 doi:10.20944/preprints202203.0087.v1

Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions

Iqbal H. Sarker[1,2,*], **Asif Irshad Khan**[3], **Yoosef B. Abushark**[3] **and Fawaz Alsolami**[3]

Abstract The Internet of Things (IoT) is one of the most widely used technologies today, and it has a significant effect on our lives in a variety of ways, including social, commercial, and economic aspects. In terms of automation, productivity, and comfort for consumers across a wide range of application areas, from education to smart cities, the present and future IoT technologies hold great promise for improving the overall quality of human life. However, cyber-attacks and threats greatly affect smart applications in the environment of IoT. The traditional IoT security techniques are insufficient with the recent security challenges considering the advanced booming of different kinds of attacks and threats. Utilizing artificial intelligence (AI) expertise, especially *machine and deep learning solutions*, is the key to delivering a dynamically enhanced and up-to-date security system for the next-generation IoT system. Throughout this article, we present a comprehensive picture on *IoT security intelligence*, which is built on machine and deep learning technologies that extract insights from raw data to intelligently protect IoT devices against a variety of cyber-attacks. Finally, based on our study, we highlight the associated *research issues and future directions* within the scope of our study. Overall, this article aspires to serve as a reference point and guide, particularly from a technical standpoint, for cybersecurity experts and researchers working in the context of IoT.

Keywords Internet of Things; cyber-attacks; anomalies; machine learning; deep learning; IoT data analytics; intelligent decision-making; security intelligence

1 Introduction

The Internet of Things (IoT) is one of the most widely used technologies today and is often described as a connected network of heterogeneous components enabling intelligent systems and services that detect, capture, distribute, and analyze data. Things in the IoT devices refer to smart devices, such as sensors, smartwatches, smart refrigerators, smoke detectors, radio frequency identification (RFID), heartbeat monitors, accelerometers, smartphones, and so on, that collect and transmit data. The number of connected things in IoT systems is increasing day by day. For instance, there will be about 20.4 billion connected things globally in 2022, compared to 8.4 billion connected things in 2020 [57]. The IoT has a significant effect on our lives in a variety of ways, including social, commercial, and economic aspects. In terms of growing the digital economy, the IoT sector is projected to grow in revenue from 892 billion in 2018 to 4 trillion by 2025 [57]. The IoT enables large-scale technological advancements and value-added services in a variety of areas of our lives, including smart homes, smart cities, transportation, logistics, smart health, retail, agriculture, and business, as well as smart metering, remote monitoring, and process automation. In terms of automation, performance, and comfort, current and future IoT applications and

[1] Swinburne University of Technology, Melbourne, VIC-3122, Australia.
[2] Department of Computer Science and Engineering, Chittagong University of Engineering & Technology, Chittagong-4349, Bangladesh.
[3] Computer Science Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah-21589, Saudi Arabia.
∗Correspondance: msarker@swin.edu.au (Iqbal H. Sarker)

services have tremendous potential for enhancing consumer quality of life. However, in the context of IoT, numerous sorts of cyber-attacks and threats are viewed as challenging problems to the expansion of IoT. Therefore, this paper focuses primarily on *IoT security intelligence* to effectively protect systems and applications from a variety of cyber-attacks and threats in IoT.

The most basic need in the IoT network is to protect all of the systems, apps, and connected devices. IoT networks' massive size introduces new challenges in a variety of areas, including device management, data management, computing, security, and privacy, etc. As the IoT grows, various security concerns are being raised as potential threats. Without a trusted system, the emerging IoT applications, such as those mentioned above, will be unable to meet the needs of people and society and may lose all their potential. Typically, IoT systems operate on several layers, including the perception or sensing layer, the networking, and data communication layer, the middleware or support layer, and the application layer. These layers are briefly discussed in Section 3. Each of these layers has a unique set of tasks and relevant technologies to perform in an IoT application, and each layer brings a new set of issues and security risks. For example, denial of service (DoS) attacks, spoofing attacks, jamming, eavesdropping, data tampering, a man in the middle attacks, and malicious, etc. are the most common IoT attacks [137]. Thus, depending on the nature of the security issues, potential IoT security solutions such as authentication, access control, threat and risk prediction, malware analysis, anomaly or intrusion detection, and prevention, etc, could be useful. Due to the advanced boom in security threats and attacks, and complexity in security incidents, the conventional techniques for dealing with them are no longer effective. Therefore an intelligent security system based on modern technologies that can address these security concerns is urgently required to protect the next-generation IoT system.

Artificial Intelligence (AI) is one of the most important technologies for developing intelligent systems, and it is considered to be a part of the Fourth Industrial Revolution (4IR) [119] [130] as well. Thus, utilizing AI knowledge, particularly, *machine and deep learning*, we can detect anomalies or unwanted malicious activities in the IoT, and, as a result, offer a dynamic security solution that is constantly improved and up to date. Typically, machine or deep learning models comprise a set of rules, methods, or complex transfer functions that extract useful insights or interesting data patterns from the security data [122]. Thus, it is possible to utilize the resultant security models to train machines to predict threats or risks at an early stage, or to identify anomalies in IoT to develop an appropriate defensive policy. Based on information gathered so far from the literature on these technologies and their use in the IoT environment, the contribution of this article is summarized as follows:

- This study concentrates on the knowledge of artificial intelligence, particularly, machine and deep learning-based IoT security solutions with their effectiveness.
- We discuss IoT environment, various IoT security challenging issues, IoT systems with various layers, and associated security issues in each layer, to highlight the scope of this study.
- We present different machine learning techniques as well as deep learning architectures and techniques, and their usage for intelligent security modeling to solve the security problems, in the environment of IoT.
- Finally, we explore the issues that have been encountered, as well as potential research opportunities and future directions, to secure and trust IoT networks and systems.

The remainder of the paper is carried out as follows: The Section 2 discusses the domain's history and reviews related work. We discuss IoT system architectures with different layers and the associated security issues in each layer in Section 3. We present various machine and deep learning-based security solutions in the IoT environment in Section 4. The challenges faced, as well as prospective study opportunities and future directions, are highlighted in Section 5, and the work is concluded in Section 6.

2 Background and Related Work

In this section, we make a comprehensive literature review on the IoT environment with various application areas, IoT security challenging issues, and recent IoT security approaches including machine learning techniques, and highlight the scope of our study.

2.1 The IoT Paradigm

The Internet of Things (IoT) represents a paradigm shift in information technology. The term 'Internet of Things,' which is also abbreviated as IoT, is composed of two key words: the first is 'Internet,' and the second is 'Things', where the Things are defined as smart devices or objects.

The Internet of Things (IoT) is one of the emerging smart technologies for the Fourth Industrial Revolution (or Industry 4.0), which represents the ongoing automation of traditional manufacturing and industrial practices [130]. The IoT refers to a network of interconnected, internet-connected devices that may collect and send data over a wireless network without the need for human intervention. Several organizations and research groups describe IoT and smart environments in a variety of ways and from a variety of perspectives. For instance, Thiesse et al. [141] define the IoT as "consisting of hardware items and digital information flows based on RFID tags". The Institute of Electrical and Electronics Engineers (IEEE) defines the IoT as a "collection of items with sensors that form a network connected to the Internet" [93]. The European Telecommunications Standards Institute (ETSI) defines "machine-to-machine (M2M) communications as an automated communications system that makes decisions and processes data operations without direct human intervention" [72]. Cisco (San Francisco), which is well-known as the worldwide leader in IT, networking, and cybersecurity solutions, has summarized the IoE (Internet-of-everything) concept "as a network that consists of people, data, things, and processes" [36].

The RFID (Radio Frequency Identification) group defines the "IoT as the worldwide network of interconnected objects uniquely addressable based on standard communication protocols" [143]. According to Cluster of European research projects on the IoT [133] - "Things are active participants in business, information and social processes where they are enabled to interact and communicate among themselves and with the environment by exchanging data and information sensed about the environment while reacting autonomously to the real/physical world events and influencing it by running processes that trigger actions and create services with or without direct human intervention". Gubbi et al. [50] define "IoT is the interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications". Atzori et al. [29] define IoT in three paradigms such as internet-oriented (middleware), things-oriented (sensors), and semantic-oriented (knowledge).

In general, the IoT's main pillars are as follows: smart devices, data, analytics, and connectivity. Thus, the IoT can be defined as a network of connected heterogeneous components that can sense, collect, transmit, and analyze data over a wireless network to enable intelligent decision making and services aimed at improving the quality of human life, where the Things are defined as smart devices or objects such as sensors, smartwatches, and smartphones, etc.

2.2 IoT-based Smart Environments

A smart environment is typically a world, where the sensors and computing devices are integrated with everyday objects through a connected network to enhance the comfort and efficiency of human life. Ahmed et al. [23] state that "the term 'smart' refers to the ability to autonomously obtain and apply knowledge, and the term 'environment' refers to the surroundings". According to Belissent et al. [32], "a smart environment uses information and communications technologies to make the critical infrastructure components and services of a city's administration, education, healthcare, public safety, real estate, transportation and utilities more aware, interactive and efficient". Recent developments in IoT have elevated it to the status of technology for creating smart environments, such as intelligent cities, intelligent healthcare systems, intelligent building management systems, etc. Figure 1, and Figure 2 depicted a graphical depiction of the total number of connected IoT devices and the worldwide IoT market [137], as well as the potential economic impact and projected market share of dominant IoT applications by 2025 [24].

The goal of such smart environments is to provide services based on data acquired by IoT-enabled sensors using intelligent methods, which has a significant impact on our lives [124] in various dimensions, such as social, commercial, as well as economic. According to the statistics of Navigant Research mentioned in Elrawy et al. [43], the global smart city services market is expected to be 225.5 billion US dollars by 2026, while 93.5 billion US dollars in 2017. A range of factors, such as usable bandwidth, serving an increasing number of users and smart objects in IoT networks, managing large volumes of data, scalable computing systems, such as cloud computing, etc., need to be considered in the implementation of the IoT paradigm for building smart environments, e.g. smart cities, for the quality of services of smart environment applications [136].

