Avrupa Bilim ve Teknoloji Dergisi
Sayı 52, S. 19-26, Kasım 2023

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
No. 52, pp. 19-26, November 2023

Research Article

IoT Veri Kümelerinde Makine Öğrenmesine Dayalı Saldırı Tespiti

Meltem Kurt Pehlivanoğlu[1*], Arman Kuyucu[2], Recep Kaya[3], Recep Aydın[4]

[1*] Kocaeli Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliğ Bölümü, Kocaeli, Türkiye, (ORCID: 0000-0002-7581-9390), meltem.kurt@kocaeli.edu.tr
[2] Kocaeli Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Kocaeli, Türkiye, (ORCID: 0000-0001-7565-1236), 190201099@kocaeli.edu.tr
[3] Kocaeli Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Kocaeli, Türkiye, (ORCID: 0000-0002-3626-1777), 190201027@kocaeli.edu.tr
[4] Kocaeli Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Kocaeli, Türkiye, (ORCID: 0000-0003-3137-3937), 200202093@kocaeli.edu.tr

(İlk Geliş Tarihi 6 Ekim 2022 ve Kabul Tarihi 6 Ekim 2023)

(**DOI:** 10.31590/ejosat.1184984)

ATIF/REFERENCE: Kurt Pehlivanoğlu, M., Kuyucu, A., Kaya, R. & Aydın, R. (2023). IoT Veri Kümelerinde Makine Öğrenmesine Dayalı Saldırı Tespiti. *Avrupa Bilim ve Teknoloji Dergisi*, (52), 19-26.

Öz

Nesnelerin İnterneti (IoT), veri paylaşmak ve internet üzerinden birbirleriyle etkileşim kurmak için sensörler, yazılımlar ve bağlantılara sahip bir cihaz ağıdır. IoT ekosisteminde giderek artan sayıdaki bu teknolojik cihazlar çok sayıda güvenlik açığı ve riskini de ortaya çıkarır. IoT cihazları, daha karmaşık makinelere ve bilgisayarlara kıyasla işletim sistemlerinde doğal güvenlik mekanizmalarının bulunmamasına bağlı olarak çeşitli siber saldırılara karşı savunmasızdır. Özellikle port tarama, Servis Hizmet Reddi (DoS) ve Dağıtık Servis Hizmet Reddi (DDoS) gibi saldırılar IoT cihazlarının güvenliğini tehdit etmektedir. DoS ve DDoS saldırıları sistemleri çökertmeyi ve hasar vermeyi amaçlarken, Port Tarama saldırısı ise sistemden veri toplamayı amaçlayan siber saldırı türlerindendir. Bu çalışmada, belirli IoT veri kümelerinde DoS, DDoS ve Port tarama saldırılarını tespit etmek için makine öğrenimi yaklaşımlarına dayalı bir izinsiz giriş tespit mekanizması öneriyoruz. Rastgele Orman, Karar Ağacı, Destek Vektör Makinesi, K-En Yakın Komşu, Naive-Bayes, Gradyan Artırma, Doğrusal Diskriminant Analizi ve Ekstra Ağaçlar makine öğrenmesi algoritmaları kullanılarak, "Bot_IoT" ve "ToN_IoT" veri kümeleri (H+V Enriched) üzerinde DoS, DDoS ve Scanning saldırıları sınıflandırılmıştır. Çok sınıflı sınıflandırma, yani üç-sınıf ve altı-sınıf, tüm modeller için ayrı ayrı gerçekleştirilmiştir. Yapılan deneyler, tüm çoklu sınıflandırma modelleri için, Gradyan Artırma sınıflandırıcı ile %99.9944 F1-skorla en iyi sınıflandırma gerçekleştirildiğini göstermiştir.

Anahtar Kelimeler: IoT, Saldırı Tespit Sistemi, DoS, DDoS, makine öğrenmesi.

Intrusion Detection based on Machine Learning in IoT Dataset

Abstract

The Internet of Things (IoT) is a network of devices that have sensors, software, and connection to share data and interact with one another through the internet. The growing quantity of these technological devices in the IoT ecosystem also exposes numerous security vulnerabilities and risks. IoT devices are vulnerable to several cyber-attacks to the lack of inherent security mechanisms in their operating systems compared to more sophisticated machines and computers. Especially, attacks such as port scanning, Denial of Service (DoS) and Distributed Denial of Service (DDoS) threaten the security of IoT devices. DoS and DDoS attacks are types of attacks that aim system crash and cause damage, and Port Scanning attacks are types of attacks that aim to collect data from the system. In this paper, we propose an intrusion detection system based on Machine Learning (ML) appropaches to detect DoS, DDoS, and Port scanning attacks in specific IoT datasets "Bot_IoT" and "ToN_IoT" (H+V Enriched). DoS, DDoS and Scanning attacks on "Bot_IoT" and "ToN_IoT" datasets are classified using Random Forest (RF), Decision Tree (DT), Support Vector Machine (SVM), K-Nearest Neighbor (KNN), Naive-Bayes (NB), Gradient Boosting (GB), Linear Discriminant Analysis (LDA) and Extra Trees (ET) machine learning algorithms. The multiclass classifications, i.e., three-class and six-class, are performed for all models individually.

