Gazi Mühendislik Bilimleri Dergisi
2019, 5(3): 258-272
Araştırma Makalesi/Research Article
https://dergipark.org.tr/gmbd

İki Seviyeli Hibrit Makine Öğrenmesi Yöntemi ile Saldırı Tespiti

Remzi ATAY[a], Duygu Evrim ODABAŞ[a], Meltem KURT PEHLİVANOĞLU[*,a]

[a,*] *Kocaeli Üniversitesi Bilgisayar Mühendisliği Bölümü, KOCAELİ 41380, TÜRKİYE*

MAKALE BİLGİSİ

Alınma: 01.08.2019
Kabul: 18.12.2019

Anahtar Kelimeler:
Saldırı Tespiti, CSE-CIC-IDS2018 Veri Kümesi, Makine Öğrenmesi

Sorumlu Yazar:
e-posta:
meltem.kurt@kocaeli.edu.tr

ÖZET

Bu çalışmada CSE-CIC-IDS2018 veri kümesi üzerinde saldırı tespiti amaçlanmıştır. Kullanılacak yöntemler tek seviyeli yöntem ve iki seviyeli hibrit yöntem olarak iki bölüme ayrılmıştır. Çalışmada Evrişimsel Sinir Ağı (CNN), Rastgele Orman, Hafif Gradyan Artırma (LGBM), (CNN + Rastgele Orman), (LGBM + Rastgele Orman) ve (Rastgele Orman + Rastgele Orman) makine öğrenmesi yöntemleri kullanılarak veri kümesi ele alınmıştır. %98 doğruluk oranı ve 0.86 macro F-skoru ile (CNN + Rastgele Orman) hibrit modelinin en iyi saldırı tespiti yaptığı görülmüştür. Ayrıca, GridSearch ile hiperparametre optimizasyonu yapılmış, Sentetik Azınlık Aşırı Örnekleme Tekniği (SMOTE) ve yüksek korelasyonlu özniteliklerin tespit üzerindeki etkisi incelenmiştir. Çalışma, CSE-CIC-IDS2018 veri kümesi üzerinde ilk defa iki seviyeli hibrit çoklu sınıflandırma kullanıldığı için özgündür.

https://dx.doi.org/10.30855/gmbd.2019.03.07

A Two-Level Hybrid Machine Learning Method for Intrusion Detection

ARTICLE INFO

Received: 01.08.2019
Accepted: 18.12.2019

Keywords:
Intrusion Detection, CSE-CIC-IDS2018 Dataset, Machine Learning

Corresponding Authors
e-mail:
meltem.kurt@kocaeli.edu.tr

ABSTRACT

The aim of this study is to perform intrusion detection on CSE-CIC-IDS2018 dataset. The methods to be used were divided into two parts as one level method and two level hybrid method. In this study, we handled this dataset by using Convolutional Neural Network, Random Forest, Light Gradient Boosting Machine, (CNN + Random Forest), (LGBM + Random Forest) and (Random Forest + Random Forest) machine learning methods. (CNN + Random Forest) was found to be the best intrusion detection method with 98% accuracy score and 0.86 macro F-score. In addition, hyperparameter optimization was performed with GridSearch and the effect of Synthetic Minority Over-sampling Technique and high correlated features on detection was investigated. The study is unique because of that is the first time used the two-level hybrid multi classifying on CSE-CIC-IDS2018 dataset.

https://dx.doi.org/10.30855/gmbd.2019.03.07

1. GİRİŞ *(INTRODUCTION)*

Saldırı Tespit Sistemleri (STS), korunacak ağa dışarıdan veya içeriden yapılan saldırıları tespit etmeyi ve önlemeyi amaçlar. Saldırı Tespit Sistemleri temel olarak imza tabanlı ve anomali tabanlı olarak ikiye ayrılabilir. İmza tabanlı sistemler, daha önce görülen ve bilinen saldırı tiplerinin bir veri tabanında saklanması ile gerçeklenirken anomali tabanlı sistemler gerçek zamanlı paketlerin düzenli ve normal paketler ile aykırılıklarını değerlendirir. Bu aykırılıkların tespiti için genel olarak makine öğrenmesi yöntemleri kullanılır. Bu çalışmada da makine öğrenmesi yöntemleriyle saldırı tespiti amaçlanmıştır.

Var olan saldırı tespit amaçlı veri kümeleri incelendiğinde saldırı çeşitliliği açısından az sayıda güncel veri kümesi bulunmaktadır. Çalışmada 2018 yılında hazırlanmış, saldırı çeşitliliği yüksek olan CSE-CIC-IDS2018 [1] veri kümesi üzerinde saldırı tespiti amaçlanmıştır. Literatürdeki çalışmalar incelendiğinde bu veri kümesi üzerindeki tüm saldırı tiplerini çoklu sınıflandıran tutarlı bir çalışmaya rastlanmamıştır, çalışma bu yönüyle özgün değer taşımaktadır.

Bu çalışmada Tek Seviyeli Yöntem ve İki Seviyeli Hibrit Yöntem olmak üzere iki farklı yöntemin CSE-CIC-IDS2018 veri kümesi üzerinde saldırı tespit başarısı test edilmiştir. Tek seviyeli yöntemde Rastgele Orman, LGBM ve CNN sınıflandırma algoritmaları ile veri kümesi üzerinde saldırı türleri çoklu sınıflandırılmıştır. Ancak Tek Seviyeli Yöntemde kullanılan sınıflandırıcıların yanlış sınıflandırdığı gözlemlerin doğru sınıflandırılabilmesi için, iki seviyeden oluşan (ilk seviyede ikili sınıflandırma yapılıp ikinci seviyede çoklu sınıflandırma yapılarak saldırı türü tespiti) hibrit yöntemin sınıflandırma başarısına etki edip etmeyeceği araştırılmıştır. İki Seviyeli hibrit (Seviye 1 + Seviye 2) yöntemde, önerilen model Seviye 1 ve Seviye 2 olmak üzere iki aşamadan oluşmaktadır. Seviye 1'de; veri kümesi üzerinde saldırı olup olmadığının tespiti için Rastgele Orman, LGBM ve CNN algoritmaları ayrı ayrı denenerek ikili sınıflandırma yapılmıştır. Seviye 2'de ise, Seviye 1'de saldırı olarak tespit edilen gözlemlerin tümü, Rastgele Orman algoritması için test verisi olarak kullanılarak çoklu sınıflandırma yapılmıştır. Elde edilen deneysel sonuçlar incelendiğinde, İki Seviyeli Hibrit yöntem kullanımının veri kümesi üzerinde saldırı tespit başarısını arttırdığı görülmüştür. En yüksek başarımı veren model, CNN algoritması ile ikili sınıflandırmanın ardından Rastgele Orman yöntemi ile çoklu sınıflandırma yapan İki Seviyeli yöntemdir. Yöntemde, %98 doğruluk oranı ve 0.86 F-skor macro ortalamasıyla saldırı tespiti yapılmıştır.

Çalışmanın ikinci bölümünde literatürde saldırı tespit amaçlı makine öğrenmesi ve derin öğrenme yöntemlerini kullanan çalışmalar verilmiştir. Üçüncü bölümde ise CSE-CIC-IDS2018 veri kümesine ait ayrıntılı bilgiler verilmiş olup, dördüncü bölümde ise çalışma kapsamında önerilen iki seviyeli hibrit model detaylandırılarak ve elde edilen sonuçlar analiz edilmiştir. Son bölümde elde edilen sonuçlar değerlendirilerek ileride yapılması planlanan çalışmalardan bahsedilmiştir.

