Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi
Sayı 7, S. 275-280, 7, 2023

Araştırma Makalesi

IJANSER
https://as-proceeding.com/index.php/ijanser
ISSN: 2980-0811

International Journal of Advanced Natural Sciences and Engineering Researches
Volume 7, pp. 275-280, 7, 2023

Research Article

Yapay Zekâ Teknikleri Kullanılarak IOT Cihazlarda DDos Saldırı Tespiti

Fuat SUNGUR[1*], Halit BAKIR [2]

[1]*Savunma Teknolojileri Anabilim Dalı / Lisansüstü Eğitim Enstitüsü, Sivas Bilim ve Teknoloji Üniversitesi, Türkiye*
[2]*Bilgisayar mühendislik bölümü / Mühendislik ve Doğa Bilimleri Fakültesi, Sivas Bilim ve Teknoloji Üniversitesi, Türkiye*

[*]*(sungurbey58@hotmail.com) Başlıca yazarın mail adresi*

(Geliş Tarihi: 17 Ağustos 2023, Kabul Tarihi: 28 Ağustos 2023)

(1st International Conference on Recent and Innovative Results in Engineering and Technology ICRIRET 2023, August 16-18, 2023)

ATIF/REFERENCE: Sungur, F. & Bakır, H. (2023). Yapay Zekâ Teknikleri Kullanılarak IOT Cihazlarda DDos Saldırı Tespiti, *International Journal of Advanced Natural Sciences and Engineering Researches*, 7(7), 275-280.

Özet – Yazılım tanımlı ağlar (SDN) geleneksel ağ yapıları ile kıyaslandığında küçük ağ ortamlarında daha verimli çalışmaktadır. Bu nedenle evde, işte hatta her yerde gerek iletişim için gerekse ihtiyaçlarımız için kullandığımız nesnelerin interneti (IoT) cihazlarında sıklıkla tercih edilmektedir. SDN tabanlı ağlardaki kontrol ve veri ortamlarımın bağımsız çalışması SDN tabanlı ağların daha anlaşılabilir olmasını sağlamıştır. Bu nedenle SDN'ler IoT cihazların iletişiminde geleneksel ağ yapılarına göre daha basit ve kullanışlıdır. Hayatımızı inanılmaz derecede kolaylaştıran IoT cihazlar etrafımızı kuşatırken bu cihazların ne kadar güvende olduğu sorunu ile karşı karşıya kalıyoruz. Buradan yola çıkarak bu çalışmada SDN tabanlı IoT cihazlara uygulanabilecek hizmet reddi saldırılarının tespiti ele alındı. Makine öğrenme tekniklerinden Rasgele orman, Karar ağaçları, Gradyan arttırıcı, XGBoost ve derin öğrenme tekniklerinden Derin sinir ağları (DNN) ve Evrişimli sinir ağları (CNN) kullanılarak saldırı tespit modelleri oluşturuldu. Oluşturulan modeller kıyaslanarak en iyi model ortaya çıkarıldı. Derin sinir ağları ve Evrişimli sinir ağları birlikte kullanılarak hibrit bir model oluşturuldu. Oluşturulan modelde 0,99 tahmin başarısı elde edildi.

Anahtar Kelimeler – Yazılım Tanımlı Ağ, IoT, Dos DDos Saldırı, Derin Öğrenme, Makine Öğrenmesi

