Journal of the Faculty of Engineering and Architecture of Gazi University 37:4 (2022) 1945-1956

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Deep learning and machine learning based anomaly detection in internet of things environments

Ali Gökdemir[1]*, Ali Çalhan[2]

[1]Department of Information Technologies, Zonguldak Vocational and Technical Anatolian High School, 67030, Zonguldak, Turkey
[2]Department of Computer Engineering, Engineering Faculty, Duzce University, 81620, Düzce, Turkey

Highlights:

- Anomaly analysis using deep learning algorithm
- Detection of duplication, interception and modification attacks in the IoT environment
- Evaluation of LSTM algorithm in terms of performance metrics compared to SVM and NB algorithms

Keywords:

- IoT
- Machine learning
- Deep learning
- Anomaly
- IoT security

Article Info:

Research Article
Received: 04.07.2021
Accepted: 14.11.2021

DOI:

10.17341/gazimmfd.962375

Correspondence:

Author: Ali Gökdemir
e-mail: aligokdemir@gmail.com
phone: +90 546 584 8777

Graphical/Tabular Abstract

Classical machine learning and deep learning were compared in detecting attacks on IoT environments. Due to its success in anomaly detection in the literature, Support Vector Machines (SVM) and Naive Bayes (NB) algorithms from classical machine learning algorithms were preferred. As a deep learning algorithm, the Long Short-Term Memory (LSTM) algorithm, which is mostly used in fields such as natural language processing and text processing, and which has very few studies in anomaly detection, has been chosen. With the LSTM algorithm, higher values were obtained in accuracy and f1 scores.

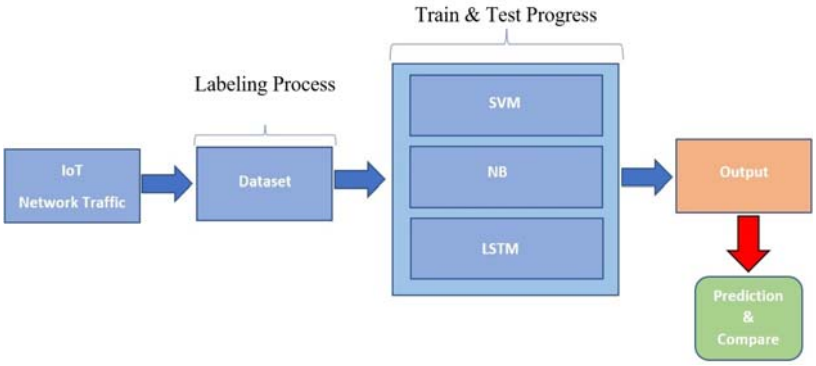


Figure A. Proposed system model for anomaly detection in IoT environments with LSTM-SVM-NB algorithms

Purpose: As the use of Internet of Things (IoT) systems has become widespread, cyber-attacks against these systems have also increased. Cyber-attacks occurring in IoT environments can include different types of attacks, such as the inability of their devices to serve, corruption, data capture, modification, or deletion. In this study, it is tried to predict duplication, interception, and modification attacks in Message Queuing Telemetry Transport (MQTT) messages using an IoT dataset with artificial intelligence techniques.

Theory and Methods:
In this study, compared to the performance metrics of SVM and NB, which are machine learning algorithms, and LSTM, which is a deep learning algorithm.

Results:
Experimental results show that the LSTM algorithm can be used in anomaly detection in the cyber security area, apart from natural language processing and text processing, which are the areas widely used in the literature. Besides, it was concluded that the LSTM algorithm achieved higher accuracy than the classical machine learning algorithms.

Conclusion:
In this paper, a comparison of deep learning and machine learning algorithms for anomaly detection in IoT environments is made. The results show that the LSTM algorithm, gives more effective results in anomaly detection than classical machine learning algorithms, but has some disadvantages in terms of working time.

Journal of the Faculty of Engineering and Architecture of Gazi University 37:4 (2022) 1945-1956

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Nesnelerin interneti ortamlarında derin öğrenme ve makine öğrenmesi tabanlı anomali tespiti

Ali Gökdemir[1]*, Ali Çalhan[2]

[1]Zonguldak Mesleki ve Teknik Anadolu Lisesi, Bilişim Teknolojileri Alanı 67030 Zonguldak, Türkiye
[2]Düzce Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 81620, Düzce, Türkiye

Ö N E Ç I K A N L A R

- Derin öğrenme algoritması kullanarak anomali analizi
- IoT ortamında çoğaltma, müdahale ve değişiklik saldırılarının tespiti
- LSTM algoritmasının SVM ve NB algoritmalarına göre performans metrikleri açısından değerlendirilmesi

Makale Bilgileri

Araştırma Makalesi
Geliş: 04.07.2021
Kabul: 14.11.2021

DOI:
10.17341/gazimmfd.962375

Anahtar Kelimeler:
IoT,
makine öğrenmesi,
derin öğrenme,
anomali,
IoT güvenliği

ÖZ

Internet ve kablosuz haberleşme teknolojilerinin gelişmesi paralelinde IoT alanında yapılan çalışmalar da ilerlemektedir. Sağlık alanında kullanılan IoT sensörleri ile hastaları yakından takip etmek kolaylaşmaktadır. Ayrıca hastalardan toplanan verilerle tedavi sürecine destek sağlayacak istatistiklerin oluşturulması sağlanabilmektedir. Ancak sağlanan imkanların yanında kablosuz iletişim kuran ve internete bağlı olan IoT cihazlarının güvenlik gibi birtakım sorunları da bulunmaktadır. Sağlık çevrelerinde kullanılan IoT'nin farklı katmalarına yönelik yapılan saldırılar neticesinde ciddi sorunlar oluşabilmektedir. Sağlık alanındaki hassas verilerin bu saldırılardan herhangi birine maruz kalmasıyla, verilerin yetkili kullanıcıların erişemeyeceği şekilde değiştirilmesi veya saldırgan tarafından ele geçirilmesi gibi olumsuz sonuçları olabilmektedir. Bu makalede, IoT ağlarında gerçek dünya davranışlarını içeren eksiksiz ve etiketli bir IoT veri kümesi kullanarak Message Queuing Telemetry Transport (MQTT) mesajında çoğaltma, müdahale ve değişiklik saldırılarını yapay zekâ teknikleri kullanarak tahmin etmeye çalışılmıştır. Kullanılan veri seti üzerinde SVM algoritması Doğruluk %85, f1 %98, Duyarlılık %100 olarak; Naive Bayes (NB) algoritması Doğruluk %89, f1 %86, Duyarlılık %100 olarak; LSTM Kayıp %6,7, Doğruluk %98, f1 %98, Duyarlılık %98 olarak iyileştirme yapmıştır. Anormal davranışların tespitinde bir derin öğrenme algoritması olan LSTM algoritması düşük kayıp ve yüksek doğruluk verisi ile mevcut makine öğrenimi yaklaşımlarından daha iyi performans göstermiştir.

Deep learning and machine learning based anomaly detection in internet of things environments

H I G H L I G H T S

- Anomaly analysis using deep learning algorithm
- Detection of duplication, interception and modification attacks in the IoT environment
- Evaluation of LSTM algorithm in terms of performance metrics compared to SVM and NB algorithms

Article Info

Research Article
Received: 04.07.2021
Accepted: 14.11.2021

DOI:
10.17341/gazimmfd.962375

Keywords:
IoT,
machine learning,
deep learning, anomaly,
IoT security

ABSTRACT

In parallel with the development of Internet and wireless communication technologies, studies in the field of IoT are also progressing. With the IoT sensors used in the healthcare field, it becomes easier to follow the patients closely. In addition, it is possible to create statistics that will support the treatment process with the data collected from the patients. However, besides the provided facilities, IoT devices that communicate wirelessly and are connected to the internet also have some problems such as security. Serious problems can occur as a result of attacks on different layers of IoT, which is used in healthcare environments. Exposure of sensitive data in the field of Health to any of these attacks can have negative consequences, such as changing the data out of reach of authorized users or capturing it by an attacker. This article attempts to predict duplication, interception, and modification attacks in Message Queuing Telemetry Transport (MQTT) message using artificial intelligence techniques using a complete and labeled IoT dataset containing real world behaviors in IoT networks. On the dataset used, SVM algorithm has Accuracy 85%, f1 98%, Recall 100% values; Naive Bayes (NB) algorithm has Accuracy 89%, f1 86%, Recall 100% values; LSTM has Loss 6.7%, Accuracy 98%, f1 98%, Recall 98%. The LSTM algorithm, which is a deep learning algorithm in detecting abnormal behaviors, has performed better than existing machine learning approaches with low loss and high accuracy data.

