EAI Endorsed Transactions
on Security and Safety
Research Article EAI.EU

A Comprehensive Survey on Intrusion Detection based Machine Learning for IoT Networks

Hela Mliki[1,2,*], Abir Hadj Kaceam[2], Lamia Chaari[2]

[1]Science Faculty of Gabes, University of Gabes, Tunisia
[2]Laboratory of Technology and Smart Systems (LT2S), Digital Research Center of Sfax (CRNS), University of Sfax, Tunisia

Abstract

The Internet of things (IoT) is a new ubiquitous technology that relies on heterogeneous devices and protocols. The IoT technologies are expected to offer a new level of connectivity thanks to its smart devices able to enhance everyday tasks and facilitate smart decisions based on sensed data. The IoT could collect sensitive data and should be able to face attacks and privacy issues. The IoT security issue is a hot topic of research and industrial concern. Indeed, threats against IoT devices and services could cause security breaches and data leakage. Aiming to identify attempts to abuse the IoT systems and mitigate malicious events, this paper studied the Intrusion Detection Systems (IDS) based on Machine Learning (ML) techniques. The ML approach could provide good tools to detect novel intrusion activities in a timely manner. This paper, therefore, highlighted the related issues to develop secured and efficient IoT services. It tried to allow a comprehensive review of IoT features and design. It mainly focused on intrusion detection based on the machine learning schema and built a taxonomy of different IoT attacks and threats. This paper also compared between the different intrusion detection techniques and established a taxonomy of machine leaning methods for intrusion detection solutions.

Received on 04 February 2021; accepted on 24 September 2021; published on 06 October 2021

Keywords: Internet of Things (IoT), Wireless sensor Network (WSN), Machine Learning (ML), Intrusion Detection (ID)

doi:10.4108/eai.6-10-2021.171246

1. Introduction

The Internet of Things (IoT) is a technology trend able to provide new features and services. Indeed, the estimation shows that the number of connected devices being used will reach 75 billion by 2025 [1]. The fast development of IoT applications is due to new technological developments mainly in the fields of Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSN). IoT generates a large amount of data that need to be managed appropriately for further processing and analysis. Thanks to its ubiquitous and pervasive fashion, cloud computing is an efficient solution for IoT data management and monitoring. It provides shared resources such as storage, computing and application via a cloud services platform connected to the Internet. Both of the IoT system and the cloud exchange data via the Internet to provide the needed services. However, time sensitive applications require reduced network latency. This could be the case of an industry where machines are connected to a network and must be able to react urgently to an incident. In such a scenario a solution that extends the cloud to be closer to the objects that produce and react on the IoT data is an urgent need. This solution is called Fog computing. Thus, fog computing (referred also as edge computing) is supposed to store data close to the device object rather than routing all the information through a centralized data center in the cloud via Internet. Consequently, it contributes to providing reduced response time and network latency, and saving the backbone bandwidth to enhance Quality of Service (QoS). In addition, it protects sensitive IoT data from being transmitted outside the local area network [2, 3].

*Corresponding author. Email: mliki.hela@gmail.com

Nevertheless, there are various security risks that pose a threat to the cloud and fog computing. As the IoT system sensitive information would be submitted to a third-party cloud service provider, users should be sure that they choose a reliable service provider that guarantees data security. While the cloud computing is deployed with protected facilities managed and monitored by the cloud operators, Fog is deployed in a rather vulnerable environment. Its systems are significantly smaller than clouds. Consequently, it has reduced resources to support security and threat detection operations [4, 5].

The device objects on the IoT network involve some new techniques such as self-optimization, self-configuration, and self-management, which allows objects to set up and control themselves without any users' interference to adapt to the platform they are operating in. Thus, IoT could maintain interoperability communication between different kinds of infrastructure and software protocols, such as human-to-human communication, human-to-thing communication, or thing-to-thing communication. It can cover many fields such as healthcare, automobiles, entertainment, industrial appliances, sports, and homes.

Unlike the traditional networks, IoT networks hold protocols such as IPv6 over Low powerWireless Personal Area Network (6LoWPAN), IEEE 802.15.4, Constrained Application Protocol (CoAP), IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) [6]. Nevertheless, IoT applications face serious challenges caused by the heterogeneity and complexity of the data sources. Indeed, the different protocols used in IoT networks have been designed without any security background. Thus, an attacker could leverage vulnerabilities and limitations in these protocols by a range of exploitation techniques for malicious activities. Accordingly, detecting anomalies in IoT traffic could be vital for the protection of networks and information systems. Therefore, Intrusion Detection Systems (IDS) is a necessary line of defense for detecting attacks. IDS developed for IoT could face the challenge of determining the attack or the malicious partners. They are classified mainly into three categories depending on the used detection methods: Anomaly detection, Misuse detection, and Hybrid detection. Since machine learning provides a good technological tool for anomaly detection, IDS could consider machine learning as a solution to be applied to solve security issues [7, 8].

The contribution of this paper, relative to the recent literature in the field, can be summarized as follows: i) The scope of this survey is different from other survey papers published in the field, i.e., this paper aimed to put emphasis on the used intrusion detection techniques based on machine learning for IoT networks. ii) This paper provided an overview of the related research work. iii) This paper studied the IoT network security issues and pointed out the necessity of intrusion detection system as a solution for detecting anomalies in IoT networks traffic. iv) This review paper compared the intrusion detection techniques and machine learning approaches. v) This paper provided taxonomies for attacks and anomalies detection schema.

The rest of this paper is organized as follows: Section 2, surveyed the IoT components, architectures, protocols, and challenges. Next, section 3 provided an overview of the different security challenges and attacks in the IoT system. Then, section 5 studied the intrusion detection system and compared the intrusion detection different approaches. Thereafter, section 6, was devoted to studying and classifying the machine learning methods. Before concluding our survey, section 7 recapitulated the different related IoT survey works in the literature.

2. Background

The aim of this paper was to build an effective study and taxonomy of IoT threats and intrusion detection solutions based on machine leaning methods. To this end, and in a first step, we need to understand the IoT system design and components.

The IoT system extended the currently available internet services to allow connection between different device objects. This was achieved thanks to sensing equipments and various communications protocols. The main process of an IoT system can be summarized as follows:

i) Data generation : it represents the device objects that generate data.

ii) Data sensing : it collects and generates data at the edge network.

iii) Fog computing : it allows processing data close to the objects. Thus, it accelerates awareness and response to incident events.

iv) Thing connection : it could use wired or wireless communication and incorporates a Body Area Network (BAN) or a Personal Area Network (PAN). It includes a gateway, which provides connectivity with the internet network.

v) WAN : It enables a global network connection and communication.

vi) Cloud and services : it includes enterprise data systems, PCs and mobile devices. It provides services such as cloud computing and remote access.

Multiple devices could be connected in a network. The IoT devices are used in different domains and some of them are the following:

i) Home domain, which consists of smart devices designed to enhance people's lives and automate tasks. Alexa and Google Home are examples of smart home devices.

ii) Healthcare domain, which aims to improve the doctors care to their patients and to keep them safe. Among the many IoT applications a patient can use, we can cite sensors, medical device assimilation and remote monitoring devices. A pacemaker, placed under the skin in a patient chest to help regulate heartbeat, is an example of healthcare devices used by medical agents.

iii) Transportation domain, which includes connected vehicles that can be updated and accessed via the cloud. It helps keep the vehicle inside lanes and allows automated braking. Automatic Braking and Self-Steering are example of transportation domain devices.

iv) Commerce domain, which helps online retailing businesses and physical stores to carry on their commerce operation more efficiently and quickly. The IoT devices can be used at sales terminals for customers to purchase goods and also to automatically keep track of inventory. A square card reader is an example of commerce domain devices.

v) Financial domain, which allows customers to access their banking data and track the finances operations in real-time. It provides easy access to customers to manage their credit and debit card services. Banks can collect data about customers from the used devices to help improve the offered service and provide financial advice. ATM and Venmo are examples of financial domain devices.

vi) Industrial domain, which consists of systems control manufacturing equipment, as well as instruments like pressure sensors. Cloud-based systems include programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA), and industrial control systems (ICS).

vii) Military domain, which incorporates IoT technologies application in the military field used for warfare and combat operations. Examples of military domain devices are: robots, unmanned aerial vehicles for surveillance, and human-wearable biometrics for combat.

viii) Infrastructure domain, which enables smart city connectivity through disparate connected sources : sensors, devices, mobile and video cameras. It helps agencies to provide better city services and allows solutions for environmental problems, traffic congestion and safety issues. E.g. Cisco Kinetic for Cities is a platform that can automate traffic and street lights, prevent crime by increasing surveillance and optimize trash pickup.

The IoT system could be deployed with IoT devices that transmit data over the Internet network using IPv6 protocol, and/or with a local communication typically based on protocols like Ethernet (wired or wireless), Bluetooth, 6LoWPAN, IEEE 802.15.4, Wi-Fi. A new connectivity technology that fits energy constrained IoT devices, known as Low-Power Wide Area Networks (LPWAN), allows exchanging small data packets. It facilitates data transmission over longer range, at a lower cost and with a better energy optimization compared to other connectivity options. It includes different competing standards and technologies such as SIGFOX, LoRa, Ingenu, NB-IoT and LTE-M.

Figure 1 illustrates the main IoT system components at different process phases.

WSN is an IoT subset that addresses the use of wireless-connected sensors. It allows a real time control of the physical sensing domains such as healthcare and Transportation. The IoT facilitates the interconnection of many heterogeneous devices over the Internet, which brought about the need for a multi-layer archictecture. However, so far, the number of proposed architectures has not converged to one model because of the different views of the authors. Nerveless, a basic model has three layers: the perception layer, the network layer, and the application layer [9, 10]. They are defined as follows :

i) The perception layer, which aims to collect data (e.g., humidity, temperature, pH level, and pressure) from the physical system under control sensed thanks to sensors. This layer can be divided into two sublayers: perception nodes such as sensors and controllers; and a perception network that network that is connected to the network layer.

ii) The network layer, which assures data network transmission and provides a pervasive access environment to the next layer (i,e., the application layer). This layer defines routing, network management and data transmission to different devices through a heterogeneous network.

iii) The application layer, it checks data and sends them to the ultimate users to provide an access to their smart resources such as intelligent computation and business services. It, then, represents, an interface for the end-users to communicate with their IoT devices.

Table 1 illustrates some of the main supported standard protocols for each layer.

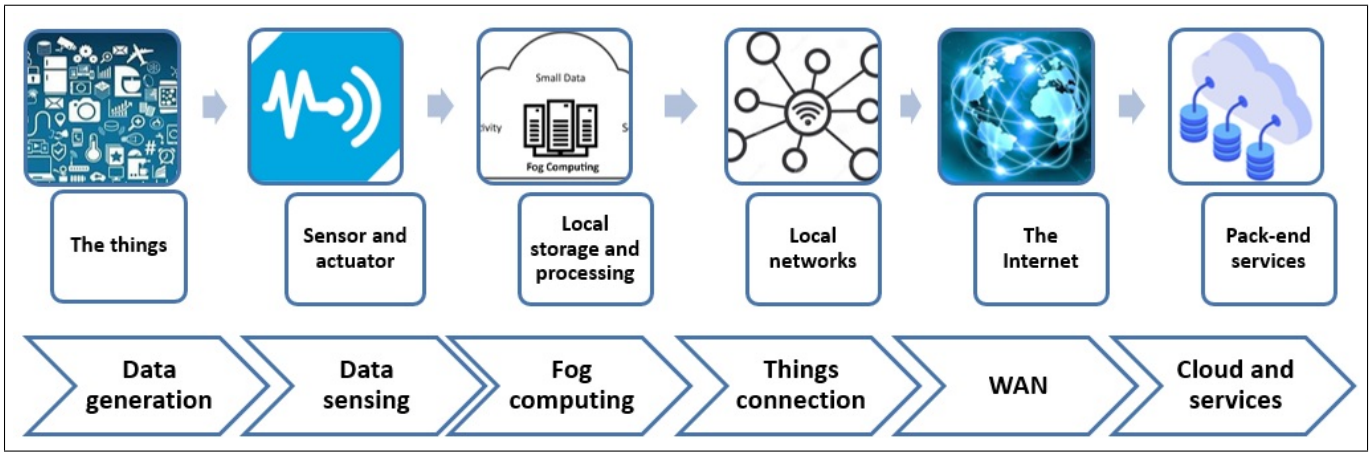

Figure 1. The IoT system process.

Still IoT has several challenges compared to the traditional network. Indeed, the IoT system can maintain complex and heterogeneous data and each layer of its architecture has its own communication protocol. In addition, the IoT devices are set up on Low-power and Lossy Networks (LLNs). However, LLNs are stressed by dynamism, reduced memory, and power handling. These features are not considered in the standard Internet. Thus, examining security threats on IoT should be in parallel with LLNs, which faces energy and connectivity constraints [11]. A new generation of IoT systems, knows as Cognitive IoT (CIoT), enables autonomous interaction, context awareness and perception action between physical or virtual objects. Authors in [12] investigate potential threats and attacks on CIoT.

