değişkenlerinin gereksiz olduğu ve bu değişkenlerin modelde önyargıya neden olduğundan dolayı çıkarılması önerilmiş ve veri setimizden de çıkarılmıştır. Sonuç olarak, uygulanan veri temizleme adımları sonrasında elde edilen 39 özniteliğe sahip veri setinin son hali EK-1'de verilmiştir.

5.2.2. Öznitelik dönüşümü ve normalizasyon

Birçok pratik veri bilimi aktivitesinde, veri seti kategorik değişkenler içermektedir. Makine öğrenmesi ve istatistiksel tabanlı algoritmalar gerekli hesaplama işlemleri için sayısal değerlere ihtiyaç duymaktadır. Etiket kodlama, kategorik etiketlerin makine tarafından okunabilir sayısal değerlere dönüştürülmesidir. Bu kısımda veri setimizle ilgili olarak

kategorik değerlerin sayısal değerlere dönüştürülme yöntemi ve ölçeklendirme tekniği açıklanmaktadır. Veri setimizi incelediğimizde proto, state ve service isimli özniteliklerin kategorik değerlere sahip olduğu görülmektedir. Kategorik değerlere sahip olan bu değişkenlere, Google Colab ortamında scikit-learn kütüphanesinin LabelEncoder yaklaşımı uygulanarak sayısal değerlere dönüşümü gerçekleştirilmektedir. Proto isimli protokol özniteliği; TCP=114, UDP=120, UNES=122, ARP=6 olacak şekilde 135 farklı sayısal değere dönüştürülmesi sağlanmıştır. Ardından state isimli durum özniteliği CLO=1, CON=2 ECO=3, ECR=4, FIN=5 olmak üzere 16 farklı sayısal değere dönüştürülmüştür. Aynı şekilde service isimli öznitelik de DHCP=1, DNS=2, FTP=3, HTTP=4, SMTP=9 gibi 13 farklı sayısal değerle ifade edilmiştir. Son olarak, doğrusal korelasyona dayalı öznitelik seçimini hedef değişkeni ve öznitelikler arasında uygulayabilmek ve korelasyon katsayılarını elde etmek için saldırı isimlerini içeren labels (sınıf) özniteliğinin sayısal değere dönüştürülmesi gerçekleştirilmiştir. Şekil 5.5'te hedef değişkenine ait saldırı türlerinin satır sayısı bakımından dağılımı verilmiştir.

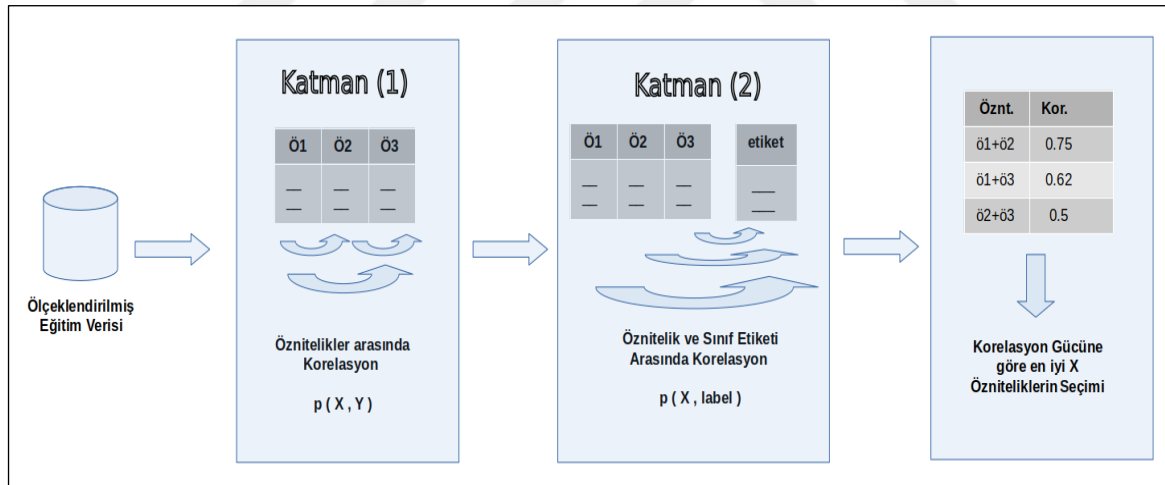


Şekil 5.4. Saldırı dağılımları bakımından veri setinin dağılımı

Gereksiz özniteliklerin temizlenmesi ve sayısal değerlere dönüşüm işleminden sonra ölçeklendirme yöntemi uygulanır. Anomali olarak üretilen, ama anomali anlamına gelmeyen aşırı uç değerler hem önyargılı sonuçların elde edilmesine hem de Pearson korelasyon katsayısı üzerinde aşırı etkiye sahip olabilmektedir [87]. Bu durumda hem Pearson korelasyonunun gerektirdiği normal dağılım varsayımını [87] karşılayacak hem de orijinal değerlerin dağılımlarını bozmadan 0-1 aralığında olacak şekilde ortak bir ölçeğe getirmek üzere verilere lineerlik katan Min-Max normelleştirme yöntemi uygulanmıştır. Ölçeklendirme yöntemi, python programlama dilinin sunmuş olduğu scikit-learn kütüphanesi kullanılarak gerçekleştirilmiştir. Bu yöntem hedef değişkeni hariç diğer tüm özniteliklere uygulanmış ve veri kümesi üzerinde oluşan önyargının etkisi kaldırılmıştır.

5.3. Deneyin Uygulanması

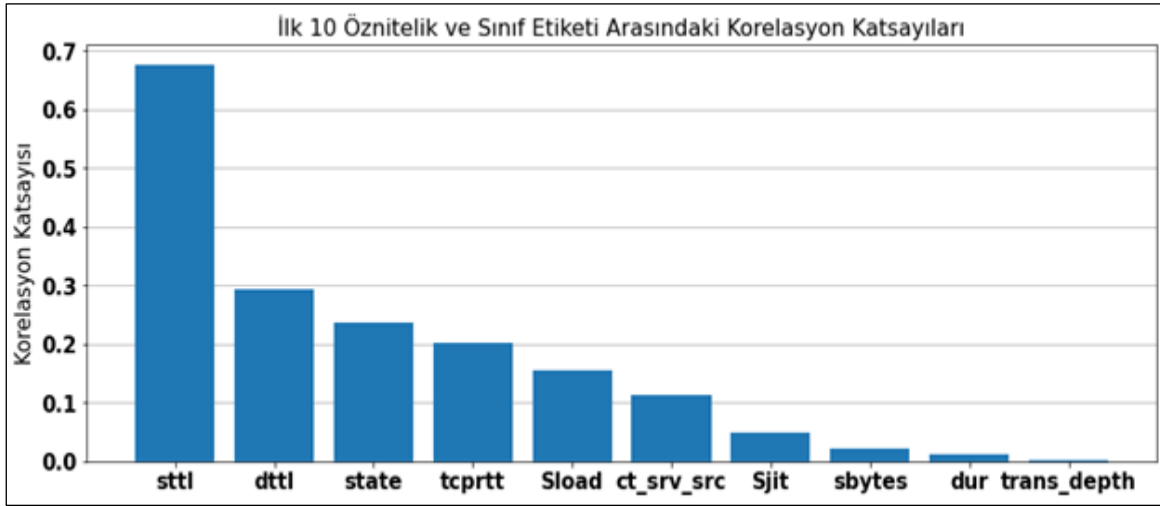
Çalışmanın bu bölümünde önerilen öznitelik seçimi ve basitleştirilmiş Mahalanobis mesafesi yaklaşımlarının nasıl uygulandığı açıklanmaktadır. Geçek hayatta veri setleri çok fazla boyutta öznitelige sahip olmakla birlikte veri seti boyutu büyüdükçe model oluşturma sürecinde harcamamız gereken zaman ve işlem gücü de artmaktadır. Veri temizleme, dönüştürme ve normalleştirme gibi veri ön işleme adımlarından sonra ilk olarak iki katmandan oluşan doğrusal Pearson korelasyona dayalı öznitelik seçimi yöntemi uygulanmıştır. Katman (1) olarak adlandırılan ilk aşamada, Pearson korelasyon yöntemi uygulanarak öznitelikler (öznitelik-öznitelik) arasında korelasyon katsayı değerleri hesaplanmıştır. Bu süreçte katsayı değerleri hesaplanırken proto, service ve state gibi kategorik değerler alan özniteliker ve hedef değişkeni hariç tutulmuştur. EK-3'te öznitelikler arasında hesaplanan korelasyon katsayılarına ait sıcaklık haritasının görseli verilmiştir. Ardından veri setindeki gereksiz öznitelikleri kaldırmak için hesaplanan korelasyon katsayılarının mutlak değerleri alınmış ve Çizelge 4.3'te korelasyon ilişki yorumu tablosuna göre değerlendirilmiştir.



Şekil 5.5. İki katmanlı doğrusal korelasyona dayalı öznitelik seçimi (LCFS)

Çoğu araştırmacı $p < 0,1$ katsayısının çok zayıf ve $p > 0,90$ katsayısının çok güçlü olduğu konusunda hemfikir olsa da aradaki katsayı değerlerinin üzerine durulması gerekmektedir. Aradaki katsayı değerleri değerlendirildiğinde, 0,65'lik bir korelasyon katsayısının uygulanan genel kurala bağlı olarak “iyi” veya “orta” bir ilişki yönüne sahip olduğu yorumlanabilir [87]. Yaptığımız çalışma kapsamında, Eid ve arkadaşlarının [10] kullandığı $p > 0,1$ katsayı ölçeği yerine birbiriyle $p > 0,6$ 'dan yüksek katsayıya sahip öznitelik çiftlerinin yüksek korelasyona sahip olduğu kabul edilmiştir. Bu durumda her iki özniteliğin hedef

değişkenini tahmin etmede aynı bilgiyi içerdiği ve bir özneliğin verebileceği bilgiyi diğer özneliğin de sağlayabildiği anlamına gelmektedir. Böylece bir özneliğin gereksiz olduğu kabul edilip veri setinden kaldırılmıştır [10]. Uygulanan katman (1) sonucunda birbiriyle düşük korelasyon ilişkisine sahip yeni öznelik alt kümesi elde edilmiştir. Şekil 5.6'da doğrusal korelasyona dayalı öznelik yöntemine ait sürecin görseli verilmiştir.



