IoT Security and Machine Learning

Sarah Almalki [1], Hatim Alsuwat[2], Dr. Emad Alsuwat[1],
s44180317@students.tu.edu.sa, Hssuwat@uqu.edu.sa, Alsuwat@tu.edu.sa
[1] Department of Computer Science, College of Computers and Information Technology, Taif University, Saudi Arabia
[2] Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Saudi Arabia

Summary

The Internet of Things (IoT) is one of the fastest technologies that are used in various applications and fields. The concept of IoT will not only be limited to the fields of scientific and technical life but will also gradually spread to become an essential part of our daily life and routine. Before, IoT was a complex term unknown to many, but soon it will become something common. IoT is a natural and indispensable routine in which smart devices and sensors are connected wirelessly or wired over the Internet to exchange and process data. With all the benefits and advantages offered by the IoT, it does not face many security and privacy challenges because the current traditional security protocols are not suitable for IoT technologies. In this paper, we presented a comprehensive survey of the latest studies from 2018 to 2021 related to the security of the IoT and the use of machine learning (ML) and deep learning and their applications in addressing security and privacy in the IoT. A description was initially presented, followed by a comprehensive overview of the IoT and its applications and the basic important safety requirements of confidentiality, integrity, and availability and its application in the IoT. Then we reviewed the attacks and challenges facing the IoT. We also focused on ML and its applications in addressing the security problem on the IoT.

Keywords:
Internet of Things; IoT security and privacy; machine learning; deep learning; IoT attack.

1. Introduction

In recent years, we have witnessed a tremendous development in the Internet of Things (IoT) system and its latest quantum leap in achieving a globally interconnected infrastructure of virtual and physical objects. These things are interrelated with each other for exchanging information and data for different services and new applications, whether wired or wireless [1][4]. The IoT has become one of the greatest concerns in technology today and the latest revolution in the world of the Internet. Connecting devices via the Internet has become possible with the use of IoT; such a connection lets us benefit from data in creating services that improve our working and routine life [1][3]. The IoT aims to improve operations in various sectors as it has raised business efficiency by providing many models. It has also contributed to reducing costs, encouraging innovations, creating new job opportunities, and providing advanced practical solutions for individuals, companies, and institutions (e.g., education, industry, mining, health, tourism, energy, water, transportation, environment, security, entertainment, welfare, and other various sectors), which contributes to improving the quality of life. Every year, the volume of data for devices connected to the IoT increases worldwide. By 2025, the expected volume of data for IoT devices will reach 79.4 ZB, which is an excessively large number, indicating that the future depends on the IoT in most different fields and sectors [4][6]. The number of devices connected to the IoT globally has increased dramatically in the recent years. At the end of 2018, about 22 billion devices were connected to the IoT worldwide. By 2030, about 50 billion IoT devices are expected to be used in all parts of the world, which will cause the construction of a gigantic network of interconnected devices, from smartphones to home devices [4][5]. The number of IoT-connected devices around the world (in billions) in 2018, 2025, and 2030 is shown in Fig. 1.

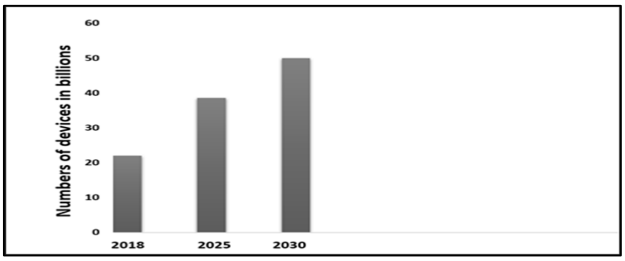

Fig. 1 Number of IoT-connected Devices Worldwide (in billions).

Despite its countless great benefits, the IoT also has many security and privacy challenges that must be given attention [2][3]. The IoT has remarkably affected all aspects of people's lives, whether economic, commercial, and social. Considerable efforts have been made to address the problems of security and privacy on the IoT, and traditional encryption methods and principles have been applied. Nevertheless, the characteristics that represent the IoT make the current solutions inappropriate and insufficient to address the security and privacy problems of IoT networks, which are caused by several reasons such as restrictions. These reasons are based on resources, heterogeneity, and big data that are shared across IoT devices, as well as the dynamic nature of the IoT [4][7]. Therefore, machine learning (ML) and deep learning (DL) technologies, which can enable embedded intelligence in IoT devices and systems, should be utilized to address various security and privacy issues [7].

This paper is organized into six sections as follows. Section 2 presents a general overview of the IoT and its security and protection requirements. It also includes the challenges and attacks on the IoT and ML applications in Internet security, as well as their types. In Section 3, we discuss the latest studies that focused on the security of the IoT and the use of ML in maintaining security and privacy and addressing attacks and security challenges on the IoT. In Section 4, we review the future challenges facing the IoT. Finally, Section 5 concludes this paper.

2. Background

This section reviews a comprehensive overview of the IoT and its advantages, discusses the security requirements of the IoT, and reviews the most important challenges and attacks that threaten the security of the IoT. Then, it discusses the most important applications of ML and DL in the security of the IoT.

2.1 IoT Overview

In 1999, the idea of IoT was proposed by Kevin Ashton, who is also the creator of the Automatic Identification Center at MIT; according to Ashton,

Manuscript received May 5, 2022
Manuscript revised May 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.5.16

“The Internet of Things has the power to change the world, just as the Internet has done. Maybe more than that” [8]. After a period, specifically in 2005, the idea of the IoT was formally introduced and proposed by the International Telecommunication Union (ITU) [8][9]. In 2012, the ITU introduced the IoT as “A global infrastructure for the information society, providing advanced services by connecting things (physical and virtual) based on existing, advanced, and interoperable information and communication technologies” [9]. Many definitions of the IoT have been introduced by researchers and organizations from several points of view, but one common concept is that the IoT works effectively and efficiently for sharing information and data, which leads to a better, effective, and efficient world, thereby providing services and facilitating human life [10]. The IoT is considered one of the most promising technologies concerned with improving the quality of people’s lives by building new and useful applications and software that facilitate routine daily activities efficiently [8][10]. Many of the common characteristics of the IoT are summarized in Table 1.