3. IoT Attacks

The IoT can be affected by different threats and malicious attacks. This could cause serious damage to the system in any of the IoT architecture layers and harm its reputation. This section provided some some possible attacks targeting security at each each layer (i.e., perception layer, network layer and application layer).

3.1. Perception Layer Attacks

The perception layer can be exposed to many physical and hardware attacks. Indeed, due to the diversity of the deployment environment and the dynamic change in the network topology, the sensor nodes in the perception layer usually use ad-hoc network technology and wireless communication. In such environment, attackers can easily eavesdrop on communication between nodes. Furthermore, the nodes usually use the sleep mode to prolong the life of the resource power; however, the attackers can keep the node in a working state to accelerate the energy consumption [51–54]. Some of the common attacks on the perception layer are as follows:

i) Node capture attacks, which can be achieved via physically replacing the entire node, or tampering the node hardware to capture and control a device. Indeed, when a node is compromised, the confidential information like group communication key, cryptographic keys or access keys will be exposed to the attacker. In addition, the attacker can inject a fake malicious node in the network to act as an authorized node in the network connection; after that, he is likely to copy the associated information transmitted over the network and use it for further attacks to compromise the security of the entire IoT network.

ii) Malicious code injection attacks allowing the attacker to inject the malicious code into the memory and control a device in a IoT network. In order to allow the injection of a malicious code into the system, the attacker can leverage the attack on the system from the end-user, use a debug module or use some hacking techniques. This kind of attack can execute specific control functions and grant access into the IoT system.

iii) False data injection attacks, which occurs when the attacker is able to inject false or malicious data instead of real one. It stops the real measurement data transmission by the captured node and replaces the real information by the transmission of false data through a tampered node to the ultimate user. Thus, the entire network could fall into the attacker control and a Denial of Service (Dos) attack can be performed.

Table 1. IoT communication protocols.

Layer	Protocol	Description
Perception layer	IEEE 802.15.4 [13, 14]	- It is a standard that covers the physical layer and Mac layer of a low rate Wireless Personal Area Network (WPAN). - WSN is one of the target applications of this standard. - Internet Engineering Task Force (IETF) has proposed standards within IEEE 802.15.4 to simplify the integration between Internet and LLNs (low-power and lossy networks).
	RFID [15–17]	- It automatically identifies and control objects through radio wave. - The principle object of RFID is to rapidly exchange information, provide efficiency of manufacturing and the whole life cycle of the supply chain for the delivery and dispatch speeds.
	Bluetooth Low Energy (BLE) [18–21]	- It is a low-power wireless technology. - It works with many IoT commercials applications such as smart watches, fitness trackers, and smart appliances.
	WBAN (802.15.6) [22, 23]	- It is a standard for short range, low power, and reliable wireless communication for human body area network. - It can be deployed in several applications such as health monitoring and ambient living environments.
Network layer	Z Wave [24, 25]	- It is a low-power wireless communication protocol. - It is specified for applications that need very small data transmission information such as household appliance control, access control and wearable health-care control.
	LoRaWAN [26–30]	- It is a media access control protocol for Low Power Wide Area Networks (LPWAN). - It is developed to allow low-powered devices to communicate with Internet-connected applications over long range wireless connections.
	Sigfox [31–34]	- It allows the transmission of small data packet for wireless network to connect low-power devices. - It is a competitor of LoRaWAN in the LPWAN domain.
	6LoWPAN [35–37]	- IPv6 over Low power Wireless Personal Area Networks has an adapted header format to connect the endpoint devices, and addresses IPV6 packet in the network layer infrastructure. - The IETF 6LoWPAN working group proposes an adaptation of new communication generation, and, technologies that can be supported by the IEEE 802.15.4
	RPL [38, 39]	- It is a routing Protocol for Low Power and Lossy Networks. - It supports optimal routing requirements by creating a robust topology over lossy links.
	Wi-Fi [40, 41]	- It is a widely used communication protocol among IoT devices. - It is based on the IEEE 802.11 standards family and IEEE802.11n is the common Wi-fi used standard. -It is an excessive power consumer for some IoT application.
	Cellular [41–43]	- GSM/3G/4G/5G are cellular communication protocols for IoT applications that requires operation over long distance. - They can send and transfer a high amount of data. - They are costly and cause high power consumption for many IoT applications.
Application layer	Constrained Application Protocol (CoAP) [44–46]	- It is released by IETF Internet Engineering Task Force for application request–response protocol layer. - It allows physical objects to deliver services to users on the Internet. - It was designed by using a subset of the HTTP methods.
	Message Queue Telemetry (MQTT) [46–48]	- It was created by IBM and targets lightweight machine-to-machine (M2M) communications. - It is a messaging protocol for the IoT and M2M . - It is a Publish/subscribe pattern. - It is arranged to be a lightweight protocol suitable for networks with unreliable or low-frequency links.
	Data Distribution Service (DDS) [49, 50]	- It is a standard for expandable, high-performance, and real-time M2M communication. - It includes two main layers : Data-Centric Publish-Subscribe (DCPS), which defines information delivery to the subscribers; and Data-Local Reconstruction Layer (DLRL), which provides an interface to the DCPS functionalities.

iv) Side Channel Attacks (SCA); these aim to leak the secret key used in encryption to protect the sensitive data. This kind of attacks use different techniques to eavesdrop the data transmission device and determines when an encryption key is used to access a device.

v) Replay attacks; these target the authentication and key agreement schemes and aim to transmit legitimate information to the target node in order to earn the IoT system trust. The attacker can easily capture, record, then, replay the legitimate traffic in a wireless channel to cause, for example, energy drain at the sensor nodes.

vi) Spoofing attacks; these work by disguising a malicious device to look like an authorized one. Tricking the router into allowing it on the network. Since the disguised malicious device can communicate with the router, it can inject malwares to be spread to all the other devices on the network. IP spoofing and RFID spoofing are examples of IoT spoofing attacks. There are further attacks that could be achieved via a spoofing attack such as accelerating the node power consumption and decreasing the node lifetime by causing the node to re-send the data. Such action events could increase significantly the network traffic and cause denial of service.

vii) Eavesdropping attack, where the attacker can sniff out the confidential delivered data and interfere in a channel link. Thus, the attacker can pump noise signal, intercept, read and save data to create a denial of service.

3.2. Network Layer Attacks

The network layer is a hardware and software infrastructure for for data routing and transmission received from the perception layer. Hence, the network layer often hosts the perception layer attacks as well as other types of attacks [55, 56]. The most common attacks can be identified as follows:

i) Man in the Middle attacks, where the attacker injects a malicious device that can be virtually located between two communicating victim nodes. The attacker steals the identify information of these two victim nodes using eavesdropping and spoofing attacks. This allows the malicious node to behave as a legitimate one, store and forward the victim nodes data. The victim nodes cannot detect the malicious node and assume that they directly communicate with each other.

ii) Denial-of-Service attacks (DoS), which are performed when the attacker floods normal nodes with requests. This kind of attack can bombard the IoT network by generating a large amount of traffic to consume resources or bandwidth of the legitimate nodes. There is a wide range of DoS attacks launched against the IoT such as Ping of Death, Tear Drop, UDP flood, SYN flood, and Land Attack.

iii) Sinkhole attacks, which is the most destructive attack since it prevents communication among network devices and it is used to launch further attacks. Indeed, a compromised node aims to attract all the traffic from adjacent nodes using routing metrics in routing protocols. This attack prevents the destination node from obtaining the valid and complete sensed information. In addition, it can be the basis of other attacks such as selective forwarding and wormhole attacks.

iii) Sybil attack, which denotes an attempt to control a peer network by forging multiple fake identities. The attacker broadcasts massages with multiple fake identifications in a WSN to compromise the effectiveness of the systems. Such an attack could cause the system to generate wrong reports and lose privacy. To outside observers, these multiple fake identities give the impression of being real unique identities [57].

3.3. Application Layer Attacks

Attackers could exploit the vulnerabilities in the software application, and then launch phishing attacks, virus, worms, Trojan Horse, Spyware and malicious scripts [58–60]. Several possible attacks in the IoT application layer can be categorized as follows:

i) Phishing attack, which uses infected emails or phishing Web applications to gain access to the confidential data by spoofing the user authentication credential.

ii) Virus, Worms, Trojan Horse, Spyware, which are malicious programs that can infect the software applications. They aim to cause tampered data, denial of service and missing or stolen information.

iii) Malicious Scripts, which are embedded in Web pages or served by an advertisement. It scans the network for IoT devices and, then, takes control of them.

4. Security Challenges and Open Issues in the IoT

Security is the main challenge in the IoT network design. Indeed, the IoT devices are designed to be light weight, have low computation power, low battery life and low memory. As incorporating security features are resource expensive, IoT devices are often found to be less protected and in recent times, more IoT devices have been attacked due to high profile security flaws.

In addition, IoT is a heterogeneous system that interconnect diverse peripheries different in terms of capacity, complexity, size, data, quantity and type. This heterogeneity has an important influence over the protocol and network security services that must be implemented in the IoT.

Hence, it is important to implement policies that define the data management, protection and transmission in an efficient way. A mechanism is needed to enforce such policies and identify the service level agreements in each involved service. Besides, access and privilege management mechanisms are required to prevent unauthorized access to the IoT resources. Without an efficient cryptographic algorithm with an adequate key management and security protocols, the users' privacy and security can be threatened; and any IoT node detected by a malicious user could be exploited to collect information for successful attack.

However, since IoT is based on the Internet, it inherits and even extends its security problems due to the different new protocols implemented for IoT without taking into account the notion of security background. Indeed, once a device is connected to the Internet, it becomes vulnerable to potential security breaches caused by hacking and phishing techniques. Therefore, as IoT is becoming a reality, serious efforts should be made to design and implement security schema able to be integrated within the IoT system processes.

The IoT security services require providing: confidentiality, integrity, and availability [61–64]. These security requirements are defined as follows:

i) Confidentiality : IoT can interconnect, store and transfer sensitive information from a large number of devices such as human, machine, sensor, and protocol (e.g. RFID, Zig bee) in real time. Nevertheless, since it is easy to intercept personal information by a malicious user, it has become urgent to secure the message, and the stored data against unauthorized individuals. It is important to guarantee that only authorized users can access the information securely and prevent eavesdropping or attacks. A cryptographic mechanism is also needed to ensure that anonymity and piracy can not access or process the data. Besides, each object in IoT has to be able to identify and authenticate other objects. However, authentication could be a challenge in the IoT network because of the huge number of entities (i.e., millions of smart objects, service providers, processing units, users), the emerged standards and self configuring protocols that make authentication a complex process compared to the traditional network.

ii) Integrity : IoT needs a security process, that provides a reliable service and ensures an effective control action to pick up any modification in the network and to detect system threat. Therefore, it is necessary to define a mechanism that prevent injection attacks. However, integrity cannot be reliable because of the IoT low computational power.

iii) Availability : It is necessary to provide accessible data to IoT users, whenever necessary, despite the huge number of users in real time. Indeed, it is important to offer services that are always available and continuous whenever the data and devices are requested. Availability is an important need for the successful deployment of IoT systems. However, IoT systems and devices could be unavailable because of attacks events such as : DoS and eavesdropping attacks.

Security issues in IoT systems are increasingly imperative with the expanding number of attacks. Unlike the conventional systems, the IoT systems are subject to more threats than the conventional systems because of the qualities of the IoT devices characteristics and communication protocols. As a matter of fact, IoT devices are usually outfitted with lower battery and micro-controllers, which makes them easily overflowed. In addition, the used communication protocols such as Bluetooth, Zig-Bee, Wifi or GSM are prone to attacks. On the other hand, during the communication process, some of the data could be lost and, thus, affect the network efficiency in data management. Designing the communication nodes and managing the huge exchange of data among huge number of objects is an additional challenge.

4.1. IoT security Challenges in Different Layers

The IoT basic architecture has three layers and each of which should deploy mechanisms to handle security challenges. Nevertheless, each layer suffers some security issues [51, 65], which should be solved for confidentiality, availability and integrity services requirements [66]. Hence, this section discussed the various security challenges and protective measures for each IoT layer.

Security at the Perception Layer. Security at the perception layer should provide mechanisms against hardware attacks. This layer includes different sensor types that could detect physical attacks. As the perception layer is designed to collect or forward information between the sensors, data confidentiality need to be ensured. Indeed, the system should be able to prevent any unauthorized user from accessing the data, exclude any unauthorized device and reject prohibited flow from accessing the network. Confidentiality solution at the perception layer could include digital signatures to withstand unauthorized access. In addition, symmetric and asymmetric encryption algorithms are needed to encrypt data for data privacy protection, by converting it into a code, so that it would not be understood by the undesired parties [67, 68]. To enforce user privacy in RFID systems, there are privacy-friendly authentication protocols implemented for RFID. These are based on well-established symmetric-key cryptographic building blocks. In addition, they require a lower reader complexity than $O(N)$, where N is the number of tags in the database. The literature shows that designing a privacy-friendly protocol is still a challenging task [69, 70]. The attacker injected node in the network can put out of sight sensitive information like identity and location. Consequently, this node is sensed anonymous by the IoT network. As a solution, a K-anonymity approach is recommended for low processing devices. k-anonymity is a privacy protection approach used to protect against identity disclosure. This approach is required when there is a need to share users records in such a way that the individuals' identities of those who are subject of the data cannot be re-identified [71]. On the other hand, it is necessary to provide an integrity service process to mitigate data tempering. Each device in the perception layer should be supplied by error detection mechanism such as parity bit and checksum. Cryptographic hash function could also be deployed to guarantee the data integrity at the perception layer [72, 73]. Most of the attacks at this layer can be resolved by designing a physically secured devices. It involves components like data acquisition unit design, radio frequency circuits and chip selection. Such components should not be

easily changeable and should be of high quality. The antenna design for wireless communication should be implemented to cover a good distance communication to guarantee the availability of the system [74].