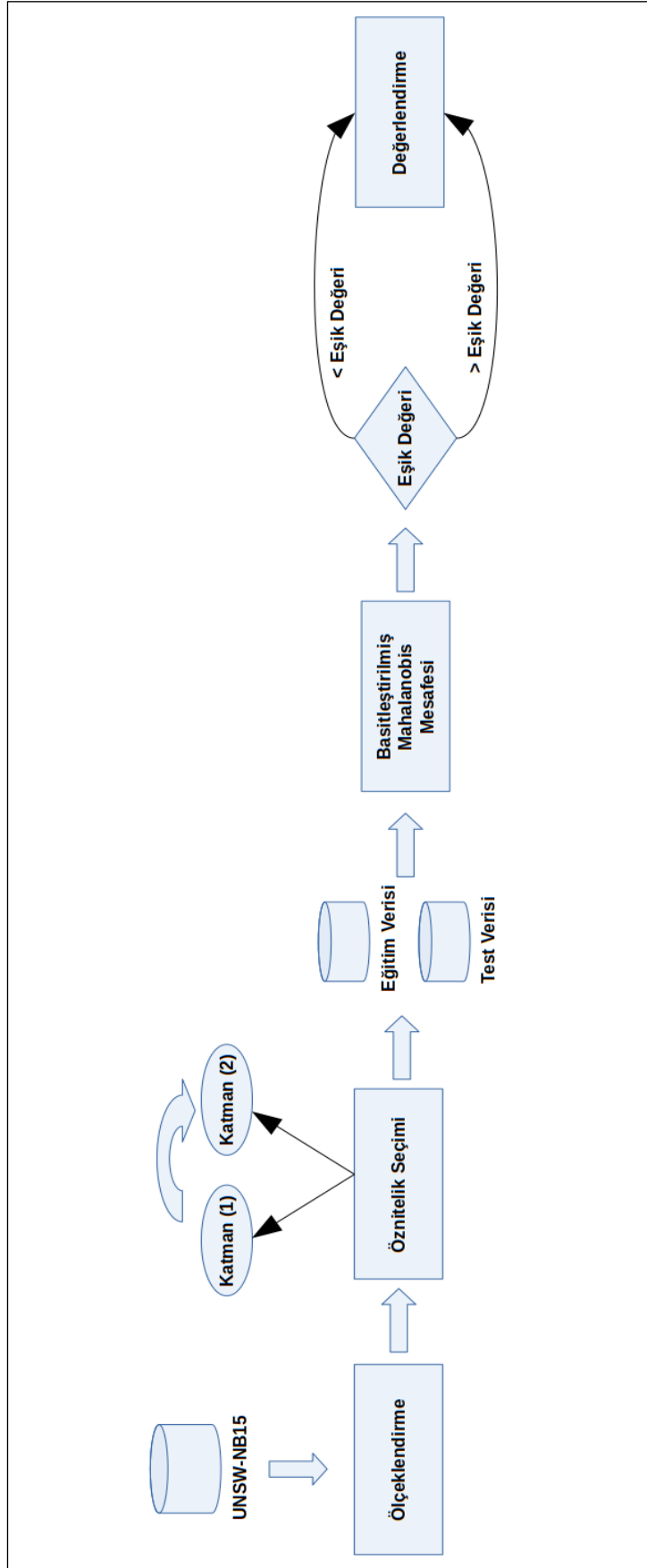
Şekil 5.6. Büyükten küçüğe doğru hedef değişkeniyle ilgili ilk on öznelik sıralaması

Katman (2) aşaması, birinci katmandan seçilen öznelik alt kümesi kullanılarak hedef değişkeni ve öznelikler arasında en güçlü korelasyonu bulmak üzere uygulanmıştır. Ardından hedef değişkeni ve öznelikler arasında korelasyon katsayıları hesaplanmış ve hedef değişkeniyle ilgi düzeyine göre büyükten küçüğe doğru sıralanmıştır. Böylece hangi özneliklerin hedef değişkenini daha yüksek doğruluk oranıyla tahmin edebileceği belirlenebilmiştir. Şekil 5.7'de görüldüğü üzere hedef değişkenini tahmin etmede kullanılabilecek en önemli 10 özneliğin, büyükten küçüğe doğru sıralanmış grafiği mevcuttur.

İlgili öznelikler belirlendikten sonra veri seti üzerinde mesafeyi özneliklerin dağılımına göre hesaplayan istatistiksel tabanlı Mahalanobis tekniği seçilmiştir. Ancak Mahalanobis tekniği, öznelik sayısı arttığında pratikte başarısız olmakla birlikte sınırlı sayıda değişken kullanılarak hesaplanabilmektedir [90]. Bu nedenle, öznelik sayısı kısıtı ve kovaryans matris karmaşıklığı olmayan basitleştirilmiş Mahalanobis mesafesi uygulanmıştır. Profile dayalı saldırı tespit yöntemi kullandığımızdan dolayı Mahalanobis mesafe değerlerinin normal ağ trafiğini içeren eğitim veri seti üzerinde elde edilmesi gerekmektedir. Bu nedenle seçilen öznelik sayısına göre (3, 5, 7, ve 10 gibi) her öznelik için standart sapma (σ) ve ortalama (μ) değerleri, normal ağ trafiğini içeren eğitim veri kümesi üzerinde hesaplanmakta

olup python ortamında std ve mean isimli değişkenlerde saklanmaktadır. Mesafe değerlerini hesaplamak adına SMD formülünü incelediğimizde ise mesafe değerinin sıfır olmasını engelleyen düzleştirme faktörünün (α) hesaplanmasının gerektiği görülmektedir. Ancak 2,5 milyon satır içeren büyük ölçekteki veri seti üzerinde çalıştığımızdan dolayı α 'nın sıfır olarak verilmesi mesafe değerlerini etkilemediği ortaya çıkmıştır. Sonuç olarak SMD değerleri, mevcut normal ağ trafiği verileriyle her öznitelik için hesaplanan sapma (σ) ve ortalama (μ) değerlerinin formüle uygun hesaplanmasıyla elde edilmektedir. Böylece çoklu öznitelige sahip olan veri seti, tek değişkenli mesafe özniteligine/sütununa dönüştürülmüştür.

Son aşamada ise sınıflandırma mekanizmasının anomali değerleri tespit etmede önem arz ettiği görülmektedir. Bu kapsamda, hesaplanan normal Mahalanobis mesafe değerleri üzerinde ortalama (μ) ve standart sapma (σ) kullanılarak normal ağ profilini temsil eden istatistiksel üç sigma kuralı, sınıflandırma yöntemi olarak kullanılmıştır. İstatistiksel temelli üç sigma yaklaşımı, büyük veri ölçeğinde daha az hesaplama maliyeti gerektirmesi ve anomali tespiti için herhangi bir ön bilgiye sahip olma zorunluluğu gerektirmediğinden dolayı tercih edilmiştir. Üç sigma kuralına göre normal dağılım gösteren veri seti üzerinde normal veriler, üç standart sapma (3σ) aralığında olmalıdır. Normal ağ trafiğini içeren eğitim veri kümesi üzerinde anomali değerleri tespit edecek ve veri setinin dağılımına göre $0,5\sigma - 3\sigma$ arasında değişen üst ($\mu + \alpha\sigma$) ve alt ($\mu - \alpha\sigma$) sınırlar oluşturulmuştur. Ardından yeni gelen mesafe verileri normal profili temsil eden eşik değerleriyle karşılaştırıldığında, üst ve alt limitler aralığında yer alıyorsa normal ağ trafiği olarak işaretlenirken, bu limitler dışındaki mesafe değerleri anomali ağ trafiği olarak işaretlenmiştir. Böylece yeni gelen verinin sistemimiz için tehdit olup olmadığı tespit edilmiş olur. Sonuç olarak yeni gelen mesafe değeri sıfıra ne kadar yakınsa eskiyle yeni verinin birbirine benzediğine ve normal ağ trafiğine denk geldiği ifade edilmektedir. Fakat eskiyle yeni verinin sıfırdan farklı olması durumunda ise anomali ağ trafiği olduğu anlamına gelmektedir. Şekil 5.8'de önerilen yaklaşımın uygulama adımlarına ait model mimarisi verilmiştir.



Şekil 5.7. Önerilen modelin mimarisi

5.4. Performans Değerlendirilmesi

Değerlendirme kısmında, önerilen yaklaşımın anomalileri nasıl bir başarı oranıyla tespit edildiği ölçülmektedir. Yürütülen deneyler dört farklı başlık altında değerlendirilmiştir. Birinci başlık altında önerilen yöntem UNSW-NB15 veri seti üzerinde hedef değişkeniyle ilgili 3, 4, 5, 7 ve 10 gibi farklı öznitelik sayıları bakımından test edilmiştir. Diğer başlıklar kapsamında, dengesiz dağılım gösteren UNSW-NB15 veri setinin dengeli hale getirilip değerlendirilmesi ve LCFS yöntemi olmadan tüm öznitelikler üzerinde uygulanması gibi deneyler yürütülmüştür. Bununla birlikte, daha doğru bir öğrenme süreci oluşturmak ve aşırı öğrenme hakkında daha net bir bilgi elde etmek amacıyla modelimiz 10 kat çapraz doğrulama yöntemi kullanılarak değerlendirilmiştir. Kullanılan 10 kat çapraz doğrulama yöntemi, veri setini rastgele 10 eşit boyutlu veri setine bölmektedir. Ardından bölünen 10 farklı alt kümeden, her biri (k-1) modelin performansını test etmek üzere doğrulama verisi olarak kullanılır. Özetlemek gerekirse k-1 test veri seti olarak kullanıldığında geriye kalan dokuz adet veri kümesi olan k-9 eğitim verisi olarak kullanılmaktadır. Sonuç olarak çapraz doğrulama sürecinde, tüm gözlemlerin hem eğitim hem de doğrulamada kullanılması için k defa tekrarlanıp, k bölmelerinden her birinin doğrulama için bir kez kullanılması sağlanır [12], [23].

Modelimizin performansını değerlendirmek için Çizelge 5.4'te verilen karmaşıklık matrisi üzerinden değerlendirme metrikleri hesaplanmıştır. Karmaşıklık matrisi gerçek pozitif, gerçek negatif, yanlış pozitif ve yanlış negatif tahmin değerlerinden oluşmaktadır.

Çizelge 5.4. Karmaşıklık matrisi

		Gerçek	
		Anomali	Normal
Tahmin	Anomali	TP	FP
	Normal	FN	TN

Gerçek pozitif (TP): Anomali olan verilerin anomali olarak tahmin edilmesidir.

Gerçek Negatif (TN): Normal olan verilerin normal olarak tahmin edilmesidir.

Yanlış Pozitif (FP): Gerçekte normal olan verinin anomali olarak tahmin edilmesidir.

Yanlış Negatif (FN): Gerçekte anomali olan verinin normal olarak tahmin edilmesidir.