Table 1: IoT Characteristics

Characteristic	***Description***
Large Scale	IoT devices are growing exponentially. Therefore, controlling the IoT that contains many interconnected devices is necessary. This interconnection between devices also results in a large amount of data to be exchanged, which results in problems related to the interpretation and analysis of these data.
Heterogeneity	Many devices, which are considered having different capabilities and characteristics in the IoT, are communicating with one another and connected with different protocols. Thus, the connected devices in the IoT use different and multiple models and standards and impose many restrictions on the devices.
Intelligence	IoT devices are characterized by intelligence as they combine devices and complex algorithms in programs, making them able to choose smart decisions in various situations and interact with one another in an intelligent manner.
Interconnectivity	IoT devices are connected to the global information and communication infrastructure, such that people can reach them anytime and anywhere and connect locally or globally. This connection depends on the type of applications and services provided by the IoT service providers. Global connectivity is similar to connecting to a smart home by managing the infrastructure and mobile infrastructure. Examples of local connectivity are a group of sensors.
Sensing	Sensors in the IoT are the most important and basic parts as they can be used to perceive and understand the surrounding environment variables and then build data and information that determine their state. Different sensing technologies provide accurate perceptions of the surrounding environment and make people understand and perceive the physical world.
Low-power and Low-cost Communication	On the IoT and its devices, the massive connectivity of devices provides and requires solutions that support low-energy, as well as cost-effective hardware operations across the network.
Dynamic Environment	The ability of devices on the IoT is characterized by communication and compatibility with the objects of our environment without the necessity of specifying the restrictions and limits of the IoT network, which distinguishes it by making it a dynamic system. IoT devices can also be modified dynamically depending on changing and different circumstances and situations.
Context Awareness	IoT devices have many sensors that are interested in collecting and storing data from the surrounding environment, and these devices take many appropriate decisions on the stored data, such that they are aware of the context.
Complex System	The IoT system has billions of different heterogeneous organisms, its software has numerous capabilities. However, the IoT system also has many limitations associated with time, energy, and memory, making its management a highly difficult process.
Self-configuring	IoT devices are considered smart and capable of self-configuration. Different from other devices wherein users must intervene to perform any operation, IoT devices can work and configure completely without user intervention, as they can ensure that the programs are updated jointly and communicate with the manufacturer.
Unique Identity	In the IoT, every object uses its own identifier that is recognized by the IoT as an IP address. IoT manufacturers are interested in providing unique identifiers. The identifier is used to upgrade and update IoT devices to the appropriate system. In addition, these IoT devices contain modern interfaces that enable users to view data and perform tasks, such as remote administration and analysis.
Safety	Safety is one of the most important characteristics to ensure the quality and performance of IoT networks. It is considered an important feature for both users and devices because Internet connection exposes data that are being transferred and exchanged.

2.2 Security Requirements for IoT

One of the important and necessary criteria is to pay attention to the security of the IoT system. This criterion can be achieved through the use and application of the standard security requirements approved for the confidentiality, integrity, and availability (CIA) and the importance of their application in the IoT system [11].

- **Confidentiality**: It is the exchange of data and information between the sender and the receiver who is authorized to do so without having access to the content and communication data by any unauthorized person or any harmful user. Communication must be protected, and two guarantees are confidential and protected [11][12]. In view of IoT devices, the confidentiality and protection of data and contact information within the communication network must also be guaranteed. Confidentiality and non-access by any unauthorized person should be ensured when transferring data and exchanging messages among IoT devices [11][13].
- **Integrity**: It is to ensure that data are not modified by any unauthorized person nor tampered with by the receiver and the sender. In the IoT, to ensure that the content of data and messages between the sender and the receiver guarantee that the communication is safe and protected against any manipulation by any intrusive person, a safety and integrity check must be performed in every part of the node in which people share the exchange of data between the connected devices [11][12].
- **Availability**: It is the availability of services provided upon request by authorized users in the system. Therefore, it must be ensured that a malicious intruder or unauthorized user cannot disrupt the services provided by IoT devices or the network and that the connection or the quality and capabilities of the services provided are unaffected [11][13].

In addition to the implementation of CIA, providing security in the IoT is important and necessary. However, other security requirements that must be implemented at the levels of the IoT infrastructure, and node authentication is one of the main security problems that must be secured to avoid unauthorized access to the node at the physical layer level [13][14] and make a secure communication channel between the nodes of the IoT against any type of attacks on the IoT. The encryption algorithm and protocol and their use provide an important aspect of encrypting the exchange of data between IoT devices that use limited resources [2][14]. As for the communication layer or the network, security measures must be taken to protect the connection, as well as the need for identity authentication to address and prevent nodes that exist illegally [2][13]. A distributed denial-of-service (DDoS) attack is a widespread and common occurrence in the communication or network layer; thus, security and protection are important against a DDOS attack occurring in nodes that are not related to this layer, and such an attack is one of the most dangerous attacks on the IoT [2]. Moreover, the availability and use of application security mechanisms are necessary to provide protection and security for information and data stored in cloud computing in data abstraction, accumulation, and edge-computing level. In addition, strong encryption algorithms must be used to protect data, as well as a virus program that is constantly updated. At the level of applications and cooperation, authentication must be implemented and approved to provide protection and security for user privacy. Furthermore, taking care of password management is important for information security at this level [2][13][14]. Fig. 2. shows the security requirements at each level of the IoT.

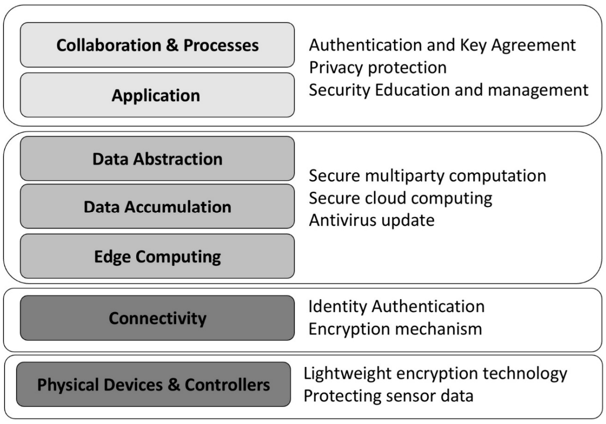

Fig. 2 Security Requirements at Each Level of the IoT.

2.3 Security Challenges and attacks in IoT

Notably, the original Internet was not designed to keep pace with the nature of the IoT. Therefore, providing technology and mechanisms that protect and ensure the security of data and users on the IoT is considerably important [3][4][16]. The increase in IoT devices, the large volume of data that are exchanged among devices, and the dynamic nature of the IoT system has led to the presence of many attacks and security challenges that must be addressed, given that communication channels can be used to monitor users and track the actions they take and other attacks that cause a loss of security and user privacy [7][15][16]. Attacks can be divided on the IoT system into four main categories, namely, physical, software, networks, and encryption attacks [15][16][17]. Fig. 3. shows security attacks in IoT.

2.3.1. Physical Attacks

Physical attacks focus on the attack on the hardware components of the IoT system, which actually requires the attacker to run the attack to be close to the IoT system to gain access to the devices [3]. This type of attack is considered relatively the most difficult to achieve because it requires potentially expensive materials to perform the attack. In a physical attack, an attacker can directly access devices and then manipulate their components in many ways to gain access to physical devices; one of the most prominent methods that attackers use is social engineering, which enables them to access devices and inflict physical damage on them, and then they can perform other attacks [4][18]. This type of attack can cause other connected attacks that cause great damage, such as when the alarm system in smart homes fails, which may lead to the occurrence of burglary or other damages that cause physical damage in the smart home environment [4][18]. In addition, changing the sensor and using a harmful sensor indicates that sensitive data may leak to the attacker. A man-in-the-middle (MITM) attack can also occur due to the malicious node being injected into the network, which gives the attacker permission to perform other attacks within the IoT environment, such as tampering with devices and changing routing tables. The manipulation of security keys and such changes affect communication and data exchange in the upper layers [3][15]. As mentioned earlier, the social engineering methods used by most of the attackers in this type are among the most common and varied methods to manipulate users to access data, but their purpose is to physically access the environment of the IoT system [19]. Several different forms of physical attacks include node tampering, malicious node injection, physical damage, and social engineering. Table 2 Shows several different forms of physical attacks.

