Asia-Pacific Journal of Information Technology and Multimedia 12(1) 2023: 13 – 38
https://doi.org/10.17576/apjitm-2023-1201-02

Internet of Things (IoT) Intrusion Detection by Machine Learning (ML): A Review

Iman Farhadian Dehkordi[1], Kooroush Manochehri[2], Vahe Aghazarian[1]

[1]Department of Computer Engineering, Central Tehran Branch, Islamic Azad University, Tehran, Iran
[2]Department of Computer Engineering, Amirkabir University of Technology (Tehran Polytechnic), Garmsar Campus, Iran

**Corresponding author: iman.farhadian@gmail.com*

Received 1 October 2023
Accepted 17 January 2023, Available online 1 June 2023

ABSTRACT

One of today's fastest-growing technologies is the Internet of Things (IoT). It is a technology that lets billions of smart devices or objects known as "Things" collect different kinds of data about themselves and their surroundings utilizing different sensors. For example, it could be used to keep an eye on and regulate industrial services, or it could be used to improve corporate operations. But the IoT currently faces more security threats than ever before. This review paper discusses the many sorts of cybersecurity attacks that may be used against IoT devices. Also, K-Nearest Neighbour (KNN), Support Vector Machine (SVM), Decision Tree (DT), Random Forest (RF), Naive Bayes (NB), and Artificial Neural Network (ANN) are examples of Machine Learning (ML) approaches that can be employed in IDS. The goal of this study is to show the results of analyzing various classification algorithms in terms of confusion matrix, accuracy, precision, specificity, sensitivity, and f-score to Develop an Intrusion Detection System (IDS) model.

Keywords: Dataset; Internet of Things (IoT); Intrusion Detection System (IDS); IoT attacks; Machine Learning (ML)

INTRODUCTION

Electrical equipment is linked to a server and data is transferred without the intervention of people in the IoT (Chaabouni et al. 2019; Hassija et al. 2019; Khan & Salah 2018; Lu & Da Xu 2018; Singh et al. 2020; Stoyanova et al. 2020). Users can remotely manage machines from anywhere, making them vulnerable to lots of threats. So, the security of the IoT system is very concerned about the increasing number of smart devices today because the devices contain private and important user information (Hassija et al. 2019; Khan & Salah 2018; Singh et al. 2020). In his study presentation in 1999, Kevin Ashton first utilized the term IoT. IoT has been employed in various connectivity protocols to connect the person and the virtual world through various smart devices and services (Adat & Gupta 2018; Fawzi et al. 2019). Smart home and portable products, for instance, provide information about the buyer's position, health details, contact details, etc., that must be secure and confidential (Al-Sultan et al. 2019). Because most

IoT devices are resource-constrained (i.e., batteries, bandwidth, storage, and calculation), extraordinarily configurable and sophisticated protection strategies based on algorithms are not available (Ammar et al. 2018; Chernyshev et al. 2017; Vashi et al. 2017). Protecting IoT devices from hostile hackers presents some difficulties:

1. IoT devices must be able to work with a wide range of systems and protocols. They also need to meet a wide range of needs and expectations. A security administrator will have a lot of difficulty protecting all of these from an attacker (Restuccia et al. 2018).
2. One IoT device's security solution may not be suitable for another device. As a result, a single security solution will not be able to protect all IoT devices. Different companies create, manufacture, and deploy IoT devices. Thus, it is not obvious who will be accountable for the security of IoT devices.
3. IoT devices are small and light, with limited memory and processing capability.

The majority of security actions taken by manufacturers of IoT devices are built on computationally costly algorithms and protocols with significant overhead. As a result, it will be challenging to implement these ideas on IoT devices (Restuccia et al. 2018). All this data will be transferred wirelessly, which opens the IoT up to a variety of security risks such as jamming, message injecting, spoofing, denial of service, and eavesdropping (Chen et al. 2018). ML approaches are used in intrusion prevention and detection systems to detect malicious traffic. As a kind of AI, it employs algorithms to extract data's meaning and then makes predictions about the future using that meaning (Furbush 2018). Healthcare, finance, and retail are just a few of the industries where ML can be used. Customer spending habits are predicted, medical concerns are predicted, and bank fraud is detected using AI algorithms (Jmj 2018). Due to the significant yearly growth in cyberattacks, ML techniques are being combined to assist fight the growing dangers of cyberattacks. One of the numerous uses of machine learning in the area of cybersecurity is network threat analysis that may be described as assessing network threats (Dosal 2018). Incoming and outgoing traffic can be monitored using ML to identify possibly suspicious activity (Groopman & Insights 2019). In this context, intrusion detection is a well-researched topic. IDS utilize ML to enhance their capacity to operate autonomously and raise the alert on a suspected attack (Almseidin et al. 2017).

Anthi et al. (2019) proposed an innovative and intelligent three-layer IDS architecture. An investigation by Nugroho et al. (2020) indicated that employing DL algorithms and Artificial Neural Networks (RNN, DNN, and ANN) for intrusion classification yielded the highest percentage of success in 2015-2020. Based on the results of the experimental research by Islam et al. (2021), it can be stated that Bi-LSTM beats all other DL approaches in this study of numerous datasets. Seyfollahi and Ghaffari (2021) provided a comprehensive overview of IoT intrusion research. A systematic literature review of IoMT security and privacy challenges, as well as how ML technologies are employed to solve them, was published by Hameed et al. (2021). Adnan et al. (2021) gave a review of the literature on the issue of IDSs and their problems. Si-Ahmed et al. (2022) did a detailed survey on how to protect the IoMT using an IDS-based ML system. Eriza and Survadi (2021) listed some IDS directions for IoT attacks. As can be seen, in recent years, there have been a lot of reviews and surveys in this field, which indicates the importance of this topic. In contrast, the majority of reviews and survey papers just compare various works and don't go into detail about the numerous kinds of IoT attacks that may be launched. This review paper was produced to be put next to other papers because of the importance of this. We believe our priority is to find out which of the many ML methods will have the most impact in preventing hacks against the IoT networks. As a result, what

makes this review stand out from others is the effort made to gather all the information required to comprehend the ideas on a fundamental level. Studying this paper will help the reader better understand IoT networks, attack types, machine learning basics, and some popular datasets offered for IDSs and IoT IDSs. The following are the paper's main contributions:

1. The definition, layers, and challenges of IoT are examined.
2. As part of the IoT, recent and possible attacks are being looked into.
3. A variety of ML approaches are discussed.
4. Some popular datasets in IDSs and IoT IDSs are examined.
5. The classification performance of several ML approaches is summarized.

The following is a summary of the contents of the paper: The IoT will be introduced in Section 2. Section 3 will discuss various IoT security attacks, and Section 4 will discuss IoT intrusion detection methods and ML algorithms. Section 5 provides an overview of some of the most recent IoT intrusion detection datasets. Section 6, on the other hand, contrasts, and analyses performance ratings of similar works. Section 7 has conclusion and future insight.

IOT DEFINITION

The IoT refers to the trillions of physical objects connected to the internet and worldwide storage and data exchange. Anything from pill to aircraft can now be transformed into a part of IoT by the evolution of expensive computer chips and a broad-based wireless network (Ameen & Ali 2018; Hassan et al. 2021; Malallah et al. 2021; Zebari et al. 2019). By connecting and joining sensors to all these different things, AI is used to otherwise dumb things so they can share real-time data without requiring a human. IoT makes our society more intelligent and adaptive and fuses the digital and physical worlds (Alaba et al. 2017; Arko et al. 2019; Khalid & Ameen 2021; Nižetić et al. 2020).

IOT LAYERS

Perception layer

The perception layer consists of sensors and actuators (Khattak et al. 2019). Sensors sense their surroundings, whereas actuators operate as controllers, taking action depending on the data they collect. Node capturing attacks that an attacker grabs or replaces a sensor with a malicious node, are possible. The attacker can inject false or malicious code into these nodes via an over-the-air firmware or software upgrade, resulting in false data injection or malicious code injection attacks (OS & Bhanu 2018).

Network layer

The sensing layer delivers data to the network layer, which the computational unit processes further. Multi-device attacks make this layer highly susceptible (Mrabet et al. 2020). Because data is so important, and data breaches are simpler to commit during the data transmission stage, IoT devices are vulnerable to Data Transit attacks.

Application layer

Smart applications including healthcare, smart homes, smart cities, and others are found in the application layer. Because this layer interacts with end-users directly, data theft and privacy are key problems (Tewari & Gupta 2020). This layer, like the others, is vulnerable to a malicious code injection attack. Service interruption attacks are similar to denial of service attacks in that they disrupt service. During an attack, certain users are granted the unique

privilege of giving legal users access, but if this access is hacked, the entire system can be attacked. As a result, access control attacks at the application layer are a serious concern (Ahlawat et al. 2020). Figure 1 shows the Three-layer IoT architecture.

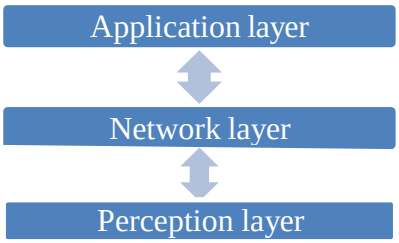

FIGURE 1. Three-layer IoT architecture

IoT security challenges

In the 21st century, IoT device security has been a burning problem. On one side, IoT connects the whole universe and takes it close. On the other, it opens various windows for attacks of various kinds (Tahsien et al. 2020; Yang et al. 2017; Zeebaree et al. 2020).

