International Journal of Advanced Engineering Research and Science (IJAERS)
Peer-Reviewed Journal
ISSN: 2349-6495(P) | 2456-1908(O)
Vol-9, Issue-6; Jun, 2022
Journal Home Page Available: https://ijaers.com/
Article DOI: https://dx.doi.org/10.22161/ijaers.96.35

Artificial Intelligence approaches for IoT Security: State of Art

Ismail Chahid, Mohammed Benabdellah

ACSA Laboratory, Faculty of Science, Mohammed 1st University Oujda, Morocco
Email: i.chahid@ump.ac.ma
Email : med_benabdellah@yahoo.fr

Received: 05 Jan 2022,

Received in revised form: 15 May 2022,

Accepted: 21 Jun 2022,

Available online: 28 Jun 2022

Keywords*— *IoT, Machine Learning, Deep Learning, Security, Blockchain.

***Abstract*—** *With an estimation of more than 35 billion interconnected smart devices by the end of 2021, Internet of Things (IoT) is one of the most rapidly growing technologies in the last decade. However, the complexity nature of IoT systems and the exponential amount of data collected and exchanged between Things relieve a big challenge in terms of security and privacy. Implementing classical security measures, such as encryption, authentication, access control, network and application security for IoT devices is no more effective against sophisticated Cyber-attacks. Artificial intelligence (AI) approaches such as Machine Learning (ML), Deep Learning (DL) and Blockchain can be leveraged to enhance the security of IoT and deal with its various problems. In this paper, we will describe the IoT technology and its domain of application, the protocols used to communicate between smart devices, security issues and existing AI solution.*

I. INTRODUCTION

Internet of Things (IoT) is a network of smart devices with the capability of communicating and sharing information over the internet. These smart things can be deployed in many different environments to collect data. The applications domains of IoT are various like smart home, smart city, healthcare, smart transportation system, agriculture and smart grid system. As estimated, there will be more than 35 billion IoT devices connected by the end of 2021. IoT devices can generate exponential data, which make it very difficult in term of processing and storing. Three layers constitute the pillars of IoT architecture. Physical, network, and application layer.

Devices in the physical layer, are embedded with sensors that can detect and interact with the environment. For example, in smart homes, devices like thermostat can help control the home's temperature with no human interaction and it can be adapted according to the user's activity or the temperature outside the house. In a smart hospital, IoT devices can help monitoring hygiene by preventing patients from being infected. IoT technology comes with lots of challenges.

Data storage, standardization, processing, inter-operability, trust management, identity, availability, confidentiality, integrity, security, and privacy are some of the open challenges in various IoT applications [1]. In section 1 of this paper work we will try to describe the IoT technology, its infrastructure and protocols, the vulnerabilities and the different known attacks. Section 2 is where we will give an overview of different known Artificial Intelligence approaches to help enhancing the security of IoT technology.

II. INTERNET OF THINGS (IOT) INFRASTRUCTURE, PROTOCOLS AND APPLICATION

Real time applications can benefit a lot from Internet of Things (IoT). To build an intelligent system IoT need to

integrates radio frequency identification (RFID), sensors, smart devices, and interconnexion between these Things. The IoT has different types of a network like a distributed, ubiquitous, grid, and vehicular. The applications of IoT made a huge impact in day to day life like sensors deploy in the patient body to monitoring in critical condition, monitoring gas leakage in smart kitchen, agriculture field, smart car parking, smart transportation, tracking goods details in supply chain system using sensors in the vehicle. The sensors are resource constraint devices connected through wired or wirelessly across heterogeneous networks. The IoT networks are possessed different security, privacy, and vulnerable to the attacker.

1.1. IoT infrastructure

IoT application consists of different smart things that collect, process, compute and communicate with other smart things. IoT has three layers physical, network, and application layer. Recently industries are developed many things which are embedded with intelligent things. As shown in Fig. 1 IoT infrastructure consists of not only sensors, but it also integrates with some emerging technology. The IoT application is based on either IoT-Cloud or IoT-Fog-Cloud.