1. GİRİŞ

Bugün sahip olduğumuz ağ ve internet, birçok hizmet alanında, dinamik nesne, cihaz ve uygulamalarda kullanılmasının yanında global anlamda iletişim düzlemi olarak ta kullanılmaktadır [1]. Bunun yanında hayatımızın vazgeçilmez bir parçası olan Nesnelerin interneti cihazları (IoT) ağ ve internet trafiğini daha da çoğaltarak karmaşıklığı arttırmıştır. Geleneksel ağlar daha çok büyük ağ yapılarının işlevsel kullanımı içindir ve yapı itibariyle IoT cihazların yoğun trafiğini ve karmaşıklığını sadeleştirecek şekilde tasarlanmamıştır. İşte burada Yazılım Tanımlı ağlar (SDN) devreye girmektedir. Kontrol düzlemi ve veri düzleminin bağımsız çalıştığı Yazılım Tanımlı Ağlar ağ kontrolünü tek bir noktada merkezîleştirilerek ağı tek bir yönetim noktasından kontrol etmektedir[1], [2]. SDN'lerdeki merkezi komuta sistemi diğer klasik ağlara göre uygulanması ve kontrol edilmesi daha kolaydır. Diğer yandan SDN'lerdeki merkezi kontrol noktasının varlığı SDN ve bağlı cihazları özellikle hizmet reddi saldırılarına (Dos) karşı kolay hedef haline getirebilmektedir.

Bu çalışmada, SDN tabanlı IoT cihazlarda Dos ve Dağıtılmış hizmet reddi saldırıları (DDos) tespit modeli önerilmiştir. Büyük çaplı fabrikalardan evimizde kullandığımız küçük ev aletlerine kadar birçok alanda IoT cihazlar bulunmaktadır. Bu cihazların güvenliğinin sağlanması kişisel bilgi

güvenliği açısından önem arz etmektedir. Ayrıca IoT cihazların hizmet reddine uğraması da günlük iş akışında ciddi sorunlara yol açabilir.

Makine öğrenmesi ve derin öğrenme modellerinin gün geçtikçe daha da değer kazandığı günümüzde saldırı tespit sistemlerinin de bu çalışmalardan ilham alarak gelişmesi kaçınılmaz olmuştur. SDN tabanlı IoT cihazların Dos/DDos saldırılarına karşı oluşturulacak saldırı tespit modeli makine öğrenmesi ve derin öğrenme teknikleri kullanılarak oluşturulmuş ve karşılaştırmalı bir çalışma hazırlanmıştır.

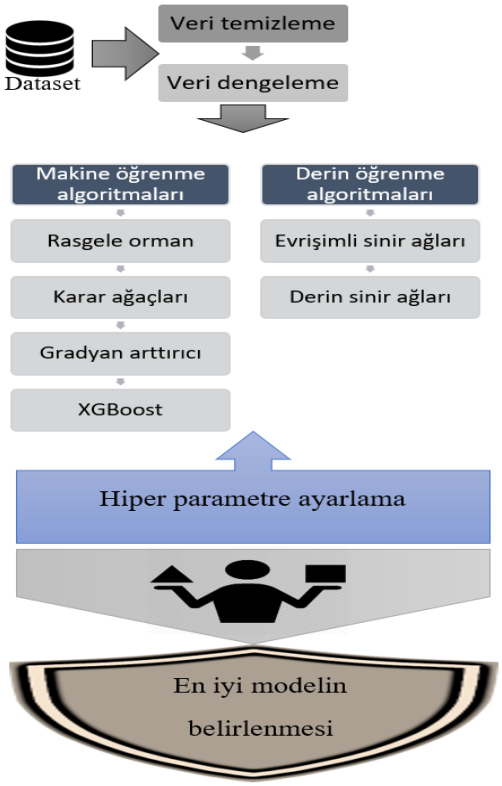
Derin öğrenme teknikleri ön plana çıkarılarak mevcut veri setinden olabildiğince güncel, performanslı, zaman ve maliyet açısından verimli bir model oluşturulmuştur. Derin öğrenme tekniklerinden Derin sinir ağları (DNN) ve Evrişimli Sinir Ağları (CNN) kullanılarak hibrit bir model oluşturulmuştur.

Çalışmanın SDN'li IoT cihazlara uygulanan DDos saldırılarının tespitinde kollektif bir model ortaya koyarak diğer çalışmalardan farklı bir perspektifte ışık tutması amaçlanmıştır.