IoT apps are applied across an open network for various purposes, making their devices more user-friendly (Ali & Ameen 2018). On the one hand, IoT places human life at greater risk due to various risks and attacks; on the other hand, IoT makes it simpler and more compliant in technical terms (Fawzi et al. 2018; Makhdoom et al., 2018). IoT device security is becoming a burning concern because IoT devices are accessed from anywhere without user consent (Aziz & Ameen 2021; Fawzi et al. 2018). A wide kind of security system must be deployed to secure IoT products. However, IoT device's physical structure limits their computer functionality, limiting the implementation of a complex security protocol (Abomhara & Køien 2015; Benkhelifa et al. 2018).

It is necessary to consider the features that characterize protection when defining a stable IoT. Security specifications are grouped into three major sections in a standard IoT program: confidentiality, integrity, and authentication (Oracevic et al. 2017).

1. In keeping information hidden from third people, confidentiality means discretion. Sensitive sensors demand privacy, for example, with crucial military information. The WSN system is one of the most often requested features. If a WSN's reports are manipulated, forces may be misled, which might benefit the adversary. In vital social and industrial applications, confidentiality is equally critical (Oracevic et al. 2017).
2. To maintain the integrity of IoT data, the communication receiver must confirm that messages received during transmission or delivery have not been altered. The integrity of the data confirms that the sent data is not altered or distorted. It is particularly significant because even when intruders cannot obtain data, the network may not perform effectively if compromising nodes damage the sent data. Indeed, data is modified without an intruder if the communication connection is not dependable. Integrity control guarantees that accidental and deliberate changes in the message are detected (Oracevic et al. 2017).
3. The authentication process determines if a communication comes from where it is claimed or what it is proclaimed to be. The sensor nodes shall determine the identification and authenticity of the peer node they are conveying. Authenticity ensures an authentic message. MAC is brief information used for message authentication and provides the message's integrity and validity (Fawzi et al. 2016; Oracevic et al. 2017).

IOT ATTACKS

IoT devices come with a high level of danger. Attackers routinely take advantage of the ease and low cost of IoT device cyber-attacks to get valuable data. As a result of most IoT security flaws, services might be disrupted, and sensitive data exposed. These security risks may potentially be physical security threats, posing a risk to human life.
It's possible that cybercriminals may utilise security holes in IoT devices to acquire access to our personal information. The many types of cybersecurity attacks that may be employed against IoT systems will be discussed in this section.

Physical attacks

The IoT exposes a greater physical access and possible attacks due to its distributed and dispersed nature. A node or sensor's data might be altered by an attacker, putting the whole sensor network at risk. Attackers must physically access an IoT device before they can launch an attack on its hardware components (Rizvi et al. 2018). These attacks may compromise the IoT hardware's operation.

Node tampering

Sensor nodes may be damaged via node tampering, which is a physical attack on an IoT device that compromises its security. Access to and modification of sensitive data like shared cryptographic keys will be made possible via the physical modification of the node as a whole or a portion of it. (Andrea et al. 2015).

Side-channel analysis

A hacker might employ side-channel analysis to get the AES secret keys used in connected streetlights as part of a physical attack on the IoT. The noninvasive attack of acquiring sensitive data, including secret keys, by looking at the electromagnetic radiation or power signature generated by an IC is known as side-channel analysis (Meneghello et al. 2019). Connected streetlights update their firmware using AES encryption. It also protects the security of these modifications by limiting their accessibility to those who have the AES secret keys. In the event an attacker gains access to these secret keys, the streetlight network will be under their control. These attacks can only be carried out if the attacker is close enough to the device. The security of medical devices, portable devices, and bank cards can be at risk from these attacks.

Radiofrequency jamming

IoT devices' wireless connections may be disrupted or prevented with the use of a radio frequency jammer. It has the ability to break network connections in IoT devices, limiting their capacity to interact with the internet (Butun et al. 2019).

NETWORK ATTACKS

The bulk of these attacks take place on IoT networks. In order to conduct these attacks, the attacker doesn't need to be near the network.

Traffic Analysis Attack

It is referred to as a "traffic analysis attack" on a network when an attacker intercepts and examines communications in order to obtain information from communication patterns (Butun et al. 2019). Personal information and other data may be sniffed by an attacker due to IoT devices' wireless properties. Before attempting this kind of attack, an attacker will

attempt to gather network information. He can accomplish this by employing sniffing software such as packet sniffers, port scanners, and so on.

An attacker may get useful information from IoT network packets via timing and frequency analysis. An IoT device that uses SSH for authentication can be the target of a timing attack by an attacker. Because SSH transmits every keystroke message during the interactive session, he'll use the time information to make passwords weaker.

Selective Forwarding

Network nodes that transmit traffic along the right route might be targeted by this attack, which occurs when a network node drops part of the data passing through it. Selective forwarding attacks come in a variety of forms. As an example, a malicious node may drop packets from a specific node or a set of nodes. A DoS attack may be carried out on one node or a group of nodes due to this vulnerability (Leloglu 2016). A "neglect and greed" attack is another type of selective forwarding attack. In this case, the infected node misses a number of messages at random (Leloglu 2016).

Sybil Attack

It is possible for an attacker to appear in several places at once by using the Sybil Node, which is a rogue node that imitates other nodes (Husamuddin & Qayyum 2017). A hacker's Sybil attack may result in neighboring WSN nodes accepting false information. A Sybil node, for example, may vote many times in a WSN voting system, leading to a fake decision (Husamuddin & Qayyum 2017).

Sinkhole Attack

Sinkhole attacks on IoT devices may be used to take control of a network node by stealing all traffic from surrounding nodes (Abdul-Ghani et al. 2018). In addition to causing network congestion, this attack might also lead to higher node energy consumption. The IoT may also be vulnerable to DoS attacks if all packets are rejected instead of being sent to the target.

Botnet Attack

It is a group of malware-infected devices connected to the internet and monitored by hackers. DDoS, credential leaks, illegal access, and data theft attacks are just a few of the botnet tactics that cybercriminals employ (Wright & Cache 2015).

IoT botnets are being built to launch botnet attacks because of the abundance of unprotected IoT devices. A botnet attack involves an attacker planting malware in IoT devices to accept instructions from command and control servers and then carrying out harmful actions.

Hello-Flood Attack

There may be an abnormally large volume of worthless or unexpected messages in an attack known as the Hello Flood. An attacker may produce a huge volume of network traffic by repeatedly broadcasting a meaningless message from a rogue node (Hassan 2019).

Man in the Middle Attack

Intercepting or altering network traffic may be accomplished by a MITM attack, in which an attacker sits between two users (Abdul-Ghani et al., 2018). In order to do malicious acts like obtaining credentials or manipulating data, the attacker may pose as a genuine user.

Because of their inadequate security and lack of mitigation measures, many IoT devices are vulnerable to MITM attacks. Attackers may conduct these attacks through IoT by sending incorrect instructions to devices and acquiring control.

Application Attacks

Using application attacks, an attacker may get access to the private data of users and utilize it for their own purposes. Code injection and buffer overflow are two common application vulnerabilities that attackers use to gain unauthorized access to IoT applications. Attackers may compromise IoT application security by misconfiguring the code or using an unsecured API. Malware such as ransomware, rootkits, trojans, worms, viruses, and other forms of malware may potentially target IoT device applications for illegal access.

Code Injection

This attack takes advantage of software flaws to infiltrate the system with malicious malware. It is possible to use code injection attacks to steal important information from users, acquire complete control of the device, or disseminate malware (Chen et al. 2018). Code injection attacks are most often seen in HTML script injection and Shell injection. In the event that an attacker is successful in conducting a code injection attack, IoT devices will be rendered unresponsive, putting the privacy of their users at risk. It may also force any IoT gadget to shut down completely.

Buffer Overflow

A software or process in this attack writes additional data to a specified memory block or buffers. Buffer overflow attacks overflow buffer boundaries, allowing malicious code to be inserted. To store code and data segments, memory layouts or buffers are utilized in a variety of applications. These buffers contain boundaries that allow code and data to be collected. The buffer may overflow if an attacker delivers a lengthy data sequence to a specific section of the buffer. In such a case, it will alter the data in order to run malicious code, such as entering a code section and disturbing the program's control flow (Ling et al. 2017). Buffer overflow attacks include double-free, format string attacks, integer errors and stack/heap-based buffer overflows. One of the most common IoT application attacks is the buffer overflow (Chen et al. 2018). It could let an attacker become an administrator on an IoT device and run any code he wants on it. For example, hackers found a buffer overflow vulnerability in the ZyXel NBG6716 wifi router, which enabled them to take control of local networks (Ling et al. 2017).

SQL Injection

Whenever a malicious SQL query is sent to an unsecured SQL database field, a SQL injection occurs (Rizvi et al. 2018). SQL injection is a significant application threat that may impact a wide range of systems, including IoT. An attacker may get privilege escalations via SQL injection, providing him more control over the IoT system.

Session Hijacking

An attacker may use this technique to get access to the users' sensitive personal information. An attacker may mimic a legitimate user by using authentication and session management security flaws in a session hijacking attack (Leloglu 2016).