*Sorumlu Yazar/Yazarlar / Corresponding Author/Authors : *aligokdemir@gmail.com, alicalhan@duzce.edu.tr / Tel: +90 546 584 8777

1. GİRİŞ (INTRODUCTION)

Cihazların internet üzerinden birbirlerine bağlanarak etkileşim halinde olduğu göz alıcı bir teknoloji olan Nesnelerin İnterneti (IoT), birbirine bağlı olan cihazlarla veri alışverişi yapan sensörler, elektronik devreler ve yazılımın beraber çalıştığı fiziksel sistemlerdir [1]. Hızla gelişen IoT teknolojisi daha önce erişilemez olan ortamlarda çalışabilen çok çeşitli ve uygun maliyetli sensörlerin ve yazılımların geliştirilmesine neden olmuştur [2]. IoT çevrelerinde kullanılan sensörlerin kullanım alanları oldukça yaygın hale gelmiştir. Bunların başında akıllı şehirler, akıllı ulaşım, akıllı tarım, akıllı sağlık sistemleri gelmektedir. Bununla beraber, IoT cihazları kablosuz ortam üzerinden veri iletimi gerçekleştirdiğinden IoT cihazları ve IoT çevreleri siber saldırılar için kolay bir hedeftir [3]. IoT çevrelerinde kullanılan sensörler ve diğer cihazlar daha geniş bir alana yayılmış olma durumunda, gerçekleştirilecek siber saldırıların daha fazla etkiye sahip olması muhtemel sonuçlardandır [4]. Bu sebeple, siber saldırılardan korunmak için güvenli bir IoT altyapısının tasarlanması gerekmektedir [5]. IoT çevrelerinde kullanılan cihazların yapılandırma ayarları ve güvenlik önlemleri nedeniyle bazı güvenlik açıkları meydana gelebilmekte ve bu sorunlar önemli veri kayıplarına veya izinsiz erişimlere neden olabilmektedir. IoT ekosisteminin gelişmesiyle birlikte bu sistemleri hedef alan düşmanca faaliyetler genişlemekte ve daha şiddetli hale gelmektedir [6]. IoT çevreleri uygulama alanlarına yönelik olarak tasarlanan ve toplanan veriler üzerinden gerçekleştirilen veri analizlerinde, sensörler tarafından izlenen bir sistem içindeki yeni veya olağandışı durumları tanımlamaya ihtiyaç duyulmaktadır. Bu olağan dışı durumlar anomali olarak adlandırılır [7]. Andrew vd. göre IoT bağlamında bir anomalinin genel tanımı; bir sistemin durumundaki beklenmedik bir değişikliğin yerel veya küresel normunun dışında olan ölçülebilir sonuçlarıdır [2].

IoT çevrelerinde anomali durumlarının tanımlanması ve tespiti için veri analizine dayalı makine öğrenmesi, derin öğrenmesi yaklaşımı gibi teknikler kullanılmaktadır. Veri analizine dayalı tekniğin avantajı, diğer metodolojilere göre daha hızlı çalışması ve bilinmeyen tehditlerden kaynaklanan sorunun üstesinden gelebilmesidir [5]. Bu nedenle, bu makalede veri analizine dayalı teknikler kullanılmıştır. Makalenin temel amacı, IoT çevrelerinde gerçekleştirilen müdahale (interception), çoğaltma (duplication) ve değişiklik (modification) saldırılarını tespit edebilen bir model geliştirmektir. Burada, sistemi anormal durumdayken algılayabilen ve koruyabilen Derin öğrenme tabanlı bir çözüm önerilmiştir. Bu görev için, iki makine öğrenimi sınıflandırıcısı ile bir derin öğrenme sınıflandırıcısından yararlanılmıştır. Ardından, makalenin ikinci bölümünde detaylı bir literatür araştırması yapılmıştır. Üçüncü bölümünde anomali yaklaşımı ve türleri anlatılmış hemen sonrasında ise makale kapsamında gerçekleştirilen çalışmalara yer verilmiştir. Dördüncü bölümde elde edilen bulgular gösterilmiş ve son bölüm olan tartışma bölümünde dikkat edilmesi gereken hususlar belirtilmiştir.

2. DENEYSEL METOT (EXPERIMENTAL METHOD)

IoT, insanların ve nesnelerin herhangi bir ağı kullanarak, herhangi bir bilgiyi veya veriyi iletmesine olanak sağlamasıdır [8]. Sağlık alanında kullanılan IoT teknolojisi ile Elektrokardiyografi (EKG)'nin yorumlanması, X-Ray kullanarak hastalık tespiti, genomik verilerde örüntü bulma, kanser tespiti için otomatik bir patolojik sistem, beyin sinyali modellemesi gibi tüm bu karmaşık çalışmalar yerine getirilebilmektedir [5]. Aikaterini vd. yapmış olduğu çalışmada, Dağıtılmış Hizmet Reddi (DDoS) gibi siber saldırıların tespiti için tüm ağ altyapısını verimli bir şekilde izlemeyi amaçlayan dağıtılmış bir algılama sistemi (GNN) önermişlerdir. Önerdikleri sistemde, işbirlikçi doğadan yararlanmak için her bir IoT aracına grafik sinir ağı modeli uygulamışlardır. Bu modelde IoT cihazları, yazılım tanımlı ağ (SDN) ileticileri, Fog Nodes gibi aktif ağ düğümlerinde monitörler kullanmışlar, anormallik tespiti için bant genişliği ve güç tüketimi gibi tahsis edilen kaynakların dağılımını incelemişlerdir. Önerilen GNN sistemi Random Forest (RF), Destek Vektör Makinesi (SVM) ve Decision Tree algoritmalarına göre daha iyi sonuçlar vermiştir [6].

Yusuf Furkan Yavuz vd. [9] Routing ataklarının derin öğrenme tabanlı tespiti üzerinde bir çalışma yapmışlardır. Çalışmalarında daha gerçekçi bir IoT ortamı oluşturmak için Contiki/Cooja simülasyon yazılımı üzerinde 1000 düğüm ile IoT Yönlendirme Saldırısı Veri Seti (IRAD) adında bir veri seti üretmişler ve Versiyon numarası değişikliği ile Hello Flood ataklarını incelenmişlerdir. Elde ettikleri PCAP dosyası üzerinde normalizasyon işlemleri yaparak yönlendirme (routing) saldırılarını tespit etmişlerdir.

Swarna Priya vd. [10] öngörülemeyen siber saldırıları sınıflandırmak ve tahmin etmek için IoMT ortamında etkili ve verimli izinsiz giriş tespit sistemi (IDS) geliştirmek için derin bir sinir ağı (DNN) kullanmıştır. DNN sonuçları ile diğer makine öğrenme algoritmalarını kapsamlı bir şekilde karşılaştırmışlar ve DNN'nin En Yakın Komşuluk (KNN), Naive Bayes (NB), Rastgele Orman (RF), SVM'ye göre ortalama olarak doğrulukta %15, zaman karmaşıklığında ise %30 daha iyi bir performans verdiğini tespit etmişlerdir. Olivier Brun vd. [11] IoT bağlantılı bir ev ortamına yönelik siber güvenlik tehditlerini analiz etmek için rastgele sinir ağlarına (RNN) dayalı bir yaklaşımın ilkelerini ve tasarımını sunmuştur. Çalışmada IoT ağ geçitlerine karşı başlatılabilecek ağ saldırılarını analiz edilip, bunları tespit edilmesi için ilgili metrikleri belirlenmiştir. Veri paketleri incelenerek geliştirilen RNN modelinin saldırıları doğru şekilde algıladığını ortaya koymuşlardır.

Eirini Anthi vd. [12] IoT cihazlarına yönelik Hizmet Reddi (DoS) saldırılarının tespiti için bir model geliştirmiştir. 4 gün boyunca IoT cihazları Wireshark programı ile izlenmiş, veri toplanmış ve sonra bir veri seti hazırlanmıştır. DoS saldırılarının tespiti için makine öğrenmesi sınıflandırıcıları kullanılmıştır. A. Diro vd. [13] IoT çevrelerine saldırıların tespit edilmesini sağlamak için derin öğrenme modelini

önermişlerdir. Derin öğrenme modelinin performansı, geleneksel makine öğrenme yaklaşımları ile karşılaştırılmıştır. Elde edilen sonuçlar derin öğrenme modeli kullanan sistemin daha üstün olduğunu göstermiştir.

