IoT Güvenliği için Kullanılan Makine Öğrenimi ve Derin Öğrenme Modelleri Üzerine Bir Derleme

Literatür Makalesi/Review Article

Hami SATILMIŞ*, Sedat AKLEYLEK
Bilgisayar Mühendisliği, Ondokuz Mayıs Üniversitesi, Samsun, Türkiye
hami.satilmis@bil.omu.edu.tr, sedat.akleylek@bil.omu.edu.tr
(Geliş/Received:30.07.2021; Kabul/Accepted:23.10.2021)
DOI: 10.17671/gazibtd.976591

Özet— Nesnelerin internetini (internet of things - IoT) oluşturan cihazlar ve bu cihazları birbirine bağlayan ağlar hızlı bir şekilde yaygınlaşmaktadır ve evrim geçirmektedir. Buna paralel olarak, IoT cihazlarına ve ağlarına yönelik saldırılar da hız kesmeden artmaya devam etmektedir. Bu derleme çalışmasında, genel olarak IoT ağlarındaki anormallik tabanlı saldırıları tespit etmek ve azaltmak için önerilen, makine öğrenimi ve derin öğrenme modellerinden oluşan güncel yaklaşımlar özetlenmiştir. Önerilen yaklaşımlar hakkında kısa bilgiler verilmektedir ve bu yaklaşımların avantajlarından ve dezavantajlarından bahsedilmektedir. Bu çalışmanın ana hedefi olarak, önerilen yaklaşımlarda kullanılan makine öğrenimi ve derin öğrenme modelleri ile ilgili, üç araştırma sorusunun yanıtı aranmaktadır. Bu araştırma sorularından birincisi, "IoT güvenliğinde kullanılan makine öğrenimi ve derin öğrenme modelleri, hangi metriklerle değerlendirilmektedir? ", ikincisi, "IoT güvenliği açısından, makine öğrenimi ve derin öğrenme modellerinde hangi veri kümeleri kullanılmaktadır? " ve üçüncüsü ise, "IoT güvenliğinde hangi makine öğrenimi ve derin öğrenme modelleri kullanılmaktadır ve bunların uygulama alanları nelerdir? ". Bu çalışmada son olarak, incelenen çalışmalardaki eksiklikler tespit edilmektedir. Böylece, IoT güvenliği ile ilgili gelecekteki çalışmalar için bir bakış açısı sağlanmaktadır.

Anahtar Kelimeler— derin öğrenme, IoT güvenliği, makine öğrenimi

A Review of Machine Learning and Deep Learning Models Used for IoT Security

Abstract— Internet of things (IoT) devices and networks connecting these devices are rapidly spreading and evolving. In parallel, attacks against IoT devices and networks continue to increase unabated. In this review, current approaches, consisting of machine learning and deep learning models, which are recommended to detect and mitigate anomaly -based attacks in IoT networks in general, are summarized. Brief information about the proposed approaches is given, and the advantages and disadvantages of these approaches are mentioned. As the main objective of this paper, answers to three research questions about machine learning and deep learning models used in the proposed approaches are sought. The first of these research questions is, "With which metrics are machine learning and deep learning models used in IoT security evaluated? ", the second is, "In terms of IoT security, which datasets are used in machine learning and deep learning models? " and the third is, "Which machine learning and deep learning models are used in IoT security and what are their application areas? ". Finally, deficiencies encountered in the studies are noted. Thus, a perspective is provided for future work on IoT security.

Keywords— deep learning, IoT security, machine learning

1. GİRİŞ (INTRODUCTION)

Nesnelerin interneti (internet of things - IoT), aralarında haberleşebilen ve veri transferi yapabilen birbirine bağlı milyonlarca IoT cihazından oluşmaktadır. IoT cihazlarının kullanım alanları, başta Batı Avrupa, Kuzey Amerika ve Çin olmak üzere dünya genelinde artmaktadır [1]. IoT cihazları günümüzde, ev, ofis, sağlık, ulaşım, tarım gibi insan yaşamını etkileyen her alanda yaygın olarak kullanılmaktadır. Bu cihazlar, insan hayatını birincil

derecede etkileyen sağlık sektörü gibi alanlarda alınacak hayati kararlarda rol oynamaktadır. Business Insider'ın 2020 yılında yayınladığı raporda [2], 2019 yılında sayısı yaklaşık 8 milyar olan IoT cihazlarının, 2027 yılında 41 milyardan fazla olacağı öngörülmektedir. IoT cihazlarının sayısındaki bu artış göz önüne alındığında, bu cihazların genişleyen teknoloji pazarında büyük bir pay oranına sahip olacağı çıkarımına varılmaktadır. [2]'de, 2027 yılına kadar IoT pazarının yıllık 2,4 trilyon doları aşacağından bahsedilmektedir.

Geçmişten günümüze IoT cihazları, insan hayatını içeren her alanda oldukça önemli faydalar sağlamaktadır. IoT cihazlarından oluşan akıllı evler, akıllı hastaneler, akıllı araçlar ve akıllı ağlar gibi uygulamalar normal hayatta hızla yaygınlaşmaktadır. IoT cihazlarının bu geniş uygulama alanlarıyla birlikte, IoT cihazlarındaki güvenlik ve gizlilik konuları, dikkate alınması gereken en önemli sorunların başında gelmektedir. Bu bağlamda, IoT cihazlarında kullanılan teknolojilerin, cihazların güvenliğini ve gizliliğini tamamen sağlayacak düzeyde yeteneklere sahip olmaları gerekmektedir. Başka bir ifadeyle, IoT cihazlarının güvenlik açıkları, mümkün oldukça en az seviyede olması gerekmektedir. Buna paralel olarak, birbirine bağlı cihazların artışıyla, bu cihazlara yönelik büyük kapasiteli saldırıların gerçekleştirilmesine olanak sağlamaktadır.

IoT cihazlarının yaygınlaşmasıyla birlikte artan güvenlik sorunlarının başında, IoT ağlarındaki anormallikler gelmektedir. Ağ anormallikleri kısaca, normal bir ağ trafiğinden sapmalar olarak ifade edilmektedir. Genellikle, sel (flood) ve yoklama (probing) gibi saldırılar ağ anormalliklerine neden olmaktadır. IoT ağlarında meydana gelen anormallikler, Saldırı tespit sistemi (intrusion detection system - IDS) kullanılarak tespit edilmektedir. IDS, gizlilik, bütünlük ve kullanılabilirlik (confidentiality, integrity and availability - CIA) güvenlik ilkelerine karşı ağ trafiğini izleyen ve inceleyen bir sistemdir [3]. Standart bir IDS sistemi, veri toplama ve ön işleme bileşeni, analiz bileşeni ve tepki bileşeni olmak üzere üç ana bileşenden oluşmaktadır [4]. Veri toplama ve ön işleme bileşeni, ham ağ trafiği verilerini toplamaktadır ve verileri ön işleme sokarak, analiz bileşenin kullanacağı özellikleri seçmektedir. IDS'nin en önemli bileşini olan analiz bileşeni, özellikleri kullanarak bir normal ağ trafiği modeli oluşturmaktadır. Daha sonra, normal ağ trafiği modeli sayesinde anormal trafiği tespit etmektedir. IDS'nin son bileşeni olan tepki bileşeni ise, anormal trafik tespit edildiğinde alarm vermektedir ve saldırıya karşı gerçekleştirilicek eylem için yöneticiye uyarı sinyali göndermektedir [5].

Otuz yılı aşkın bir süredir, farklı yöntemlere dayalı değişik saldırı tespit sistemleri üzerine çalışmalar devam etmektedir [5,6]. Son yıllarda, IoT ağlarındaki anormallikleri tespit etmek için, makine öğrenimi ve derin öğrenme modellerine dayalı çeşitli yaklaşımlar önerilmektedir [7-12]. Anormallikleri tespit etmek için kullanılan makine öğrenimi veya derin öğrenme modelleri, kötü huylu trafik akışını, normal ağ trafiğini karakterine göre ayırt etmektedir [13]. Makine öğrenimi modelleri olarak, destek vektör makinesi (support vector machine - SVM), karar ağaçları (decision trees - DT), k-en yakın komşular (k-nearest neighbors - KNN) ve k-ortalamalar (k-means) gibi denetimli veya denetimsiz öğrenme algoritmaları kullanılmaktadır. Derin öğrenme modelleri olarak ise, evrişimli sinir ağları (convolutional neural networks - CNN), tekrarlayan sinir ağları (recurrent neural network - RNN) ve otomatik kodlayıcı (autoencoder - AE) gibi denetimli veya denetimsiz yapay sinir ağları tercih edilmektedir.

1.1. İlgili Derlemeler (Related Reviews)

Bu alt bölümde, IoT güvenliğindeki makine öğrenimi ve derin öğrenme tabanlı yaklaşımlarla ilgilenen mevcut derleme çalışmaları (yakın tarihte yayımlanan veya yüksek atıf sayısına sahip) ele alınmıştır. Bu derleme çalışmalarından bazıları, sistematik literatür derlemesi yöntemini benimsemektedir. Sistematik literatür derlemesi, bir konu hakkında hazırlanmış araştırma sorularına yanıt bulmak için, belirlenen kriterlere göre seçilen çalışmaların sistemli bir şekilde incelenmesidir. Tablo 1, ele alınan derleme çalışmalarının ve bu derleme çalışmasının özelliklerini özetlemektedir.

[14]'te, makine öğrenimi ve derin öğrenme tabanlı IoT güvenlik yaklaşımları incelenmektedir. Ancak, sistematik olmayan bu derlemede, derin öğrenme modellerinin hangi saldırı türlerine karşı kullanıldığına dair gerekli bilgiler verilmemektedir. Bir diğer sistematik olmayan [15]'teki derlemede, IoT güvenliği bağlamında makine öğrenimi ve derin öğrenme modellerinin üç farklı yönüne odaklanılmaktadır. Bu yönler, saldırılara karşı makine öğrenimi ve derin öğrenme modellerinin kullanımı, bu modellerin zayıflıkları ve bu modeller kullanılarak IoT ortamlarına karşı siber saldırılar gerçekleştirme olarak gruplanmaktadır. [16]'da, IoT ortamlarındaki anormalliklerin tespiti, analizi ve tahmini açısından önerilen yaklaşımları, istatistiksel, makine öğrenimi ve derin öğrenme modelleri olarak sınıflandıran sistematik bir derleme çalışması sunulmaktadır. [17]'de, IoT güvenliği ile ilgili hem makine öğrenimi hem de derin öğrenme modellerini benimseyen yaklaşımlar, sistematik olmayan bir şekilde incelenmektedir. Ancak, incelenen yaklaşımlarda kullanılan veri kümelerine ait detaylı bilgiler verilmemektedir. [18]'de yazarlar, sadece IoT güvenliği için önerilen yaklaşımlardaki derin öğrenme modellerine odaklanmaktadır. Bu sistematik olmayan derleme çalışmasında, IoT ortamlarındaki veri örneklerinden oluşan veri kümelerinin datayı bir incelemesi verilmektedir. Sistematik olmayan [19]'da derlemede, IoT güvenliğinde tercih edilen derin öğrenme yöntemlerinden ve büyük veri teknolojisinden bahsedilmektedir. [20]'de, IoT'nin güvenlik gereksinimlerini karşılayan yapay zeka (artificial intelligence - AI) tekniklerinin sistematik bir incelemesi verilmektedir. [21]'de, IoT mimarisinin farklı katmanları için önerilen makine öğrenimi tabanlı güvenlik çözümleri üzerinde durulmaktadır. [22] derlemesi, IoT'nin güvenliği için önerilen yaklaşımlardaki makine öğrenimi ve derin

öğrenme modellerine odaklanmaktadır ve sistematik olmayan bir derlemedir. [23]'te, güvenlik ve gizlilik sorunları için IoT'deki derin öğrenme uygulamaları ile ilgili kapsamlı bir inceleme sağlanmaktadır. Bununla birlikte, derin öğrenme modellerinin, IoT güvenliği özelinde zayıf tarafları vurgulanmaktadır. [24]'te, makine öğrenimi modellerine dayalı IoT güvenliği yaklaşımları, bunlara karşı gerçekleştirilen saldırı türleri ve makine öğrenimi modellerinde kullanılan veri kümeleri sistematik bir şekilde değerlendirmektedir. [25]'te, farklı IoT güvenlik senaryolarına uygulanan derin öğrenme modelleri hakkında sistematik bir inceleme gerçekleştirilmektedir. Ek olarak, derin öğrenme modellerinde kullanılan veri kümeleri detaylandırılmaktadır. Çeşitli IDS konumlandırma stratejilerine ve IDS analiz stratejilerine odaklanan [26]'da, IoT ağlarındaki saldırıları tespit etmek için kullanılan makine öğrenimi ve derin öğrenme modelleri sistematik olmayan bir şekilde incelenmektedir.

Tablo 1. IoT güvenliğindeki makine öğrenimi ve derin öğrenme tabanlı yaklaşımları derleyen çalışmalar ve özellikleri
(Studies reviewing machine learning and deep learning-based approaches in IoT security and their features)

Derleme	Dergi	Yıl	Sistematik mi ?	Makine Öğrenimi ve Derin Öğrenme Birlikte mi ?	Genellikle Anormallik Odaklı mı ?	Veri Kümesi Detayı Var ?
[14]	IEEE Signal Processing Magazine	2019	Hayır	Evet	Hayır	Yok
[15]	IEEE Access	2019	Hayır	Evet	Hayır	Yok
[16]	IEEE Access	2019	Evet	Evet	Evet	Yok
[17]	IEEE Communications Surveys & Tutorials	2020	Hayır	Evet	Hayır	Yok
[18]	Journal of Information Security and Applications	2020	Hayır	Hayır	Hayır	Var
[19]	Computer Communications	2020	Hayır	Hayır	Hayır	Var
[20]	IEEE Access	2020	Hayır	Evet	Hayır	Yok
[21]	Journal of Network and Computer Applications	2020	Hayır	Hayır	Hayır	Yok
[22]	IEEE Communications Surveys & Tutorials	2020	Hayır	Evet	Hayır	Yok
[23]	Security and Communication Networks	2021	Hayır	Hayır	Hayır	Var
[24]	Internet of Things	2021	Evet	Evet	Hayır	Var
[25]	Computer Science Review	2021	Evet	Hayır	Hayır	Var
[26]	Archives of Computational Methods in Engineering	2021	Hayır	Evet	Hayır	Hayır
Bu çalışma	-	-	Evet	Evet	Evet	Var

1.2. Motivasyon ve Kapsam (Motivation and Scope)

Bu sistematik literatür derlemesinde, IoT ağlarındaki anormallik tabanlı saldırıları tespit etmek için geliştirilen, makine öğrenimi ve derin öğrenme modellerini kullanan yaklaşımlara odaklanılmaktadır. Bu derlemenin, sistematik olması, makine öğrenimi ve derin öğrenme modellerini kapsaması, genellikle anormallik odaklı olması ve kullanılan veri kümelerine ait detaylara yer vermesi ile, Tablo 1'deki derleme çalışmalarından ayrılmaktadır. IoT güvenliği alanındaki araştırmacılara, yararlı ve ayrıntılı bilgiler sağlanması amacıyla hazırlanan bu sistematik derlemenin genel kapsamı şu şekildedir:

- IoT ağlarındaki anormallik tabanlı saldırıları tespit etmek için geliştirilen yaklaşımların önerildiği çalışmalar, sistematik bir şekilde seçilmektedir.

- Seçilen çalışmalarda önerilen yaklaşımlar incelenmektedir ve bu yaklaşımlara ait bilgiler özetlenmektedir.
- Yaklaşımlarda, hangi makine öğrenimi ve derin öğrenme modellerinin kullanıldığı belirtilmektedir.
- Modellerin performanslarını değerlendirmek için, çalışmalarda tercih edilen metriklerden bahsedilmektedir.
- Modellerin eğitimi ve testi için kullanılan veri kümelerine ait detaylı bilgiler sunulmaktadır.
- Modellerin deneyler sonucunda ulaştıkları performans değerleri ve karşılaştırıldıkları modeller verilmektedir.

Son olarak, incelenen çalışmalarda karşılaşılan eksiklikler ifade edilmektedir ve bu eksikliklerin, hangi durumlara neden olabilecekleri hakkında bilgilendirme yapılmaktadır.

1.3. Organizasyon (Organization)

Bu çalışmada, Bölüm 2'de, çalışmada bahsedilen teknik bilgilerin daha anlaşılır olabilmesi için, genel bilgiler verilmektedir. Bölüm 3'te, incelenen çalışmaların sistematik bir şekilde seçilmesinde yürütülen aşamalar açıklanmaktadır. Bölüm 4'te, seçilen çalışmalarda önerilen yaklaşımlar kısaca özetlenmektedir ve bu yaklaşımların altında yatan ana düşünceler, avantajlar ve dezavantajlar bir tablo halinde sunulmaktadır. Bölüm 5'te, sistematik bir derlemede olması gereken araştırma sorularının cevapları aranmaktadır. Bölüm 6'da, incelenen çalışmalarda karşılaşılan açık sorunlar ifade edilmektedir. Son bölümde ise, bu çalışmanın genel olarak neler içerdiğinden kısaca bahsedilmektedir. Tablo 2, bu çalışmada sıkça kullanılan kısaltmaların bir listesini vermektedir.