Authentication and Authorization Attacks

Authentication and authorization methods on many IoT devices are vulnerable, enabling attackers to remotely control and acquire administrative access to the device (Hassan 2019). Poor authentication and authorization systems often let people log in using weak passwords. Using a brute force attack, an attacker may rapidly get these passwords. Furthermore, if an attacker grants illegal administrative access to a file or directory, he may use this vulnerability to construct other attacks and gain administrator power. As soon as an attacker gets into a smart

home building's authentication and authorization systems, he may be able to do things like open the door.

Zigbee Attacks

A wireless network standard called Zigbee is used a lot in the IoT because it's cheap and doesn't use a lot of power (Meneghello et al. 2019). IoT devices, from home security routers to systems that keep track of patients in hospitals, often have it built in. Zigbee is often considered a natural choice for enabling IoT because of its low cost, low power, and simple technology (Abdul-Ghani et al. 2018). However, it is subject to a wide range of security concerns.

Eavesdropping Attack

An eavesdropping attack against Zigbee networks is possible since many of them do not utilize encryption. Even though Zigbee employs encryption, attackers may detect the existence of a Zigbee network using unencrypted Zigbee frame metadata such as node addresses, PAN IDs, and Mac addresses (Abdul-Ghani et al. 2018). An eavesdropping attack may be carried out using the KillerBee framework's zbdump utility (Wright & Cache 2015). The username and password of a user may be obtained via an eavesdropping attack.

Replay Attack

In a replay attack, an attacker will resend the frames exactly as they were sent by the original user (Abdul-Ghani et al. 2018). The content of replayed data, as well as the protocol used to send it, have a significant impact on the outcome of a replay attack. An attacker might, for example, collect data from a smart bulb's traffic. He can control the smart bulb's on/off the event by replaying these packets. Many ZigBee stacks are susceptible to replay attacks because they do not encrypt communication. An attacker might utilise the KillerBee zbreplay tool to execute replay attacks on Zigbee-enabled IoT devices (Wright & Cache 2015).

Packet Forging Attacks

Hackers inject packets into the Zigbee network to intercept or interrupt packets, which is known as packet forgery (Abdul-Ghani et al. 2018). These forge packets may seem to be normal. As a result, detecting malicious behavior as a result of packet forging attacks would be challenging.

Z-Wave Attacks

IoT devices utilize the Z-Wave protocol, which is a widely utilized wireless home automation protocol. Z-Wave wireless chipsets are embedded in millions of IoT devices, including heating systems, home alarms, lights, and door locks. It allows smart IoT devices to communicate, exchange data and instructions (Wright & Cache 2015). Several security exploits are possible against Z-Wave.

Z-Wave Downgrade Attack

The S2 Z-wave security pairing protection method is supported by Z-wave. An attacker, on the other hand, may degrade the higher S2 security level to the lower S0 security standard. Because of this, an attacker may be able to acquire an encryption key, making the device vulnerable to attack (Wright & Cache 2015).

As a result of this vulnerability, two connected smart devices may feel that one of them does not meet the higher S2 security standard. As a result, both may be forced to use the old S0 security standard. It is possible for a hacker to target IoT devices using the default encryption key for previous versions of S0 security, which is "0000000000000000" (Wright & Cache 2015).

Z-Wave Injection Attack

Integrity protection and basic encryption are missing from many Z-wave devices. An attacker may use this flaw to replay captured traffic or inject arbitrary packet content to manipulate Z- Wave nodes. (Wright & Cache 2015).

Z-Wave MITM Attack

It is possible for an attacker to get access to Z-Wave communications via an MITM attack. Numerous Z-Wave devices make no attempt to authenticate the controller's identity. Because any Z-Wave controller that supports the CLASS SECURITY command class may be used to intercept the integration process with a target device, an attacker can do so (Wright & Cache 2015). Victims might be persuaded to join a malicious network by using this. Table 1 shows the different kinds of cyber security attacks performed against IoT devices.

TABLE 1. Various cyber-attacks against IoT devices (Islam & Aktheruzzaman 2020)

Classification	Security Attacks	Security Impacts
Physical Attacks	Node tempering, Side-channel Analysis, Radiofrequency jamming	An IoT device might be physically damaged as well as its data corrupted by hackers utilizing these techniques.
Network Attacks	Traffic analysis, Selective forwarding, Sybil, Sinkhole, Botnet, Hello-flood, MITM	By using these vulnerabilities, hackers will be able to gain remote control of IoT devices and send them incorrect instructions.
Application Attacks	Code injection, Buffer overflow, SQL injection, Session Hijacking, Authentication and Authorization	As long as hackers can get into the IoT application layer, they will be able to get their hands on sensitive data.
Zigbee Attacks	Eavesdropping, Replay, Packet forging	In the process of these attacks, attackers will be able to gather sensitive data as well as Zigbee traffic.
Z-Wave Attacks	Downgrade, Injection, MITM	Through these attacks, attackers will be able to compromise the security of Z-Wave devices.

INTRUSION DETECTION SYSTEM

Monitoring of a network for potentially harmful traffic is made possible with the help of an IDS. Two different kinds of IDS may be used to implement an IDS. Signature-based detection is one of them, while anomaly-based detection is another. To detect whether incoming traffic is malicious, signature-based IDSs compare it to a database of previously identified attack signatures. It implies that an attack may be identified simply by looking up the signature in the database. Network traffic is analyzed by an anomaly-based IDS in order to look for unusual behavior within the normal flow of data.

Signature-based IDS has a major flaw in that it is always susceptible to new attacks or a hacker changing the attack to avoid being identified by the signature database. IDS based on anomalies may be trained to detect either normal or attack data, making them a better fit for ML. The integration of ML and IDS, however, does not come without its drawbacks. Sommer and Paxson (2010) found a number of issues in their research. One significant issue is that models may generate false positives, making the IDS useless since typical data causes it to alarm the system. Despite the study's age, it remains a critical concern when ML and

IDS are combined. So, it's critical to find models that generate the fewest false positives (Bhavani & Mangla 2022; Churcher et al. 2021; Otoum & Nayak 2021).

Intrusion detection using ML

It is necessary to keep in mind that ML is a branch of AI where a dataset is fed into an algorithm or, here, a model, which is used to find patterns and generate predictions based on the present data (Aminanto & Aminanto 2022). Only a little amount of study has been done on IDS utilizing ML on IoT networks. As a result, research recently utilized the DARPA ML datasets to evaluate models such as MLP, RF, NB, and SVM (Foley et al. 2020). RF was shown to be one of the best models for accuracy, receiver operating characteristic curve, mean absolute percentage error, and root means squared error. It's important to note, however, this research has two significant flaws: This study used datasets from DARPA that were almost two decades old when it was published. The datasets did not include any multi-class testing, which is another issue.

The Bot-IoT dataset was also utilized by Alsamiri and Alsubhi (2019), which included NB, MLP, adaptive boosting, RF, ID3, quadratic discriminant analysis, and KNN models. The study produced excellent accuracy, precision, sensitivity, time, and F1 score findings. This study made use of a current dataset and a range of ML algorithms. However, no multi-class testing was conducted in this research for any of the models.

The authors of Hasan et al. (2019) utilized various ML techniques for multi-class classifying. This study used a dataset produced by the researchers but not accessible to the general public to evaluate techniques such as ANN, RF, and DT. The research found that RF was a suitable classifier for multi-class classifying. This study discovered that high-quality results may be obtained using multi-class classifications. Additional algorithm testing may assist to improve the study findings.

Anthi et al. (2019) proposed an innovative and intelligent three-layer IDS architecture that can identify and differentiate between IoT devices in a network, detect malicious or benign network activity, and determine which attack was delivered on which connected device automatically. An investigation by Nugroho et al. (2020) indicated that employing DL algorithms and RNN, DNN, and ANN for intrusion classification yielded the highest percentage of success in 2015- 2020.

Based on the results of the experimental research by Islam et al. (2021), it can be stated that Bi-LSTM beats all other DL approaches in this study of numerous datasets. However, because of the huge data and other unforeseen circumstances, Bi-LSTM may not perform as expected. Seyfollahi and Ghaffari (2021) provided a comprehensive overview of IoT intrusion research. They looked at IoT IDSs and techniques that might be used in IoT IDSs from 2009 to 2021. These publications were classified using a categorization based on the following characteristics: authentication technique, IDS displacement, protection risk, identification method, and IDS architectonics. A look at the designs of IoT IDSs has led researchers to believe that they are still in the beginning stages.

A systematic literature review of IoMT security and privacy challenges, as well as how ML technologies are employed to solve them, was published by Hameed et al. (2021). By reviewing the research's content, such as methodologies, good features, limits, tools, and datasets, the outcomes of this study demonstrated that ML approaches are useful in tackling IoMT security challenges with promising results.

Adnan et al. (2021) gave a review of the literature on the issue of IDSs and their problems. The paper focused on the use of ML for IoT IDS. They looked at three major ML issues when dealing with IoT IDSs: evolving and concept drift, high dimensionality, and computational complexity.

Si-Ahmed et al. (2022) did a comprehensive survey on how to protect the IoMT using an IDS-based ML system. They introduced the general IoMT architecture. Then they listed the needs as well as potential risks to IoMT security. They then looked into ML-based approaches for IoMT protection and divided them into three categories: data collection, transmission, and storage, as well as the benefits, drawbacks, and datasets utilized. Finally, they discuss the many challenges and drawbacks of employing ML in these various areas. That study is meant to show that ML can protect complex systems like IoMT, as well as show that it can meet IoMT's unique rules.