2.3 What Makes IoT Security Challenging?

Many personal and commercial equipment are becoming "smart" as the digital revolution takes hold. On IoT networks, traditional security and privacy approaches may fail. The dynamic nature of IoT connectivity introduces a new set of security challenges. The following are some examples:

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 March 2022 doi:10.20944/preprints202203.0087.v1

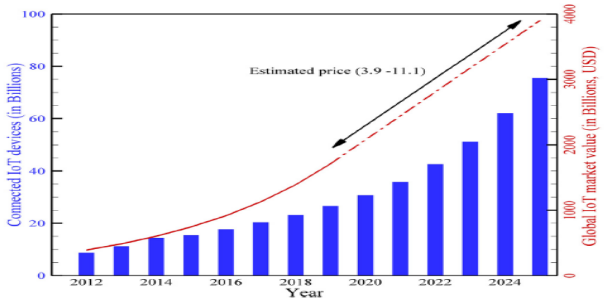

Fig. 1: Total connected IoT devices and global IoT market so far and future prediction.

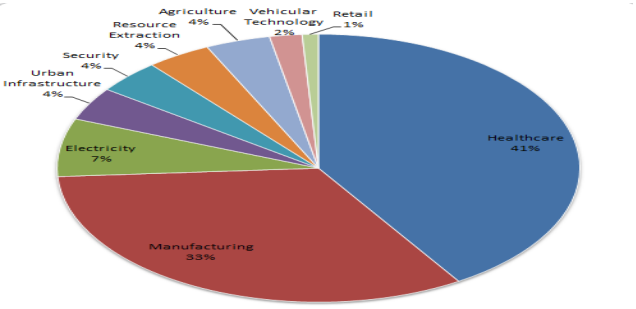

Fig. 2: Potential economic impact and projected market share of dominant IoT applications by 2025.

- *Heterogeneity:* IoT intends to connect a huge number of heterogeneous devices [82] to enable advanced applications that can improve human life quality. As a result, IoT devices come in a variety of shapes and sizes, resulting in a diverse set of hardware and software schemes.
- *Volume:* In IoT, a large number of devices, i.e., billions of smart devices [57], are interconnected, which are coupled with the high volume, velocity, and structure of real-world data.
- *Inter-connectivity:* The IoT refers to the interconnection between devices, the information they send and receive to one another, like a conversation. Thus, IoT networks are accessed with the nature of any time, and anywhere [82].
- *Structure and vulnerability:* Various types of attacks, such as cookie theft, cross-site scripting, structured query language injection, session hijacking, and often distributed denial of service, are vulnerable to IoT devices. On a large, self-organized IoT network, the vulnerability to distributed denial of service attacks typically grows [57].
- *Dynamism:* As IoT devices are continually removed and added, the nature of the network reconfiguration is dynamic and must be adaptable [82].
- *Proximity:* In short-range communications, ad hoc networks may rely on local devices. Proximity means that an IoT-enabled object changes and behaves according to the current location [34].
- *Latency and reliability:* The main challenges in industrial IoT networks include low-latency and high-reliability wireless communication. Sensitive applications like surgical devices, assembly line production, and traffic monitoring, etc. require high-reliable, and low-latency communication [89].
- *Cost, resource, and energy consumption:* An IoT device is a piece of hardware with a sensor that transmits data from one place to another over the Internet. The systems should be configured to reduce needed resources as well as costs due to a large number of sensors in a complex system application [82].
- *Security and privacy protection:* Consumer and proprietary data must be secured and protected, particularly in sensitive domains, such as healthcare applications [82].
- *Intelligent decision-making :* For many IoT applications, sophisticated decisions should be intelligent, according to the preferences of the users, and must be made in real-time.

Although most of these issues are shared by many Internet access points, the constraints of IoT devices, as well as the dynamic nature and complexity of the environment in which they operate, magnify many of these concerns beyond the scope of traditional security capabilities.

2.4 Related work and the Scope of this Study

Several studies have been done on IoT security. For instance, the authors in [68] present a survey of IoT security issues, where they review and categorize the popular security issues, such as attacks, threats, concerning the IoT layered architecture, networking, communication, and management. Another study on IoT security has been presented in [94].

The authors in [153] present several research challenges and opportunities related to IoT security, where they have considered the general security background of IoT. In [56], an overview of the current status of IoT security research, as well as associated tools like IoT modelers and simulators, was presented. In [91], the authors provide an overview of security concepts, technological and security concerns, viable solutions, and prospective approaches for safeguarding the IoT. They give their analysis of the current state and issues of IoT security in their survey, which takes into account three layers of architecture: perception layer, network layer, and application layer. The authors of [57] undertake an

IoT security survey that takes into account application domains, security threats, and solution architectures. A taxonomy on IoT vulnerabilities, attack vectors, attacks that exploit such vulnerabilities, and corresponding methodologies, has been presented in [99]. In [26], a study on IoT security is presented by the authors, which focuses on the most recent IoT security threats and vulnerabilities identified via a thorough assessment of current IoT security studies.

In addition to these surveys, many research on machine learning have been conducted. For example, in the paper [145], the authors explore the threat model for IoT systems and evaluate IoT security solutions based on machine-learning methods like supervised learning, unsupervised learning, and reinforcement learning. They explore methods to data privacy protection that use learning-based IoT authentication, access control, secure offloading, and malware detection. The authors examine the security requirements, attack vectors, and other discussions in [61], focused on computer learning for the IoT networks. In [25], a survey of computer and deep learning techniques for IoT security was presented. In [154], the impact of IoT new features on protection and privacy considering new threats, existing solutions and challenges was addressed. In order to construct data-driven security systems employing machine and deep learning techniques, it's important to understand the nature of data including various forms of cyber threats and related features. There are several such datasets exist in the area of cybersecurity. Hence, we have summarized as NSL-KDD [139], UNSW-NB15 [97], DARPA [147] [85], CAIDA [4] [3], ISOT'10 [14] [13], ISCX'12 [5] [128], CTU-13 [10], CIC-IDS [9], CIC-DDoS2019 [6], MAWI [64], ADFA IDS [146], CERT [84] [48], EnronSpam [12], SpamAssassin [17], LingSpam [15], DGA [1] [2] [11] [151], Malware Genome project [155], Virus Share [18], VirusTotal [19], Comodo [7], Contagio [8], DREBIN [74], Microsoft [16], Bot-IoT [71]. The machine and deep learning based model can be built utilizing these datasets, according to the problem domain. For instance, a neural network based deep learning model is used to build an intrusion detection model utilizing NSL-KDD dataset [45]. In [38], the authors use several such NSL-KDD [139], UNSW-NB15 [97], CIC-IDS [9], while analyzing their machine learning-based network intrusion detection model for IoT security.

Unlike the previous studies, this paper focuses on artificial intelligence knowledge, particularly machine and deep learning-based IoT security solutions. For this, we present different machine learning techniques as well as deep learning architectures and techniques, and their usage for intelligent security modeling to solve the security problems, in the context of IoT.

3 IoT System Architectures and Security Issues

In this section, we first highlight the attack surface areas of the IoT, and then we summarize the security issues through the overall architecture of an IoT system.

3.1 IoT Attack Surface Areas

In the following, we summarize surface areas for IoT attacks, or areas where threats and vulnerabilities can exist in IoT systems and applications. These are:

- *Devices:* IoT devices are one of the most common ways that cyberattacks are initiated. Memory, firmware, the physical interface, the web interface, and network resources are all aspects of an IoT system that can be vulnerable. Attackers can take advantage of vulnerable update systems, outdated components, and risky default settings, among other things.
- *Communication channels:* Attacks against IoT components could originate via the communication channels that link them to one another. Protocols used in IoT systems could have security vulnerabilities that could compromise the whole system. IoT systems are vulnerable to well-known network attacks, such as denial of service (DoS) and spoofing, which may cause significant damage.
- *Applications and software:* Vulnerabilities in the web applications and associated software of IoT devices might cause systems to be compromised. Web apps, for example, can be used to steal user credentials or to distribute malicious firmware upgrades.

3.2 Architectures and Security Issues

Based on the IoT attack surface areas highlighted above, in this section, we summarize the security issues through the overall architecture of an IoT system. Several architectures for IoT have been proposed by different researchers and research groups. Conventional IoT architecture is considered to have three layers, such as the perception layer, the network layer, and the application layer [91]. However, the support or middleware layer is considered as an important layer later, according to the needs for data processing and intelligent decision making, which lies between the network layer and the application layer. In several cases, the IoT architectures are based on a network layer and a support layer according

to the needs. Furthermore, the concept of cloud computing for the support layer has been included in some studies of IoT systems. In this paper, we take into account the most popular four-layered IoT architecture, such as the perception layer, the networking, and data communication layer, middleware layer, and the application layer, shown in Figure 3, while discussing the security threats and attacks in the domain of IoT security.