Elde edilen karmaşıklık matrisinden, modelimizin başarısını değerlendirdiğimiz doğruluk, kesinlik, duyarlılık, f1 skor ve yanlış alarm oranı gibi performans ölçütleri hesaplanmaktadır.

Doğruluk: Sınıflandırma problemlerinde doğru tahmin edilen veri oranını hesaplamak için kullanılan klasik bir ölçümdür [14]. Veri seti dengeli sınıf etiketiyle dağıldığı ve çarpık olmadığı durumlarda bu metrik kullanışlı olurken, dengesiz sınıf etiketine sahip veri seti üzerinde pek kullanışlı değildir [25]. Eş. 5.1’de verilen ölçüm metriği, doğru tahmin edilen pozitiflerin ve negatiflerin toplamının tüm satır sayısına bölünmesiyle hesaplanmaktadır.

$$\text{Doğruluk} = \frac{TP + TN}{TP + TN + FP + FN} \quad (5.1)$$

Kesinlik: Eş. 5.2’de verildiği üzere doğru bir şekilde tahmin edilen pozitif verilerin, pozitif tahmin edilen tüm verilere oranıdır [25]. Bu metrik, gerçekte pozitif değerler alan pozitif tahminlerin yüzdesini vermektedir. Özellikle tahmin kesinliğinden emin olmak istediğimiz ve yanlış pozitiflerin yüksek olduğu durumlarda kullanılmaktadır.

$$\text{Kesinlik} = \frac{TP}{TP + FP} \quad (5.2)$$

Tespit Oranı (Duyarlılık): Doğru bir şekilde pozitif olarak sınıflandırılan pozitifleri gösteren ölçüttür. Aynı zamanda pozitif tespit oranı olarak da bilinmektedir [14]. Yanlış negatif tahminlerinin yüksek olduğu durumlarda kullanılmaktadır. Anomali sınıflandırma problemlerinde en yüksek tespit oranı hedeflenmekte ve bu yüksek tespit oranı anomali değerlerin doğru bir şekilde tespit edildiği anlamına gelmektedir. Tespit oranı Eş. 5.3’teki gibi hesaplanmaktadır.

$$\text{Tespit Oranı (Duyarlılık)} = \frac{TP}{TP + FN} \quad (5.3)$$

F1 Skor: Kesinlik ve duyarlılık ölçütlerinin harmonik hesaplaması alınarak elde edilir. Eş. 5.4’te f1 skor formülü verilmiştir. Dengesiz veri setleri üzerinde yanlış pozitif ve negatifin önemli olduğu durumlarda uygun olan bir ölçümdür. Yanlış etiketlenmiş verilerde doğruluk ölçütünden daha iyi sonuçlar vermektedir.

$$\text{F1 Skor} = \frac{2 * (\text{Kesinlik} * \text{Duyarlılık})}{\text{Kesinlik} + \text{Duyarlılık}} \quad (5.4)$$

Yanlış Alarm Oranı (FPR): Toplam yanlış pozitif sayısının, yanlış pozitif sayısı ve gerçek negatif sayısına bölünmesiyle hesaplanmaktadır [25]. Eş. 5.5'te verilen pozitif olmayan ancak pozitif olduğu tahmin edilen verilerin, pozitif olmayan toplam veri sayısına bölünmesidir.

$$\text{Yanlış Alarm Oranı (FPR)} = \frac{FP}{FP+TN} \quad (5.5)$$

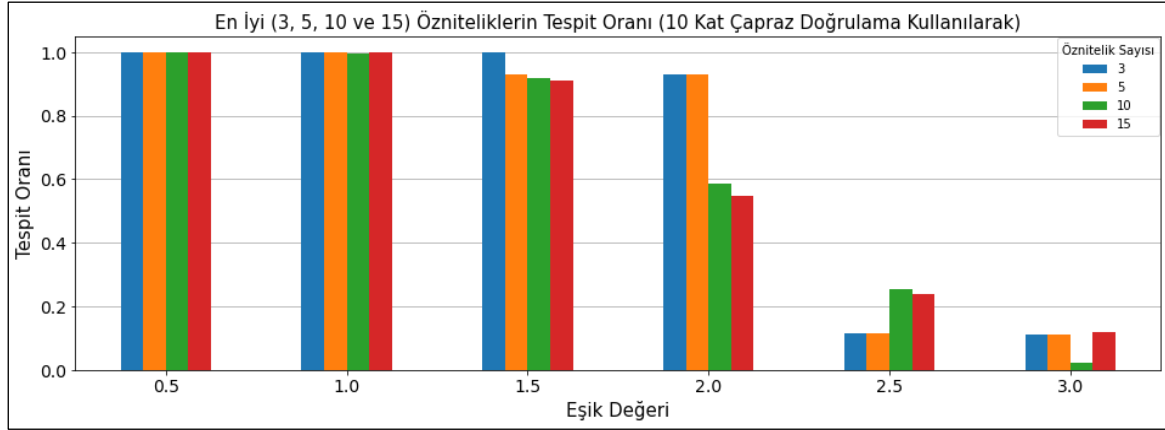
5.4.1. LCFS ve basitleştirilmiş Mahalanobis mesafesi deney sonuçları

Bu kısımda, SMD ve LCFS yöntemi kullanılarak deney gerçekleştirilmiştir. Ardından, modelin etkinliği 10 kat çapraz doğrulama yöntemi kullanılarak ölçülmüştür. Önerilen yaklaşım 2,25 milyon satır normal ağ trafiği kullanılarak eğitilmiş olup hem anomali hem de normal ağ trafiğini içeren 254.044 satır veri seti üzerinde test edilmiştir.

Çizelge 5.5. LCFS ve SMD performansı (ilk üç öznitelik kullanarak)

Eşik Değeri	0,5σ	1σ	1,5σ	2σ	2,5σ	3σ
Doğruluk	%97,799	%98,205	%98,38	%97,69	%87,89	%87,98
Kesinlik	%85,21	%87,689	%88,78	%89,31	%61,51	%64,49
Tespit Oranı	%99,946	%99,827	%99,82	%92,90	%11,53	%11,14
F1 Skor	%91,99	%93,36	%93,98	%91,07	%19,42	%19,009
Yanlış Alarm (FPR)	%2,51	%2,02	%1,82	%1,60	%1,04	%0,88

Çizelge 5.5'te verilen deney sonuçları incelendiğinde, hedef değişkeniyle en yüksek alaka seviyesine sahip ilk üç ve ilk dört öznitelik kullanılarak en iyi FPR değerlerinin 2σ, 2,5σ ve 3σ eşik seviyelerinde sırasıyla %1,60, %1,04 ve %0,88 olarak elde edildiği görülmüştür. En iyi sonuçları elde ettiğimiz ilk üç ve ilk dört öznitelikler sırasıyla state, dtl, stl ve tcprtt'dir. Tespit oranı ve F1 skor bakımından ilk üç ve ilk dört özniteliklerin performansı eşik değeri 1σ seviyesinde incelendiğinde ise sırasıyla %99,82 ve %93,36 başarı oranları elde edildiği görülmüştür. Ancak 2,5σ ve 3σ eşik seviyelerinde ilk üç ve ilk dört özniteliklerin gösterdiği FPR ve tespit oranı performansının düştüğü, öznitelik sayısının artması durumunda da benzer şekilde düşüş gösterdiği fark edilmiştir. Çizelge 5.5'te görüldüğü üzere seçilen öznitelik sayısına bakılmaksızın, eşik değeri arttığında tespit oranında da görünür bir performans düşüklüğü meydana geldiği gözlemlenmiştir. Dolayısıyla yeni gelen anomalilerin, modelin eğitildiği normal ağ trafiği ortalamasına yakın değerlere sahip olduğu veya normal ağ trafiği ortalamasından en fazla 0.5σ ila 1.5σ aralığında saptığı anlaşılmaktadır. Bu nedenle en yüksek tespit oranı 0.5σ ila 1.5σ aralığında elde edilmiştir.



Şekil 5.8. Farklı öznitelik sayılarının artan eşik değeri ile tespit oranına etkisi

Şekil 5.8’de verilen 3, 5, 10 ve 15 özniteliğe ait tespit oranları değerlendirildiğinde, ilk üç özniteliğin en iyi tespit oranını 0,5 σ , 1 σ ve 1,5 σ eşik değeri seviyelerinde ortaya koyduğu görülmüştür. Sonuç olarak Çizelge 5.5’ten ve Şekil 5.8’den en iyi tespit oranının 0,5 σ , 1 σ ve 1,5 σ eşik değerlerinde elde edildiği anlaşılmaktadır. Bununla birlikte eşik değeri seviyesi 1,5 σ ’dan 3 σ ’ya doğru yükseldiğinde, yanlış pozitif alarm oranının da %2,02’den %0,88’e azaldığı görülmektedir.

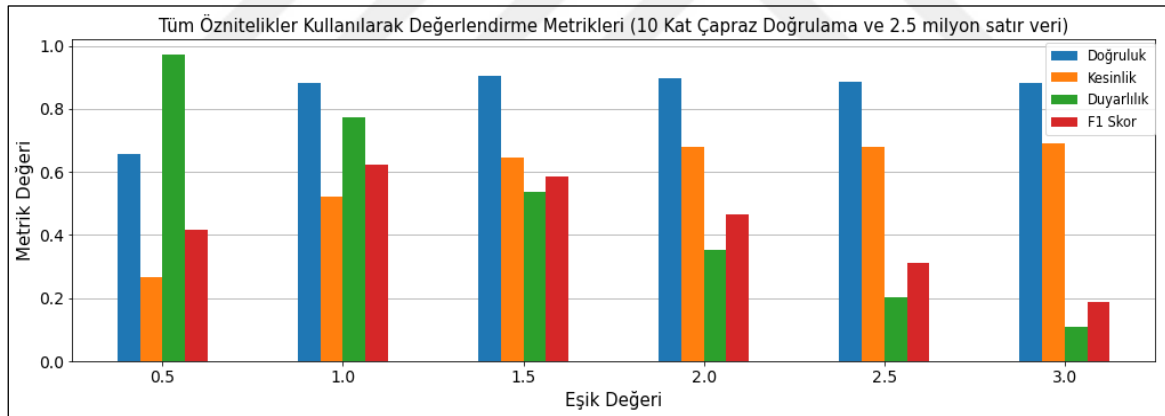
5.4.2. LCFS kullanılmadan basitleştirilmiş Mahalanobis mesafesi deney sonuçları

Bu bölümde, LCFS kullanılmadan SMD yönteminin tespit oranını değerlendirmek üzere deney gerçekleştirilmiştir. Deney kapsamında SMD yöntemi 2,25 milyon satır veri kümesinden yalnızca normal ağ trafiği kullanılarak eğitilmiştir. Ardından 10 kat çapraz doğrulama kullanılarak hem anomali hem de normal ağ trafiğini içeren 254.044 satırdan oluşan veri seti üzerinde test edilmiştir. Yürütülen eğitim ve test deneyleri, veri ön işleme aşamasında eksik veriler nedeniyle üç özniteliğin hariç tutulmasıyla birlikte 39 öznitelik (38 öznitelik ve 1 hedef değişkeni) üzerinde gerçekleştirilmiştir.