Eriza and Survadi (2021) listed the following IDS directions for IoT attacks: A: To decrease the complexity, the relevance degree of each feature in the dataset may be evaluated. B: Any feature extraction approach may assist in obtaining a more accurate representation of the features. C: Particularly for IoT applications, lightweight is always desired.

A dearth of datasets and real hardware means that little research has been done on intrusion detection in IoT networks. All datasets use simulated IoT devices operating on standard PCs. Research on multi-class classification is similarly lacking, perhaps because a particular multi- class dataset doesn't exist. Data from all available datasets must be combined with proper labeling for each class before multi-class testing can be performed. ML tasks may be performed by a variety of models, each with its own set of mathematical equations that drive the data analysis (Kalnoor & Gowri 2022; Kumar et al. 2022; Kumar & Akthar 2022). We'll go through KNN, SVM, DT, RF, NB, and ANN, among other ML algorithms, in the following subsections.

K-Nearest Neighbor

As one of the most basic ML models, KNN seems to be a supervised learning model (Ali et al. 2019). KNN is lazy since it does not need any training, but it does use the training data when generating predictions to classify the data (Ali et al. 2019). KNN utilizes the Value of k, which can be updated to any number, and is used to find the data points that are the closest to each other. It is predicated on the notion that data points with similar characteristics would group (Harrison 2019). KNN is a good model for detecting intrusions, as shown by many studies. KNN's ability to discriminate between attack and non-attack data was examined by Liao and Vemuri (2002). This study found that KNN was an efficient attack data detection model with a low rate of false-positive rate. Furthermore, KNN's effectiveness was recently examined in Nikhitha and Jabbar (2019) and came to the same conclusion. The research found that KNN outperformed SVM and DT as an effective model.

Support Vector Machine

Using a hyperplane, the supervised learning approach SVM separates training data from future prediction classification. Hyperplanes are used to divide a dataset into two classes. Data points are classified according to these decision boundaries. SVM has been shown to be an effective model for detecting intrusions. In Yao et al. (2006) study, an improved SVM model was built for intrusion detection. The study was successful in developing the model, but it only proved to be a small improvement above conventional SVM, showing that the model can properly classify attack data without any enhancements or boosting. Other recent research evaluated the abilities of SVM and ANN to classify attack data (Cahyo et al. 2016). SVM

divides data using a hyperplane, which may be defined as follows:

$$ax + b = 0 \quad (1)$$

where a is the vector of the same dimensions as the input feature vector x and b is the bias. In this case, ax can be written as $a^1x^1 + a^2x^2 + \cdots + a^nx^n$ where n is the number of dimensions of the feature vector x. The following expression is used when making predictions:

$$y = sign(ax - b) \quad (2)$$

where $sign$ is a function that returns either $+1$ or -1 depending on whether the input is a positive number or a negative number. This value is used to define the prediction of what Class the feature vector belongs to. x_i is the feature vector and i and y_i is the label that can either be $+1$ or -1 and can be written as the follows:

$$ax_i - b \geq +1 \; if \; y_i = +1 \quad (3)$$

$$ax_i - b \leq -1 \; if \; y_i = -1 \quad (4)$$

There are mathematical functions used in SVMs, and these mathematical functions are referred to as kernels. The kernel gives data as input and converts it into the format needed for processing. RBF, Gaussian kernel, sigmoid, polynomial, nonlinear, Linear, and other kernels may be used.

Decision Tree

DTs have supervised learning algorithms that aid in the creation of a visual model representation. When creating a DT, you'll use a hierarchical model that looks like a network diagram with numerous interconnected nodes. As you can see from the tree structure, these nodes represent the attributes of the dataset that were tested. There is a link between these branches and another node or classification (Sharma & Kumar, 2016). The prediction data is processed via the nodes until it can be classified, and the training data is utilized to build the tree. Based on the study, DT is a good model for intrusion detection. DT was compared to many other models, like NB and KNN, in Stampar and Fertalj (2015) study. DT and NB were shown to be superior to ANNs, which dominated the IDS research. An IDS for connected cars in smart cities was developed by Aloqaily et al. (2019) research. The DT model was found to be the most accurate and had the lowest false-positive rate in this study. As previously stated, DT uses the training data to construct a hierarchical model that generates nodes that act as predictions tests. Selecting the root node as well as the other nodes that comprise the DT are necessary steps in creating the DT. So, with entropy being utilized in this case, there are a variety of options. Entropy measures the probability that a data point chosen at random will be incorrectly classified, and it is defined as follows:

$$E = \sum_{i=1}^{C} -P_i \, log_2(P_i) \quad (5)$$

where P_i is the probability of the data being classified to a given Class of i and C is the class's number. For the root node, the property with the lowest entropy is used.

Random Forest

In comparison to the DT model, the supervised learning method RF seems to be more efficient. Two fundamental ideas are responsible for the model's randomness. For model training, data is randomly distributed throughout the trees, thus some trees use the same data many times. The first concept says this. Model variance should be reduced to reduce the difference between predicted and actual results (Koehrsen 2018). When dividing nodes in trees, the second concept involves just utilizing a limited subset of the features (Dubey 2018). Overfitting happens when a model overfits itself by using training data to enhance its predictions. When making predictions using RF, the total data Class is calculated by averaging the predictions of the tree (Ali et al. 2019). Because several trees with a variety of training data and various feature selections are utilized for predictions rather than depending on one tree to classify, RF seems to enhance the DT. When generating predictions, it provides for a more balanced data analysis. The RF model works well for detecting intrusions. To this aim, Farnaaz and Jabbar (2016) compared RF's intrusion detection performance to that of other frameworks. They found that the RF model surpassed all others in terms of accuracy, precision, sensitivity, and F1 score.

Naive Bayes

NB is a probabilistic algorithm that calculates the probability of each feature vector and its outcome. When calculating the event probability occurring based on previous occurrences, the posterior probability method is employed. The following is a definition:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} \tag{6}$$

where $P(A|B)$ is the posterior probability, $P(A)$ is known as the prior probability, $P(B)$ is the marginal likelihood (evidence), and $P(B|A)$ is referred to as the probability. The following formula may be applied to datasets:

$$P(y|x) = \frac{P(x|y)P(y)}{P(x)} \tag{7}$$

where y is the variable of Class and x is the feature vector of size n shown as the following:

$$x = (x_1, x_2, x_3, \dots, x_n) \tag{8}$$

ANN

An ANN, an ML model based on the way the human brain functions and is informed by the human brain, can be employed to conduct supervised learning. Neurons or nodes are used to represent the layers of an ANN (Saritas & Yasar 2019). In an ANN, there are three layers: the input, the hidden, and the output layer. The input layer transfers any new information it receives to the hidden layer for further processing as soon as it is available. The results are sent to the output layer via the hidden layer. The output layer is responsible for displaying the ANN's results once they have been calculated (Karn 2016). During supervised learning, the network receives the required inputs and outputs to train. Weights are given to the connections between the network's nodes. Errors in the networks are propagated back to the nodes and new weights are applied as a result. This procedure is continued until the error is reduced to a minimum, at which point the test data may be sent into the network (Maind & Wankar 2014). The following is a description of how to train an ANN:

The initial stage in training the ANN is to multiply the input values x_i by the weights w_i and then sum the values as follows:

$$x_i.w_i \;=\; (x_1.w_1) \;+\; (x_2.w_2) \;+\; \cdots \;+\; (x_n.w_n) \tag{9}$$

The second step includes adding the summed values to the bias (b) of the hidden layer node as shown as the following:

$$z \;=\; x_i.w_i \;+\; b \tag{10}$$

The third step is to pass the z value through an activation function such as ReLU and Softmax. ReLU ($R_{(z)}$) can be determined as follows:

$$y \;=\; R(z) \;=\; max(0, z) \tag{11}$$

where z is the input to a neuron. When $z < 0$, the function will output 0, and, when $z \geq 0$, the output is simply the input. Softmax can be determined as follows:

$$y \;=\; s(z)i \;=\; \frac{e^{Zi}}{\sum_{j=1}^{n} e^{Zj}} \tag{12}$$

where e is the natural logarithm base, z is a vector of the inputs, and i and j sequentially indexes the input and output units.

The loss must be calculated during the ANN's training in order for the network to be able to assess its performance and make relevant changes. The next step is to compute the loss and then adjust the weights and biases in order to reduce the loss to the bare minimum. Gradients may be used to see how the cost function (C) varies in proportion to weights w_i (This is an estimate of a neural network's success based on the training data and predicted output). The C gradient for the weights was computed using the chain rule as follows:

$$\frac{\partial C}{\partial w_i} = \frac{\partial C}{\partial \hat{y}} \times \frac{\partial \hat{y}}{\partial z} \times \frac{\partial z}{\partial w_i} \tag{13}$$

where $\frac{\partial C}{\partial \hat{y}}$ is the gradient of the cost function, $\frac{\partial \hat{y}}{\partial z}$ is the gradient of the predicted value, and $\frac{\partial z}{\partial w_i}$ is the gradient of z in regard to w_i.

Attacks on IoT are best detected using an ANN, which has been used many times in the past. Anitha and Arockiam (2019) recently developed ANN-based models for identifying IoT-based attacks. When tested, the model performed well and may now be used to detect intrusions in IoT networks. Shenfield et al. (2018) demonstrate how to build ANNs for intrusion detection purposes. According to the findings of this study, the model showed an extremely low false- positive rate and near-perfect accuracy, resulting in outstanding outcomes.