2. İLGİLİ ÇALIŞMALAR *(RELATED STUDIES)*

Wankhede ve Kshirsagar 2018 yılındaki çalışmalarında [2], CICIDS2017 veri kümesindeki sadece belirli bir günde yapılan DoS saldırıları üzerinde Rastgele Orman ve Yapay Sinir Ağı (Artificial Neural Network-ANN) yöntemlerini kullanarak saldırı tespiti yapmışlardır. Bunun yanında, gözlem sayısının tespit başarısına etkisini incelemek için, eğitim verisinin %20-80 arasında gözlemi kullanılarak Rastgele Orman ve Çok Katmanlı Algılayıcı (Multi Layer Perceptron-MLP) algoritmalarının başarımları karşılaştırılmıştır. Rastgele Orman yönteminin %99.95 doğruluk oranı ile daha başarılı olduğu ve Rastgele Orman yöntemi için %50, MLP yöntemi için %30 gözlem oranının en iyi (optimal) olduğu görülmüştür.

Sharafaldin ve arkadaşları 2018 yılındaki çalışmalarında [1], ağ trafiği dinlenmesi ve saldırı tespiti için oluşturulan veri kümelerindeki saldırı çeşitliliği yetersizliğinden dolayı CICIDS2017 veri kümesini oluşturmuşlardır. Bu veri kümesi üzerinde k En Yakın Komşu (k Nearest Neighbor-k-NN), Rastgele Orman, Tekrarlı İkilikçi Ağacı (Iterative Dichotomiser 3-ID3), Adaboost, MLP, Naive Bayes ve Karesel Diskriminant Analizi (Quadratic Discriminant Analysis-QDA) yöntemleri saldırı tespiti amaçlı kullanılmıştır. 0.98 F-skoru ile ID3 algoritması en iyi sonucu vermiştir.

Aksu ve Aydın 2018 yılındaki çalışmalarında [3], MLP ve Destek Vektör Makinesi (Support Vector Machine-SVM) yöntemlerini kullanarak CICIDS2017 veri kümesi üzerinde port tarama saldırılarını tespit etmişlerdir. Veri kümesi üzerindeki yalnızca port tarama saldırıları üzerinde MLP ile 0.65, SVM ile 0.95 F-skoru ile saldırı tespiti yapılmış ve 7 katmanlı MLP modeli ile daha başarılı saldırı tespiti yapıldığı gösterilmiştir.

Kanimozhi ve Jacob 2019 yılındaki çalışmalarında [4], CSE-CIC-IDS2018 (CIC-AWS-2018) veri kümesindeki Botnet (Bot) saldırılarını MLP yöntemini kullanarak tespit etmişlerdir. Bunun yanında varsayılan hiperparametreler ile aşırı uyum (overfitting) durumuna düşen model üzerinde GridSearch yöntemi ile hiperparametre optimizasyonu yapmışlardır. Önerilen yöntem ile Botnet saldırıları %99.97 doğruluk oranı ile sınıflandırılmıştır.

Zhou ve Pezaros 2019 yılındaki çalışmalarında [5], CSE-CIC-IDS2018 veri kümesi üzerinde eğitilen bir modelin, hiç görmediği tipteki saldırılar (Zero-Day)

üzerindeki başarısını incelemişlerdir. 6 farklı makine öğrenmesi yöntemi (Rastgele Orman, Gaussian Naive Bayes, Karar Ağacı, MLP, kNN, QDA) 10-Katlamalı Çapraz Doğrulama (10-Fold Cross Validation) ile bu veri kümesi üzerinde saldırı tespit amaçlı denenmiştir. Denemeler her bir saldırı tipi için normal trafik ile ikili karşılaştırılarak yapılmış ve en başarılı yöntemin Karar Ağacı (Decision Tree) olduğu tespit edilmiştir. Daha sonra model, eğitim veri kümesi üzerinde Normal ve Saldırı olmak üzere etiketlenip eğitilerek, test veri kümesi için 1 haftalık normal trafik ve 6 farklı yeni saldırı trafiği (ZeroAccess, DDoS bot'a darkness, Google doc macadocs, Bitcoin miner, Drowor worm, Nuclear ransomware, False content injection, Ponmocup trojan) oluşturulmuştur. Karar ağacı yöntemi ile bu test kümesi üzerinde %96 doğruluk oranı ile saldırı tespiti yapılmıştır.

Yulianto ve arkadaşları 2019 yılındaki çalışmalarında [6], CICIDS2017 veri kümesi üzerinde AdaBoost algoritmasının performansını iyileştirmişlerdir. Saldırı türleri açısından dengesiz olan CICIDS2017 veri kümesi üzerinde Temel Bileşen Analizi (Principal Component Analysis-PCA), SMOTE ve Topluluk Öznitelik Seçimi (Ensemble Feature Selection-EFS) yöntemleri ile performans iyileştirmesi denenmiştir. Karşılaştırmalı sonuçlara göre, AdaBoost algoritmasının performansını 0.90 F-skoru ile en çok iyileştiren yöntemin, SMOTE ve EFS algoritmalarının birlikte kullanımı olduğu görülmüştür.

Ullah ve Mahmoud 2019 yılındaki çalışmalarında [7], Nesnelerin İnterneti (Internet of Things-IoT) ağlarında anormallik tespiti için CICIDS2017 ve UNSW-15 veri kümeleri üzerinde iki seviyeli (hibrit) bir model geliştirmişlerdir. Birinci seviyede Karar Ağacı yöntemi kullanılarak ikili sınıflandırma (Normal, Saldırı) yapılmış ve saldırı olarak sınıflandırılan paketler ikinci seviyeye sokulmuştur. İkinci seviyede aşırı örnekleme (oversampling) ve alt örnekleme (undersampling) yöntemleri olan Yinelemeli Öznitelik Elemesi (Recursive Feature Elimination-RFE), SMOTE ve Düzenlenmiş En Yakın Komşu (Edited Nearest Neighbors-ENN) kullanılarak öznitelik elemesi yapılmıştır. CICIDS2017 veri kümesi için ilk ve ikinci seviyede 1.0 F-skoru (ağırlıklı ortalama F-skor); UNSW-15 için ilk seviyede 0.99, ikinci seviyede 0.97 F-skoru (ağırlıklı ortalama F-skor) ile saldırı tespiti yapılmıştır.

Wani ve arkadaşları 2019 yılındaki çalışmalarında [8] SVM, Rastgele Orman ve Naive Bayes yöntemlerini kullanarak Bulut Bilişim Ortamı üzerinde DDoS saldırıları tespiti yapmışlardır. Çalışmada oluşturulan veri kümesi üzerinde 9 öznitelik kullanılarak en başarılı sonuç 0.998 F-skoru ile SVM algoritmasından alınmıştır.

Yang ve arkadaşları 2019 yılındaki çalışmalarında [9], NSL-KDD ve UNSW-NB15 veri kümeleri üzerinde Düzenlenmiş Yoğunluk Zirve Kümelemesi Algoritması (Modified Density Peak Clustering Algorithm-MDPCA) ve Derin İnanç Ağlarını (Deep Belief Network-DBN) kullanarak etkili bir saldırı tespit sistemi oluşturmayı amaçlamışlardır. Boyut azaltımı için eğitim kümesi üzerinde, MDPCA yöntemi ile benzer özelliklere sahip alt kümeler oluşturularak, DBN modeli bu örneklerle eğitilmiştir. Bunun yanında kNN, Multinomial Naive Bayes (MNB), Rastgele Orman, SVM, Yapay Sinir Ağı (Artificial Neural Network-ANN), DBN, Deep Neural Networks (DNN), Spektral Kümeleme ve Derin Sinir Ağları Topluluk Algoritması (Spectral Clustering and Deep Neural Network Ensemble Algorithm-SCDNN), Kendi Kendine Öğrenme Tekniği (Self-taught Learning Technique-STL) Tekrarlayan Sinir Ağları (Recurrent Neural Networks-RNN), Çok Sınıflı Kademeli Yapay Sinir Ağı (Multiclass Cascade of Artificial Neural Network-CASCADE-ANN), Beklenti Maksimizasyonu Kümelemesi (Expectation Maximization Clustering-EM Clustering) ve Karar Ağacı yöntemleri de denenmiştir. İki veri kümesi üzerinde de önerilen MDPCA-DBN yönteminin en iyi sonucu verdiği görülmüştür.