Çizelge 5.6. LCFS öznitelik seçimi kullanılmadan SMD performansı (ilk üç öznitelik kullanılarak)

Eşik Değeri	0,5 σ	1 σ	1,5 σ	2 σ	2,5 σ	3 σ
Doğruluk	%65,51	%88,10	%90,41	%89,72	%88,69	%88,10
Kesinlik	%26,48	%51,99	%64,59	%68,08	%67,81	%69,18
Tespit Oranı	%97,21	%77,33	%53,62	%35,35	%20,22	%10,71
F1 Skor	%41,63	%62,18	%58,60	%46,53	%31,15	%18,55
Yanlış Alarm (FPR)	%39,1	%10,3	%4,3	%2,4	%1,4	%0,7

SMD yöntemi her standart sapma seviyesini değerlendirmek üzere uygulanmaktadır. Çizelge 5.6’da verilen sonuçlar değerlendirildiğinde, 3σ eşik değerinde %0,7 ile en düşük yanlış alarm oranı elde edilirken, $0,5\sigma$ eşik değerinde %97,21 ile en yüksek tespit oranı elde edildiği görülmüştür. Bununla birlikte σ eşik seviyesi $0,5\sigma$ ’dan 3σ ’ya doğru yükseldiğinde, yanlış alarm oranının sistem performansını olumlu etkileyecek şekilde %39,1’den %0,7’ye düştüğü gözlemlenmiştir. Diğer performans ölçütlerine baktığımızda ise σ seviyeleri yükseldikçe doğruluk ve kesinlik oranı artarken, tespit oranı ve f1 skor oranlarının azaldığı görülmektedir. Bu, sistem performansını olumsuz yönde etkilediği anlamına gelmektedir. Çizelge 5.6 ve Şekil 5.10’daki sonuçlar, LCFS kullanılarak uygulanan SMD yaklaşımının, tespit ve yanlış alarm oranı bakımından daha olumlu sonuçlar sağladığı görüşünü desteklemektedir. Sonuç olarak Nİ ağ saldırı mimarisinde önemli bir faktör olan gereksiz özniteliklerin çıkarılması, hem hesaplama karmaşıklığının keskin bir şekilde azalmasına hem de tespit oranının olumlu yönde artmasına etki ettiği görülmüştür. Şekilde 5.10’da, farklı eşik seviyelerinde veri setinin tüm öznitelikleri kullanılarak elde edilen sonuçların grafiksel gösterimi verilmiştir.



Şekil 5.9. Tüm öznitelikler kullanılarak farklı eşik değerleri üzerinde değerlendirme ölçütleri

5.4.3. Diğer çalışmalarla karşılaştırma sonuçları

LCFS ve SMD yaklaşımının deney sonuçları literatürdeki diğer çalışmalar ile doğruluk, tespit oranı ve yanlış pozitif oranı olmak üzere üç farklı değerlendirme ölçütü bakımından karşılaştırılmıştır. Çizelge 5.7’de UNSW-NB15 veri setini kullanan farklı istatistiksel tabanlı öznitelik seçimi tekniklerinin üç farklı değerlendirme metriği bakımından karşılaştırıldığına dair sonuçlar verilmiştir. Değerlendirme sonuçları kapsamında, CorrCorr [12] yöntemine göre önerilen modelin yanlış alarm oranı bakımından daha düşük sonuç elde ettiği gözlemlenmiştir. Doğruluk (%98,38) ve tespit oranı (%99,82) bakımından, diğer

çalışmalardan daha yüksek sonuç elde ettiği görülmüştür. Bununla birlikte CorrCorr [12] öznitelik seçim yönteminin önerildiği çalışma incelendiğinde, $0,5\sigma$ eşik seviyesinden 1σ 'e doğru yükseldiğinde tespit oranının da %100'den %56,80'e doğru ani bir şekilde düştüğü fark edilmiştir. Fakat LCFS ve SMD'ye dayalı önerilen modelde, eşik seviyesinin $0,5\sigma$ 'dan 2σ 'ya doğru yükseldiği durumda, %99,94'ten %92,90'a doğru azalan tespit oranı aralığı elde edildiği ve önemli ölçüde azalan bir tespit oranı değişkenliği göstermediği gözlemlenmiştir. Ayrıca diğer çalışmalara göre daha iyi anomali tespit oranı gösterdiği gözlemlenmiştir.

Çizelge 5.7. UNSW-NB15 veri seti üzerinde farklı istatistiksel tabanlı öznitelik seçim yöntemlerinin karşılaştırılması

Makaleler	Doğruluk	Tespit Oranı	Yanlış Alarm (FPR)
Finite Dirichlet Mixture Model [44]	%94,30	%93,90	%5,80
CorrCorr + Mahalanobis [12]	%93,27	%56,80	%1,12
LCFS + SMD (mevcut çalışma)	%98,38	%99,82	%1,82

Diğer karşılaştırma çalışması ise aynı LCFS öznitelik seçimini kullanan, ancak sınıflandırma algoritması olarak karar ağacını uygulayan bir çalışma üzerinde gerçekleştirilmiştir. Eid ve arkadaşlarının çalışmasında [10] yalnızca F1 ölçütü değerlendirme metriği olarak sunulduğundan, Çizelge 5.8'de mevcut önerilen çalışma ile sadece F1 ölçütü bakımından karşılaştırılmıştır.

Çizelge 5.8. Aynı LCFS öznitelik seçimini kullanan çalışmanın mevcut yöntemle karşılaştırılması

Makale	F1 Ölçütü
LCFS + C4.5 [10]	%99,1
LCFS + SMD (mevcut çalışma)	%93,8

Aynı öznitelik seçimi kullanıldığında, istatistiksel SMD modeliyle makine öğrenmesine dayalı yaklaşım arasında performans bakımından birbirine yakın sonuçlar elde edildiği ve SMD sınıflandırıcısının daha az hesaplama maliyeti gerektirdiği görülmüştür. Eid ve arkadaşlarının [10] çalışması üzerinde farklı makine öğrenimi algoritması, doğruluk ve diğer değerlendirme metrikler kullanarak testler gerçekleştirilse bile, önerilen model ile karşılaştırıldığında farklı veri setlerinin kullanıldığının dikkate alınması gerekmektedir. Eid ve arkadaşlarının [10] çalışmasında güncel olmayan saldırı türlerini içeren NSL-KDD veri setinin kullanıldığı göz önünde bulundurulmalıdır. Özellikle kullanılan veri seti kapsamında

ortaya çıkan en çarpıcı sonuç, önerilen yaklaşımın model oluşturma ve kullanım bakımından daha az zaman ve alan gerektiren istatistiksel yaklaşımlara dayalı olmasıdır [21], [22]. Eid ve arkadaşlarının [10] kullandığı C4.5 sınıflandırıcının, önerilen istatistiksel SMD sınıflandırıcısına kıyasla daha yüksek hesaplama gücü gerektirdiği de göz önünde bulundurulmalıdır.

Çizelge 5.9. UNSW-NB15 veri setini kullanan makine öğrenimine dayalı yöntemlerin karşılaştırılması

Makaleler	Doğruluk	Yanlış Alarm (FPR)
RF-800 [38]	%95,5	%7,22
Karar Ağacı [29]	%85,56	%15,78
Rastgele Orman [45]	%94,94	%0,898
LCFS + SMD (Mevcut Çalışma)	%98,38	%1,82

Son olarak Çizelge 5.9’da mevcut çalışmamızın literatürde diğer makine öğrenmesine dayalı çalışmalar ile doğruluk ve yanlış alarm oranı bakımından karşılaştırılması gerçekleştirilmiştir. Çizelge 5.9’da doğruluk ve yanlış alarm bakımından UNSW-NB15 veri setini kullanan literatür çalışmalarına ait karşılaştırma tablosu sunulmuştur. Önerilen model, doğruluk oranı bakımından diğer çalışmalar ile karşılaştırıldığında %98,38 oranla en yüksek sonucu elde ettiği görülmüştür. Bununla birlikte yanlış alarm oranı bakımından karar ağacı [29] ve RF-800 [38] çalışmaları ile karşılaştırıldığında, önerilen modelin %1,82 daha yüksek yanlış alarm oranına ulaştığı görülmüşürken, rastgele orman [45] yöntemine göre de daha düşük başarı oranına ulaştığı görülmüştür. Özetlemek gerekirse, önerilen modelin doğruluk oranı bakımından karşılaştırılan literatür çalışmaları [29], [38], [45] arasında en yüksek doğruluk oranını elde ettiği gözlemlenmiştir. Bununla birlikte yanlış alarm oranı bakımından saldırı tespit sistemleri için oldukça iyi bir sonuç elde ettiği görülmüştür. Önerilen istatistiksel tabanlı SMD sınıflandırıcısı, literatür çalışmalarına kıyasla model oluşturma ve kullanım bakımından daha az hesaplama maliyeti gerektirmektedir [21], [22].

5.4.4. Dengeli veri seti üzerinde deney sonuçları

Dengesiz veri setlerinin her zaman yanıltıcı içgörülerin elde edilmesine neden olduğu sınıflandırma alanında iyi bilinmektedir. Geleneksel öğrenme yöntemleri, ilk olarak dengeli veri setleri için tasarlanmış olup dengesiz veri kümeleri üzerinde eğitildiğinde, sayı bakımından çoğunluğa sahip olan sınıf etiketini üretme eğilimi gösterirler [97]. Bu nedenle deney kapsamında, önerilen ikili sınıflandırma yönteminin dengeli dağılım gösteren veri seti üzerinde duyarlı olup olmadığını test etmek üzere deneyler gerçekleştirilmiştir. Sınıf

dengesizliği sorununu çözmeye yönelik çoğunluğa sahip sınıf etiketinden rastgele satırların kaldırılması gerçekleştirilmiştir.