Table 2: Types of Physical Attacks in IoT

Attack	*Description*
Node Tampering	The goal of this type of physical attack is to reach the sensor node or work to physically destroy it, access and change it in its entirety, or change parts of its hardware with the aim of accessing and destroying sensitive data or using them in other attacks.
Malicious Code Injection	The attacker works in this type by performing a malicious physical injection using a code for the IoT node, which contributes to the attacker's access to the IoT system.
Physical Damage	The attacker attempts to gain access to the area that contains the IoT devices to damage them by destroying the IoT device system. This type of attacker must be in the same place or building in which the IoT devices are located to destroy and harm them.
Social Engineering	The attacker exploits the users and their lack of awareness of the importance of maintaining the security of the IoT devices and their environment and manipulates them. In this manner, the attacker can access the IoT system to obtain sensitive information or perform operations aimed at accomplishing the attacker's goals.
RF Interference on RFIDs	This attack works on the availability of IoT sensors as the attacker routes the various noise signals to affect the quality of communication using radio frequency (RF) signals that work with RFID devices. The signals interfere, which affects communication.
Malicious Node Injection	In this type, the attacker acts as a controller in the data flow between the nodes of the IoT, where the attacker can access and see sensitive data by running a new malicious node to work between the nodes in the IoT system.

2.3.2 Software Attacks

Software attacks are among the most dangerous attacks that threaten all systems in the programs, as weaknesses and gaps are targeted and exploited to link data or devices with the purpose of destroying or destroying them or stealing sensitive data. Security flaws are also exploited to inject viruses or malware into the system [2][3]. There are several different forms of Software attacks in IoT such as DoS Attack, Worms Virus and Spyware, Phishing Attacks and Malicious Scripts. Table 3. Shows Different Forms of Software attacks in IoT.

Table 3: Different Forms of Software Attacks in IoT

Attack	*Description*
Denial-of-Service (DoS) Attack	The attacker exploits the application layer to perform a DoS attack, which is known because it affects all users of the IoT system and the environment, as this attack gives the attacker power to access system data on the IoT, bans system users, and controls their powers.
Worms Virus and Spyware	This type of attack aims to access and steal or destroy sensitive information and data, as well as affect the system's availability of IoT devices by injecting malicious software into the system.
Phishing Attack	This type of attack takes advantage of social engineering to collect sensitive data from a system of IoT devices and exploit the system's login information or other important information through phishing and its methods.
Malicious Scripts	It is a malicious script that the attacker uses to access important information and sensitive data in the IoT system, as these scripts are executed by the authorized users of the system, using several tricks from the attacker and taking advantage of the Internet connection feature.

2.3.3 Networks Attacks

The IoT system is a group of connected networks within the environment of the IoT system to communicate among IoT devices or transfer various data among networks; in network attacks, the attacker exploits the Internet connection to access data, and it is not required to be close to the network of the IoT system because the attack works similar to Internet connection and network gaps [2][3]. Keeping the network secure is important to be able to contain and control attacks. An attacker can exploit a compromised node and then take advantage of it and use it as a fake redirect node. This type is associated with sensor networks and poses a threat to the IoT [4]. Several different forms of networks attacks in IoT include RFID spoofing, RFID cloning, RFID unauthorized access, MITM attack, and routing information attack. Table 4 shows different forms of networks attacks in IoT.

Table 4: Different Forms of Networks Attacks in IoT

Attack	***Description***
RFID Spoofing	The attacker can access data on the IoT system by impersonating RFID signals to obtain the sensitive data in the RFID card. Then, the attacker uses the original spoofed identifier, such that the sent data appear to be from the original source. Thus, the attacker can access the data and the system as a legal node.
RFID Cloning	In this type of attack, the attackers copy the data of one RFID tag to another, which causes both tags to contain the same data that were copied.
RFID Unauthorized Access	In this type of attack, the RFID nodes are easy to penetrate, such that the attacker can read, modify, or destroy the data in the RFID nodes because most of the RFID nodes do not have appropriate authentication techniques.
Traffic Analysis Attack	The goal of this attack is to obtain sensitive data that pass through the network. Thus, the attacker collects the information needed for the attack by analyzing the traffic inside the network.
MITM	In this type, the attacker relies on placing a malicious node inside the IoT system, and this node is located within a network between two connected nodes, which allows the harmful node to monitor all the data that are transferred and see the possibility of stealing or damaging them.
Sinkhole Attack	This attack aims to disrupt the service within the network by stealing important data and not to redirect any incoming packet to the connected destinations, and the packets are ignored.
Routing Information Attack	The goal of this attack is to disrupt traffic within the network and send error messages. This objective is performed by changing the contents of the routing table and the information in it. As a result, the data are sent to wrong destinations, and the network crashes.

2.4 ML in IoT Security

In this section, we review the most important algorithms and types of ML and its features and applications in Internet security.

2.4.1 ML Algorithms

ML algorithms can be classified into four categories: supervised, unsupervised, semi-supervised, and reinforced learning algorithms.

- **Supervised Learning**: It is one of the ML classifications that is implemented when specific goals are defined to be able to reach a certain number of inputs, where the data are classified using the classified ordered data, followed by training. Then, the rules are automatically arranged from the available data, the categories are determined, and the location is then predicted. Each element belongs to a specific category [20][21].
- **Unsupervised Learning**: In this classification, the goals to be achieved are not defined. Only the input is provided, and the data are not required in a categorized manner. In this type, the existence of similarity between the data can be investigated and classified into groups [20].
- **Semi-supervised Learning**: This type falls between the two previous types as either no specific labels exist for all the observations in the data set or clear names are present for all observations in practical situations. The material cost of classification is usually high because it requires skilled experts. Thus, the nodes have no specific designations, although they exist and are defined in several semi-supervised algorithms [20].
- **Reinforcement Learning**: This type has no specific results, as the agent learns through the presence of comments after the importance of interacting with the surrounding environment. The agent also takes actions and decide based on the reward that he will receive (whether the agent can be rewarded for good deeds or punished for bad deeds), and the presence of the criteria and limitations for feedback he uses to maximize the rewards. This algorithm is inspired by the forms of human and animal learning behaviors, as these behaviors appear to be arranged in dynamic applications in an attractive and distinctive manner to robots, where the system begins to learn and implement specific tasks without performing clear programming; moreover, the appropriate reward function should be selected and organized because the agent learns based on the accumulated reward [4][21].

Supervised and unsupervised learning techniques are concerned with focusing on the problems and methods of data analysis, whereas reinforcement learning focuses on providing solutions to problems of interest in comparison and decision making [4][21]. The choice of ML technology focuses on the type and nature of the data that have been entered, as it depends on the focus on identifying the required input and output data; moreover, supervised learning is used in the scenario where the system is trained and taught on the importance of assigning the inputs to the outputs requested [21]. An important example of supervised learning techniques is classification and regression, where regression works in a continuous manner, whereas classification works with separate outputs. Many different regression techniques, such as support vector regression (SVR), polynomial regression, and linear regression, are all important and commonly used techniques. Classification also works with the arrangement of separate output values.