Yılmaz ve Şen 2019 yılındaki çalışmalarında [10] ISOT ve CICIDS2017 veri kümeleri üzerinde Dilbilgisel Gelişim (Grammatical Evolution-GE) algoritmasını kullanarak erken botnet tespitini amaçlamışlardır. Önerilen yöntemde GE modeli, bu veri kümeleri içindeki botnet ve normal trafik ile eğitilmiştir. Gerçek zamanlı veriden farklı boyutta pencereler ile trafik akışı elde edilmiş ve bu akışlar önerilen model ile sınıflandırılmıştır. Önerilen yöntemle literatürdeki diğer çalışmalara kıyasla ISOT veri kümesi üzerinde en iyi doğruluk oranı sağlanmıştır.

McKay ve arkadaşları 2019 yılındaki çalışmalarında [11], CICIDS2017 veri kümesi üzerinde Rastgele Orman, OneR, kNN, J48, MLP ve Naive-Bayes yöntemlerini kullanarak botnet saldırı tespitini amaçlamışlardır. Çalışmada veri kümesi dengeli ve normal (orijinal oranı koruyarak) olarak iki farklı şekilde bölünmüş ve dengeli veri kümesi ile eğitilen tüm yöntemlerin daha iyi sonuç verdiği

gözlenmiştir. Bunun yanında %98,73 doğruluk oranıyla en iyi sonuç J48 ile elde edilmiştir.

Ferrag ve Maglaras 2019 yılındaki çalışmalarında [12], Drone taşıma servisleri için Blokchain tabanlı bir taşıma sistemi sunmuşlardır. Bunun yanında güvenlik için bir de saldırı tespit yöntemi geliştirmişlerdir. CSE-CIC-IDS2018 veri kümesi üzerinde SVM, RNN, CNN ve Rastgele Orman yöntemlerini Brute-Force, Web, DoS, DDoS, Botnet ve Infilteration saldırılarını tespit etmek için uygulamışlardır. Sırasıyla elde ettikleri en yüksek doğruluk oranı değerleri %92.19, %96.12, %96.18, %98.55, %98.71 ve %96.23 tür.

Lin ve arkadaşları 2019 yılındaki çalışmalarında [13], CSE-CIC-IDS2018 veri kümesi üzerinde 7 temel sınıflı saldırı tespiti gerçekleştirmişlerdir. Model, Uzun Kısa Süreli Hafıza (Long Short Term Memory-LSTM) yöntemi ile gerçeklenmiş ve Attention Mechanism (AM) yöntemi ile daha iyi performans amaçlanmıştır. Web ve Infilteration ataklarının tespit başarısızlığı görülmüş ve dengesizlik probleminin çözülmesi için bu sınıflar üzerinde SMOTE yöntemi kullanılmıştır. Ayrıca normal trafik rastgele altörneklenmiş ve yalnızca 2 milyon örnek bırakılmıştır. Saldırı tespitinin başarımını değerlendirmek için doğruluk oranı, precision, recall ve f-skor değerleri verilmiştir. Ancak çalışmada verilen precision, recall ve f-skor değerleri birbirleri ile çelişmektedir. Örn. 0.93 precision ve 0.17 recall sonuçları alınan bir sınıf için 0.93 f-skor değeri elde edildiği iddaa edilmiştir.

Filho ve arkadaşları 2019 yılındaki çalışmalarında [14], CIC-DOS, CICIDS2017, CSE-CIC-IDS2018 ve kendi geliştirdikleri veri kümeleri üzerinde Rastgele Orman yöntemi ile DoS saldırı tespiti yapmayı amaçlamışlardır. Veri kümeleri için sırasıyla 0.999, 0.992, 1.000 ve 0.995 F-skor değerleri elde edilmiştir.

Kanimozhi ve Jacob 2019 yılındaki çalışmalarında [15], CSE-CIC-IDS2018 veri kümesi üzerinde kNN, Naive Bayes, SVM, Rastgele Orman, AdaBoost ve MLP yöntemlerini kullanarak botnet saldırı tespiti gerçekleştirmişlerdir. Ayrıca yöntemlerin kalibrasyon eğrileri üzerinden performansları değerlendirilmiştir. kNN, Naive Bayes, SVM, Rastgele Orman, AdaBoost ve MLP yöntemleri için elde edilen F-skor değerleri sırasıyla; 0.9984, 0.9953, 0.9994, 0.9992, 0,9992 ve 0,9998`dir. F-skor değeriyle doğru orantılı olarak, kalibrasyon eğrisi mükemmel eğriye en yakın olan yöntemin de MLP olduğu verilmiştir.

Literatürdeki yapılan çalışmalar incelendiğinde, CSE-CIC-IDS2018 veri kümesini kullanan altı farklı çalışmaya [4,5,12,13,14,15] rastlanmıştır. [4, 15]'te verilen çalışmalarda sadece Botnet saldırıları tespit edilmiş ancak diğer saldırı türleri ele alınmamıştır. [5]'te verilen çalışmada ise CSE-CIC-IDS2018 veri kümesi üzerinde en iyi makine öğrenmesi yöntemini bulmak için, saldırılar tek tek normal trafik ile karşılaştırılmış ancak saldırı tiplerinin birbirleriyle karşılaştırması yapılmamıştır, ilgili çalışmada sadece Zero-Day saldırılarının tespiti amaçlanmıştır. [12]'de verilen çalışmada ise sınıf sayısı 7'ye indirerek çoklu sınıflandırma yapılmıştır yalnızca doğruluk oranı sonuçları paylaşılmıştır. Ancak doğruluk oranı CSE-CIC-IDS2018 gibi dengesiz bir veri kümesinde yanıltıcı bir metriktir, bu metriğe ek olarak diğer metriklerin de, özellikle F-skor değerinin verilmesi uygundur. [13]'te verilen çalışmada 7 temel sınıf üzerinde tespit yapılmış, precision, recall ve F-skor değerleri verilmiştir. Ancak verilen bilgiler birbirleri ile çelişmektedir, çalışma tutarsızdır. [14]'te verilen çalışmada yalnızca DoS saldırılarının tespiti yapılmış ve diğer saldırı türleri ele alınmamıştır. Bu çalışmada ise CSE-CIC-IDS2018 veri kümesi üzerindeki tüm saldırıların tespiti için en iyi başarımı gösteren iki seviyeli hibrit bir model önerilmiştir. Çalışma bu yönüyle özgün olup, bu verisetini kullanan diğer çalışmalarda önerilen yöntemlerden farklıdır.

3. VERİ KÜMESİ ÖZELLİKLERİ *(DATA SET SPECIFICATIONS)*

Çalışmada kullanılan veri kümesi CSE-CIC-IDS2018, CICIDS2017 veri kümesinin güncellenmiş halidir ve bilinen en yeni saldırı trafiği veri kümesidir. Bu veri kümesi Kanada Siber Güvenlik Enstitüsü (CIC) ve İletişim Güvenliği Kurumu (CSE) tarafından Amazon AWS LAN ağı üzerinde toplanarak oluşturulmuştur.

Veri kümesinde BruteForce (Web, XSS, FTP, SSH), Botnet, DoS (Hulk, SlowHTTPTest, GoldenEye, Slowloris), DDoS (HOIC, LOIC-UDP, LOIC-HTTP), Web Saldırıları (SQL Injection) ve Ağa içeriden sızma (Infilteration) olmak üzere 6 tipte 14 farklı saldırı türü (2,746,934 tane gözlem) vardır. CICFlowMeter-V3 [16] kullanılarak elde edilen paketler ağ trafik akışlarına dönüştürülmüş ve 80 öznitelik sunulmuştur. Saldırı tipleri ve bu saldırılara ait gözlem sayılarının dağılımı Tablo 1'de verilmiştir.