Literatürde bazı çalışma örneklerine rastlanmıştır. Hasan ve ark. [3] SDN tabanlı ağlarda Botnet tespiti için DNN tekniklerini kullanarak oluşturduğu modelde 0,99 F1 skoru elde ettiler. Tang ve ark. [4] önerdikleri DNN modelinde SDN ağlarda Dos saldırılarını tespit ettiler. NSL-KDD veri setini kullandıkları çalışmada 0,74 F1 skoru elde ettiler. Narayanadoss ve ark. [5] SDN tabanlı IoT cihazlarda DDos saldırıları tespit ettikleri DNN modelinde 0,87 tahmin başarısı elde ettiler. Farrag ve ark. [6] SDN tabanlı IoT cihazlarda botnet saldırılarını tespit etmek için önerdikleri DNN modelinde CICDDos2019 veri setinde 0,58, TON-IoT veri setinde 0,95 F1 skoru elde ettiler. Bakour ve ark. [7] ağ izinsiz giriş tespitinde tabu arama ve saf genetik algoritmayı birleştirdiler. Önerdikleri hibrit sistemde 0,99 tespit oranı elde ettiler. Doğan ve ark. [8] Makine öğrenme yöntemlerinin hiper parametrelerini ayarlayarak ağdaki saldırı tespitini yaptılar. Yapay sinir ağları ve makine öğrenme algoritmaları kullanarak Yapay sinir ağlarında 0,99 tespit başarısı ve en yüksek skoru elde ettikleri makine öğrenme algoritması XGBoost'ta 0,99 tespit başarısı elde ettiler.

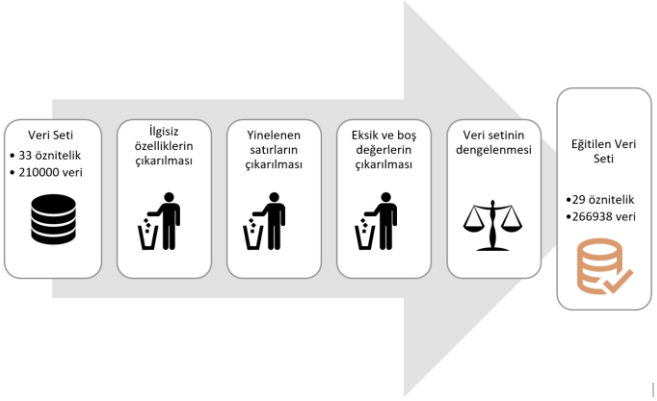
2. MATERYAL VE YÖNTEM

Çalışma veri setinin hazırlanması, yapay zekâ algoritmalarının uygulanması ve uygulama sonuçlarının karşılaştırılarak eni iyi modelin belirlenmesi olmak üzere üç aşamadan oluşmuştur. Çalışmanın aşamalarını gösteren akış şeması Şekil 1'de gösterilmiştir.



Şekil 1. Akış şeması

Bu çalışmada Sarıca ve ark. [9] tarafından hazırlanan SDN-Dataset kullanıldı. Veri seti Dos, DDos, bağlantı noktası taraması, OS parmak izi, Fuzzing saldırıları ile oluşturulmuştur. Veri seti 33 öz nitelik ve 210000 satırdan oluşmaktadır. Veri seti temizleme işlemleri yapılarak sadeleştirildi, SMOTETomek yöntemi ile dengelendi. Şekil 2'de veri seti hazırlama işlemleri gösterilmiştir.



Şekil 2. Veri seti hazırlama

2.1. Yazılım Tanımlı Ağlar

SDN, cihazlarda veri ortamını kontrol ortamından ayıran bir yaklaşımdır. Operatörler bu sayede ağ yapılandırması ve kontrolü üzerinde otoriter bir denetime sahip olurlar. SDN ağ koordinasyonuna esneklik katar. Ortam değişkenlerine ve operatörlere uyum sağlamayı ve ağ verimliliğini en üst düzeye çıkarmayı kolaylaştırır [10]. Geleneksel ağlarda anahtarlar, yönlendiriciler, veri ve kontrol ortamları bütünleşik bir şekilde iç içe geçmiştir. Bu ağlarda cihazlar hem verilerin nasıl işleneceğine karar verir hem de kontrol ve koordinasyonun nasıl olacağına karar verirler. Bu durum büyük ve dinamik ağlarda koordinasyonu zor bir durumu beraberinde getirir. SDN'de ise ağı yöneten merkezi bir denetleyici yardımı ile veri ortamı ve kontrol ortamını birbirinden ayırılarak işlemler basitleştirilir.