Mahmudul Hasan vd. [5] IoT sistemlerindeki saldırıları ve anormallikleri doğru bir şekilde tahmin etmek için çeşitli makine öğrenimi modellerinin performansları karşılaştırmıştır. Kullanılan makine öğrenimi algoritmaları (ML) Lojistik Regresyon (LR), SVM, Karar Ağacı (DT), RF ve Yapay Sinir Ağı (ANN)'dır. Performans karşılaştırmasında kullanılan değerlendirme metrikleri doğruluk (accuracy), kesinlik (precision), duyarlılık (recall), f1 skoru ve alıcı çalışma karakteristik eğrisi altındaki alandır. Sistem Karar Ağacı, Rastgele Orman ve Yapay Sinir Ağı için %99,4 test doğruluğu elde etmiştir. Kullanılan teknikler aynı doğruluğa sahip olsa da diğer ölçümler Rastgele Orman'ın nispeten daha iyi performans gösterdiğini ortaya çıkarmıştır.

Özlem vd. [14] trafik ağlarında anomali tespiti yapmak için bir yöntem önermiştir. Önerdikleri yöntemde karar ağacı algoritmasını kullanmışlardır. Ayrıca önerdikleri yöntemi Britanya Kolumbiyası'nın 2016 yılına ait bir trafik veri setini (trafik kazaları, çalışma faaliyetleri, yol koşulları) kullanarak test etmişlerdir. Karar ağaçları ile anomali tespitinin uygulaması kısmında Weka'daki J48 algoritması (Java tabanlı) kullanılmıştır. Elde edilen sonuçlar Weka içinde bulunan diğer bir makine öğrenmesi algoritması olan bayes ağları ile de karşılaştırılmıştır. Elde edilen sonuçlar incelendiğinde örneklerin, J48 algoritması kullanılarak %97,69, bayes ağları algoritması kullanılarak %93,96 oranında doğru sınıflandırıldığı görülmüştür.

Çetin Kaya vd. [15] yapmış oldukları çalışmada anomali olmayan davranışları tespit etmede, karar ağaçları sınıflandırıcısının diğer makine öğrenmesi sınıflandırıcılara oranla daha başarılı olduğu sonucuna varmıştır. Aynı çalışmada DOS saldırısının tespitinde karar ağaçları, YSA ve KNN algoritmalarının %100'e yakın olumlu sonuca ulaştığını belirtmişlerdir. Çalışmalarında probe saldırılarının tespitinde KNN, DT ve YSA'nın daha iyi sonuç verdiği ortaya konmuştur. Yine aynı çalışmada yerelden uzağa (R2L) ve kullanıcıdan köke (U2R) saldırıları özelinde Naive Bayes haricindeki sınıflandırıcıların daha yüksek sonuçlar verdiği tespit edilmiştir.

Vital Ford [16], istenmeyen e-posta algılama, virüs algılama gibi karmaşık alanlardaki çeşitli zorlukların üstesinden gelmek için makine öğrenimi uygulamalarının öneminden bahsetmiştir.

Teik-Toe vd. [17] kötü amaçlı yazılım saldırısı veri kümesini araştırmış ve benzersiz bir Bulanık K-Ortalama (FKM) kümeleme algoritması geliştirmiştir. FKM Algoritması ile anomaliyi tespit edebilen bir model sunmuşlardır. FKM algoritması ile lineer regresyon karşılaştırılması yapılmış ve %85'e %90 oranında daha fazla doğruluk oranı elde edilmiştir. Kallol vd. [18] yapmış oldukları çalışmada akıllı sağlık ağ altyapıları için bir güvenlik mimarisi önermektedir: Mimari, sanal ağ işlevleri olarak geliştirilen ve dağıtılan çeşitli güvenlik bileşenlerini veya hizmetlerini kullanır. Bu güvenlik mimarisinde, yalnızca kimliği doğrulanmış ve güvenilir IoMT cihazları hastalara şifreleme tabanlı bir iletişim protokolü ile hizmet vererek, gizliliği koruyan ve güvenilir bir sağlık hizmeti ağı altyapısı oluşturulmaktadır.

Jean Paul vd. [19], bilinen saldırıların zararlarını azaltmanın ve hastaların mahremiyetini korumanın yanı sıra, saldırıları tespit etmek ve önlemek için beş farklı katmana bölünmüş bir güvenlik çözümü önermiştir. Çalışmalarında IoMT cihazlarının kablosuz iletişim protokollerinin güvenliliğin sağlanması ve siber saldırılardan korunması için çalışanların eğitilmesi gerektiğini ortaya koymuşlardır.

Mohammad Wazid vd. [20], IOT/IOMT haberleşme ortamında zararlı yazılım tespit şemalarının karşılaştırmalı bir çalışmasını yapmışlardır. Buna göre kesinlik (precision), duyarlılık (recall), doğruluk (accuracy) ve f1-skoru hesaplanması gerekliliğinden bahsetmişlerdir.

Yukarıda bahsedilen çalışmalar, makine öğrenmesi ve derin öğrenme algoritmalarının sınırlı ve izole ağlarda kullanılmasının umut verici bir potansiyelinin olduğunu ortaya koymaktadır. Daha çok doğal dil işleme ve metin işleme gibi tekniklerde kullanılan, tekrarlayan sinir ağları tabanlı LSTM gibi derin öğrenme algoritmalarının siber güvenlik çerçevesindeki anomali tespitinde kullanılması önemlidir. Geliştirilen modelin klasik makine öğrenmesi algoritmalarına göre kullanım avantajlarını ve dezavantajlarını ortaya koyması diğer araştırmacılara yol gösterecektir.

2.1. Anomali Yaklaşımı (Anomaly Approach)

Anomali tabanlı saldırı tespit sistemlerinde tercih edilen yöntemler arasında enformasyon teorisi, sınıflandırma tabanlı, istatistiksel anomali tabanlı, kümeleme tabanlı ve en yakın komşu tabanlı yöntemler bulunmaktadır [21]. Bu çalışmada sınıflandırma tabanlı anomali yaklaşımı üzerinde durulmuştur.

2.1.1. Sınıflandırma tabanlı anomali yaklaşımı (Classification based anomaly approach)

Farklı türdeki problemler için farklı sınıflandırma yaklaşımı geliştirilmiş olmasına rağmen, bu makalede sadece sunucu tabanlı (host based) yaklaşımlar incelenmiştir.

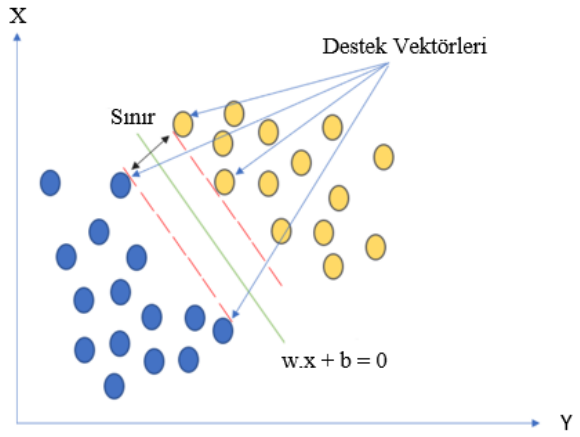
2.1.1.1. Destek vektör makineleri (SVM) sınıflandırıcı modeli (Support vector machines (SVM) classifier model)

Destek vektör makineleri, iki ayrı sınıfa ait verileri, birbirinden uygun bir şekilde ayırmak için kullanılan bir makine öğrenmesi algoritmasıdır. Yapısal risk azaltma ilkesine dayalı olarak geliştirilmiştir [22]**.** Denetimli makine öğrenmesi algoritma sınıfına giren SVM algoritmasında veri etiketleme yapılır. SVM kendine girdi olarak gelen verileri 2 sınıfa (anomali veya anomali değil) ayırmaktır. Şekil 1'de

kesikli çizgilerle gösterilen vektörler destek vektörü olarak isimlendirilir. Ayrım çizgisi de bu vektörler üzerinden geçer. İki ayrım çizgisinin ortasındaki doğru fonksiyonu Eş. 1 ile hesaplanarak çizilir [23].

$$f(\vec{x}) = \vec{w}^T \vec{x} + b = 0 \quad (1)$$

Denklemde "*w*" ve "*x*" vektörel büyüklüktür.