[*] Sorumlu Yazar: meltem.kurt@kocaeli.edu.tr

The experimental results show that the GB classifier can achieve the best classification with an F1-score of 99.9944% for all multiclass classification.

Keywords: IoT, Intrusion Detection System, DoS, DDoS, machine learning.

1. Giriş

Saldırı Tespit Sistemleri (STS), ağlara veya sistemlere yapılan siber saldırıları gerçekleşirken ya da gerçekleştikten sonra tespit etmeye ve bu saldırılara karşı savunmayı amaçlayan makine öğrenme veya derin öğrenme tabanlı sistemlerdir.

Nesnelerin İnterneti (Internet of Things-IoT) araçlarının sayıları ve kullanım alanları her geçen gün artmaktadır. 2021 yılında IoT cihaz sayısı %8'lik artış ile 12.2 milyara ulaşmıştır. Bu cihazların sayısının 2025 yılında 27 milyar olması öngörülmektedir. IoT cihazlarının büyük bir kısmı düşük işlem gücünden dolayı şifrelemeyi yapılamadığından dolayı saldırılara karşı savunmasız kalmaktadır. IoT cihaz sayısındaki artış göz önüne alındığında bu cihazları savunma gerekliliği ortaya çıkmaktadır.

Bu çalışmada "Bot_IoT" (Koroniotis vd., 2018) ve "ToN_IoT" (Booij vd., 2022) veri kümelerinin birleştirilmesi ile oluşturulmuş ve (Erfani vd., 2021)'de verilen "H+V Enriched" veri kümesi yeni bir saldırı tespit modelinin geliştirilmesi amaçlı kullanılmıştır. Bot_IoT veri kümesi 2018 yılında UNSW Canberra'daki Cyber Range Laboratuvarında bir ağ ortamı tasarlanarak, ToN_IoT veri kümesi ise UNSW Canberra Cyber, Mühendislik ve Bilgi Teknolojileri Okulu (SEIT), UNSW Canberra'nın IoT Laboratuvarında oluşturulmuştur. Bot_IoT veri kümesi servis taraması, işletim sistemi tespiti, DoS, DDoS, veri hırsızlığı saldırılarından oluşurken, ToN_IoT veri kümesi ise tarama, DoS, DDoS, fidye yazılım, arka kapı, injection, XSS, şifre ve aradaki adam saldırılarından oluşmaktadır.

1.1. Motivasyon ve Katkı

Bu çalışmada 2021 yılında geliştirilen DoS, DDoS ve Scanning saldırılarının yer aldığı "Bot_IoT" ve "ToN_IoT" veri kümeleri kullanılmıştır. Bu çalışmada, (Erfani vd., 2021)'de verilen çalışmadaki fikir ele alınarak veri kümeleri birleştirilmiş, birleştirilen yeni veri kümesi üzerinde Rastgele Orman, Gradient Boosting, Karar Ağacı, SVM, KNN, NB, LDA, ET algoritmaları kullanılarak (bu algoritmalar için ayrıntılı bilgilendirme (Ray, 2019) çalışmasından erişilebilir) çoklu saldırı sınıflandırma problemi üzerine çalışılmıştır. Literatürde yer alan deneysel sonuçlar değerlendirildiğinde, bu çalışmada önerilen birçok model literatürde yer alan modellerden daha yüksek başarım elde etmiştir.

1.2. Organizasyon

Makalenin ikinci bölümünde geçmiş yıllarda yapılan ilgili çalışmalar hakkında bilgi verilmiştir. Üçüncü bölümde ise kullanılan veri setleri ve saldırı türleri açıklanmış olup devamında veri önişleme adımlarından bahsedilmiştir. Dördüncü bölümde yapılan deneyler detaylandırılarak sunulmuştur. Son bölümde ise deneysel sonuçlar değerlendirilerek ileriki çalışmalardan bahsedilmiştir.

2. İlgili Çalışmalar

Literatürde, ağ tabanlı saldırıları içeren farklı veri setleri üzerinde, makine öğrenmesi ve/veya derin öğrenme yöntemleriyle saldırı tespitini hedefleyen birçok çalışma yer almaktadır. Bu çalışmalar arasında özellikle son yıllarda yayımlanan ve IoT veri kümeleri üzerinde saldırı tespiti yapan çalışmalar dikkate alınarak kapsamlı bir araştırma gerçekleştirilmiştir.

Bu çalışmalarda kullanılan veri kümeleri, kullanılan modeller, çoklu model olup olmadığı bilgisi, ikili/çoklu sınıflandırma bilgisi ve başarı değerlendirme metrikleri ayrıntılı olarak Tablo 1'de sunulmuştur.

Woźniak ve arkadaşları çalışmalarında (Woźniak vd., 2020) IoT-23 veri kümesi üzerinde kötü amaçlı yazılım tehdidi tespiti için derin öğrenme tabanlı bir model önermişlerdir. Çalışmada LSTM ve RNN modelleriyle en yüksek %99.9957 doğruluk değeri elde edilmiştir.