2.2. IoT cihazlarda Yazılım Tanımlı Ağlar

IoT cihazların bağlı bulunduğu ağlar çok çeşitliliği, protokolleri ve ağ altyapısından dolayı çeşitli dezavantajları barındırır[10]. Bu zorluklara karşı SDN mimarinde çözümler bulunsa da herkes tarafından kabul edilen ve standartlaştırılmış bir yapı bulunmamaktadır. IoT cihazlarda SDN tabanlı mimarinin çeşitliliği IoT cihazların çok fazla türü ve çok farklı kullanım alanı olmasından kaynaklanmaktadır. Bu nedenle SDN tabanlı IoT cihazlar farklı protokolleri barındırabilmektedir. Diogo ve ark. [11] IoT cihazlar için SDN tabanlı önerdikleri mimari altyapı, kontrol ve uygulama olmak üzere üç katmandan oluşur. Cihazlar, sensörler ve nesneler altyapı katmanında kontrol edilir. Kontrol katmanı, kimlik, güvenlik, erişim, doğrulama gibi sistem kontrollerini yapar. Uygulama katmanı ise operatör ve kullanıcı arasında güvenliği sağlar[11].

2.3. Hizmet Reddi Saldırıları

Tek bir kaynaktan olan hizmet reddi saldırıları Dos olarak adlandırılırken birçok kaynaktan yapılan hizmet reddi saldırıları ise DDos olarak adlandırılmaktadır. Bu saldırılar, ağ, cihaz veya sistemin işleyişini aksatarak iş operasyonlarını kesintiye uğratır. Dos/DDos saldırılarının çalışma prensibi basittir. Ağ trafiği arttırılarak aşırı yükleme yapılır ve sunucu kaynakları yoğun, gereksiz trafik nedeniyle işleyemez hale gelir. Bu sayede rutin iş ve işlemler yapılamaz hale gelir. DDos saldırılarında genellikler saldırganlar birçok cihazı bot denilen zombi bilgisayarlar dönüştürerek saldırmak istedikleri hedefe yönlendirirler. Dod/DDos saldırıların amacı hizmet aksatmak olsa da hizmet akışını bozarak ağ açıklarını bulma, bilgi hırsızlığı gibi amaçlara da hizmet edebilmektedir.

2.4. XGBoost

Temelde karar ağaçlarına dayanan ve gradiyent eğim arttırma metotlarını kullanan yöntemdir. Tüm değerlere bakmak yerine verileri parçalayarak hesaplamalar yapar. Bu, algoritmanın diğer algoritmalara oranla daha performanslı çalışmasını sağlar [12].

2.5. Rasgele Orman

Rasgele orman tekniği ikili ve çoklu sınıflandırma problemlerinde kullanılan ve performanslı çalışan bir tekniktir. Daha az parametre ile daha iyi sonuçlara ulaşılabilir. Rasgele orman algoritmasında ağaç sayısının attırılmasından optimal ağaç sayısının belirlenmesi önemlidir. Sınıflandırmalarda düğümü sonlandıracak bir karar gelene kadar düğüm dallanmaya devam eder. Düğümler ve dallar nihayetinde bir eşit noktasında tahmin yapılır [13].

2.6. Gradyan Arttırıcı

Zayıf olasılıkların bir araya getirilerek karar ağaçlarının oluşturulduğu, bu sayede modelin genel hatasının azaltıldığı yöntemdir. Karar ağaçlarında olduğu gibi düğüm ve dallardan oluşur. Daha iyi sonuç veren düğümler izlenerek tahmin yapılır. [14].