Security at the Network Layer. Security mechanisms implemented at the network layer, along with the perception layer, build an additional defense layer for the IoT system. It could implement the following security schema:

i) Routing security : several routing mechanisms suffer from stability and reliability problems. Therefore, a secure routing is one of the main features for sensor systems safe usage. A secure routing is ensured by routing the data through multiple paths, which increase the network error detection. It reduces energy consumption, increases the network lifetime and prevent black hole attacks [75, 76]. Simultaneously, the IPSec Security channel is a good solution to decide whether the sender IP is real or not. Indeed, IPSec supplies two security features types : authentication and encryption. This solution may help avoid eavesdropping and data tempering attacks [77].

ii) Sinkhole attack detection : a Sinkhole attack is a compromised node inside the network that launches attacks. Based on the routing metric used in the routing protocol, the compromised node publicizes useful way to attract all the traffic from adjacent nodes and use these nodes to route the traffic. The Sinkhole attack causes extensive threat, since it is a fundamental phase to launch additional attacks. Challenges exist in detecting, and providing resistance to a sinkhole attack in the WSN network [78–81].

iii) Secure Management : IoT involves billions of connected devices that need to be managed, therefore, IoT operators require an effective device management platform to address IoT security challenges. Such platform allows operators to manage these billions of devices that communicate with the base station, to scale quickly and cost effectively and provide visibility into data traffic. It needs several key distribution management techniques for encryption and maintaining routing information [82–84].

iv) Secure localization : IoT services may rely on location information in order to report geographically meaningful data. Localization algorithms design and techniques have to implement countermeasures to mitigate fake locality information provided by an attacker using spoofing techniques [85–87].

v) Self-organization : it is a countermeasure technique to preserve communication among devices in a network after a failure caused by disasters or attacks; and thus, sustain network availability. A key distribution mechanism could be a challenge for software based on public-key cryptographic systems [88, 89].

Security at the Application Layer. Security mechanisms implemented at the application layer complement the other layers of defense deployed at the network and perception layers for the IoT system.

Data confidentiality, integrity and availability should be guaranteed in the application layer. Various applications are provided to a large number of users. Therefore, a proper authentication mechanism should be provided in order to prevent the access of illegal users into the system. For data recovery purposes, the storage systems transfer data through different channels to different locations. Such a process involves data integrity and user privacy. Consequently, a proper mechanism for data recovery and storage process should be implemented [90]. This layer could face buffer overflow vulnerabilities if the programmer software implementation does not respect the standard recommendation. Then, such vulnerabilities could be leveraged by attackers to achieve their aims. To correct security' failures, risk assessment is a fundamental technique to define potential threat and risk associated with an IoT system. It is used to come up with new threats to the system, and helps to better identify continual control for reducing risks during the risk mitigation process [91, 92]. Some of the security measures required in this layer can be listed as follows:

i) Intrusion detection : it generates alarms on the occurrence of any suspicious activity in the system. It keeps track of the intruders activities in log files. Misuse and anomaly detections are among the different intrusion detection existing techniques [73].

ii) Firewalls : it monitors and filters the incoming and outgoing traffic based on defined security rules [93, 94].

ii) Anti-virus, Anti-adware and Anti-Spyware these software solutions are essential to ensure security consistency, confidentiality, and reliability in the IoT environment.

5. Intrusion Detection

Despite the growing and advanced research in the domains of computer network, security is still be threatened. Therefore, many security solutions are developed to tackle attacks. Intrusion Detection (ID) is a security solution that aims to identify

malicious activities attempts to abuse a network system. Typically, an Intrusion Detection System (IDS) detects vulnerabilities, notifies malicious activities, and enables preventive measures. It monitors the network traffic and can address the illegitimate access, spiteful activities, or policy stealing. Due to the IoT characteristics in terms of diversity of the components such as protocol, connected devices, and network architecture; the IoT network is considered as a vulnerable environment to multiple attacks. Therefore, it is important to implement an IDS as a defense line in the IoT network. The main purpose of an IDS is to dynamically monitor a network traffic and classify them as normal or anomalous. It analyzes the traffic and triggers alarms when an anomaly is detected [95, 96]. The IDS alarms can be classified into four categories as follows :

i) The true positive represents the detected normal traffic types that are correctly identified as normal by the system.

ii) The true negative represents the detected anomalous traffics that are correctly identified as anomaly or attacks by the system.

iii) The false positive represents the detected normal traffic types that are identified as anomalous traffic.

iv) The false negative represents the detected anomalous traffic types that are identified as normal traffic.

A perfect system should have reduced false alarms (i,e., false negative and false positive) [97].

Intrusion detection techniques, used in IDS could be classified into three categories: misuse based IDS, anomaly based IDS, and hybrid based IDS. They are defined as follows:

i) Misuse-Based IDS technique is also known as signature based detection. It detects anomaly by using a set of signatures (or rules) for known attacks in a database. This technique can detect known attacks efficiently and generate very low false alarms. However, it is unable to detect new attacks of which it does not have the signatures in the database [98].

ii) Anomaly based IDS technique is also known as event based detection technique or outliers detection. This technique builds the profile of normal activities, then, it detects malicious activities by analyzing the profiles that deviate from normal activity. Indeed, it classifies activities into normal behavior and malicious behavior, and considers malicious behavior as an intrusion. This technique can detect new attacks and has a high detection rate. However, it could generate a considerable number of false alarms. This technique uses three categories of methods to generate the considered behavior model: statistical based, knowledge based, and machine learning based [99–101].

iii) The hybrid based IDS combines the benefits of both misuse and anomaly based detection technique. Thus, it has two detection modules, one for new attacks detection, and the other for known attacks detection. Nevertheless, this technique is not recommended for an IoT system as it consumes resources and energy [102, 103].

IDS could be sorted out into three types based on location of deployment in real time as follows:

i) Network-based intrusion detection system (NIDS), which is placed along a network segment or boundary and monitors traffics on that segment. It could detect attacks launched by outside attackers who want to gain unauthorized access to the network to steal or disrupt the network system [104–106].

ii) A host-based intrusion detection system (HIDS); this is a software installed on individual systems to be monitored. An HIDS can only monitor the individual host system and not the entire network. It can detect an internal activity, identify the user who accessed and the resources he used, and prevent illegitimate access [107–109].

iii) Hybrid system, which is a technique that integrates both NIDS and HIDS. Thus, it is perfect in terms of security and attacks detection [110].

IDS could perform online or offline detection. The online detection manages the network packets data in real time, whereas the offline detection processes stored data in logs files for example. In the IoT networks, the IDS could be deployed in the border router or in every physical object. Placing the IDS in the border router, could detect intrusion attacks from the internet against the objects in a network segment. However, deploying the IDS in every physical object requires more resources (i,e., energy, processing and storage. This could be an issue due to Low power and Lossy Network (LLN) nodes sources limitations. Another solution consists in distributing IDS agents across some dedicated nodes to gain more processing capacity. Nevertheless, such a solution faces the challenge of how to organize the network in different regions for an optimal performance [111]. Based on the IDS architectures, it is possible to classify IDS into the following categories:

i) Centralized IDS: the entire IDS is placed in the network center, either remote or host-based location [112, 113].

ii) Distributed IDS: the IDS nodes are joined among multiple nodes in the network and the detection responsibility is shared amongst them [114, 115].

iii) Hierarchical IDS: It may be stand alone or in combination with another architecture type in which some nodes have a higher detection control than others. Decentralized architectures could be grouped under hierarchical cluster [116, 117].

iv) Hybrid IDS: It represents any combination of the cited above architecture. This category is often exploited in tandem with multiple detection methods [118, 119].

Figure 2 illustrates the different IDS categories according to detection time, architecture, location and detection methods features.

Table 2, reviews the IDS proposals for IoT based on detection methods.

6. Machine Learning

Machine learning (ML) is a sub-domain of artificial intelligence domain. It studies the knowledge from the training data and supports diverse applications domains such as computer science, signal processing, and telecommunication. It can solve mathematical and complex problems and has proved accuracy in detecting attacks and misbehavior in different security solution. ML algorithms can also be used in IDS for classifying behaviors as normal or anomalous by building models able to detect patterns to predict intrusion. The challenge with the IDS based ML implementation consist in how to build a model with a reduced number of false alarms and good recognition accuracy. Considering the IoT heterogeneous environment and its dynamic behavior, anomaly based ML technique could be a key solution to boost the detection of current, new and subtle attacks and improve the detection performance. After the features have been extracted from the data source, different ML methods could be implemented to classify the data. The obtained results can be leveraged by the IDS to make decision. The ML classification involves two phases: a training phase and a testing one. The training phase learns the features distribution and generates a model able to detect patterns. Then, in the testing phase, the model is applied to detect any abnormality [135–137]. Figure 3 shows the process to achieve the ML classification. In this figure, the test and training data are preprocessed to remove noise. In the training data set, feature selection methods are used to extract relevant feature sets, which are used in the training classifier. The normalization step standardizes the range of different data feature values. Finally, in the classification phase, a classifier algorithm is deployed. The ML techniques consist of three categories: supervised, unsupervised, and semi-supervised approaches.

This section builds taxonomy for different ML techniques that can be used in the IDS context .

6.1. Feature Selection Methods

Features selection simplifies the interpretation model, removes information redundancy, decreases the training times, and increases the classifier's efficiency. Features selection is based on the following three techniques for feature reduction [138–140]:

i) The wrapper technique, which generates relevant features subsets from a feature vector based on the learning algorithm performance.

ii) The filter technique, which generates relevant features subsets from a feature vector regardless of the learning algorithm performance. It evaluates features relevance according to heuristics based on general data characteristics.

iii) Hybrid technique, which exploits the important features of both wrapper and filter methods.

Principal Component Analysis. The Principal Component Analysis (PCA) is a filter method used to extract relevant data and present it as a set of variables called principal components. When a large amount of data needs to be approximated by a complex model structure, PCA is the adequate tool for data reduction by simplifying the data matrix. PCA estimates the variables correlation structure and a variable importance is defined by the size of its residual variance. Indeed, PCA projects the matrix X into vectors T and P' to reveal the dominating characteristics of a multivariate data set. A projection matrix P' is used to project X down on an A-dimensional subspace leading to T the object coordinates in this plane. The score vectors t_a represents the columns in T. However, the loading vectors P_a represents the row in P and holds the direction coefficients of the PC (hyper) plane. The vectors t_a and P_a are orthogonal. The deviations between projections and the original coordinates define the residuals, which are collected in the matrix E. PCA in a matrix form represents the least squares [141, 142]. Hence, X could be defined as follows:

$$X = 1\overline{x} + TP' + E \tag{1}$$

Here, $\overline{x}$ is the mean vector that is explicitly included in the model formulation.

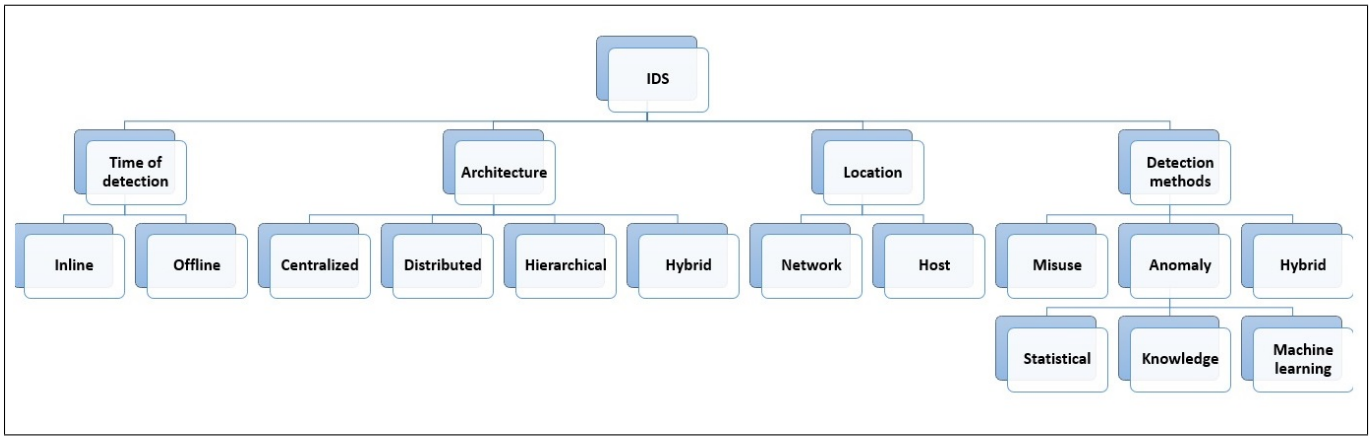

Figure 2. IDS categories

Table 2. Summary of IDS for IoT in recent literature.