INTRUSION DETECTION FOR IOT

While IDS technology has advanced significantly for traditional networks, existing solutions are insufficient for IoT devices. First of all, it is crucial to consider the processing and storage capabilities of network nodes that host IDS agents. System administrators in traditional networks generally place IDS agents on more powerful nodes. Nodes in IoT networks often have limited resources. As a result, it is more challenging to locate nodes in IoT systems that can host IDS agents. The network's structure is the second distinguishing feature. End devices are directly linked to specific nodes (e.g., wireless access points, switches, and routers) in traditional networks, which are responsible for forwarding packets to the destination. Multihop networks are typical in the IoT. Then, regular nodes can both forward packets and act as end devices at the same time. For example, sensors that can communicate over short distances are put on light poles in IoT-based street lighting systems (Shahzad et al. 2016). The data acquired by a sensor is then sent along a route of sensors installed on various light poles until it reaches an Internet gateway. IDSs have unique issues when dealing with this sort of architecture. The last feature is connected to certain network protocols. IEEE 802.15.4, 6LoWPAN, RPL, and CoAP are some of the protocols used in IoT networks that are not used in traditional networks. When implementing IDS, new requirements and vulnerabilities resulting from various protocols must be taken into consideration (Zarpelão et al. 2017). Except for the differences already mentioned, IDSs in common networks and IDSs in IoTs are the same.

MOST WELL-KNOWN DATASETS

There are several datasets offered for IDSs and IoT IDSs. This section talks about some popular datasets offered for IDSs and IoT IDSs because it's impossible to explain each one here.

KDD99

Since 1999, the KDD99 dataset has been the most widely used for detecting attacks based on data from the DARPA IDS assessment in 1998. There are 41 features in this dataset, and it may be classified as either a normal or a specific attack. Attacks include DoS, U2R, R2L, and probing attacks (Murali & Jamalipour, 2019).

NSL-KDD

The NSL-KDD dataset, which many people use as a benchmark, was made better from the main KDD'99 dataset by removing 78% and 75% of the train and test data, respectively (Dhanabal & Shantharajah, 2015). The dataset includes about 42 features (1 dependent, 41 independent) and a separate train and test set, designated as KDDTrain+ and KDDTest+, respectively, with total records of 125,973 and 22,544. In addition, there are 39 attacks divided into four classifications: DoS, Prob, U2R, and R2L (Tavallaee et al., 2009).

KYOTO

This dataset has 24 statistical features, 14 of which are standard and 10 of which are new. Using honeypot systems established at Kyoto University, the first 14 standard features were retrieved based on the KDD Cup 99 dataset. Song et al. (2011) have also added 10 more features, which will make it easier for them to study what is happening on the network.

IOT DEVICE NETWORK LOGS

Kaggle (Kaggle, 2020) is used to find IoT Device Network Logs, which are then preprocessed on IoT devices according to network based IDSs. The dataset contains 477,426 records with 14 different features that are divided into 5 classifications: Normal, Wrong Setup, DDoS, Data Type Probing, Scan, and MITM.

Distributed Smart Space Orchestration System

Pahl and Aubet (2018) provided the DS2OS, a publicly available open-source synthetic dataset gathered via Kaggle. They created the dataset by collecting application layer traffic traces for 24 hours from 4 distinct IoT sites with a variety of services: smartphones, smart doors, thermostats, batteries, washing machines, movement sensors, thermometers, and light controllers. The dataset includes 357,952 records, 13 features, and 8 non-identical classifications: DoS, Data type Probing, Malicious Control, Malicious Operation, Scan, Spying, Wrong Setup, and Normal.

IoT Intrusion Dataset 2020

The fifth dataset is the IoTID20, which was developed by Ullah and Mahmoud (2020a) and is based on Kang et al. (2019). A total of 625,783 records are contained within the IoTID20 dataset. 83 network features and 3 label features are included in the dataset. The total number of records is classified as follows: Mirai, Scan, DoS, Normal, and MITM. The following 7 subclasses are created from these classes: Mirai Brute force, Mirai HTTP Flooding, Mirai UDP Flooding, Scan Host Port, Scan Port OS, Syn Flooding, and ARP Spoofing.

IoT Botnet Dataset 2020

IoT Botnet Dataset 2020 was created utilizing a network traffic flow analysis tool in order to enhance and expand the amount of flow as well as network features based on a complete IoT network (Ullah & Mahmoud 2020b). There are 46 network features, 2 label features, and a few flow features in the original one. On the other hand, the developed one includes 83 network features, including 3 labeling features: ‘Label’, ‘Cat’, and ‘Sub_cat’. It has 1,940,389 records (10% of the whole dataset) and is classified into 2 labels: normal and anomalous, including 5 classes: DoS, DDOS, Reconnaissance, Normal, and Theft, that is further divided into 11 subclasses: Normal, DDoS-HTTP, DDoS-TCP, DDoS-UDP, DoS-HTTP, DoS-TCP, DoS-TCP, OS-Fingerprint, Service-Scan, Keylogging, and Data-Exfiltration (Islam et al. 2021).

ML CLASSIFIERS' PERFORMANCE

With the advancement of technology and the introduction of new kinds of malware, hackers are getting more complex and deadly, rendering conventional attack protection techniques ineffective. Because of this, securing an IoT system with minimal resources becomes more challenging. ML techniques are one of the most frequently utilized methods for detecting these attacks. Several ML techniques have been shown to be very useful in preventing security and privacy attacks. Table 2 summarizes the performance of different ML methods. RF, DT, NB, KNN, SVM, LDA, and others are examples of prominent ML methods. TPR and FPR are the true positive and false-positive rates, respectively, in Table 2.

TABLE 2. Malware, Intrusions, and Other Attacks Performance Comparison Using ML Algorithms

References	Feature Selection Techniques	Algorithm	Dataset	Results
Karmous et al. (2022)	-	CART	Light Motion	F1 score: 0.93971939
			Thermostat	F1 score: 1.000000
			Weather	F1 score: 0.999912
		KNN	Light Motion	F1 score: 0.93793367
			Thermostat	F1 score: 0.99997085
			Weather	F1 score: 0.9990051
		RF	Light Motion	F1 score: 0.94209184
			Thermostat	F1 score: 1.000000
			Weather	F1 score: 1.000000
Saheed et al. (2022)	PCA	XgBoost	UNSW-NB15	Accuracy: 99.99
				Precision: 1.00
				F1 score: 1.00
		CatBoost		Accuracy: 99.99
				Precision: 1.00
				F1 score: 99.99
		KNN		Accuracy: 99.98
				Precision: 1.00
				F1 score: 99.99
		SVM		Accuracy: 99.98
				Precision: 1.00
				F1 score: 99.99
		QDA		Accuracy: 99.97
				Precision: 99.99
				F1 score: 99.98
		NB		Accuracy: 97.14
				Precision: 96.72
				F1 score: 97.94
Manhas and Kotwal (2021)	-	KNN	KDD'99	Accuracy: 92.78
				Precision: 0.990684
				Recall: 82.05
				F1 score: 0.897615
		SVM		Accuracy: 92.59
				Precision: 0.989431
				Recall: 81.65
				F1 score: 0.894688
		MLP		Accuracy: 92.46
				Precision: 0.991393
				Recall: 81.14
				F1 score: 0.892455
		DT		Accuracy: 95.09
				Precision: 0.964311
				Recall: 90.64
				F1 score: 0.934463
		NB		Accuracy: 91.71
				Precision: 0.992839

				Recall: 79.06	
				F1 score: 0.880299	
Abdelmoumin et al. (2021)	-	SVM-PCA-NN (AUC)	IoT Botnet	Accuracy: 93.4	
				Precision: 93.4	
				Recall: 1	
				F1 score: 95.6	
			IoT Fridge	Accuracy: 85.2	
				Precision: 1	
				Recall: 0	
				F1 score: 0	
		SVM-PCA-NN (F1 Score)	IoT Botnet	Accuracy: 93.4	
				Precision: 93.4	
				Recall: 1	
				F1 score: 95.6	
			IoT Fridge	Accuracy: 85.2	
				Precision: 1	
				Recall: 0	
				F1 score: 0	
		SVM-PCA-NN (Accuracy)	IoT Botnet	Accuracy: 6.5	
				Precision: 0	
				Recall: 1	
				F1 score: 00	
			IoT Fridge	Accuracy: 85.2	
				Precision: 1	
				Recall: 0	
				F1 score: 0	
Liu et al. (2021)	BPSO	SVM	NSL-KDD	DoS attack	DR: 82.9
				DoS attack	FAR: 1.18
Saba et al. (2021)	GA	DT	NSL-KDD	Accuracy: 99.5	
		SVM		Accuracy: 99.2	
		Ensemble		Accuracy: 99.8	
Banadaki et al. (2021)	-	XGBoost	CICIDS2017	Accuracy: 99.6	
				Precision: 98.7	
				Recall: 98.4	
				F1 score: 97.9	
Ahmad et al. (2021)	-	RF	UNSW-NB15	Binary	Accuracy: 98.67
				Multiclass	Accuracy: 97.37
				Flow features	Accuracy: 96.96
				Transport features	Accuracy: 91.40
				Top features	Accuracy: 97.54
		SVM		Binary	Accuracy: 97.69
				Multiclass	Accuracy: 95.67
				Flow features	Accuracy: 89.78
				Transport features	Accuracy: 82.96
				Top features	Accuracy: 89.93
		ANN		Binary	Accuracy: 94.78
				Multiclass	Accuracy: 91.67
				Flow features	Accuracy: 86.37
				Transport features	Accuracy: 81.63
				Top features	Accuracy: 87.68