Birinci deney kapsamında oranlı bir şekilde 50.000 normal ve 50.000 anomali test veri seti elde etmek için 2,5 milyon satır içeren veri seti rastgele örneklem ile 250.000 normal ve 250.000 anomali olmak üzere 500.000 satırlık dengeli veri setine indirgenmiştir. Ardından elde edilen dengeli veri seti üzerinde LCFS yöntemi uygulanıp eğitim için %80 ve test için %20 olacak şekilde bölünmüştür. Böylece oranlı bir şekilde 50.000 normal ve 50.000 anomali test veri seti elde edilmiştir. Birinci dengeli deney sonucunda hedef değişkeniyle en yüksek alaka seviyesine sahip ilk üç ve ilk dört öznitelik sonuçları karşılaştırıldığında, $0,5\sigma$ eşik seviyesinde %100'lük bir tespit oranı elde edilirken f1 skoru bakımından %84,42 başarı oranı elde edildiği görülmüştür. Ancak eşik değeri seviyesinin $0,5\sigma$ 'dan 3σ 'ya doğru yükseldiği durumda, tespit oranının %100'den %0,04'e doğru önemli ölçüde düştüğü fark edilmiştir. Aynı zamanda eşik değeri seviyesi $0,5\sigma$ 'dan 3σ 'ya doğru yükseldiğinde yanlış alarm oranının da %0,0'a düştüğü görülmüştür. Birinci dengeli dağılım gösteren test veri setinden elde edilen sonuçlar doğrultusunda anomali değerlerin ortalamaya yakın değerler aldığı görülmektedir. Bu nedenle en iyi tespit oranının da ortalamaya en yakın olan $0,5\sigma$ eşik seviyesinde elde edildiği gözlemlenmiştir. Çizelge 5.10'da 50.000 normal ve 50.000 anomali dengeli test veri setine ait deney sonuçları verilmiştir.

Çizelge 5.10. İlk üç öznitelik ve 10 kat çapraz doğrulama kullanılarak 50.000 normal ve 50.000 anomali dengeli test veri setinin performansı

Eşik Değeri	$0,5\sigma$	1σ	$1,5\sigma$	2σ	$2,5\sigma$	3σ
Doğruluk	%81,53	%58,40	%58,23	%58,48	%55,10	%49,99
Kesinlik	%73,04	%89,44	%91,20	%93,44	%91,18	%100
Tespit Oranı	%100	%19,10	%18,29	%18,29	%11,36	%0,04
F1 Skor	%84,42	%31,48	%30,47	%30,59	%20,21	%0,09
Yanlış Alarm (FPR)	%36,94	%2,25	%1,76	%1,28	%1,10	%0,0

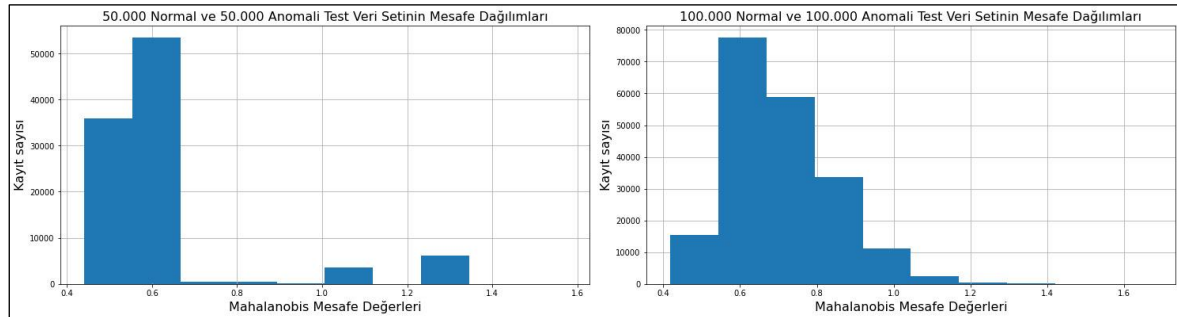
İkinci dengeli deney ortamı ise dengeli veri seti boyutu arttığında performans bakımından değişkenliği incelemek üzere eşit olarak bölünmüş 100.000 normal ve 100.000 anomali veri örnekleme üzerinde gerçekleştirilmiştir. Ancak ikinci deney veri seti birinci deneydeki gibi 100.000 normal ve 100.000 anomali olacak şekilde otomatik olarak oranlı bölünememektedir. Büyük veri ölçeğinde 2,5 milyon satır içeren veri setinde 321.283 anomali değer içerdiğinden oranlı bir şekilde en fazla 64.256 normal ve 64.256 anomali değer içerecek şekilde oranlı bölünebilmektedir. Bu nedenle orijinal veri setinden 100.000

anomali içerecek şekilde alt örnekleme (down-sampling) işlemi uygulanmıştır. Böylece oransal olarak bölündüğünde 100.000 normal ve 100.000 anomali içeren test veri seti elde edilmiştir. Deney sonucunda veri setini en iyi temsil eden ilk üç ve ilk dört öznitelik sonuçları karşılaştırıldığında ise $0,5\sigma$ eşik seviyesinde iken tespit oranının %56,27'ye, yanlış alarm oranının da %48,16'ya ulaştığı gözlemlenmiştir. Elde edilen %48,16'lık yüksek yanlış alarm oranının, çoğu ağ saldırı sistemleri için kabul edilemez bir değerdir. Ancak eşik değeri seviyesi $0,5\sigma$ 'nın üzerine çıktığında ise yanlış alarm seviyesinin %0,0'a, tespit oranının da %56,27'den %0,40'a kadar düştüğü görülmüştür. Çizelge 5.11'de test veri setine ait performans değerleri verilmiştir.

Çizelge 5.11. İlk üç öznitelik ve 10 kat çapraz doğrulama kullanılarak 100.000 normal ve 100.000 anomali dengeli test veri setinin performansı

Eşik Değeri	$0,5\sigma$	1σ	$1,5\sigma$	2σ	$2,5\sigma$	3σ
Doğruluk	%54,04	%56,80	%54,83	%52,32	%50,41	%50,14
Kesinlik	%53,88	%62,88	%72,93	%80,23	%72,27	%78,83
Tespit Oranı	%56,27	%33,21	%15,38	%6,16	%1,34	%0,40
F1 Skor	%55,05	%43,46	%25,41	%11,45	%2,63	%0,80
Yanlış Alarm (FPR)	%48,16	%19,59	%5,70	%1,51	%0,51	%0,10

Sonuç olarak yürütülen dengeli veri setleri deneyleri değerlendirildiğinde, her iki dengeli veri setinin farklı dağılımlar gösterdiği görülmüştür. Birinci deneyde normal ve anomali mesafe değerlerinin 0.45 ile 0.65 aralığında yoğun bir şekilde dağıldığı, ikinci deneyde ise değerlerin 0.41 ile 1.0 aralığında dağılım gösterdiği gözlemlenmiştir. Bu nedenle, her iki veri setinden elde ettiğimiz sonuçlarda da farklı performans değerleri elde edilmiştir. Şekil 5.10'da her iki deneyin test veri setine ait görseli verilmiştir.



Şekil 5.10. Dengeli veri setlerine ait mesafe değerlerinin dağılımı



6. DEĞERLENDİRME VE SONUÇ

Nesnelerin interneti (Nİ), sağlıktan endüstriye kadar pek çok alanda kullanılmakta olup büyük verinin üretilmesinde de temel kaynağı oluşturmaktadır. Gelişen teknoloji ile birlikte bu cihazlara yapılan saldırı sayıları her geçen gün artmaktadır. Veri boyutu arttıkça da ağ saldırılarını tespit eden yaklaşımlarda daha fazla hesaplama maliyeti söz konusu olmaktadır. Dolayısıyla bu cihazlara yapılan saldırıları daha düşük hesaplama karmaşıklığıyla tespit etmek önem kazanmaktadır. Bu nedenle, Nİ cihazlarında saldırıları tespit edebilecek güvenlik çözümlerinin geliştirilmesine gereksinim duyulmaktadır. Tez çalışmasında, Nİ cihazlarında model oluşturma ve kullanım açısından daha az karmaşıklığa sahip anomali tabanlı yeni bir saldırı tespit yaklaşımı önerilmektedir. Böylece büyük veri ortamında artan ağ saldırılarının daha az hesaplama karmaşıklığıyla tespit edilmesi amaçlanmaktadır. Bununla beraber geleneksel Mahalanobis mesafesinde mevcut olan kovaryans matris karmaşıklığını çözen basitleştirilmiş Mahalanobis mesafesinin genel ağ saldırılarında performans ölçütleri bakımından etkinliği de değerlendirilmektedir.

Uygulama aşamasında; dört farklı CSV formatında indirilen UNSW-NB15 veri setinin birleştirilmesi, temizlenmesi, öznitelik dönüşümü ve ölçeklendirme gibi veri ön işleme adımları takip edilmiştir. Ardından büyük veri setini daha az boyutta öznitelik ile temsil etmek üzere iki katmandan oluşan doğrusal korelasyona dayalı öznitelik seçme (LCFS) yöntemi kullanılmıştır. Öznitelikleri seçmek için istatistikte yaygın olarak kullanılan ve literatürde en önemli iyilik ölçütü olarak belirtilen Pearson korelasyon katsayısı tercih edilmiştir. Birinci katmanda, sürekli (ondalık) değerlere sahip olan öznitelikler arasında korelasyon katsayısına göre boyut azaltma yöntemi uygulanmıştır. $P > 0,6$ 'dan büyük korelasyon katsayısına sahip öznitelik çiftlerinin yüksek ilişki düzeyine sahip olduğu kabul edilmekte ve hedef değişkenini tahmin etmede aynı bilgiyi içermektedir. Bu nedenle iki öznitelikten biri gereksiz kabul edilip veri setinden çıkarılmıştır. İkinci katman aşaması ise birinci katmandan geriye kalan öznitelikler kullanılarak öznitelikler ve hedef değişkeni arasında en yüksek korelasyon katsayısına sahip öznitelikleri elde etmek üzere uygulanmıştır. Ardından öznitelikler ve hedef değişkeni arasında hesaplanan korelasyon katsayıları büyükten küçüğe doğru sıralanıp hedef değişkenin daha yüksek doğruluk oranıyla tahmin edilebileceği N adet özniteliğin seçimi yapılmıştır. Öznitelik seçiminden sonra anomalilerin tespit edildiği sınıflandırma yöntemi olarak Mahalanobis mesafesi uygulanmıştır. Ancak klasik Mahalanobis mesafesinin sınırlı sayıda öznitelik ile

hesaplanmasından ve veri boyutu arttıkça kovaryans matrisinin hesaplama karmaşıklığından dolayı yerine basitleştirilmiş Mahalanobis mesafesinin (SMD) kullanılması önerilmiştir. Böylece çoklu öznitelige sahip olan veri kümesinin tek değişkenli mesafe öznitelğine dönüşümü gerçekleştirilmiştir. Hesaplanan tek değişkenli mesafe değerleri üzerinde tespit mekanizması olarak literatürde en çok kabul gören ortalama (μ), standart sapma (σ) ve 1-3 arası değişen alfa (α) değerlerinden oluşan istatistiksel temelli bir eşik değer (üç sigma) yöntemi kullanılmıştır. Eğitim aşamasına gelindiğinde, normal ağ trafiğini içeren veri kümesi kullanılarak hesaplanan mesafe değerleri üzerinde $0,5\sigma$ ile 3σ aralığında değişen alt ($\alpha\sigma - \mu$) ve üst ($\alpha\sigma + \mu$) sınırlara sahip eşik değerleri hesaplanmaktadır. Yeni gelen ağ verileri üzerinde mesafe değerleri değerlendirildiğinde alt ve üst sınırlar arasında yer alan değerler normal ağ trafiği olarak işaretlenmiştir. Eşik değerleri dışında yer alan test verilerine baktığımızda ise anomali ağ trafiği olarak işaretlenip sistem için oluşan tehditler tespit edilmiş olur.