Tablo 2. Kısaltmalar ve açılımları
(Abbreviations and expansions)

Kısaltma	Açılımı	Kısaltma	Açılımı
IDS	Saldırı Tespit Sistemi (Intrusion Detection System)	MLP	Çok Katmanlı Algılayıcı (Multilayer Perceptron)
SVM	Destek Vektör Makinesi (Support Vector Machine)	LSTM	Uzun Kısa Süreli Bellek (Long Short Term Memory)
DT	Karar Ağacı (Decision Tree)	RF	Rastgele Orman (Random Forest)
KNN	k-En Yakın Komşular (k-Nearest Neighbors)	SAE	Yığınlanmış Otomatik Kodlayıcı (Stacked Autoencoder)
CNN	Evrişimli Sinir Ağları (Convolutional Neural Networks)	MI	Karşılıklı Bilgi (Mutual Information)
RNN	Tekrarlayan Sinir Ağları (Recurrent Neural Network)	AI	Yapay Zeka (Artificial Intelligence)
AE	Otomatik Kodlayıcı (Autoencoder)	HT	Hoeffding Ağacı (Hoeffding Tree)
DoS	Hizmet Reddi (Denial of Service)	BP	Geri Yayılım (Backpropagation)
DDoS	Dağıtılmış Hizmet Reddi (Distributed Denial of Service)	RT	Rastgele Ağaç (Random Tree)
DBN	Derin İnanç Ağları (Deep Belief Networks)	DFNN	Derin İleri Beslemeli Sinir Ağları (Deep Feedforward Neural Network)
GA	Genetik Algoritma (Genetic Algorithm)	DD	Veri Seli/Baskını (Data Deluge)
LR	Doğrusal Regresyon (Linear Regression)	RRS-k-means	Tekrarlayan Rastgele Örnekleme-k-Ortalamalar (Repeated Random Sampling-k-Means)
NN	Sinir Ağları (Neural Networks)	ANN	Yapay Sinir Ağları (Artificial Neural Networks)
BN	Bayes Ağı (Bayesian Network)	ELM	Aşırı Öğrenme Makinesi (Extreme Learning Machine)
A1DE	Ortalama Tek Bağımlılık Tahmincisi (Averaged One Dependence Estimator)	SDELM	Yarı Denetimli Derin Aşırı Öğrenme Makinesi (Semisupervised Deep Extreme Learning Machine)
A2DE	Ortalama Çift Bağımlılık Tahmincisi (Averaged Two Dependence Estimator)	SDN	Yazılım Tanımlı Ağ (Software Defined Networking)
NB	Naive Bayes	KPNN	Kalman Geri Yayılım Sinir Ağı (Kalman Backpropagation Neural Network)
TP	Doğru Pozitif (True Positive)	ROC	İslem Karakteristik Eğrisi (Receiver Operating Characteristic Curve)

TN	Doğru Negatif (True Negative)	AUC	Eğri Altında Kalan Alan (Area Under the ROC Curve)
FP	Yanlış Pozitif (False Positive)	MCC	Mathew'in İlişki Katsayısı (Mathew's Correlation Coefficient)
FN	Yanlış Negatif (False Negative)	DR	Tespit Oranı (Detection Rate)
ACC	Doğruluk (Accuracy)	ER	Hata Oranı (Error Rate)
PRC	Kesinlik (Precision)	TAT	Eğitim Süresi (Training Time)
REC	Duyarlılık (Recall)	TET	Test Süresi (Testing Time)
SPC	Özgüllük (Specificity)	TOT	Toplam Süre (Total Time)
F1	F1-Skor (F1-Score)	TTB	Yapım Süresi (Time to Build)
TPR	Doğru Pozitif Oran (True Positive Rate)	DS	Tespit Hızı (Detection Speed)
FPR	Yanlış Pozitif Oran (False Positive Rate)	ACT	Ortalama İşlem Süresi (Average Computational Time)
FAR	Yanlış Alarm Oran (False Alarm Rate)	ADT	Ortalama Tespit Süresi (Average Detection Time)
FNR	Yanlış Negatif Oran (False Negative Rate)	AT	Ortalama Verimlilik (Average Throughput)

2. TEKNİK ALTYAPI (TECHNICAL INFRASTRUCTURE)

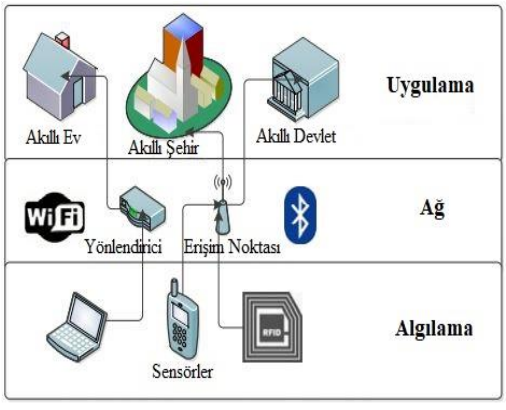
Bu bölüm, IoT mimarisine, IoT cihazlarındaki güvenlik açıklıklarına, bu cihazlara karşı yapılan bazı saldırılara ve makine öğrenimi ve derin öğrenme modellerine kısa bir genel bakış sağlamaktadır.

2.1. IoT Mimarisi (IoT Architecture)

IoT kısaca, fiziksel nesnelerin, internet aracılığı ile iletişim kurabildikleri bir ağ olarak tanımlanmaktadır. Daha açık bir ifadeyle IoT, makineden makineye, insandan insana veya insandan makineye gibi çeşitli iletişim modellerinden yararlanan heterojen cihazların birbirine bağlanması olarak ifade edilmektedir [27]. Şekil 1, IoT mimarisinin yaygın olarak kabul edilen genel yapısını göstermektedir. IoT mimarisi genellikle, fiziksel veya algılama katmanı, ağ veya iletişim katmanı ve uygulama katmanı olarak adlandırılan üç ana katmandan oluşmaktadır [28].

Iot mimarisinin ilk katmanı olan fiziksel katman, gerçek dünyadaki sıcaklık ve nem değişimi gibi olayları algılamaktadır ve bu olaylarla ilgili verileri toplamaktadır. Günümüz bilgi sistemlerindeki büyük verilerin büyük bir kısmı, fiziksel katman tarafından üretilmektedir [29]. Ancak, bu katman tarafından üretilen veriler hamdır. Bu verilerin doğru yorumlanabilmesi için, verilerin uygulama katmanına ulaşması gerekmektedir [25]. Bu katmanda genellikle sınırlı veri hızına sahip Bluetooth, WIFI ve IEEE 802.15.4 gibi kısa menzilli iletişim ve RFID, GPS gibi algılama cihazları kullanılmaktadır [5].

Ara katman olan ağ katmanı, fiziksel katman tarafından elde edilen verileri, uygulama katmanına iletmektedir. Bu katmandaki ana zorluklardan biri, internete bağlı milyarlarca cihazın IP adreslerinin birbirinden farklı olmasını sağlamaktır. Bu zorluk, IPv6 adresleme protokolü kullanılarak hafifletilmektedir. Bu katmandaki başka bir zorluk, taşınan veri paketlerinin boyutlarıyla ilgilidir ve bu zorluk, uygun sıkıştırma yetenekleri sağlayabilen protokoller kullanılarak çözülmektedir. Diğer bir zorluk ise, yönlendirme işlemleri ile ilgilidir. Yönlendirme protokolleri, akıllı nesnelerin hareketliliğini ve esnekliğini desteklemesi gerekmektedir [25]. Bu desteği sağlayan RPL (Routing Protocol for Low-Power and Lossy Networks - Düşük Güçlü ve Kayıplı Ağlar için Yönlendirme Protokolü) [30] gibi yönlendirme protokolleri, IoT cihazlarının sınırlı bellek ve güç kapasiteleri göz önünde bulundurularak geliştirilmektedir. Ağ katmanında, daha uzun mesafeli iletişime olanak sağlayan IEEE 802.3 ve IEEE 802.11 4G gibi iletişim teknolojileri tercih edilmektedir.



Şekil 1. Üç katmanlı IoT mimarisi
(Three layer IoT architecture)

Son katman olan uygulama katmanı ise, algılanan verilerden anlamlı bilgiler çıkarabilmek için, bu verileri işlemektedir. Bu katmanda verilerden yararlı bilgiler elde etmek için, makine öğrenimi veya derin öğrenme modelleri kullanılmaktadır [31]. Elde edilen bilgiler genellikle, uygulamalar ve fiziksel nesneler tarafından karar vermek

için kullanılmaktadır [5]. Uygulama katmanı, cihazlar ve uygulamalar arasındaki etkileşimi ve iletişimi sağlayan yazılımları içermektedir [32]. Akıllı şehirler, akıllı araçlar, akıllı ulaşım ve akıllı evler gibi uygulama alanları ile alakalı yazılımlar, uygulama katmanında bulunmaktadır.

2.2. IoT'nin Zayıflıkları ve Saldırı Türleri (Weaknesses of IoT and Types of Attacks)

Bu alt bölümde, IoT cihazlarındaki ve ağlarındaki zayıflıklardan ve bu zayıflıklardan yararlanmaya çalışan siber saldırıların bazılarından kısaca bahsedilmektedir.

Botnet saldırıları: IoT cihazlarının sınırlı bellek ve işlem kapasitelerine sahip olmalarından dolayı, bu cihazlar siber saldırılara karşı savunmasız hale gelmektedir. Dolayısıyla, siber saldırganlar bu cihazları kolayca ele geçirmektedir ve onları bir bot (robot) veya zombi haline getirmektedir. Bot haline gelen milyonlarca cihaz, bot ağlarını (botnet) oluşturmaktadır. Bu botnet'ler, çeşitli büyük ölçekli saldırılarda kullanılmaktadır. Botnet saldırıları olarak adlandırılan bu saldırılar, WEB sunucularında http sayfalarını açık tutarak sunucu kaynaklarını yavaşça tüketmektedir ve sonunda sunucunun normal isteklere yanıt verememesine neden olmaktadır. Bununla birlikte, diğer büyük ölçekli saldırılar, hacim tabanlı saldırılardır. Bu saldırılarda, kritik sistemlere yüksek trafik hacimleri gönderilmektedir ve böylece, kritik sistemler normal isteklere yanıt veremez hale gelmektedir. Hacim tabanlı saldırılara örnek olarak, DDoS, paket sel (packet flooding), TCP SYN flood, UDP flood, ICMP flood gibi saldırılar gösterilmektedir [33].

DoS/DDoS saldırıları: DoS saldırısı, ağı istenmeyen trafik veya isteklerle boğarak, bant genişliği gibi kaynakları normal kullanıcılar için kullanılamaz hale getirmeyi hedeflemektedir. Bu amacı gerçekleştirmek için DDoS saldırısında, botnet'ler kullanılmaktadır. DDoS saldırıları genellikle, ağ saldırıları, protokol saldırıları ve uygulama katmanı saldırıları olarak sınıflandırılmaktadır [34]. Şimdiye kadar bilinen en büyük ölçekli DDoS saldırısı, "Mirai" olarak adlandırılan botnet saldırısıdır [35]. 2016 yılında gerçekleştirilen bu saldırı, Twitter, GitHub, Netflix gibi büyük platformları erişilemez hale getirmiştir. DoS/DDoS saldırılarına örnek olarak, flood saldırıları, genişletme (amplification) saldırıları, mantıksal yazılım (logical software) saldırıları gibi saldırılar verilmektedir [36].

Paket sel (flooding) saldırıları: Bir başka büyük ölçekli saldırı türü olan paket flooding saldırıları, internet katmanındaki bir ana bilgisayarın, aldığı paketler üzerinde herhangi bir kontrolünün bulunmaması açıklığından yararlanmaktadır [37]. IoT cihazları, internet bağlantısına sahip olmalarından ve IoT trafiğinin, bir ağ geçidine veya bir saldırı tespit sistemine ulaşmadan önce birden fazla sapma yapabilmesinden dolayı, flooding saldırılarına karşı savunmasızlardır [24]. Bir yönlendiriciden alınan paketlerde, kaynak yönlendirici ile alakalı bilgiler bulunmamaktadır. Bu açıklığı kullanan saldırganlar, kaynak IP adresini taklit ederek, hedef alıcıyı sahte paketlerle doldurmaktadır. Flooding saldırılarına, TCP SYN flood, UDP flood ve ICMP flood saldırıları örnek olarak gösterilmektedir.

Sybil ve internet dolandırıcılığı (spoofing) saldırıları: Sybil saldırılarında saldırgan, aynı anda birkaç sahte kimlik kullanarak, ağın kapasitesini düşürmektedir. İnternet dolandırıcılığı saldırılarında (spoofing attacks) ise saldırgan, normal bir kullanıcının kimliğine bürünerek, kaynaklara yetkisiz erişim hakkı elde etmektedir [38]. ARP Spoofing, IP Spoofing ve DNS Server Spoofing saldırıları, spoofing saldırılarının değişik versiyonlarıdır [39].

Ortadaki adam (man-in-the-middle) saldırısı: Ortadaki adam saldırısında saldırgan, iki taraf arasındaki haberleşmeyi gizlice dinlemektedir ve aradaki bağlantıya müdahale etmektedir [40]. Ortadaki adam saldırıları arasında, oturum çalma (session hijacking), bağlantı noktası çalma (port stealing), zehirleme (poisoning) gibi farklı amaçlar bulunmaktadır [39].

2.3. Makine Öğrenimi ve Derin Öğrenme Yöntemleri (Machine Learning and Deep Learning Methods)

Denetimli öğrenme, örnek girdi-çıktı çiftlerine göre, bir girdiyi bir çıktıyla eşleyen fonksiyonu öğrenmeye yönelik bir makine öğrenimi görevidir. Denetimli makine öğrenimi ve derin öğrenme modelleri, tümüyle etiketli veri örneklerinden oluşan veri kümeleriyle eğitilmektedir. Eğitilen yöntemler, girdi olarak aldıkları verinin sınıf etiketini tahmin etmektedir veya veri örneklerini sınıflandırmaktadır. SVM, DT, KNN gibi makine öğrenimi ve CNN, RNN gibi derin öğrenme modelleri, denetimli öğrenme modelleridir.

Denetimsiz öğrenme, etiketlenmemiş verilerden örüntüleri öğrenmeye yönelik bir makine öğrenimi görevidir. Denetimsiz makine öğrenimi modelleri, etiketsiz veri örnekleri kullanılarak eğitilmektedir. Denetimsiz öğrenmede amaç, eğitim verileri içinde önceden bilinmeyen benzerlik ilişkilerini bulmak ve veri kümesinde bulunan benzerliklerden yararlanarak, etiketlenmemiş verileri bir etiket grubuna dahil etmektir. Denetimsiz öğrenme modelleri arasında, k-ortalamalar, hiyerarşik kümeleme (hierarchical clustering), DBSCAN gibi makine öğrenimi ve AE, sınırlandırılmış Boltzmann makineleri (restricted Boltzmann machines - RBM), DBN gibi derin öğrenme modelleri bulunmaktadır.

Yarı denetimli öğrenme, denetimli ve denetimsiz öğrenmenin bir kombinasyonudur. Başka bir ifadeyle, hem etiketli veri örnekleri (az miktarda) hem de etiketlenmemiş veri örnekleri (büyük miktarda) bu öğrenme yönteminde kullanılmaktadır. Bu öğrenmeye örnek olarak, üretken çekişmeli ağlar (generative adversarial networks - GAN) gibi derin öğrenme modelleri gösterilmektedir.

Takviyeli öğrenme, deneme yanılma yoluyla öğrenen ajanlar sağlayarak, bu ajanların eylemleri sonucunda ortamın nasıl etkilendiğini gözlemlemektedir. Bu

öğrenmede ajanlar, iyi eylemleri için ödüllendirilmektedir ve kötü eylemleri için cezalandırılmaktadır [41]. Derin Q-öğrenme (deep Q-learning - QL) modeli, takviyeli öğrenme yöntemini içermektedir.

3. ARAŞTIRMA YÖNTEMİ (RESEARCH METHOD)

Bu bölümde, makine öğrenimi veya derin öğrenme tabanlı IoT güvenliğine odaklanan çalışmalar seçilirken uygulanan yöntemden ve elde edilen sayısal verilerden bahsedilmektedir. Ayrıca, bu derleme çalışmasını önceki derlemelerden farklı hale getiren özellikler listelenmektedir.