Taghavinejad et al. (2020)	CART	HDT	NSL-KDD	Accuracy: 83.1485	
				Precision: 97.2193	
				Recall: 72.4694	
				F1 score: 83.0394	
Kumar et al. (2019)	-	Improved NB	Collected from the Google Play Store and Chinese App store (6192 benign, 5560 malware apps)	TPR: 98.2	
				FPR: 98.2	
				Accuracy: 98	
		NB		TPR: 80.5	
				FPR: 80.7	
				Accuracy: 90.5	
		SVM		TPR: 95.2	
				FPR: 95.2	
				Accuracy: 95	
		KNN		TPR: 75.8	
				FPR: 87.5	
				Accuracy: 92	
Lei et al. (2019)	-	ANN	In 2014, PlayDrone provided 10956 benign samples (Viennot et al., 2014), Play Store provided 4000 new apps in 2018 (Google Play Store, 2019), and VirusShare provided 28848 harmful samples (VirusShare, 2019).	For 2014 and a benign dataset	Precision: 99.1
					Recall 99. 2
					F1 score: 99.8
				For 2018 and a benign dataset	Precision: 92.2
					Recall: 94.7
					F1 score: 93.4
Doshi et al. (2018)	-	KNN	Custom	Accuracy: 99.5	
		LSVM		Accuracy: 92.1	
		DT		Accuracy: 99.5	
		RF		Accuracy: 99.8	
		NN		Accuracy: 98.9	
Kumar et al. (2018)	-	RF	-	Features: Permission	Accuracy: 92.79
Abdulhammed et al. (2018)	ZeroR	AdaBoost	AWID	Best performance RF with 32 features	Accuracy: 99.64
		RF			
		RT			Precision: 0.995
		J48			
		logit Boost			Recall: 0.966
		MLP			

The suggested PCA-XgBoost, PCA-CatBoost, PCA-KNN, PCA-SVM, PCA-QDA, and PCA- NB by Saheed et al. (2022) showed excellent accuracy when compared to the TABLE 2. Their experimental findings were superior to previous papers regarding precision and F1 score, and also the accuracy of the two approaches they developed. They were 99.99% successful.

CONCLUSION AND FUTURE INSIGHT

This paper looks back at previous papers on the subject of intrusion detection. The major goal of this research was to look at the use of machine learning in IoT intrusion detection. As a result, the IoT's basic definition, layers, and challenges were investigated initially. Then there was a look at IoT attacks. The definition of IDS and several ML approaches were then given. Then, some popular datasets offered for IDSs and IoT IDSs were given. Finally, the performance of the previous papers in ML classifiers was investigated.

According to the review, which used numerous metric measures to assess classifier performance, The suggested PCA-XgBoost, PCA-CatBoost, PCA-KNN, PCA-SVM, PCA-QDA, and PCA-NB show excellent accuracy when compared to the TABLE 2. They were superior to previous papers regarding precision, F1 score, and accuracy of the two approaches they developed. They had a 99.99% success rate. To achieve excellent model performance, most researchers use the hybrid classification method rather than individual classification when designing intrusion detection systems. The complexity of large datasets can be reduced by using dimension reduction. As a result, the best features for classifying are chosen, which leads to better accuracy and speed.

Based on this review, an ML-based technique can be used to identify attacks on many types of IoT networks. It is possible to implement a variety of methods in ML today, including SVM, DT, RF, NB, ANN, AL, ND, and DL. Big data and IoT networks require a wide range of DL methods for IDSs. This algorithm may be implemented using any of the signature-based detection, anomaly-based detection, or hybrid IDS solutions.

ABBREVIATIONS

6LoWPA N	IPv6 over Low-power Wireless Personal Area Network	GA	Genetic Algorithm	ND	Novelty Detection
AES	Advanced Encryption Standard	HDT	Hybrid of Decision Trees	NN	Neural Network
AI	Artificial Intelligence	H-ELM	Hierarchical - Extreme Learning Machine	NSL- KDD	Network Security Laboratory - Knowledge Discovery in Databases
AL	Active Learning	HFSA	Hybridized Feature Selection Approach	PART	Partial decision tree algorithm
ANN	Artificial Neural Network	IC	Integrated Circuit	PCA	Principal Component Analysis
AUC	Area under the ROC Curve	ID3	Iterative Dichotomiser 3	PSO	Particle Swarm Optimization
AWID	Aegean Wi-Fi Intrusion Dataset	IDS	Intrusion Detection System	QDA	Quadratic Discriminant Analysis
BPSO	Binary Particle Swarm Optimization	IoMT	Internet of Medical Things	R2L	Remote-to-Local
CART	Classification And Regression Tree	IoT	Internet of Things	RBF	Radial Basis Function
CIC-IDS2017	Canadian Institute for Cybersecurity - Intrusion Detection Sysstem 2017	IoTID20	IoT Intrusion Dataset 2020	RF	Random Forest

CSE-CIC-IDS2018	Communications Security Establishment - Canadian Institute for Cybersecurity - Intrusion Detection Sysstem 2018	KDD	Knowledge Discovery in Databases	RFE	Recursive Feature Elimination
CNN	Convolutional Neural Network	KNN	K-Nearest Neighbor	RIPPER	Repeated Incremental Pruning to Produce Error Reduction
CoAP	Constrained Application Protocol	LDA	Linear Discriminant Analysis	RNN	Recurrent Neural Networks
DARPA	Defense Advanced Research Projects Agency	LSTM	Long Short-Term Memory	RPL	Low-Power and Lossy Networks
DDoS	Distributed Denial of Service	LSVM	Lagrangian Support Vector Machine	RT	Random Tree
DL	Deep Learning	MAC	Message Authentication Code	SDN	Software Defined Networks
DNN	Deep Neural Networks	MITM	Man In The Middle	SU	Symmetrical Uncertainty
DoS	Denial of Service	ML	Machine Learning	SVM	Support Vector Machine
S2OS	Distributed Smart Space Orchestration System	MLP	Multi-Layer Perceptron	U2R	User-to-Root
DT	Decision Tree	MNBIDS	Modified Naïve Bayes Intrusion Detection System	UNSW-NB15	University of New South Wales - New Benchmark 2015
ELM	Extreme Learning Machine	NB	Naive Bayes	WSN	Wireless Sensor Network

REFERENCES

Abdelmoumin, G., Rawat, D. B., & Rahman, A. 2021. On the performance of machine learning models for anomaly-based intelligent intrusion detection systems for the internet of things. *IEEE Internet of Things Journal*.

Abdul-Ghani, H. A., Konstantas, D., & Mahyoub, M. 2018. A comprehensive IoT attacks survey based on a building-blocked reference model. *International Journal of Advanced Computer Science and Applications*, *9*(3), 355-373.

Abdulhammed, R., Faezipour, M., Abuzneid, A., & Alessa, A. 2018. Effective features selection and machine learning classifiers for improved wireless intrusion detection. 2018 International symposium on networks, computers and communications (ISNCC),

Abomhara, M., & Køien, G. M. 2015. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 65–88-65–88.

Adat, V., & Gupta, B. B. 2018. Security in internet of things: issues, challenges, taxonomy, and architecture. *Telecommunication Systems*, *67*(3), 423-441.

Adnan, A., Muhammed, A., Abd Ghani, A. A., Abdullah, A., & Hakim, F. 2021. An intrusion detection system for the internet of things based on machine learning: Review and challenges. *Symmetry*, *13*(6), 1011.

Ahlawat, B., Sangwan, A., & Sindhu, V. 2020. IoT system model, challenges and threats. *Int. J. Sci. Technol. Res*, *9*(3), 6771-6776.

Ahmad, M., Riaz, Q., Zeeshan, M., Tahir, H., Haider, S. A., & Khan, M. S. 2021. Intrusion detection in internet of things using supervised machine learning based on application and transport layer features using UNSW-NB15 data-set. *EURASIP Journal on Wireless Communications and Networking*, *2021*(1), 1-23.

Al-Sultan, M. R., Ameen, S. Y., & Abduallah, W. M. 2019. Real time implementation of stegofirewall system. *International Journal of Computing and Digital Systems*, *8*(5), 498-504.

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. 2017. Internet of things security: A survey. *Journal of Network and Computer Applications*, *88*, 10-28.

Ali, N., Neagu, D., & Trundle, P. 2019. Evaluation of k-nearest neighbour classifier performance for heterogeneous data sets. *SN Applied Sciences*, *1*(12), 1-15.

Ali, Z. A., & Ameen, S. Y. 2018. Detection and prevention cyber-attacks for smart buildings via private cloud environment. *International Journal of Computing and Network Technology*, *6*(01), 27-33.

Almseidin, M., Alzubi, M., Kovacs, S., & Alkasassbeh, M. 2017. Evaluation of machine learning algorithms for intrusion detection system. 2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY),

Aloqaily, M., Otoum, S., Al Ridhawi, I., & Jararweh, Y. 2019. An intrusion detection system for connected vehicles in smart cities. *Ad Hoc Networks*, *90*, 101842.