- *Security Issues at Perception or Sensing Layer*: The perception layer is a hardware layer consisting of physical devices and sensors in different forms, thus also known as the sensing layer. These devices or sensors such as mechanical, electrical, electronic, or chemical sensors, are connected with the physical world to capture different kinds of information according to the particular IoT applications. WSN, RFID, and other types of sensing and identifying systems are the key technologies employed in the perception layers [140]. There are four major cybersecurity issues: i) wireless signal strength; ii) sensor node exposure in IoT devices; ii) dynamic nature of IoT topology; and iv) communication, computation, storage, and memory constraints, exist in this layer [98] [87]. To defend the IoT network, this layer employs three popular mechanisms as node authentication, lightweight encryption and the access control mechanism [87].
  Many attacks and crimes target the confidentiality of the perception layer that is common in practice. Examples include node capturing, malicious code, fake data injection, replay attacks, side-channel attacks, etc. [57]. For example, a node capturing attack can cause a node to stop delivering genuine data, destroying the entire network and even compromising the security of the entire IoT application. False data or malicious code injection attacks might produce false results and cause the IoT application to malfunction. Eavesdropping, often known as sniffing or snooping, is a type of attack that uses unsecured network communications to acquire data in transit between devices. A replay attack is defined as spoofing, changing, or repeating the identifying information of smart devices in an IoT network. A time attack occurs when an attacker steals the encryption key associated with time and other critical data [129]. Aside from direct attacks on the nodes, a variety of side-channel attacks may result in sensitive data being leaked.
- *Security Issues at Networking and Data Communications Layer*: The main purpose of this layer is to transmit the information collected by the perceptual layer, as described above. At this layer, cutting-edge technologies such as Wi-Fi, LTE, Bluetooth, 3G/4G, ZigBee, and others are used to operate cloud computing platforms, Internet gateways, switching, and routing devices, among other things [87]. At this layer, the most important cybersecurity issues are confidentiality, privacy, and compatibility. At this layer, attackers have a high probability of evidencing criminal activity through phishing, distributed denial-of-service (DDoS/DoS), data transit attacks, routing attacks, identity authentication, and encryption, among other methods [57] [51].
  For example, this layer of IoT is extremely vulnerable to phishing attacks, which aim to steal personal data such as credit card and login information or to infect victims' devices with malware [57]. Access attack, also known as an advanced persistent threat, occurs when an unauthorized individual or adversary gains access to the IoT network because IoT apps are constantly receiving and transferring valuable data. The most prevalent and destructive attacks on a network are denial of service (DoS) and distributed denial of service (DDoS) attacks, which cause network resources to be exhausted and service to be unavailable. Furthermore, attackers may use routing attacks like sinkhole attacks, wormhole attacks, and others to reroute routing paths during data transmission.
- *Security Issues at Middleware or Support Layer*: It's a layer of software that exists between the network and the application. As a result, this layer is usually in charge of IoT device service management, as well as data processing and intelligent operations on data with decision-making. It can be seen as a dependable support platform, similar to the cloud [50], that makes this layer in the IoT system easier to use. In several cases, the more distributed fog computing technologies have been used to replace the centralized cloud environment, resulting in improved performance and faster response times [35]. At this level, the authenticity, integrity, and confidentiality of all transmitted data should be checked and maintained [87].
  Although the middleware layer is essential for delivering a secure and dependable IoT application, it is also vulnerable to attacks such as insider attacks, man-in-the-middle attacks, SQL injection attacks, signature wrapping attacks, cloud malware injection, cloud flooding attacks, and so on [57] [73]. Internal attackers intentionally modify and extract data or information within the network in a malicious inside attack [81]. Through a SQL injection attack, an attacker can include malicious SQL queries in a program to obtain sensitive data from any user

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 March 2022 doi:10.20944/preprints202203.0087.v1

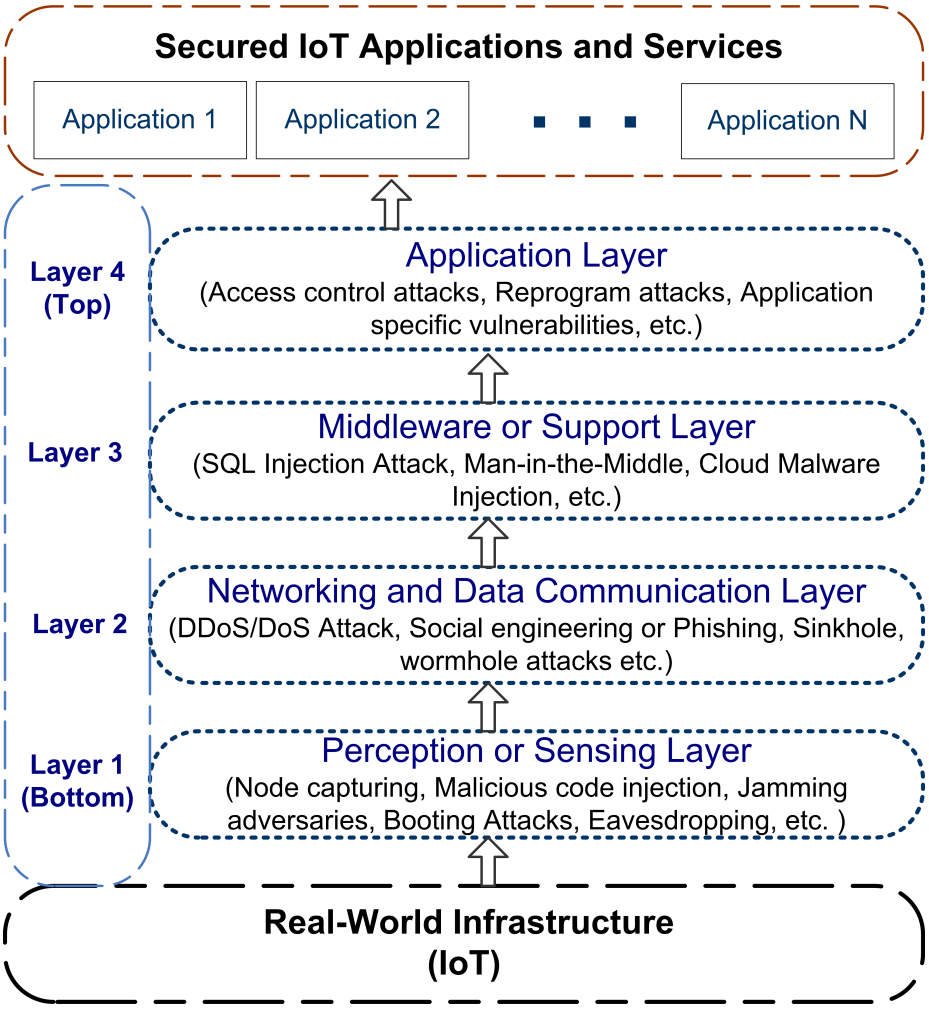

Fig. 3: Various security issues at different layers namely, the perception, network, middleware, and application layers of IoT architecture and systems, which are needed to handle intelligently for secured IoT applications and services in various real-world scenarios.

and even change database records. A virtualization attack occurs when a virtual machine is harmed and its effects spread to other virtual machines. Cloud malware injection allows an attacker to take control of a cloud, inject malicious code, or even implant a virtual machine into a cloud. Cloud flooding attacks, which increase the workload on cloud servers, may have a significant impact on cloud servers.

– *Application layer*: The application layer is responsible for controlling the overall management of IoT apps that interact with users in a personalized way. A personal computer, smartphone, or any smart object or device that can utilize IoT services via Internet connectivity can serve as the interface. In numerous application domains, such as smart homes, smart cities, industrial, building, and health applications, the application layer is dependent on the information processed in the middleware layer [69]. Different applications may have different levels of security needs, depending on the application environment and the necessity. As an example, the security method used in online banking should be more secure than the one used in exchanging climate change forecast information. Many security issues must be addressed at the application layer, including access control attacks, malicious code attacks, sniffing attacks, reprogram attacks, data breaches, service interruption attacks, application vulnerabilities, and software bugs, to name a few examples [57] [75]. In the application layer, malicious data is transferred and exchanged amongst smart devices at the application layer. Practitioners and academics have major issues in protecting data privacy and security as well as identifying things. The attacker injects malware into the system via the use of viruses, worms, Trojan horses, and spyware to deny service,

manipulate data, and/or gain access to confidential data [149]. Service interruption attacks, often known as DDoS attacks, prevent genuine consumers from using IoT applications by intentionally making servers or networks too busy to respond. Attackers may use sniffer programs to monitor network traffic in IoT applications to get access to confidential user data. An attacker might quickly destroy a system in an unauthorized access attack by restricting access to IoT-related services or destroying existing data [87]. Furthermore, attackers may attempt to remotely reprogram IoT devices, which might result in the IoT system being hacked.

As discussed above, several security threats and attacks might happen in each layer of an IoT system. In addition, Zero-day attack [27] [33] [126] that is used to refer to the threat posed by an unknown security [127] [95], are considered as the serious potential security threats. Thus, an in-depth analysis of detecting these cyber-attacks is important, where the knowledge of artificial intelligence, particularly, machine learning methods as well as deep learning architectures or techniques can be considered as a good solution in securing the system from such anomalies in the domain of IoT security.

4 Machine and Deep learning Techniques in IoT Security Solutions

Machine and deep learning techniques are well-known as AI techniques that can help the IoT devices to learn from the experience representing as data, and behave accordingly. The learning models are often comprised of a set of rules, procedures, or sophisticated 'transfer functions' that may be used to uncover relevant security incident trends in IoT data, as well as recognize and predict behavior [42]. As a result, in an IoT context, both machine learning and deep learning can operate in dynamic IoT networks without the requirement for human or user intervention. The potential role of machine learning and deep learning techniques in developing a data-driven model for IoT security intelligence is shown in Figure 4. Several machine learning methods can be used to learn from IoT security data, including classification and regression analysis, clustering, rule-based methods, feature optimization methods [114], and deep learning methods based on artificial neural networks, such as the multi-layer perceptron network, convolutional network, recurrent network, etc. [113] [112]. Thus, in the following section, we will discuss how different machine and deep learning methods can be applied to security solutions in the context of IoT.

4.1 Classification and Regression Techniques

In the area of machine learning, both classification and regression methods are well-known and widely used. A classification task in IoT security is usually defined as predicting a fixed discrete value/category, such as [anomaly, normal] or [attack-1, attack-2, attack-3, etc.] outcome, whereas a regression work is defined as predicting a continuous or numeric value, such as the impact of attacks. Several popular classification techniques, such as k-nearest neighbors [22], support vector machines [67], navies Bayes [65], adaptive boosting [46], and logistic regression [78], decision tree [105], IntrudTree [115], BehavDT [117], ensemble learning such as random forests [37], exist that can categorize security incidents in order to address different IoT security issues, including intrusion or attack detection, malware analysis, and anomaly or fraud detection in IoT.