2.7. Karar Ağaçları

Değişkenlere özellikler hakkında bir takım yönlendirici sorular sorarak düğümler oluşturulur. Her düğüm ve soru bir alt düğüme yönlendirme yapar. Bu şekilde hiyerarşik bir yapı oluşturularak tahmin yapılır [15].

2.8. Derin Öğrenme Modeli

Derin öğrenme yapay sinir ağlarını kullanır. Bu sinir ağları canlılardaki sinir ağlarına benzer. Yapay sinir ağları veri analizi, tahmin, olasılık ve birçok görevi yerine getirmek için çok karmaşık ve katmanlı yapı kullanır. Derin sinir ağları makine öğreniminin bir alt dalıdır. Derin öğrenme yöntemleri ile çok büyük veriler analiz edilebilir. Derin öğrenme algoritmaları bu veriler üzerinde

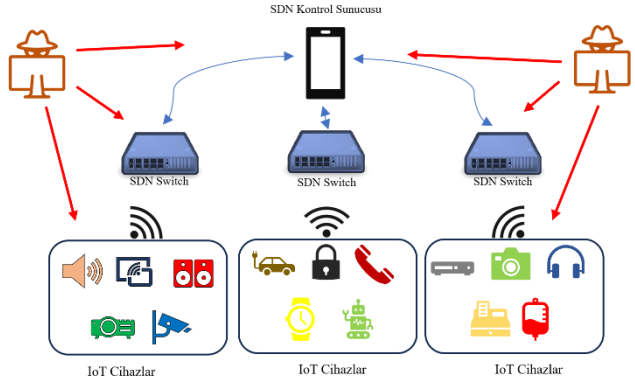
öğrenme yaparak ilerler. Yaygın olarak Evrişimli sinir ağları (CNN), Derin sinir ağları (DNN), Tekrarlayan sinir ağları (RNN), Uzun-kısa süreli Bellek Sinir Ağları (LSTM) kullanılmaktadır. Derin öğrenme teknikleri görüntü işleme, doğal dil işleme, oyun ve yapay zekâ, sağlık, robotik ve birçok alanda etkin olarak kullanılmaktadır [16], [17], [18] , [19] , [20].

Şekil 3'te bu çalışmada önerilen derin öğrenme modeline ait sinir ağı ve katman yapısı gösterilmiştir.

```
Model: "sequential_2"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 conv1d_4 (Conv1D)           (None, 29, 1)             2

 conv1d_5 (Conv1D)           (None, 29, 16)            32

 batch_normalization_4 (Batc  (None, 29, 16)           64
 hNormalization)

 max_pooling1d_2 (MaxPooling  (None, 14, 16)           0
 1D)

 conv1d_6 (Conv1D)           (None, 12, 32)            1568

 batch_normalization_5 (Batc  (None, 12, 32)           128
 hNormalization)

 conv1d_7 (Conv1D)           (None, 10, 32)            3104

 max_pooling1d_3 (MaxPooling  (None, 5, 32)            0
 1D)

 flatten_1 (Flatten)         (None, 160)               0

 dense_8 (Dense)             (None, 64)                10304

 dense_9 (Dense)             (None, 128)               8320

 dense_10 (Dense)            (None, 1)                 129

=================================================================
Total params: 23,651
Trainable params: 23,555
Non-trainable params: 96
```

Şekil 3. Derin öğrenme tabanlı modele ait sinir ağı yapısı

Bu çalışmada SDN tabanlı IOT cihazlarda Dos/DDos saldırı tespit modeli oluşturulmuştur. Şekil 4'te SDN tabanlı IoT cihazlara yapılabilecek muhtemel saldırı senaryosu gösterilmiştir.