Alsamiri, J., & Alsubhi, K. (2019). Internet of things cyber attacks detection using machine learning. *Int. J. Adv. Comput. Sci. Appl*, *10*(12), 627-634.

Ameen, S. Y., & Ali, A. L. S. H. 2018. A comparative study for new aspects to quantum key distribution. *Journal of Engineering and Sustainable Development*, *11*(1), 45-57.

Aminanto, A. E., & Aminanto, M. E. 2022. Deep learning models for intrusion detection in Wi-Fi networks: A literature survey. *Sustainable Architecture and Building Environment*, 115-121.

Ammar, M., Russello, G., & Crispo, B. 2018. Internet of things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, *38*, 8-27.

Andrea, I., Chrysostomou, C., & Hadjichristofi, G. 2015. Internet of things: Security vulnerabilities and challenges. 2015 IEEE symposium on computers and communication (ISCC),

Anitha, A. A., & Arockiam, L. 2019. ANNIDS: artificial neural network based intrusion detection system for internet of things. *Int. J. Innov. Technol. Explor. Eng. Regul*(2019), 8.

Anthi, E., Williams, L., Słowińska, M., Theodorakopoulos, G., & Burnap, P. 2019. A supervised intrusion detection system for smart home IoT devices. *IEEE Internet of Things Journal*, *6*(5), 9042-9053.

Arko, A. R., Khan, S. H., Preety, A., & Biswas, M. H. 2019. *Anomaly detection In IoT using machine learning algorithms* Brac University.

Aziz, Z. A. A., & Ameen, S. Y. A. 2021. Air pollution monitoring using wireless sensor networks. *Journal of Information Technology and Informatics*, *1*(1), 20-25.

Banadaki, Y., Brook, J., & Sharifi, S. 2021. Design of intrusion detection systems on the internet of things infrastructure using machine learning algorithms. NDE 4.0 and Smart Structures for Industry, Smart Cities, Communication, and Energy,

Benkhelifa, E., Welsh, T., & Hamouda, W. 2018. A critical review of practices and challenges in intrusion detection systems for IoT: Toward universal and resilient systems. *IEEE communications surveys & tutorials*, *20*(4), 3496-3509.

Bhavani, A. D., & Mangla, N. 2022. A review on intrusion detection approaches in resource-constrained IoT environment. In *Mobile Computing and Sustainable Informatics* (pp. 171-183). Springer.

Butun, I., Österberg, P., & Song, H. 2019. Security of the internet of things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials*, *22*(1), 616-644.

Cahyo, A. N., Hidayat, R., & Adhipta, D. 2016. Performance comparison of intrusion detection system based anomaly detection using artificial neural network and support vector machine. AIP Conference Proceedings,

Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. 2019. Network intrusion detection for IoT security based on learning techniques. *IEEE Communications Surveys & Tutorials*, *21*(3), 2671-2701.

Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q., Ray, S., & Jin, Y. 2018. Internet-of-things security and vulnerabilities: Taxonomy, challenges, and practice. *Journal of Hardware and Systems Security*, *2*(2), 97-110.

Chernyshev, M., Baig, Z., Bello, O., & Zeadally, S. 2017. Internet of things (IoT): Research, simulators, and testbeds. *IEEE Internet of Things Journal*, *5*(3), 1637-1647.

Churcher, A., Ullah, R., Ahmad, J., Masood, F., Gogate, M., Alqahtani, F., Nour, B., & Buchanan, W. J. (2021). An experimental analysis of attack classification using machine learning in iot

networks. *Sensors*, *21*(2), 446.
Dhanabal, L., & Shantharajah, S. 2015. A study on NSL-KDD dataset for intrusion detection system based on classification algorithms. *International Journal of Advanced Research in Computer and Communication Engineering*, *4*(6), 446-452.
Dosal, E. 2018. Advantages of a network threat analysis. In: Compuquip.
Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine learning ddos detection for consumer internet of things devices. 2018 IEEE Security and Privacy Workshops (SPW),
Dubey, A. 2018. *Feature Selection Using Random forest*. Retrieved August 19 from https://towardsdatascience.com/feature-selection-using-random-forest-26d7b747597f
Eriza, A. A., & Survadi, M. 2021. Literature review of machine learning models on intrusion detection for internet of things attacks. 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET),
Farnaaz, N., & Jabbar, M. 2016. Random forest modeling for network intrusion detection system. *Procedia Computer Science*, *89*, 213-217.
Fawzi, L. M., Alqarawi, S. M., Ameen, S. Y., & Dawood, S. A. 2019. Two Levels alert verification technique for smart oil pipeline surveillance system (SOPSS). *International Journal of Computing and Digital Systems*, *8*(02), 115-124.
Fawzi, L. M., Ameen, S. Y., Alqaraawi, S. M., & Dawwd, S. A. 2018. Embedded real-time video surveillance system based on multi-sensor and visual tracking. *Appl. Math. Infor. Sci*, *12*, 345-359.
Fawzi, L. M., Ameen, S. Y., Dawwd, S. A., & Alqaraawi, S. M. 2016. Comparative study of ad-hoc routing protocol for oil and gas pipelines surveillance systems. *International Journal of Computing and Network Technology*, *4*(02).
Foley, J., Moradpoor, N., & Ochenyi, H. 2020. Employing a machine learning approach to detect combined internet of things attacks against two objective functions using a novel dataset. *Security and Communication Networks*, *2020*.
Furbush, J. 2018. *Machine learning: A quick and simple definition*. Retrieved August 19 from https://www.oreilly.com/content/machine-learning-a-quick-and-simple-definition/
Google Play Store. (2019). https://play.google.com/store
Groopman, J., & Insights, K. 2019. *Understand the top 4 use cases for AI in cybersecurity*. Retrieved August 19 from https://searchsecurity.techtarget.com/tip/Understand-the-top-4-use-cases-for-AI-in-cybersecurity
Hameed, S. S., Hassan, W. H., Latiff, L. A., & Ghabban, F. 2021. A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches. *PeerJ Computer Science*, *7*, e414.
Harrison, O. 2019. Machine learning basics with the k-nearest neighbors algorithm.[online] towards data science. In.
Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. 2019. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet of Things*, *7*, 100059.
Hassan, R. J., Zeebaree, S. R., Ameen, S. Y., Kak, S. F., Sadeeq, M. A., Ageed, Z. S., Adel, A.-Z., & Salih, A. A. 2021. State of art survey for iot effects on smart city technology: challenges, opportunities, and solutions. *Asian Journal of Research in Computer Science*, 32-48.
Hassan, W. H. (2019). Current research on internet of things (IoT) security: A survey. *Computer networks*, *148*, 283-294.
Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. 2019. A survey on IoT security: application areas, security threats, and solution architectures. *IEEE Access*, *7*, 82721-82743.
Husamuddin, M., & Qayyum, M. (2017). Internet of things: A study on security and privacy threats. 2017 2nd International Conference on Anti-Cyber Crimes (ICACC),
Islam, M. R., & Aktheruzzaman, K. 2020. An analysis of cybersecurity attacks against internet of things and security solutions. *Journal of Computer and Communications*, *8*(4), 11-25.
Islam, N., Farhin, F., Sultana, I., Kaiser, M. S., Rahman, M. S., Mahmud, M., Hosen, A., & Cho, G. H. 2021. Towards machine learning based intrusion detection in IoT networks. *Comput. Mater. Contin*, *69*, 1801-1821.
Jmj, A. 2018. *5 Industries that heavily rely on Artificial Intelligence and Machine Learning*. Retrieved August 19 from https://medium.datadriveninvestor.com/5-industries-that-heavily-rely-on-