Several popular examples of classification algorithms have been used for K-neighbor closest and support vector machine (SVM), as well as logistic regression [4]. Some or both classification and regression algorithms are used (e.g., neural networks). Unsupervised learning techniques are used when the output data are not specific, and the system in this case must work to discover the structure through the raw data; hence, unsupervised learning techniques are used to teach and empower the system [20][21]. Unsupervised learning can be used to group objects with several specific criteria for pairing and similarity, such as K-mean clustering. The degree of predictive accuracy of these analyses focuses on the accuracy and quality of using ML techniques and algorithms to develop models and the accuracy of their ability to analyze predictive values for future data. Algorithms, such as SVR, Naive Bayes (NB), and neural networks can be used for predictive modeling [4].

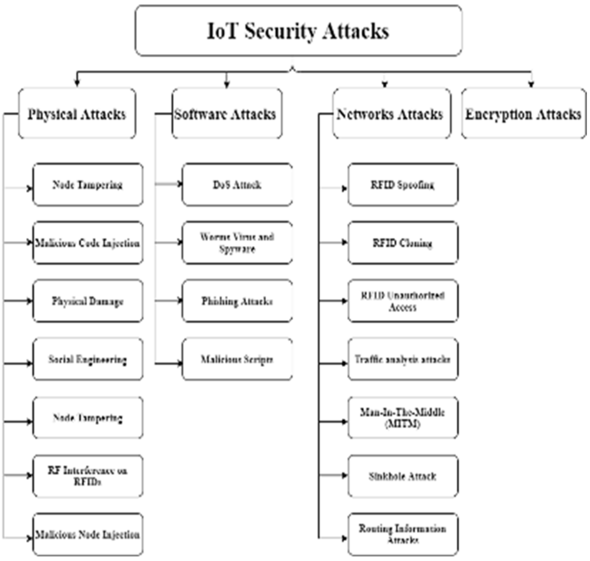

Fig. 3 Categories of Security Attacks in IoT.

- **<u>DL</u>**: It is one of the important ML techniques, where the neural network inside it consists of a group of neurons that are formed and considered as variables and are linked to each other through weighted connections that can be considered parameters, such that they are present in them. The required set of outputs is achieved, and the unsupervised or network unsupervised learning method link is communicated. In DL, we focus on defining large deep neural networks, which limits the number of layers in the network [4][20]. DL technologies are characterized by distributed computing and are also distinguished by the importance and application of learning and analysis to an extremely large set of disaggregated, unclassified, and unsupervised data, where a model of learning and characterization is simulated by the motivation of a class-based learning and comprehension process in the human brain [4][22]. DL models and technologies contribute to many important and different ML applications (e.g., speech recognition, natural language processing, provision of improved ordered classification modeling, and better generation of many samples of data). The models also benefit from the process of data compression and restoration in many different areas, temporal and spatial, due to the accuracy of its work in identifying patterns and features in a large set of data and extracting the relationships between them depending on time [22].

2.4.2 ML in IoT Security

ML algorithms and techniques have been adopted and applied on a large scale and are constantly evolving in many technologies and applications in the real world due to their distinct nature in contributing to solving problems effectively [4][20]. Recently, ML algorithms and techniques have been used in many important areas, such as the IoT and the preservation of the development of security and protection in it in several advanced ways. Current advances in ML technologies are driven by work to improve and develop many new advanced algorithms and the need for big data [22]. Here, we discuss the most effective and widespread ML algorithms and their most important advantages and disadvantages, as well as their applications in IoT security. Among these algorithms are SVM, Bayesian algorithms, decision trees (DT), random forest (RF), k-nearest neighbor (KNN), and association rule (AR) algorithms.

1. **SVM**: SVM algorithms are used to create a classification by constructing a division and arrangement in the attributes and amount of data present between several classes, such that the distance between each metric level is determined against the sample points that are frequently overridden in each category of data. SVM algorithms is capable of generalization and is broadly compatible with the amount of data that has many features corresponding to a small number of sample points. SVM devices are also characterized as flexible for expansion and have high ability and accuracy to detect intrusion and are distinguished by their detection in real time [4][23]. One of the main disadvantages is that data for SVM-based models are difficult to understanding and interpret. One of the most important applications of SVM algorithms in the security of the IoT is their ability to detect intrusion, detect malware, and detect and monitor attacks in smart networks [24].

2. **Bayesian algorithms**: Bayes' theory is concerned with explaining the probability of any accident based on the presence of information related to it. For example, a DoS attack is linked to traffic data, and the attack is detected within the network. Therefore, Bayes' theorem can be used to interpret and evaluate the probability of a traffic attack occurring only by looking at past traffic data. One of the most important ML algorithms used based on Bayes' theory is the NB classifier [2][4]. NB is known for its simplicity. It depends on calculating the extent of probability using Bayes' theorem to explain certain features. For example, intrusion can be detected depending on the use of traffic classification and whether it is normal or unusual, such that features (e.g., connection duration, connection status, and protocol-type Communication (TCP and UDP)) can be classified using an NB classifier. NB is characterized by calculating the extent of subsequent probability and by being easy, fast, and simple in implementing and determining the requirements and data of the training sample. One of the most important disadvantages of NB is that it deals with each feature independently of the other, which makes it unable to capture and identify useful evidence through the relationships and interactions between the features [24]. NB plays an effective role in the security of the IoT by using its features in detecting the presence of network penetration [23].
3. **DT**: DT-based classification methods are primarily concerned with how to sort samples based on their feature values. Each vertex (node) in any tree is classified as a feature, and an edge (branch) representation is associated with a value that it should represent in a sample. The sample is classified and represented in an ordered manner, starting from the place of the origin and everything related to the values of its features. The theme that well arranges training samples is the pinnacle of the tree parentage [23][24]. Several criteria can measure and determine the optimum feature that represents the optimal partitioning of training sample data, including the representation and acquisition of data and information. DT is concerned with building a prediction model to interpret learning from the presence of training samples by interpreting and representing them in groups as branches and leaves. The chosen model is then relied upon to determine the prediction and represent it to the new model category. DT is one of the simplest and easiest algorithms to use [4][25]. However, it needs plenty of storage space, which is a disadvantage because of its structure. DT is used in Internet security to detect the presence of intrusion in devices and networks and identify suspicious traffic sources [23].
4. **RF**: RF relies on building many DTs and working on combining them to reach the result of obtaining an orderly, accurate, and distinct prediction model to work on reaching the best results and overall improvement proposals. Among the most important features of RF is powerful and accurate installation [4]. It requires a small number of input parameters and data. However, one of its drawbacks is that the RF may not be effectively practical when used in applications that require real-time determination and contain a large set of required training data. RF is highly effective and used in IoT security in detecting the presence of intrusion in devices in IoT environment; it also detect DDoS attacks and identify existing and unauthorized IoT devices [23][25].
5. **KNN**: KNN algorithm is concerned with identifying a new sample based on the votes of the most suitable number chosen by its closest neighbors, as KNN relies in its decision to choose the category of the existing unknown samples based on the selection of the voices of its closest neighbors [4]. KNN is a good technique widely used in ML, and it is effective and accurate for infiltration detection. However, one of its disadvantages is the method for determining the best and appropriate value for k, which is extremely difficult and time consuming due to the difference in the value of k from one data set to another. This algorithm is considered effective in detecting intrusions on the IoT [23].
6. **AR algorithms**: AR algorithms are interested in making a clear study of the existence of the relationship between the set of variables in the training data to make a comparison and determine the most important correlations and similarities and thus create a model. Then, this model is relied upon to make the prediction of the existence of the new sample class. AR algorithms are clear, simple, uncomplicated, and easy to use. However, one of its main drawbacks is the high time complexity [4]. Moreover, in some cases, the assumptions made by these algorithms are considered useless and unsuitable for implementation. AR algorithms play a role in detecting intrusion in devices and networks of the IoT [25].