Tablo 1. Veri Kümesindeki Gözlem Sayıları

Saldırı Türü	Gözlem Sayısı
Normal	13390249
Bot	286191
Brute Force Web	611
Brute Force XSS	230
DDOS HOIC	686012
DDOS LOIC UDP	1730
DDoS LOIC HTTP	576191
DoS GoldenEye	41508
DoS Hulk	461912
DoS SlowHTTPTest	139890
DoS Slowloris	10990
FTP BruteForce	193354
Infilteration	160639
SQL Injection	87
SSH Bruteforce	187589

Tablodan da görüleceği gibi veri kümesinde yer alan saldırı tiplerinin gözlem sayılarının dağılımı dengesizdir. Veri kümesi içerisindeki Infilteration saldırısı, diğer saldırıların aksine ağa içeriden sızma yolunu izlediğinden normal trafik ile çok benzerlik göstermektedir. Bu sızma işlemi genellikle kurbana gönderilen zararlı yazılım içeren bir e-posta ile veya Adobe Acrobat Reader gibi hassas yazılımların zaaflarından faydalanarak kurban bilgisayarda Nmap ve portscan gibi araçları kullanmayı sağlayacak bir arka kapı yaratarak uygulanır. Bu çalışmada ve literatürde var olan çalışmalarda Infilteration saldırısının başarı ile tespit edildiği görülmemiştir. Infilteration saldırı tipinin makine öğrenmesi ve derin öğrenme metodları ile tespit edilmesinin zorluğu gösterilmiştir.

4. ÖNERİLEN YÖNTEM VE DENEYSEL SONUÇLAR *(RECOMMENDED METHODS AND EXPERIMENTAL RESULTS)*

Çalışmada saldırı tespiti için kullanılan modellere ait kapsamlı bilgiler aşağıda verilmiştir. Çalışma kapsamında veri önişleme adımından sonra önerilen yöntem tek seviyeli ve iki seviyeli olarak ele alınmıştır. İki seviyeden kasıt, test kümesindeki verilerin ardışık olarak iki farklı modele sokulmasıdır. İlk seviyede gözlemin saldırı olup olmadığı (ikili sınıflandırma) tespit edilir, ikinci seviyede ise ilk seviyede saldırı olarak nitelenen gözlemlerin saldırı türü belirlenir. Böylece oluşan hibrit modelin genel başarımı arttırması beklenmektedir.

4.1. Veri Önişleme *(Data Preprocessing)*

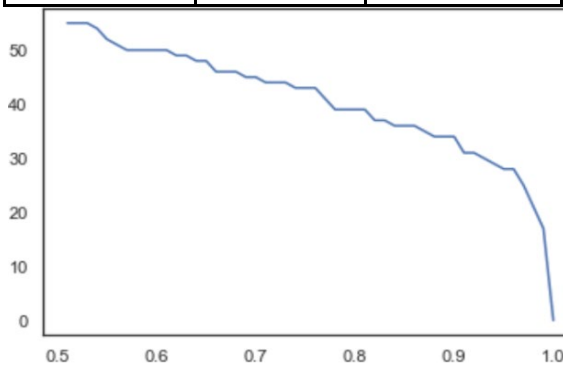
Paylaşılan veri kümesinde CICFlowMeter-V3 ile öznitelikler çıkarılmış ve Flow ID, Source IP, Source Port ve Destination IP öznitelikleri veri kümesinden atılmıştır. Ayrıca, bir saldırıda, saldırı zamanı önemsiz ve ilgisiz olduğundan, saldırı zamanının saldırı durumu veya tipi ile herhangi bir ilişkisi olmadığından Timestamp özniteliği veri kümesinden atılmıştır. Eksik bilgi içeren Flow Byts/s ve Flow Pkts/s öznitelik değerleri medyanları ile doldurulmuştur. Standart sapması 0 olan Bwd PSH Flags, Bwd URG Flags, Fwd Byts/b Avg, Fwd Pkts/b Avg, Fwd Blk Rate Avg, Bwd Byts/b Avg, Bwd Pkts/b Avg ve Bwd Blk Rate Avg öznitelikleri saldırı tespiti için gereksiz ve etkisiz olduğundan veri kümesinden atılmıştır. Ayrıca sonsuz değer içeren gözlem değerleri veri kümesinden kaldırılmıştır. Veri kümesinin %25'i (4,034,296 gözlem) test verisi olarak, kalan %75'i ise (12,102,887 gözlem) eğitim verisi olarak ayrıldıktan sonra eğitim süresini kısaltmak, eğitim kümesini daha dengeli hale getirmek ve normal trafik gözlem sayısını 500,000'e indirmek için yaklaşık 9,5 milyon normal trafik gözlemi yalnızca eğitim kümesi içinden rastgele atılmıştır. Sonuç olarak Tablo 2'de görüleceği üzere, eğitim kümesi 2,560,176 ve test kümesi 4,034,296 gözlemden oluşmaktadır. Eğitim kümesindeki normal trafik gözlem sayısının 500,000'e indirilmesinin sebebi; normal trafik gözlem sayısının veri kümesinde en çok rastlanan DDOS HOIC (514,590 gözlem) saldırısının seviyesine çekilmek istenmesidir.

Standart sapması sıfır olan öznitelikler atıldığında kalan 70 öznitelik ile yapılan eğitimlerin sürelerini azaltmak için birbirleri ile korelasyonu yüksek olan öznitelikler tespit edilmiştir. Atılacak öznitelikleri belirleyecek korelasyon eşik değerinin dirsek yöntemi (elbow method) uygulanarak 0.9-1.00 arasında olduğu tespit edilmiştir. Bu yönteme ait elde edilen korelasyon eşik değeri-atılacak öznitelik sayısı grafiği Şekil 1'de verilmiştir. Şekil 2'de, Şekil 1'de tespit edilen değer aralığının grafiği verilmiş olup 0.96 korelasyon eşik değeri olarak belirlenmiştir. 0.96 eşik

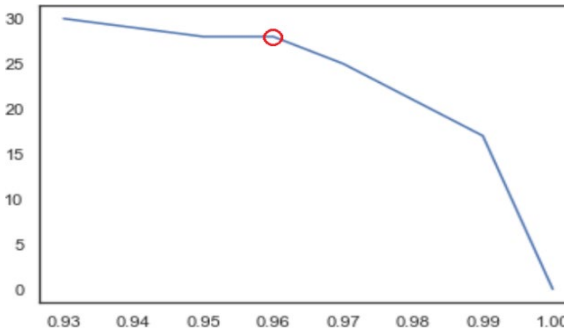
değerinde yüksek korelasyona sahip özniteliklerin atıldığı veri kümesi yalnızca tek seviyeli yöntemdeki LGBM modeli için başarımı arttırdığından sadece bu modelde uygulanmıştır.