Performans kapsamında; önerilen model 3, 4, 5, 7 ve 10 gibi farklı öznitelik sayıları ve 10 kat çapraz doğrulama yöntemi kullanılarak değerlendirilmiştir. Model başarısını değerlendirmek üzere LCFS ile SMD, öznitelik seçimi kullanılmadan SMD, makine öğrenimine dayalı diğer yaklaşımlarla karşılaştırma ve dengeli dağılım gösteren veri seti de olmak üzere dört farklı deney gerçekleştirilmiştir. LCFS ile SMD yönteminin deney sonuçları incelendiğinde, saldırı tespit sistemleri için önemli olan en yüksek tespit oranının %99,82 ile %99,946 arasında ve en düşük yanlış alarm oranının da %0,88 ile %1,04 arasında elde edildiği görülmüştür. Öznitelik seçimi kullanılmadan gerçekleştirilen deneyler değerlendirildiğinde, $0,5\sigma$ eşik seviyesinde en yüksek tespit oranının %97,1 olarak elde edildiği ve eşik seviyesinin 1σ 'dan 3σ 'ya doğru arttığında ise tespit oranının %77,33'ten %10,71'e doğru hızlı bir şekilde düşüşe geçtiği gözlemlenmiştir. LCFS kullanılarak ve LCFS kullanılmadan yürütülen her iki deneyde $0,5\sigma$ eşik seviyesinde en yüksek tespit oranına ulaşılmış ve 3σ eşik seviyesine doğru arttıındaysa tespit oranının azaldığı görülmüştür. Elde edilen bulgulara göre veri setinin sola çarpık dağılım gösterdiği söylenebilir. Makine öğrenimine dayalı RF-800 [38], karar ağacı [29] ve rastgele orman [45] gibi literatür çalışmalarıyla doğruluk ve yanlış alarm ölçütleri bakımından kıyaslandığında ise %98,38 ile en yüksek doğruluk oranı ve rastgele orman [45] yönteminden sonra %1,82'lik oranla en düşük yanlış alarm oranı elde edilmiştir. Son olarak, dengeli dağılım gösteren test veri seti üzerinde yapılan deneyler değerlendirildiğinde $0,5\sigma$ eşik seviyesinde 50.000 normal ve 50.000 anomali test verilerinde %100'lük tespit oranı elde edildiği, ancak

eşik seviyesinin 1σ değerine yükselmesi durumunda tespit oranının %19,1'e düştüğü gözlemlenmiştir. Bununla birlikte 100.000 normal ve 100.000 anomali kayıt sayısını içeren test veri setinde en yüksek tespit oranının %56,27 olarak elde edildiği görülmüştür. Sonuç olarak dengeli veri seti sonuçları değerlendirildiğinde, her iki test veri setinin farklı dağılımlar gösterdiği ve bu nedenle farklı performans değerleri elde edildiği gözlemlenmiştir.

Yürütülen literatür taraması sonucunda Nİ alanında daha az hesaplama karmaşıklığıyla anomalileri tespit eden yöntemlere ihtiyaç duyulduğu anlaşılmıştır. Dolayısıyla Nİ ağ saldırı tespitinde kullanılabilecek ve klasik Mahalanobis mesafesinin hesaplama karmaşıklığını giderecek, LCFS ile SMD'yi birleştiren özgün bir çalışmayla literatüre katkı sağlanmıştır. Doğruluk, tespit oranı, duyarlılık, f1 skor ve yanlış alarm ölçütleri bakımından değerlendirildiğinde ise incelenen literatür çalışmalarından daha yüksek veya onlara yakın sonuçlar elde edilebileceği kanıtlanmıştır. Gelecek çalışmalarda; gerçek ağ ortamından elde edilen veri seti üzerinde değerlendirilmesi, gerçek zamanlı Nİ ortamına uygulanması ve farklı öznelik seçimi yöntemleriyle deneyler gerçekleştirilmesi hedeflenmektedir.



KAYNAKLAR

1. Ge, M., Bangui, H., and Buhnova, B. (2018). Big Data for Internet of Things: A Survey. *Future Generation Computer Systems*, 87, 601-614.
2. Zarpelão, B. B., Miani, R. S., Kawakani, C. T., and de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, 84, 25-37.
3. Ahmed, E., Yaqoob, I., Hashem, I. A. T., Khan, I., Ahmed, A. I. A., Imran, M., and Vasilakos, A. V. (2017). The role of big data analytics in Internet of Things. *Computer Networks*, 129, 459-471.
4. Newman, P. (2018). IoT Report: How Internet of Things technology growth is reaching mainstream companies and consumers. Business Insider.
5. da Costa, K. A. P., Papa, J. P., Lisboa, C. O., Munoz, R., and de Albuquerque, V. H. C. (2019). Internet of Things: A survey on machine learning-based intrusion detection approaches. *Computer Networks*, 151, 147-157.
6. Ahmed, M., Naser Mahmood, A., and Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, 60, 19-31.
7. Srinivasan, N., and Vaidehi, V. (2007). *Reduction of False Alarm Rate in Detecting Network Anomaly using Mahalanobis Distance and Similarity Measure*. In 2007 International Conference on Signal Processing, Communications and Networking, Chennai, India, 366-371.
8. Moustafa, N., and Slay, J. (2015, November). *UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)*. In 2015 military communications and information systems conference (MilCIS), Canberra, Australia, 1-6.
9. Mahdavinejad, M. S., Rezvan, M., Barekatain, M., Adibi, P., Barnaghi, P., and Sheth, A. P. (2018). Machine learning for Internet of Things data analysis: A survey. *Digital Communications and Networks*, 4(3), 161-175.
10. Eid, H. F., Hassanien, A. E., Kim, T. H., and Banerjee, S. (2013, September). *Linear correlation-based feature selection for network intrusion detection model*. In International Conference on Security of Information and Communication Networks, Berlin, Heidelberg, 240-248.
11. Zhang, F., and Wang, D. (2013, July). *An effective feature selection approach for network intrusion detection*. In 2013 IEEE eighth international conference on networking, architecture and storage, Xi'an, China, 307-311.
12. Gottwalt, F., Chang, E., and Dillon, T. (2019). CorrCorr: A feature selection method for multivariate correlation network anomaly detection techniques. *Computers & Security*, 83, 234-245.
13. Aghdam, M. H., and Kabiri, P. (2016). Feature selection for intrusion detection system using ant colony optimization. *International Journal of Network Security*, 18(3), 420-432.

14. Vimalkumar, K., and Radhika, N. (2017, September). *A big data framework for intrusion detection in smart grids using apache spark*. In 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, India, 198-204.
15. Yu, L., and Liu, H. (2004). Efficient feature selection via analysis of relevance and redundancy. *The Journal of Machine Learning Research*, 5, 1205-1224.
16. Dy, J. G., and Brodley, C. E. (2004). Feature selection for unsupervised learning. *Journal of machine learning research*, 5, 845-889.
17. Anwer, H. M., Farouk, M., and Abdel-Hamid, A. (2018, April). *A framework for efficient network anomaly intrusion detection with features selection*. In 2018 9th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 157-162.
18. Patil, N., Das, D., and Pecht, M. (2015). Anomaly detection for IGBTs using Mahalanobis distance. *Microelectronics Reliability*, 55(7), 1054-1059.
19. Wang, Y., Miao, Q., Ma, E. W., Tsui, K. L., and Pecht, M. G. (2013). Online anomaly detection for hard disk drives based on mahalanobis distance. *IEEE Transactions on Reliability*, 62(1), 136-145.
20. Hu, Z., Xiao, M., Zhang, L., Liu, S., and Ge, Y. (2016). Mahalanobis distance based approach for anomaly detection of analog filters using frequency features and Parzen window density estimation. *Journal of Electronic Testing*, 32(6), 681-693.
21. Wang, K., and Stolfo, S. J. (2004). Anomalous Payload-Based Network Intrusion Detection. E. Jonsson, A. Valdes ve M. Almgren (Ed.), Recent Advances in Intrusion Detection, In Lecture Notes in Computer Science (C. 3224, ss. 203-222). Berlin, Heidelberg: Springer.
22. Villamarín-Salomón, R., and Brustoloni, J. C. (2008, January). *Identifying botnets using anomaly detection techniques applied to DNS traffic*. 2008 5th IEEE consumer communications and networking conference, Las Vegas, NV, USA.
23. Li, Q., Tan, Z., Jamdagni, A., Nanda, P., He, X., and Han, W. (2017, August). *An intrusion detection system based on polynomial feature correlation analysis*. 2017 IEEE Trustcom/BigDataSE/ICCESS, 978-983.
24. Tan, Z., Jamdagni, A., He, X., Nanda, P., and Liu, R. P. (2013). A system for denial-of-service attack detection based on multivariate correlation analysis. *IEEE transactions on parallel and distributed systems*, 25(2), 447-456.
25. Buczak, A. L., and Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications surveys & tutorials*, 18(2), 1153-1176.
26. Makani, R., and Reddy, B. V. R. (2018). Taxonomy of machine leaning based anomaly detection and its suitability. *Procedia computer science*, 132, 1842-1849.
27. Ahmed, M., Mahmood, A. N., and Islam, M. R. (2016). A survey of anomaly detection techniques in financial domain. *Future Generation Computer Systems*, 55, 278-288.