Şekil 1. SVM algoritma sınıflandırıcı modeli gösterimi (SVM algorithm classifier model representation)

Subbulakshmi vd. [24], Dağıtılmış Hizmet Reddi (DDoS) saldırılarına karşı Derin öğrenme ve SVM kullanan bir Sınıflandırma Sistemi geliştirmiştir. Geliştirilen Snort adlı sistem derin öğrenme kullanan sınıflandırıcının ortalama doğruluğu %83 olarak hesaplanmışken, bu oran destek vektör makineleri için %99 olarak hesaplanmıştır.

H. Sedjelmaci ve Feham [25], izinsiz girişin tespiti için kablosuz sensör ağında SVM sınıflandırma algoritmasından yararlanmışlardır. Hizmet Reddi (Denial of Service) ve Probe saldırıları özelinde yapılan çalışmada %98 doğruluk ve %95 tespit oranı elde edilmiştir.

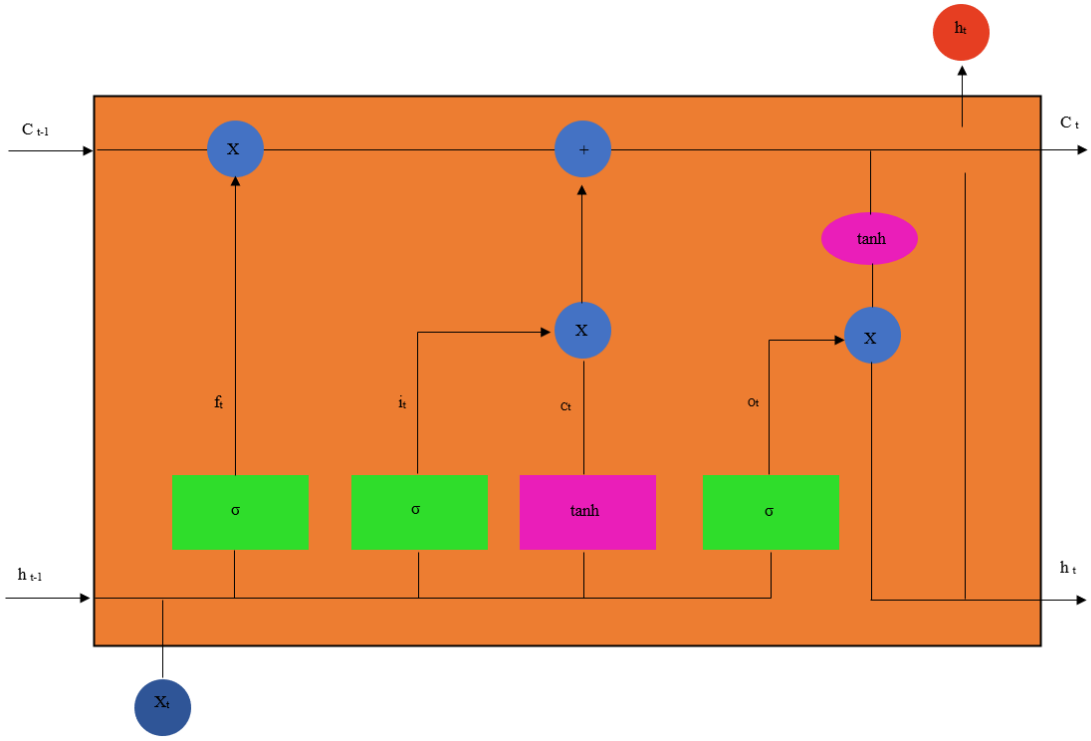
2.1.1.2. Naive Bayes Sınıflandırıcı Modeli
(Naive Bayes Classifier Model)

NB sınıflandırıcı, basitliği ile bilinen yaygın olarak kullanılan bir denetimli sınıflandırıcıdır [26]. NB sınıflandırıcısı, daha önce gerçekleşmiş bir olayın olasılığı verildiğinde, başka bir olayın olma olasılığını bulur. Bayes teoremi matematiksel olarak Eş. 2 ile ifade edilir.

$$P(M \mid N) = (P(N \mid M)P(M))/(P(N)) \quad (2)$$

NB, temel olarak, N olayının doğru olduğu veya halihazırda meydana geldiği göz önüne alındığında, M olayının gerçekleşme olasılığını bulmaya çalışmaktadır. Eşitlikteki;

- *P (M|N)*, N olayı gerçekleştiğinde M olayının gerçekleşme olasılığını
- *P(M)*, M olayının gerçekleşme olasılığını
- *P(N|M)*, N olayı gerçekleştiğinde M olayının gerçekleşme olasılığını
- *P(N)*, N olayının gerçekleşme olasılığını temsil etmektedir.



Şekil 2. LSTM mimari yapısı (Structure of LSTM)

Literatürde izinsiz giriş tespiti için trafiği normal veya anormal olarak sınıflandırmak için Naive Bayes sınıflandırıcısı sıklıkla kullanılmaktadır. Bayesian ağının hesaplama süresi düşük olduğu ve veri setinin çok büyük oldu durumlarda NB sınıflandırıcısını kullanmak verimli olacaktır [27]. David vd. [28] tek bir sensör veri akışı üzerinde çalışabilir veya birleştirilmiş anormallik tespiti gerçekleştirmek için yaptıkları çalışmada NB anomali dedektörünün veriler üzerinde hatalı verileri belirlemede %0,80 yanlış pozitif (false positive) ve %0,16 yanlış negatif (false negative) oranları ile iyi performans gösterdiğini ortaya koymuşlardır.

Mayank ve Neminath [29], HTTP saldırılarını algılamak için bir sınıf Çok Terimli Naive Bayes sınıflandırıcısını anomali dedektörü olarak uyarlamışlardır. OCPAD (Veri yükü tabanlı anomali için bir sınıf Naive Bayes sınıflandırıcı tespit etme) adını verdikleri sistemde Akademik bir ağdan toplanan 1 milyon HTTP paketinden oluşan büyük bir veri kümesiyle yaptıkları deneyler sonucunda, OCPAD' in yüksek bir algılama oranına (%100'e kadar) ve %0,6'dan az yanlış pozitif oranına sahip olduğunu ortaya çıkarmışlardır.

2.1.1.3. LSTM sınıflandırıcı modeli (LSTM classifier model)

Uzun Kısa Vadeli Bellek (Long Short Term Memory) modeli 1997 yılında Hochreiter ve Schmidhuber tarafından geliştirilmiştir [30]. LSTM algoritması uzun vadeli bağımlılıkları öğrenebilen özel bir RNN algoritması türüdür. LSTM algoritmasına ait mimari yapı Şekil 2'de gösterilmiştir.

LSTM mimarisinde kapı olarak adlandırılan birtakım yapılar bulunmaktadır. Bu yapılar sinir hücresine bilgi ekleme ve çıkarma gibi görevleri yerine getirmektedir [30]. LSTM yapısında bulunan kapılar ve görevleri şunlardır:

Unut Kapısı (f_t): Önceki çıkış ile o anlık giriş arasında bir analiz yaparak 0 ile 1 arasında bir değer üretmektedir.
Giriş Kapısı (i_t): Hangi yeni değerlerin saklanacağına karar veren yapıdır.
Çıkış kapısı (o_t): Eski verilerin bir sonraki hücreye aktarılmasını sağlayan yapıdır.

Ayrıca hafıza hücreleri ise $\boldsymbol{c_t}$ olarak isimlendirilmiştir.

LSTM mimarisi kullanılarak konuşma/metin işleme gibi konularda yapılan çalışmalarda oldukça iyi sonuçlar verdiği görülmektedir [31]. Alex vd. [32] 32 binden fazla elle yazılmış karakterleri tespit etmede LSTM sınıflandırıcısından yararlanmış ve denedikleri diğer yöntemlere göre daha başarılı sonuçlar almıştır. Zeynep Hilal Kilimci çalışmasında, borsa yönünün tahmin edilmesi amacıyla LSTM algoritmasını performansını karşılaştırmış ve literatürdeki önceki çalışmalardan önemli ölçüde üstün olduğunu ortaya koymuştur [33]. Literatürde LSTM sınıflandırıcı modeli kullanan anomali tespitine rastlanılmamıştır.

2.2. Gerçekleştirilen Çalışmalar (Performed Studies)

Bir IoT cihazı ile sunucu arasında veri güvenliği iyi yapılandırılmamış bir zayıf bağlantı bulunursa, bir saldırgan ağ trafiğine müdahale edebilir ve IoT cihazlarının çeşitli ağlar üzerinden ilettiği hassas derecedeki bilgileri çalınabilir. Bu çalışmada IoT çevrelerine yapılan 3 adet saldırı üzerinde durulmuştur. Bu saldırılar müdahale, çoğaltma ve değiştirme türü saldırılardır.