For instance, the support vector machine classification technique is used in profiling abnormal behavior of IoT devices [80], and for detecting android malware for reliable IoT services [53]. Random forest technique is used to detect anomalies [39] [103], denial of service attack [41], IoT intrusion detection service [106] [96], smart city anomaly detection [28] etc. Similarly, a naive Bayes based classification model is used to detect anomalies [135], and a logistic regression-based method to detect malicious IoT botnets [104] [31]. On the other hand, a regression model is useful for predicting attacks quantitatively or to predict the impact of an attack, such as worms, viruses, or other malicious software [62]. Similarly, a quantitative security model, e.g., phishing in a certain period or network packet parameters, regression techniques could be useful [122]. Several popular regression techniques such as Linear, Logistic, Polynomial, Ridge, Lasso, regression trees, Principal components, ElasticNet, Poisson, Negative binomial, Stepwise, Partial least squares regression [144] etc. exist that can be used to build the quantitative security model according to their working principle in machine learning. For instance, the linear regression-based model is used to identify the cyber attack origin [76], and multiple regression analysis is used for correlating human traits and cybersecurity behavior intentions [49]. Similarly, regression regularization methods such as Lasso, Ridge, or ElasticNet, can enhance security attacks analysis to get a better outcome considering the high dimensionality of IoT security data [52].

Thus, we can conclude that the classification techniques can be used to build the prediction and clas-

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 March 2022 doi:10.20944/preprints202203.0087.v1

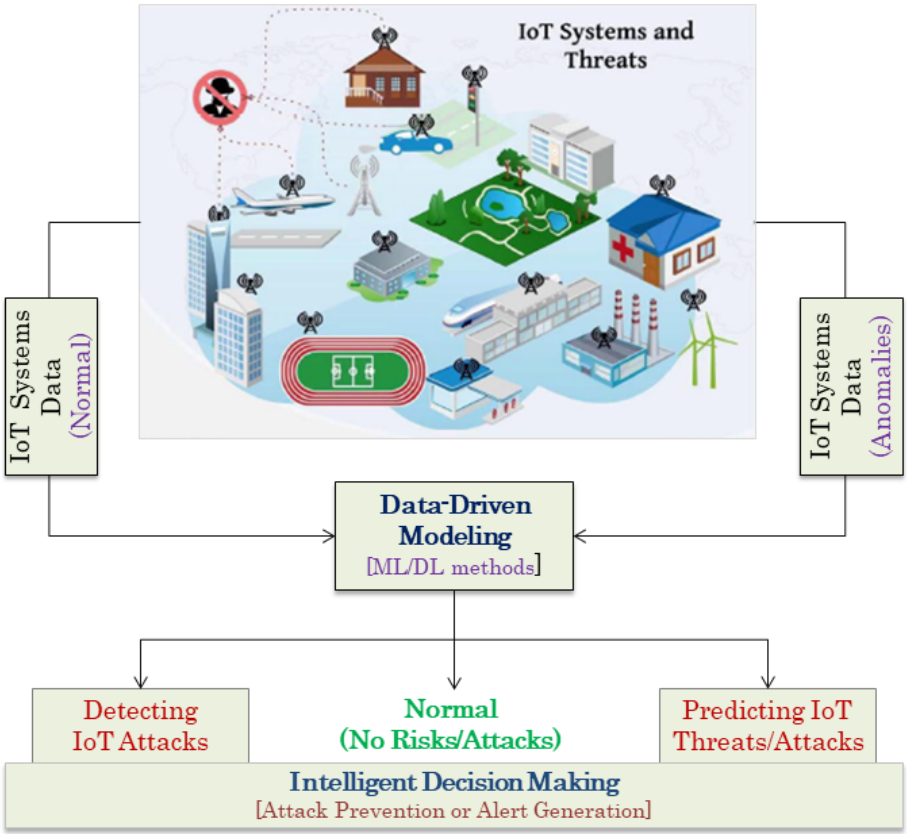

Fig. 4: Illustration of the potential role of the machine learning and deep learning methods while building data-driven model for IoT security intelligence.

sification model [123] utilizing the relevant data in the domain of IoT security, while the regression technique is mainly the impact of the model [62] through determining the predictor strength, time-series causes, or the effect of the relations, considering the security attributes and the outcome.

4.2 Clustering Techniques

In machine learning, clustering is another popular task for analyzing IoT security data, which is considered unsupervised learning. It can cluster or create groups of a set of data points based on the measurement for similarity and dissimilarity in the security data generated by IoT devices from diverse sources. Thus, clustering could contribute to the discovery of hidden patterns and structures in data, allowing for the detection of abnormalities or attacks in IoT. Partition, Hierarchy, Fuzzy Theory, Distribution, Density, Graph Theory, Grid, Fractal Theory, and other perspectives can be used to cluster data. [148]. K-means [90], K-medoids [107], single linkage [131], complete linkage [132], agglomerative clustering, bottom-up BOTS [118], DBSCAN, OPTICS, Gaussian Mixture Model [148], are the popular concepts of clustering algorithms. These clustering techniques can be used to solve various IoT security problems. For instance, the k-Means algorithm is used in profiling the abnormal behavior of IoT devices [80]. A dynamic threshold-based approach can be used to detect the outlier or noisy instances in data [110]. A fuzzy clustering approach is used in IoT intrusion detection [86]. To analyze system log data for cybersecurity applications clustering approaches are useful to extract useful insights or knowledge [77]. Thus, by uncovering hidden patterns and structures in IoT security data, the clustering techniques can play a significant role through measuring the behavioral similarity or dissimilarity, to solve various security problems, such as outlier detection, anomaly detection, signature extraction, fraud detection, cyber-attack detection, etc. in the domain of IoT.

4.3 Rule-based Techniques

A rule-based system extracting rules from data, can mimic human intelligence, which is a system that ap-

plies rules to make an intelligent decision [111]. Thus, rule-based systems can play a significant role in IoT security through learning security or policy rules from data [119]. Association rule learning is a prominent method of discovering associations or rules among a set of available attributes in a security dataset in the field of machine learning [20]. Several types of association rules have been proposed in the area, such as frequent pattern based [21] [60], [88], tree-based [55], logic-based [44], fuzzy-rules [138], belief rule [156] etc. The rule learning techniques such as AIS [20], Apriori [21], Apriori-TID and Apriori-Hybrid [21], FP-Tree [55], Eclat [152], RARM [40] exist that can be used to solve IoT security problems and intelligent decision making. For instance, an association rule-mining algorithm-based network intrusion detection has been presented in [125]. Moreover, fuzzy association rules are used to build a rule-based intrusion detection system [138]. To analyze IoT malware activities, an FP-tree association rule-based study has been conducted in [100].

Although a rule-based approach is easy to adopt, it has high time complexity because of generating a huge number of associations or frequent patterns depending on the support and confidence values, and consequently, make the model complex [21] [137]. An effective association model could minimize this issue. For instance, in our earlier paper, Sarker et al. [121], we present a rule learning approach that effectively discovers the association rules that are non-redundant and reliable, and thus could play a significant role in the domain of IoT security as well. The rules can also be used to build knowledge-based systems or rule-based expert systems [120] to solve more complex security problems in IoT. Each of these systems consists of a set of policy rules to define the scope of what kind of activities should be allowed on a network, where each rule is either explicitly allow or deny. Even new zero-day attacks are blocked that utilize rule-driven controls or filters security policy monitoring.

4.4 Security Feature Optimization and Principal Component Analysis

For an effective IoT security system based on the machine learning approach, security feature engineering and optimization are considered key issues in IoT cyber threat landscape. The reason is that the security features and corresponding IoT data directly influence the machine learning-based security models and thus a data dimensionality reduction technique is important [102]. Feature engineering is the general term used to construct and modify security attributes or variables to effectively develop machine learning-based security models [114]. As today's IoT security datasets may include features that are less relevant or not at all important, effectively modeling cyber attacks or abnormalities is challenging. A security model with these qualities can lead to several issues, including excessive variance, overfitting, high computing cost and model preparation, and a lack of generalization, all of which can degrade prediction accuracy [115]. Thus an optimal number of security features selection based on their impact or importance [115] could minimize such issues while building an IoT security model with high dimensional data sets. Several approaches such as wrapper methods such as recursive feature elimination, forward feature selection; filter methods such as Pearson correlation, chi-squared test, analysis of variance test; or embedded methods such as regularization, Lasso, Ridge, or ElasticNet, tree-based feature importance [114] can be used. Along with feature selection, principal component analysis (PCA) [114] is utilized to generate new brand components that capture the majority of the relevant information. While developing a machine learning-based security modeling, these new brand components may help handle large dimensions of IoT security data, such as IoT network traffic anomaly detection [58].

4.5 Deep Neural Network Learning-based Approaches

Deep learning (DL) is a subset of machine learning that developed from the Artificial Neural Network (ANN), which offers a computational architecture for learning from data by combining multiple processing levels, such as input, hidden, and output layers, into a single network [54]. Thus deep learning techniques are also capable to learn from IoT security data through these layers, and known as hierarchical learning methods because of their knowledge capturing nature in deep architecture. Deep learning outperforms typical machine learning algorithms in a variety of situations, especially when learning from huge security datasets. Several IoT-based devices and their applications or systems produce a large amount of security data in the IoT environment; consequently, depending on the datasets, DL approaches may deliver better results. Depending on the characteristics and nature of the security data, different deep learning architectures such as Multi-layer perceptron (MLP), convolutional neural networks (CNN), recurrent neural networks (RNN), deep belief networks (DBN), or hybrid networks can be used to build IoT security modeling [113] [147], as discussed below.

– *Multilayer perceptron (MLP):* A multilayer perceptron (MLP), often known as a feedforward artificial neural network, is the fundamental building block

Table 1: A summary of using machine learning techniques in IoT security.