Detection method	References	Descriptions
Misuse-based IDS	D. Midi et al. Date 2017 [120]	- This research work proposes a self-adapting, knowledge-driven expert intrusion detection system for IEEE 802.15.4 and WiFi network, called Kalis. -The proposed system is able to detect attacks in real time across a wide range of protocols for IoT. - Kalis was implemented using Java on an Odroid xu3 development board and uses a TelosB [121] wireless sensor mote with a custom TinyOS [122] application as bridge to interact with the IEEE 802.15.4 traffic. - Performance evaluation shows that the proposed solution Kalis has the highest performance compared to Snort and Trad. IDS (i.e, Kalis accuracy = 100% and Kalis detection rate= 91%. Snort accuracy =76% and Snort detection rate=89%. Trad. IDS accuracy=75% and Trad. IDS detection rate=48%).
	N. U. Sheikh et al. Date 2018 [123]	- This research work proposes a signature based intrusion detection system using a fast pattern matching algorithm which outperforms existing signature based IDS in detecting known attacks. - The proposed system generates different attack type signatures from the training dataset KDD Cup 99. - It evaluates the false positive and false negative performance using simulation.
	W. Li et al. Date 2019 [124]	- This research work proposes a generic framework application called CBSigIDS for IDS with distributed architecture. The framework uses block-chain technology to check the shared rules between the IDS nodes, thus, it builds a trusted signature database. - The research work uses simulation to evaluate the performance of the proposed application under worm and flooding attack. - The proposed CBSigIDS framework is compared to a block-chain-based SDN application called DistBlockNet.
Anomaly-based IDS	V. L. L. Thing Date 2017 [125]	- This research work proposed an anomaly detection and classification solution using deep learning algorithm for the IEEE 802.11 wireless device network. - It considers the classification as a multi-class problem (i.e., flooding type attacks, legitimate traffic, impersonation type attacks and injection type attacks) - The proposed solution achieves an overall accuracy of 98.6688% in classifying the attacks.
	N.Moustafa et al. Date 2018 [126]	- This research work proposes an AdaBoost ensemble method, using three techniques of Decision Tree, Naive Bayes and Artificial Neural Network, was applied to enhance the overall performance in terms of time processing, detection rate, and accuracy. - It aims to propose a solution to defend against botnet attacks in an IoT network. - It uses the UNSW-NB15 [127] and NIMS botnet datasets [128] to extract the protocols data sources. - Simulation is used to evaluate the performance of the proposed schema.
	S.Prabavathy et al. Date 2018 [129]	- This research work proposes a distributed detection mechanism for IoT applications using fog computing. - The proposed mechanism is implemented using Extreme Learning Machine (ELM) algorithm at distributed fog nodes. The ELM algorithm is exploited to identify the attacks in incoming traffic from IoT virtual clusters. - The NSL-KDD dataset was used for training and testing the mechanism. - To evaluate the performance of the proposed mechanism, accuracy, detection rate, false alarm rate and response time were evaluated and studied.

	H.mliki et al. Date 2019 [130]	- This research work studies and compares the performances of the classical machine learning methods: Support Vector Machine (SVM), K-Nearest Neighbor (KNN), and K-means. - The NSL-KDD dataset was used for training and testing the mechanism. - The performance metrics considered in this study are Accuracy, Detection Rate, False Alarm Rate, Recall, Precision, F1- Score, Time Training and Time Assigned Label. - The authors propose a solution to the enhancement of the system detection by leveraging the multi-level tweak.
	S. Krishnaveni et al. Date 2020 [131]	- This research work proposes an anomaly detection system for cloud computing. - It uses Support Vector Machine as a machine learning method for profile training based on NSL-KDD dataset.
Hybrid-based IDS	H. Bostani et al. Date 2017 [132]	- This research work proposes a hybrid intrusion detection solution for detecting routing attacks in IoT (i.e., sinkhole and selective forwarding attacks), as well as blackhole, rank, and wormhole attacks in a 6LoWPAN network. - The proposed solution can achieve a true positive rate equal to 76.19% and a false positive rate equal to 5.92% when both selective-forwarding and sinkhole attacks are launched simultaneously. - The proposed solution can achieve a true positive rate equal to 96.02% and a false positive rate equal to 2.08% in detecting wormhole attack.
	S. Choudhary et al Date 2019 [133]	- This research work aims to enhance the detection of selective forwarding and sinkhole attack in the 6LoWPAN environment using a routing protocol RPL. - It proposes a hybrid intrusion detection schema for detecting two routing attacks (i.e.,sinkhole and selective-forwarding attacks). - The proposed schema shows a true positive rate of 96.3% and false positive rate of 6.1%.
	A. N. Jaberand et al. Date 2020 [134]	- This research work proposes a solution that combines a fuzzy c means clustering (FCM) algorithm with support vector machine (SVM) to enhance the detection system accuracy in cloud computing environment. - The NSL-KDD dataset was used for training and testing the solution.

Correlation-based feature selection. Correlation-based feature selection (CFS) is a filter feature selection method. This method does not depend on any particular data transformation. It measures the correlation between nominal features, thus, numeric features need to be transferred into discrete counterparts. CFS assumes that features are conditionally independent given the class they belong to. It can identify relevant features when moderate feature dependencies exist. However, when features strongly depend on others because of the class they belong to, CFS may fail to select all the relevant features . The interesting features subsets contain features that are uncorrelated with each other and highly correlated with the class [143–145]. The correlation between a composite test consisting of the summed components and the outside variable can be predicted from the following equation :

$$r_{zc} = \frac{k\overline{r_{zi}}}{\sqrt{k+k(k-1)\overline{r_{ii}}}} \quad (2)$$

Here, r_zc is the correlation between the summed components and the outside variable, k is the number of features components; $\overline{r}_{zi}$ is the average of correlations between components and the outside variable; and $\overline{r}_{ii}$ is the average inter-correlations between components.

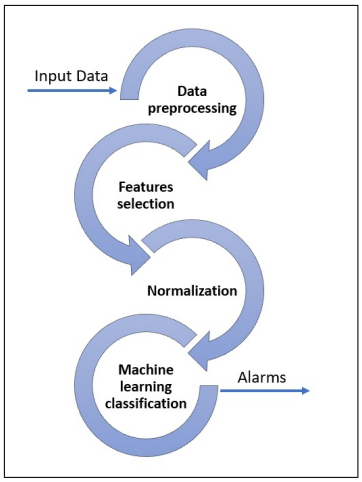

Figure 3. ML classification process.

Information Gain. Information Gain (IG) is a filter method for feature selection. It measures how much an attribute is useful in a given set of feature vectors. IG measures the reduction in entropy, which is a way to measure the level of impurity in a data sample. It calculates the IG entropy for each attribute and ranks them in a decreasing order. Each attribute gains a score from 1 to 0. Attributes with higher IG entropy represents the relevant one and they are considered as the input subset of features to the next dimensionality reduction step [146, 147]. The estimated information required to classify a given instance in as follows :

$$I(d_1, d_2, ..d_m) = -\sum_{i=1}^{m} \frac{d_i}{D}.\log_2(\frac{d_i}{D}) \quad (3)$$

Here, m is the number of classes, D is the total instances number in the training set, and di is the instances number of class i in the training set.

Attribute Ratio. Attribute Ratio (AR) method is a filter technique for feature selection. It is calculated by features frequency or average (Avg). Before calculating AR, we need to calculate the class ratio (CR). CR defines the ratio of each class for attribute i. CR is calculated through two methods according to the type of attributes [148, 149]. The AR feature selection formula is as follows :

$$AR(i) = MAX(CR(y)) \tag{4}$$

Here, CR represents the class ratio. For numeric attributes, the CR is calculated as follows :

$$CR(y) = \frac{Avg(C(y)}{AVG(total)} \tag{5}$$

For binary attributes, the CR is calculated as follows :

$$CR(y) = \frac{Frequency(1)}{Frequency(0)} \tag{6}$$

Genetic Algorithm. The Genetic algorithm (GA) is a heuristic algorithm inspired from the natural selection, where fitter creatures survive and their genes are simulated. The GA starts with a random population of individuals and improves the population using three operators: selection, crossover, and mutation. The best solution in the last population is returned as the best global optimum approximation for a given problem. This algorithm evaluates each individual fitness in the population using a fitness function. It associates probabilities to individuals and select them with a selection mechanism for creating the next generation proportional to their fitness values. The selection operator is able to choose the best solution since the probability is proportional to the fitness. There are many selection techniques used to choose the best solution such as the fuzzy selection, the fitness uniform selection [150], the proportional selection [147], the linear rank selection [147], and the steady-state reproduction [151]. The GA algorithm uses the crossover and mutation operators that simulate the biological process for introducing diversity to the population. With the crossover operator two solutions selected randomly are combined to produce two new solutions. There are different techniques for this operator notably the single point and double point techniques [152]. The mutation operator prevents solutions from becoming similar and increases avoiding local solutions probability. There are many techniques in the literature for the mutation operator such as the power mutation, Uniform [153], Gussian [154], shrink [155], supervised mutation [156], uniqueness mutation [157], and varying probability mutation [158–160].

Binary Particle Swarm Optimization. Binary Particle Swarm Optimization (BPSO) is a wrapper method. The PSO technique is a population-based algorithm, where each individual in a population corresponds to a particle. Each particle represents a candidate solution to the problem at hand. Particles change their positions by flying around in a multidimensional search space until a relatively unchanged position has been found, or until computational limitations are exceeded. Each particle has its fitness evaluated by a fitness function. A particle fitness value is called a personal best $pbest$ solution achieved so far. The particle, which has the best solution among all $pbest$, is called the global best particle $gbest$ [161, 162]. A particle velocity and position update can be described as follows :

$$\begin{aligned} v_i^d(t+1) = v_i^d(t) + c_1 r_1 * (pbest_i^d(t) - x_i^d(t))) \\ + c_2 r_2 * (gbest^d(t) - x_i^d(t)) \end{aligned} \tag{7}$$

$$x_i^d(t+1) = x_i^d(t) + v_i^d(t+1) \tag{8}$$

Here, d is the particle dimension, t is the iteration, $r1$ and $r2$ are random number in the interval $(0, 1)$, and $c1$ and $c2$ are positive acceleration constants.

An improved Binary Particle Swarm Optimization:. An Improved Binary Particle Swarm Optimization technique (IBPSO) is a solution proposed to improve the BPSO technique. This IBPSO technique aims to prevent particles from getting trapped in a local optimum by introducing a boolean algebra operation. In fact, it assumes that the particles have fallen into the local optimum when the $gbest$ values are unchanged after three generations. The particles have to be induced to leave the local optimum using the 'and logical operation' *'and'* $pbest$ of all particles [163, 164].

IBPSO+IG. The Improved Binary Particle Swarm Optimization and Information Gain technique (IBPSO+IG) is a hybrid solution to enhance the IBPSO technique. This hybrid solution combines filter and wrapper feature selection methods. First, IG is used to calculate the importance of each feature with respect to the class. Then, to effectively remove usefulness features, the traditional BPSO and the improved BPSO wrapper methods are used to select the features again [163].

6.2. Supervised ML Approaches

The supervised approaches are predictive models developed based on a labeled training dataset that contains normal and anomalous data instances. New data instances are compared with the model to determine which class they belong to. There are several supervised machine learning algorithms such as linear classifier, K-Nearest Neighbor (KNN), Decision Tree, and Artificial Neural Network [165, 166].

Linear classifier.

Logistic regression The logistic regression is a predictive analysis. This technique is used to conduct the analysis when the dependent variable is binary. It is a statistical way of modeling a binomial outcome. The outcome can be 0 or 1, which performs a binary classification of positive class from negative one. It uses a sigmoid curve to output a probability value and, thus, performs a classification [167]. Its hypothesis function is as follows :

$$h(x) = S(w_0 + w_0 x_1 + ...w_n x_n) \quad (9)$$

$$S_Z = \frac{1}{1+e^{-z}} \quad (10)$$

$S(w)$ is the sigmoid curve with as output an estimated classification likelihood.

Support Vector Machines The Support Vector Machines (SVM) technique divides the space into planes and finds a separating hyperplanes between them to classify data. Then, a new unseen data point is classified based on which side of the hyperplane it falls. The SVM technique is suitable for medium-sized datasets of features with similar meaning. The advantages of SVM technique are its scalability and its capabilities to perform real-time intrusion detection and update the training patterns dynamically [168–170]

Naive Bayes It is a probabilistic machine learning model. This classifier is based on the Bayes theorem. It learns parameters by considering that the value of each feature is independent of the other features given the class variable. Then, it collects simple per-class statistics from each feature. This classification technique is faster in training compared to the other linear classifiers and it is good for very large datasets and high-dimensional data. However, it often provides the worst generalization and accuracy performances of the linear classifier techniques [171, 172].