Tablo 2. Eğitim ve Test Kümesindeki Gözlem Sayıları

Saldırı Türü	Eğitim Kümesi Gözlem Sayısı	Test Kümesi Gözlem Sayısı
Normal	500000	3347538
Bot	214555	71636
Brute Force Web	454	157
Brute Force XSS	180	50
DDOS HOIC	514590	171422
DDOS LOIC UDP	1308	422
DDoS LOIC HTTP	431871	144320
DoS GoldenEye	31042	10466
DoS Hulk	346618	115294
DoS SlowHTTPTest	104927	34963
DoS Slowloris	8264	2726
FTP BruteForce	144998	48356
Infilteration	120659	39980
SQL Injection	68	19
SSH Bruteforce	140642	46947
Toplam	**2560176**	**4034296**



Şekil 1. Korelasyon eşik değeri-atılacak öznitelik sayısı grafiği



Şekil 2. Dirsek yöntemine göre belirlenen korelasyon eşik değeri

4.2. Smote

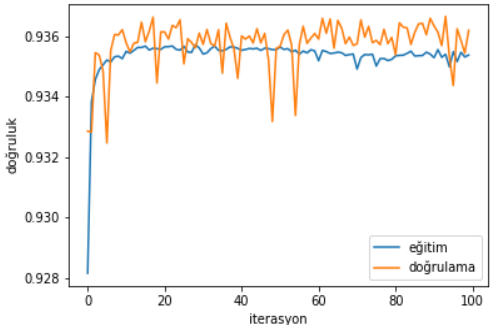
Veri kümesindeki dengesizliği aşmak için SMOTE yöntemi denenmiştir. Rastgele Orman ve LGBM yöntemlerinin SMOTE kullanılarak ve kullanılmadan elde edilmiş F-skor sonuçları Tablo 3'te verilmiştir. Tabloda elde edilen sonuçlar ele alındığında, Rastgele Orman yöntemi için sadece Brute Force Web, Brute Force XSS saldırılarının başarım oranının sırasıyla 0.03 ve 0.06 arttığı gözlemlenmiştir, diğer saldırı tipleri için değişim gözlenmemiştir. LGBM için, Brute Force Web, Brute Force XSS, DDOS LOIC UDP, DDoS LOIC HTTP, DoS GoldenEye, DoS SlowHTTPTest ve DoS Slowloris saldırılarının başarım oranlarının sırasıyla 0.03, 0.17, 0.15, 0.01, 0.03, 0.01, 0.14 arttığı, normal trafik ve Infilteration saldırısının başarım oranlarının ise sırasıyla 0.14 ve 0.19 azaldığı görülmüştür. Bu nedenle çalışma kapsamında SMOTE yönteminin sonuçlara olan zayıf etkisi ele alındığında, saldırı tespiti için etkili bir yöntem olmadığı görülmüştür. Bu nedenle SMOTE yöntemi kullanılmamıştır.

Tablo 3. Rastgele Orman ve LGBM Algoritmaları Üzerinde SMOTE Etkisi

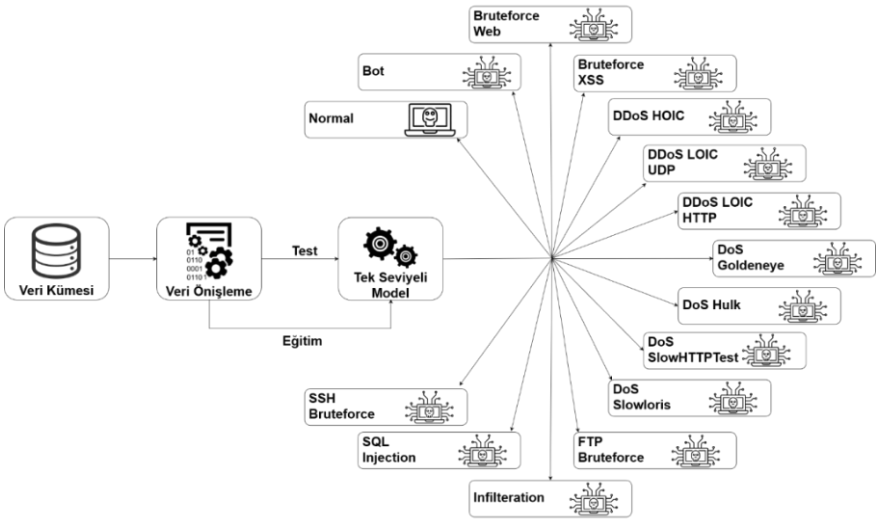
Saldırı Türü / Yöntem (F-skor)	Rastgele Orman	Rastgele Orman SMOTE	LGBM	LGBM SMOTE
Normal	0.97	0.97	**0.99**	0.85
Bot	1.00	1.00	1.00	1.00
Brute Force Web	0.44	**0.47**	0.04	**0.07**
Brute Force XSS	0.81	**0.87**	0.10	**0.27**
DDoS HOIC	1.00	1.00	1.00	1.00
DDoS LOIC UDP	0.91	0.91	0.73	**0.88**
DDoS LOIC HTTP	1.00	1.00	0.99	**1.00**
DoS GoldenEye	1.00	1.00	0.97	**1.00**
DoS Hulk	1.00	1.00	1.00	1.00
DoS SlowHTTPTest	0.61	0.61	0.61	**0.62**
DoS Slowloris	1.00	1.00	0.82	**0.96**
FTP BruteForce	0.79	0.79	0.79	0.79
Infilteration	0.16	0.16	**0.25**	0.06
SQL Injection	0.67	0.67	0.00	**0.12**
SSH Bruteforce	1.00	1.00	1.00	1.00

4.3. Tek Seviyeli Yöntem *(One Level Method)*

Tek seviyeli yöntemde saldırı tespiti için LGBM, CNN ve Rastgele Orman algoritmaları saldırı türlerinin çoklu sınıflandırılması için ayrı ayrı denenmiştir. Yöntem mimarisi Şekil 3'te ayrıntılı verilmiştir. Veri önişleme adımından sonra model eğitilerek test verileriyle test edilir. LGBM yöntemi için 'boosting_type' hiperparametresi 'dart' olarak seçilmiştir ve korelasyonu 0.96 eşik değerinden yüksek olan öznitelikler atılarak eğitim yapılmıştır. CNN yöntemi için 2 tane bir boyutlu evrişimsel katman, 2x2 filtreli havuzlama (Pooling) katmanı, düzleştirme (Flatten) katmanı, 'relu' aktivasyon fonksiyonlu ve %10 Dropout değeri olan 512 nöronlu 2 tane tam bağlantılı katman ve 15 nöronlu, aktivasyon fonksiyonu softmax olan çıkış katmanı içeren bir ağ kullanılmıştır. 100 iterasyon ile eğitilen modelin iterasyon-doğruluk oranı grafiği Şekil 4'te verilmiştir.



Şekil 4. Tek seviyeli CNN için iterasyon-doğruluk grafiğ



Şekil 3. Tek seviyeli yöntemin mimarisi

Rastgele Orman yönteminin hiperparametre seçimi ve optimizasyonu 3-fold Cross Validation ile GridSearch yöntemi ile yapılmıştır. Test edilen hiperparametreler aşağıda verilmiştir.

- max_features = 'sqrt', 02, 0.3, 0.4, 0.5, 0.6
- min_samples_split = 2:5 (2,3,4,5), 6:10, 15, 17, 30, 45, 70, 100, 200
- min_samples_leaf = 1, 2, 3, 4, 8
- n_estimators = 20, 40, 80

Test edilen hiperparametreler içinden max_features için 0.4, min_samples_split için 5, min_samples_leaf için 1 ve n_estimators için 80 değerleri en iyi sonuçlar elde edildiği için seçilmiştir. Cross Validation sonuçları Tablo 4'te verilmiştir.

Tablo 4. Cross Validation Sonuçları

Değerlendirme Ölçütü	F-skor Macro Ortalaması
Fold-1	0.8832
Fold 2	0.8794
Fold 3	0.8840
Ortalama	**0.8822**

4.4. İki Seviyeli Yöntem *(Two Level Method)*

İki seviyeli yöntemin genel yapısı Şekil 5'te verilmiştir. Şekilde de görüldüğü gibi, bu yöntemde model iki aşamadan oluşmaktadır. İlk seviyede veri kümesi üzerinde saldırı olup olmadığının tespiti için Rastgele Orman, LGBM ve CNN yöntemleri ayrı ayrı kullanılarak ikili sınıflandırma yapılmıştır. İkinci seviyede ise, ilk seviyede saldırı olarak tespit edilen gözlemler ikinci seviyede Rastgele Orman modeli için test verisi olarak kullanılmıştır. Eğitim için ise, Seviye 1 ikili etiketlemeden sonra eğitilirken Seviye 2 veri önişlemeden hemen sonra eğitilir. Seviye 1 ve Seviye 2 için ayrıntılı bilgiler aşağıdaki alt başlıklarda verilmiştir.