Booij ve arkadaşları çalışmalarında (Booij vd., 2021) ToN_IoT veri kümesinin istatistiksel analizi ve makine öğrenmesi değerlendirmesini yapmışlardır. Ayrıca veri kümesi birkaç veri kümesiyle karşılaştırılmış ve heterojenliğin önemi vurgulanmıştır. Çalışmada ToN_IoT ve IoT-23 veri kümeleri üzerinde en yüksek doğruluk değerleri RF modeli ile sırasıyla %98.075, %99.986 olarak elde edilmiştir.

Kozik ve arkadaşları çalışmalarında (Kozik vd., 2021) ağ akışlarını yakalayan, önceden tanımlanan bir zaman aralığında öznitelik vektörlerini hesaplayan ve bu vektörleri ikili sınıflandırıcıya vererek tespit çıktılarını üreten bir çözüm önerisi sunmuşlardır. Çalışmada en yüksek F-skor değeri %94.5 TFNN modeli ile elde edilmiştir.

Sahu ve arkadaşları çalışmalarında (Sahu vd., 2021) kötü amaçlı cihazları etkili bir şekilde tespit eden derin öğrenme tabanlı saldırı tespit mekanizması önerilmiştir. Çalışmada kullanılan veri kümesi 20 tane virüslü Raspberry Pi IoT cihazından toplanmıştır. Ek olarak önerilen model, yakın zamanda önerilen derin öğrenme bazlı saldırı tespit mekanizmalarından daha iyi sonuç vermiştir. Çalışmada çoklu sınıflandırmada CNN modelinde %82.04 F-skor, %80.67 kesinlik, %83.48 hassasiyet ve %82.17 doğruluk elde edilmiş olup, bu değerler Tablo 3'de verilen değerlerin ortalaması alınarak hesaplanmıştır.

Ullah ve Mahmoud çalışmalarında (Ullah ve Mahmoud, 2021) IoT ağları için yeni bir anomali bazlı izinsiz giriş tespit sistemi geliştirmişlerdir. Çalışmada, evrişimli sinirsel ağ modeli kullanılarak çok sınıflı sınıflandırma modeli oluşturulmuştur. Öğrenme aktarımı, çok sınıflı önceden eğitilmiş bir konvolüsyonel sinir ağı modelini kullanarak ikili ve çok sınıflı sınıflandırmayı uygulamak için kullanılmaktadır. Çalışmada farklı veri kümeleri üzerinde çoklu sınıflandırma yapılmış olup, her veri kümesi üzerinde en yüksek doğruluk değerleri: Bot_IoT veri kümesinde CNN1D modelinde %99.97, IoT Network Intrusion veri kümesinde CNN1D modelinde %97.76, MQTT-IoT-IDS2020 veri kümesinde CNN2D modelinde %99.93 ve IoT-23 veri kümesinde CNN1D modelinde %99.96 olarak elde edilmiştir.

2021 yılında yapılan çalışmada (Ioannou ve Vassiliou, 2021), IoT'de kullanılan düşük güçlü ve kısa menzilli ağlarda kötü niyetli davranışları tespit etmek için SVM modellerininin kullanılması önerilmiştir. İki SVM yaklaşımı (C-SVM ve OC-SVM) değerlendirilmiştir. C-SVM iki sınıf vektör değeri gerektirir (biri normal ve diğeri anormal aktivite için) ve OC-SVM sadece normal davranış aktivitesini gözlemlemektedir. Her iki yaklaşım da anormal aktiviteyi izleyen ve tespit eden bir saldırı tespit sisteminin (IDS) parçası olarak kullanıldı. Çalışmada C-SVM modelinde %92.3 hassasiyet, OC-SVM modelinde ise %82.1 hassasiyet değeri elde edilmiştir.

2021 yılında yapılan bir diğer çalışmada (Erfani vd., 2021), IoT veri setlerini iki yönde zenginleştirmek için bir sistem önerilmektedir: dikey ve yatay. Dikey görünüm, son teknoloji IoT veri setlerini birleştirmektedir. Yatay görünüm ise IoT cihazlarının davranışını daha çeşitli ayarlarda sunmak için benzersiz ve yeni bir dizi öznitelik önermektedir. Deneysel sonuçlarda, önerilen yöntem tarafından geliştirilen yeni simüle edilmiş veri setlerinin, çeşitli makine öğrenimi algoritmaları ile siber güvenlik saldırılarını sınıflandırmada daha iyi performans elde ettiği gösterilmektedir. Çalışmada Bot_IoT veri kümesinde DT modelinde %99.56 F-skor, ToN_IoT veri kümesinde DT modelinde ise %99.25 F-skor değeri elde edilmiştir.

2022 yılında yapılan çalışmada (Nascita vd., 2022), IoT-23 veri kümesi üzerinde derin öğrenmeye dayalı trafik sınıflandırıcıları kullanılmış ve bunların IoT saldırı sınıflandırmasındaki etkinlikleri değerlendirilmiştir. Çalışmada en yüksek doğruluk değeri MIMETIC modeli ile %99.93 olarak elde edilmiştir.