K-Nearest Neighbor. It builds the model by storing the training dataset. To make a prediction for a new unseen data point, it finds the closest data points in the training dataset, which is considered as the nearest neighbors. This technique is generally used with small datasets [173, 174].

Decision Tree. Learning a decision tree means learning the sequence questions that gets us to the answer most quickly. These questions are called tests. A decision tree is a flowchart-like structure in which each internal node represents a test on an attribute. Each branch represents the test outcome, and each leaf node (i.e., terminal node) represents a class label. The paths from root (i.e., the entire sample) to leaf (i.e., terminal node) represent the classification rules. This technique is simple to interpret. However, it requires high computation, it is often relatively inaccurate, and unstable (i.e., a small change in the data can lead to a large change in the structure of the optimal decision tree) [175].

Artificial Neural Network. This technique is a brain-inspired system, which mimic the way humans learn. The neural networks consists of the artificial neuron called perceptron. Neural networks have input and output layers, as well as hidden layers consisting of units that transform the input into results the output layer can use. This technique can be viewed as linear models generalizations that perform multiple stages of processing to come to a decision [176].

6.3. Unsupervised ML Approaches

Unsupervised approaches associated no explicit labels with the training dataset. It aims to learn about data by modeling the structure and the distribution of the data. There are several unsupervised machine learning algorithms such as K-means clustering, Hidden Markov Model, and Fuzzy Logic [177].

K-means Clustering. The k-means clustering method was leveraged in WSN for intrusion detection to enhance security in IoT systems [178, 179]. This method aims to generate k clusters from a given dataset by iteratively allocating each data point according to the existing features to one of the k clusters. As a result, each cluster will hold samples with similar features. Indeed, the k centroids, which define the clusters centers, are estimated. Then, each data point is assigned to its nearest cluster centroid using the square Euclidean distance. After that, the cluster centroids are recalculated by computing all the samples mean assigned to that cluster. These steps are iterated until no sample that can modify the clusters exists. It is clear that this method depends on specifying the parameter k, which defines the clusters number, before executing the algorithm [180].

Hidden Markov Model. The Hidden Markov Model (HMM) method is a probabilistic model with mathematical structure. It is designed by a state sequence that has the Markovian property and an observation sequence where each symbol is emitted by the current state. In this method, the set of states are connected by transition probabilities and the states are from a first order Markov chain. Many extensions have been proposed in the literature in order to boost this method, such as the Higher-Order HMMs (HOHMM) and the Student's t-Mixture Model (SMM). The HMM is able to capture the dependencies between the consecutive sequences and it is considered as a readable probabilistic graph model. However, it has an important computational complexity and many of its parameters are freely estimated [181, 182].

Fuzzy Logic. This method is able to deal with uncertainty; therefore, it has been widely used for network threats detection. It is a useful method when decision should be made based on non-numerical and imprecise information. The Fuzzy logic systems rely in their decisions on inputs in the form of linguistic variables derived from membership functions. Membership functions are formulas used to define the fuzzy set to which a value belongs and the membership degree in that set. Fuzzification operations in this method map mathematical input values into fuzzy membership functions. However, the defuzzification operations map a fuzzy output membership function into a continuous variable that can be used for decision purposes. This method has been used in correlation with IDS. However, the fuzzy logic is not enough to detect all attack types. It should be combined with other classifiers to perform well [183, 184].

6.4. Semi-Supervised ML Approaches

With semi-supervised approaches, the training data instances contain only labels for normal class. Data instances are not labeled for the anomalous class. Semi-supervised approaches allocate great interest in machine learning because it can exploit available unlabeled data to improve supervised learning tasks when the labeled data are expensive or scarce. The most common semi-supervised algorithms are the Expectation–Maximization [185] with generative mixture models [186], and the transductive SVM algorithm [187–189].

7. Related Surveys

This section introduced the related works that survey and overview the intrusion detection techniques using machine learning algorithms in the IoT network by highlighting their main contributions. There are many surveys that discuss the intrusion detection, privacy and security issues for IoT. Despite the various research works dealing with intrusion detection systems, it is still infancy for IoT applications. As far as we know, there are scarce investigations focused on over-viewing intrusion detection using machine learning mechanisms for IoT network. We focused on intrusion detection for IoT network using machine learning algorithms in this paper. In order to compare our survey to the existing IoT network overviews and surveys, table 3 sets side by side our survey work and other recent works that study security issues and intrusion detection in the IoT network.

8. Conclusion

IoT is a technology trend that enables new protocols, applications and services. It is able to connect a large number of physical objects to the Internet, and produces extensive data traffic in the network. However, the IoT traffic could be leveraged to conceive malicious activities. Indeed, IoT systems have some security flaws and vulnerabilities, the commonest of which is that when attackers may misuse this emerging technology to threaten users' privacy. Therefore, security issues cannot be neglected and IoT security solutions should be developed. This paper elaborated taxonomy of the IoT security challenges and attacks, and highlighted the open issues in IoT security. It surveyed and provided taxonomy of various intrusion detection methods that are possible to mitigate different attacks. The intrusion detection techniques are classified into three types based on the detection mechanism: signature-based IDS, anomaly-based IDS, and specification-based IDS. Signature based IDS can detect all known attacks based on their signatures. However, with anomaly-based IDS, the IDS builds a normal activity profile, which represents the normal behaviors that are accepted in the network system. Then, it becomes able to trigger alert in anomaly detection, which mismatch the normal behavior. The specification-based IDS technique exploits the benefits of both signature and anomaly-based detection techniques. It attempts, then, to detect known as well as unknown attacks. Machine learning is a field in the artificial intelligence (AI), which has been already applied in multiple disciplines and can bring a potential benefit to the IoT security systems. Accordingly, this paper presented a comprehensive study of different machine leaning methods used for intrusion detection in the IoT network context. These methods could be classified into three categories based on the availability of labeled data traffic: supervised, unsupervised, and semi-supervised methods.

References

[1] Statista Research Department (2016), Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025, Available at https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. Online; accessed 19 March 2020.

[2] Malik, A. and Om, H. (2017) Cloud computing and internet of things integration: Architecture, applications, issues, and challenges. *Sustainable Cloud and Energy Services* : 1–24.

[3] Kaur, K., Garg, S., Aujla, G.S., Kumar, N., Rodrigues, J.J. and Guizani, M. (2018) Edge computing in the industrial internet of things environment: Software-defined-networks-based edge-cloud interplay. *IEEE communications magazine* **56**: 44–51.

[4] Stergiou, C., Psannis, K.E., Kim, B.G., and Gupta, B. (2018) Secure integration of iot and cloud computing. *Future Generation Computer Systems* **78**: 964–975.

Table 3. Recent surveys on IoT security.

	Authors and Publication Date	Studied Points
Surveys and overviews on Intrusion Detection	N. A. Azeez and al. Date 2020 [190]	- It provides an update overview of the intrusion detection systems. - It discusses the use of the IDS to detect and identify vulnerabilities. - It studies the prevention mechanisms applied to avoid intrusion.
	A. Ahmim and al. Date 2020 [191]	- It studies some supervised machine learning schema for IDS. - It surveys intrusion detection systems and their mechanisms. - It reviews common public data sets used in experiments.
	K. A.P. da Costa and al. Date 2019 [192]	- It overviews research progress in security-related issues in IoT environments. - It discusses methods based on machine learning and evolutionary computation.
	D. Kumar and al. Date 2019 [193]	- It presents comprehensive investigation of security for IoT systems. - It proposes a taxonomy for the IoT ecosystem. - It provides state-of-the-art attacks on IoT systems and their defenses.
	C. Patel and al. Date 2019 [194]	- It discusses security challenges for IoT. - It examines cyber threats, attacks and security solutions for IoT.
	N. Chaabouni and al. Date 2019 [195]	- It identifies and classifies IoT threats. - It studies and compare intrusion detection systems based on machine learning techniques.
	A.Mudassar and al. Date 2019 [196]	- It discusses the generic architecture of IoT and protocols. - It surveys IoT security challenges and issues.
	S. Deep and al. Date 2019 [197]	- It examines security and privacy issues at each layer of the IoT system. - It overviews the existing security solutions for IoT.
	L.Deng and al. Date 2018 [198]	- It overviews the IoT network security issues. - It discusses some intrusion detection technologies and compares between them.
	E. Benkhelifa and al. Date 2018 [199]	- It discusses protocols and technologies of the IoT system. - It studies Intrusion Detection Systems (IDS) architecture. - It identifies security issues in IoT architectures and examines some proposed solutions.
	N. Zhang and al. Date 2017 [200]	- It provides a large-scale empirical analysis of 83M IoT devices in 16M real-world homes. - It analyzed the security profile of different IoT devices and networks. - It describes the current landscape of IoT devices and their security posture.
	Z.A.Khan and al. Date 2017 [114]	- It examines the trust based intrusion detection mechanism for IoT used to allow nodes building trust relation with their adjacent nodes, which guide the messages routing through the network. - It proposes a design and evaluation for intrusion detection system mechanisms for IoT that uses a trust management technique to detect intruder nodes.
	B.B.Zarpelão and al. Date 2017 [201]	- It surveys the IDS research work for IoT. - It proposes a classification of intrusion detection systems based on their placement strategy, detection technique and security threat.
Our contribution	H.Mliki and al. Date 2020	- This paper studies network technologies and services at each layer in the basic IoT model. - Elaborates a taxonomy of the IoT security challenges and attacks. - Surveys the existing intrusion detection mechanisms for the IoT network and elaborates a taxonomy to classify these mechanisms. - Develops a comprehensive study of different machine learning methods used for intrusion detection in the IoT network context.

[5] Fu, J.S., Liu, Y., Chao, H.C., Bhargava, B.K. and Zhang, Z.J. (2018) Secure data storage and searching for industrial iot by integrating fog computing and cloud computing. *IEEE Transactions on Industrial Informatics* **14**: 4519–4528.

[6] Kaur, K. (2018) A survey on internet of things–architecture, applications, and future trends. *First International Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar, India* : 581–583.

[7] Ammar, M., Russello, G. and Crispo, B. (2018) Internet of things: A survey on the security of iot frameworks. *Journal of Information Security and Applications* **38**: 8–27.

[8] Cui, L., Yang, S., Chen, F., Ming, Z., Lu, N. and Qin, J. (2018) A survey on application of machine learning for internet of things. *International Journal of Machine Learning and Cybernetics* **9**: 1399–1417.

[9] Aswale, P., Shukla, A., Bharati, P., Bharambe, S. and Palve, S. (2018) An overview of internet of things: Architecture, protocols and challenges. *Information and Communication Technology for Intelligent Systems. Smart Innovation, Systems and Technologies* **106**: 299–308.

[10] Muccini, H. and Moghaddam, M.T. (2018) Iot architectural styles. *Software Architecture. ECSA 2018. Lecture Notes in Computer Science* **11048**: 68–85.

[11] Verma, H. and Chahal, K. (2017) A review on security problems and measures of internet of things. In *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)*: 71–76.

[12] chaari Fourati, L., Fourati, M. and Benmnaouer, A. (2018) Security challenges against cognitive iot development. In *2018 14th International Wireless Communications Mobile Computing Conference (IWCMC)*: 1069–1073.

[13] for Information technology, I.S. (2006) *Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*. Tech. rep., Telecommunications and information exchange between systems—Local and metropolitan area networks— Specific requirements.

[14] Yen, L.H. and Tsai, W.T. (2010) The room shortage problem of tree-based zigbee/ieee 802.15.4 wireless networks. *Computer Communications* **33**: 454–462.

[15] Haddara, M. and AnnaStaaby (2018) Rfid applications and adoptions in healthcare: A review on patient safety. *Procedia Computer Science* **138**: 80–88.

[16] Li, C.T., Lee, C.C., Weng, C.Y. and Chen, C.M. (2018) Towards secure authenticating of cache in the reader for rfid-based iot systems. *Peer-to-Peer Networking and Applications* **11**: 198–208.

[17] Park, S.S. (2018) An iot application service using mobile rfid technology. *International Conference on Electronics, Information, and Communication (ICEIC), Honolulu, HI, USA* : 1–4.

[18] ren Lin, J., Talty, T. and Tonguz, O.K. (2015) On the potential of bluetooth low energy technology for vehicular applications. *IEEE Communications Magazine* **53**(1): 267–275.

[19] Raza, S., Misra, P., He, Z. and Voigt, T. (2017) Building the internet of things with bluetooth smart. *Ad Hoc Networks* **57**: 19–31.

[20] Collotta, M., Pau, G., Talty, T. and Tonguz, O.K. (2018) Bluetooth 5: A concrete step forward toward the iot. *IEEE Communications Magazine* **56**(7): 125–131.

[21] Fürst, J., Chen, K., Kim, H.S. and Bonnet, P. (2018) Evaluating bluetooth low energy for iot. In *2018 IEEE Workshop on Benchmarking Cyber-Physical Networks and Systems (CPSBench)*: 1–6.