4.4.1. Seviye 1 *(Level 1)*

İlk seviyede veri kümesi, saldırı ve normal trafik olmak üzere ikili etiketlenmiştir. Etiketlenmiş veri üzerinde Rastgele Orman, LGBM ve CNN yöntemleri denenmiştir. Bu seviyenin kullanılmasındaki amaç, veri kümesinde yoğun olarak gözlenen normal trafiği filtrelemektir. CNN modelindeki ağın yapısı tek seviyeli CNN modelindeki ağın yapısı ile aynıdır. LGBM modeli için tek seviyeli modelden farklı olarak, korelasyonu 0.96 eşik değerinin üzerinde olan öznitelikler kaldırılmamıştır. Rastgele Orman modelinde max_features için 0.2, min_samples_split için 75, min_samples_leaf için 1 ve n_estimators için 80 değerleri kullanılmıştır.

Tablo 5'te uygulanan yöntemler ve başarımları verilmiştir. Tablo'da elde edilen sonuçlar değerlendirildiğinde F-skor değerleri birbirine yakın çıktığından, tüm modellerden elde edilen çıktılar Seviye 2'nin girdisi olarak kullanılmıştır.

Tablo 5. Seviye 1 Başarımları

Değerlendirme Ölçütü	LGBM	Rastgele Orman	CNN
F-skor	0.95	0.94	0.95
Doğruluk Oranı	0.98	0.98	0.98

4.4.2. Seviye 2 *(Level 2)*

Seviye 1'de saldırı olarak tespit edilen gözlemler, Seviye 2'de Rastgele Orman yöntemi ile sınıflandırılmıştır. Seviye 2'deki Rastgele Orman modeli için tek seviyeli modelde kullanılan hiperparametrelerin aynıları kullanılmıştır. Seviye 1'de kullanılan modellerin tahminleri ile Rastgele Orman modeli (Seviye 2) test edilir. İki Seviyeli model için elde edilen sonuçlar incelendiğinde, Seviye 1 için CNN modelinin kullanılması ve sonrasında Rastgele Orman algoritması ile sınıflandırma yapılmasının (CNN + Rastgele Orman) başarımı arttırdığı görülmüştür.

Seviye 2 için eğitim yaklaşımları ele alındığında; İki Seviyeli modelde Seviye 1'de tüm veri kümesi ile eğitim yapılırken Seviye 2'deki modelin eğitimi için ise iki yaklaşım uygulanabilir. Bu yaklaşımlardan ilki, tüm veri kümesi ile eğitim, diğeri ise normal trafik içermeyen (sadece saldırıların yer aldığı) veri kümesi ile eğitimdir.

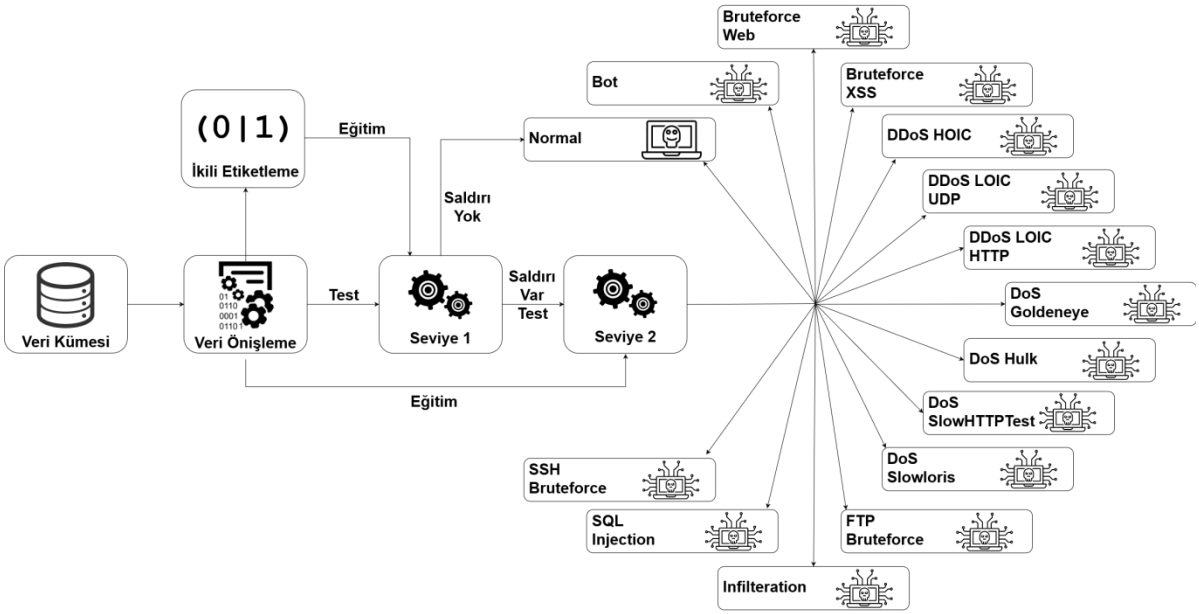
Çalışmada Seviye 2'de her iki yaklaşım da denenmiştir. Her iki yaklaşımın da avantaj ve dezavantajları vardır. Tüm veri kümesi ile eğitim yaklaşımının avantajı, Seviye 1'in, saldırı olarak yanlış nitelendirdiği (False Positive) gözlemler için, Seviye 2'de bu hatanın düzeltilme (True Negative) ihtimalidir. Dezavantajı ise Seviye 1'in saldırı olarak

doğru nitelendirdiği (True Positive) gözlemleri normal trafik olarak yanlış niteleme (False Negative) ihtimalidir. Sadece saldırı kümesi ile eğitim yaklaşımının avantajı, eğitim sırasında normal trafiği görmediği için, Seviye 1'in saldırı olarak doğru nitelendirdiği (True Positive) gözlemleri normal trafik ile karıştırmamasıdır. Dezavantajı ise Seviye 1'in, saldırı olarak yanlış nitelendirdiği (False Positive) gözlemlerin düzeltilmemesidir.

İki yaklaşım arasında seçim yapmak için her bir modelin (Rastgele Orman + Rastgele Orman, LGBM + Rastgele Orman ve CNN + Rastgele Orman) Seviye 2'deki eğitimi için iki yaklaşım da denenmiştir. Çalışma kapsamında önerilen iki seviyeli hibrit model için elde edilen sonuçlar analiz edildiğinde Seviye 2'de tüm veri kümesi ile eğitim yaklaşımının kullanılmasının her üç model için de daha başarılı olduğu görülmüştür. Tablo 6'da Rastgele Orman + Rastgele Orman modeli için her iki yaklaşımın F-skor sonuçları ayrı ayrı verilmiştir. Sadece bu modelin verilmesinin nedeni iki yaklaşım arasındaki macro F-skor farkının en yüksek olmasıdır. Tablo incelendiğinde, özellikle Brute Force XSS ve SQL Injection saldırı türleri için tüm veri kümesi ile eğitim yaklaşımının başarısı açıktır.

Eğitim verisinin tümünün kullanımı daha iyi sonuç verdiğinden önerilen hibrit model için Seviye 2'de tüm veri kümesi ile eğitim yapılmıştır.