Used Technique	Purpose	References
SVM	profiling abnormal behavior of IoT devices	[80]
SVM	detecting android malware for reliable IoT services	[53]
RF	to detect anomalies	[39], [28]
RF	to detect denial of service attack	[41]
RF	IoT intrusion detection service	[106], [96]
NBC	to detect anomalies	[135]
LR	to detect malicious IoT botnets	[104], [31]
LR	to predict the impact of an attack, such as worms, viruses, or other malicious software	[62]
Regression Regularization	to handle high dimensionality of IoT security data, to enhance security attacks analysis	[52]
k-Means	profiling the abnormal behavior of IoT devices	[80]
fuzzy cluster	IoT intrusion detection	[86]
FP-tree	To analyze IoT malware activities	[100]
PCA	handling high dimensions of IoT security data, IoT network traffic anomaly detection	[58]
MLP	detecting malicious botnet traffic from IoT devices	[63]
MLP	a security threat analysis of the IoT	[59]
CNN	denial-of-service attacks detection in IoT Networks	[134]
CNN	android malware detection	[92]
multi-CNN	intrusion detection	[83]
LSTM-RNN	to detect and classify the malicious apps	[142]
LSTM+CNN	to detect and mitigate phishing and Botnet attack across multiple IoT devices	[101]

of deep learning algorithms. A typical MLP comprises an input layer, one or more hidden layers of an output layer, and one or more output layers. Each node in one layer is linked to a certain weight in the next layer via a chain of connections. The weight values are updated internally by MLP as the model is being developed via the backpropagation process. Such MLP network is used to build an intrusion detection model utilizing NSL-KDD dataset [45], malware analysis [66], to generate explanation in IoT environments [47], detecting malicious botnet traffic from IoT devices [63]. To perform a security threat analysis of the IoT, MLP based network is used in [59], where the model classifies the network data as normal or as under attack.

– *Convolutional neural networks (CNN):* The CNN [79] improves on the traditional ANN design, which includes convolutional layers, pooling layers, and fully connected layers. Each of these levels takes into account optimized parameters, reducing the complexity. CNN also employs a dropout to address the problem of overfitting, which can occur in the MLP network. It is commonly utilized in numerous areas such as natural language processing, audio analysis, picture processing, and other autocorrelated data in recent years because it takes advantage of the two-dimensional (2D) structure of the input data. CNN may also be used in the area of Internet of Things (IoT) security. Using a CNN-based deep learning model for intrusion detection, such as denial-of-service (DoS) attacks [134], to detect malware [150], android malware detection [92]. Furthermore, an intrusion detection model based on multi-CNN fusion may be utilized [83]. In the IoT environment, some innovative CNN-based deep learning models with lightweight architecture could reduce computations and provide higher performance with constrained resources.

– *Recurrent neural network (RNN):* A recurrent neural network (RNN) is another kind of ANN in which the connections between nodes form a directed graph along a temporal sequence. The RNN model, which is derived from feedforward neural networks, can process variable-length sequences of inputs by using their internal state, or memory. It is possible to use the RNN model for IoT security, as well as natural language processing and voice recognition, because of its capacity to effectively handle sequential data. Internet of Things (IoT) devices produce a significant quantity of sequential data from several sources, such as network traffic flows, time-dependent data, and so on. When the behavior patterns of the threat are time-dependent, using recurrent connections can help neural networks detect security concerns. The reason for this is that it contains a characteristic called Long Short Term

Memory (LSTM) that allows it to retain prior inputs, making it a particularly helpful model for time series prediction. Such an LSTM model-based recurrent network can be used for several purposes in the domain of security, such as intrusion detection [70], to detect and classify the malicious apps [142] etc.

In addition to these deep learning models, hybrid network models, such as the ensemble of classifiers, LSTM network with the combination of CNN, can also be applied for detecting IoT attacks, such as malware detection [150], phishing, and Botnet attack detection and mitigation across multiple IoT devices [101]. Other deep learning models, such as a deep belief network (DBN) based security model, may be used to IoT security[30] [108]. In our earlier paper Sarker et al. [113], we have explored different types of deep learning techniques with their taxonomy dividing into discriminative for supervised tasks, generative for unsupervised tasks, and hybrid techniques that can be used according to the data characteristics. In Table 1, we have summarized how various machine learning methods including deep learning are used to solve various security issues in the domain of IoT. Thus, we can infer that the above-mentioned machine or deep learning techniques, as well as their variants or modified lightweight approaches, can play a significant role in data-driven security analytics in the IoT environment.

5 Research Issues and Directions

Our study on the machine and deep learning-based security solutions raises concerns in the area of IoT security. As a consequence, in this section, we describe and analyze the challenges that have been encountered, as well as possible research possibilities and future directions for securing IoT networks and systems.

The effectiveness and efficiency of a machine learning or deep learning-based IoT security solution are primarily determined by the nature and features of the data, as well as the learning algorithms' performance. There are a variety of machine and deep learning techniques available to evaluate data and extract insights, as detailed in Section 4. As a result, choosing an appropriate learning algorithm for the intended application in IoT security can be challenging. The reason behind this is that based on the data qualities, the results of different learning algorithms may vary [123] [114]. If the wrong learning algorithm is chosen, unexpected results may occur, resulting in a loss of effort as well as the model's efficacy and accuracy. In the same way, unnecessary IoT security data might result in garbage processing and inaccurate outcomes. If the IoT data is bad, such as non-representative, poor-quality, irrelevant attributes, or an inadequate quantity for training, machine or deep learning security models may become worthless or yield reduced accuracy, or they may even become worthless. Future research opportunities and directions in the topic of IoT security include the following:

- In the world of IoT, gathering security data is not easy. The dynamic characteristics of IoT, such as heterogeneity, covered briefly in Section 2, allows for the generation of massive amounts of data at a high frequency from various domains. Collecting security data in the IoT is not a straightforward endeavor. For further analysis, it is critical to gather and manage relevant IoT-generated data for target applications, such as security in smart city applications, to facilitate further investigation. As a result, while working with IoT-generated data, a more in-depth analysis of data gathering methods is required.
- Many ambiguous values, missing values, outliers, and erroneous data may be discovered in historical or raw IoT security data. The machine learning or deep learning methods presented in Section 4 in IoT security have a significant impact on data quality and training availability, and hence on the IoT security model. As a result, cleaning and preprocessing the various security data generated in an IoT environment is a challenging task. To effectively apply learning algorithms in the domain of IoT security, improvement of current methods or the development of new data preparation techniques are expected.
- It is critical for an effective IoT security solution to consider the constraints or capabilities of IoT devices and systems where learning-based security models are utilized, as addressed briefly in Section 4. As a consequence, there should be a trade-off between security and device capabilities in terms of data storage, computing, data processing, and decision-making, and communication resources. Therefore, an in-depth investigation is required to discover the most appropriate machine or deep learning methods.
- Because of the huge amount of redundant processing, the classical learning techniques outlined in Section 4 may not be directly applicable to IoT devices in various circumstances. The association rule learning technique [21], for example, in a rule-based system may extract redundant generation from IoT security data, making the decision-making process complex and ineffective [121]. As a result, a better understanding of the benefits and limitations of existing learning methods is required, making the de-

velopment of new lightweight algorithms or methods for IoT devices a challenging task.
– Compared to older patterns, a recent malicious behavioral trend is more likely to be intriguing and significant for forecasting or detecting attacks in IoT security. As a result, rather than considering conventional data analysis, the idea of recency analysis, i.e. current pattern-based extracted insight or knowledge [116], may be more appropriate in a variety of situations. Thus another difficult challenge is to propose new lightweight solutions for IoT devices that take into consideration current data patterns, and eventually to construct a recency-based IoT security model.

In the above, within the scope of our learning-based study in the area of IoT security, we have reviewed and explored several research directions. Besides, incorporating context-aware computing in IoT security could be another potential research direction. In the context of IoT computing, context-awareness typically refers to the capability of a system to gather its surrounding information and adapt behaviors accordingly. A wider sense of security contextual knowledge [109] [120] can then be used to assess whether a suspicious behavior occurs or not, such as temporal, spatial, individuality, dependence, activity, or relationship between events or interactions, etc. An approach might allow an end-user, for example, to browse the network from within the office, but refuse access if the end-user tries to connect to public Wi-Fi. The design of adaptive security solutions based on the principle of context-aware computing may therefore be another research problem in the IoT security area.

6 Conclusion

In this paper, we have presented a comprehensive overview of the literature on IoT security intelligence, which covers the IoT paradigm, IoT-based smart environments, related security concerns with machine learning solutions. We have also reviewed the recent studies for IoT security to make the position of this paper. A thorough study on the IoT system architectures with its layer-wise cyber-attacks that are needed to detect and protect the IoT devices and systems. As a consequence, we have briefly explored how various types of machine and deep learning approaches might be employed for security solutions in the IoT context. Depending on the data characteristics, a successful IoT security model should have the appropriate machine or deep learning modeling. Before the system can assist in making intelligent decisions, an effective learning algorithm must be developed using the obtained IoT security knowledge connected with the target application.

Finally, we have discussed and addressed the issues that have arisen, as well as potential research directions and future approaches that are based on learning techniques. As a result, the challenges that have been highlighted present promising research possibilities in the field, which must be addressed with effective solutions to enhance IoT security over time. Overall, we believe that our study on machine and deep learning-based security solutions points in the direction of a promising path and can be used as a reference guide for future IoT security research and implementations by academic and industry experts.

Competing interests

The authors declare that they have no competing interests.