Islam ve arkadaşları çalışmalarında (Islam vd., 2022), Banking Fraud Detection veri kümesi kullanarak finansal kuruluşlara yönelik DDoS saldırılarının tespit edilmesi amaçlanmıştır. Çalışmada SVM modeli diğer makine öğrenimi ve derin öğrenme yaklaşımlarına oranla %99.8 doğruluk değeri ile en yüksek skora sahiptir.

Jarjis ve arkadaşları çalışmalarında (Jarjis vd., 2023) Bot_IoT ve ToN_IoT veri kümesini bir arada kullanarak bu veri kümesi üzerinde farklı makine öğrenmesi modelleri kullanarak saldırı tespit sistemi geliştirilmiştir. Çalışmada, modeller arasından XGB modeli tüm değerlendirme metrikleri için %100 skor elde etmiştir.

Literatürde özellikle Bot_IoT ve ToN_IoT veri kümelerini birarada kullanan çalışmalar değerlendirildiğinde, (Jarjis vd., 2023)'de XGB modeli tüm metrikler için en yüksek skor değeri %100'ü elde etse de ilgili çalışmada yer alan diğer makine öğrenmesi modelleri için başarımlar yüksek değildir. Bu çalışmada aynı veri kümesi üzerinde, GB modellerinin yanı sıra, diğer makine öğrenmesi modellerinin de başarımlarının yükseltilmesi hedeflenmiştir.

Tablo 1. İlgili Çalışmaların Özeti (Summary of the Related Works)

Referans	**Veri Kümesi**	**Model**	**ÇS/İS**
(Woźniak vd., 2020)	*IoT-23*	*LSTM+RNN*	*İS*
(Booij vd., 2021)	*ToN_IoT, IoT-23*	*BS, RF, MLP*	*İS*
(Kozik vd., 2021)	*IoT-23*	*TFNN, DT, RF, AB*	*İS*
(Sahu vd., 2021)	*IoT-23*	*2D-CNN+LSTM*	*ÇS/İS*
(Ullah ve Mahmoud, 2021)	*Bot_IoT, IoT Network Intrusion, MQTT-IoT-IDS2020, IoT-23*	*1D-CNN, 2D-CNN,3D-CNN*	*ÇS/İS*
(Ioannou ve Vassiliou, 2021)	*Kendi Veri Kümeleri*	*C-SVM, OC-SVM*	*İS*
(Erfani vd., 2021)	*Bot_IoT, ToN_IoT, Bot_IoT ve ToN_IoT (H+V Enriched)*	*RF, DT, SVM, KNN, NB(Bernoulli), GB, LDA, ET*	*ÇS*
(Nascita vd., 2022)	*IoT-23*	*MIMETIC, 1D-CNN 2D-CNN+LSTM, NB, DT, RF, BG*	*ÇS*
(Islam vd., 2022)	*Banking Fraud Detection (Kaggle)*	*SVM, KNN, RF*	*ÇS*
(Jarsis vd., 2023)	*Bot_IoT ve ToN_IoT (H+V Enriched)*	*RF, DT SVM ,KNN XGB*	*ÇS*
Önerilen Model	*Bot_IoT ve ToN_IoT (H+V Enriched)*	*RF, DT, SVM, KNN, NB(Bernoulli), GB, LDA, ET*	*ÇS*

ÇS: Çoklu Sınıflandırma. İS: İkili Sınıflandırma. Teknik: AdaBoost (AB), BG: Bagging Sınıflandırıcısı (Bagging Classifier), BS: Artırma Sınıflandırıcısı (Boosting Classifier), CNN: Evrişimli Sinir Ağı (Convolutional Neural Network), GB: Gradyan Artırma (Gradient Boosting), LSTM: Uzun kısa süreli bellek (Long Short-Term Memory), MLP: Çok Katmanlı Algılayıcılar (MultiLayer Perceptron), RNN: Yinelemeli sinir ağı (Recurrent Neural Network), SVM: Destek Vektör Makinesi (Support Vector Machine), TFNN: Dönüştürücü Bazlı Sinir Ağı (Transformer-based Neural Network), MIMETIC: Derin Öğrenme Tabanlı Mobil Trafik Sınıflandırıcı Multi Modeli (Multimodal DL-based Mobile Traffic Classification), XGB: Aşırı Gradyan Artırma (eXtreme Gradient Boosting)

3. Önerilen Saldırı Tespit Modeli

3.1. Veri Kümesi

Bu çalışmada, 2021 yılında yapılan çalışmada (Erfani vd., 2021) yer alan "H (Horizontal-Yatay) + V (Vertical-Dikey) Enriched" veri kümesi kullanılmıştır. Dikey görünüm, son teknoloji IoT veri kümelerini birleştirmektedir. Yatay görünüm ise IoT cihazlarının davranışını daha çeşitli ayarlarda sunmak için benzersiz ve yeni bir dizi öznitelik önermektedir. "H+V Enriched" veri kümesi "Bot_IoT" ve "ToN_IoT" veri kümelerine yeni öznitelikler eklenmesi ve bunların birleştirilmesi ile oluşturulmuştur. Çalışmada kullanılan veri kümesinde 53391 gözlem ve 92 öznitelik bulunmaktadır. Tablo 2'de bu öznitelikler verilmiştir. "H+V Enriched" veri kümesi üç farklı saldırı türü içermektedir: DoS, DDoS ve port scanning (port tarama). DoS saldırısında hedef sisteme tek bir kaynaktan yüklü bir ağ trafiği gönderilerek, hedef sistemi yavaşlatmak/çökertmek amaçlanmaktadır. DDoS saldırısı ise tek bir kaynak yerine çok sayıda ele geçirilen cihazlardan oluşan botnet ağından başlatılır. DDoS hedefe katlanarak artan istekler göndererek saldırı gücünü artırır. Port taramada, hedef bilgisayarda açık olan portlar bulunarak, bu portlardan hedef sistem hakkında birçok bilgi elde edilir.