Müdahale: Bu saldırı, IoT kablosuz altyapılarının gizliliğini tehlikeye atmayı amaçlayan her türlü saldırıyı kapsar. Örneğin, bir saldırgan -bu durumda kulak misafiri olarak adlandırılır- kablosuz trafiği havadan yakalar ve gizli ve özel bilgileri çıkarmak için trafiği analiz eder [34]. Bu uygulamada müdahale saldırısı, gönderilen bazı paketleri rastgele silme olarak nitelendirilmiştir.

Değişiklik: Bu saldırı, kablosuz bir IoT altyapısında mesajların ve depolanan verilerin içeriğini yasa dışı olarak değiştirmeyi amaçlayan her türlü saldırıyı kapsar. Örneğin, bir saldırgan ağ mesajlarını yakalayabilir, içeriklerini değiştirebilir ve ardından henüz bu mesajları almamış olan IoT düğümlerine iletebilir [34]. Bu uygulamada değişiklik saldırısı, gönderilecek sıcaklık verisinin, belirlenmiş modeli takip etmeden değiştirilmesi olarak ele alınmıştır.

Çoğaltma: Bu saldırıda, bir saldırgan kablosuz kanalı duyabilir ve kulak misafiri olan parça ile uyumlu olarak kopya bir parça oluşturur. Çoğaltma saldırısında saldırgan gizlice dinlenen bir parçayı çoğaltır. Daha sonra bu parçayı hedefe doğru gönderir ve parçalanmış paketlerin başarılı bir şekilde işlenmesini bozar [35]. Bu uygulama içinde çoğaltma, başlangıçta planlanan sayıdan daha fazla jeton gönderme olarak ele alınmıştır.

Veri Seti

Bu çalışmada, 2020 yılında Laura vd. tarafından [36] oluşturulan Anomali Tespiti için Veri Seti (DAD) adını verdikleri bir veri seti kullanılmıştır. DAD, belirli gerçek dünya davranışlarının bir kopyasını içeren eksiksiz ve etiketli bir IoT veri kümesidir. Veri setini gerçek bir ortama yaklaştırmak için veriler, Yakın alan iletişimi (NFC) akıllı pasif sensör teknolojisine dayalı sıcaklık sensörleri ile fiziksel bir veri merkezinden elde edilmiştir. NFC, yüksek frekans ve düşük bant genişliği ile kısa mesafeden temassız iletişimi ve bilgi paylaşımını sağlayan bir teknolojidir [37]. Farklı yaklaşımlar uygulandıktan sonra, son olarak zaman serileri kullanılarak matematiksel modelleme yapılması tercih edilmiştir. Veri kümesinin oluşturulması için gerekli sanal altyapı; her biri dahili IoT ağına bağlı dört soğutma ünitesi sensörüne sahip beş sanal makine, bir MQTT aracısı ve dört istemci düğümünden oluşmaktadır. MQTT çalıştığı ağ üzerinde esnek ve hızlı haberleşme yeteneğine sahip aynı zamanda ağ üzerinde çatışmaya sebep olmayan bir iletişim protokolüdür [38]. DAD, beş güne yayılmış anormal paketlerle yedi günlük ağ etkinliğinden oluşan etiketli bir veri kümesidir [36]. Bu veri kümesinde üç farklı anormallik

türü vardır: MQTT mesajında çoğaltma, müdahale ve değişiklik. Yedi günlük veri kümesine ait günlük saldırı dağılımı aşağıda belirtildiği gibidir.

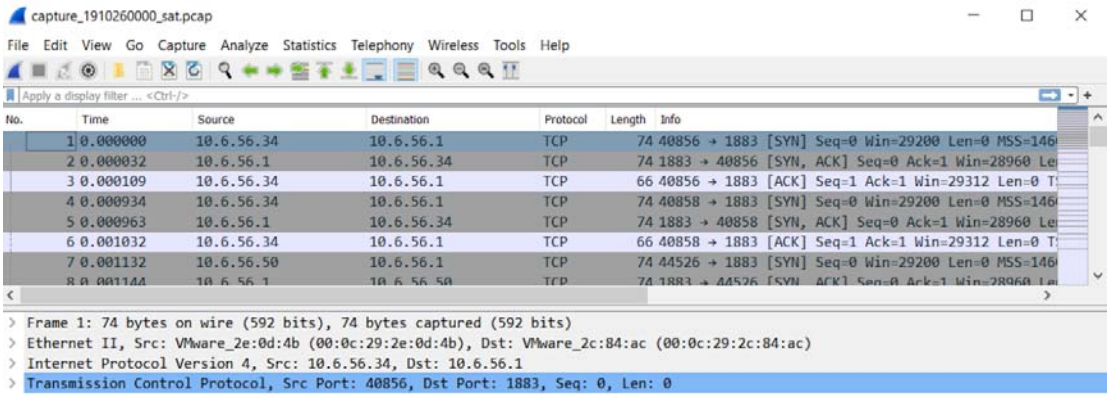
- Pazartesi: Herhangi bir saldırı yapılmadı.
- Salı: Bazı paketler kaldırıldı, bu nedenle paketler saldırı olarak etiketlenmedi.
- Çarşamba: Değişiklik saldırısı saat 4ve 6 arasında yapıldı.
- Perşembe: Araya ekleme (insertion) saldırısı saat 3'te 5 dakikadan daha kısa sürede yapıldı.
- Cuma: Müdahale, çoğaltma ve değişiklik saldırıları karışık olarak saat 14-16 arası yapıldı.
- Cumartesi: Müdahale, çoğaltma ve değişiklik saldırıları karışık olarak saat 14-16 arası yapıldı.
- Pazar: Herhangi bir saldırı yapılmadı.

Geliştiriciler tarafından araştırmacılar için veri setine ait 3 tür dosya üretilmiştir. Bunlar CVS, PCAP ve XML türü dosyalardır. Çalışmamızda, her üç saldırının karışık bir şekilde yapıldığı cuma gününe ait PCAP dosyaları alınarak işlenmiştir. PCAP dosyaları öncelikle Wireshark programı kullanılarak açılmış ve ağ trafiği analiz edilmiştir (Şekil 3).

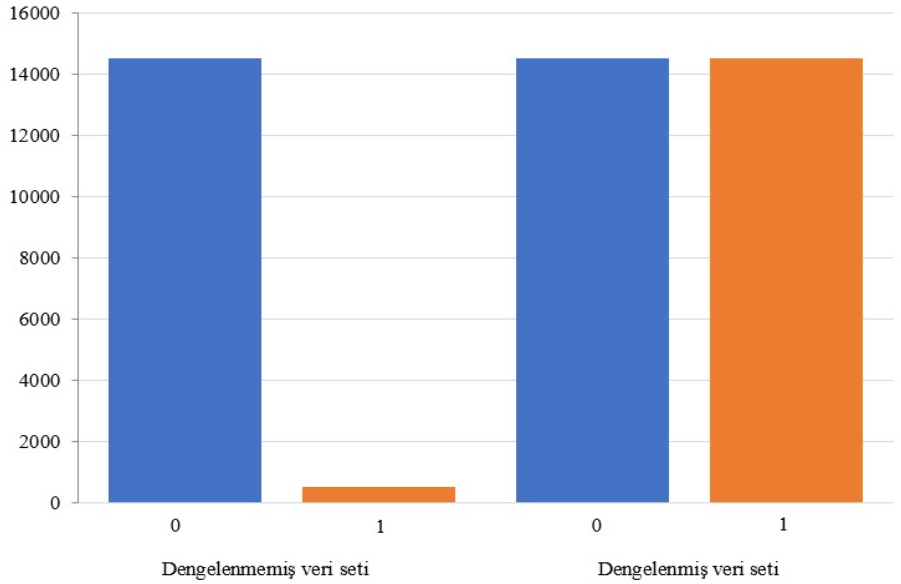
3. DENEYSEL SONUÇLAR (EXPERIMENTAL RESULTS)

Ağ trafiği yeni bir CSV dosyası olarak dışa aktarılmıştır. Elde edilen yeni CSV dosyasına, geliştiriciler tarafından üretilen etiketli CVS dosyasından etiket (label) sütunu alınmış ve kendi elde ettiğimiz yeni CSV dosyasına yeni bir sütun olarak eklenmiştir. Bu şekilde veri seti üretimi tamamlanmıştır.