[22] Hasan, K., Biswas, K., Ahmed, K., S.Nafi, N. and Islam, M.S. (2019) A comprehensive review of wireless body area network. *Journal of Network and Computer Applications* **143**: 178–198.

[23] Nabila, A. and Mohamed, E.B. (2019) A qos based comparative analysis of the ieee standards 802.15.4 802.15.6 in wban-based healthcare monitoring systems. In *2019 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)*: 1–5.

[24] minh Linh An, P. and Kim, T. (2018) A study of the z-wave protocol: Implementing your own smart home gateway. In *2018 3rd International Conference on Computer and Communication Systems (ICCCS)*: 411–415.

[25] Naidu, G.A. and Kumar, J. (2019) Wireless protocols: Wi-fi son, bluetooth, zigbee, z-wave, and wi-fi. In K, S.H.S.R.K.G.R.G.S. [ed.] *Innovations in Electronics and Communication Engineering* (Springer, Singapore), **65**, chap. Lecture Notes in Networks and Systems, 229–239.

[26] Lavric, A. and Petrariu, A.I. (2018) Lorawan communication protocol: The new era of iot. In *2018 International Conference on Development and Application Systems (DAS)*: 74–77.

[27] Haxhibeqiri, J., Poorter, E.D., Moerman, I. and Hoebeke, J. (2018) A survey of lorawan for iot: From technology to application. *Sensors* **18**: 1–38.

[28] Jalaian, B., Gregory, T., Suri, N., Russell, S., Sadler, L. and Lee, M. (2018) Evaluating lorawan-based iot devices for the tactical military environment. In *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*: 124–128.

[29] Mekki, K., Bajic, E., Chaxel, F. and Meyer, F. (2018) Overview of cellular lpwan technologies for iot deployment: Sigfox, lorawan, and nb-iot. In *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*: 197–202.

[30] Ayoub, W., Samhat, A.E., Nouvel, F., Mroue, M. and Prévotet, J.C. (2019) Internet of mobile things: Overview of lorawan, dash7, and nb-iot in lpwans standards and supported mobility. *IEEE Communications Surveys Tutorials* **21**(2): 1561–1581.

[31] Lavric, A., Petrariu, A.I. and Popa, V. (2019) Sigfox communication protocol: The new era of iot? In *2019 International Conference on Sensing and Instrumentation in IoT Era (ISSI)*: 1–4.

[32] Mekki, K., Bajic, E., Chaxel, F. and Meyer, F. (2018) Overview of cellular lpwan technologies for iot deployment: Sigfox, lorawan, and nb-iot. In *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*: 197–202.

[33] Khalifeh, A., Aldahdouh, K.A., Darabkh, K.A. and Al-Sit, W. (2019) A survey of 5g emerging wireless technologies featuring lorawan, sigfox, nb-iot and lte-m. In *2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET)*: 561–566.

[34] Osman, N.I. and Abbas, E.B. (2018) Simulation and modelling of lora and sigfox low power wide area network technologies. In *2018 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)*: 1–5.

[35] Chere, M., Ngqondi, T. and Bembe, M. (2019) Wireless low power area networks in the internet of things: A glimpse on 6lowpan. In *2019 International Conference on Electronics, Information, and Communication (ICEIC)*: 1–10.

[36] Nikshepa and Pai, V. (2018) 6LowPan—performance analysis on low power networks. In S., S. and I., B.R.C.J.K. [eds.] *International Conference on Computer Networks and Communication Technologies* (Springer, Singapore), **15**, chap. Lecture Notes on Data Engineering and Communications Technologies, 145–156.

[37] Al-Kashoash, H.A.A., Kharrufa, H., Al-Nidawi, Y. and Kemp, A.H. (2019) Congestion control in wireless sensor and 6lowpan networks: toward the internet of things. *Wireless Networks* **25**: 493–4522.

[38] Witwit, A.J.H. and Idrees, A.K. (2018) A comprehensive review for rpl routing protocol in low power and lossy networks. In mamory S., A. and A., A.J.H. [eds.] *New Trends in Information and Communications Technology Applications* (Springer, Cham), **938**, chap. Communications in Computer and Information Science, 50–66.

[39] Ghaleb, B., Al-Dubai, A.Y., Ekonomou, E., Alsarhan, A., Nasser, Y., Mackenzie, L.M. and Boukerche, A. (2019) A survey of limitations and enhancements of the ipv6 routing protocol for low-power and lossy networks: A focus on core operations. *IEEE Communications Surveys Tutorials* **21**(2): 1607–1635.

[40] Higginbotham, S. (2018) Wi-fi vs. internet of things [internet of everything]. *IEEE Spectrum* **55**(4): 22–22.

[41] Qiao, L., Zheng, Z., Cui, W. and Wang, L. (2018) A survey on wi-fi halow technology for internet of things. In *2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2)*: 1–5.

[42] Li, S., Xu, L.D. and Zhao, S. (2018) 5g internet of things: A survey. *Journal of Industrial Information Integration* **10**: 1–9.

[43] Jameel, F., Hamid, Z., Jabeen, F., Zeadally, S. and Javed, M.A. (2018) A survey of device-to-device communications: Research issues and challenges. *IEEE Communications Surveys Tutorials* **20**(3): 2133–2168.

[44] Iglesias-Urkia, M., Orive, A., Urbieta, A. and Casado-Mansilla, D. (2019) Analysis of coap implementations for industrial internet of things: a survey. *Journal of Ambient Intelligence and Humanized Computing* **10**: pages2505–2518.

[45] Çorak, B.H., Okay, F.Y., Güzel, M., Şahin Murt and Ozdemir, S. (2018) Comparative analysis of iot communication protocols. In *2018 International Symposium on Networks, Computers and Communications (ISNCC)*: 1–6.

[46] Ansari, D.B., Atteeq-Ur-Rehman and Mughal, R.A. (2018) Internet of things (iot) protocols: A brief exploration of mqtt and coap. *International Journal of Computer Applications* **179**(27): 9–14.

[47] Gündoğan, C., Kietzmann, P., Lenders, M., Petersen, H., Schmidt, T.C. and Wählisch, M. (2018) Ndn, coap, and mqtt: a comparative measurement study in the iot. *Proceedings of the 5th ACM Conference on Information-Centric Networking* : 159–171.

[48] Yassein, M.B., Shatnawi, M.Q., Aljwarneh, S. and Al-Hatmi, R. (2017) Internet of things: Survey and open issues of mqtt protocol. In *2017 International Conference on Engineering MIS (ICEMIS)*: 1–6.

[49] Pardo-Castellote, G. (2003) Omg data-distribution service: architectural overview. In *23rd International Conference on Distributed Computing Systems Workshops, 2003. Proceedings.*: 200–206.

[50] Auliva, R.S., Sheu, R.K., Liang, D. and Wang, W.J. (2018) Iiot testbed: A dds-based emulation tool for industrial iot applications. In *2018 International Conference on System Science and Engineering (ICSSE)*: 1–4.

[51] Ahemd, M.M., Shah, M.A. and Wahid, A. (2017) Iot security: A layered approach for attacks and defenses. In *2017 International Conference on Communication Technologies (ComTech)*: 104–110.

[52] Adat, V. and Gupta, B.B. (2018) Security in internet of things: issues, challenges, taxonomy, and architecture. *Telecommunication Systems* **67**: 423–441.

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

[54] Kumar, S., Sahoo, S., Mahapatra, A., Swain, A.K. and Mahapatra, K. (2017) Security enhancements to system on chip devices for iot perception layer. In *2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*: 151–156.

[55] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H. and Zhao, W. (2017) A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal* **4**(5): 1125–1142.

[56] Deogirikar, J. and Vidhate, A. (2017) Security attacks in iot: A survey. In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*: 32–37.

[57] Zhang, K., Liang, X., Lu, R. and Shen, X. (2014) Sybil attacks and their defenses in the internet of things. *IEEE Internet of Things Journal* **1**(5): 372–383.

[58] Gupta, B.B., Arachchilage, N.A.G. and Psannis, K.E. (2018) Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems* **67**: 247–267.

[59] Rizvi, S., Orr, R., Cox, A., Ashokkumar, P. and R.Rizvi, M. (2020) Identifying the attack surface for iot network. *Internet of Things* **9**: 1–30.

[60] Berger, S., Bürger, O. and Röglinger, M. (2020) Attacks on the industrial internet of things – development of a multi-layer taxonomy. *Computers and Security* : 1–41.

[61] Patel, C. and Doshi, N. (2018) Security challenges in iot cyber world. In A., H.A.E.M.A.S.S. [ed.] *Security in Smart Cities: Models, Applications, and Challenges* (Springer, Cham), chap. Lecture Notes in Intelligent Transportation and Infrastructure, 171–191.

[62] Alqassem, I. and Svetinovic, D. (2014) A taxonomy of security and privacy requirements for the internet of things (iot). In *2014 IEEE International Conference on Industrial Engineering and Engineering Management*: 1244–1248.

[63] Oh, S.R. and Kim, Y.G. (2017) Security requirements analysis for the iot. In *2017 International Conference on Platform Technology and Service (PlatCon)*: 1–6.

[64] Zhou, J., Cao, Z., Dong, X. and Vasilakos, A.V. (2017) Security and privacy for cloud-based iot: Challenges. *IEEE Communications Magazine* **55**(1): 26–33.

[65] Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A. and Kikiras, P. (2015) On the security and privacy of internet of things architectures and systems. In *2015 International Workshop on Secure Internet of Things (SIoT)*: 49–57.

[66] Minoli, D., Sohraby, K. and Kouns, J. (2017) Iot security (iotsec) considerations, requirements, and architectures. In *2017 14th IEEE Annual Consumer Communications Networking Conference (CCNC)*: 1006–1007.

[67] Elaguech, M., Kchaou, A., Youssef, W.E.H., Othman, K.B. and Machhout, M. (2019) Performance evaluation of lightweight block ciphers in soft-core processor. In *2019 19th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*: 101–105.

[68] Xiao-Mei, L. and Yong, Q. (2019) Research on led lightweight cryptographic algorithm based on rfid tag of internet of things. In *2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*: 1717–1720.

[69] Avoine, G., Bingöl, M.A., Carpent, X. and Yalcin, S.B.O. (2013) Privacy-friendly authentication in rfid systems: On sublinear protocols based on symmetric-key cryptography. *IEEE Transactions on Mobile Computing* **12**(10): 2037–2049.

[70] Wang, C., Wang, D., Tu, Y., Xu, G. and Wang, H. (2020) Understanding node capture attacks in user authentication schemes for wireless sensor networks. *IEEE Transactions on Dependable and Secure Computing* : 1–1.

[71] SWEENEY, L. (2002) k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* **10**(5): 557–570.

[72] Ozdemir, S. and Xiao, Y. (2011) Integrity protecting hierarchical concealed data aggregation for wireless sensor networks. *Computer Networks* **55**: 1735–1746.

[73] Acharya, R. and Asha., K. (2008) Data integrity and intrusion detection in wireless sensor networks. In *2008 16th IEEE International Conference on Networks*: 1–5.

[74] Mo, Y., Kim, T.H.J., Brancik, K., Dickinson, D., Lee, H., Perrig, A. and Sinopoli, B. (2012) Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE* **100**(1): 195–209.

[75] Airehrour, D., Gutierrez, J. and Ray, S.K. (2016) Secure routing for internet of things: A survey. *Journal of Network and Computer Applications* **66**: 198–213.

[76] Kamble, A., Malemath, V.S. and Patil, D. (2017) Security attacks and secure routing protocols in rpl-based internet of things: Survey. In *2017 International Conference on Emerging Trends Innovation in ICT (ICEI)*: 33–39.

[77] Zhu, Y. and Zhou, D. (2020) Security technology of wireless sensor network based on ipsec. In O., X.Z.P.R.H.M.L.G. [ed.] *Cyber Security Intelligence and Analytics* (Springer, Cham), **1146**, chap. Advances in Intelligent Systems and Computing, 92–97.

[78] Cervantes, C., Poplade, D., Nogueira, M. and Santos, A. (2015) Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things. In *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*: 606–611.

[79] Liu, Y., Ma, M., Xiong, N.N., Liu, A. and Zhu, Y. (2020) Design and analysis of probing route to defense sink-hole attacks for internet of things security. *IEEE Transactions on Network Science and Engineering* **7**(1): 356–372.

[80] Taghanaki, S.R., Jamshidi, K. and Bohlooli, A. (2019) Deem: A decentralized and energy efficient method for detecting sinkhole attacks on the internet of things. In *2019 9th International Conference on Computer and Knowledge Engineering (ICCKE)*: 325–330.

[81] Tahir, S., Bakhsh, S.T. and Alsemmeari, R.A. (2019) An intrusion detection system for the prevention of an active sinkhole routing attack in internet of things. *International Journal of Distributed Sensor Networks* **15**: 1–10.

[82] Ahmad, Z., Abbasi, M.H., Khan, A., Mall, I.S., Khan, M.F.N. and Sajjad, I.A. (2020) Design of iot embedded smart energy management system. In *2020 International Conference on Engineering and Emerging Technologies (ICEET)*: 1–5.