Tablo 2. Çalışmada Kullanılan Veri Kümesi (Dataset Used in the Study)

No	Öznitelik	No	Öznitelik	No	Öznitelik	No	Öznitelik
1	ts	24	flow_active_time	47	TNP_per_proto_tcp	70	IPv
2	flow_duration	25	Min	48	TNP_per_proto_udp	71	MAC
3	Header Length	26	Max	49	spkts	72	LLC
4	Source IP	27	Std	50	dpkts	73	fin_flag_number
5	Destination IP	28	IAT	51	sbytes	74	syn_flag_number
6	Source Port	29	Tot size	52	dbytes	75	rst_flag_number
7	Destination Port	30	Tot sum	53	Tnp_per_proto	76	urg_flag_number
8	Protocol Type	31	AVG	54	AR_P_proto_P_src_ip	77	ece_flag_number
9	Protocol Name	32	Magnitude	55	AR_P_proto_P_dst_ip	78	cwr_flag_number
10	Duration	33	Radius	56	AR_P_proto_P_sport	79	ack_count
11	src_ip_bytes	34	Covariance	57	AR_P_proto_P_dport	80	syn_count
12	dst_ip_bytes	35	Variance	58	Max_flow_duration	81	fin_count
13	src_pkts	36	Number	59	Min_flow_duration	82	TnP_per_dport
14	dst_pkts	37	Pearson Correlation	60	Sum_flow_duration	83	N_IN_Conn_P_Src_IP
15	Rate	38	Weight	61	Avg_flow_duration	84	N_IN_Conn_P_Dst_IP
16	Srate	39	MQTT	62	IRC	85	Wifi_Type
17	Drate	40	CoAP	63	TCP	86	Wifi_Subtype
18	psh_flag_number	41	HTTP	64	UDP	87	DS status
19	ack_flag_number	42	HTTPS	65	DHCP	88	Fragments
20	urg_count	43	DNS	66	ARP	89	wifi_src
21	rst_count	44	Telnet	67	RARP	90	wifi_dst
22	Std_flow_duration	45	SMTP	68	ICMP	91	Sequence number
23	flow_idle_time	46	SSH	69	IGMP	92	Protocol Version

92 özniteliğe sınıflandırma yapılabilmesi için "label", "label2" ve "label3" olmak üzere 3 yeni öznitelik eklenmiştir. Eğer veri "Bot_IoT" (bu veri kümesi Bot_iot_DoS_new, Bot_iot_DDoS_new, Bot_iot_scanning alt veri kümelerini içerir) veri kümesinden geldiyse "label2" özniteliği "1", "ToN_IoT" (bu veri kümesi Ton_iot_DoS, Ton_iot_DDoS_new, Ton_iot_scanning_new alt veri kümelerini içerir) veri kümesinden geldiyse "label2" özniteliği "2" yapılmıştır. "label" özniteliği ise saldırı tipi ile ilişkilendirilmiş olup DoS için "1", "DDoS" için "2" ve "Scanning" için "3" ataması yapılmıştır. "label3" ise "label2" ve "label" özniteliklerinde yer

alan verilerin sırayla birleşiminden oluşmaktadır. Yeni öznitelikler eklendikten sonra oluşan veri kümesi "H+V.csv" dosyası olarak kaydedilmiştir. Tablo 3'de yeni eklenen özniteliklere ait etiket isimlendirmeleri verilmiştir.

Tablo 3. Veri Kümesine Yeni Eklenen Etiketler (Newly Added Labels to the Dataset)

Veri Kümesi	label2	label	label3
Bot_iot_DoS_new	*1*	*1*	*11*
Bot_iot_DDoS_new	*1*	*2*	*12*
Bot_iot_scanning	*1*	*3*	*13*
Ton_iot_DoS	*2*	*1*	*21*
Ton_iot_DDoS_new	*2*	*2*	*22*
Ton_iot_scanning_new	*2*	*3*	*23*

3.2. Veri Önişleme

3.2.1. Kodlama

Veri kümesinde "Source IP, Destination IP, Protocol_name, TnP_per_dport, N_IN_Conn_P_Src_IP, N_IN_Conn_P_Dst_IP, TnP_per_Proto, AR_P_Proto_P_SrcIP, AR_P_Proto_P_Dst_IP, AR_P_Proto_P_sport, AR_P_Proto_P_dport" olmak üzere 11 tane obje tipinde öznitelik tespit edilmiştir. Bu obje tipindeki özniteliklere etiket kodlaması (label encoding) uygulanarak ilgili veri kümesinde güncellemeler yapılmıştır. Ayrıca performans karşılaştırması yapabilmek için IP adreslerinin bulunduğu "Source IP" ve "Destination IP" özniteliklere one hot encoding uygulanmıştır. One hot encoding sonrası "Source IP" özniteliğinden 2356, "Destination IP" özniteliğinden 96 tane yeni öznitelik elde edilmiş olup "Source IP" ve "Destination IP" öznitelikleri çıkarılmıştır.