Supervised learning algorithms are used with labeled data in IoT networks and environment to work on spectrum sensing, identifying and estimating channels and security, adapting and filtering, and solving localization problems [4]. Supervised learning includes two types of techniques, namely, classification and regression. Classification algorithms are used in supervised ML to make predictions and work on modeling existing data classes. Conversely, regression algorithms are used to make predictions of the values of numerical variables that are continuous. Several classification algorithms include SVM, DT, RF, and NB [4][22]. SVM classification algorithm uses kernels, which are used for coupling and finding the differences between any two points operating from two classes. SVM model decision boundaries have nonlinear precision [4]. However, SVM is highly memory-intensive, which makes it difficult to identify and find the right kernel and to work with the models with large data classes. Therefore, using RF is better than SVM [21]. NB algorithm is used to model and represent real-world problems, such as to classify and interpret text and to perform spam detection. RF algorithms are also among the best algorithms for modeling real-world problems [2][4][22]. It is better in terms of ease of implementation and method of adaptation to different amounts of existing data set. But it takes more time and effort to train [4][25].

3. Related Works

Many studies have focused on the security and privacy on the IoT. However, we focus on the most important and recent published studies from 2018 to 2021. Moreover, we discuss studies that have specifically dealt with the use of ML and algorithmic techniques in providing solutions to IoT security problems.

3.1 Security and Privacy in IoT

In [2], the authors presented a discussion on the importance of achieving the security of the IoT, achieving privacy, and the existence of safety and ethics in the use of IoT devices. They provided a comprehensive overview of the IoT system and configuration and its important and basic characteristics. Then, the authors discussed the most important security challenges facing the IoT and the importance of achieving security requirements and best practices for working to protect IoT devices and networks. They also shed light on the most important security threats and the most important proposed solutions to maintain privacy on the IoT environment. The importance of safety on the IoT system and the most important ethics were also discussed, focusing on the necessary need for ethical design for IoT devices. Finally, a smart city model was presented as an example for a case study, verifying various security threats and providing proposed security solutions to achieve a high level of security in a smart city.

The authors in [26] provided a comprehensive description of a group of common attacks that make up security problems for IoT devices for consumers in an IoT environment, and they provided several suggestions and strategies that mitigate the potential security risks of these attacks. The authors presented recommendations to address security problems in unsafe devices that depend on the IoT, such as critical infrastructure installations, and smart homes. Solutions to security problems should not be mere ideas, but sectors must cooperate to implement them and address gaps and attacks that threaten Internet security devices now and in the future.

In [27], the authors presented an integrated survey to conduct security testing on IoT devices. They proposed an open-source platform that collects and accurately identifies vulnerabilities in IoT networks and connections. In this platform, the basic system works with high flexibility, as it can be modified easily to enable additional options, such as tests, as well as adding new functions and security assessment tools. This test exists without human intervention and works with good quality and accuracy, given that it works to report the presence and identify security problems in IoT devices and can identify attacks against these devices. It is also designed to focus on monitoring communication with interconnected devices, enabling the system to alert if a harmful activity is detected. To prove the capabilities of this test, it was used to examine and identify vulnerabilities and attacks in the two IoT devices, which is a smart lamp and a wireless camera.

In [28], the authors presented a comprehensive detailed review of the challenges and obstacles facing security on the IoT, as well as reviewing security issues in the IoT environment and discussing them, reviewing important emerging technologies that are interested in working to achieve safety and privacy and ensuring a high degree of trust and security in Internet applications and networks. Four important technologies are currently reviewed and discussed, namely, fog and blockchain computing, edge computing, ML technologies, and the influence of each technology at work to increase the level of security and protection in IoT devices and applications.

The authors in [29] analyzed the security problems related to each layer of the IoT separately and proposed new security solutions for each problem. The authors also presented an analysis of the heterogeneous integration process present in the layers of the IoT, discussing its security issues in detail as a whole and working to find solutions to it. They compared and identified security issues between the IoT and those found in traditional networks and suggested many open security solutions to the problems of the Internet and its devices.

In [30], the authors presented a comprehensive analysis of security issues and especially data in IoT devices and networks. They also provided an overview and discussion of the most important current and future developing trends in the field of the IoT and the progress of the rapid development in the IoT environment.

In [31], the authors provided a comprehensive overview of the IoT environments that are concerned with the existence of BCMs and play an important role. They discussed the importance of the concept of blockchain in the security of the Internet and its development in recent years as it was only interested in digital currency, although blockchain has entered into many fields now. The results showed that BCM is part Only those who solve IoT security problems and due to the contract of IoT devices and their restrictions still need other protection and safety mechanisms.

In [32], the authors presented a comprehensive survey to discuss the main security problems facing the IoT. They provided a comprehensive review and classification of the most common security problems that are concerned with creating layers of the IoT, as well as engineering the protocols that are used in networks and communications on the IoT environment. The authors identified the most important security and privacy requirements for the IoT. In addition, they discussed the attacks and threats and the most important recently proposed security solutions. They also tabulated and drew a map explaining the most important problems and threats to IoT security, as well as presented the suggested solutions found in previous studies. Importantly, the authors also provided an overview of the blockchain and how it has become a key factor in providing solutions to many IoT security threats and problems. The authors also identified the most important open research problems in the field of Internet security and the challenges it faces in the future.

3.2 ML in IoT Security

In [16], the authors provided a comprehensive overview of the IoT and its most important areas of application. They demonstrated and explained basic security issues using the CIA triangle and discussed the security issues of each layer. The authors then provided a systematic overview of the most important technologies to address security problems on the IoT, namely ML, artificial intelligence (AI), and blockchain. Finally, they presented a study analysis and the most important security issues presented by ML, AI, and blockchain with the security challenges facing the IoT in the future.