3.1. Araştırma Soruları ve Amaçları (Research Questions and Objectives)

Bu sistematik literatür derlemesi, IoT cihazlarına veya sistemlerine karşı gerçekleştirilen saldırıları önlemek veya tespit etmek için geliştirilen, makine öğrenimi veya derin öğrenme tabanlı saldırı tespit etme yaklaşımlarını incelemeyi hedeflemektedir. Bu hedefe ulaşmak için, iyi huylu ve kötü huylu ağ trafiğini ayırt edebilmek için hangi makine öğrenimi veya derin öğrenme modellerinin kullanıldığına odaklanılmaktadır. Bununla birlikte, modelleri değerlendirmek için kullanılan metriklere ve modellerin eğitimi ve testi için, hangi tür veri kümelerinin tercih edildiğine yoğunlaşılmaktadır. Bu sistematik derlemenin hedefine ulaşması için cevapları aranan araştırma soruları (AS) ve bu soruların amaçları, Tablo 3'te gösterilmektedir.

Tablo 3. Araştırma soruları ve amaçları
(Research questions and objectives)

	Araştırma Soruları	Amaçları
AS1	IoT güvenliğinde kullanılan makine öğrenimi ve derin öğrenme modelleri, hangi metriklerle değerlendirilmektedir?	IoT güvenliğinde kullanılan makine öğrenimi ve derin öğrenme modellerinin gösterdikleri performansların, ne anlam ifade ettiğini öğrenmek.
AS2	IoT güvenliği açısından, makine öğrenimi ve derin öğrenme modellerinde hangi veri kümeleri kullanılmaktadır?	IoT güvenliğinde kullanılan makine öğrenimi ve derin öğrenme modellerinin eğitimi ve testi için hangi tür veri kümelerinin tercih edildiğini belirlemek ve bu veri kümelerinin özelliklerini öğrenmek.
AS3	IoT güvenliğinde hangi makine öğrenimi ve derin öğrenme modelleri kullanılmaktadır ve bunların uygulama alanları nelerdir?	IoT cihazlarının veya sistemlerini saldırılardan korumak için önerilen yaklaşımlarda kullanılan makine öğrenimi ve derin öğrenme modellerini ve bu modellerin görevlerini belirlemek ve gösterdikleri performansları değerlendirmek.

3.2. Arama Stratejisi (Search Strategy)

Bu sistematik literatür derlemesinde, incelenecek çalışmaları elde edebilmek için aşağıdaki dört temel veri tabanında araştırma yapılmaktadır:

- Scopus, çeşitli bilimsel araştırma alanında yayımlanan teknik ve akademik çalışmalara erişilmesi için detaylı arama seçeneği sunan veri tabanıdır.
- IEEE Xplore, Elektrik ve Elektronik Mühendisleri Enstitüsü'nün (Institute of Electrical and Electronics Engineers - IEEE), elektrik mühendisliği, elektronik, bilgisayar bilimi ve diğer ilgili alanlarda teknik ve bilimsel literatürü içeren veri tabanıdır.
- Web of Science (WoS), bilim, sosyal bilimler, sanat ve beşeri bilimler alanındaki akademik yayınları içeren veri tabanıdır.
- ScienceDirect, Elsevier tarafından yayınlanan dergilerdeki teknik ve bilimsel makalelere erişim imkanı veren veri tabanıdır.

Yukarıda belirtilen akademik veri tabanları, incelenecek çalışmaları bulabilmek için detaylı ve işlevsel arama motorları sağlamalarından dolayı tercih edilmektedir. Öte yandan, diğer akademik veri tabanları Google Scholar ve SpringerLink veri tabanlarının arama motorlarında, filtreleme ve ileri seviye arama yapma yeteneklerinin kısıtlı oldukları gözlemlenmiştir. Bu nedenden dolayı, Google Scholar ve SpringerLink veri tabanları bu derleme çalışmasında tercih edilmemiştir.

Tablo 3'te gösterilen araştırma soruları, yukarıda belirtilen dört veri tabanında araştırma yapabilmek için uygun sorgulara dönüştürülmesi gerekmektedir. Tablo 4, dört veri tabanında araştırma yapmak için kullanılan sorgu cümlelerini ve alanlarını göstermektedir.

3.3. Arama Süreci ve Filtreleme Kriterleri (Search Process and Filtering Criteria)

Tablo 4'teki sorgular sonucu listelenen çalışmalar arasında seçim ve eleme yapabilmek için belirlenen kriterler, Tablo 5'te verilmektedir.

Bu sistematik literatür derlemesinde, 2019 yılından 2021 yılına kadar yayımlanan çalışmalar içinden seçim yapılmaktadır (SK2). Bu tarih aralıklarının seçilmesinin nedeni ise, 2019 yılından önce yayımlanan çalışmaları kapsayan birçok derleme çalışmasının

gerçekleştirilmesidir. Ardından, belirlenen tarih aralığındaki İngilizce diliyle yazılmış dergi çalışmaları (SK1) arasından, Q1 veya Q2 seviyeli dergilerde yayımlanan (SK3) ve IoT güvenliği için makine öğrenimi veya derin öğrenme modellerinin kullanıldığı çalışmalar (SK4) listelenmektedir. Dolayısıyla, kitap, konferans ve ön baskı aşamasındaki yayınlar elenmektedir. Sonuç olarak, 43'ü Scopus, 44'ü IEEE Xplore, 39'u WoS ve 7'si ScienceDirect'den olmak üzere toplam 133 tane çalışma elde edilmektedir.

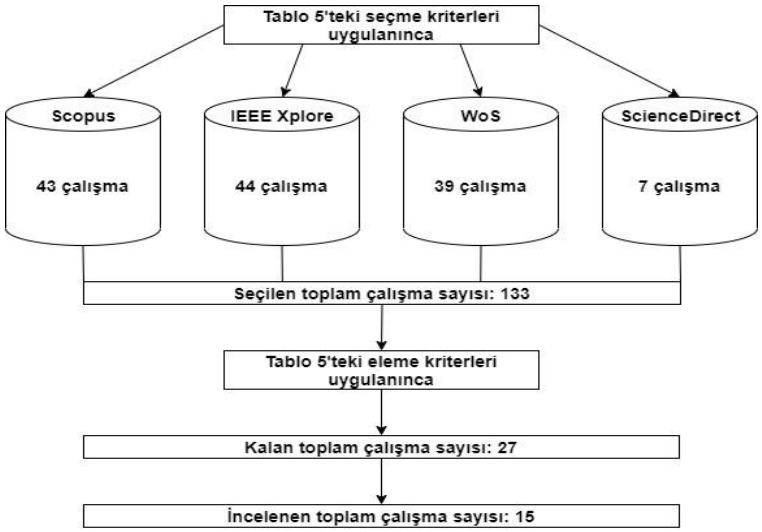
Tablo 4. Sorgu cümleleri ve alanları
(Query sentences and search fields)

Veri Tabanı	Sorgu Cümlesi	Sorgu Alanı
Scopus	TITLE-ABS-KEY(("Machine Learning" OR "Deep Learning") AND ("IoT security" OR "Internet of Things Security"))	Başlık, özet ve anahtar kelimeler
IEEE Xplore	(("All Metadata": "iot security" OR "internet of things security") AND ("All Metadata":"machine learning" OR "deep learning"))	Tüm meta verileri
WoS	TS = (("IoT Security" OR "Internet of Things Security") AND ("Machine Learning" OR "Deep Learning"))	Konu
ScienceDirect	("Machine Learning" OR "Deep Learning") AND ("Iot Security" OR "Internet of Things Security")	Başlık, özet ve anahtar kelimeler

Tablo 5. Seçme ve eleme kriterleri
(Selection and elimination criteria)

Seçme Kriterleri (SK)		Eleme Kriterleri (EK)	
SK1	Bir dergide yayımlanan İngilizce diliyle yazılmış çalışmalar	EK1	Çalışmanın bir literatür araştırması veya derleme olması
SK2	2019-2021 yılları arasında yayımlanan çalışmalar	EK2	Çalışmanın IoT ağındaki anormalliklerin tespit edilmesi ile ilgilenmemesi
SK3	Çalışmanın yayımlandığı derginin Q1 veya Q2 seviyeli olması	EK3	Çalışmada kullanılan veri kümelerinden bahsedilmemesi
SK4	IoT güvenliği için makine öğrenimi veya derin öğrenme modellerinin kullanıldığı çalışmalar	EK4	Çalışmanın makine öğrenimi ve derin öğrenme modellerine odaklanmaması

Daha sonra, 133 çalışma içerisinde tekrarlayan (duplicate) çalışmalar ve derleme ya da literatür araştırması olan çalışmalar (EK1) atılmaktadır ve toplam 51 tane çalışma elde kalmaktadır. Bu işlemlerden sonra, 51 tane çalışmanın özeti incelenmektedir. İnceleme sonucunda, IoT ağ güvenliğindeki anormalliklerin tespiti ile (EK2) ilgilenmeyen, kullanılan veri kümelerinden bahsetmeyen (EK3) ve IoT güvenliği için makine öğrenimi veya derin öğrenme modellerine odaklanmayan (EK4) çalışmalar elenmektedir. Tüm bu seçme ve eleme işlemleri sonucunda, incelenmeye hazır toplam 27 tane çalışma kalmaktadır. 27 tane çalışmadan ise, Tablo 3'teki araştırma sorularının cevaplarını içeren 15 tane çalışma, bu derlemenin kapsamında incelenmektedir. Şekil 2, incelenecek çalışmaların seçiminde uygulanan araştırma yöntemine, genel bir bakış açısı sağlamaktadır.



Şekil 2. İncelenecek çalışmaların seçimi için uygulanan araştırma yönteminin genel işleyişi
(The general operation of the research method applied for the selection of the studies to be examined)

4. ÇALIŞMALARIN KISA ÖZETLERİ (BRIEF SUMMARY OF THE STUDIES)

[42]'de araştırmacılar, IoT ortamlarındaki saldırıların tespitinde kullanılan bir derin öğrenme modelindeki sinir ağı yapısının, sadece tek bir saldırı türü için yüksek tespit doğruluğuna sahip olabileceğinden bahsetmektedir. Saldırıların yüksek doğruluk oranı ile tespit edilmesi amacıyla araştırmacılar, her bir saldırı türü için, en uygun sinir ağı yapısını ayarlayan geliştirilmiş bir genetik algoritma (genetic algorithm - GA) ile bir DBN saldırı tespit modeli önermişlerdir. Önerilen GA, her bir saldırı türü için farklı sinir ağı yapıları üretmektedir. GA tarafından üretilen farklı sinir ağı yapıları, saldırının türüne göre çeşitli DBN modelleri oluşturmada kullanılmaktadır. Böylece, farklı saldırı türlerinin tespiti için, yüksek doğruğa sahip çeşitli DBN modelleri elde edilmektedir. Önerilen saldırı tespit modelini değerlendirmek için, NSL-KDD veri kümesi [43] kullanılmaktadır. Değerlendirme sonucunda, GA tarafından üretilen farklı saldırı türlerine özel sinir ağlarından oluşan DBN modelleri, farklı tür saldırıları %97,78 - %99,45 arasındaki doğruluk oranlarıyla tespit etmektedir.

[44]'te, IoT cihazlarının davranışlarını izlemek ve olası saldırıları tespit etmek için istatistiksel öğrenmeye dayalı bir anormallik tespit etme yöntemi önerilmektedir. Önerilen yöntem, normal IoT davranışlarını gözlemek için, CPU kullanımı, bellek tüketimi, ağ çıktısı gibi basit sistem istatistiksel verileri kullanmaktadır. Bu istatistiksel veriler, IoT uygulama programı arayüzleri ile elde edildiği için, önerilen yöntem platformdan bağımsız olmaktadır. IoT uygulamaları göz önünde bulundurularak, Önerilen yöntemin uygunluğunu değerlendirmek için, LR, NN ve RNN modelleri eğitilmektedir. Eğitilen modellerin hataları, anormalliği tespit etmek için eşikleme tekniklerinde kullanılmaktadır. Önerilen yöntemde, yerel uç değer faktörü (local outlier factor - LOF), kümülatif istatistik eşiği (cumulative statistic thresholding - CUSUM) ve uyarlanabilir çevrimiçi eşikleme (adaptive online thresholding - AOT) olmak üzere üç farklı eşikleme tekniği sunulmaktadır. Önerilen yöntemin eğitimde ve değerlendirmesinde kullanılacak veri örneklerini elde etmek için, bir IoT ortamı simülasyonunda, yetkisiz erişim (unauthorized access), port tarama (port scan), virüs ve flood saldırıları gerçekleştirilmektedir. Saldırılar sonucunda, dört özniteliğe sahip veri örnekleri toplanmaktadır. Bu veri örneklerinin oluşturduğu veri kümesi kullanılarak gerçekleştirilen deneylerde, NN modelleri yaklaşık 0,67 ortalama mutlak hata (mean absolute error - MAE) oranı ile, LR ve RNN modellerine kıyasla daha iyi performans göstermektedir. Buna karşın, NN modeline yakın performans gösteren LR modelinin karmaşıklığı ve hesaplama gereksinimleri, NN modeline göre daha az olmaktadır. Bundan dolayı, LOF, CUSUM ve AOT tekniklerinde LR modeli kullanılmaktadır. LOF, CUSUM ve AOT tekniklerini anormallik tespit etme performanslarını karşılaştırmak için, F1-Skor ve duyarlılık metrikleri tercih edilmektedir. Karşılaştırma sonucunda AOT tekniği, en yüksek 0,8030 F1 ve 0,9474 REC değerleri ile en iyi performansa ulaşmaktadır.

[45]'teki araştırmacılara göre, DDoS gibi saldırılara karşı koyabilmek için önerilen saldırı tespit sistemleri genellikle, ağ trafiği akışlarından veya imzalardan çıkartılan öznitelikleri kullanmaktadır. Ayrıca, özniteliklerin manuel bir şekilde çıkarılmasından ve bu nedenden dolayı, kötü amaçlı trafik akışının tespit edilmesinde geç kalınabileceğinden bahsedilmektedir. Bu sorunların üstesinden gelebilmek için [45]'te, trafik örüntülerini otomatik olarak çıkaran ve CNN ile AE'den oluşan, D-PACK olarak adlandırılan anormal trafik tespit etme sistemi önerilmektedir. D-PACK sistemi önceki çalışmalardaki sistemlerden farklı olarak, trafik akışlarındaki toplam paketleri kontrol etmek yerine akış başına ilk birkaç paketin belli baytlarını inceleyerek trafik örüntülerini oluşturmaktadır. Bu farklılığa ek olarak D-PACK sistemi, ham paketlerle (veri temizlemesinden sonra) doğrudan çalışabilmektedir. Başka bir ifadeyle, trafik örüntülerini oluşturmaktadır, girdi verilerini okumaktadır ve tespit kararını verebilmektedir. D-PACK sistemi, USTC-TFC2016 [46], Mirai-RGU [47] ve D-PACK sistemi için gerçek veriler ile oluşturulan Mirai-CCU [45] veri kümeleri kullanılarak eğitilmektedir ve performansı ölçülmektedir. [45]'teki deneylere göre D-PACK sistemi, her bir trafik akışının sadece iki paketini ve her bir paketten 80 baytı incelese bile, neredeyse %100 doğrulukla ve %1'den daha az yanlış negatif ve yanlış pozitif oranlarıyla kötü amaçlı trafiği tespit edebilmektedir.