Şekil 4. Muhtemel saldırı senaryosu

Çalışma Intel Core i7-9750H 2,60GHz CPU, 16GB Ram, NVidia GeForce GTX 1650 (4GB), 512 GB SSD donanımlarına sahip bilgisayar kullanılarak gerçekleştirilmiştir. Bilgisayarda Windows 10 Pro 64 Bit işletim sistemi bulunmaktadır.

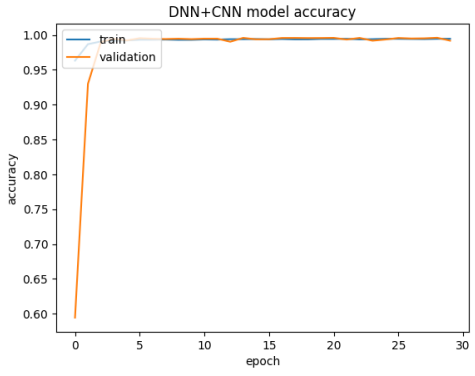
3. BULGULAR

Veri setini işlemek için Python programlama dili tercih edildi. Uygulama aşamasında Tensorflow, Keras, Pandas, Numpy, Matplotlib, Seaborn, Sklearn, Imblearn gibi kütüphaneler kullanılmıştır. Çalışmada kullanılan veri seti [9] %80 eğitim (eğitim setinin %10'u doğrulama (validation)) %20 test olarak kullanıldı. Algoritmaların sonuçları Tablo 1'de verilmiştir. Tablo 1'deki sonuçlara göre hem makine öğrenme algoritmaları hem de derin öğrenme modeli ile başarılı sonuçlar elde edildi.

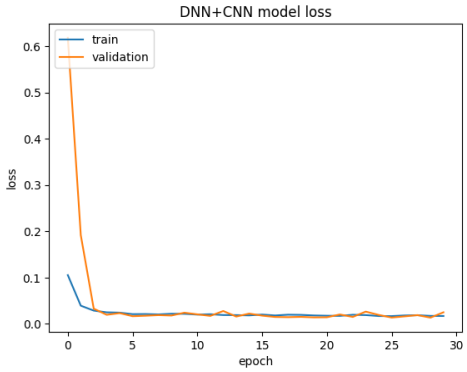
Tablo 1. Algoritma sonuçları

Algoritma	**Precision**	**Recall**	**F1 score**	**CV score**
DNN+CNN	0,99	0,99	0,99	-
Random Forest	0,99	0,99	0,99	0,99
Decision Tree	0,88	0,54	0,67	0,73
XGBoost	0,99	0,99	0,99	0,99
Gradient Boosting	0,99	0,99	0,99	0,99

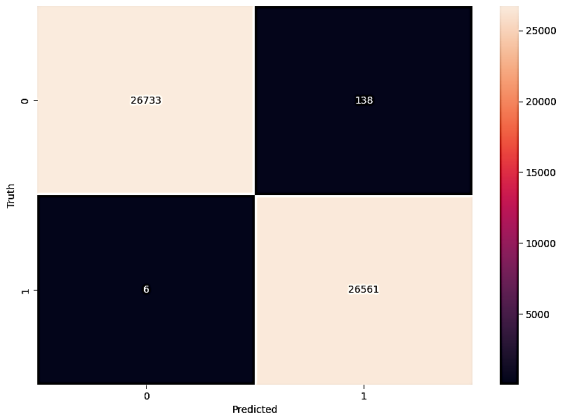
Şekil 4 ve Şekil 5'te derin öğrenme modeline ait accuracy ve loss grafikleri gösterilmiştir. Şekil 6'da derin öğrenme modeline ait karşılaştırma matrisi gösterilmiştir.