[83] Langendörfer, J.M.B..A.S..M.V.M..D.G..P. (2015) Smartie project: Secure iot data management for smart cities. In *2015 International Conference on Recent Advances in Internet of Things (RIoT)*: 1–6.

[84] Novo, O. (2019) Scalable access management in iot using blockchain: A performance evaluation. *IEEE Internet of Things Journal* **6**(3): 4694–4701.

[85] Chen, L., Thombre, S., Järvinen, K., Lohan, E.S., Alén-Savikko, A., Leppäkoski, H., Bhuiyan, M.Z.H. *et al.* (2017) Robustness, security and privacy in location-based services for future iot: A survey. *IEEE Access* **5**: 8956–8977.

[86] Zhang, P., Nagarajan, S.G. and Nevat, I. (2017) Secure location of things (slot): Mitigating localization spoofing attacks in the internet of things. *IEEE Internet of Things Journal* **4**(6): 2199–2206.

[87] Gope, P., Amin, R., Islam, S., Kumar, N. and Bhalla, V.K. (2018) Lightweight and privacy-preserving rfid authentication scheme for distributed iot infrastructure with secure localization services for smart city environment. *Future Generation Computer Systems* **83**: 629–637.

[88] Ahmed, F. (2019) Self-organization: A perspective on applications in the internet of things. In KC., L.X.W. [ed.] *Natural Computing for Unsupervised Learning* (Springer, Cham), chap. Unsupervised and Semi-Supervised Learning, 51–64.

[89] Athreya, A.P. and Tague, P. (2013) Network self-organization in the internet of things. In *2013 IEEE International Workshop of Internet-of-Things Networking and Control (IoT-NC)*: 25–33.

[90] Rao, T.A. and ul Haq, E. (2018) Security challenges facing iot layers and its protective measures. *International Journal of Computer Applications* **179**: 1–5.

[91] Nurse, J.R., Creese, S. and Roure, D.D. (2017) Security risk assessment in internet of things systems. *IT Professional* **19**(5): 20–26.

[92] Wang, T. (2019) The information security risk assessment model based on improved electre method. *Proceedings of the 2019 7th International Conference on Information Technology: IoT and Smart City* : 570–574.

[93] Maheshwari, N. and Dagale, H. (2018) Secure communication and firewall architecture for iot applications. In *2018 10th International Conference on Communication Systems Networks (COMSNETS)*: 328–335.

[94] Gupta, N., Naik, V. and Sengupta, S. (2017) A firewall for internet of things. In *2017 9th International Conference on Communication Systems and Networks (COMSNETS)*: 411–412.

[95] Gaurav, A., Kumar, S.S. and Chetan, A. (2017) International journal of advanced research in computer science. *International Journal of Advanced Research in Computer Science* **8**: 499–50.

[96] Taher, K.A., Jisan, B.M.Y. and Rahman, M.M. (2019) Network intrusion detection using supervised machine learning technique with feature selection. In *2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST)*: 643–646.

[97] Ernst, J., Hamed, T. and Kremer, S. (2018) A survey and comparison of performance evaluation in intrusion detection systems. In K, D. [ed.] *Computer and Network Security Essentials* (Springer, Cham), 555–568.

[98] Hubballi, N. and Suryanarayanan, V. (2014) False alarm minimization techniques in signature-based intrusion detection systems: A survey. *Computer communications* **49**: 1–17.

[99] Bhuyan, M.H., Bhattacharyya, D.K. and Kalita, J.K. (2014) Network anomaly detection: Methods, systems and tools. *IEEE Communications Surveys Tutorials* **16**(1): 303–336.

[100] Patcha, A. and Jung-MinPark (2007) An overview of anomaly detection techniques: Existing solutions

and latest technological trends. *Computer Networks* **51**: 3448–3470.

[101] P.García-Teodoro, J.Díaz-Verdejo, G.Maciá-Fernández and E.Vázquez (2009) Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers and Security* **28**: 18–28.

[102] Aydin, M.A., Zaim, A.H. and Ceylan, K.G. (2009) A hybrid intrusion detection system design for computer network security. *Computers and Electrical Engineering* **35**: 517–526.

[103] Alem, S., Espes, D., Martin, E., Nana, L. and Lamotte, F.D. (2019) A hybrid intrusion detection system in industry 4.0 based on isa95 standard. In *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*: 1–8.

[104] Chandak, T., Ghorpade, C. and Shukla, S. (2019) Effective analysis of feature selection algorithms for network based intrusion detection system. In *2019 IEEE Bombay Section Signature Conference (IBSSC)*: 1–5.

[105] Shin, M.S., Kim, E.H. and Ryu, K.H. (2004) False alarm classification model for network-based intrusion detection system. In Yang Z.R., Yin H., E.R. [ed.] *Intelligent Data Engineering and Automated Learning* (Springer, Berlin, Heidelberg), **3177**, chap. Lecture Notes in Computer Science, 259–265.

[106] Kim, D.S. and Park, J.S. (2003) Network-based intrusion detection with support vector machines. In HK, K. [ed.] *Information Networking* (Springer, Berlin, Heidelberg), **2662**, chap. Lecture Notes in Computer Science, 747–756.

[107] Rice, T.R., Seppala, G., Edgar, T., Choi, E., Cain, D. and Mahserejian, S. (2019) Development of a host-based intrusion detection and control device for industrial field control devices. In *2019 Resilience Week (RWS)*, **1**: 105–111.

[108] Ali, F.A.B.H. and Len, Y.Y. (2011) Development of host based intrusion detection system for log files. In *2011 IEEE Symposium on Business, Engineering and Industrial Applications (ISBEIA)*: 281–285.

[109] Vokorokos, L. and Baláž, A. (2010) Host-based intrusion detection system. In *2010 IEEE 14th International Conference on Intelligent Engineering Systems*: 43–47.

[110] Rajput, D. and Thakkar, A. (2019) A survey on different network intrusion detection systems and countermeasure. In N., S.N.P.L.N.H.H.P.N. [ed.] *Emerging Research in Computing, Information, Communication and Applications* (Springer, Singapore), **906**, chap. Advances in Intelligent Systems and Computing, 497–506.

[111] Benkhelifa, E., Welsh, T. and Hamouda, W. (2018) A critical review of practices and challenges in intrusion detection systems for iot: Toward universal and resilient systems. *IEEE Communications Surveys Tutorials* **20**(4): 3496–3509.

[112] Wang, Z. and Zhu, Y. (2017) A centralized hids framework for private cloud. In *2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*: 115–120.

[113] Ahmim, A., Maglaras, L., Ferrag, M.A., Derdour, M. and Janicke, H. (2019) A novel hierarchical intrusion detection system based on decision tree and rules-based models. In *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*: 228–233.

[114] Khan, Z.A. and Herrmann, P. (2017) A trust based distributed intrusion detection mechanism for internet of things. In *2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)*: 1169–1176.

[115] Bernieri, G. and Pascucci, F. (2019) Improving security in industrial internet of things: A distributed intrusion detection methodology. In C., A. [ed.] *Security and Privacy Trends in the Industrial Internet of Things* (Springer, Cham), chap. Advanced Sciences and Technologies for Security Applications, 161–179.

[116] Yu-Fang Zhang, Zhong-Yang Xiong and Xiu-Qiong Wang (2005) Distributed intrusion detection based on clustering. In *2005 International Conference on Machine Learning and Cybernetics*, **4**: 2379–2383 Vol. 4.

[117] Ghaeini, H.R. and Tippenhauer, N.O. (2016) Hamids: Hierarchical monitoring intrusion detection system for industrial control systems. *roceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy* : 103–111.

[118] Sedjelmaci, H., Senouci, S.M. and Ansari, N. (2018) A hierarchical detection and response system to enhance security against lethal cyber-attacks in uav networks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* **48**(9): 1594–1606.

[119] Hajisalem, V. and ShahramBabaie (2018) A hybrid intrusion detection system based on abc-afs algorithm for misuse and anomaly detection. *Computer Networks* **136**: 37–50.

[120] Midi, D., Rullo, A., Mudgerikar, A. and Bertino, E. (2017) Kalis — a system for knowledge-driven adaptable intrusion detection for the internet of things. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*: 656–666.

[121] A.Prayati, Ch.Antonopoulos, T.Stoyanova, T.Stoyanova, C.Koulamas and G.Papadopoulos (2010) A modeling approach on the telosb wsn platform power consumption. *Journal of Systems and Software* **83**: 1355–1363.

[122] Levis, P., Madden, S., Polastre, J., Szewczyk, R., Whitehouse, K., Gay, A.W.D., Hill, J. *et al.* (2005) Tinyos: An operating system for sensor networks. In E., W.W.R.J.A. [ed.] *Ambient Intelligence* (Springer, Berlin, Heidelberg), 115–148.

[123] Sheikh, N.U., Rahman, H., Vikram, S. and AlQahtani, H. (2018) A lightweight signature-based ids for iot environment. *Cryptography and Security* : 1–4.

[124] Li, W., Tug, S., Meng, W. and YuWang (2019) Designing collaborative blockchained signature-based intrusion detection in iot environments. *Future Generation Computer Systems* **96**: 481–489.

[125] Thing, V.L.L. (2017) Ieee 802.11 network anomaly detection and attack classification: A deep learning approach. In *2017 IEEE Wireless Communications and Networking Conference (WCNC)*: 1–6.

[126] Moustafa, N., Turnbull, B. and Choo, K.R. (2019) An ensemble intrusion detection technique based

on proposed statistical flow features for protecting network traffic of internet of things. *IEEE Internet of Things Journal* **6**(3): 4815–4830.

[127] Moustafa, N. and Slay, J. (2015) 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)*: 1–6.

[128] Yavanoglu, O. and Aydos, M. (2017) A review on cyber security datasets for machine learning algorithms. In *2017 IEEE International Conference on Big Data (Big Data)*: 2186–2193.

[129] Prabavathy, S., Sundarakantham, K. and Shalinie, S.M. (2018) Design of cognitive fog computing for intrusion detection in internet of things. *Journal of Communications and Networks* **20**(3): 291–298.

[130] Mliki, H., Kaceam, A.H. and Chaari, L. (2019) Intrusion detection study and enhancement using machine learning. In A., K.S.C.F.C.B.N.H.K. [ed.] *Risks and Security of Internet and Systems* (Springer, Cham), **2026**, chap. Lecture Notes in Computer Science, 263–278.

[131] Krishnaveni, S. and Sivamohan, P.V.K.J. (2020) Anomaly-based intrusion detection system using support vector machine. In B., D.S.L.C.D.S.P. [ed.] *Artificial Intelligence and Evolutionary Computations in Engineering Systems* (Springer, Singapore), **1056**, chap. Advances in Intelligent Systems and Computing, 723–731.

[132] Bostani, H. and Sheikhan, M. (2017) Hybrid of anomaly-based and specification-based ids for internet of things using unsupervised OPF based on mapreduce approach. *Computer Communications* **98**: 52–71.

[133] Choudhary, S. and Kesswani, N. (2019) Cluster-based intrusion detection method for internet of things. In *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*: 1–8.

[134] Jaber, A.N. and Rehman, S.U. (2020) Fcm–svm based intrusion detection system for cloud computing environment. *Cluster Computing* .

[135] Li, J., Qu, Y., Chao, F., Shum, H.P.H., Ho, E.S.L. and Yang, L. (2019) Machine learning algorithms for network intrusion detection. In L., S. [ed.] *AI in Cybersecurity* (Springer, Cham), **151**, chap. Intelligent Systems Reference Library, 151–179.

[136] Khaled, A.A.U. and El-Sayed, M.E.A. (2018) Intrusion detection taxonomy and data preprocessing mechanisms. *Special Section: Soft Computing and Intelligent Systems: Techniques and Applications* **35**(3): 1369–1383.

[137] Liu, C., Liu, Y., Yan, Y. and Wang, J. (2020) An intrusion detection model with hierarchical attention mechanism. *IEEE Access* : 1–1.

[138] Taher, K.A., Jisan, B.M.Y. and Rahman, M.M. (2019) Network intrusion detection using supervised machine learning technique with feature selection. In *2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST)*: 643–646.

[139] Aljawarneh, S., Aldwairi, M. and Yassein, M.B. (2018) Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *Journal of Computational Science* **25**: 152–160.

[140] Labani, M., Moradi, P., Ahmadizar, F. and Jalili, M. (2018) A novel multivariate filter method for feature selection in text classification problems. *Engineering Applications of Artificial Intelligence* **70**: 25–37.

[141] Abdi, H. and Williams, L.J. (2010) Principal component analysis. *WIREs Computational Statistics* **2**: 433–459.

[142] Candès, E.J., Li, X., Ma, Y. and Wright, J. (2009) Robust principal component analysis? *Journal of the ACM* **11**: 1–39.

[143] Hall, M.A. (2000) Correlation-based feature selection of discrete and numeric class machine learning. In *2000 Working Papers* (University of Waikato, Department of Computer Science), chap. Computer Science Working Papers.

[144] Chormunge, S. and Jena, S. (2018) Correlation based feature selection with clustering for high dimensional data. *Journal of Electrical Systems and Information Technology* **5**: 542–549.