Elde edilen deneysel sonuçların tümü analiz edildiğinde saldırı tespitinde kullanılacak hibrit modeller için (CNN + Rastgele Orman) yönteminin birinci yaklaşım ile birlikte kullanımı en yüksek başarımı elde etmiştir. Infilteration saldırılarının tespit başarısının düşük olduğu tespit edilmiş ve ağ üzerinde normal trafik ile en çok benzerlik gösteren saldırı olduğu görülmüştür.



Şekil 5. İki Seviyeli Hibrit Yöntemin Mimarisi

Tablo 6. İki Seviyeli Yöntem İçin Eğitim Yaklaşım Seçimi Sonuçları

Saldırı Türü / Yaklaşım (F-skor)	Tüm Veri Kümesi İle Eğitim	Yalnız Saldırı Kümesi İle Eğitim
Normal	0.99	0.99
Bot	1.00	1.00
Brute Force Web	**0.47**	0.41
Brute Force XSS	**0.91**	0.47
DDOS HOIC	1.00	1.00
DDOS LOIC UDP	0.92	0.92
DDoS LOIC HTTP	1.00	1.00
DoS GoldenEye	1.00	1.00
DoS Hulk	1.00	1.00
DoS SlowHTTPTest	0.61	0.61
DoS Slowloris	1.00	1.00
FTP BruteForce	0.79	0.79
Infilteration	**0.29**	0.28
SQL Injection	**0.81**	0.14
SSH Bruteforce	1.00	1.00
Macro Ortalama	**0.85**	0.77
Doğruluk Oranı	**0.97**	0.97

Yöntemlerin performans karşılaştırmaları için F-skor, precision ve recall değerleri sırasıyla Tablo 7, Tablo 8 ve Tablo 9'da verilmiştir. Tablo 7'de, Tek Seviyeli yöntem için elde edilen sonuçlar incelendiğinde, LGBM ve CNN sınıflandırma algoritmalarının doğruluk oranı yüksek olsa da saldırı tespiti başarısının düşük olduğu görülmüştür. Normal trafiği iyi sınıflandıran bu modeller veri kümesinin normal trafik ağırlıklı (veri kümesinin %83'ü) olmasından dolayı yüksek doğruluk oranına ulaşmıştır. CSE-CIC-IDS 2018 gibi dengesiz veri kümelerinde F-skor başarımı daha doğru bir ölçüm vermektedir. Bunun yanında modelin genel performansını vermek için en uygun ortalama yöntemi 'macro' ortalamadır. Macro ortalama, gözlem sayılarından bağımsız, ağırlıksız bir ortalama alma yöntemidir. Tüm sınıfların tespit başarısının eşit önemde olduğu durumlarda kullanılır.Tablo 8 ve 9 incelendiğinde iki seviyeli hibrit modelin genel olarak precision değerlerini iyileştirdiği gözlemlenmiştir. Recall değerleri tek seviyeli Rastgele Orman modeli ile en iyi sonucu vermiştir. Ancak precision ve recall metrikleri tek başlarına değerlendirme için yeterli metrikler değildir. Precision, False Negative (Tip 2 hata) değerini, Recall ise False Negative (Tip 1 hata) değerini dikkate almaz. Bu yüzden Tablo 7'de değerleri verilen f-skor metriği en anlamlı ölçüm yöntemidir. Tablo 7 incelendiğinde iki seviyeli hibrit modellerin genel olarak performansı arttırdığı ve CNN + Rastgele Orman yönteminin aralarında en iyi sonucu verdiği görülmüştür. Infilteration saldırısı denenen 6 yöntemin hiçbirinde başarı ile tespit edilememiştir.

Tablo 7. Tek Seviyeli ve İki Seviyeli Yöntemlerin F-skor Değerleri Açısından Karşılaştırılması

Saldırı Türü	**Tek Seviyeli Yöntem**			**İki Seviyeli Yöntem**		
	LGBM (F-skor)	**Rastgele Orman (F-skor)**	**CNN (F-skor)**	**(LGBM + Rastgele Orman) (F-skor)**	**(Rastgele Orman + Rastgele Orman) (F-skor)**	**(CNN + Rastgele Orman) (F-skor)**
Normal	**0.99**	0.97	**0.99**	**0.99**	**0.99**	**0.99**
Bot	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
Brute Force Web	0.04	0.52	0.61	0.73	0.47	**0.76**
Brute Force XSS	0.10	**0.93**	0.61	0.92	0.91	0.92
DDOS HOIC	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
DDOS LOIC UDP	0.73	**0.92**	0.82	**0.92**	**0.92**	**0.92**
DDoS LOIC HTTP	0.99	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
DoS GoldenEye	0.97	**1.00**	0.99	**1.00**	**1.00**	**1.00**
DoS Hulk	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
DoS SlowHTTPTest	**0.61**	**0.61**	**0.61**	**0.61**	**0.61**	**0.61**
DoS Slowloris	0.82	**1.00**	0.96	0.99	**1.00**	**1.00**
FTP BruteForce	**0.79**	**0.79**	**0.79**	**0.79**	**0.79**	**0.79**
Infilteration	0.25	0.16	0.24	**0.30**	0.29	0.28
SQL Injection	0.00	**0.89**	0.39	0.67	0.81	0.59
SSH Bruteforce	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
Macro Ortalama	0.69	0.85	0.80	**0.86**	0.85	**0.86**
Doğruluk Oranı	0.97	0.94	**0.98**	**0.98**	0.97	**0.98**

Tablo 8. Tek Seviyeli ve İki Seviyeli Yöntemlerin Precision Değerleri Açısından Karşılaştırılması

Saldırı Türü	**Tek Seviyeli Yöntem**			**İki Seviyeli Yöntem**		
	LGBM (Precision)	**Rastgele Orman (Precision)**	**CNN (Precision)**	**(LGBM + Rastgele Orman) (Precision)**	**(Rastgele Orman + Rastgele Orman) (Precision)**	**(CNN + Rastgele Orman) (Precision)**
Normal	**0.99**	**0.99**	**0.99**	**0.99**	**0.99**	**0.99**
Bot	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
Brute Force Web	0.02	0.38	0.65	0.91	0.38	**0.92**
Brute Force XSS	0.05	0.94	0.83	0.94	**1.00**	0.96
DDOS HOIC	0.99	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
DDOS LOIC UDP	0.57	0.88	0.70	**0.90**	0.89	0.89
DDoS LOIC HTTP	0.98	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
DoS GoldenEye	0.95	**1.00**	0.99	**1.00**	**1.00**	**1.00**
DoS Hulk	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
DoS SlowHTTPTest	**0.77**	**0.77**	0.75	**0.77**	**0.77**	**0.77**
DoS Slowloris	0.71	**1.00**	0.93	**1.00**	**1.00**	**1.00**
FTP BruteForce	**0.72**	**0.72**	0.71	**0.72**	**0.72**	**0.72**
Infilteration	0.23	0.09	0.21	**0.30**	0.22	**0.30**
SQL Injection	0.00	0.94	0.41	0.71	**1.00**	**1.00**
SSH Bruteforce	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
Macro Ortalama	0.67	0.85	0.81	0.88	0.86	**0.90**

Tablo 9. Tek Seviyeli ve İki Seviyeli Yöntemlerin Recall Değerleri Açısından Karşılaştırılması

Saldırı Türü	**Tek Seviyeli Yöntem**			**İki Seviyeli Yöntem**		
	LGBM (Recall)	**Rastgele Orman (Recall)**	**CNN (Recall)**	**(LGBM + Rastgele Orman) (Recall)**	**(Rastgele Orman + Rastgele Orman) (Recall)**	**(CNN + Rastgele Orman) (Recall)**
Normal	0.98	0.94	**0.99**	**0.99**	0.98	**0.99**
Bot	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
Brute Force Web	0.50	**0.86**	0.57	0.61	0.64	0.65
Brute Force XSS	0.86	**0.92**	0.48	0.90	0.84	0.88
DDOS HOIC	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
DDOS LOIC UDP	**1.00**	0.95	0.98	0.95	0.95	0.95
DDoS LOIC HTTP	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
DoS GoldenEye	0.99	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
DoS Hulk	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
DoS SlowHTTPTest	0.51	0.51	**0.52**	0.51	0.51	0.51
DoS Slowloris	0.98	**1.00**	**1.00**	0.99	**1.00**	**1.00**
FTP BruteForce	**0.89**	**0.89**	0.87	**0.89**	**0.89**	**0.89**
Infilteration	0.28	**0.48**	0.28	0.29	0.40	0.27
SQL Injection	0.16	**0.84**	0.37	0.63	0.68	0.42
SSH Bruteforce	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**
Macro Ortalama	0.81	**0.89**	0.80	0.85	0.86	0.84

4. İLERİKİ ÇALIŞMALAR *(ADVANCED STUDIES)*

Bu çalışmada CSE-CIC-IDS2018 veri kümesi üzerinde saldırı tespit amaçlı, tek seviyeli model kullanılarak yanlış sınıflandırma kaynaklı düşen başarımın, iki seviyeli hibrit bir model kullanılarak arttırılabileceği önerilmiştir.