artificial-intelligence-and-machine-learning-53610b6c1525
Kaggle. 2020. *Iot Device Network Logs*. https://www.kaggle.com/speedwall10/iot-device-network-logs
Kalnoor, G., & Gowri Shankar, S. 2022. A model-based system for intrusion detection Using novel technique-hidden markov bayesian in wireless sensor network. In *Information and Communication Technology for Competitive Strategies (ICTCS 2020)* (pp. 43-53). Springer.
Kang, H., Ahn, D. H., Lee, G. M., Yoo, J., Park, K. H., & Kim, H. K. 2019. IoT network intrusion dataset. *IEEE Dataport*.
Karmous, N., Aoueileyine, M. O.-E., Abdelkader, M., & Youssef, N. 2022. A Proposed Intrusion Detection Method Based on Machine Learning Used for Internet of Things Systems. International Conference on Advanced Information Networking and Applications,
Karn, U. 2016. A quick Introduction to neural networks. *Obtenido de the data science blog: https://ujjwalkarn. me/2016/08/09/quick-intro-neural-networks*.
Khalid, L. F., & Ameen, S. Y. 2021. Secure Iot integration in daily lives: A review. *Journal of Information Technology and Informatics*, *1*(1), 6-12.
Khan, M. A., & Salah, K. 2018. IoT security: Review, blockchain solutions, and open challenges. *Future generation computer systems*, *82*, 395-411.
Khattak, H. A., Shah, M. A., Khan, S., Ali, I., & Imran, M. (2019). Perception layer security in internet of things. *Future Generation Computer Systems*, *100*, 144-164.
Koehrsen, W. 2018. *An Implementation and Explanation of the Random Forest in Python*. Retrieved August 19 from https://towardsdatascience.com/an-implementation-and-explanation-of-the-random-forest-in-python-77bf308a9b76
Kumar, A., Kuppusamy, K., & Aghila, G. 2018. FAMOUS: Forensic Analysis of MObile devices Using Scoring of application permissions. *Future Generation Computer Systems*, *83*, 158-172.
Kumar, G. R., Seshanna, K. V., Basha, S. R., & Babu, G. A. (2022). An experimental investigation of PCA-Based intrusion detection approach Utilizing machine learning algorithms. In *Mobile Computing and Sustainable Informatics* (pp. 249-258). Springer.
Kumar, P. S., & Akthar, S. 2022. Execution improvement of intrusion detection system through dimensionality reduction for UNSW-NB15 information. In *Mobile Computing and Sustainable Informatics* (pp. 385-396). Springer.
Kumar, R., Zhang, X., Wang, W., Khan, R. U., Kumar, J., & Sharif, A. 2019. A multimodal malware detection technique for Android IoT devices using various features. *IEEE access*, *7*, 64411-64430.
Lei, T., Qin, Z., Wang, Z., Li, Q., & Ye, D. 2019. EveDroid: Event-aware Android malware detection against model degrading for IoT devices. *IEEE Internet of Things Journal*, *6*(4), 6668-6680.
Leloglu, E. (2016). A review of security concerns in internet of things. *Journal of Computer and Communications*, *5*(1), 121-136.
Liao, Y., & Vemuri, V. R. 2002. Use of k-nearest neighbor classifier for intrusion detection. *Computers & security*, *21*(5), 439-448.
Ling, Z., Luo, J., Xu, Y., Gao, C., Wu, K., & Fu, X. 2017. Security vulnerabilities of internet of things: A case study of the smart plug system. *IEEE Internet of Things Journal*, *4*(6), 1899-1909.
Liu, J., Yang, D., Lian, M., & Li, M. (2021). Research on classification of intrusion detection in internet of things network layer based on machine learning. 2021 IEEE International Conference on Intelligence and Safety for Robotics (ISR),
Lu, Y., & Da Xu, L. 2018. Internet of things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, *6*(2), 2103-2115.
Maind, S. B., & Wankar, P. 2014. Research paper on basic of artificial neural network. *International Journal on Recent and Innovation Trends in Computing and Communication*, *2*(1), 96-100.
Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. 2018. Anatomy of threats to the internet of things. *IEEE communications surveys & tutorials*, *21*(2), 1636-1675.
Malallah, H., Zeebaree, S. R., Zebari, R. R., Sadeeq, M. A., Ageed, Z. S., Ibrahim, I. M., Yasin, H. M., & Merceedi, K. J. 2021. A comprehensive study of kernel (issues and concepts) in different operating systems. *Asian Journal of Research in Computer Science*, 16-31.
Manhas, J., & Kotwal, S. 2021. Implementation of intrusion detection system for internet of things using machine learning techniques. In *Multimedia Security* (pp. 217-237). Springer.

Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. 2019. IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet of Things Journal*, *6*(5), 8182-8201.

Mrabet, H., Belguith, S., Alhomoud, A., & Jemai, A. 2020. A survey of IoT security based on a layered architecture of sensing and data analysis. *Sensors*, *20*(13), 3625.

Murali, S., & Jamalipour, A. 2019. A lightweight intrusion detection for sybil attack under mobile RPL in the internet of things. *IEEE Internet of Things Journal*, *7*(1), 379-388.

Nikhitha, M., & Jabbar, M. 2019. K nearest neighbor based model for intrusion detection system. *Int. J. Recent Technol. Eng*, *8*(2), 2258-2262.

Nižetić, S., Šolić, P., González-de, D. L.-d.-I., & Patrono, L. 2020. Internet of things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *Journal of Cleaner Production*, *274*, 122877.

Nugroho, E. P., Djatna, T., Sitanggang, I. S., Buono, A., & Hermadi, I. 2020. A review of intrusion detection system in IoT with machine learning approach: Current and future research. 2020 6th International Conference on Science in Information Technology (ICSITech),

Oracevic, A., Dilek, S., & Ozdemir, S. 2017. Security in internet of things: A survey. 2017 International Symposium on Networks, Computers and Communications (ISNCC),

OS, J. N., & Bhanu, S. M. S. 2018. A survey on code injection attacks in mobile cloud computing environment. 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence),

Otoum, Y., & Nayak, A. 2021. AS-IDS: Anomaly and signature based IDS for the internet of things. *Journal of Network and Systems Management*, *29*(3), 1-26.

Pahl, M.-O., & Aubet, F.-X. 2018. All eyes on you: Distributed Multi-Dimensional IoT microservice anomaly detection. 2018 14th International Conference on Network and Service Management (CNSM),

Restuccia, F., D'Oro, S., & Melodia, T. 2018. Securing the internet of things in the age of machine learning and software-defined networking. *IEEE Internet of Things Journal*, *5*(6), 4829-4842.

Rizvi, S., Kurtz, A., Pfeffer, J., & Rizvi, M. 2018. Securing the internet of things (IoT): A security taxonomy for IoT. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE),

Saba, T., Sadad, T., Rehman, A., Mehmood, Z., & Javaid, Q. 2021. Intrusion detection system through advance machine learning for the internet of things networks. *IT Professional*, *23*(2), 58-64.

Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. *Alexandria Engineering Journal*, *61*(12), 9395-9409.

Saritas, M. M., & Yasar, A. 2019. Performance analysis of ANN and Naive Bayes classification algorithm for data classification. *International Journal of Intelligent Systems and Applications in Engineering*, *7*(2), 88-91.

Seyfollahi, A., & Ghaffari, A. 2021. A review of intrusion detection systems in RPL routing protocol based on machine learning for internet of things applications. *Wireless Communications and Mobile Computing*, *2021*.

Shahzad, G., Yang, H., Ahmad, A. W., & Lee, C. 2016. Energy-efficient intelligent street lighting system using traffic-adaptive control. *IEEE Sensors Journal*, *16*(13), 5397-5405.

Sharma, H., & Kumar, S. (2016). A survey on decision tree algorithms of classification in data mining. *International Journal of Science and Research (IJSR)*, *5*(4), 2094-2097.

Shenfield, A., Day, D., & Ayesh, A. 2018. Intelligent intrusion detection systems using artificial neural networks. *ICT Express*, *4*(2), 95-99.

Si-Ahmed, A., Al-Garadi, M. A., & Boustia, N. 2022. Survey of machine learning based intrusion detection methods for internet of medical things. *arXiv preprint arXiv:2202.09657*.

Singh, R. P., Javaid, M., Haleem, A., & Suman, R. 2020. Internet of things (IoT) applications to fight against COVID-19 pandemic. *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, *14*(4), 521-524.

Sommer, R., & Paxson, V. 2010. Outside the closed world: On using machine learning for network intrusion detection. 2010 IEEE symposium on security and privacy,

Song, J., Takakura, H., Okabe, Y., Eto, M., Inoue, D., & Nakao, K. 2011. Statistical analysis of honeypot data and building of Kyoto 2006+ dataset for NIDS evaluation. Proceedings of the first workshop on building analysis datasets and gathering experience returns for security,

Stampar, M., & Fertalj, K. 2015. Artificial intelligence in network intrusion detection. 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO),

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. 2020. A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, *22*(2), 1191-1221.

Taghavinejad, S. M., Taghavinejad, M., Shahmiri, L., Zavvar, M., & Zavvar, M. H. 2020. Intrusion detection in IoT-based smart grid using hybrid decision tree. 2020 6th International Conference on Web Research (ICWR),

Tahsien, S. M., Karimipour, H., & Spachos, P. 2020. Machine learning based solutions for security of internet of things (IoT): A survey. *Journal of Network and Computer Applications*, *161*, 102630.

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. 2009. A detailed analysis of the KDD CUP 99 data set. 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications,

Tewari, A., & Gupta, B. B. 2020. Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. *Future generation computer systems*, *108*, 909-920.

Ullah, I., & Mahmoud, Q. H. 2020a. A scheme for generating a dataset for anomalous activity detection in IoT networks. Canadian Conference on AI,

Ullah, I., & Mahmoud, Q. H. 2020b. A Technique for Generating a Botnet Dataset for Anomalous Activity Detection in IoT Networks. 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC),

Vashi, S., Ram, J., Modi, J., Verma, S., & Prakash, C. 2017. Internet of things (IoT): A vision, architectural elements, and security issues. 2017 international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC),

Viennot, N., Garcia, E., & Nieh, J. 2014. A measurement study of google play. The 2014 ACM international conference on Measurement and modeling of computer systems,

VirusShare. (2019). https://virusshare.com

Wright, J., & Cache, J. 2015. *Hacking exposed wireless: Wireless security secrets & solutions*. McGraw-Hill Education Group.

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. 2017. A survey on security and privacy issues in internet of things. IEEE Internet of Things J. 4 (5), 1250–1258 (2017). In.

Yao, J., Zhao, S., & Fan, L. 2006. An enhanced support vector machine model for intrusion detection. International Conference on Rough Sets and Knowledge Technology,

Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. 2017. A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, *84*, 25-37.

Zebari, I. M., Zeebaree, S. R., & Yasin, H. M. 2019. Real time video streaming from multi-source using client-server for video distribution. 2019 4th Scientific International Conference Najaf (SICN),

Zeebaree, S., Ameen, S., & Sadeeq, M. 2020. Social media networks security threats, risks and recommendation: A case study in the kurdistan region. *International Journal of Innovation, Creativity and Change*, *13*, 349-365.