The authors in [33] presented a security framework with a new approach that is based on ML and automatically fits into the different and multiple aspects of security and privacy related to the IoT. This framework links the most important factors that enable the functioning of software-defined networks (SDNs) and knowledge of virtual simulation that is linked to network function virtualization (NFV) to mitigate the risks of various security threats. The work of this AI framework is characterized by the combination of the monitoring and interaction factors based on AI and the presence of the use of the most important ML models for the purpose of analyzing network patterns. Supervised learning, the system of mining for distributed data and the neural network, was used in the work of this framework. The results of the experiments on this framework showed a high efficiency in detecting attacks that threaten the security of the IoT. The authors evaluated the experiment using a true intelligent build scenario based on a single class SVM. The accuracy of the anomaly detection result is 99.71%. It is a high percentage that demonstrates the efficiency of this framework in detecting security threats on the IoT.

In [34], the authors proposed a new technique to provide protection and security for the privacy of sites, depending on the existence of a tree structure and anonymous box. This proposed mechanism provides protection for the site and its privacy and provides security for the services designated for smart stations. The authors ran simulations that showed effective results and made the time available to create the group shorter. The combined subset of the unknown group is considered the largest, and the study proved that the multiple classification algorithm BDT-SVM works accurately on the possibility of obtaining useful results that improve the accuracy of the intrusion detection system (IDS) and penetration, thereby reducing the time to detect intrusion and attacks on the system.

In [35], the authors applied SVM to accurately interpret and analyze traffic data and its distinctive patterns and then discover the presence of anomalies between them. In this study, the implementation of the SVM algorithm and its effectiveness for classifying and analyzing a quantity of traffic data in three cities in the UK were discussed. Implementation and analysis were conducted using a Raspberry Pi3 processor acting as a recruitment router and ML algorithm for SVM with the help of Python Scikit libraries. This approach was used to prove the maintenance of security protocols, deal with various heterogeneous data, and protect the system from attacks.

The authors in [36] presented a new approach to working on IoT authentication due to the large number of IoT devices lacking security, and the number will increase significantly in the future. Therefore, they worked on authentication for the PHY layer concerned with analyzing and using fingerprints to determine the original characteristics of the devices and the RF-DNA. The results in this study were 100% successful, which is an extremely high percentage, in performing identity verification for authorized users by conducting three experiments on randomly selecting six radio devices. The result indicated that all types of attack that were performed to impersonate the radio identity were rejected, and the noise ratios were determined by 3 dBm using RF-DNA fingerprinting based on Relief-F algorithm.

In [37], the authors presented an integrated comprehensive survey of the most important studies that discussed the IDS for IoT devices and networks in the period of 2015–2019. The authors discussed the most important strategies and methods for identifying and analyzing IDS sites and focused on strategies for analyzing and interpreting IDS in the environment of IoT devices and networks. They also analyzed and clarified the most important various breaches that devices and networks are exposed to on the IoT and ways to deal with them using ML techniques and algorithms and DL techniques that are effective in detecting and identifying the most important attacks in the IoT environment. The authors were also interested in presenting the most important future challenges facing IoT devices in terms of the security and privacy of their users.

In [38], the authors were mainly concerned with designing a smart, accurate, and self-functioning system that relies mainly on the IoT and is distinctive in terms of ease of use and the way it is comfortably worn. Their study contributes to helping users in the event of a security problem that causes them fear and panic by sharing the users' location and helping them find the nearest safe place to go. The proposed system is easy to use and is designed in a safe manner, depending on the KNN algorithm to easily detect intrusions and keep it safe, as well as using ML algorithms that help ensure the safety of the designed system. The system is protected, such that it cannot be reached by an unauthorized person. It is controlled with raspberry pi.

The study in [39] concerns the clarification of a system that works to detect intrusion (IDS) based on DL and ML to face the various attacks in IoT networks and devices. The authors suggested using long short-term memory (LSTM), as well as ML algorithms, such as KNN, to create a model aimed at attack detection and then compare and evaluate the performance of the algorithms used based on several criteria (e.g., detection time, geometric mean computation, and sensitivity presence). The performance of the improved IDS was compared and evaluated with the presence of a large number of BoT-IoT data sets.

In [40], the authors presented several anomaly detections schemes (ADSs), which are concerned with the implementation and identification of the SVM, to work on detecting and identifying breaches and various security attacks in the IoT. Then, they classified the different ADS approaches and provided a comprehensive discussion of the various algorithms and techniques of ML and AI that have been applied in cooperation with the SVM classifier to identify anomalies.

In [41], the authors presented a new framework model and identified a hybrid problem-solving algorithm for identifying malicious traffic methods and detecting attacks using learning algorithms and their applications on the IoT. They implemented and defined a set of information and data based on BoT-IoT and then categorized 44 subtle and powerful features of ML algorithms. Then, they cataloged five specific effective ML algorithms that classify and identify harmful and extraneous traffic, and criteria that measure the function of the ML algorithm were then presented. This approach was conducted to determine which ML algorithm works most effectively and accurately in classifying and finding IoT anomalies and detecting intrusion. The experimental results showed the effectiveness of the proposed model with high accuracy with a set of ML algorithms.

The authors in [42] presented a framework designed to identify and discover DDoS present in a network environment of the IoT that relies on ML techniques. They implemented one of the effective ML algorithms, which is the Bayes algorithm, and applied it to each key to detect harmful and strange traffic. The authors also provided a central platform that synchronizes parameters accurately between the keys due to a lack of accurate identification of training data in each key. A wide range of evaluation and comparison of the proposed algorithm and its method of operation with many modern schemes was conducted to evaluate its performance and effectiveness.

In [43], the authors proposed a service structure that depends entirely on the cloud to determine the requirements of ML models. The service structure also ensures the suitability of ML models in the operational configurations of the various IoT devices to maintain the security of the devices in a high degree and ensure the effectiveness of the operational configurations. The heavy weight in the cloud (e.g., selecting features; creating the model; and working on training, verification, and validation) is a result of reducing the burden of IDS maintenance on the device and IoT network and maintaining the existence of the security model as a service in the cloud.

In [44], the authors presented a new proposal based on a secure demand-side management (DSM) engine, which relies on ML algorithms. The proposed method works in a network that promotes and uses the IoT. It is responsible for the necessity to define a high level of energy efficiency and quality, depending on the order of priorities. Then, a proposal was made for an easy and flexible model for controlling intrusion and infiltration within the smart grid. The elastic factor predicts dishonest entities using the ML classifier. The simulation results for the proposed model revealed that the DSM is efficient with high accuracy intrusion detection and is good at using less energy for the smart grid.

Table 5: Suggested Security Methods Using ML Algorithms.