Veri seti üzerinde makine öğrenme algoritmalarının çalıştırılması için veri seti, sınıf dengesi yapılarak dengeli hale getirilmiştir (Şekil 4). Makine öğrenme algoritmaları ile çalışılırken karşılaşılan en büyük problemlerden biri karar sınıfına ait veri dağılımın dengeli olmamasıdır. Model oluşturulurken azınlıkta olan veri türü (1 ile etiketlenenler) eğitim veri setinde az sayıda ya da hiç yer alamayabilir. Bu durum uygulanan modelin performans ölçümünde yanılgıya sebep olmaktadır [39]. Bu sebeple veri setindeki 1 ve 0



Şekil 3. Wireshark yazılımı kullanılarak ağ analizi ekranı (Network analysis screen using Wireshark software)



Şekil 4. Dengeli olmayan ve dengeli veri seti (Unbalanced and balanced dataset)

etiketli verilerin sayıları eşitlenerek dengeli hale getirilmiştir. Çalışmada, makine öğrenmesi algoritmalarından Naive Bayes (NB) ve Destek Vektör Makinesi (SVM) ile LSTM (Long Short-Time Memory) derin öğrenme algoritması karşılaştırmaları yapılmıştır.

Veri seti dengeli hale getirilmeden önce ve dengeli hale getirildikten sonra NB ve SVM algoritmalarının gösterdiği performans Tablo 1 ve Tablo 2'de gösterilmiştir.

Veri seti üzerinde dengeleme işlemi yapılmadan ve yapıldıktan sonra NB ve SVM algoritmaları kullanılarak yapılan anomali tespitinde alınan Doğruluk, f1 ve Duyarlılık test sonuçları sırası ile Şekil 5 ve Şekil 6'da gösterilmiştir.

Bu sonuçlara göre makine öğrenmesi algoritmalarından olan NB ve SVM algoritmalarında veri seti dengeli hale getirildikten sonra (balanced) hem eğitim (train) hem de test sonuçlarında daha iyi değerler elde edilmiştir.

LSTM derin öğrenme algoritması kullanılarak yapılan anomali analizinin bulguları Tablo 3'te gösterilmiştir.

LSTM derin öğrenme algoritması IoT çevrelerinden elde edilen veri seti üzerinde yapılan anomali tespitinde Doğruluk (accuracy), f1, Duyarlılık (recall) sonuçlarında klasik makine öğrenme algoritmalarına göre daha iyi sonuçlar verdiği bulunmuştur. Sonuçlar Şekil 7'de gösterilmiştir.

Ayrıca modelimizin tahmin ettiği değerler ile etiketlerin gerçek değerleri arasındaki farkın mutlak değerine dayanan kayıp (loss) değeri ise %5'tir (Şekil 8).

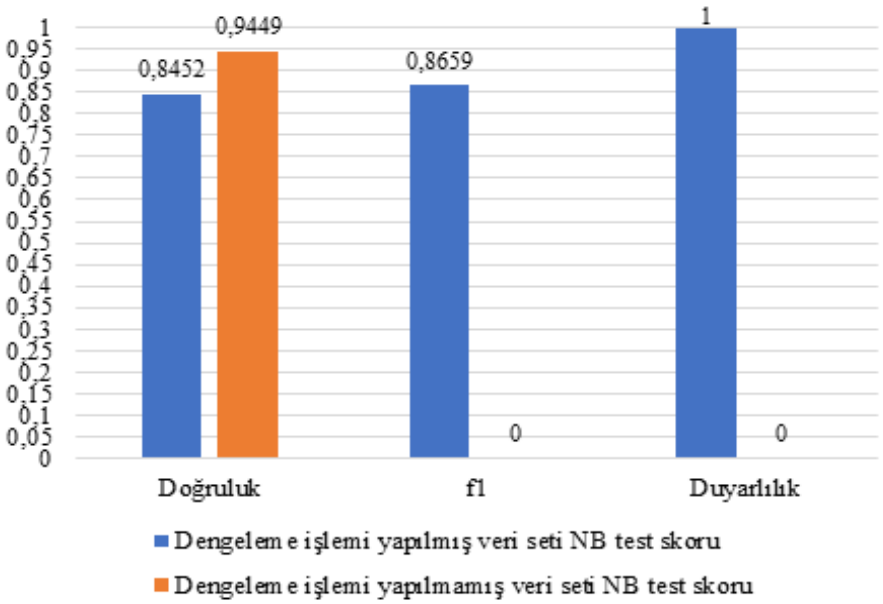
Ancak LSTM derin öğrenme algoritmasının ve klasik makine öğrenme algoritmalarının çalışmaları sırasında geçen süre dikkate alındığında klasik makine öğrenme algoritmalarının daha avantajlı olduğu görülmüştür. LSTM ile SVM ve NB algoritmaların süre açısından karşılaştırmaları Tablo 4'te gösterilmiştir.

Tablo 1. Veri seti dengeli hale getirilmeden önce metrik sonuçları (Metric results before the dataset is balanced)

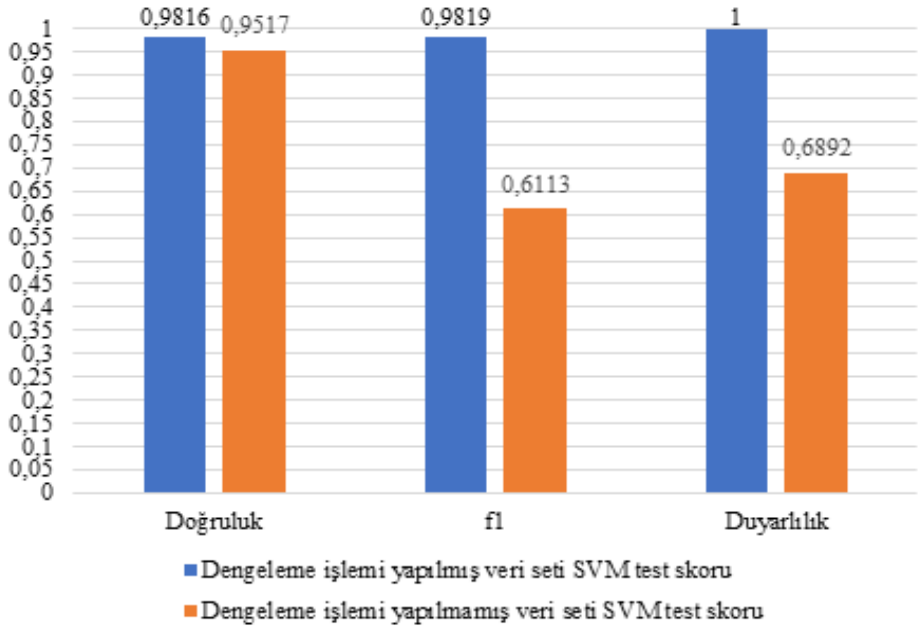
	Doğruluk	f1	Duyarlılık
NB Train Score	0,9514	0,0	0,0
NB Test Score	0,9449	0,0	0,0
SVM Train Score	0,9624	0,6768	08104
SVM Test Score	0,9517	0,6113	0,6892

Tablo 2. Veri seti dengeli hale getirildikten sonra metrik sonuçları (Metric results after data set is balanced)

	Doğruluk	f1	Duyarlılık
NB Train Score	0,8473	0,8675	1,0
NB Test Score	0,8452	0,8659	1,0
SVM Train Score	0,9801	0,9804	1,0
SVM Test Score	0,9816	0,9819	1,0



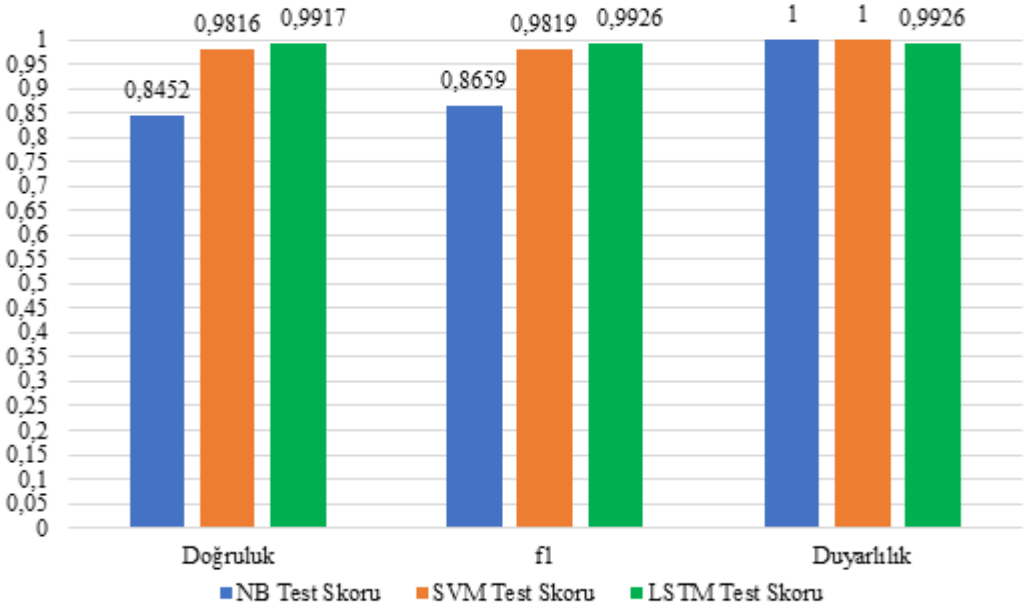
Şekil 5. NB algoritması kullanılarak dengeleme işlemi yapılmış ve yapılmamış veri seti üzerinde Doğruluk, f1 ve Duyarlılık test sonuçları karşılaştırması
(Comparison of Accuracy, f1 and Sensitivity test results on the balanced and unbalanced dataset using the NB algorithm)