References

1. Alexa top sites. available online: https://aws.amazon.com/alexa-top-sites/ (accessed on 20 october 2019).
2. Bambenek consulting—master feeds. available online: http://osint.bambenekconsulting.com/feeds/ (accessed on 20 october 2019).
3. Caida anonymized internet traces 2008 dataset. http://www. caida.org/data/passive/passive-2008-dataset.xml/ (accessed on 20 october 2019).
4. Caida ddos attack 2007 dataset. http://www.caida.org/data/ passive/ddos-20070804-dataset.xml/ (accessed on 20 october 2019).
5. Canadian institute of cybersecurity, university of new brunswick, iscx dataset, url http://www.unb.ca/cic/datasets/index.html/ (accessed on 20 october 2019).
6. Cic-ddos2019 [online]. available: https://www.unb.ca/cic/datasets/ddos-2019.html/ (accessed on 28 march 2020).
7. Comodo. available online: https://www.comodo.com/home/internet-security/updates/vdp/database. php (accessed on 20 october 2019).
8. Contagio. available online: http://contagiodump.blogspot.com/ (accessed on 20 october 2019).
9. Cse-cic-ids2018 [online]. available: https://www.unb.ca/cic/ datasets/ids-2018.html/ (accessed on 20 october 2019).
10. The ctu-13 dataset. available online: https://stratosphereips.org/category/datasets-ctu13 (accessed on 20 october 2019).
11. Dgarchive. available online: https://dgarchive.caad.fkie.fraunhofer.de/site/ (accessed on 20 october 2019).
12. Enronspam. available online: https://labs-repos.iit.demokritos.gr/skel/i-config/downloads/enron-spam/ (accessed on 20 october 2019).

13. The honeynet project. http://www.honeynet.org/chapters/france/ (accessed on 20 october 2019).
14. Isot botnet dataset. https://www.uvic.ca/engineering/ece/isot/datasets/index.php/ (accessed on 20 october 2019).
15. Lingspam. available online: https://labs-repos.iit.demokritos.gr/skel/i-config/downloads/lingspampublic.tar.gz/ (accessed on 20 october 2019).
16. Microsoft malware classification (big 2015). available online: http://arxiv.org/abs/1802.10135/ (accessed on 20 october 2019).
17. Spamassassin. available online: http://www.spamassassin.org/publiccorpus/ (accessed on 20 october 2019).
18. Virusshare. available online: http://virusshare.com/ (accessed on 20 october 2019).
19. Virustotal. available online: https://virustotal.com/ (accessed on 20 october 2019).
20. Rakesh Agrawal, Tomasz Imieliński, and Arun Swami. Mining association rules between sets of items in large databases. In *ACM SIGMOD Record*, volume 22, pages 207–216. ACM, 1993.
21. Rakesh Agrawal, Ramakrishnan Srikant, et al. Fast algorithms for mining association rules. In *Proc. 20th int. conf. very large data bases, VLDB*, volume 1215, pages 487–499, 1994.
22. David W Aha, Dennis Kibler, and Marc K Albert. Instance-based learning algorithms. *Machine learning*, 6(1):37–66, 1991.
23. Ejaz Ahmed, Ibrar Yaqoob, Abdullah Gani, Muhammad Imran, and Mohsen Guizani. Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges. *IEEE Wireless Communications*, 23(5):10–16, 2016.
24. Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, 17(4):2347–2376, 2015.
25. Mohammed Ali Al-Garadi, Amr Mohamed, Abdulla Al-Ali, Xiaojiang Du, Ihsan Ali, and Mohsen Guizani. A survey of machine and deep learning methods for internet of things (iot) security. *IEEE Communications Surveys & Tutorials*, 2020.
26. Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, and Faiz Alotaibi. Internet of things security: A survey. *Journal of Network and Computer Applications*, 88:10–28, 2017.
27. Mamoun Alazab, Sitalakshmi Venkatraman, Paul Watters, Moutaz Alazab, et al. Zero-day malware detection based on supervised learning algorithms of api call signatures. 2010.
28. Ibrahim Alrashdi, Ali Alqazzaz, Esam Aloufi, Raed Alharthi, Mohamed Zohdy, and Hua Ming. Ad-iot: Anomaly detection of iot cyberattacks in smart city using machine learning. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0305–0310. IEEE, 2019.
29. Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.
30. Nagaraj Balakrishnan, Arunkumar Rajendran, Danilo Pelusi, and Vijayakumar Ponnusamy. Deep belief network enhanced intrusion detection system to prevent security breach in the internet of things. *Internet of Things*, page 100112, 2019.
31. Rohan Bapat, Abhijith Mandya, Xinyang Liu, Brendan Abraham, Donald E Brown, Hyojung Kang, and Malathi Veeraraghavan. Identifying malicious botnet traffic using logistic regression. In *2018 Systems and Information Engineering Design Symposium (SIEDS)*, pages 266–271. IEEE, 2018.
32. Jennifer Bélissent et al. Getting clever about smart cities: New opportunities require new business models. *Cambridge, Massachusetts, USA*, 193:244–77, 2010.
33. Leyla Bilge and Tudor Dumitraş. Before we knew it: an empirical study of zero-day attacks in the real world. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 833–844. ACM, 2012.
34. Miodrag Bolic, Majed Rostamian, and Petar M Djuric. Proximity detection with rfid: A step toward the internet of things. *IEEE Pervasive Computing*, 14(2):70–76, 2015.
35. Flavio Bonomi, Rodolfo Milito, Preethi Natarajan, and Jiang Zhu. Fog computing: A platform for internet of things and analytics. In *Big data and internet of things: A roadmap for smart environments*, pages 169–186. Springer, 2014.
36. Joseph Bradley, Jeff Loucks, James Macaulay, and Andy Noronha. Internet of everything (ioe) value index. *White Paper CISCO and/or its affiliates*, 2013.
37. Leo Breiman. Random forests. *Machine learning*, 45(1):5–32, 2001.
38. Nadia Chaabouni, Mohamed Mosbah, Akka Zemmari, Cyrille Sauvignac, and Parvez Faruki. Network intrusion detection for iot security based on learning techniques. *IEEE Communications Surveys & Tutorials*, 21(3):2671–2701, 2019.
39. Yaping Chang, Wei Li, and Zhongming Yang. Network intrusion detection based on random forest and support vector machine. In *2017 IEEE international conference on computational science and engineering (CSE) and IEEE international conference on embedded and ubiquitous computing (EUC)*, volume 1, pages 635–638. IEEE, 2017.
40. Amitabha Das, Wee-Keong Ng, and Yew-Kwong Woon. Rapid association rule mining. In *Proceedings of the tenth international conference on Information and knowledge management*, pages 474–481. ACM, 2001.
41. Rohan Doshi, Noah Apthorpe, and Nick Feamster. Machine learning ddos detection for consumer internet of things devices. In *2018 IEEE Security and Privacy Workshops (SPW)*, pages 29–35. IEEE, 2018.
42. Sumeet Dua and Xian Du. *Data mining and machine learning in cybersecurity*. CRC press, 2016.
43. Mohamed Faisal Elrawy, Ali Ismail Awad, and Hesham FA Hamed. Intrusion detection systems for iot-based smart environments: a survey. *Journal of Cloud Computing*, 7(1):21, 2018.
44. Peter A Flach and Nicolas Lachiche. Confirmation-guided discovery of first-order rules with tertius. *Machine Learning*, 42(1-2):61–95, 2001.
45. Felipe De Almeida Florencio, Edward David Moreno Ordonez, Hendrik Teixeira Macedo, Ricardo José Paiva De Britto Salgueiro, Filipe Barreto Do Nascimento, and Flavio Arthur Oliveira Santos. Intrusion detection via mlp neural network using an arduino embedded system. In *2018 VIII Brazilian Symposium on Computing Systems Engineering (SBESC)*, pages 190–195. IEEE, 2018.
46. Yoav Freund, Robert E Schapire, et al. Experiments with a new boosting algorithm. In *Icml*, volume 96, pages 148–156. Citeseer, 1996.