28. Goldstein, M., and Uchida, S. (2016). A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. *PloS one*, 11(4), e0152173.
29. Moustafa, N., and Slay, J. (2016). 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*, 25(1-3), 18-31.
30. Chen, M., Mao, S., and Liu, Y. (2014). Big data: A survey. *Mobile networks and applications*, 19(2), 171-209.
31. Gandomi, A., and Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International journal of information management*, 35(2), 137-144.
32. İnternet: Schroeck, M., Shockley, R., Smart, Dr. J., Romero-Morales, D., and Tufano, P. (2012). Analytics: The real-world use of big data, *IBM Institute for Business Value in collaboration with the Saïd Business School*, University of Oxford, URL: <https://www.ibm.com/downloads/cas/ONBGKB82>, Son Erişim Tarihi: 13.06.2021
33. Ambusaidi, M. A., He, X., Nanda, P., and Tan, Z. (2016). Building an intrusion detection system using a filter-based feature selection algorithm. *IEEE transactions on computers*, 65(10), 2986-2998.
34. Kohavi, R., and John, G. H. (1997). Wrappers for feature subset selection. *Artificial intelligence*, 97(1-2), 273-324.
35. Biesiada, J., and Duch, W. (2007). *Feature Selection for High-Dimensional Data—A Pearson Redundancy Based Filter*. M. Kurzynski, E. Puchala, M. Wozniak ve A. Zolnierrek (Ed.), Computer Recognition Systems 2 in, Advances in Soft Computing (C. 45, ss. 242-249). Berlin, Heidelberg: Springer Berlin Heidelberg.
36. Mitchell, T. M. (2006). *The Discipline of Machine Learning*. Pittsburgh, PA, USA: Carnegie Mellon University, School of Computer Science, Machine Learning Department.
37. Wu, N., and Zhang, J. (2006). Factor-analysis based anomaly detection and clustering. *Decision Support Systems*, 42(1), 375-389.
38. Primartha, R., and Tama, B. A. (2017, November). *Anomaly detection using random forest: A performance revisited*. In 2017 International conference on data and software engineering (ICoDSE), Palembang, Indonesia.
39. Muniyandi, A. P., Rajeswari, R., and Rajaram, R. (2012). Network anomaly detection by cascading k-Means clustering and C4. 5 decision tree algorithm. *Procedia Engineering*, 30, 174-182.
40. Chen, C., Gong, Y., and Tian, Y. (2008, October). *Semi-supervised learning methods for network intrusion detection*. In 2008 IEEE international conference on systems, man and cybernetics, Singapore, 2603-2608.
41. Shon, T., and Moon, J. (2007). A hybrid machine learning approach to network anomaly detection. *Information Sciences*, 177(18), 3799-3821.
42. Gadal, S. M. A. M., and Mokhtar, R. A. (2017, January). *Anomaly detection approach using hybrid algorithm of data mining technique*. In 2017 International Conference on

- Communication, Control, Computing and Electronics Engineering (ICCCCEE), Khartoum, Sudan, 1-6.
43. Al-Jarrah, O. Y., Siddiqui, A., Elsalamouny, M., Yoo, P. D., Muhaidat, S., and Kim, K. (2014, June). *Machine-learning-based feature selection techniques for large-scale network intrusion detection*. In 2014 IEEE 34th international conference on distributed computing systems workshops (ICDCSW), 177-181.
 44. Moustafa, N., Creech, G., and Slay, J. (2017). *Big data analytics for intrusion detection system: Statistical decision-making using finite dirichlet mixture models*. In Data analytics and decision support for cybersecurity, 127-156.
 45. Verma, A., and Ranga, V. (2020). Machine learning based intrusion detection systems for IoT applications. *Wireless Personal Communications*, 111(4), 2287-2310.
 46. Timčenko, V., and Gajin, S. (2018). *Machine learning based network anomaly detection for IoT environments*. In ICIST-2018 Conference, Kopaonik, Serbia.
 47. Abdulhammed, R., Faezipour, M., Abuzneid, A., and AbuMallouh, A. (2018). Deep and machine learning approaches for anomaly-based intrusion detection of imbalanced network traffic. *IEEE sensors letters*, 3(1), 1-4.
 48. Pajouh, H. H., Dastghaibfard, G., and Hashemi, S. (2017). Two-tier network anomaly detection model: a machine learning approach. *Journal of Intelligent Information Systems*, 48(1), 61-74.
 49. Ravale, U., Marathe, N., and Padiya, P. (2015). Feature selection based hybrid anomaly intrusion detection system using K means and RBF kernel function. *Procedia Computer Science*, 45, 428-435.
 50. Emadi, H. S., and Mazinani, S. M. (2018). A novel anomaly detection algorithm using DBSCAN and SVM in wireless sensor networks. *Wireless Personal Communications*, 98(2), 2025-2035.
 51. Tonejc, J., Güttes, S., Kobekova, A., and Kaur, J. (2016). Machine Learning Methods for Anomaly Detection in BACnet Networks. *Journal of Universal Computer Science*, 22(9), 1203-1224.
 52. Zhang, J., Gardner, R., and Vukotic, I. (2019). Anomaly detection in wide area network meshes using two machine learning algorithms. *Future Generation Computer Systems*, 93, 418-426.
 53. Doshi, R., Apthorpe, N., and Feamster, N. (2018, May). *Machine learning ddos detection for consumer internet of things devices*. In 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 29-35.
 54. Casas, P., Fiadino, P., and D'Alconzo, A. (2016, April). *Machine-Learning Based Approaches for Anomaly Detection and Classification in Cellular Networks*. In 8th Traffic Monitoring and Analysis (TMA2016) Workshop, Louvain La Neuve, Belgium.
 55. Domb, M., Bonchek-Dokow, E., and Leshem, G. (2017). Lightweight adaptive Random-Forest for IoT rule generation and execution. *Journal of Information Security and Applications*, 34, 218-224.

56. Dromard, J., Roudière, G., and Owezarski, P. (2016). Online and scalable unsupervised network anomaly detection method. *IEEE Transactions on Network and Service Management*, 14(1), 34-47.
57. Kaya, Ç. (2016). Saldırı Tespit Sistemlerinde Makine Öğrenmesi Tekniklerinin Kullanılması: Karşılaştırmalı Performans Analizi, Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.
58. Mahamat, S. B., and Çeken, C. Anomaly Detection in Software-Defined Networking Using Machine Learning. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 7(1), 748-756.
59. Tian-yi, Y., Shi-yue, L., and Jun-yi, L. (2019). Network Traffic Anomaly Detection Based on Incremental Possibilistic Clustering Algorithm. *Journal of Physics: Conference Series*, 1284, 012067.
60. Christensen, R. L., Sznaiar, M., Wisniewski, R., and Sørensen, K. K. (2018). Unsupervised Fault Detection of Refrigeration Containers using a Mahalanobis Inverse Moment Matrix Polynomial. *IFAC-PapersOnLine*, 51(24), 249-254.
61. Salem, O., Liu, Y., and Mehaoua, A. (2013). Anomaly Detection in Medical Wireless Sensor Networks. *Journal of Computing Science and Engineering*, 7(4), 13.
62. Dai, D. (2017). On high-dimensional Mahalanobis distances. Department of Economics and Statistics, Linnaeus University.
63. Nguyen, T. T., and Vu, T. D. (2019). Identification of multivariate geochemical anomalies using spatial autocorrelation analysis and robust statistics. *Ore Geology Reviews*, 111(1-3), 102985.
64. Khalastchi, E., Kalech, M., Kaminka, G. A., and Lin, R. (2015). Online data-driven anomaly detection in autonomous robots. *Knowledge and Information Systems*, 43(3), 657-688.
65. Park, J., Choi, D. H., Jeon, Y.-B., Nam, Y., Hong, M., and Park, D.-S. (2018). Network anomaly detection based on probabilistic analysis. *Soft Computing*, 22(20), 6621-6627.
66. Cerquitelli, T. (2017). Predicting Large Scale Fine Grain Energy Consumption. *Energy Procedia*, 111, 1079-1088.
67. Vilaça, E. S., Vieira, T. P., de Sousa, R. T., and da Costa, J. P. C. (2019, October). *Botnet traffic detection using RPCA and Mahalanobis Distance*. In 2019 Workshop on Communication Networks and Power Systems (WCNPS), Brasilia, Brazil, 1-6.
68. Hou, Y., Chen, Z., Wu, M., Foo, C. S., Li, X., and Shubair, R. M. (2020, May). *Mahalanobis Distance Based Adversarial Network for Anomaly Detection*. In ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Barcelona, Spain, 3192-3196.
69. Çakmakçı, S. D., Kemmerich, T., Ahmed, T., and Baykal, N. (2020). Online DDoS attack detection using Mahalanobis distance and Kernel-based learning algorithm. *Journal of Network and Computer Applications*, 168, 102756.
70. Hoque, N., Kashyap, H. ve Bhattacharyya, D. K. (2017). Real-time DDoS attack detection using FPGA. *Computer Communications*, 110, 48-58.

71. Shukla, A. S. ve Maurya, R. (2018). Entropy-Based Anomaly Detection in a Network. *Wireless Personal Communications*, 99(4), 1487-1501
72. Hoang, D. H., and Nguyen, H. D. (2018, February). *A PCA-based method for IoT network traffic anomaly detection*. In 2018 20th International conference on advanced communication technology (ICACT), Chuncheon, Korea (South), 381-386.
73. Gottwalt, F., Chang, E., and Dillon, T. (2018, July). *Analysis of Feature Selection Techniques for Correlation-Based Network Anomaly Detection*. In International Conference on Applications and Techniques in Cyber Security and Intelligence, 10-16.
74. Jin, X., Ma, E. W., Cheng, L. L., and Pecht, M. (2012). Health monitoring of cooling fans based on Mahalanobis distance with mRMR feature selection. *IEEE Transactions on Instrumentation and Measurement*, 61(8), 2222-2229.
75. Dash, M., Choi, K., Scheuermann, P., and Liu, H. (2002, December). *Feature selection for clustering-a filter solution*. In 2002 IEEE International Conference on Data Mining, 2002. Proceedings, 115-122.
76. Chen, Z., Yeo, C. K., Francis, B. S. L., and Lau, C. T. (2016, July). *Combining MIC feature selection and feature-based MSPCA for network traffic anomaly detection*. In 2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC), 176-181.
77. Iglesias, F., and Zseby, T. (2015). Analysis of network traffic features for anomaly detection. *Machine Learning*, 101(1), 59-84.
78. Haq, N. F., Onik, A. R., and Shah, F. M. (2015, November). *An ensemble framework of anomaly detection using hybridized feature selection approach (HFSA)*. In 2015 SAI Intelligent Systems Conference (IntelliSys), 989-995.
79. Jyothsna, V., and Prasad, V. R. (2016). FCAAIS: Anomaly based network intrusion detection through feature correlation analysis and association impact scale. *ICT Express*, 2(3), 103-116.
80. Tama, B. A., and Rhee, K. H. (2017). Attack classification analysis of IoT network via deep learning approach. *Research Briefs on Information & Communication Technology Evolution*, 3, 1-9.
81. Dahiya, P., and Srivastava, D. K. (2018). Network intrusion detection in big dataset using spark. *Procedia computer science*, 132, 253-262.
82. Kanimozhi, V., and Jacob, P. (2019). Unsw-nb15 dataset feature selection and network intrusion detection using deep learning. *International Journal of Recent Technology and Engineering*, 7(5S2), 443-446.
83. Kasongo, S. M., and Sun, Y. (2020). Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset. *Journal of Big Data*, 7(1), 1-20.
84. Bharambe, A., Ravindran, R., Suchdev, R., and Tanna, Y. (2014, August). *A robust anomaly detection system*. In 2014 International Conference on Advances in Engineering and Technology Research (ICAETR-2014), 1-7.