[145] Eid, H.F., Hassanien, A.E., hoon Kim, T. and Banerjee, S. (2013) Linear correlation-based feature selection for network intrusion detection model. In A.I., A. and K., H.A.B. [eds.] *Advances in Security of Information and Communication Networks* (Springer, Berlin, Heidelberg), **381**, chap. Communications in Computer and Information Science, 240–248.

[146] Raileanu, L.E. and Stoffel, K. (2004) Theoretical comparison between the gini index and information gain criteria. *Laura Elena Raileanu and Kilian Stoffel* **41**: 77–93.

[147] Roobaert, D., Karakoulas, G. and Chawla, N.V. (2006) Information gain, correlation and support vector machines. In L.A., G.I.N.M.G.S.Z. [ed.] *Feature Extraction* (Springer, Berlin, Heidelberg), **207**, chap. Studies in Fuzziness and Soft Computing, 463–470.

[148] Aydin, M., Butun, I., Bicakci, K. and Baykal, N. (2020) Using attribute-based feature selection approaches and machine learning algorithms for detecting fraudulent website urls. In *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*: 0774–0779.

[149] Choi, S.H. and Chae, H.S. (2014) Feature selection using attribute ratio in nsl-kdd data. *International Conference Data Mining, Civil and Mechanical Engineering, Bali, Indonesia* .

[150] Hutter, M. (2002) Fitness uniform selection to preserve genetic diversity. In *Proceedings of the 2002 Congress on Evolutionary Computation. CEC'02 (Cat. No.02TH8600)*, **1**: 783–788 vol.1.

[151] Syswerda, G. (1989) Uniform crossover in genetic algorithms. *Proceedings of the 3rd International Conference on Genetic Algorithms* : 2–9.

[152] Srinivas, M. and Patnaik, L.M. (1994) Genetic algorithms: a survey. *Computer* **27**(6): 17–26.

[153] Srinivas, M. and Patnaik, L.M. (1994) Adaptive probabilities of crossover and mutation in genetic algorithms. *IEEE Transactions on Systems, Man, and Cybernetics* **24**(4): 656–667.

[154] Hinterding, R. (1995) Gaussian mutation and self-adaption for numeric genetic algorithms. In *Proceedings of 1995 IEEE International Conference on Evolutionary Computation*, **1**: 384–.

[155] higeyoshi Tsutsui and Fujimoto, Y. (1993) Forking genetic algorithm with blocking and shrinking modes (fga). *the 5th International Conference on Genetic Algorithms, Urbana-Champaign, IL, USA* : 206–215.

[156] Oosthuizen, G. (1987) Supergran: a connectionist approach to learning, integrating genetic algorithms and graph induction. *Genetic algorithms and their applications:proceedings of the second International Conference on Genetic Algorithms* : 132–139.

[157] Mauldin., M.L. (1984) Maintaining diversity in genetic search. *AAAI-84 Proceedings* : 247–250.

[158] links open overlay panelCarol A.Ankenbrandt, A. (1991) An extension to the theory of convergence and a proof of the time complexity of genetic algorithms. *Foundations of Genetic Algorithms* **1**: 53–68.

[159] Mirjalili, S. (2019) Genetic algorithm. In *Evolutionary Algorithms and Neural Networks* (Springer, Cham), **780**, chap. Studies in Computational Intelligence, 43–55.

[160] İpek Uysal, E., Demircioğlu, G., Kale, G., Bostanci, E., Güzel, M.S. and Mohammed, S.N. (2019) Network anomaly detection system using genetic algorithm, feature selection and classification. In *2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*: 1–5.

[161] Zhang, X., Zhang, Q., Chen, M., Sun, Y., Qin, X. and Li, H. (2018) A two-stage feature selection and intelligent fault diagnosis method for rotating machinery using hybrid filter and wrapper method. *Neurocomputing* **275**: 2426–2439.

[162] Bansal, J.C. (2018) Particle swarm optimization. In J., B., P., S. and N., P. [eds.] *Evolutionary and Swarm Intelligence Algorithms* (Springer, Cham), **779**, chap. Studies in Computational Intelligence, 11–23.

[163] Lalit, K. and Kumari, B.K. (2019) An improved bpso algorithm for feature selection. In U., K.A.T., I., S. and N., S. [eds.] *Recent Trends in Communication, Computing, and Electronics* (Springer, Singapore), chap. Lecture Notes in Electrical Engineering, 505–513.

[164] Dong, C. and LixinZhao (2019) Sensor network security defense strategy based on attack graph and improved binary pso. *Safety Science* **117**: 81–87.

[165] Singh, A., Thakur, N. and Sharma, A. (2016) A review of supervised machine learning algorithms. In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*: 1310–1315.

[166] Harikrishnakumar, R., Dand, A., Nannapaneni, S. and Krishnan, K. (2019) Supervised machine learning approach for effective supplier classification. In *2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA)*: 240–245.

[167] Collins, M., Schapire, R.E. and Singer, Y. (2002) Logistic regression, adaboost and bregman distances. *Machine Learning* **48**: 253–285.

[168] Hsu, C.W. and Lin, C.J. (2002) A comparison of methods for multiclass support vector machines. *IEEE Transactions on Neural Networks* **13**(2): 415–425.

[169] Drucker, H., Donghui Wu and Vapnik, V.N. (1999) Support vector machines for spam categorization. *IEEE Transactions on Neural Networks* **10**(5): 1048–1054.

[170] Hearst, M.A., Dumais, S.T., Osuna, E., Platt, J. and Scholkopf, B. (1998) Support vector machines. *IEEE Intelligent Systems and their Applications* **13**(4): 18–28.

[171] Amor, N.B., Benferhat, S. and Elouedi, Z. (2004) Naive bayes vs decision trees in intrusion detection systems. *Proceedings of the 2004 ACM symposium on Applied computing* : 420–424.

[172] Lowd, D. and Domingos, P. (2005) Naive bayes models for probability estimation. *Proceedings of the 22nd international conference on Machine learning* : 529–536.

[173] Dudani, S.A. (1976) The distance-weighted k-nearest-neighbor rule. *IEEE Transactions on Systems, Man, and Cybernetics* **SMC-6**(4): 325–327.

[174] C.Bezdek, J., K.Chuah, S. and DavidLeep (1986) Generalized k-nearest neighbor rules. *Fuzzy Sets and Systems* **18**: 237–256.

[175] Safavian, S.R. and Landgrebe, D. (1991) A survey of decision tree classifier methodology. *IEEE Transactions on Systems, Man, and Cybernetics* **21**(3): 660–674.

[176] Abraham, A. (2005) Artificial neural networks. In Sydenham, P.H. and Thorn, R. [eds.] *Handbook of Measuring System Design* (John Wiley and Sons), chap. AI Signal Processing Techniques, 901–908.

[177] Celebi, M.E. and Aydin, K. [eds.] (2016) *Unsupervised Learning Algorithms* (Springer, Cham).

[178] Han, G., Wang, H., Guizani, M., Chan, S. and Zhang, W. (2018) Kclp: A k-means cluster-based location privacy protection scheme in wsns for iot. *IEEE Wireless Communications* **25**(6): 84–90.

[179] Bharti, A.K., Verma, N. and Verma, D.K. (2019) Cluster analysis of iot data based on mapreduce technique. *International Journal of Research and Analytical Reviews (IJRAR)* **6**: 262–269.

[180] Steinley, D. (2010) K-means clustering: A half-century synthesis. *British Journal of Mathematical and Statistical Psychology* **59**: 1–34.

[181] Tamposis, I.A., Theodoropoulou, M.C., Tsirigos, K.D. and Bagos, P.G. (2018) Extending hidden markov models to allow conditioning on previous observations. *Journal of Bioinformatics and Computational Biology* **16**(5): 1–17.

[182] Zheng, Y., Jeon, B., Sun, L., Zhang, J. and Zhang, H. (2018) t-hidden markov model for unsupervised learning using localized feature selection. *IEEE Transactions on Circuits and Systems for Video Technology* **28**: 2586–2598.

[183] Li, J., Qu, Y., Chao, F., Shum, H.P., Ho, E.S. and Yang, L. (2019) Machine learning algorithms for network intrusion detection. In L., S. [ed.] *AI in Cybersecurity* (Springer, Cham), **151**, chap. Intelligent Systems Reference Library, 151–179.

[184] Hamamoto, A.H., Hamamoto, A.H., Carvalho, L.F., Sampaio, L.D.H., Abrao, T. and Proenca, M.L. (2018) Network anomaly detection system using genetic algorithm and fuzzy logic. *Expert Systems with Applications* **92**: 390–402.

[185] Wang, X., Wen, J., Alam, S., Jiang, Z. and Wu, Y. (2016) Semi-supervised learning combining transductive support vector machine with active learning. *Neurocomputing* **173**: 1288–1298.

[186] McLachlan, G.J., Lee, S.X. and Rathnayake, S.I. (2019) Finite mixture models. *Annual review of statistics and its application* **6**: 55–378.

[187] Devi, E.R. and Suganthe, R. (2020) Enhanced transductive support vector machine classification with grey wolf optimizer cuckoo search optimization for intrusion detection system. *Special Issue: Special Issue on Advances in Metaheuristic Optimization Algorithms (AMOA2018)* **32**: 1–11.

[188] Chaaboun, N., Mosbah, M., Zemmari, A. and Faruki, P. (2019) Network intrusion detection for iot security based on learning techniques. *IEEE Communications Surveys Tutorials* **21**(3): 2671–2701.

[189] Idhammad, M., Afdel, K. and Belouch, M. (2018) Semi-supervised machine learning approach for ddos detection. *Applied Intelligence* **48**: 3193–3208.

[190] Azeez, N.A., Bada, T.M., Misra, S., Adewumi, A., der Vyver, C.V. and Ahuja, R. (2020) Intrusion detection and prevention systems: An updated review. In N., S., A., C. and V., B. [eds.] *Data Management, Analytics and Innovation* (Springer, Singapore), **1042**, chap. Advances in Intelligent Systems and Computing, 685–696.

[191] Ahmim, A., Maglaras, M.A.F.L., Derdour, M., Janicke, H. and Drivas, G. (2020) Taxonomy of supervised machine learning for intrusion detection systems. In A., K. and P., K.E.T. [eds.] *Strategic Innovative Marketing and Tourism* (Springer, Cham), chap. Springer Proceedings in Business and Economics, 619–628.

[192] da Costa, K.A., Papa, J.P., Lisboa, C.O., Munoz, R. and de Albuquerque, V.H.C. (2019) Internet of things: A survey on machine learning-based intrusion detection approaches. *Computer Networks* **151**: 147–157.

[193] Kumar, D., Shen, K., Case, B., Garg, D., Alperovich, G., Kuznetsov, D., Gupta, R. *et al.* (2019) All things considered: An analysis of iot devices on home networks. In *28th USENIX Security Symposium (USENIX Security 19)* (Santa Clara, CA: USENIX Association): 1169–1185. URL https://www.usenix.org/conference/usenixsecurity19/presentation/kumar-deepak.

[194] Patel, C. and Doshi, N. (2019) Security challenges in iot cyber world. In A., H., M., E., S., A. and A., S. [eds.] *Security in Smart Cities: Models, Applications, and Challenges* (Springer, Cham), chap. Lecture Notes in Intelligent Transportation and Infrastructure, 171–191.

[195] Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C. and Faruki, P. (2019) Network intrusion detection for iot security based on learning techniques. *IEEE Communications Surveys Tutorials* **21**(3): 2671–2701.

[196] Ahmad, M., Younis, T., Habib, M.A., Ashraf, R. and Ahmed, S.H. (2019) A review of current security issues in internet of things. In M., J., F., K. and M., A. [eds.] *Recent Trends and Advances in Wireless and IoT-enabled Networks* (Springer, Cham), chap. EAI/Springer Innovations in Communication and Computing, 11–23.

[197] Zheng, S.D.X., Jolfaei, A., Yu, D., Ostovari, P. and Bashir, A.K. (2019) A survey of security and privacy issues in the internet of things from the layered context. *CoRR* **abs/1903.00846**. URL http://arxiv.org/abs/1903.00846. 1903.00846.

[198] Deng, L., Li, D., Yao, X., Cox, D. and Wang, H. (2019) Mobile network intrusion detection for iot system based on transfer learning algorithm. *Cluster Computing* **22**: 9889–9904.

[199] Benkhelifa, E., Welsh, T. and Hamouda, W. (2018) A critical review of practices and challenges in intrusion detection systems for iot: Toward universal and resilient systems. *IEEE Communications Surveys Tutorials* **20**(4): 3496–3509.

[200] Zhang, N., Demetriou, S., Mi, X., Diao, W., Yuan, K., Zong, P., Qian, F. *et al.* (2017) Understanding iot security through the data crystal ball: Where we are now and where we are going to be. *CoRR* **abs/1703.09809**. URL http://arxiv.org/abs/1703.09809. 1703.09809.

[201] Zarpelão, B.B., Miani, R.S., Kawakani, C.T. and de Alvarenga, S.C. (2017) A survey of intrusion detection in internet of things. *Journal of Network and Computer Applications* **84**: 25–37.