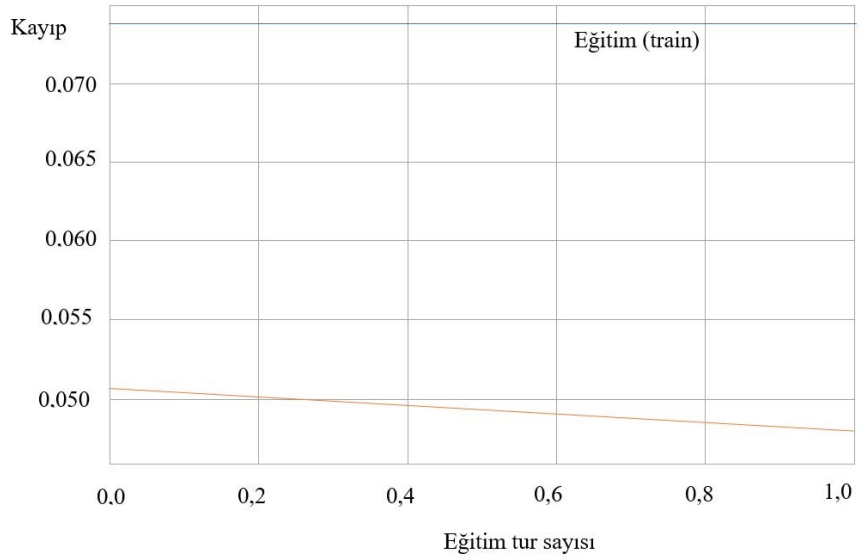
Şekil 6. SVM algoritması kullanılarak dengeleme işlemi yapılmış ve yapılmamış veri seti üzerinde Doğruluk, f1 ve Duyarlılık test sonuçları karşılaştırması
(Comparison of Accuracy, f1 and Sensitivity test results on the balanced and unbalanced dataset using the SVM algorithm)

Tablo 3. Veri seti üzerinde LSTM derin öğrenme algoritması çalıştırılması sonucu metrik sonuçları
(Metric results after running LSTM deep learning algorithm on the dataset)

LSTM	Doğruluk	f1	Duyarlılık	Kayıp	Süre
	0,9917	0,9926	0,9926	0,0503	29,9 sn



Şekil 7. NB, SVM ve LSTM algoritmaları Doğruluk, f1 ve Duyarlılık değerleri karşılaştırmalı sonuçları
(NB, SVM and LSTM algorithms Accuracy, f1 and Sensitivity values comparative results)



Şekil 8. LSTM algoritması eğitim tur sayısı- kayıp grafiği (LSTM algorithm epoch-loss chart)

Tablo 4. LSTM, SVM ve NB algoritmalarının çalışma süresi açısından karşılaştırılması
(Comparison of LSTM, SVM and NB algorithms in terms of runtime)

Kullanılan Algoritma	Çalışma Süresi (sn)
SVM	2,0 sn
NB	2,1 sn
LSTM	29,9 sn

Tablo 5. Dengelenmiş ve dengelenmemiş veri seti üzerinde SVM ve NB algoritmalarının metrik sonuçları
(Metric results of SVM and NB algorithms on balanced and unbalanced dataset)

Makine Öğrenmesi Algoritması	Doğruluk		F1		Duyarlılık	
	Dengelenmemiş V.S.	Dengeli V.S.	Dengelenmemiş V.S.	Dengeli V.S.	Dengelenmemiş V.S.	Dengeli V.S.
NB Train Score	0,9514	0,8473	0,0	0,8675	0,0	1,0
NB Test Score	0,9449	0,8452	0,0	0,8659	0,0	1,0
SVM Train Score	0,9624	0,9801	0,6768	0,9804	8104	1,0
SVM Test Score	0,9517	0,9816	0,6113	0,9819	0,6892	1,0

Tablo 6. Dengelenmiş ve dengelenmemiş veri seti üzerinde LSTM algoritmalarının metrik sonuçları
(Metric results of LSTM algorithms on balanced and unbalanced dataset)

LSTM Algoritması	Doğruluk	F1	Duyarlılık	Kayıp	Süre
Dengelenmiş Veri Seti	0.5411	0.5411	0.5411	0.6643	55.0 sn
Dengelenmemiş Veri Seti	0.9917	0.9926	0.9926	0.0503	29.9 sn

LSTM algoritması da bir derin öğrenme algoritması olduğu için çalışma süresi açısından bir dezavantaja sahiptir. Bunun sebebi eğitim tur sayısı (epoch) ve aynı anda kaç verinin işleneceğine karar veren batch size'den kaynaklanmaktadır. Derin öğrenme tekniklerinde kullanılan bu parametreler klasik makine öğrenme algoritmalarında kullanılmadığından makine öğrenme algoritmaları daha kısa sürede sonuç üretmektedir. Bununla beraber LSTM algoritması ile anomali tespitinde "Doğru Pozitif oranı" ve "Doğruluk oranı" daha yüksek olduğu görülmektedir. IoMT ağlarında LSTM ve diğer derin öğrenme algoritmaların tercih edilmesi ancak kullanılacak modele ait batch size ve epoch sayısını dikkatle test etmesi gerekmektedir.

SVM ve NB üzerinde yapılan çalışmalar klasik makine öğrenmesi algoritmalarında dengeli bir veri setinde çalışmanın olumlu sonuçlar ortaya koyduğunu göstermektedir. Bu durum Tablo 5'te gösterilmiştir. Aynı veri seti üzerinde LSTM algoritması kullanılarak yapılan anomali tespitinde ise tersi bir durum yaşanmıştır. Dengeli hale getirilen veri setinde sonuç metrik değerleri daha düşük çıkmıştır. Bu durum Tablo 6'da gösterilmiştir.

4. SONUÇLAR (CONCLUSIONS)

Veri setini dengelemek için yapılan olumlu (saldırı türü olmayan ve 0 olarak etiketlenen) veriler ile olumsuz (saldırı türü olan ve 1 olarak etiketlenen) veriler sayı olarak eşitlenmesi işlemi ile daha fazla verinin algoritma tarafından analiz edilmesi anlamına gelmektedir. Bu durum süreyi artırmaktadır. Ayrıca Derin öğrenme algoritmalarında dengelenmiş veri setinin görüntü işleme işlemlerinde daha olumlu sonuçlar ürettiğine dair bulgular mevcutken [40], LSTM algoritmasında bu durum anomali tespiti üzerine odaklanan çalışmamızda tersine sonuçlanmıştır. Bu sonuç, derin öğrenme algoritmaları kullanılacak çalışmalarda veri setinin dengelenmesi seçeneğini göz ardı edilebileceğini ortaya koymaktadır.
Bu makalede yapılan çalışma ile literatüre aşağıdaki gibi katkılar sağlanmıştır:

- LSTM algoritmasının literatürde yaygın olarak kullanıldığı alan olan doğal dil işleme ve metin işleme alanları haricinde siber güvenlik alanı anomali tespitinde de kullanılabileceği ortaya çıkartılmıştır.
- Anomali tespitinde LSTM derin öğrenme algoritması ile klasik makine öğrenme algoritmalarının karşılaştırmaları yapılmıştır.
- Anomali tespiti için kullanılan veri setindeki anomali davranışlarının sayısının daha az olması beklenmektedir. Bu sebeple klasik makine öğrenme algoritmalarından olan SVM ve NB algoritmaları kullanılarak anomali tespiti yapılacaksa, veri setinin dengelenmesi gerektiği tespit edilmiştir.
- LSTM algoritmasının klasik makine öğrenme algoritmalarına oranla daha yüksek doğruluğa ulaştığı sonucuna varılmıştır.