3.2.2. Öznitelik Seçimi

Veri kümesinin özniteliğini yansıtmayan özniteliklerin başarımı düşürmesini engellemek amacıyla her bir veri kümesindeki özniteliklerin önemlilik derecesini hesaplanıp öznitelik seçimi yapılmıştır.

En çok başarıya sahip ve öznitelik önemliliği hesaplanabilen RF ve DT makine öğrenme modelleri seçilmiştir. Bu modeller 10 kez farklı test ve eğitim verileri ile çalıştırılıp, öznitelik önemlilik derecesi ve toplamda 20 çalıştırmada en çok tekrar etme sayısına göre öznitelikler seçilmiştir. Ham veri kümesinde 92 adet öznitelik bulunmaktadır. Öznitelik seçimi sonucunda sırasıyla 25 (15 farklı öznitelik bu özniteliklerin içerisinde yer almaktadır.), 15 öznitelik elde edilmiştir. "Destination IP" ve "Source IP" özniteliklerine kodlama yapıldığında 2542 öznitelikli yeni bir veri kümesi oluşmuştur. Bu veri kümesine öznitelik seçimi yapıldığında üç-sınıf sınıflandırmada sırasıyla 97, 49; altı-sınıf sınıflandırmada 93, 60 öznitelik elde edilmiştir.

3.2.3. Hiper Parametre Ayarlaması (Hyperparameter Tuning)

Daha efektif ve başarılı sonucu alabilmek için son adım olarak hiper parametre ayarlaması yapılmıştır. Ayarlama için GridSearchCV fonksiyonu kullanılmıştır. Bu fonksiyon, parametre olarak verilen hiper parametre değerlerinden oluşabilecek bütün olasılıkları deneyerek en yüksek çapraz doğrulama başarısını elde eden parametreleri bulmaktadır.

4. Deneysel Sonuçlar

Çalışma kapsamında çoklu sınıflandırma kullanılmış olup üç-sınıf (DoS, DDoS, Scanning) ve altı-sınıf (Bot_iot_DoS, Bot_iot_DDoS, Bot_iot_scanning, Ton_iot_DoS, Ton_iot_DDoS, Ton_iot_scanning) için modeller eğitilmiş ve test edilmiştir.

Tablo 4 ve 5'de kullanılan "V(Varsayılan)" gösterimi Erfani ve arkadaşlarının yaptıkları çalışmada (Erfani vd., 2021) kullanılan parametreleri ifade etmektedir. Ancak bazı algoritmalarda parametreler varsayılan değerlerle kullanıldığında aşırı öğrenme (overfitting) olmaktadır. Bunu engellemek amaçlı bazı algoritmalara "max_depth" parametresi eklenmiştir. Tablo 4 ve 5'de kullanılan "A(Ayarlama)" gösterimi ise hiper parametre ayarlaması işlemini ifade etmektedir. İlgili tablolarda verilen Öznitelik Sayısı sütununda tahminlenmeye çalışılan etiket özniteliği eklenmemiştir.

4.1. Üç-sınıf Sınıflandırma

DoS, DDoS, Scanning saldırılarının sınıflandırılması için RF, GB, NB, ET, KNN, LDA, DT ve SVM algoritmaları test edilmiştir. Yapılan deneyler sonucunda üç-sınıf sınıflandırma ile elde edilen en iyi F1-skor, kesinlik, hassasiyet ve doğruluk skorları Tablo 4'de verilmiştir. Tablodan da görüleceği gibi en iyi F1 skoru %99.9944 ve %99.9944 doğruluk değeri ile GB algoritması ile elde edilmiştir. Bu sonuç hiper parametre ayarlaması ve öznitelik mühendisliği yapılarak elde edilmiştir.

Tablo 4. Üç-Sınıf Sınıflandırma için Modellerin Başarımı (Performance of Models for Three-Class Classification)

Algoritma	Parametreler	Öznitelik Sayısı	V/A	ÖM	F-Skor (F1)	Kesinlik (Precision)	Hassasiyet (Recall)	Doğruluk (Accuracy)
RF	*criterion='entropy', max_depth=5, n_estimators=20,random_state=42*	*49*	*A*	*Var*	*99.9775*	*99.9775*	*99.9775*	*99.9775*
DT	*ccp_alpha=0.0001, criterion='entropy', max_depth=5, max_features='auto', random_state=42*	*15*	*A*	*Yok*	*99.9831*	*99.9832*	*99.9831*	*99.9831*
SVM	*C=1000*	*97*	*A*	*Var*	*75.8154*	*76.9561*	*78.9033*	*78.9033*
KNN	*leaf_size=1, n_neighbors=30, p=1, weights='distance'*	*15*	*A*	*Yok*	*92.2829*	*92.1251*	*92.7672*	*92.7672*
NB	*alpha=1e-10, binarize=10000.0, fit_prior=False*	*25*	*A*	*Yok*	*94.4306*	*94.8991*	*94.2970*	*94.2970*
GB	*n_estimators=45, random_state=42*	*97*	*A*	*Var*	*99.9944*	*99.9944*	*99.9944*	*99.9944*
LDA	*tol=1e-10*	*97*	*A*	*Yok*	*99.9003*	*99.9016*	*99.8994*	*99.9009*
ET	*Criterion = gini , n_estimators=100 , Max_depth = 4*	*15*	*V*	*Yok*	*99.8765*	*99.8772*	*99.8763*	*99.8763*