85. Han, J., Kamber, M., and Pei, J. (2012). Data Preprocessing. Data Mining: Concepts and Techniques In (3rd ed., ss. 83-124). Waltham, USA: Morgan Kaufmann.
86. Said, D., Stirling, L., Federolf, P., and Barker, K. (2011, July). *Data preprocessing for distance-based unsupervised Intrusion Detection*. In 2011 Ninth Annual International Conference on Privacy, Security and Trust, 181-188.
87. Schober, P., Boer, C., and Schwarte, L. A. (2018). Correlation coefficients: appropriate use and interpretation. *Anesthesia & Analgesia*, 126(5), 1763-1768.
88. Zou, K. H., Tuncali, K., and Silverman, S. G. (2003). Correlation and simple linear regression. *Radiology*, 227(3), 617-628.
89. De Maesschalck, R., Jouan-Rimbaud, D., and Massart, D. L. (2000). The mahalanobis distance. *Chemometrics and intelligent laboratory systems*, 50(1), 1-18.
90. Lin, R., Khalastchi, E., and Kaminka, G. A. (2010, May). *Detecting anomalies in unmanned vehicles using the mahalanobis distance*. In 2010 IEEE international conference on robotics and automation, Anchorage, AK, USA, 3038-3044.
91. Son, S., Gil, M. S., and Moon, Y. S. (2017, February). Anomaly detection for big log data using a Hadoop ecosystem. In 2017 IEEE International Conference on Big Data and Smart Computing (BigComp), Jeju, Korea (South), 377-380.
92. İnternet: A. Sharma. Free GPUs for Everyone! Get Started with Google Colab for Machine Learning and Deep Learning. URL: <https://www.analyticsvidhya.com/blog/2020/03/google-colab-machine-learning-deep-learning>, Son Erişim Tarihi: 05.04.2021.
93. İnternet: Google Colab - What is Google Colab?, *Tutorialspoint* URL: https://www.tutorialspoint.com/google_colab/what_is_google_colab.htm, Son Erişim Tarihi: 03.04.2021.
94. Bisong, E. (2019). Google Colaboratory. Building Machine Learning and Deep Learning Models on Google Cloud Platform In (ss. 59-64). Apress, Berkeley, CA.
95. Rahm, E., and Do, H. H. (2000). Data cleaning: Problems and current approaches. *IEEE Data Engineering Bulletin*, 23(4), 3-13..
96. Zoghi, Z., and Serpen, G. (2021). Unsw-nb15 computer security dataset: Analysis through visualization. *arXiv preprint*, arXiv:2101.05067.
97. Wei, Q., and Dunbrack Jr, R. L. (2013). The role of balanced training and testing data sets for binary classifiers in bioinformatics. *PloS one*, 8(7), e67863.

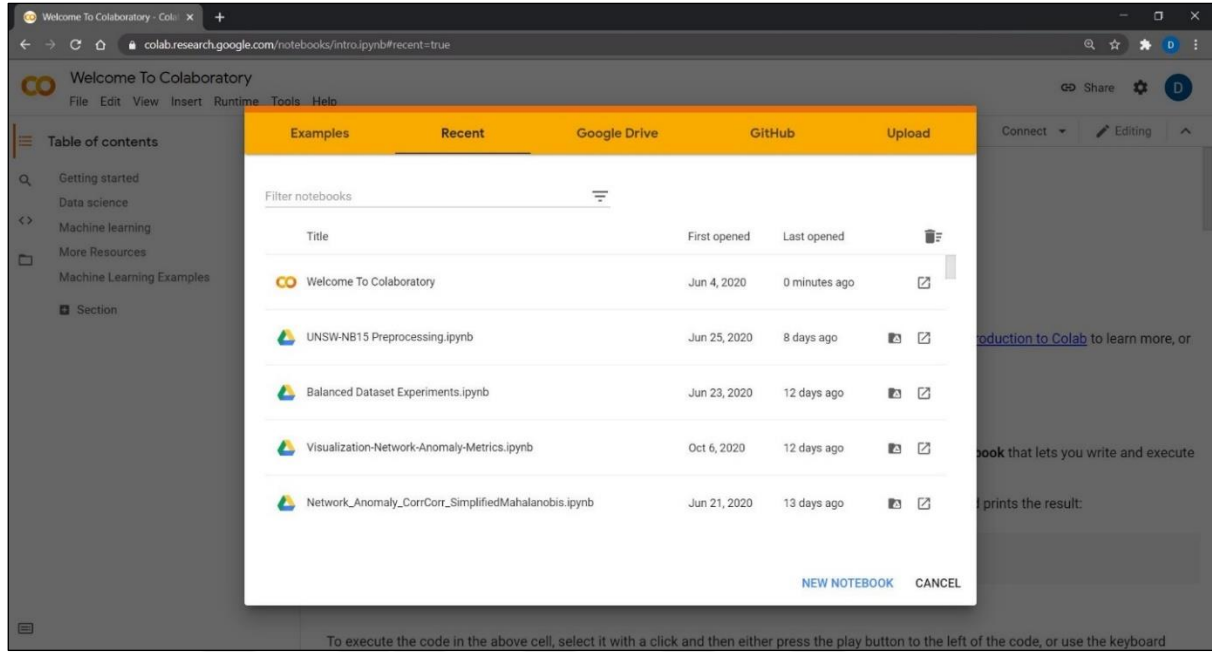


EKLER

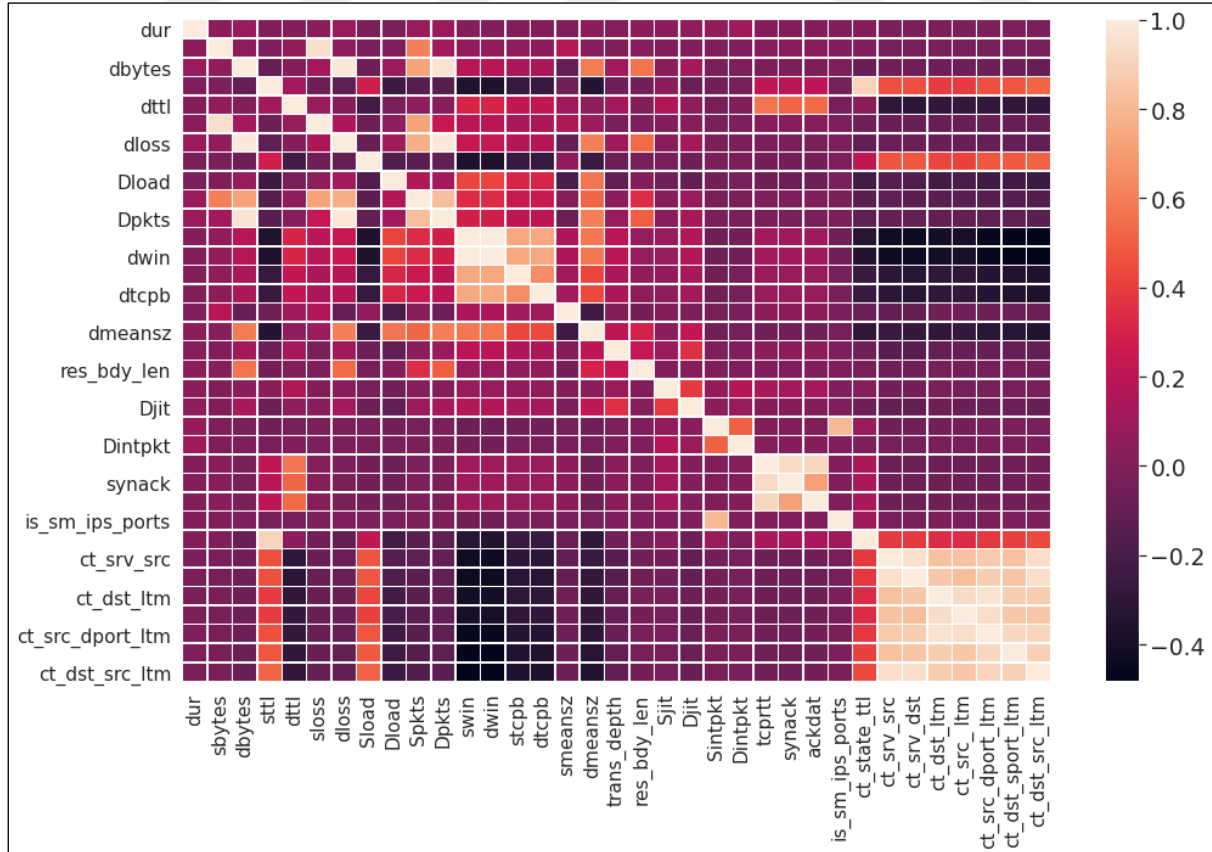
EK-1. Veri ön işleme ve öznitelik seçimi sonrası veri setindeki öznitelikler

Sütün No	Özellik İsmi	Veri Tipi	Sütün No	Özellik İsmi	Veri Tipi
1	Proto	object	21	Trans_depth	int
2	State	object	22	Res_bdy_len	int
3	Dur	float	23	Sjit	float
4	Sbytes	int	24	Djit	float
5	Dbytes	int	25	Sintpkt	float
6	Sttl	int	26	Dintpkt	float
7	Dttl	int	27	Tcprtt	float
8	Sloss	int	28	Synack	float
9	Dloss	int	29	Ackdat	float
10	Service	object	30	Is_sm_ips_ports	int
11	Sload	float	31	Ct_state_ttl	int
12	Dload	float	32	Ct_srv_src	int
13	Spkts	int	33	Ct_srv_dst	int
14	Dpkts	int	34	Ct_dst_ltm	int
15	Swin	int	35	Ct_src_ltm	int
16	Dwin	int	36	Ct_src_dport_ltm	int
17	Stcpb	int	37	Ct_dst_sport_ltm	int
18	Dtcpb	int	38	Ct_dst_src_ltm	int
19	Smeansz	int	39	Labels	int
20	Dmeansz	int			

EK-2. Google Colab ortamında projenin notebookları



EK-3. Özniteliklerin korelasyon katsayılarına ait sıcaklık haritası





GAZİLİ OLMAK AYRICALIKTIR..