Şekil 5. DNN+CNN model accuracy grafiği

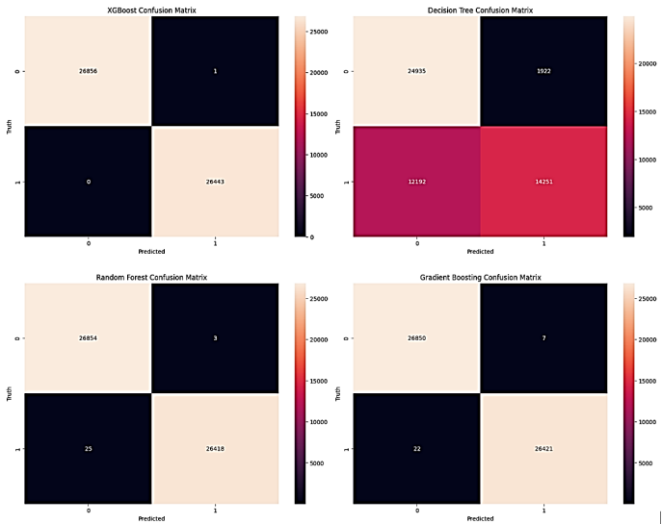


Şekil 6. DNN+CNN model loss grafiği



Şekil 7. DNN+CNN model karşılaştırma matrisi

Şekil 8'da makine öğrenmesi algoritmalarına ait karşılaştırma matrisleri verilmiştir.



Şekil 8. Makine öğrenme algoritmaları karşılaştırma matrisleri

TARTIŞMA

Derin öğrenme tekniklerinin saldırı tespit sistemlerinin oluşturulmasında avantajları olduğu gibi dezavantajları da bulunmaktadır. Derin öğrenme teknikleri çok büyük veri kümelerini analiz ederek öğrenme gerçekleştirebilir ancak bununla birlikte veri kümelerinin iyi hazırlanması, hiper parametre ince ayarlarının yapılması performansı attıracaktır. Ayrıca veri kümelerindeki dengesizlik öğrenme oranını etkilemektedir. Bu modelden ilham alarak gelecekte yapılacak çalışmalarda önerilen saldırı tespitinin geliştirilmesi için hiper parametre ince ayarları ve maliyeti azaltmak için öznitelik seçimi gibi çalışmalar yapılabilir.

SONUÇLAR

SDN tabanlı IoT cihazlara uygulanabilecek Dos/DDos saldırılarının tespit edilmesinde Derin öğrenme tekniklerinin önemli bir yeri vardır. Derin öğrenme teknikleri makine öğrenmesi teknikleri kadar iyi performans gösterir. Bu çalışmada SDN tabanlı IoT cihazlar için hazırlanmış SDN-Veri seti kullanıldı. Oluşturulan veri seti her ne kadar simüle edilerek hazırlansa da veri seti kullanılarak saldırı tespiti açısından çok iyi sonuçlar alındı. Veri setinde kullanılan Derin öğrenme teknikleri ile 0,99 tahmin başarısı elde edildi. Bu çalışmanın sonraki araştırmalar ışık tutmasını umuyoruz. Ayrıca IoT cihazların güvenliğinde yeni çalışmalar yapmak için bu çalışmayı ön adım olarak görüyoruz.

TEŞEKKÜR

Veri setini hazırlayarak kullanıma sundukları için Sarıca ve ark. [9] şükranlarımızı sunuyoruz.

KAYNAKLAR

[1] M. Alsaeedi, M. M. Mohamad, and A. A. Al-Roubaiey, "Toward Adaptive and Scalable OpenFlow-SDN Flow Control: A Survey," *IEEE Access*, vol. 7, pp. 107346–107379, 2019, doi: 10.1109/ACCESS.2019.2932422.

[2] D. Kreutz, F. M. V. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, Jan. 2015, doi: 10.1109/JPROC.2014.2371999.

[3] T. Hasan *et al.*, "Securing industrial internet of things against botnet attacks using hybrid deep learning approach," *IEEE Trans Netw Sci Eng*, 2022.

[4] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in *2016 international conference on wireless networks and mobile communications (WINCOM)*, IEEE, 2016, pp. 258–263.