V/A: Varsayılan(V), Ayarlama(A). **ÖM:** Öznitelik Mühendisliği

4.2. Altı-Sınıf Sınıflandırma

Bot_iot_DoS, Bot_iot_DDoS, Bot_iot_scanning, Ton_iot_DoS, Ton_iot_DDoS, Ton_iot_scanning veri kümesine göre etiketlenmiş saldırıların sınıflandırılması için RF, GB, NB, ET, KNN, LDA, DT ve SVM algoritmaları test edilmiştir.

Yapılan deneyler sonucunda altı-sınıf sınıflandırma ile elde edilen en iyi f-skor (F1), kesinlik, hassasiyet ve doğruluk (accuracy) skorları Tablo 5'de verilmiştir. Tabloya göre en iyi F1 skoru %99.9944 ve %99.9944 doğruluk ile GB ve KNN algoritmaları ile elde edilmiştir.

Tablo 5. Altı-Sınıf Sınıflandırma için Modellerin Başarımı (Performance of Models for Six-Class Classification)

Algoritma	Parametreler	Öznitelik Sayısı	V/A	ÖM	F1-Skor	Kesinlik	Hassasiyet	Doğruluk
RF	*criterion='entropy', max_depth=4, max_features='log2', n_estimators=20, random_state=42*	*15*	*A*	*Yok*	*99.9273*	*99.9305*	*99.9269*	*99.9269*
DT	*ccp_alpha=0.001, criterion='entropy', max_depth=6, max_features='auto', random_state=42*	*15*	*A*	*Yok*	*99.9831*	*99.9831*	*99.9831*	*99.9831*
SVM	*C=1000*	*15*	*A*	*Yok*	*81.6558*	*89.7824*	*87.2835*	*87.2835*
KNN	*n_neighbors=50, metric='chebyshev'*	*15*	*A*	*Yok*	*99.9775*	*99.9775*	*99.9775*	*99.9775*
NB	*alpha=1e-10, binarize=10000.0*	*93*	*A*	*Var*	*93.5177*	*94.9464*	*94.7167*	*94.7167*
GB	*learning_rate=0.2, n_estimators=40, random_state=1024*	*93*	*A*	*Var*	*99.9944*	*99.9944*	*99.9944*	*99.9944*
LDA	*Solver = svd*	*92*	*V*	*Yok*	*92.1905*	*92.4153*	*92.3728*	*92.9785*
ET	*criterion = 'gini', n_estimators=100, max_depth=4*	*15*	*V*	*Yok*	*99.9831*	*99.9832*	*99.9831*	*99.9831*

V/A: Varsayılan(V), Ayarlama(A). **ÖM**: Öznitelik Mühendisliği

Tablo 6' da bu çalışmaya en benzer ("H+V Enriched" veri kümesini kullanan) çalışmalarda (Erfani vd., 2021; Jarjis vd., 2023) elde edilen deneysel sonuçlar F1 skor ve doğruluk metrikleri açısından karşılaştırılmıştır. Elde edilen sonuçlar değerlendirildiğinde, bu çalışmada önerilen üç ve altı sınıf sınıflandırma modellerinin başarımlarının diğer çalışmalara göre referans alınan bu iki çalışmadan daha iyi sonuçlar elde edildiği görülmektedir. Veri kümesi üzerinde yapılan veri ön işleme adımları ve uygun hiper parametrelerin seçimi sayesinde, diğer çalışmalarda en başarısız model olan SVM modelinin bile önerilen modellerde doğruluk başarımlarının arttırıldığı gözlemlenmiştir. (Jarjis vd., 2023)'de verilen çalışmada XGB algoritması ile en yüksek başarım elde edildiği için, bu çalışmada bu model kullanılmamıştır.