The security issue like data privacy [13] , machine to machine communication [14] , real-time monitoring [15] and IoT testbed [16] needs to be addressed for efficient IoT applications. IoT architecture may be centralized, decentralized and distributed structure. IoT applications can face many challenges issues in term of processing and computing in real-time. Cloud computing has emerged as a key technology to provides more storage and data processing and assures security. But as the technology continue to grow, IoT applications start to demand processing and computing in the edge of the network in most of the real-time monitoring. So that quick action can be taken like monitoring the health condition of the serious patient, fire detection. When processing and computing are done on the edge of the network using fog devices, it becomes more vulnerable to the attacker as their devices are lightweight device traditional security is not applicable. During analytic data, a technique like a machine learning is recently used to make the IoT system more intelligent and independent to make a decision. The different smart devices are connected to make an application using some standard protocols. The security issue exists in IoT infrastructure, which needs to be addressed to build trust among end-users and make the system temper-proof. The data interoperability [17] in the IoT system works using an intelligent algorithm.

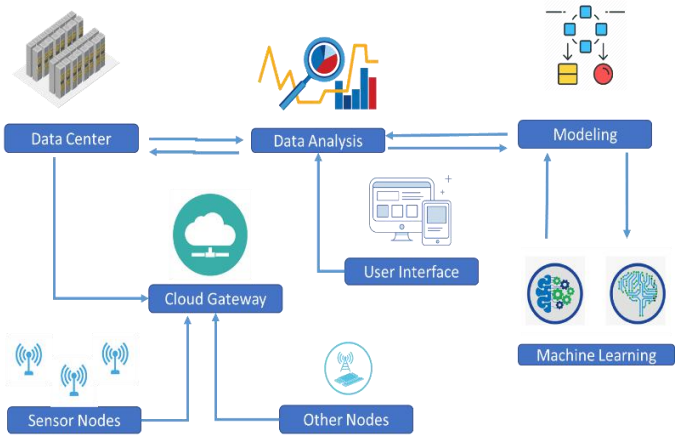

Figure 1. IoT Infrastructure

1.2. IoT Protocols

IoT protocols are the essential characteristics that make interaction and communication possible between things (devices, sensors, servers…). Here some main classic and mostly used IoT protocols:

1.2.1. CoAP

As defined in RFC 7252, Constrained Application Protocol (CoAP), is a specialized Internet Application Protocol for constrained devices. It allows those devices called “nodes” to use similar protocols to communicate with the wider Internet. CoAP is designed to be used between devices on the same restricted network.

1.2.2. TCP

Transmission Control Protocol (TCP) is a connection-oriented communications protocol that provides the facility to ex- change messages in a network between computer devices.

1.2.3. MQTT

MQTT (MQ Telemetry). It is a lightweight, straightforward publish-subscribe network-messaging protocol for devices with low bandwidth and high latency. It usually uses TCP/IP but also can be supported by network protocols that provide ordered, bi-directional and lossless connections. The main goal of the protocol is to reduce the consumption of network bandwidth and resources without degradation of delivery assurance and reliability.

1.2.4. AMQP

An open standard for transferring business messages between applications or organizations is the Advanced Message Queuing Protocol (AMQP). It connects systems, feeds business processes with the information they need, and transmits the instructions that achieve their goals reliably forward.

1.2.5. UDP

A Transport Layer protocol is the User Datagram Protocol (UDP). UDP is part of the Internet Protocol suite, known as UDP / IP. Like TCP, this protocol is unstable and unconnected. There is thus no need to create a link before transferring data.

1.2.6. REST

REST (State Transfer Member) is a software architectural style based on web standards that was created to guide the design and development of the architecture for the World Wide Web. It turns around resources where each element is a resource, and a resource is accessed using standard HTTP methods through a specific interface. Roy Fielding introduced REST in 20 0 0. A REST server offers access to resources in REST architecture, and REST user accesses and modifies resources. Here, URIs / global IDs classify each asset. REST uses a variety of representations to describe a resource such as text, JSON, XML.

1.2.7. DCCP

DCCP provides a way for congestion-control mechanisms to be accessed without having to implement them at the ap- plication layer. It allows flow-based semiconducting, as in the Transmission Control Protocol (TCP), but does not provide reliable delivery on-order. Sequenced transmission across multiple streams is not possible in DCCP, as in the Stream Control Transmission Protocol (SCTP). A DCCP link requires both the network acknowledgment and data traffic. Acknowledgments notify a sender that their packets have arrived and whether they have been labeled with an Explicit Notification of Conges- tion (ECN).