IoT ağlarındaki DoS saldırı trafiğinin tespit edilebilmesi için [48]'de, bağımlılık tahmincilerine dayalı MultiScheme ve Voting olarak isimlendirilen sınıflandırma teknikleri önerilmektedir. Önerilen sınıflandırma tekniklerinde bağımlılık tahmicileri olarak, BN sınıflandırıcıları olan A1DE ve A2DE tahmincileri kullanılmaktadır. Önerilen sınıflandırma teknikleri, türlerinin ilk örnekleridir. Çünkü bu sınıflandırma tekniklerinde, ağ trafiği parametreleri arasında bir ilişki kurulmaktadır. Ağ trafiği parametreleri arasında bir ilişki kurulmasıyla, kötü niyetli davranışlar için ağ trafiğinin analizi daha doğru ve etkili olmaktadır. Önerilen MultiScheme ve Voting sınıflandırma tekniklerini eğitmek ve performanslarını ölçmek için, gerçek bir fiziksel ortamdan elde edilen verilerden oluşan veri kümesi kullanılmaktadır. Önerilen sınıflandırma tekniklerinin performansları, A1DE, A2DE, NB, BN, C4.5 ve MLP olmak üzere altı modelin performansı ile karşılaştırılmaktadır. Farklı sayıda öznitelikler seçilerek gerçekleştirilen deneylerde, beş öznitelik kullanıldığında, MultiScheme sınıflandırma tekniği ile A2DE modeli en yüksek 0,9914 doğruluk oranına sahip olmaktadır. Altı öznitelik kullanıldığında, 0,9959 doğruluk oranıyla, MultiScheme sınıflandırma tekniği ve A2DE modeli aynı en yüksek doğruluk oranına ulaşmaktadır. Yedi öznitelik kullanıldığında ise, yine en yüksek doğruluğa aynı oranda (0,9994) olacak şekilde MultiScheme sınıflandırma tekniği ve A2DE modeli ulaşmaktadır. Buna karşın, deneylerin tümü eğitim süresi açısından değerlendirildiğinde, MultiScheme sınıflandırma tekniği ile aynı doğruluk değerlerine sahip olan A2DE modeli, en verimli sınıflandırıcı olmaktadır. Voting sınıflandırma tekniği ise, MultiScheme sınıflandırma tekniğinin gösterdiği performansa yakın sonuçlar vermektedir. Deneyler

sonucunda elde edilen bulgulara genel bir bakış açısıyla bakıldığında, A2DE modelinin performansı, tüm sınıflandırıcılar ve modeller arasında en iyisi olmaktadır. Buna rağmen, MultiScheme ve Voting sınıflandırma teknikleri, iki veri sınıfı arasında sınırlı bir sınıf farkı gösteren veri kümeleri için daha iyi performans sağlamaktadır. Öte yandan, A2DE'nin üstün performansını doğrulamak için, BoT-IoT veri kümesi [49] kullanılarak A1DE ve A2DE modelleri test edilmektedir. Test sonucunda, A2DE modeli altı saldırı türü içerisinden ikisini, A1DE modeline göre daha iyi oranlarda tespit etmektedir. Geri kalan saldırı türlerinde ise, A1DE ve A2DE modelleri aynı tespit etme oranına sahip olmaktadır.

[50]'de, Modbus protokolü [51] üzerinden IoT ağ trafiğini izleyen ve modüller halinde IoT sensörlerinde bulunan LSTM derin öğrenme modellerinden oluşan bir topluluğu eğitmek için, ağ paketlerini çıkaran bir yaklaşım sunulmaktadır. Sunulan yaklaşımda, altı tane LSTM modeli ile bir DT birleştirilerek bir topluluk elde edilmektedir ve topluluğun çıktısı ile ağ trafiğinin türü belirlenmektedir. Bu yaklaşım, IoT ağlarına karşı gerçekleştirilen farklı türdeki saldırıları, değişik zaman periyotlarında tespit edebilmektedir. Yaklaşımın verimliliği, gerçek dünyadaki bir Modbus ağ trafiğinden çıkartılan verilerden oluşan veri kümesi [50] kullanılarak değerlendirilmektedir. Değerlendirme sonucunda sunulan yaklaşım, IoT cihazlarına yönelik saldırıları %99'un üzerinde bir doğrulukla tespit ettiği görülmektedir. Bu doğruluk oranı ile sunulan yaklaşım, KNN, SVM, MLP ve RF modellerinden ve LSTM modellerinin her birinden daha iyi performs göstermektedir.

IoT cihazlarının genellikle sınırlı hesaplama kaynaklarına sahip olmalarından dolayı, geniş hesaplama kaynakları gerektiren geleneksel makine öğrenimi tabanlı IDS'lerde bu tür cihazlarda çalıştırılması uygun değildir [12]. Bu sorunu çözmek için [12]'deki yazarlar, sınırlı kaynaklara sahip IoT veya uç (edge) cihazlarda kullanılabilecek şekilde, IMPACT olarak isimlendirdikleri bir saldırı tespit etme sistemi geliştirmişlerdir. IMPACT sistemi, SAE, MI ve C4.8 wrapper yöntemlerini kullanarak, öznitelikleri seçmektedir ve sayılarını azaltmaktadır. Böylece, IMPACT sistemi, sınırlı kaynaklara sahip IoT veya uç cihazlarında kullanılmaya elverişli hale gelmektedir. IMPACT sisteminde saldırıları tespit etmek için ise, gradyan tabanlı doğrusal bir SVM mimarisi kullanılmaktadır. IMPACT sistemini eğitmek ve değerlendirmek için, AWID veri kümesi kullanılmaktadır. AWID veri kümesindeki taklit etme saldırılarını (impersonation attack) karşı test edilen IMPACT sistemi, %97,64 tespit oranı (detection rate - DR) ve %1,20 yanlış alarm oranı (false alarm rate - FAR) ile %98,22 doğruluk oranı elde etmektedir. Bu oranlarla IMPACT sistemi, [52-55] çalışmalarında önerilen saldırı tespit sistemleri ile karşılaştırılmaktadır ve daha iyi bir performans verdiği sonucuna varılmaktadır. Bunlara ek olarak [12]'de, AWID veri kümesindeki öznitelikler incelenmektedir ve IMPACT sisteminin performansını arttırmak için, hangi özniteliklerin daha etkili olabileceği araştırılmaktadır.

[56]'da, yanlış öznitelik seçimi nedeniyle makine öğrenmesi yöntemlerinin, IoT ağlarındaki kötü amaçlı trafikleri yanlış sınıflandırdıkları ifade edilmektedir. Bu sorunu çözmek için [56]'da ilk olarak, etkili öznitelik seçmek amacıyla bijective soft set yöntemi [57] kullanılmaktadır. Bijective soft set yöntemine ek olarak, öznitelik seçiminde kullanılması için, CorrACC olarak isimlendirilen yeni bir metrik önerilmektedir. CorrACC metriği, bağlılık öznitelik değerlendirmesi (correlation attritube evaluation - CAE) metriğinden ve ACC metriğinden oluşmaktadır. Daha sonra, belirli bir makine öğrenmesi yönteminde kullanılacak etkili öznitelikleri seçmek için, wrapper özellik seçme tekniğine dayanan ve CorrACC tabanlı yeni bir öznitelik seçim algoritması önerilmektedir. Corracc olarak adlandırılan bu öznitelik seçimi algoritmasını ve bijective soft set yöntemini değerlendirmek için, Bot-IoT veri kümesi ile dört farklı (C4.5, NB, RF ve SVM) makine öğrenmesi modeli kullanılmaktadır. Deney sonuçlarına göre, Corracc algoritması ve bijective soft set yöntemi ile elde edilen en iyi özniteliklerin kullanılmasıyla, makine öğrenmesi modelleri %95 üzerinde doğruluk oranına ulaşmaktadır.

İşbirlikçi IDS (collaborative IDS - CIDS), veri alışverişi ve paylaşımı yoluyla, IoT ağlarında tek bir tespit edicinin performansını iyileştirmek için geliştirilmektedir [58]. Denetimli makine öğrenmesi yöntemleri, sınıf etiketlerini içeren veri örneklerine ihtiyaç duymaktadır. Sınıf etiketlerini içeren veri örneklerini gerçek IoT ağlarından elde etmenin zorluğunu vurgulayan [58]'deki araştırmacılar, bu zorluğu hafifletmek için, anlaşmazlık tabanlı yarı denetimli öğrenmeye (disagreement-based semi-supervised learning - DASSL) dayanan bir öğrenme algoritması geliştirmişlerdir. Buna ek olarak [58]'de, DAS-CIDS (DASSL-CIDS) olarak adlandırılan ve DAS algoritmasına dayanan bir işbirlikçi saldırı tespit etme sistemi önerilmektedir. Farklı makine öğrenmesi modelleri arasından en iyi performansa sahip olanı seçen DASSL algoritmasında, J48 karar ağacı modeli seçilmektedir. DASSL algoritmasını değerlendirmek için, DARPA veri kümesi [59] ve gerçek veri örneklerinden oluşan bir veri kümesi kullanılmaktadır. DARPA veri kümesi ile gerçekleştirilen deneylerde, DASSL algoritması 0.243 hata oranı ile, [60]'da elde edilen hata değerinden (0,25'in üzerinde) daha düşük hata değerine ulaşmaktadır. Sekiz öznitelikli 5563 tane snort alarm [61] örneği içeren gerçek bir veri kümesi kullanılarak gerçekleştirilen deneyde ise, DASSL algoritması yaklaşık 0,286 ER oranı elde etmektedir. KNN, SVM, RF ve J48 modelleri ile karşılaştırılan DASSL algoritması, %10,5 ER ve %92,48 DR ile diğer algoritmalardan daha iyi performansa sahip olmaktadır. Öte yandan, DAS-CIDS sisteminin performansı, KNN, SVM, RF ve J48 modelleri ile karşılaştırılarak, gerçek bir IoT ortamında incelenmektedir. İncelemeler sonucunda en iyi performansa, %8,2 ER ile DAS-CIDS sistemi ulaşmaktadır.

[62]'de, IoT sistemlerine karşı gerçekleştirilen farklı saldırıları tespit etmek için, SDN ve ağ işlev sanallaştırma (network function virtualization - NFV) tabanlı güvenlik özelliklerinden yararlanmakta olan, AI ve makine

öğrenmesi modellerine dayalı bir güvenlik çerçevesi önerilmektedir. ETSI ZSM [63] vizyonuna uygun olarak önerilen güvenlik çerçevesinde, yalnızca ağ örüntüleri/imza tanıma yoluyla bilgi tabanlı saldırı tespiti değil, aynı zamanda normal davranıştan sapmalara dayalı anormallik tabanlı saldırı tespiti ile başa çıkmak için makine öğrenmesi modelleri kullanılmaktadır. Önerilen güvenlik çerçevesindeki, IDS görevini üstlenmekte olan AI tabanlı tepki ajanı (AI-based reaction agent) modülünün performansı, NSL-KDD veri kümesi ile değerlendirilmektedir. AI tabanlı tepki ajanı modülünde sırasıyla, J48, BN, RF, HT makine öğrenmesi modelleri denenmektedir. Denemeler sonucunda, farklı saldırı türleri içerisinde genel olarak en iyi performansa, %99,9 kesinlik oranı ile RF modeli ulaşmaktadır. Bu makine öğrenmesi modellerinden farklı olarak, en optimum katman ve nöron sayısına sahip bir BP modeli, AI tabanlı tepki ajanı modülüne dahil edilmektedir. BP modeli içeren AI tabanlı tepki ajanı modülü, gerçekleştirilen deneyler sonucunda %98,7 PRC oranına sahip olmaktadır. Ek olarak, bir AdaBoost modeli de, AI tabanlı tepki ajanı modülüne eklenmektedir ve %99,8'lik PRC oranında performans göstermektedir. AI tabanlı tepki ajanı modülünde ayrı ayrı kullanılan, RF, BP ve AdaBoost modelleri ile literatürdeki ilgili çalışmalarda önerilen modeller karşılaştırıldığında, RF ve AdaBoost modelleri diğerlerine göre daha iyi performans göstermektedir. Öte yandan, gerçek bir ortamdan elde edilen, her biri toplam 67876 tane aynı veri örneklerini içeren ve farklı özniteliklere ayrılmış dört farklı veri kümesi ile, önerilen çerçevenin anormallik tespit performansı ölçülmektedir. Ölçümler sırasında, önerilen çerçevede IDS görevini gerçekleştirmek için tek sınıf-SVM (one class-SVM) modeli kullanılmaktadır. Ölçümler sonucunda, önerilen çerçeve, %99,71 doğruluk oranına sahip olmaktadır.

IoT ağlarına karşı gerçekleştirilen DDoS saldırılarının tespiti, tanımlanması, sınıflandırılması ve azaltılması için [64]'te, FlowGuard olarak adlandırılan uç merkezli bir IoT savunma çerçevesi sunulmaktadır. IoT ağlarına en yakın uç sunucularda çalıştırılan FlowGuard çerçevesinin trafik akışı filtreleme bileşeni, farklı DDoS saldırı türlerine ait veri örneklerini barındıran bir tablo yardımıyla, DDoS içeren trafik akışlarını engellemektedir. Ek olarak bu bileşende, davranışları tam olarak anlaşılamayan trafik akışlarının DDoS türü içerip içermedikleri, FlowGuard çerçevesi için önerilen bir algoritma ile tespit edilmektedir. FlowGuard çerçevesinin bir diğer bileşeni olan akış işleyici bileşeninde ise, kesin olarak anlaşılamayan şüpheli trafik akışlarının gerçekten DDoS içerip içermediğini tanımlamak için LSTM modeli kullanılmaktadır. Bu bileşende ayrıca, LSTM modeli tarafından kesin olarak tanımlanan DDoS trafik akışları içerisindeki DDoS saldırı türleri, CNN modeli ile sınıflandırılmaktadır. FlowGuard çerçevesi, bir simülasyon ortamı oluşturularak elde edilen bir veri kümesi ile, CICDDoS2019 [65] veri kümesi birleştirilerek değerlendirilmektedir. Değerlendirme sonucunda LSTM modeli, trafik akışlarında DDoS saldırısının olup olmadığını en yüksek %98,9 doğruluk oranıyla tanımlamaktadır. Bu doğruluk oranıyla birlikte LSTM modeli, literatürdeki ilgili bir çalışmada [65] önerilen ID3, RF, NB ve LR modellerinden daha iyi performans göstermektedir. DDoS saldırı türlerini sınıflandıran CNN modeli ise, %99,9 oranında doğru sınıflandırma yapmaktadır.

[66]'daki yazarlar, IoT ağlarındaki anormallikleri ve bu ağlara karşı gerçekleştirilen saldırıları tespit etmek için, çok sayıda makine öğrenmesi modelleri arasından en verimli olanını seçen hibrit bir algoritma önermişlerdir. Önerilen algoritmada, bijective soft set yönteminden yararlanılmaktadır. Bilindiği kadarıyla, bijective soft set yöntemi, makine öğrenmesi modeli seçimi için ilk kez kullanılmaktadır. Önerilen hibrit algoritmada, BN, C4.5, NB, RF ve RT makine öğrenmesi modelleri kullanılmaktadır ve bu modeller içerisinden en verimli olanı saldırı tespiti için seçilmektedir. Öte yandan, [66]'da, önerilen hibrit algoritma ile birlikte, veri kümesindeki örnek verilerin özniteliklerinin çıkartılması ve seçilmesi işlemlerinin bulunduğu bir saldırı tespit etme çerçevesi sunulmaktadır. Çerçevenin performansını değerlendirmek için, Bot-IoT veri kümesi kullanılmaktadır. BN, C4.5, NB, RF ve RT modelleri üzerinde gerçekleştirilen deneyler sonucunda, NB modeli %99,79 doğruluk oranıyla en yüksek doğruluğa sahip olmasa bile, modeli oluşturma zamanı açısından en az zaman harcandığı (yaklaşık 4,03 saniye) için en verimli model olmaktadır. ACC, PRC, REC, TPR ve zaman (time) metriklerini en verimli modeli seçmek için kullanmakta olan hibrit algoritmada da NB modeli, aynı doğruluk ve zaman değerleriyle en verimli model olarak seçilmektedir.

[67]'yi temel olarak alan [68]'de, IoT'deki botnet saldırılarının davranışlarını temsil eden, tamamen statik olan yeni bir yazdırılabilir dize bilgileri (printable strings information - PSI) köklü [69] alt grafik tabanlı öznitelikler önerilmektedir. PSI köklü alt grafik tabanlı öznitelikler, daha az bellek alanı gerektirmektedir ve işlem süresini azaltmaktadır. PSI köklü alt grafik tabanlı öznitelikleri üretmek için, IoTPOT [70], VirusShare (2019) veri kümeleri ve IoT SOHO web sitesindeki veri örnekleri kullanılmaktadır. Üretilen PSI köklü alt grafik tabanlı özniteliklerin verimliliklerini ve sağlamlıklarını göstermek için, RF, DT, torbalama (bagging), KNN ve SVM makine öğrenmesi modelleri kullanılmaktadır. Bu modellere, PSI köklü alt grafik tabanlı öznitelikleri ile tanımlanan veri örnekleri girdi olarak verilmektedir. Gerçekleştirilen deneyler sonucunda, modellerin her biri IoT'deki botnet saldırılarını, %97'den daha yüksek oranda ve düşük zaman harcayarak tespit etmektedir.

[72]'de, denetimli makine öğrenmesi modellerinde kullanmak için, büyük boyutlu IoT ağlarına ait veri örneklerini içeren etiketli veri kümelerinin elde edilmesinin zor olduğu vurgulanmaktadır. Bu zorluğun üstesinden gelmek için [72]'deki yazarlar, IoT saldırılarını tespit etme sürecinde kullanmak amacıyla, SDRK olarak adlandırdıkları yarı denetimli makine öğrenmesi modelini sunmuşlardır. SDRK modeli, denetimli DFNN modelinden ve denetimsiz kümeleme yöntemlerinden yararlanmaktadır. Araştırmacılar ayrıca, SDRK modelinde kümeleme yöntemi olarak kullanılmak amacıyla, k-

ortalamalar kümeleme yöntemi tabanlı denetimsiz tekrarlayan rastgele örnekleme k-ortalamalar (repeated random sampling-k-means - RRS-k-means) kümeleme yöntemi önermişlerdir. SDRK modelini eğitmek ve değerlendirmek için kullanılacak veri kümesi, gerçek bir ortamda, DDoS saldırısının bir türü olan DD saldırısı sonrası elde edilen veri örneklerinden oluşmaktadır. Bu gerçek veri kümesi ile gerçekleştirilen deney sonuçlarına göre SDRK modelinin, DD saldırılarını %98,2 doğruluk oranıyla, ANN, NB, KNN ve ELM modellerinden daha iyi tespit ettiği görülmektedir. Öte yandan, NSL-KDD veri kümesini kullanan SDRK modeli ise, literatürdeki ilgili çalışmalarda önerilen modellere kıyasla, %99,78'lik doğruluk oranı ile en iyi performansı göstermektedir.