Tablo 6. Literatürde "H+V Enriched" Veri Kümesini Kullanan Çalışmalar ile Önerilen Modellerin Karşılaştırılması

Model	**(Erfani vd., 2021)**		**(Jarjis vd., 2023)**		**Önerilen Model (Üç-Sınıf Sınıflandırma)**		**Önerilen Model (Altı-Sınıf Sınıflandırma)**	
	F1 Skoru	**Doğruluk**	**F1 Skoru**	**Doğruluk**	**F1 Skoru**	**Doğruluk**	**F1 Skoru**	**Doğruluk**
RF	*97.62*	*97.66*	*99.0175*	*99.0214*	***99.9775***	***99.9775***	*99.9273*	*99.9269*
DT	*99.96*	*99.96*	*99.978*	*99.979*	***99.9831***	***99.9831***	***99.9831***	***99.9831***
SVM	*76.41*	*77.13*	*78.3414*	*78.7336*	*75.8154*	*78.9033*	***81.6558***	***87.2835***
KNN	*81.41*	*81.96*	*91.233*	*91.231*	*92.2829*	*92.7672*	***99.9775***	***99.9775***
NB	*53.02*	*55.16*	-	-	***94.4306***	*94.2970*	*93.5177*	***94.7167***
GB	*99.86*	*99.86*	-	-	***99.9944***	***99.9944***	***99.9944***	***99.9944***
LDA	*91.19*	*91.63*	-	-	***99.9003***	***99.9009***	*92.1905*	*92.9785*
ET	*99.43*	*99.43*	-	-	*99.8765*	*99.8763*	***99.9831***	***99.9831***
XGB	-	-	***100***	***100***	-	-	-	-

5. Sonuç ve İleriki Çalışmalar

Bu çalışmada, DoS, DDoS ve scanning saldırılarını içeren "Bot_IoT" ve "ToN_IoT" veri kümelerinin birleştirilmesi ile elde edilen "H+V Enriched" olarak adlandırılan veri kümesi saldırı tespiti amaçlı kullanılmıştır. Çalışmada saldırıların çoklu sınıflandırılması hedeflenmiş olup, üç ve altı sınıf sınıflandırma olmak üzere iki farklı çoklu sınıflandırma probleminin çözülmesi üzerine çalışılmıştır.

Saldırı sınıflandırması amaçlı RF, DT, SVM, KNN, NB, GB, LDA, ET algoritmaları kullanılarak modeller eğitilmiştir. Bunun yanı sıra farklı sayıda öznitelikler seçilerek model başarımları test edilmiştir. Deneysel sonuçlar incelendiğinde, hiper parametre ayarlaması yapıldığında çalışmada kullanılan tüm modellerin skorlarında iyileşme gözlemlenmiştir. Literatürde aynı veri kümesini kullanan diğer çalışmalar göz önünde bulundurulduğunda, bu çalışmada önerilen modellerin birçoğunun, ilgili çalışmalardaki modellerden çok daha başarılı olduğu açıktır. İleriki çalışmalarda artımlı makine öğrenmesi modelleri tabanlı bir saldırı tespit sisteminin geliştirimesi hedeflenmektedir.

Kaynakça

Booij, T. M., Chiscop, I., Meeuwissen, E., Moustafa, N., & Den Hartog, F. T. (2021). ToN_IoT: The role of heterogeneity and the need for standardization of features and attack types in IoT network intrusion data sets. IEEE Internet of Things Journal, 9(1), 485-496.

Erfani, M., Shoeleh, F., Dadkhah, S., Kaur, B., Xiong, P., Iqbal, S., ... & Ghorbani, A. A. (2021, October). A feature exploration approach for IoT attack type classification. In 2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech) (pp. 582-588). IEEE.

Falcao, A. X., & Papa, J. P. (Eds.). (2022). Optimum-Path Forest: Theory, Algorithms, and Applications. Academic Press.

Ioannou, C., & Vassiliou, V. (2021). Network attack classification in IoT using support vector machines. Journal of sensor and actuator networks, 10(3), 58.

Islam, U., Muhammad, A., Mansoor, R., Hossain, M. S., Ahmad, I., Eldin, E. T., ... & Shafiq, M. (2022). Detection of distributed denial of service (DDoS) attacks in IOT based monitoring system of banking sector using machine learning models. Sustainability, 14(14), 8374.

Jarjis, A. H., Al Zubaidi, N. Y. S., & Pehlivanoglu, M. K. (2023). Cyber Attacks Classification on Enriching IoT Datasets. EAI Endorsed Transactions on Internet of Things, 9(3).

Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. Future Generation Computer Systems, 100, 779-796.

Kozik, R., Pawlicki, M., & Choraś, M. (2021). A new method of hybrid time window embedding with transformer-based traffic data classification in IoT-networked environment. Pattern Analysis and Applications, 24(4), 1441-1449.

Nascita, A., Cerasuolo, F., Di Monda, D., Garcia, J. T. A., Montieri, A., & Pescapè, A. (2022, May). Machine and deep learning approaches for IoT attack classification. In IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 1-6). IEEE.

Ray, S. (2019, February). A quick review of machine learning algorithms. In 2019 International conference on machine learning, big data, cloud and parallel computing (COMITCon) (pp. 35-39). IEEE.

Sahu, A. K., Sharma, S., Tanveer, M., & Raja, R. (2021). Internet of Things attack detection using hybrid Deep Learning Model. Computer Communications, 176, 146-154.

Ullah, I., & Mahmoud, Q. H. (2021). Design and development of a deep learning-based model for anomaly detection in IoT networks. IEEE Access, 9, 103906-103926.

Woźniak, M., Siłka, J., Wieczorek, M., & Alrashoud, M. (2020). Recurrent neural network model for IoT and networking malware threat detection. IEEE Transactions on Industrial Informatics, 17(8), 5583-5594.