1.2.8. RSVP

The Resource Reservation Protocol (RSVP) is a transport layer [1] protocol designed to use the distributed infrastructure model to reserve resources across a network. RSVP works over an IPv4 or IPv6 and sets up resource reservations for multi- cast or unicast data flows, initiated by the recipient. It does not transmit data from applications but is similar to a control protocol, such as the Internet Control Message Protocol (ICMP) or the Internet Group Management Protocol (IGMP). RSVP is set out in RFC 2205.

1.2.9. SCTP

The Stream Control Transmission Protocol (SCTP) is a computer networking communication protocol that operates at the transportation layer and serves a similar role to the popular TCP and UDP protocols. It is defined in RFC 4960 by IETF.SCTP incorporates some of the features of both UDP and TCP: it is message-oriented like UDP and ensures secure, in-sequence congestion-controlled transmission of messages like TCP. It differs from those protocols by providing multi-homing and redundant paths to increase resilience and reliability.

1.2.10. CLNS

Connectionless mode Network Service (CLNS) or simply Connectionless Network Service is an OSI Network Layer data- gram service that does not require a circuit to be set up before data is transmitted, and routes messages to their destinations independently of any other messages. CLNS is not an Internet service but offers features similar to those offered by the Internet Protocol (IP) and User Datagram Protocol (UDP) in an OSI Network environment.

1.2.11. ICMP

Connectionless-mode Network Service (CLNS) or simply Connectionless Network Service is an OSI Network Layer data- gram service that does not allow a circuit to be set up before data is transmitted and routes messages to their destinations independently of any other messages. As such, it is a best-effort rather than a “reliable” delivery service. CLNS is not an Internet service but offers features similar to those offered by the Internet Protocol (IP) and User Datagram Protocol (UDP) in an OSI Network environment.

1.2.12. ISDN

Integrated Services Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. The key feature of ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system. In the emergency mode of IoT devices, the ISDN facility can be useful.

1.3. Application Domain

IoT applications are nowadays developed in many fields. The development of many open-source platforms like Azure IoT Suite, IBM Watson, Amazon Web Services (AWS), Oracle IoT, Kaa, Bevywise IoT platform used for industrial IoT, IoTIFY cloud-based platform used to build scalable IoT applications. Most of the opensource platform is enabled with AI and ML technology for intelligent processing and computing the information. The manufacture of smart devices that can read, process, and computing the things makes the IoT as one of the emerging fields. There are many application areas where IoT is used. IoT has already made an impact on enhancing and increasing the efficiency of the system.

1.3.1. Smart home

The IoT makes the traditional home system into an intelligent one. The refrigerator, smart television, security camera, gas sensors, temperature sensor, light system all

can sense the home environment, communicate and connect to the internet through wired or wireless. Even the refrigerator can place an order to the registered retail shop and give notification to the user. Due to the development of smart things, the living standard becomes more comfortable. In paper [18], authors design a smart home system based on IoT technology. Using technology like IoT and Fog computing home converted into an intelligent home system where monitoring of the home can be done remotely as well as processing can be done instantly. The authentication of devices is essential to prevent unwanted access to the IoT network. The authors in Satapathy et al. [19] and Panda et al. [20] proposed different authentication schemes for a smart home network. Still, some security issues [21] , are exist in IoT based smart home systems.

1.3.2. Smart hospital

Since the development of IoT patient monitoring in real-time is possible with the use of sensors and fog/edge computing, the paper [22], authors have proposed an IoT-cloud based framework for data collection in the healthcare system. Similarly, in Moosavi et al. [23], authors performed the authentication and authorization of the smart devices in the healthcare system. In the healthcare system, privacy is one of the main issues, so proper security and privacy protocol need to be developed to secure the system.