47. Iván García-Magariño, Rajarajan Muttukrishnan, and Jaime Lloret. Human-centric ai for trustworthy iot systems with explainable multilayer perceptrons. *IEEE Access*, 7:125562–125574, 2019.
48. Joshua Glasser and Brian Lindauer. Bridging the gap: A pragmatic approach to generating insider threat data. In *2013 IEEE Security and Privacy Workshops*, pages 98–104. IEEE, 2013.
49. Margaret Gratian, Sruthi Bandi, Michel Cukier, Josiah Dykstra, and Amy Ginther. Correlating human traits and cyber security behavior intentions. *computers & security*, 73:345–358, 2018.
50. Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. *Future generation computer systems*, 29(7):1645–1660, 2013.
51. Brij B Gupta, Aakanksha Tewari, Ankit Kumar Jain, and Dharma P Agrawal. Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, 28(12):3629–3654, 2017.
52. Desta Haileselassie Hagos, Anis Yazidi, Øivind Kure, and Paal E Engelstad. Enhancing security attacks analysis using regularized machine learning techniques. In *2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)*, pages 909–918. IEEE, 2017.
53. Hyo-Sik Ham, Hwan-Hee Kim, Myung-Sup Kim, and Mi-Jung Choi. Linear svm-based android malware detection for reliable iot services. *Journal of Applied Mathematics*, 2014, 2014.
54. Jiawei Han, Jian Pei, and Micheline Kamber. *Data mining: concepts and techniques*. Elsevier, 2011.
55. Jiawei Han, Jian Pei, and Yiwen Yin. Mining frequent patterns without candidate generation. In *ACM Sigmod Record*, volume 29, pages 1–12. ACM, 2000.
56. Wan Haslina Hassan et al. Current research on internet of things (iot) security: A survey. *Computer networks*, 148:283–294, 2019.
57. Vikas Hassija, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal, and Biplab Sikdar. A survey on iot security: application areas, security threats, and solution architectures. *IEEE Access*, 7:82721–82743, 2019.
58. Dang Hai Hoang and Ha Duong Nguyen. A pca-based method for iot network traffic anomaly detection. In *2018 20th International Conference on Advanced Communication Technology (ICACT)*, pages 381–386. IEEE, 2018.
59. Elike Hodo, Xavier Bellekens, Andrew Hamilton, Pierre-Louis Dubouilh, Ephraim Iorkyase, Christos Tachtatzis, and Robert Atkinson. Threat analysis of iot networks using artificial neural network intrusion detection system. In *2016 International Symposium on Networks, Computers and Communications (ISNCC)*, pages 1–6. IEEE, 2016.
60. Maurice Houtsma and Arun Swami. Set-oriented mining for association rules in relational databases. In *Data Engineering, 1995. Proceedings of the Eleventh International Conference on*, pages 25–33. IEEE, 1995.
61. Fatima Hussain, Rasheed Hussain, Syed Ali Hassan, and Ekram Hossain. Machine learning in iot security: current solutions and future challenges. *IEEE Communications Surveys & Tutorials*, 2020.
62. Venkatesh Jaganathan, Priyesh Cherurveettil, and Premapriya Muthu Sivashanmugam. Using a prediction model to manage cyber security threats. *The Scientific World Journal*, 2015, 2015.
63. Yousra Javed and Navid Rajabi. Multi-layer perceptron artificial neural network based iot botnet traffic classification. In *Proceedings of the Future Technologies Conference*, pages 973–984. Springer, 2019.
64. Xuyang Jing, Zheng Yan, Xueqin Jiang, and Witold Pedrycz. Network traffic fusion and analysis against ddos flooding attacks with a novel reversible sketch. *Information Fusion*, 51:100–113, 2019.
65. George H John and Pat Langley. Estimating continuous distributions in bayesian classifiers. In *Proceedings of the Eleventh conference on Uncertainty in artificial intelligence*, pages 338–345. Morgan Kaufmann Publishers Inc., 1995.
66. ElMouatez Billah Karbab, Mourad Debbabi, Abdelouahid Derhab, and Djedjiga Mouheb. Maldozer: Automatic framework for android malware detection using deep learning. *Digital Investigation*, 24:S48–S59, 2018.
67. S. Sathiya Keerthi, Shirish Krishnaj Shevade, Chiranjib Bhattacharyya, and Karuturi Radha Krishna Murthy. Improvements to platt's smo algorithm for svm classifier design. *Neural computation*, 13(3):637–649, 2001.
68. Minhaj Ahmad Khan and Khaled Salah. Iot security: Review, blockchain solutions, and open challenges. *Future generation computer systems*, 82:395–411, 2018.
69. R Khan, S Khan, R Zaheer, and S Khan. Future internet: The internet of things architecture, possible applications and key challenges in: 2012 10th international conference on frontiers of information technology, 257–260. *IEEE, Islamabad*, 10, 2012.
70. Jihyun Kim, Jaehyun Kim, Huong Le Thi Thu, and Howon Kim. Long short term memory recurrent neural network classifier for intrusion detection. In *2016 International Conference on Platform Technology and Service (PlatCon)*, pages 1–5. IEEE, 2016.
71. Nickolaos Koroniotis, Nour Moustafa, Elena Sitnikova, and Benjamin Turnbull. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. *Future Generation Computer Systems*, 100:779–796, 2019.
72. Srdjan Krčo, Boris Pokrić, and Francois Carrez. Designing iot architecture (s): A european perspective. In *2014 IEEE World Forum on Internet of Things (WF-IoT)*, pages 79–84. IEEE, 2014.
73. Dennis Kügler. "man in the middle" attacks on bluetooth. In *International Conference on Financial Cryptography*, pages 149–161. Springer, 2003.
74. Rajesh Kumar, Zhang Xiaosong, Riaz Ullah Khan, Jay Kumar, and Ijaz Ahad. Effective and explainable detection of android malware based on machine learning algorithms. In *Proceedings of the 2018 International Conference on Computing and Artificial Intelligence*, pages 35–40. ACM, 2018.
75. Sathish Alampalayam Kumar, Tyler Vealey, and Harshit Srivastava. Security in internet of things: Challenges, solutions and future directions. In *2016 49th Hawaii International Conference on System Sciences (HICSS)*, pages 5772–5781. IEEE, 2016.
76. Mohammed Lalou, Hamamache Kheddouci, and Salim Hariri. Identifying the cyber attack origin with partial observation: a linear regression based approach. In *2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS* W)*, pages 329–333. IEEE, 2017.
77. Max Landauer, Florian Skopik, Markus Wurzenberger, and Andreas Rauber. System log clustering approaches for cyber security applications: A survey. *Computers & Security*, 92:101739, 2020.

78. Saskia Le Cessie and Johannes C Van Houwelingen. Ridge estimators in logistic regression. *Journal of the Royal Statistical Society: Series C (Applied Statistics)*, 41(1):191–201, 1992.
79. Yann LeCun, Léon Bottou, Yoshua Bengio, and Patrick Haffner. Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, 86(11):2278–2324, 1998.
80. Soo-Yeon Lee, Sa-rang Wi, Eunil Seo, Jun-Kwon Jung, and Tai-Myoung Chung. Profiot: Abnormal behavior profiling (abp) of iot devices based on a machine learning approach. In *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, pages 1–6. IEEE, 2017.
81. Shancang Li and Li Da Xu. *Securing the internet of things*. Syngress, 2017.
82. Shancang Li, Li Da Xu, and Shanshan Zhao. The internet of things: a survey. *Information Systems Frontiers*, 17(2):243–259, 2015.
83. Yanmiao Li, Yingying Xu, Zhi Liu, Haixia Hou, Yushuo Zheng, Yang Xin, Yuefeng Zhao, and Lizhen Cui. Robust detection for network intrusion of industrial iot based on multi-cnn fusion. *Measurement*, 154:107450, 2020.
84. Brian Lindauer, Joshua Glasser, Mitch Rosen, Kurt C Wallnau, and L ExactData. Generating test data for insider threat detectors. *JoWUA*, 5(2):80–94, 2014.
85. Richard P Lippmann, David J Fried, Isaac Graf, Joshua W Haines, Kristopher R Kendall, David McClung, Dan Weber, Seth E Webster, Dan Wyschogrod, Robert K Cunningham, et al. Evaluating intrusion detection systems: The 1998 darpa off-line intrusion detection evaluation. In *Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00*, volume 2, pages 12–26. IEEE, 2000.
86. Liqun Liu, Bing Xu, Xiaoping Zhang, and Xianjun Wu. An intrusion detection method for internet of things based on suppressed fuzzy clustering. *EURASIP Journal on Wireless Communications and Networking*, 2018(1):113, 2018.
87. Yang Lu and Li Da Xu. Internet of things (iot) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, 6(2):2103–2115, 2018.
88. Bing Liu Wynne Hsu Yiming Ma. Integrating classification and association rule mining. In *Proceedings of the fourth international conference on knowledge discovery and data mining*, 1998.
89. Zheng Ma, Ming Xiao, Yue Xiao, Zhibo Pang, H Vincent Poor, and Branka Vucetic. High-reliability and low-latency wireless communication for internet of things: challenges, fundamentals, and enabling technologies. *IEEE Internet of Things Journal*, 6(5):7946–7970, 2019.
90. James MacQueen. Some methods for classification and analysis of multivariate observations. In *Fifth Berkeley symposium on mathematical statistics and probability*, volume 1, 1967.
91. Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, and Imran Zualkernan. Internet of things (iot) security: Current status, challenges and prospective measures. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 336–341. IEEE, 2015.
92. Niall McLaughlin, Jesus Martinez del Rincon, Boo-Joong Kang, Suleiman Yerima, Paul Miller, Sakir Sezer, Yeganeh Safaei, Erik Trickel, Ziming Zhao, Adam Doupé, et al. Deep android malware detection. In *Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy*, pages 301–308, 2017.
93. Roberto Minerva, Abyi Biru, and Domenico Rotondi. Towards a definition of the internet of things (iot). *IEEE Internet Initiative*, 1(1):1–86, 2015.
94. Daniel Minoli and Benedict Occhiogrosso. Blockchain mechanisms for iot security. *Internet of Things*, 1:1–13, 2018.
95. Sophia Moganedi. Undetectable data breach in iot: Healthcare data at risk. In *ECCWS 2018 17th European Conference on Cyber Warfare and Security V2*, page 296. Academic Conferences and publishing limited, 2018.
96. TagyAldeen Mohamed, Takanobu Otsuka, and Takayuki Ito. Towards machine learning based iot intrusion detection service. In *International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems*, pages 580–585. Springer, 2018.
97. Nour Moustafa and Jill Slay. Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set). In *2015 military communications and information systems conference (MilCIS)*, pages 1–6. IEEE, 2015.
98. Farooq Muhammad, Waseem Anjum, and Khairi Sadia Mazhar. A critical analysis on the security concerns of internet of things (iot). *International Journal of Computer Applications*, 111(7):1–6, 2015.
99. Nataliia Neshenko, Elias Bou-Harb, Jorge Crichigno, Georges Kaddoum, and Nasir Ghani. Demystifying iot security: an exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations. *IEEE Communications Surveys & Tutorials*, 21(3):2702–2733, 2019.
100. Seiichi Ozawa, Tao Ban, Naoki Hashimoto, Junji Nakazato, and Jumpei Shimamura. A study of iot malware activities using association rule learning for darknet sensor data. *International Journal of Information Security*, 19(1):83–92, 2020.
101. Gonzalo De La Torre Parra, Paul Rad, Kim-Kwang Raymond Choo, and Nicole Beebe. Detecting internet of things attacks using distributed deep learning. *Journal of Network and Computer Applications*, page 102662, 2020.
102. Morteza Safaei Pour, Elias Bou-Harb, Kavita Varma, Nataliia Neshenko, Dimitris A Pados, and Kim-Kwang Raymond Choo. Comprehending the iot cyber threat landscape: A data dimensionality reduction technique to infer and characterize internet-scale iot probing campaigns. *Digital Investigation*, 28:S40–S49, 2019.
103. Rifkie Primartha and Bayu Adhi Tama. Anomaly detection using random forest: A performance revisited. In *2017 International conference on data and software engineering (ICoDSE)*, pages 1–6. IEEE, 2017.
104. Anton O Prokofiev, Yulia S Smirnova, and Vasiliy A Surov. A method to detect internet of things botnets. In *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pages 105–108. IEEE, 2018.
105. J. Ross Quinlan. C4.5: Programs for machine learning. *Machine Learning*, 1993.
106. Paulo Angelo Alves Resende and André Costa Drummond. A survey of random forest based methods for intrusion detection systems. *ACM Computing Surveys (CSUR)*, 51(3):1–36, 2018.
107. Lior Rokach. A survey of clustering algorithms. In *Data Mining and Knowledge Discovery Handbook*, pages 269–298. Springer, 2010.