Ref.	***Year***	***ML Algorithm***	***Security Technique***	***Results***
[33]	2020	SVM	A new approach that is based on ML and automatically fits into the different and multiple aspects of security and privacy related to the IoT. This framework links the most important factors that enable the functioning of SDNs and knowledge of virtual simulation that is	The experiment results on this framework showed a high efficiency in detecting attacks that threaten the security. The accuracy of the anomaly detection result is 99.71%. This high percentage demonstrates the

			linked to NFV to mitigate the risks of various security threats.	efficiency of this framework in detecting security threats on the IoT
[34]	2020	BDT-SVM	A new technique for providing protection and security for the privacy of sites, depending on the existence of a tree structure and anonymous box. This proposed mechanism provides protection for the site and its privacy and provides security for the services designated for smart stations.	The study proved that the multiple classification algorithm BDT-SVM works accurately in obtaining useful results that improve the accuracy of the IDS and penetration and thus reduce the time to detect intrusion and attacks on the system.
[36]	2020	SVM	A new approach on IoT authentication, given the large number of IoT devices lacking security, and the number will increase significantly in the future. Therefore, a method was proposed for the authentication for the PHY layer concerned by analyzing and using fingerprints to determine the original characteristics of the devices and the RF-DNA.	The results in this study were 100% successful, which is an extremely high percentage, in performing identity verification for authorized users by conducting three experiments on randomly selecting six radio devices.
[38]	2020	KNN	A smart, accurate, and self-functioning system, which relies mainly on the IoT and is distinctive in terms of ease of use and the way it is comfortably worn, was designed. It depends on the KNN algorithm to easily detect intrusions and keep it safe, as well as use ML algorithms that help ensure the safety of the designed system.	The results proved the efficiency of the system by using the KNN algorithm to easily detect interferences, in addition to the use of ML algorithms that helped ensure the integrity of the designed system.
[39]	2020	KNN	A system that works to detect intrusion (IDS) based on DL and ML to face the various attacks in IoT networks and devices. The authors suggested using LSTM, as well as ML algorithms, such as KNN.	IDS enhanced the performance, and it was compared and evaluated against a large number of BoT-IoT data sets and was proven effective and efficient.
[41]	2020	Bayesian algorithms	A new framework model was proposed, and a hybrid problem-solving algorithm was used to identify malicious traffic methods and detect attacks using learning algorithms and their applications on the IoT.	The results showed the effectiveness of the proposed model with high accuracy with a set of ML algorithms.
[42]	2020	Bayesian algorithms	A framework was designed to identify and discover DDoS present in a network environment of the IoT that relies on ML techniques.	The framework was applied in a wide range of evaluation, and comparison of the proposed algorithm and its modus operandi were conducted with many modern schemes to evaluate its performance, effectiveness, and efficiency.
[44]	2020	Bayesian algorithms	A new method was proposed based on a secure DSM engine, which relies on ML algorithms that work in a network that promotes and uses the IoT.	The simulation results for the proposed model revealed that DSM is efficient, with high accuracy intrusion detection, and is good at using less energy for the smart grid.

4. Discussion

In this comprehensive survey, we discussed 21 recent studies that covered several important aspects of security and privacy on the IoT environment. These studies also provided the most important and latest solutions to address security attacks that threaten the security of devices and networks on the IoT environment by using ML algorithms. The authors made many new proposals to address the security flaws in Internet devices and networks. One of the most important ML algorithms that have been used in recent studies is SVM. This algorithm is flexible and extensible. It is also distinguished by its ability to accurately detect intrusion inside networks and devices of the IoT.

To achieve authentication and confidentiality on the IoT environment, the authors used SVM. In one study, the authors proposed a new methodology, which concerns the most important factors that enable the functioning of SDNs and knowledge of virtual simulation that is linked to NFV to mitigate the risks of various security threats. This framework has proven its effectiveness and efficiency in dealing with security risks by relying on SVM. On the basis of the lack of security and privacy in most IoT devices, the authors presented in another study a new methodology based on authentication of the PHY layer concerned with the analysis and the use of fingerprints to determine the original characteristics of the devices and RF-DNA. By relying on SVM, this methodology has also proven to be highly effective and efficient.

To achieve integrity and data integrity within devices and networks in an IoT environment, the authors recommended in many of the studies we have reviewed the use of KNN in many of the new methodologies presented. KNN is a good technique widely used in ML that is effective and accurate for infiltration detection. This algorithm is considered effective on the IoT in detecting intrusions. In one of the studies that we discussed, the authors presented a smart and accurate system that relies mainly on the IoT and is distinguished in terms of ease of use and flexibility and depends on the KNN algorithm to easily detect intrusions and attacks and ensure the safety of the designed system. This designed system has proven effective in preserving the integrity of sensitive devices and data.

Traffic in IoT devices is characterised by diversity, large volume of data, and greatly variable speeds. Therefore, most ML algorithms and techniques are considered inadequate to be compatible with IoT devices and networks and to maintain effective and flexible data management. Therefore, appropriate modifications must be performed to improve and develop ML algorithms and maintain the security of devices and networks in the environment of the IoT.

Many complex memory and processing problems in ML algorithms need improvement and development. ML algorithms and techniques also lack the flexibility and compatibility, with large data to process. IoT devices and networks are considered to have limited capabilities and limited processing standards. Therefore, applying traditional ML algorithms in resource-limited environments, such as the IoT environment, is pointless. In addition, the data of IoT devices must be dealt in real time directly; however, the application of ML technologies is not suitable for processing data directly in real time, and it cannot deal with the continuous large flows of data from devices and networks simultaneously. Such data in an extremely large form are the most important measure of trading systems for the Internet, and they appear to be transforming into various environments within an environmental cycle of radiation. Thus, ML algorithms face a problem in processing data within the IoT environment due to their ineffectiveness in dealing with data of different forms linguistically and grammatically. In view of heterogeneity, solutions should be found in future studies to suit ML approaches in IoT devices, which will increase continuously in the future.

5. Conclusion

With the increasing development of IoT devices and the increase in their number and their users, the IoT has become one of the most important technologies of the current and future times, which will be relied upon mainly in routine daily life. Focusing on the safety aspect, maintaining privacy, and solving the security problems facing IoT devices and networks are necessary. In this paper, we presented a comprehensive survey of the most recent and important research conducted from 2018 to 2021. In this paper, we reviewed a comprehensive overview of the IoT and its applications. Then, we discussed the CIA security requirements on the IoT and how to achieve them. We also reviewed the attacks and challenges facing the IoT. We focused on ML algorithms and their applications in addressing the security problem on the IoT. This paper will be useful and practical for readers in gaining a deeper understanding and knowledge of the security aspects that threaten the security and privacy of the IoT, its devices, and applications. We will continue to search in the future for more modern methods and methodologies that focus mainly on raising the level of security and solving the privacy problems that threaten the IoT in all fields.

References

[1] H. F. Atlam, R. Walters, and G. Wills, "Internet of things: state-of-the-art, challenges, applications, and open issues," International Journal of Intelligent Computing Research (IJICR), vol. 9, pp. 928-938, 2018.

[2] H. F. Atlam and G. B. Wills, "IoT security, privacy, safety and ethics," in Digital twin technologies and smart cities, ed: Springer, pp. 123-149, 2020.

[3] L. a. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT Privacy and security: Challenges and solutions," Applied Sciences, vol. 10, p. 4102, 2020.

[4] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," IEEE Communications Surveys & Tutorials, vol. 22, pp. 1686-1721, 2020.

[5] Number of connected devices worldwide 2030. (n.d.). Retrieved from Statista website: https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/

[6] Global IoT connections data volume 2019 and 2025. (n.d.). Retrieved from Statista website: https://www.statista.com/statistics/1017863/worldwide-iot-connected-devices-data-size/

[7] M. S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, et al., "Machine learning for Internet of Things data analysis: A survey," Digital Communications and Networks, vol. 4, pp. 161-175, 2018.