1.3.3. Smart city

The ever-growing city has lots of problems like traffic management, waste management, waste management, and environmental management. The city needs a solution to monitor and control the problem exist. In papers [24,25], authors explained the challenges that exist in implementing smart cities and done a survey in detail about how IoT can solve an existing problem. Using IoT and associated technology, a smart city can be developed to enhance the living standard of the city, maintaining the security and privacy issue of the citizen.

1.3.4. Smart transportation

In recent times traffic is one of the major problems in a city. The intelligent transportation system is the need of the hour. The IoT enables vehicles can collect information from the roadside unit and process to get the details about journey path, time, and traffic details. Some of the research work [26,27] addressed the smart transportation issue using IoT. In paper [28], the authors proposed the IoT-ITS system for the transportation system. The authors in Dey et al. [29] proposed a “Magtrack” to detect condition of the road surface using in-build mobile sensors and machine learning concepts.

1.3.5. Smart grid

The smart grid is one of the application areas of IoT, where a grid system can be made automation using IoT. The electric power generation and distribution among consumers can be monitor in real-time. The cybersecurity solution approach [30] is explained in detail. The architecture of the IoT-Cloud based system proposed by the authors in paper [31]. The efficient, economical and distribution can be improved using the IoT technology in the smart grid system.

1.3.6. Supply chain system

The IoT smart devices, once used in a supply chain management system, can fundamentally change the traditional way to monitor the transport system. By using the IoT technique, the material is easily located, their current condition, packing details, and it is easy to track how goods are a move through the supply chain. It increases to maintain the demand-supply of good, easy to monitor the material movement, real-time tracking, efficient storage, energy efficient, and distribution. The authors in Li et al. [33], explained how tracking and tracing could be done in real-time using the IoT system. Similarly, in paper [34,35] authors, discussed the IoT based architecture and risk management in the supply chain system. In paper [34], authors have proposed artificial intelligent integration with IoT for the retail shop supply chain system.

1.3.7. Smart retails

The retail sector also using IoT services along with artificial intelligent [36] to enhance productivity, improve store operation, and to take the decision in real-time to manage the inventory system.

1.3.8. Agriculture

Agriculture is one of the promising application areas in IoT. In a smart agriculture system by deploying the sensors to monitor the soil quality, water management, crop growing condition, etc. which improve the farming efficiency by reducing time and cost. In real-time, a user can monitor all details from the remote locations. In paper [37,38] authors proposed smart irrigation using machine learning and IoT to enhance farming. similarly, in paper [39,40], smart water management and weather conditions in the agriculture system are explained in detail. Likewise, in paper [41,42], smart agriculture system integration with IoT technologies is explained in detail. As some of the work already done in the field of agriculture, still some security issues exist like mobility, infrastructure, and secure processing of the collected data.

1.4. Security attacks in internet of things

Jamming attack

Jamming attack is a subset of DoS attacks where the attacker tries to affect the communication channel in paper [43] authors also explained the details about the jamming attacks.

Dos attack

Dos attack is one of the common attacks used in IoT applications. Most of the IoT devices are a low-end device which is vulnerable to the attacker. The attacker gets under the data traffic stream through device connection or infrastructure.

Denial of service (DoS)

Denial of service (DoS) attacks, consists of a huge volume of network packets, targeting the node present in the application causes service interrupt in real-time.

IDS Attack

Intrusion detection system (IDS) is the process in which network traffic is control by the attacker. There are some types of IDS attacks, like misuse detection, anomaly detection, Host-based IDS, and Network-based IDS. The authors in paper [45] described the IDS attacks in IoT network. Malicious node attack is possible in a distributed IoT network due to the heterogeneous nature of the smart devices. The identify the genius node or fake node in the network is a challenging one. In paper [46] authors proposed a perception and K-mean to build the trust among the node and detect the malicious node.

Malicious node attack

Malicious node attack is possible in a distributed IoT network due to the heterogeneous nature of the smart devices. The identify the genius node or fake node in the network is a challenging one. In paper [46] authors proposed a perception and K-mean to build the trust among the node and detect the malicious node.

Power analysis attack

Power analysis attack and its corresponding solution approach are explained in papers [47,48]. This attack is mainly made to gain the computational power of the nodes so that the basic cryptographic algorithm is not possible to execute. In an IoT network, privacy also needs to be maintained to build trust among the node. Internal attack in paper [49] and Access control attack in paper [50] are discussed in details.