Saldırı tespit amacıyla LGBM, CNN ve Rastgele Orman yöntemleri denenmiş olup, ayrıca bu yöntemlerin ikili sınıflandırmasının ardından uygulanan çok sınıflı Rastgele Orman modeli ile iki seviyeli hibrit bir model oluşturulmuştur. Elde edilen deneysel sonuçlar analiz edildiğinde Seviye 1 ve Seviye 2 için sırasıyla CNN ve Rastgele Orman yöntemlerinin birlikte kullanıldığı İki Seviyeli yöntem, 0.86 F-skor macro ortalaması ile en yüksek başarıma sahiptir.

İleriki çalışmalarda, özellikle infilteration saldırı tespitinin başarımının arttırılması amaçlı, hibrit model üzerinde farklı makine öğrenmesi ve derin öğrenme yöntemlerinin denenmesi ve eş zamanlı saldırı tespiti yapan bir modelin geliştirilmesi planlanmaktadır.

KAYNAKLAR *(REFERENCES)*

[1] Iman Sharafaldin, Arash Habibi Lashkari, and Ali A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization”, *in ICISSP*, Prague, Czech Republic, 2018, pp. 108-116

[2] S. Wankhede and D. Kshirsagar, "DoS Attack Detection Using Machine Learning and Neural Network," *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, Pune, India, 2018, pp. 1-5. *Conference on Information Systems Security and Privacy (ICISSP)*, Portugal, January 2018.

[3] D. Aksu and M. Ali Aydin, "Detecting Port Scan Attempts with Comparative Analysis of Deep Learning and Support Vector Machine Algorithms," *2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT)*, Ankara, Turkey, 2018, pp. 77-80.

[4] V. Kanimozhi and T. P. Jacob, "Artificial Intelligence based Network Intrusion Detection with Hyper-Parameter Optimization Tuning on the Realistic Cyber Dataset CSE-CIC-IDS2018 using Cloud Computing," *2019 International Conference on Communication and Signal Processing (ICCSP)*, Chennai, India, 2019, pp. 33-36.

[5] Zhou, Qianru and Dimitrios Pezaros. “Evaluation of Machine Learning Classifiers for Zero-Day Intrusion Detection - An Analysis on CIC-AWS-2018 dataset.” *ArXiv* abs/1905.03685v1, 2019.

[6] Yulianto, Arif & Sukarno, Parman & Anggis Suwastika, Novian, “Improving AdaBoost-based Intrusion Detection System (IDS) Performance on CIC IDS 2017 Dataset,” *Journal of Physics: Conference Series*, 1192.

[7] I. Ullah and Q. H. Mahmoud, "A Two-Level Hybrid Model for Anomalous Activity Detection in IoT Networks," *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 2019, pp. 1-6.

[8] A. R. Wani, Q. P. Rana, U. Saxena and N. Pandey, "Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques," *2019 Amity International Conference on Artificial Intelligence (AICAI)*, Dubai, United Arab Emirates, 2019, pp. 870-875.

[9] Yang Y, Zheng K, Wu C, Niu X, Yang Y. “Building an Effective Intrusion Detection System Using the Modified Density Peak Clustering Algorithm and Deep Belief Networks,” *Applied Sciences*, 9(2):238, 2019, Doi: 10.3390/app9020238.

[10] Yılmaz, Selim & Sen, Sevil, “Early Detection of Botnet Activities Using Grammatical Evolution,” Theory and Applications of Models of Computation, pp.395-404, 2019.

[11] McKay, Rob & Pendleton, Brian & Britt, James & Nakhavanit, Ben, “Machine Learning Algorithms on Botnet Traffic: Ensemble and Simple Algorithms,” *The International Conference on Compute and Data Analysis 2019 (ICCDA),* 2019.

[12] Ferrag, M.A.; Maglaras, L. DeliveryCoin: An IDS and Blockchain-Based Delivery Framework for Drone-Delivered Services. *Computers* 2019, *8*, 58. 2019.

[13] Lin P., Ye K., Xu CZ. (2019) Dynamic Network Anomaly Detection System by Using Deep Learning Techniques. In: Da Silva D., Wang Q., Zhang LJ. (eds) Cloud Computing – CLOUD 2019. CLOUD 2019. Lecture Notes in Computer Science, vol 11513. *Springer*, Cham. 2019.

[14] Francisco Sales de Lima Filho, Frederico A. F. Silveira, Agostinho de Medeiros Brito Junior, Genoveva Vargas-Solar, and Luiz F. Silveira, “Smart

Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning," *Security and Communication Networks,* vol. 2019, Article ID 1574749, 15 pages, 2019.

[15] V. Kanimozhi, T. Prem Jacob. "Calibration of Various Optimized Machine Learning Classifiers in Network Intrusion Detection System on the Realistic Cyber Dataset CSE-CIC-IDS2018 Using Cloud Computing". International Journal of Engineering Applied Sciences and Technology, 2019 Vol. 4, Issue 6, ISSN No. 2455-2143, Pages 209-213, 2019.

[16] CICFlowMeter: Network Traffic Flow Analyzer,http://netflowmeter.ca/netflowmeter.html, Accessed 28 July 2018.

Remzi ATAY

Remzi Atay 2016 yılında Kocaeli Üniversitesi Bilgisayar Mühendisliği Bölümü'nde lisans öğrenimine başlamış ve halen öğrenimine devam etmektedir. Çalışma alanları bilgisayar ağlarında güvenlik, makine öğrenmesi, yapay zeka ve şifreleme konularını içermektedir.

Duygu Evrim ODABAŞ

Duygu Evrim Odabaş 2017 yılında Kocaeli Üniversitesi Bilgisayar Mühendisliği Bölümü'nde lisans öğrenimine başlamış ve halen öğrenimine devam etmektedir. Çalışma alanları makine öğrenmesi, yapay zeka, bilgisayar ağlarında güvenlik ve şifreleme konularını içermektedir.

Meltem KURT PEHLİVANOĞLU

Meltem Kurt Pehlivanoğlu 2010 yılında Trakya Üniversitesi Bilgisayar Mühendisliği Bölümünden mezun olmuştur. 2013 yılında Trakya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalın'da yüksek lisans öğrenimini tamamlamıştır. 2018 yılında Kocaeli Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda doktora öğrenimini tamamlamıştır. 2012 yılından beri Kocaeli Üniversitesi Bilgisayar Mühendisliği Bölümü'nde Araştırma Görevlisi olarak görev yapmaktadır. Çalışma alanları şifreleme, hafif sıklet şifreleme, bilgi güvenliği, bilgisayar ağlarında güvenlik, makine öğrenmesi, yapay zeka konularını içermektedir.