[8] N. Kumar and A. Makkar, Machine learning in cognitive IoT: CRC Press, 2020.

[9] K. Alieyan, A. Almomani, R. Abdullah, B. Almutairi, and M. Alauthman, "Botnet and Internet of Things (IoTs): A Definition, Taxonomy, Challenges, and Future Directions," in Research Anthology on Combating Denial-of-Service Attacks, ed: IGI Global, pp. 138-150, 2021.

[10] P. P. Ray, "A survey on Internet of Things architectures," Journal of King Saud University-Computer and Information Sciences, vol. 30, pp. 291-319, 2018.

[11] H. F. Atlam, A. Alenezi, R. K. Hussein, and G. B. Wills, "Validation of an Adaptive Risk-based Access Control Model for the Internet of Things," International Journal of Computer Network & Information Security, vol. 10, 2018.

[12] C. Maple, "Security and privacy in the internet of things," Journal of Cyber Policy, vol. 2, pp. 155-184, 2017.

[13] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security," IEEE Internet of Things Journal, vol. 7, pp. 10250-10276, 2020.

[14] M. R. Hosenkhan and B. K. Pattanayak, "Security issues in internet of things (IoT): a comprehensive review," New Paradigm in Decision Science and Management, pp. 359-369, 2020.

[15] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, et al. "A survey of machine and deep learning methods for internet of things (IoT) security," IEEE Communications Surveys & Tutorials, vol. 22, pp. 1646-1685, 2020.

[16] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," Internet of Things, vol. 11, p. 100227, 2020.

[17] A. Mubarakali, K. Srinivasan, R. Mukhalid, S. C. Jaganathan, and N. Marina, "Security challenges in internet of things: Distributed denial of service attack detection using support vector machine ‐ based expert systems," Computational Intelligence, vol. 36, pp. 1580-1592, 2020.

[18] S. Benzarti, B. Triki, and O. Korbaa, "A survey on attacks in Internet of Things based networks," in 2017 International conference on engineering & MIS (ICEMIS), pp. 1-7, 2017.

[19] L. Hu, H. Wen, B. Wu, F. Pan, R.-F. Liao, et al., "Cooperative jamming for physical layer security enhancement in Internet of Things," IEEE Internet of Things Journal, vol. 5, pp. 219-228, 2017.

[20] J. Verbraeken, M. Wolting, J. Katzy, J. Kloppenburg, T. Verbelen, et al. "A survey on distributed machine learning," ACM Computing Surveys (CSUR), vol. 53, pp. 1-33, 2020.

[21] M. Aghbashlo, W. Peng, M. Tabatabaei, S. A. Kalogirou, S. Soltanian, et al., "Machine learning technology in biodiesel research: A review," Progress in Energy and Combustion Science, vol. 85, p. 100904, 2021.

[22] M. Mahmud, M. S. Kaiser, A. Hussain, and S. Vassanelli, "Applications of deep learning and reinforcement learning to biological data," IEEE transactions on neural networks and learning systems, vol. 29, pp. 2063-2079, 2018.

[23] Y. Meidan, M. Bohadana, A. Shabtai, M. Ochoa, N. O. Tippenhauer, et al., "Detection of unauthorized IoT devices using machine learning techniques," arXiv preprint arXiv:1709.04647, 2017.

[24] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning ddos detection for consumer internet of things devices," in 2018 IEEE Security and Privacy Workshops (SPW), pp. 29-35, 2018.

[25] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," IEEE transactions on neural networks and learning systems, vol. 27, pp. 1773-1786, 2015.

[26] T. Alladi, V. Chamola, B. Sikdar, and K.-K. R. Choo, "Consumer IoT: Security vulnerability case studies and solutions," IEEE Consumer Electronics Magazine, vol. 9, pp. 17-25, 2020.

[27] O. A. Waraga, M. Bettayeb, Q. Nasir, and M. A. Talib, "Design and implementation of automated IoT security testbed," Computers & Security, vol. 88, p. 101648, 2020.

[28] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, et al. "A survey on IoT security: application areas, security threats, and solution architectures," IEEE Access, vol. 7, pp. 82721-82743, 2019.

[29] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," Future generation computer systems, vol. 108, pp. 909-920, 2020.

[30] R. Román-Castro, J. López, and S. Gritzalis, "Evolution and trends in IoT security," Computer, vol. 51, pp. 16-25, 2018.

[31] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," Internet of Things, vol. 1, pp. 1-13, 2018.

[32] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future generation computer systems, vol. 82, pp. 395-411, 2018.

[33] M. Bagaa, T. Taleb, J. B. Bernabe, and A. Skarmeta, "A machine learning security framework for iot systems," IEEE Access, vol. 8, pp. 114066-114077, 2020.

[34] J. Li, "IOT security analysis of BDT-SVM multi-classification algorithm," International Journal of Computers and Applications, pp. 1-10, 2020.

[35] S. Sankaranarayanan and S. Mookherji, "SVM-based traffic data classification for secured IoT-based road signaling system," in Research Anthology on Artificial Intelligence Applications in Security, ed: IGI Global, pp. 1003-1030, 2021.

[36] D. Reising, J. Cancelleri, T. D. Loveless, F. Kandah, and A. Skjellum, "Radio identity verification-based IoT security using RF-DNA fingerprints and SVM," IEEE Internet of Things Journal, vol. 8, pp. 8356-8371, 2020.

[37] A. Thakkar and R. Lohiya, "A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges," Archives of Computational Methods in Engineering, vol. 28, pp. 3211-3243, 2021.

[38] B. S. Yaswanth, R. Darshan, H. Pavan, D. Srinivasa, and B. V. Murthy, "Smart Safety and Security Solution for Women using kNN Algorithm and IoT," in 2020 Third International Conference on Multimedia Processing, Communication & Information Technology (MPCIT), pp. 87-92, 2020.

[39] S. S. S. Sugi and S. R. Ratna, "Investigation of Machine Learning Techniques in Intrusion Detection System for IoT Network," in 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), IEEE, pp. 1164-1167, 2020.

[40] M. Hosseinzadeh, A. M. Rahmani, B. Vo, M. Bidaki., M. Masdari, et al., "Improving security using SVM-based anomaly detection: issues and challenges, " Soft Computing, vol. 25(4), pp. 3195-3223, 2021.

[41] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for Internet of Things in smart city, " Future Generation Computer Systems, vol. 107, pp. 433-442, 2020.

[42] W. He, Y. Liu, H. Yao, T. Mai, N. Zhang, et al., "Distributed variational bayes-based in-network security for the Internet of Things," IEEE Internet of Things Journal, vol. 8, pp. 6293-6304, 2020.

[43] M. Alsharif, and D. B. Rawat, "Study of machine learning for cloud assisted IoT security as a service," Sensors, vol. 21(4), p. 1034, 2021.

[44] M. Babar, M. U. Tariq, and M. A. Jan, "Secure and resilient demand side management engine using machine learning for IoT-enabled smart grid," Sustainable Cities and Society, vol. 62, p. 102370, 2020.