KAYNAKLAR (REFERENCES)

1- Atac C., Akleylek S., A Survey on Security Threats and Solutions in the Age of IoT, European Journal of Science and Technology, 15, 36-42, 2019.

2- Cook A., Mısırlı G., Fan Z., Anomaly Detection for IoT Time-Series Data, A Survey, IEEE Internet of Things Journal, 2019.

3- Liu X., Liu Y., Liu A., Yang L.T., Defending on–offattacks using light probing messages in smart sensors for industrial communication systems, IEEE Trans. Ind. Inf, 14 (9), 3801–3811, 2018.

4- Pajouh H.H., Javidan R., Khayami R., Dehghantanha A., Choo K-K.R., A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in iot backbone networks, IEEE Trans. Emerg. Top. Comput, 7 (2), 314-323, 2016.

5- Hasan M., Islam. M.M., Zarif MI., Hashem M.M., Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches, Internet of Things 7, 2019.

6- Protogerou A., Papadopoulos S., Drosou A., Tzovaras D., Refanidis I., A graph neural network method for distributed anomaly detection in IoT, Evolving Systems 12, 19-36, 2021.

7- Chandola, V., Banerjee, A., Kumar, V., Anomaly detection: A survey. ACM computing surveys (CSUR), 41 (3), 15, 2007.

8- Butt S.A., Arshad A., Martinez L.D., IoT Smart Health Security Threats Shariq, 2019 19th International Conference on Computational Science and Its Applications (ICCSA), 26-31, 2019.

9- Yavuz F.Y., Ünal D., Gül E., Deep learning for detection of routing attacks in the internet of things, Int J Comput Intell System 12 (1),39-58, 2018.

10- Swarna Priya R.M., Maddikunta P.K.R., Parimala M., Koppu S., Gadekallu T.R., Chowdhary C.L., Alazab M., An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture, Computer Communications 160, 139-149, 2020.

11- Brun O., Yin Y., Gelenbe E., Kadioglu Y.M., Gonzalez J.A., Ramos M., Deep Learning with Dense Random Neural Networks for Detecting Attacks Against IoT-Connected Home Environments, Security in Computer and Information Sciences, 79-89, 2018.

12- Anthi, E., Williams, L., Burnap, P., Pulse: an adaptive intrusion detection for the internet of things, Living in the Internet of Things: Cybersecurity of the IoT, 1-4, 2018.

13- A. Diro, N. Chilamkurti, Distributed attack detection scheme using deep learning approach for Internet of Things, Future Generation Computer Systems, 82, 761-768, 2017.

14- Örnek Ö., Vatan S., Sarıoğlu S., Yazıcı A., Trafik Ağlarında Anomali Tespiti, The Journal of Engineering and Architecture Faculty of Eskisehir Osmangazi University 26 (5), 132-138, 2018.

15- Kaya Ç., Yıldız O., Performance Analysis of Machine Learning Techniques in Intrusion Detection, 24th Signal Processing and Communication Application Conference (SIU), 1473-1476, 2016

16- Ford V., Applications of Machine Learning in Cyber Security, 7th International Conference on Computer Applications in Industry and Engineering, CAINE, Conference Paper, 2014

17- Teoh T.T., Nguwi Y.Y, Elovici Y., Wai-Loong Ng and Thiang S.Y., Analyst intuition inspired neural network based cyber security anomaly detection. International Journal of Innovative Computing, Information and Control, 14 (1), 379-386, 2018

18- Karmakar K.K., Varadharajan V., Tupakula U., Nepaly S., Thapa C., Towards a Security Enhanced Virtualised Network Infrastructure for Internet of Medical Things (IoMT), 6th IEEE International Conference on Network Softwarization, 257-261, 2020.

19- Paul J., Yaacoub A., Noura M., Noura H.N., Ola Salman O., Yaacoub E., Couturier R., Chehab A., Securing internet of medical things systems: Limitations, issues and recommendations, Future Generation Computer Systems 105, 581–606, 2020

20- Wazid M., Das A. K., Rodrıgues J., Shetty S., Park Y., IoMT Malware Detection Approaches: Analysis and Research Challenges, IEEE Access, 7, 182459-182476.

21- Kalıpcıoğlu K.C., Toğay C., Yolaçan E.N., Son Kullanıcılar İçin Anomali Saldırı Tespit Sistemleri, Journal of Engineering and Architecture Faculty of Eskisehir Osmangazi University, 27 (3), 199-212, 2019

22- Toraman S., Türkoğlu İ., A new method for classifying colon cancer patients and healthy people from FTIR signals using wavelet transform and machine learning techniques, Journal of the Faculty of Engineering and Architecture of Gazi University, 35 (2), 933-942, 2019.

23- Küçüksille E.U., Ateş N., Destek Vektör Makineleri ile Yaramaz Elektronik Postaların Filtrelenmesi, Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 6 (1), 2016.

24- Subbulakshmi T., Shalinie S. M., Ramamoorthi A., Detection and Classification of DDoS Attacks using Machine Learning Algorithms, European Journal of Scientific Research, ISSN 1450-216X, 47 (3), 334- 346, 2010.

25- Sedjelmaci H., Feham M., Novel Hybrid Intrusion Detection System for Clustered Wireless Sensor Network, International Journal of Network Security & Its Applications (IJNSA), 3 (4) 2011.

26- Al-Garadi M.A., Amr Mohamed, Abdulla Al-Ali, Xiaojiang Du, Mohsen Guizani, A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security-Project: Novel Deep Learning Architecture for Physical Activities assessment, mental Resilience and Emotion Detection, 2018

27- Agrawal S., Agrawal J., Survey on Anomaly Detection using Data Mining Techniques, 19th International Conference on Knowledge Based and Intelligent Information and Engineering Systems, Procedia Computer Science, 60, 708-713, 2015

28- Hill D.J., Minsker B.S., Amir E., Real-Time Bayesıan Anomaly Detection For Environmental Sensor Data, 32, 2007.

29- Swarnkar M., Hubballi N., OCPAD: One class Naive Bayes classifier for payload based anomaly detection, Expert Systems with Applications, 64, 330-339, 2016.

30- Şeker A., Banu Diri B, Balık H.H., Derin Öğrenme Yöntemleri ve Uygulamaları Hakkında Bir İnceleme, Gazi Mühendislik Bilimleri Dergisi, 3 (3), 47-64, 2017.

31- Balci F., Oralhan Z., LSTM ile EEG Tabanlı Kimliklendirme Sistemi Tasarımı, Avrupa Bilim ve Teknoloji Dergisi, Ejosat Special Issue (HORA), 135-141.

32- Graves A., Schmidhuber J., Offline Handwriting Recognition with Multidimensional Recurrent Neural Networks, 21, 2009.

33- Kilimci Z.H., Financial sentiment analysis with Deep Ensemble Models (DEMs) for stock market prediction, Journal of the Faculty of Engineering and Architecture of Gazi University, 35 (2), 635-650, 2019.

34- Lounis K., Zulkernine M., Attacks and Defenses in Short-Range Wireless Technologies for IoT, IEEE Access, 8, 88892-88932, 2020.

35- Nikravan M., Movaghar A., Hosseinzadeh M., A lightweight signcryption scheme for defense against fragment duplication attack in the 6LoWPAN networks, Peer-to-Peer Netw. Appl. Springer Science & Business Media, 12, 209–226, 2019.

36- Vigoya L., Fernandez D., Carneiro V., Cacheda F., Annotated Dataset for Anomaly Detection in a Data Center with IoT Sensors, 20 (13), 3745, 2020.

37- Kıyancı S., Mehmet Abi, A technological step in history education material: NFC, Research And Experience Journal (REJ), 4 (2), 2019.

38- Mısır O., Görkem L., Nesnelerin İnterneti için MQTT ile Hiyerarşik Haberleşme, Journal of New Results in Engineering and Natural Sciences, 2, 1-11, 2020.

39- Alan A., Karabatak M., Veri Seti-Sınıflandırma İlişkisinde Performansa Etki Eden Faktörlerin Değerlendirilmesi. Fırat Üniversitesi Mühendislik Bilimleri Dergisi, 32 (2), 531-540.

40- Segura-Bedmar I., Colón-Ruíz C., Tejedor-Alonso M.Á., Moro-Moro M., Predicting of anaphylaxis in big data EMR by exploring machine learning approaches, 87, 50-59, 2018.