Saldırı azaltma çerçevelerinin çoğunda, trafik akış tabloları bulunmaktadır ve bu tablolarda, kötü amaçlı davranışlar içeren trafik akışlarının kesilmesi için kurallar bulunmaktadır. [73]'te, akış tablosunu doldurma sorununa çözüm bulmak ve DDoS saldırılarını tespit etmek ve azaltmak için, SDN paradigmasından yararlanan bir çerçeve önerilmektedir. LEDEM olarak isimlendirilen bu çerçevede, DDoS saldırılarını tespit etmek için, SDELM modeli tercih edilmektedir. LEDEM çerçevesinde DDoS saldırılarını azaltmak için, bir algoritma önerilmektedir ve IoT türüne bağlı olarak kara listeler kullanılmaktadır. LEDEM çerçevesinin performansı, gerçek ortamdan elde edilen bir veri kümesi ve UNB-ISCX veri kümesi ile ölçülmektedir. Gerçek veri kümesi ile gerçekleştirilen ölçümler sonucunda SDELM modelinin, %97,9 doğruluk oranı ile, AdaBoost, SVM ve J48 modellerinden daha iyi tespit etme yeteneğine sahip olduğu gözükmektedir. UNB-ISCX veri kümesi kullanılarak gerçekleştirilen deneylerde ise SDELM modeli, %96,28 doğruluk oranı ile, literatürdeki ilgili çalışmalarda önerilen modellerden daha iyi performans göstermektedir. Deneyler sonucunda LEDEM çerçevesi genel olarak, literatüdeki örneklerinden daha az kaynak kullanarak, daha yüksek doğrulukta DDoS saldırılarını tespit etmektedir ve azaltmaktadır.

Beşinci nesil (5G) kablosuz iletişim sistemlerinin yaygınlaşmasıyla, IoT ağlarına karşı gerçekleştirilebilecek daha güçlü ve farklı saldırıların tespit edilmesi zorluğu için [75]'te, akıllı bir saldırı tespit çerçevesi önerilmektedir. Önerilen çerçevede, dinamik IoT ağlarındaki DDoS saldırıları tespit etmek için, KPNN modeli kullanılmaktadır. Çerçevenin performansı, CICDDoS2019 veri kümesi aracılığıyla, çeşitli simülasyonlarla değerlendirilmektedir. Değerlendirmeler sonucunda çerçeve, 0,0952 FAR ile ortalama %94 doğruluğa sahip olurken, %97,49 DR ve %91,22 PRC oranlarına ulaşmaktadır.

İncelenen çalışmaların altında yatan ana düşünceler, odak noktaları ve bu çalışmalarda önerilen yaklaşımların avantajları ve dezavantajları, Tablo 6'da özetlenmiştir.

Tablo 6. Çalışmalarda önerilen yaklaşımlara genel bir bakış açısı
(An overview of the approaches proposed in the studies)

Çalışma	Ana Düşünce	Avantajlar	Dezavantajlar
[42]	IoT ortamlarındaki saldırıları tespit etmek için kullanılan sinir ağı modellerinin yapısını, saldırı türüne göre ayarlayan bir genetik algoritma ile bir DBN saldırı tespit modeli önerilmektedir.	- Saldırı türüne göre oluşturulan DBN modellerinin yükse doğruluk oranlarına ulaşmaları - Diğer çalışmalarda önerilen saldırı tespit yöntemleriyle karşılaştırılması	- Gerçek bir ortamda değerlendirilmemesi - Diğer çalışmalarda önerilen saldırı tespit yöntemlerine kıyasla, DoS saldırı özelinde, ikinci en yüksek doğruluğa sahip olması
[44]	IoT cihazlarındaki anormal davranışları tespit etmek için, LOF, CUSUM ve AOT olarak adlandırılan eşikleme tekniklerini kullanan istatistiksel öğrenme tabanlı bir yöntem önerilmektedir.	- Platformdan ve cihazdan bağımsız çalışması - Geleneksel makine öğrenimi yöntemlerinden daha iyi performans göstermesi - Yüksek duyarlılık oranlarına ulaşması	- Diğer yöntemlerle karşılaştırılmaması - Gerçek bir IoT ortamında test edilmemesi - Performansın, anormal davranışın süresine göre önemli ölçüde değişmesi
[45]	D-PACK olarak adlandırılan, IoT trafik akış örüntülerini akışın sadece birkaç paketinden otomatik olarak çıkaran ve CNN ile AE'den oluşan bir anormallik tespit etme sistemi önerilmektedir.	- Ham veriler üzerinde işlem yapabilir - Eğitim ve anormallik tespit etme süresinin az olması - Yüksek doğruluk ve düşük FNR oranı	- Gerçek bir ortamda test edilmemiş olması - Diğer sistemlerle karşılaştırılmaması - Örüntüsü çıkarılacak trafik akışındaki paketlerin sayısının ve bu paketlerin ilk kaç baytının kullanılacağının otomatik olarak belirlenememesi
[48]	IoT ağlarındaki DoS saldırılarını tespit edebilmek için, A1DE ve A2DE bağımlılık tahmincilerinden oluşan MultiSchema ve Voting sınıflandırma yöntemleri önerilmektedir.	- Yüksek doğruluk oranıyla DoS saldırılarının tespiti - Gerçek bir IoT ağında performans değerlendirmesi - Diğer sınıflandırma yöntemleri ile karşılaştırılmaları	- A2DE bağımlılık tahmincisinden daha düşük performans göstermeleri - Eğitim sürelerinin yüksek olması

[50]	IoT sistemlerine yönelik saldırıları tespit etmek için, bir dizi LSTM modelinden ve bu modellerin çıktısını toplu olarak birleştiren bir karar ağacından oluşan yaklaşım önerilmektedir.	- IoT ağlarındaki farklı saldırıların yüksek doğrulukla tespit edilmesi - Farklı zaman aralıklarında saldırıları tespit edebilmesi - Gerçek dünyadaki veriler ile değerlendirilmesi - Diğer yaklaşımlarla karşılaştırılması	- Modbus protokolü dışında, farklı IoT protokollerinde değerlendirilmemesi
[12]	Sınırlı kaynaklara sahip IoT cihazlarının kaynaklarını en az seviyede kullanacak şekilde, MI, C4.8 wrapper yöntemlerinden ve SAE ve SVM modellerinden oluşan IMPACT isimli bir saldırı tespit sistemi önerilmektedir.	- Yüksek F1-Skor oranıyla saldırıları tespit etmesi - Diğer sistemlerle karşılaştırılması - Düşük eğitim süresi - Daha az kaynak kullanması	- Daha yüksek doğruluk, tespit etme ve daha düşük FAR oranlarına sahip sistemlerin olması - Gerçek ortamda değerlendirilmemesi - Sadece tek bir saldırı türüne karşı test edilmesi
[56]	IoT ağlarındaki kötü amaçlı trafikleri yüksek doğrulukla tespit edebilmek için, Corracc öznitelik seçim algoritması önerilmektedir ve bijective soft set yöntemi ile birlikte etkili öznitelikleri seçmek için kullanılmaktadır.	- Etkili öznitellikleri kullanan C4.5, NB, RF ve SVM modellerinin, yüksek başarıyla saldırıları tespit etmeleri	- Etkili öznitellikleri kullanan C4.5, NB, RF ve SVM modellerinin, gerçek ortamda değerlendirilmemesi - Diğer öznitelik seçme yöntemleri ile karşılaştırılmaması
[58]	Anlaşmazlık tabanlı yarı denetimli öğrenmeye dayanan DASSL olarak adlandırılan algoritma ve bu algoritmanın kullanıldığı DAS-CIDS isimli bir işbirlikçi saldırı tespit etme sistemi önerilmektedir.	- Eğitimde etiketli veri örneklerine daha az ihtiyaç duyulması - Eğitimde gerçek veri örneklerinin kullanılması - Gerçek bir ortamda test edilmesi - Diğer çalışmalarla ve denetimli makine öğrenmesi yöntemleri ile karşılaştırılması - Düşük hata ve isabet oranında işlem yapması	- Geniş veri örnekleri üzerinde etkinliğinin değerlendirilmemesi - Diğer yarı denetimli veya denetimsiz yöntemlerle karşılaştırılmaması - Gelişmiş içeriden saldırılara karşı savunmasız olması
[62]	IoT sistemlerindeki saldırıları tespit etmek için, SDN ve NFV tabanlı güvenlik özelliklerinden yararlanan, AI ve makine öğrenmesi yöntemlerine dayalı bir güvenlik çerçevesi önerilmektedir.	- Saldırıların yüksek performans ve düşük maliyetle tespit edilmesi - Anormallikleri tespit ederken yüksek doğruluğa ulaşması - Gerçek ortamdan elde edilen veri örnekleri ile değerlendirilmesi - Diğer çalışmalardaki yöntemlerle karşılaştırılması	- BP modeli içeren güvenlik çerçevesinin eğitim süresinin uzun olması
[64]	IoT ağlarındaki DDoS saldırılarının tespiti, sınıflandırılması ve azaltılması için, LSTM ve CNN modellerinden oluşan ve FlowGuard olarak adlandırılan bir uç merkezli savunma çerçevesi önerilmektedir.	- Saldırıların, yüksek doğruluk oranlarıyla tespit edilmesi ve sınıflandırılması - LSTM modelinin, diğer çalışmalardaki modellerle karşılaştırılması - Hibrit bir veri kümesi oluşturularak değerlendirilmesi	- Gerçek bir ortamda değerlendirilmemesi - CNN modelinin, diğer çalışmalardaki modellerle karşılaştırılmaması - LSTM modelinin, IoT cihazlarının gecikme süresi gereksinimlerini tam olarak karşılayamaması
[66]	IoT ağlarındaki anormallikleri ve saldırıları tespit etmek için kullanılan makine öğrenmesi modellerinin en verimlisini seçmek için, hibrit bir algoritma önerilmektedir ve bu algoritmanın kullanıldığı bir saldırı tespit çerçevesi sunulmaktadır.	- BN, C4.5, NB, RF ve RT modellerinin yüksek doğruluk oranlarına ulaşması - NB modelinin, en düşük model oluşturma zamanına sahip olması nedeniyle en verimli model olması - Hibrit algoritmanın en verimli model olarak NB modelini seçmesi	- Gerçek bir ortamda değerlendirilmemesi - BN, C4.5, NB, RF ve RT modellerinin verimliliklerinin, diğer çalışmalardaki modellerle karşılaştırılmaması - Hibrit algoritmasının, BN, C4.5, NB, RF ve RT modelleri dışında etkinliğinin bilinmemesi

[68]	IoT'deki botnet saldırılarının davranışlarını tanımlayan PSI köklü alt grafik tabanlı öznitelikler önerilmektedir ve bu öznitelikler, RF, DT, torbalama, KNN ve SVM modellerinde kullanılmaktadır.	- Her bir modelin, yüksek doğruluk ve düşük zaman harcama oranlarına ulaşması - Diğer çalışmalardaki modellerle karşılaştırılması	- Gerçek bir ortamda değerlendirilmemesi - Özniteliklerin, belirli bir tetik noktasından sonra veya belirli bir zaman aralığında çıkarılması
[72]	IoT ağlarındaki veri örneklerini içeren etiketli veri kümelerinin oluşturulmasının zor olmasından dolayı, DFNN modeli ve RRS-k-means yöntemlerinden oluşan, SDRK olarak adlandırılan bir yarı denetimli saldırı tespit etme modeli önerilmektedir.	- Yüksek doğruluk oranı ile saldırıları tespit etmesi - Düşük test süresine sahip olması - Kaynak tüketim miktarının az olması - Gerçek ortamdan elde edilen veri örnekleri ile değerlendirilmesi - Diğer çalışmalarda önerilen modellerle ve farklı modeller ile karşılaştırılması	- Sadece, DD saldırılarına karşı test edilmesi - Saldırı tespit süresinin yüksek olması
[73]	IoT'deki DDoS saldırılarını tespit etmek için, SDELM modelinden ve saldırıları azaltmak için önerilen bir algoritmadan oluşan, LEDEM olarak isimlendirilen bir çerçeve önerilmektedir.	- Yüksek doğruluk oranı ile saldırıları tespit etmesi - Düşük miktarda kaynak kullanması - Gerçek bir ortamda test edilmesi - Diğer çalışmalarda önerilen modellerle ve farklı modeller ile karşılaştırılması	- Sadece, DDoS saldırılarına karşı test edilmesi - Diğer çalışmalarda önerilen modellere kıyasla, ikinci en düşük ortalama tespit süresine sahip olması
[75]	5G kablosuz iletişim sistemlerinde IoT ağlarına karşı gerçekleştirilebilecek daha güçlü saldırıları tespit etmek için, Kalman Geri Yayılım Sinir Ağı modelinden oluşan bir çerçeve önerilmektedir.	- Düşük FAR ve yüksek tespit etme doğruluğuna sahip olması	- Gerçek bir ortamda değerlendirilmemesi - Sadece, DDoS saldırılarına karşı test edilmesi - Diğer çalışmalardaki çerçevelerle karşılaştırılmaması - Eğitim süresinin bilinmemesi

5. BULGULAR (FINDINGS)

Bu bölümde, belirlenen araştırma soruları yanıtlanmaktadır.

5.1. AS1: IoT Güvenliğinde Kullanılan Makine Öğrenimi ve Derin Öğrenme Modelleri, Hangi Metriklerle Değerlendirilmektedir? (RQ1: With Which Metrics Are Machine Learning and Deep Learning Models Used in IoT Security Evaluated?)

İncelenen çalışmalarda önerilen yaklaşımlarda kullanılan makine öğrenimi ve derin öğrenme modellerinin performansı, çeşitli metrikler aracılığıyla değerlendirilmektir. Bu metrikler, Tablo 7'de gösterilmektedir. Tablo 7'de, metriklerin ne anlam ifade ettikleri, varsa matematiksel denklemleri ve hangi çalışmalarda tercih edildikleri özetlenmektedir. Tablo 7 incelendiğinde, modellerin değerlendirmek ve en iyi modeli belirleyebilmek için, ACC, PEC, REC, F1 ve FPR/FAR metriklerinin yaygın olarak tercih edildikleri görülmektedir. Diğer metrikler ise, önerilen yaklaşımların hedeflerine özgü olarak, modellerin beklenen performans değerlerine ulaşıp ulaşmadıklarının değerlendirilmesinde ve modellerin ayırt edici olarak karşılaştırılmasında kullanılmaktadır.

5.2. AS2: IoT Güvenliği Açısından, Makine Öğrenimi ve Derin Öğrenme Modellerinde Hangi Veri Kümeleri Kullanılmaktadır? (RQ2: Which Datasets Are Used in Machine Learning and Deep Learning Models for IoT Security?)

İncelenen çalışmalarda kullanılan makine öğrenimi ve derin öğrenme modellerinin eğitimi ve testi için, farklı türde ve sayıda saldırı örneklerini içeren veri kümeleri tercih edilmektedir. Bu veri kümeleri, IoT güvenliği için önerilen yaklaşımların amacına göre seçilmektedir. Daha açık bir ifadeyle, önerilen yaklaşımlar hangi saldırı türlerini tespit etmek veya azaltmak için geliştirildiyse, o saldırı türlerine ait örnekleri içeren veri kümeleri modellerin eğitimi ve testi için kullanılmaktadır. Tablo 8'de, modellerin eğitimi ve testi için kullanılan yaygın veri kümeleri ve çalışmalara özgü olarak oluşturulan veri kümeleri verilmektedir. Tablo 8'de, veri kümelerinin içerdiği, kötü huylu ve iyi huylu örneklerin türlerinden, örneklerin istatistiksel özelliklerinden ve hangi çalışmalarda kullanıldıklarından bahsedilmektedir. Öte yandan, [58, 73] çalışmalarında kullanılan veri kümelerine ait detaylı bilgiler, kullanıldıkları çalışmalarda verilmemektedir. Bu nedenden dolayı, bu veri kümelerine ait detaylar Tablo 8'de bulunmamaktadır.