[5] A. R. Narayanadoss, T. Truong-Huu, P. M. Mohan, and M. Gurusamy, "Crossfire attack detection using deep learning in software defined its networks," in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, IEEE, 2019, pp. 1–6.

[6] M. A. Ferrag, L. Shu, H. Djallel, and K.-K. R. Choo, "Deep learning-based intrusion detection for distributed denial of service attack in agriculture 4.0," *Electronics (Basel)*, vol. 10, no. 11, p. 1257, 2021.

[7] K. Bakour, G. S. Daş, and H. M. Ünver, "An intrusion detection system based on a hybrid Tabu-genetic algorithm," in *2017 International Conference on Computer Science and Engineering (UBMK)*, Ieee, 2017, pp. 215–220.

[8] E. Doğan and H. BAKIR, "Hiperparemetreleri Ayarlanmış Makine Öğrenmesi Yöntemleri Kullanılarak Ağdaki Saldırıların Tespiti," in *International Conference on Pioneer and Innovative Studies*, 2023, pp. 274–286.

[9] A. Kaan Sarica and P. Angin, "A Novel SDN Dataset for Intrusion Detection in IoT Networks," in *2020 16th International Conference on Network and Service Management (CNSM)*, 2020, pp. 1–5. doi: 10.23919/CNSM50824.2020.9269042.

[10] J. Bhayo, S. Hameed, and S. A. Shah, "An Efficient Counter-Based DDoS Attack Detection Framework Leveraging Software Defined IoT (SD-IoT)," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3043082.

[11] P. Diogo, L. P. Reis, and N. V Lopes, "Internet of Things: A system's architecture proposal," in *2014 9th Iberian Conference on Information Systems and Technologies (CISTI)*, 2014, pp. 1–6. doi: 10.1109/CISTI.2014.6877072.

[12] T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," in *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Association for Computing Machinery, Aug. 2016, pp. 785–794. doi: 10.1145/2939672.2939785.

[13] A. Sekulić, M. Kilibarda, G. B. M. Heuvelink, M. Nikolić, and B. Bajat, "Random forest spatial interpolation," *Remote Sens (Basel)*, vol. 12, no. 10, May 2020, doi: 10.3390/rs12101687.

[14] A. Abraham, P. Dutta, J. K. Mandal, A. Bhattacharya, and S. Dutta, "Emerging technologies in data mining and information security," *Proceedings of IEMIS-2018*, 2018.

[15] C. Kingsford and S. L. Salzberg, "What are decision trees?," *Nat Biotechnol*, vol. 26, no. 9, pp. 1011–1013, 2008, doi: 10.1038/nbt0908-1011.

[16] H. Bakır and R. Bakır, "DroidEncoder: Malware detection using auto-encoder based feature extractor and machine learning algorithms," *Computers and Electrical Engineering*, vol. 110, p. 108804, 2023, doi: https://doi.org/10.1016/j.compeleceng.2023.108804.

[17] R. Ghanem, H. Erbay, and K. Bakour, "Contents-Based Spam Detection on Social Networks Using RoBERTa Embedding and Stacked BLSTM," *SN Comput Sci*, vol. 4, no. 4, p. 380, 2023, doi: 10.1007/s42979-023-01798-x.

[18] H. Bakır, A. N. Çayır, and T. S. Navruz, "A comprehensive experimental study for analyzing the effects of data augmentation techniques on voice classification," *Multimed Tools Appl*, 2023, doi: 10.1007/s11042-023-16200-4.

[19] U. Demircioğlu, A. Sayil, and H. Bakır, "Detecting Cutout Shape and Predicting Its Location in Sandwich Structures Using Free Vibration Analysis and Tuned Machine-Learning Algorithms," *Arab J Sci Eng*, 2023, doi: 10.1007/s13369-023-07917-3.

[20] H. Bakır and K. Elmabruk, "Deep learning-based approach for detection of turbulence-induced distortions in free-space optical communication links," *Phys Scr*, vol. 98, no. 6, p. 065521, 2023, doi: 10.1088/1402-4896/acd4fa.