108. Ahmed Saeed, Ali Ahmadinia, Abbas Javed, and Hadi Larijani. Intelligent intrusion detection in low-power iots. *ACM Transactions on Internet Technology (TOIT)*, 16(4):1–25, 2016.
109. Iqbal H Sarker. Context-aware rule learning from smartphone data: survey, challenges and future directions. *Journal of Big Data*, 6(1):95, 2019.
110. Iqbal H Sarker. A machine learning based robust prediction model for real-life mobile phone data. *Internet of Things*, 5:180–193, 2019.
111. Iqbal H Sarker. Data science and analytics: An overview from data-driven smart computing, decision-making and applications perspective. *SN Computer Science*, 2021.
112. Iqbal H Sarker. Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective. *SN Computer Science*, 2(3):1–16, 2021.
113. Iqbal H Sarker. Deep learning: A comprehensive overview on techniques, taxonomy, applications and research directions. *SN Computer Science*, 2021.
114. Iqbal H Sarker. Machine learning: Algorithms, real-world applications and research directions. *SN Computer Science*, 2(3):1–21, 2021.
115. Iqbal H Sarker, Yoosef B Abushark, Fawaz Alsolami, and Asif Irshad Khan. Intrudtree: A machine learning based cyber security intrusion detection model. *Symmetry*, 12(5):754, 2020.
116. Iqbal H Sarker, Alan Colman, and Jun Han. Recencyminer: mining recency-based personalized behavior from contextual smartphone data. *Journal of Big Data*, 6(1):49, 2019.
117. Iqbal H Sarker, Alan Colman, Jun Han, Asif Irshad Khan, Yoosef B Abushark, and Khaled Salah. Behavdt: a behavioral decision tree learning to build user-centric context-aware predictive model. *Mobile Networks and Applications*, 25(3):1151–1161, 2020.
118. Iqbal H Sarker, Alan Colman, Muhammad Ashad Kabir, and Jun Han. Individualized time-series segmentation for mining mobile phone user behavior. *The Computer Journal*, 61(3):349–368, 2018.
119. Iqbal H Sarker, Md Hasan Furhad, and Raza Nowrozy. Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science*, 2(3):1–18, 2021.
120. Iqbal H Sarker, Mohammed Moshiul Hoque, Md Kafil Uddin, and Tawfeeq Alsanoosy. Mobile data science and intelligent apps: Concepts, ai-based modeling and research directions. *Mobile Networks and Applications*, pages 1–19, 2020.
121. Iqbal H Sarker and ASM Kayes. Abc-ruleminer: User behavioral rule-based machine learning method for context-aware intelligent services. *Journal of Network and Computer Applications*, 168:102762, 2020.
122. Iqbal H Sarker, ASM Kayes, Shahriar Badsha, Hamed Alqahtani, Paul Watters, and Alex Ng. Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data*, 7(1):1–29, 2020.
123. Iqbal H Sarker, ASM Kayes, and Paul Watters. Effectiveness analysis of machine learning classification models for predicting personalized context-aware smartphone usage. *Journal of Big Data*, 6(1):57, 2019.
124. Hans Schaffers, Nicos Komninos, Marc Pallot, Brigitte Trousse, Michael Nilsson, and Alvaro Oliveira. Smart cities and the future internet: Towards cooperation frameworks for open innovation. In *The future internet assembly*, pages 431–446. Springer, Berlin, Heidelberg, 2011.
125. Devaraju Sellappan and Ramakrishnan Srinivasan. Association rule-mining-based intrusion detection system with entropy-based feature selection: Intrusion detection system. In *Handbook of Research on Intelligent Data Processing and Information Security Systems*, pages 1–24. IGI Global, 2020.
126. Vishal Sharma, Kyungroul Lee, Soonhyun Kwon, Jiyoon Kim, Hyungjoon Park, Kangbin Yim, and Sun-Young Lee. A consensus framework for reliability and mitigation of zero-day attacks in iot. *Security and Communication Networks*, 2017, 2017.
127. Abraham Shaw. Data breach: from notification to prevention using pci dss. *Colum. JL & Soc. Probs.*, 43:517, 2009.
128. Ali Shiravi, Hadi Shiravi, Mahbod Tavallaee, and Ali A Ghorbani. Toward developing a systematic approach to generate benchmark datasets for intrusion detection. *computers & security*, 31(3):357–374, 2012.
129. Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. Security, privacy and trust in internet of things: The road ahead. *Computer networks*, 76:146–164, 2015.
130. Beata Ślusarczyk. Industry 4.0: Are we ready? *Polish Journal of Management Studies*, 17, 2018.
131. Peter HA Sneath. The application of computers to taxonomy. *Journal of General Microbiology*, 17(1), 1957.
132. Thorvald Sorensen. method of establishing groups of equal amplitude in plant sociology based on similarity of species. *Biol. Skr.*, 5, 1948.
133. Harald Sundmaeker, Patrick Guillemin, Peter Friess, and Sylvie Woelfflé. Vision and challenges for realising the internet of things. *Cluster of European Research Projects on the Internet of Things, European Commision*, 3(3):34–36, 2010.
134. Bambang Susilo and Riri Fitri Sari. Intrusion detection in iot networks using deep learning algorithm. *Information*, 11(5):279, 2020.
135. Mayank Swarnkar and Neminath Hubballi. Ocpad: One class naive bayes classifier for payload based anomaly detection. *Expert Systems with Applications*, 64:330–339, 2016.
136. Amir Taherkordi and Frank Eliassen. Scalable modeling of cloud-based iot services for smart cities. In *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, pages 1–6. IEEE, 2016.
137. Syeda Manjia Tahsien, Hadis Karimipour, and Petros Spachos. Machine learning based solutions for security of internet of things (iot): A survey. *Journal of Network and Computer Applications*, 161:102630, 2020.
138. Arman Tajbakhsh, Mohammad Rahmati, and Abdolreza Mirzaei. Intrusion detection using fuzzy association rules. *Applied Soft Computing*, 9(2):462–469, 2009.
139. Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A Ghorbani. A detailed analysis of the kdd cup 99 data set. In *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, pages 1–6. IEEE, 2009.
140. Aakanksha Tewari and Brij B Gupta. Security, privacy and trust of different layers in internet-of-things (iots) framework. *Future generation computer systems*, 108:909–920, 2020.
141. Frederic Thiesse and Florian Michahelles. An overview of epc technology. *Sensor review*, 26(2):101–105, 2006.
142. R Vinayakumar, KP Soman, and Prabaharan Poornachandran. Deep android malware detection and classification. In *2017 International conference on ad-*

vances in computing, communications and informatics (ICACCI), pages 1677–1683. IEEE, 2017.
143. Evan Welbourne, Leilani Battle, Garret Cole, Kayla Gould, Kyle Rector, Samuel Raymer, Magdalena Balazinska, and Gaetano Borriello. Building the internet of things using rfid: the rfid ecosystem experience. *IEEE Internet computing*, 13(3):48–55, 2009.
144. Ian H Witten, Eibe Frank, Leonard E Trigg, Mark A Hall, Geoffrey Holmes, and Sally Jo Cunningham. Weka: Practical machine learning tools and techniques with java implementations. 1999.
145. Liang Xiao, Xiaoyue Wan, Xiaozhen Lu, Yanyong Zhang, and Di Wu. Iot security techniques based on machine learning: How do iot devices use ai to enhance security? *IEEE Signal Processing Magazine*, 35(5):41–49, 2018.
146. Miao Xie, Jiankun Hu, Xinghuo Yu, and Elizabeth Chang. Evaluating host-based anomaly detection systems: Application of the frequency-based algorithms to adfa-ld. In *International Conference on Network and System Security*, pages 542–549. Springer, 2015.
147. Yang Xin, Lingshuang Kong, Zhi Liu, Yuling Chen, Yanmiao Li, Hongliang Zhu, Mingcheng Gao, Haixia Hou, and Chunhua Wang. Machine learning and deep learning methods for cybersecurity. *IEEE Access*, 6:35365–35381, 2018.
148. Dongkuan Xu and Yingjie Tian. A comprehensive survey of clustering algorithms. *Annals of Data Science*, 2(2):165–193, 2015.
149. Qian Xu, Pinyi Ren, Houbing Song, and Qinghe Du. Security enhancement for iot communications exposed to eavesdroppers with uncertain locations. *IEEE Access*, 4:2840–2853, 2016.
150. Jinpei Yan, Yong Qi, and Qifan Rao. Detecting malware with an ensemble method based on deep neural network. *Security and Communication Networks*, 2018, 2018.
151. Mattia Zago, Manuel Gil Pérez, and Gregorio Martínez Pérez. Umudga: A dataset for profiling algorithmically generated domain names in botnet detection. *Data in Brief*, page 105400, 2020.
152. Mohammed Javeed Zaki. Scalable algorithms for association mining. *IEEE transactions on knowledge and data engineering*, 12(3):372–390, 2000.
153. Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, and Shiuhpyng Shieh. Iot security: ongoing challenges and research opportunities. In *2014 IEEE 7th international conference on service-oriented computing and applications*, pages 230–234. IEEE, 2014.
154. Wei Zhou, Yan Jia, Anni Peng, Yuqing Zhang, and Peng Liu. The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal*, 6(2):1606–1616, 2018.
155. Yajin Zhou and Xuxian Jiang. Dissecting android malware: Characterization and evolution. In *2012 IEEE symposium on security and privacy*, pages 95–109. IEEE, 2012.
156. Zhi-Jie Zhou, Guan-Yu Hu, Chang-Hua Hu, Cheng-Lin Wen, and Lei-Lei Chang. A survey of belief rule-base expert system. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2019.