Tablo 7. Makine öğrenimi ve derin öğrenme modellerini değerlendirmek için kullanılan metrikler
(Metrics used to evaluate machine learning and deep learning models)

Metrik	Tanım	Denklem	Kullanan Çalışmalar
TP	Doğru bir şekilde pozitif olarak sınıflandırılan pozitif örneklerin sayısı.	-	Tümü
TN	Doğru bir şekilde negatif olarak sınıflandırılan negatif örneklerin sayısı.	-	Tümü
FP	Yanlış bir şekilde pozitif olarak sınıflandırılan negatif örneklerin sayısı.	-	Tümü
FN	Yanlış bir şekilde negatif olarak sınıflandırılan pozitif örneklerin sayısı.	-	Tümü
ACC	Sınıflandırılan örnek veriler içinde doğru sınıflandırılmış örnek verilerin yüzdesi.	$\frac{TP+TN}{TP+TN+FP+FN} \times 100$	[12], [42], [45], [48], [50], [56], [62], [64], [66], [68], [72], [73], [75]
PRC	Pozitif olarak sınıflandırılan örnek verilerin, gerçekte kaç adedinin pozitif olduğunun yüzdesi.	$\frac{TP}{TP+FP} \times 100$	[42], [45], [48], [50], [56], [64], [66], [73], [75]
REC	Pozitif olarak tahmin edilmesi gereken örnek verilerin, ne kadarının pozitif olarak sınıflandırıldığının yüzdesi.	$\frac{TP}{TP+FN} \times 100$	[12], [42], [44], [45], [48], [50], [56], [64], [66], [73]
SPC	Gerçek negatif örneklerin oranı.	$\frac{TP}{TN+FP} \times 100$	[56]
F1	Kesinlik ve duyarlılık metriklerinin harmonik ortalaması.	$\frac{2 \times PRC \times REC}{PRC+REC} \times 100$	[12], [44], [45], [48], [50], [64], [68], [72], [73]
TPR	Doğru bir şekilde pozitif olarak sınıflandırılan pozitif örneklerin oranı.	$\frac{TP}{TP+FN} \times 100$	[66], [68], [72]
FPR/FAR	Yanlış bir şekilde pozitif olarak sınıflandırılan negatif örneklerin oranı.	$\frac{FP}{FP+TN} \times 100$	[12], [42], [45], [62], [66], [68], [75]
FNR	Yanlış bir şekilde negatif olarak sınıflandırılan pozitif örneklerin oranı.	$\frac{FN}{TP+FN} \times 100$	[45]
ROC	Eşik veri değerleri aralığı boyunca değiştiğinden, FPR'nin TPR'ye karşı çizilmesiyle elde edilen eğri.	-	[68]
AUC	ROC eğrisinin altında kalan alan.	-	[68]
MCC	Gerçek ve tahmin edilen ikili sınıflandırmalar arasındaki bir ilişki katsayısı.	$\frac{(TP \times TN)-(FP \times FN)}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}} \times 100$	[12], [72]
DR	Toplam pozitif örnekler arasında doğru tespit edilen pozitif örneklerin oranı.	$\frac{TP}{TP+FN} \times 100$	[42], [58], [72], [75]
ER	Modelin ne sıklıkta yanlış sınıflandırma gerçekleştirdiğinin oranı.	$\frac{FP+FN}{TP+TN+FP+FN} \times 100$	[58], [62]
TAT	Modelin eğitimi için harcanan toplam süre.	-	[62], [72]

TET	Modelin test edilmesi için harcanan toplam süre.	-	[72]
TOT	Modelin eğitimi ve testi için harcanan toplam süre.	-	[72]
TTB	Modelin oluşturulması için geçen toplam süre.	-	[12], [48]
DS	Saniyede, kaç tane trafik akışı üzerinde işlem yapıldığının sayısı.	-	[45]
ACT	Modelin, örnek veriler üzerinde gerçekleştirdiği işlemlerin ortalama süresi.	-	[75]
ADT	Bir saldırı tespit etmek için geçen ortalama süre.	-	[73]
AT	Bir saldırı sırasında IoT sunucusuna, bir saniyede kaç tane iyi huylu veri paketinin ulaştığını gösterir.	-	[73]

Tablo 8. Modellerde kullanılan veri kümeleri ve özellikleri
(Datasets and properties used in models)

Veri Kümesi	**Kötü Huylu Veri Türleri ve Sayıları**	**İyi Huylu Veri Türleri ve Sayıları**	**Toplam Veri Sayıları**	**Öznitelik Sayısı**	**Kullanan Çalışmalar**
NSL-KDD	- DDoS: 53385 - U2R: 252 - R2L: 3416 - Probing: 14410	- Normal trafik: 77054	- Kötü huylu: 71463 - İyi huylu: 77054 - Toplam: 148517	41	[42], [62], [72]
UST-TFC2016	- Tinba: 8504 - Zeus: 10970 - Shifu: 9634 - Neris: 33791 - Cridex: 461548 - Nsisay: 6069 - Geodo: 40947 - Miuref: 13481 - Virut: 33103 - Htbot: 6367	- Facetime: 6000 - Skype: 6321 - Bittorent: 7517 - Gmail: 8629 - Outlook: 7524 - WarCraf: 7883 - MySQL: 86089 - FTP: 101037 - SMB: 38937 - Weibo: 39950	- Kötü huylu: 624414 - İyi huylu: 309887 - Toplam: 934301	-	[45]
Mirai-RGU	- ACK flood: 7425 - HTTP flood: 143 - UDP flood: 32418 - DNS flood: 4852 - Mirai: 2795422 - VSE flood: 4990 - GREIP flood: 27804 - SYN flood: 118754 - UDPPLAIN flood: 19 - GREETH flood: 5	- Mixed trafik: 76725	- Kötü huylu: 2991832 - İyi huylu: 76725 - Toplam: 3068557	6	[45]
Mirai-CCU	-ACK flood: 150001 - HTTP flood: 7722 - UDP flood: 99986 - SYN flood: 763436	-	- Kötü huylu: 1021145 - Toplam: 1021145	-	[45]
[48]'deki yazarlar tarafından gerçek ortamdan elde edilen veri kümesi	- Flood saldırı trafiği: 256324	- Normal trafik: 365016	- Kötü huylu: 256324 - İyi huylu: 365016 - Toplam: 621340	7	[48]
[50]'daki yazarlar tarafından gerçek ortamdan elde edilen veri kümesi	- Man in the middle: 230330 - Modbus query flooding: 4021403 - Ping flood DDoS:	- Clean: 259635	- Kötü huylu: 5599450 - İyi huylu: 259635 - Toplam: 5859085	83	[50]

	616746 - TCP SYN flood DDoS: 730971				
AWID	- Impersonation, flooding ve injection saldırıları: 2978288	- Normal veriler: 86540744	- Kötü huylu: 2978288 - İyi huylu: 86540744 - Toplam: 89519032	156	[12]
BoT-IoT	- Service scanning: 1463364 - OS Fingerprinting: 358275 - TCP DoS/DDoS: 31863600 - UDP DoS/DDoS: 39624597 - HTTP DoS/DDoS: 49477 - Keylogging: 1469 - Data theft: 118	- UDP: 7225 - TCP: 1750 - ARP: 468 - IPV6-ICMP: 88 - ICMP: 9 - IGMP: 2 - RARP: 1	- Kötü huylu: 73360900 - İyi huylu: 9543 - Toplam: 73370443	32	[56], [66]
CICDDoS2019	- DDoS saldırıları: 30 milyondan fazla	- Normal trafik: 1 milyondan fazla	- Kötü huylu: 30 milyondan fazla - İyi huylu: 1 milyondan fazla - Toplam: 31 milyondan fazla	80	[64], [75]
[64]'teki yazarlar tarafından, bir IoT ortamı simülasyonundan elde edilen veri kümesi	- ICMP flooding saldırıları: 999974 - UDP flooding saldırıları: 999997 - TCP flooding saldırıları: 1000000 - Slow Headers saldırıları: 21087 - Slow Read saldırıları: 22015 - Slow Write saldırıları: 21137 - Slow Body saldırıları: 21535	-	- Kötü huylu: 3085745 - Toplam: 3085745	83	[64]
IoTPOT	- IoT botnet saldırıları: 4000	-	- Kötü huylu: 4000 - Toplam: 4000	-	[68]
VirusShare	- IoT botnet saldırıları: 3799	-	- Kötü huylu: 3799 - Toplam: 3799	-	[68]
[72]'deki yazarlar tarafından gerçek ortamdan elde edilen veri kümesi	- DD saldırısı: 115200	-	- Kötü huylu: 115200 - Toplam: 115200	22	[72]
[73]'deki yazarlar tarafından gerçek ortamdan elde edilen veri kümesi	- UDP flooding saldırısı: 89860	-	- Kötü huylu: 89860 - Toplam: 89860	155	[73]

5.3. AS3: IoT Güvenliğinde Hangi Makine Öğrenimi ve Derin Öğrenme Modelleri Kullanılmaktadır ve Bunların Uygulama Alanları Nelerdir? (RQ3: Which Machine Learning and Deep Learning Models Are Used in IoT Security and What Are Their Application Areas?)

IoT güvenliği için önerilen yaklaşımlarda kullanılan makine öğrenimi ve derin öğrenme modelleri, Tablo 9'da verilmektedir. Tablo 9'da, modellerin kullanım alanları, hangi veri kümeleri ile eğitildikleri ve test edildikleri, deneyler sonucunda gösterdikleri performanslar ve hangi

modellerle karşılaştırıldıkları hakkında bilgiler özetlenmektedir.

Tablo 9'a bakıldığında, [42]'de, denetimsiz öğrenme yönteminin benimsenmesinden ve yüksek boyutlu veriler üzerinde işlem yapabilmesinden dolayı, DBN modelleri tercih edilmektedir. Farklı saldırı türlerini tespit etmek için kullanılan DBN modelleri, literatürdeki ilgili örneklerlerine göre genel olarak daha yüksek başarı yüzdesi göstermektedir.

[44]'te, LR, NN ve RNN modelleri ile test edilen ve anormal davranışları tespit etmek için önerilen eşikleme yöntemlerinde, NN modelinden daha yüksek hata değerine sahip olmasına rağmen LR modelinin kullanılması tercih edilmektedir. LR modelinin tercih edilmesinin ana nedeni olarak, LR modelinin NN modeline göre daha basit olması ve IoT cihazlarında kullanımının daha rahat olması gösterilmektedir.

[45]'te, ham IoT trafik akışı verilerinin özelliklerini otomatik olarak çıkarabilmek için CNN modeli kullanılmaktadır. Çıkartılan özellikler kullanılarak, tafik akışlarının iyi huylu veya kötü huylu olarak sınıflandırılması amacıyla, etiketsiz veri örnekleri ile çalışabilmesinden dolayı AE modeli tercih edilmektedir.

[48]'de, NB modellerinde kullanılan özniteliklerin birbirlerinden bağımsız olmaları gerekliliğinden dolayı, birbirine bağımlı öznitelikleri kullanabilen A1DE ve/veya A2DE modelleri saldırıları tespit etmek için önerilmektedir. Gerçekleştirilen deneyler sonucunda A1DE ve/veya A2DE modelleri, NB, BN, C4.5 ve MLP modellerinden daha iyi performans göstermektedir. Öte yandan, tüm modeller arasında en iyi performansa, A2DE modeli ulaşmaktadır.

[50]'de, girdi verileri arasındaki bağımlılıkları belirleyebilmesinden ve büyük boyutlu veriler üzerinde işlem yapabilmesinden dolayı, saldırıları tespit etmek için LSTM modelleri kullanılmaktadır. LSTM modellerinin çıktıları ile DT modeli birleştirilerek, saldırılar sınıflandırılmaktadır. Birleştirilen model, KNN, SVM, MLP, RF ve bireysel LSTM modellerinden daha iyi performans göstermektedir.

[12]'de, IoT cihazlarında daha az kaynak tüketmek amacıyla, verilerin özniteliklerini çıkarmak için bir SAE modeli ve öznitelikler arasından seçim yapmak için MI ve C4.8 wrapper yöntemleri, önerilen saldırı tespit etme sisteminde kullanılmaktadır. Saldırıları tespit etmek için, iki sınıf etiketine sahip veri örneklerini sınıflandırma başarısından dolayı, SVM modeli tercih edilmektedir. Önerilen saldırı tespit etme sisteminin başarısı, genel olarak karşılaştırıldığı sistemlerden yüksek olsa da, ACC metriği açısından D-FES-Corr sisteminden daha düşük olduğu gözükmektedir.

[56]'da, önerilen etkili öznitelik seçme şemasının seçtiği öznitelikler, C4.5, NB, RF ve SVM modellerinde kullanılarak saldırılar tespit edilmektedir. Deneyler sonucunda C4.5 modeli genel olarak, farklı saldırıları tespit etme oranı en yüksek model olmaktadır.

[58]'de, önerilen DASSL algoritmasında temel model olarak, J48 modeli kullanımaktadır. [60] ile karşılaştırıldığında, DASSL algoritmasının daha düşük hata oranına sahip olduğu sonucuna varılmaktadır. Ayrıca, DASSL algoritması saldırıları tespit etme açısından, KNN, SVM, RF ve J48 modellerinden daha iyi performans göstermektedir.

[62]'de, saldırıları tespit etmek için, J48, BN, RF, HT, BP, AdaBoost ve SVM modelleri kullanılmaktadır. Bu modeller arasında en iyi performansı gösteren AdaBoost modeli, literatürdeki ilgili örneklerden daha yüksek doğrulukla saldırıları tespit etmektedir.

[64]'te, IoT trafik akışlarının DDoS saldırısı içerip içermediğini tespit etmek için LSTM modeli kullanılırken, DDoS saldırılarını türlerine göre sınıflandırmak için CNN modeli kullanılmaktadır. LSTM modelinin tercih edilmesinde ana neden olarak, LSTM modelinin trafik akışlarının ayırt edici özelliklerini yakalaması ve girdi veri örnekleri arasında bu ayırt edici özellikleri saklaması olarak gösterilmektedir. Öte yandan CNN modeli, benzer sayıda katmana sahip ileri beslemeli sinir ağlarına kıyasla, daha az bağlantı ve parametre ile zamana duyarlı saldırılarla başa çıkma yeteneğinden dolayı tercih edilmektedir.

[66]'da, saldırıları tespit edecek en verimli modeli seçmek için geliştirilen algoritmada, BN, C4.5, NB, RF ve RT modelleri kullanılmaktadır. Deneyler sonucunda NB modeli, geliştirilen algoritma tarafından en verimli model olarak seçilmektedir.

[68]'de, önerilen yeni özniteliklerin etkinliklerini değerlendirmek için, yaygın olarak kullanılan RF, DT, torbalama, KNN ve SVM modelleri tercih edilmektedir. Önerilen yeni öznitelikler ile oluşturulan bu modeller, literatürdeki benzer modellerden daha iyi performans göstermektedir.

[72]'de, IoT ağlarındaki saldırıları tespit etmek ve azaltmak için önerilen yöntemde, bir denetimli DFNN modeli ve denetimsiz RRS-k-means kümeleme yöntemi kullanılmaktadır. DFNN modelini tercih etmedeki ana neden olarak, genelleme hatasının az olması ve gizli katmanlardaki düğüm sayılarını kontrol etmenin mümkün olması olarak açıklanmaktadır. Önerilen yöntem, ANN, NB, KNN ve ELM modellerinden ve literatürdeki ilgili çalışmalarda önerilen modellerden daha yüksek başarı oranıyla saldırıları tespit etmektedir ve azaltmaktadır.

[73]'te, güvenlik alanında daha önce hiç kullanılmamış olan ve ELM modelini içerisinde barındıran SDELM modeli, saldırıları tespit etmek için kullanılmaktadır. SDELM modelininin temeli olan ELM modeli, eğitim aşamasının hızlı olmasından dolayı tercih edilmektedir.

SDELM modeli, AdaBoost, SVM, J48 modellerinden ve literatürdeki ilgili çalışmalarda önerilen modellerden genel olarak daha iyi performans göstermektedir.

[75]'te, DDoS saldırılarının tespit edilmesi için, KPNN modeli kullanılmaktadır. KPNN modeli, geri yayılım eğitimindeki hesaplama yükünün daha az olmasından dolayı tercih edilmektedir.

Tablo 9. Modellere genel bir bakış
(An overview of the models)

Çalışma	Kullanılan Modeller/Yöntemler ve Görevleri	Veri Kümeleri ve Kullanımları	Performans	Karşılaştırıldıkları Modeller veya Yaklaşımlar
[42]	- DBN: Genetik algoritma ile ayarlanan ağ yapılarından oluşarak, IoT ortamlarındaki farklı tür saldırıları tespit etmek	- NSL-KDD: Eğitim ve test için kullanılmaktadır.	- ACC: %98,82 - PRC: %97,36 - REC: %97,65 - DR: %97,67 - FAR: %2,65	- TANN - FC-ANN - SA-DT-SVMS - BPNN
[44]	- LOF, CUSUM ve AOT: Bu eşikleme yöntemlerini kullanarak, IoT cihazlarındaki anormal davranışları tespit etmek - LR, NN ve RNN: IoT cihazlarındaki anormal davranışları tespit etmek için, eşikleme yöntemlerine hata değerleri üretmek	- Yazarlar tarafından, bir IoT ortamı simülasyonundan elde edilen veri kümesi, eğitim ve test için kullanılmaktadır.	- REC: %94,74 - F1: %80,30	-
[45]	- CNN: Trafik akışlarına ait özellikleri çıkarmak - AE: Trafik akışını iyi huylu veya kötü huylu olarak sınıflandırmak	- USTC-TFC2016: Eğitim için iyi huylu örnekleri kullanılmaktadır. - Mirai-CCU: Test için kötü huylu örnekleri kullanılmaktadır.	- ACC: %100 - PRE: %100 - REC: %100 - F1: %100 - FNR: %0 - FPR: %0 - DS: 676 akışlar/s	-
		- USTC-TFC2016: Eğitim için, iyi huylu örnekleri ve test için, iyi ve kötü huylu örnekleri kullanılmaktadır.	- ACC: %100 - PRE: %100 - REC: %100 - F1: %100 - FNR: %0 - FPR: %0 - DS: 576 akışlar/s	
		- Mirai-RGU: Eğitim için, iyi ve kötü huylu örnekleri ve test için, kötü huylu örnekleri kullanılmaktadır.	- ACC: %99,77 - PRE: %99,93 - REC: %99,17 - F1: %99,25 - FNR: %0,02 - FPR: %0,83	
[48]	- A1DE veya A2DE: Bu modellerden en iyisini kullanarak, IoT ağlarındaki DoS saldırılarını tespit etmek	- Yazarlar tarafından gerçek bir ortamdan elde edilen yedi öznitelikli veri kümesi, eğitim ve test için kullanılmaktadır.	- ACC: %99,94 - PRE: %99,9 - REC: %99,9 - F1: %99,9 - TP: %99,9 - FP: %0,1 - TTB: 19,53 s	- A1DE - A2DE - NB - BN - C4.5 - MLP
	- A1DE ve A2DE: Bu modellerin kombinasyonunu kullanarak, IoT ağlarındaki DoS saldırılarını tespit etmek		- ACC: %99,93 - PRE: %99,9 - Recall: %99,9 - F1: %99,9 - TP: %99,9 - FP: %0,1 - TTB: 14,59 s	
[50]	- LSTM: IoT sistemlerindeki saldırıları tespit etmek - DT: LSTM modellerinin çıktılarını birleştirmek	- Yazarlar tarafından gerçek bir ortamdan elde edilen veri kümesi, eğitim ve test için kullanılmaktadır.	- ACC: %99,62 - PRE: %99,418 - REC: %98,883 - F1: %99,142	- KNN - SVM - MLP - RF

				- Bireysel LSTM modelleri
[12]	- SAE, MI ve C4.8 wrapper: Veri kümesinin özniteliklerini seçmek ve sayıları azaltmak - SVM: IoT cihazlarındaki saldırıları tespit etmek	- AWID: Eğitim ve test için kullanılmaktadır.	- ACC: %98,22 - REC: %97,64 - F1: %98,21 - FAR: %1,20 - MCC: 96,45 - TTB: 299,97	- DEMISe-RBFC [55] - DETEReD [55] - D-FES-Corr [54] - [52] - [53]
[56]	- Bijective soft set yöntemi ve Corracc algoritması: Etkili öznitelikler seçmek - C4.5, NB, RF ve SVM: Etkili öznitelikleri kullanarak saldırıları tespit etmek	- BoT-IoT: Eğitim ve test için kullanılmaktadır.	- ACC: %99,99 - PRE: %96,09 - REC: %92,3 - SPC: %99,74	-
[58]	- DASSL: Bu öğrenme algoritmasını kullanarak, etiketsiz veri örneklerini etiketlemek - J48: DASSL algoritmasında temel model olarak kullanılmak	- DARPA: DASSL algoritmasının performansını ölçmek için kullanılmaktadır.	- ER: %15	- [60]
		- Gerçek bir veri kümesi ile, DASSL algoritmasının performansını ölçmek.	- ER: %10,5 - DR: %92,48	- KNN - SVM - RF - J48
		- Yazarlar tarafından, bir IoT ortamdan elde edilen veri kümesi, eğitim ve test için kullanılmaktadır.	- DR: %8,2	- KNN - SVM - RF - J48
[62]	- J48, BN, RF, HT, BP, AdaBoost ve SVM: IoT sistemlerindeki saldırıları tespit etmek ve azaltmak	- NSL-KDD: Eğitim ve test için kullanılmaktadır.	- ACC: %99,9 - DR: %98,9 - FPR: %0,1 - TAT: 193,6 s	- F-SVM [76] - DMM [77] - TANN [78] - DBN [79] - RNN [80] - DNN [75], [81], [82] - E-DNN [83] - DFF-NN [82] - DL-SVM-DR [84]
		- Yazarlar tarafından gerçek bir ortamdan elde edilen veri kümesi, farklı öznitelikleri ile eğitim ve test için kullanılmaktadır.	- ACC: %99,71	-
[64]	- LSTM: IoT trafik akışlarının, DDoS saldırısı içerip içermediğini tespit etmek - CNN: DDoS saldırı türlerini sınıflandırmak	- CICDDoS2019: Eğitim ve test için kullanılmaktadır.	- PRE: %99,47 - REC: %99,31 - F1: %99,35	-
		- Eğitim için yazarlar tarafından, bir IoT ortamı simülasyonundan elde edilen veri kümesi ile CICDDoS2019 veri kümesinin kombinasyonu, test için ise, yazarlar tarafından elde edilen veri kümesi kullanılmaktadır.	- ACC: %100 - PRE: %100 - REC: %100 - F1: %100	
[66]	- BN, C4.5, NB, RF ve RT: En verimli modeli seçen hibrit algoritmada kullanılmak	- Bot-IoT: Eğitim ve test için kullanılmaktadır.	- ACC: %99,79 - PRE: %99 - REC: %98 - TPR: %99 - TTB: 4,03 s	-
[68]	- RF, DT, Torbalama, KNN ve SVM: Önerilen yeni özniteliklerin etkinliklerini değerlendirmek için kullanılmak	- IoT SOHO: Bu web sitesinden elde edilen iyi huylu örnekler ile, - IoTPOT ve VirusShare: Bu veri kümelerindeki kötü	- ACC: %97,2 - F1: %98 - AUC: %97,1 - TPR: %98 - FPR: %4,3	[85]'te önerilen, - RF - SVM - KNN - DT

		huylu örnekler, eğitim ve test için kullanılmaktadır.		
[72]	- DFNN modeli ve RRS-k-means yöntemi: IoT saldırılarını tespit etmek	- Yazarlar tarafından gerçek bir ortamdan elde edilen veri kümesi, eğitim ve test için kullanılmaktadır.	- ACC: %98,2 - DR: %99,3 - F1: %87,7 - MCC: %87,4 Kötü huylu veri için, - TPR: %78,6 İyi huylu veri için, - TPR: %98,1	- ANN - NB - KNN - ELM
		- NSL-KDD: Eğitim ve test için kullanılmaktadır.	- ACC: %99,78 - DR: %99,83 - F1: %99,72 - MCC: %99,44 - TAT: 1986,32s - TET: 6,59s - TOT: 1992,91s Kötü huylu veri için, - TPR: %99,62 İyi huylu veri için, - TPR: 99,79	- ELM [86] - Online Sequantial ELM [87] - ELM Fuzzy C Means [88] - DL [89] - LDA, NB, KNN [90] - GA ve DBN [42] - SVM [91] - Bat algoritması ve RF [92]
[73]	- SDELM: IoT'deki DDoS saldırılarını tespit etmek	- Yazarlar tarafından gerçek bir ortamdan elde edilen veri kümesi, eğitim ve test için kullanılmaktadır.	- F1: %97,2 İyi huylu veri için, - ACC: %97,9 - PRE: %98,1 - REC: %98,2 Kötü huylu veri için, - PRE: %97,2 - REC: %97,6	- AdaBoost - SVM - J48
		- UNB-ISCX: Eğitim ve test için kullanılmaktadır.	- F1: %96,2 - ADT: 2,3 ms - AT: 175 pps İyi huylu veri için, - ACC: %96,28 - PRE: %95,35 - REC: %97,38 Kötü huylu veri için, - PRE: %95,16 - REC: %97,27	- DBN [93] - ELM - NB [94]
[75]	KPNN: IoT ağlarındaki DDoS saldırılarını tespit etmek	- CICDDoS2019: Eğitim ve test için kullanılmaktadır.	- ACC: %94 - PRE: %91,22 - DR: %97,49 - FAR: %9,52 - ACT: 0,215 ms/veri	-

6. DEĞERLENDİRMELER (ASSESSMENTS)

İncelenen çalışmalar değerlendirildiğinde, birçok çalışmanın farklı eksikliklerinin olduğu sonucuna varılmaktadır. Bu eksiklikler aşağıdaki gibi özetlenmektedir:

- [48], [62], [72], [73] çalışmaları dışında, diğer incelenen çalışmalarda önerilen yaklaşımların gerçek bir ortamda test edilmemektedir. Dolayısıyla, bu yaklaşımların gerçek bir ortamda gösterecekleri performanslar tahmin edilememektedir.
- [12], [44], [48], [64], [72], [73], [75] çalışmaları dışında, diğer incelenen çalışmalarda kullanılan makine öğrenimi ve derin öğrenme modellerinin, hangi gerekçeler nedeniyle kullanıldıklarından detaylı ve tatmin edici bir şekilde bahsedilmemektedir. Bu nedenden dolayı, önerilen yaklaşımlarda kullanılan modeller dışında, hangi farklı modellerin kullanılabileceği sorusunu mantıklı bir şekilde yanıtlamak zor olmaktadır.
- İncelenen çalışmalarda, gerçek bir ortamdan veya simülasyon araçları tarafından elde edilen veriler ile oluşturulan veri kümeleri, herkese açık bir platformda paylaşılmamaktadır. Böylece, önerilen yaklaşımların elde ettikleri performans değerleri sorgulanabilir hale gelmektedir. Ayrıca, diğer araştırmacılar tarafından bu veri kümelerinin geliştirilmesi ve kullanılabilirliklerinin değerlendirilmesi için, veri kümelerinin herkese açık bir şekilde paylaşılması gerekmektedir.

- Önerilen yaklaşımların, farklı saldırılara karşı güvenlik açıklarından bahsedilmemektedir. Daha açık bir ifadeyle, önerilen sistemler, çerçeveler veya yöntemler, belli saldırı türlerine karşı güvenli olacak şekilde geliştirilmişlerdir. Farklı veya bilinmeyen saldırı türlerine karşı güvenlik seviyeleri tahmin edilmemektedir. Sonuç olarak, önerilen yaklaşımların gerçek bir ortamda kullanılabilirlikleri tartışmaya açık bir hale gelmektedir.
- [73], [75] çalışmaları dışında, diğer incelenen çalışmalarda kullanılan makine öğrenimi ve derin öğrenme modellerinin, kısıtlı kaynaklara sahip IoT cihazlarındaki kaynak tüketimlerinin analizi yapılmamaktadır. Dolayısıyla, kaynak tüketimi analizi yapılmayan modelleri içeren yaklaşımların, gerçek bir IoT ortamındaki verimlilikleri bilinmemektedir.
- [73] dışındaki çalışmalarda, önerilen yaklaşımların gerçek bir saldırı senaryosunda, saldırılara karşı tepki süreleri ölçülmemektedir. Bu nedenden dolayı, tepki süreleri bilinmeyen yaklaşımların, gerçek zamanda saldırılara karşı güvenlikleri gizliliğini korumaktadır.
- İncelenen çalışmalarda, kullanılan makine öğrenimi ve derin öğrenme modellerinin kaynak kodları, herkese açık bir platformda paylaşılmamaktadır. Dolayısıyla, bu modellerin, çalışmalarda belirtildiği gibi inşa edilip edilmedikleri bilinmemektedir. Ayrıca, modellere ait kaynak kodların paylaşılması, kodları inceleyen araştırmacılara, gelecekte yapacakları çalışmalar için katkıda bulunması açısından önemlidir.

7. SONUÇ (CONCLUSION)

Bu sistematik literatür derlemesinde, IoT ağlarındaki anormallik tabanlı saldırıları tespit etmek için, makine öğrenimi ve derin öğrenme modellerini kullanan çalışmalar incelenmiştir. İncelenen çalışmalar, Scopus, IEEE Xplore, WoS ve ScienceDirect akademik veri tabanlarından, Tablo 4'teki sorgu cümleleri yardımıyla elde edilmektedir. Sorgular sonucu elde edilen çalışmalar arasından 15 tanesi, yayımlanma yılları 2019 ve 2021 yılları arasında olacak şekilde, Tablo 5'te verilen seçme ve eleme kriterlerine göre seçilmiştir.

Bu derlemede ilk olarak, seçilen çalışmalarda önerilen yaklaşımlar hakkında kısa bilgiler verilmektedir. Ardından, bunların altında yatan ana düşünceler, avantajları ve dezavantajları Tablo 6'da özetlenmiştir. İkinci olarak, yaklaşımlarda kullanılan makine öğrenimi ve derin öğrenme modellerinin performansının değerlendirilmesinde kullanılan metrikler, Tablo 7'de sunulmuştur. Üçüncü olarak, modellerin eğitim ve test aşamalarında kullanılan veri kümelerine ait çeşitli bilgiler, Tablo 8'de açıklanmıştır. Dördüncü olarak, modellerin kullanım amaçları, eğitim ve test aşamalarında hangi veri kümelerinin kullanıldığı, deneyler sonucunda ulaştıklan performans değerleri ve karşılaştırıldıkları modeller, Tablo 9'da detaylandırılmıştır. Son olarak ise, incelenen çalışmalarda karşılaşılan eksikliklerden kısaca bahsedilmiştir. Sonuç olarak, bu derlemede, IoT ağlarındaki anormallik tabanlı saldırıları tespit etmek için, makine öğrenimi ve derin öğrenme modellerinden oluşan yaklaşımlar hakkında ayrıntılı bilgiler verilmiştir.

Bu derleme sadece, makine öğrenimi ve derin öğrenme modelleri kullanılarak, IoT ağlarındaki anormallik tabanlı saldırıların tespiti üzerine gerçekleştirilen çalışmalara odaklanmaktadır. Gelecek derleme çalışmasında, IoT ortamlarında gerçekleştirilen, fiziksel saldırıların, ağ saldırılarının, yazılım saldırılarının ve şifreleme saldırılarının tespiti için kullanılan makine öğrenimi ve derin öğrenme modellerinin incelenmesi hedeflenmektedir.

KAYNAKLAR (REFERENCES)

[1] R. Kandaswamy ve D. Furlonger, **Blockchain-based transformation: A gartner trend insight report**, Gartner, 2018.

[2] P. Newman, "THE INTERNET OF THINGS 2020: Here's what over 400 IoT decision-makers say about the future of enterprise connectivity and how IoT companies can use it to grow revenue", *Bus. Insid.*, 1–6, 2020.

[3] M. Almseidin, M. Alzubi, S. Kovacs, ve M. Alkasassbeh, "Evaluation of machine learning algorithms for intrusion detection system", **2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY)**, Subotica, 277–282, 14-16 September, 2017.

[4] I. Corona, G. Giacinto, ve F. Roli, "Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues", *Inf. Sci. (Ny).*, 239, 201–225, 2013.

[5] M. A. Lawal, R. A. Shaikh, ve S. R. Hassan, "Security analysis of network anomalies mitigation schemes in IoT networks", *IEEE Access*, 8, 43355–43374, 2020.

[6] J. P. Anderson, "**Computer security threat monitoring and surveillance**", Tech. Report, 1980.

[7] P. Shukla, "ML-IDS: A machine learning approach to detect wormhole attacks in Internet of Things", **2017 Intelligent Systems Conference (IntelliSys)**, London, 234–240, 7-8 September, 2017.

[8] A. Mehmood, M. Mukherjee, S. H. Ahmed, H. Song, ve K. M. Malik, "NBC-MAIDS: Naive Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks", *J. Supercomput.*, 74(10), 5156–5170, 2018.

[9] A. Saeed, A. Ahmadinia, A. Javed, ve H. Larijani, "Intelligent intrusion detection in low-power IoTs", *ACM Trans. Internet Technol.*, 16(4), 1–25, 2016.

[10] T. Luo ve S. G. Nagarajan, "Distributed anomaly detection using autoencoder neural networks in wsn for iot", **2018 IEEE international conference on communications (icc)**, Kansas City, 1–6, 20-24 May, 2018.

[11] N. Moustafa, B. Turnbull, ve K.-K. R. Choo, "An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things", *IEEE Internet Things J.*, 6(3), 4815–4830, 2018.

[12] S. J. Lee *vd.*, "IMPACT: Impersonation attack detection via edge computing using deep autoencoder and feature abstraction", *IEEE Access*, 8, 65520–65529, 2020.

[13] K. S. Sahoo, D. Puthal, M. Tiwary, J. J. P. C. Rodrigues, B. Sahoo, ve R. Dash, "An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics", *Futur. Gener. Comput. Syst.*, 89, 685–697, 2018.

[14] L. Xiao, X. Wan, X. Lu, Y. Zhang, ve D. Wu, "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?", *IEEE Signal Process. Mag.*, 35(5), 41–49, 2018.

[15] F. Liang, W. G. Hatcher, W. Liao, W. Gao, ve W. Yu, "Machine learning for security and the internet of things: the good, the bad, and the ugly", *IEEE Access*, 7, 158126–158147, 2019.

[16] M. Fahim ve A. Sillitti, "Anomaly detection, analysis and prediction techniques in iot environment: A systematic literature review", *IEEE Access*, 7, 81664–81681, 2019.

[17] F. Hussain, R. Hussain, S. A. Hassan, ve E. Hossain, "Machine learning in IoT security: Current solutions and future challenges", *IEEE Commun. Surv. & Tutorials*, 22(3), 1686–1721, 2020.

[18] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, ve H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study", *J. Inf. Secur. Appl.*, 50, 102419, 2020.

[19] M. A. Amanullah *vd.*, "Deep learning and big data technologies for IoT security", *Comput. Commun.*, 151, 495–517, 2020.

[20] H. Wu, H. Han, X. Wang, ve S. Sun, "Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey", *IEEE Access*, 8, 153826–153848, 2020.

[21] S. M. Tahsien, H. Karimipour, ve P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey", *J. Netw. Comput. Appl.*, 161, 102630, 2020.

[22] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, ve M. Guizani, "A survey of machine and deep learning methods for internet of things (IoT) security", *IEEE Commun. Surv. & Tutorials*, 22(3), 1646–1685, 2020.

[23] Y. Yue, S. Li, P. Legg, ve F. Li, "Deep Learning-Based Security Behaviour Analysis in IoT Environments: A Survey", *Secur. Commun. Networks*, 2021, 2021.

[24] R. Ahmad ve I. Alsmadi, "Machine learning approaches to IoT security: A systematic literature review", *Internet of Things*, 100365, 2021.

[25] L. Aversano, M. L. Bernardi, M. Cimitile, ve R. Pecori, "A systematic review on Deep Learning approaches for IoT security", *Comput. Sci. Rev.*, 40(100389), 2021.

[26] A. Thakkar ve R. Lohiya, "A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges", *Arch. Comput. Methods Eng.*, 28(4), 3211–3243, 2021.

[27] F. A. Alaba, M. Othman, I. A. T. Hashem, ve F. Alotaibi, "Internet of Things security: A survey", *J. Netw. Comput. Appl.*, 88, 10–28, 2017.

[28] M. Ammar, G. Russello, ve B. Crispo, "Internet of Things: A survey on the security of IoT frameworks", *J. Inf. Secur. Appl.*, 38, 8–27, 2018.

[29] R. Pecori, P. Ducange, ve F. Marcelloni, "Incremental learning of fuzzy decision trees for streaming data classification", **11th Conference of the European Society for Fuzzy Logic and Technology (EUSFLAT 2019)**, Ostrava, 748–755, 9-13 September, 2019.

[30] T. Winter *vd.*, "IPv6 routing protocol for low-power and lossy networks", *RFC6550 IETF*, 2012.

[31] E. Ahmed *vd.*, "The role of big data analytics in Internet of Things", *Comput. Networks*, 129, 459–471, 2017.

[32] M. F. Elrawy, A. I. Awad, ve H. F. A. Hamed, "Intrusion detection systems for IoT-based smart environments: a survey", *J. Cloud Comput.*, 7(1), 1–20, 2018.

[33] E. Osterweil, A. Stavrou, ve L. Zhang, "20 years of ddos: a call to action", *arXiv Prepr. arXiv1904.02739*, 2019.

[34] S. Alzahrani, L. Hong, ve others, "Generation of ddos attack dataset for effective ids development and evaluation", *J. Inf. Secur.*, 9(04), 225, 2018.

[35] M. Antonakakis *vd.*, "Understanding the mirai botnet", **26th USENIX security symposium (USENIX Security 17)**, Vancouver, BC, Canada, 1093–1110, 16-18 August, 2017.

[36] N. Moustafa, J. Hu, ve J. Slay, "A holistic review of network anomaly detection systems: A comprehensive survey", *J. Netw. Comput. Appl.*, 128, 33–55, 2019.

[37] K. Lakshminarayanan, D. Adkins, A. Perrig, ve I. Stoica, "Taming IP packet flooding attacks", *ACM SIGCOMM Comput. Commun. Rev.*, 34(1), 45–50, 2004.

[38] M. A. Khan ve K. Salah, "IoT security: Review, blockchain solutions, and open challenges", *Futur. Gener. Comput. Syst.*, 82, 395–411, 2018.

[39] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, ve P. Faruki, "Network intrusion detection for IoT security based on learning techniques", *IEEE Commun. Surv. & Tutorials*, 21(3), 2671–2701, 2019.

[40] A. K. Das, S. Zeadally, ve D. He, "Taxonomy and analysis of security protocols for Internet of Things", *Futur. Gener. Comput. Syst.*, 89, 110–125, 2018.

[41] F. Hussain, A. Anpalagan, A. S. Khwaja, ve M. Naeem, "Resource allocation and congestion control in clustered M2M communication using Q-learning", *Trans. Emerg. Telecommun. Technol.*, 28(4), e3039, 2017.

[42] Y. Zhang, P. Li, ve X. Wang, "Intrusion detection for IoT based on improved genetic algorithm and deep belief network", *IEEE Access*, 7, 31711–31722, 2019.

[43] M. Tavallaee, E. Bagheri, W. Lu, ve A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set", **2009 IEEE symposium on computational intelligence for security and defense applications**, Ottawa, Canada, 1–6, 8-10 July, 2009.

[44] F. Li, A. Shinde, Y. Shi, J. Ye, X.-Y. Li, ve W. Song, "System statistics learning-based IoT security: Feasibility and suitability", *IEEE Internet Things J.*, 6(4), 6396–6403, 2019.

[45] R.-H. Hwang, M.-C. Peng, C.-W. Huang, P.-C. Lin, ve V.-L. Nguyen, "An unsupervised deep learning model for early network traffic anomaly detection", *IEEE Access*, 8, 30387–30399, 2020.

[46] W. Wang, M. Zhu, X. Zeng, X. Ye, ve Y. Sheng, "Malware traffic classification using convolutional neural network for representation learning", **2017 International Conference on Information Networking (ICOIN)**, Da Nang, Vietnam, 712–717, 11-13 January, 2017.

[47] C. D. McDermott, F. Majdani, ve A. V Petrovski, "Botnet detection in the internet of things using deep learning approaches", **2018 international joint conference on neural networks (IJCNN)**, Rio, Brazil, 1–8, 8-13 July, 2018.

[48] Z. A. Baig, S. Sanguanpong, S. N. Firdous, T. G. Nguyen, C. So-In, ve others, "Averaged dependence estimators for DoS attack detection in IoT networks", *Futur. Gener. Comput. Syst.*, 102, 198–209, 2020.

[49] N. Koroniotis, N. Moustafa, E. Sitnikova, ve B. Turnbull, "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset", *Futur. Gener. Comput. Syst.*, 100, 779–796, 2019.

[50] M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K.-K. R. Choo, ve R. M. Parizi, "An ensemble of deep recurrent neural networks for detecting iot cyber attacks using network traffic", *IEEE Internet Things J.*, 7(9), 8852–8859, 2020.

[51] N. Goldenberg ve A. Wool, "Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems", *Int. J. Crit. Infrastruct. Prot.*, 6(2), 63–75, 2013.

[52] C. Kolias, G. Kambourakis, A. Stavrou, ve S. Gritzalis, "Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset", *IEEE Commun. Surv. & Tutorials*, 18(1), 184–208, 2015.

[53] M. E. Aminanto ve K. Kim, "Detecting impersonation attack in WiFi networks using deep learning approach", *International Workshop on Information Security Applications*, 136–147, 2016.

[54] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, ve K. Kim, "Deep abstraction and weighted feature selection for Wi-Fi impersonation detection", *IEEE Trans. Inf. Forensics Secur.*, 13(3), 621–636, 2017.

[55] L. R. Parker, P. D. Yoo, T. A. Asyhari, L. Chermak, Y. Jhi, ve K. Taha, "Demise: Interpretable deep extraction and mutual information selection techniques for IoT intrusion detection", içinde *Proceedings of the 14th International Conference on Availability, Reliability and Security*, 2019, ss. 1–10.

[56] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, ve M. Guizani, "IoT malicious traffic identification using wrapper-based feature selection mechanisms", *Comput. & Secur.*, 94, 101863, 2020.

[57] K. Gong, Z. Xiao, ve X. Zhang, "The bijective soft set with its operations", *Comput. & Math. with Appl.*, 60(8), 2270–2278, 2010.

[58] W. Li, W. Meng, ve M. H. Au, "Enhancing collaborative intrusion detection via disagreement-based semi-supervised learning in IoT environments", *J. Netw. Comput. Appl.*, 161, 102631, 2020.

[59] R. P. Lippmann *vd.*, "Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation", **Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00**, South Carolina, 12–26, 25-27 January, 2000.

[60] C.-H. Mao, H.-M. Lee, D. Parikh, T. Chen, ve S.-Y. Huang, "Semi-supervised co-training and active learning based approach for multi-view intrusion detection", **Proceedings of the 2009 ACM symposium on Applied Computing**, Honolulu Hawaii, 2042–2048, 8-12 March, 2009.

[61] M. Roesch vd., "Snort: Lightweight intrusion detection for networks.", **LISA '99: Proceedings of the 13th USENIX conference on System administration**, Seattle Washington, 99(1), 229–238, 7-12 November, 1999.

[62] M. Bagaa, T. Taleb, J. B. Bernabe, ve A. Skarmeta, "A machine learning security framework for IoT systems", *IEEE Access*, 8, 114066–114077, 2020.

[63] Internet: G. ETSI, Zero-touch network and Service Management (ZSM); Reference Architecture, https://www.etsi.org/technologies/zero-touch-network-service-management, 17.07.2021.

[64] Y. Jia, F. Zhong, A. Alrawais, B. Gong, ve X. Cheng, "Flowguard: an intelligent edge defense mechanism against IoT DDoS attacks", *IEEE Internet Things J.*, 7(10), 9552–9562, 2020.

[65] I. Sharafaldin, A. H. Lashkari, S. Hakak, ve A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy", **2019 International Carnahan Conference on Security Technology (ICCST)**, Chennai, India, 1–8, 1-3 October, 2019.

[66] M. Shafiq, Z. Tian, Y. Sun, X. Du, ve M. Guizani, "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city", *Futur. Gener. Comput. Syst.*, 107, 433–442, 2020.

[67] H.-T. Nguyen, D.-H. Nguyen, Q.-D. Ngo, V.-H. Tran, ve V.-H. Le, "Towards a rooted subgraph classifier for IoT botnet detection", **Proceedings of the 2019 7th International Conference on Computer and Communications Management**, New York, 247–251, 27-29 July, 2019.

[68] H.-T. Nguyen, Q.-D. Ngo, D.-H. Nguyen, ve V.-H. Le, "PSI-rooted subgraph: A novel feature for IoT botnet detection using classifier algorithms", *ICT Express*, 6(2), 128–138, 2020.

[69] H.-T. Nguyen, Q.-D. Ngo, ve V.-H. Le, "IoT botnet detection approach based on PSI graph and DGCNN classifier", **2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP)**, Singapore, 118–122, 28-30 September, 2018.

[70] Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, ve C. Rossow, "IoTPOT: A novel honeypot for revealing current IoT threats", *J. Inf. Process.*, 24(3), 522–533, 2016.

[71] Internet: VirusShare, "Because sharing is caring", https://virusshare.com/, 17.07.2021.

[72] N. Ravi ve S. M. Shalinie, "Semisupervised-Learning-Based Security to Detect and Mitigate Intrusions in IoT Network", *IEEE Internet Things J.*, 7(11), 11041–11052, 2020.

[73] N. Ravi ve S. M. Shalinie, "Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture", *IEEE Internet Things J.*, 7(4), 3559–3570, 2020.

[74] Internet: UNB-ISCX, Canadian Institute for Cybersecurity Datasets, https://www.unb.ca/cic/datasets/index.html, 17.07.2021.

[75] M. Almiani, A. AbuGhazleh, Y. Jararweh, ve A. Razaque, "DDoS detection in 5G-enabled IoT networks using deep Kalman backpropagation neural network", *Int. J. Mach. Learn. Cybern.*, 1–13, 2021.

[76] M. A. Ambusaidi, X. He, P. Nanda, ve Z. Tan, "Building an intrusion detection system using a filter-based feature selection algorithm", *IEEE Trans. Comput.*, 65(10), 2986–2998, 2016.

[77] N. Moustafa, G. Creech, ve J. Slay, "Big data analytics for intrusion detection system Statistical decision-making using finite dirichlet mixture models", **Data analytics and decision support for cybersecurity**, Springer, 127–156, 2017.

[78] C.-F. Tsai ve C.-Y. Lin, "A triangle area based nearest neighbors approach to intrusion detection", *Pattern Recognit.*, 43(1), 222–229, 2010.

[79] M. Z. Alom, V. Bontupalli, ve T. M. Taha, "Intrusion detection using deep belief networks", **Proc. IEEE Natl. Aerosp. Electron. Conf. NAECON**, USA, 339–344, 2016-March, 2016.

[80] C. Yin, Y. Zhu, J. Fei, ve X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks", *IEEE Access*, 5, 21954–21961, 2017.

[81] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, ve M. Ghogho, "Deep learning approach for Network Intrusion Detection in Software Defined Networking", **Proc. - 2016 Int. Conf. Wirel. Networks Mob. Commun. WINCOM 2016 Green Commun. Netw.**, Morocco, 258–263, 26-29 October, 2016.

[82] M. AL-Hawawreh, N. Moustafa, ve E. Sitnikova, "Identification of malicious activities in industrial internet of things based on deep learning models", *J. Inf. Secur. Appl.*, 41, 1–11, 2018.

[83] S. A. Ludwig, "Intrusion detection of multiple attack classes using a deep neural net ensemble", **2017 IEEE Symp. Ser. Comput. Intell. SSCI 2017 - Proc.**, Honolulu, HI, USA, 1–7, 27 November-1 December, 2018.

[84] B. Subba, S. Biswas, ve S. Karmakar, "Enhancing performance of anomaly based intrusion detection systems through dimensionality reduction using principal component analysis", **2016 IEEE Int. Conf. Adv. Networks Telecommun. Syst. ANTS 2016**, Bangalore, India, 1-6, August 2017.

[85] H. HaddadPajouh, A. Dehghantanha, R. Khayami, ve K.-K. R. Choo, "A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting", *Futur. Gener. Comput. Syst.*, 85, 88–96, 2018.

[86] R. Kozik, M. Choraś, M. Ficco, ve F. Palmieri, "A scalable distributed machine learning approach for attack detection in edge computing environments", *J. Parallel Distrib. Comput.*, 119, 18–26, 2018.

[87] S. Prabavathy, K. Sundarakantham, ve S. M. Shalinie, "Design of cognitive fog computing for intrusion detection in Internet of Things", *J. Commun. Networks*, 20(3), 291–298, 2018.

[88] S. Rathore ve J. H. Park, "Semi-supervised learning based distributed attack detection framework for IoT", *Appl. Soft Comput.*, 72, 79–89, 2018.

[89] A. A. Diro ve N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things", *Futur. Gener. Comput. Syst.*, 82, 761–768, 2018.

[90] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, ve K.-K. R. Choo, "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, 2019.

[91] S. U. Jan, S. Ahmed, V. Shakhov, ve I. Koo, "Toward a Lightweight Intrusion Detection System for the Internet of Things", *IEEE Access*, 7, 42450–42471, 2019.

[92] J. Li, Z. Zhao, R. Li, ve H. Zhang, "AI-Based Two-Stage Intrusion Detection for Software Defined IoT Networks", *IEEE Internet Things J.*, 6(2), 2093–2102, 2019.

[93] P. K. Sharma, S. Singh, ve J. H. Park, "OpCloudSec: Open cloud software defined wireless network security for the Internet of Things", *Comput. Commun.*, 122, 1–8, 2018.

[94] A. Mehmood, M. Mukherjee, S. H. Ahmed, H. Song, ve K. M. Malik, "NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks", *J. Supercomput.*, 74(10), 5156–5170, 2018.