Wormhole attack

Wormhole attack is taken place at the 6LoWPAN layer, where the attacker makes a tunnel between two nodes that are connected [51].

The Side channel security attack

The Side channel security attack in cloud-based IoT application along with the security challenges are explained in paper [52]. Similarly, Distributed Dos attack is the process where the server is unreachable so that smart nodes in the network cannot get the services it desires to get [53] .

Man-in-the-middle attack

Man-in-the-middle attack, where the attacker relays the message or change the message during the transmission in the insecure channel, explained in Li et al. [54] IoT-Fog network.

Active attacks

Active attacks is explained in Zhang et al. [55] and its corresponding solution in the physical layer of the IoT network. There are different types of active attacks possible in IoT, where attackers make changes in the target node. The authors in Raoof et al. [56] explained the Routing attacks in routing protocol lossy network based on IoT application. The Sybil attack is one most common types of attack in IoT. The authors in Zhang et al. [57] and Mishra et al. [58] study the phases of Sybil attacks and their countermeasures in the internet of things. The Deceptive attack in La et al. [59] and Spoofing attack in Zhang et al. [60] authors have addressed the corresponding attacks and their security analysis in the internet of things applications.

The Buffer overflow attacks

The Buffer overflow attacks is the process of writing the program in a block of memory where the memory space is insufficient. The A IoT network, when nodes execute the different programs in the devices for processing or computation purpose attackers, can capture that and perform memory overflow attack. The detecting buffer overflow attack and providing appropriate security design in explained in Xu et al. [61]. In a large IoT network where heterogeneous devices are connected and communicate with each other. The trust is one of the major issues in the network. The Impersonation attacks where a fake node behaves like a genius node in the network and tries to gain the information from other nodes. This is one of the most challenging issues in IoT applications where smart devices are heterogeneous and low-end devices.

III. ARTIFICIAL INTELLIGENCE FOR CYBER SECURITY

Information and communication technology researchers agree that information security (InSec) is of primary importance [44]. Consequently, a number of studies have

attempted to address this by adopting improved techniques and technological artefacts; including the use of malware detectors, intrusion detection and prevention systems (IDPS), sophisticated firewall setups and data encryption algorithms. Although some studies have argued that InSec issues can be effectively managed by focusing on human behaviour [44], others have argued that focusing on human behaviour alone is not sufficient [51]. For example, the quantum of information handled by most organizations necessitates considerable automation [12]. Hence, there is the need for an appropriate balance between humans, technology and policy management in organizational security activities.

Conventional CyberSec prevention technologies use fix algorithms and physical devices (such as sensors and detectors), thus they are ineffective at containing new cyberspace threats [44]. For instance, the first generation of antivirus systems were designed to identify viruses by scanning its bit signature. The fundamental assumption of this concept is that a virus has the same structure and bit pattern in all instances. These signatures and algorithms are therefore fixed. Although the catalog of signatures is updated on a daily basis (or whenever the device is connected to the Internet), the sophistication and regular release of vast malware make this approach ineffective. However, the introduction of signature-less approaches that are capable of detecting and mitigating malware attacks using newer methods such as behavioural detections and AIs have been argued to be more effective [62].

This suggests that advancement in AI applications have made it possible to design relatively effective and efficient systems that automatically identify and prevent malicious activities within cyberspaces [51]. They have been adopted to support existing technological methods as they provide effective standards and mechanisms to better control and prevent cyber-attacks. Despite all the benefits AI provides, the rapid evolution of approaches makes it extremely difficult for researchers to identify the most efficient technique and its impact on cyberspace security. There is no ambiguity that the general perception amongst InSec and CyberSec researchers and practitioners suggest that AI has improved organizational information security, yet to the best of our knowledge, these claims are speculative and have not been empirically substantiated. Most existing studies have either demonstrated how their innovation outperform a selection of existing methods or surveyed a sample of systems and assess their performance in comparison to theirs. In all cases, the level of selection biases is relatively high. Accordingly, there is the need for an aggregated literature that provide summaries on issues, challenges and future research directions within the domain.

Power analysis attack and its corresponding solution approach are explained in papers [47,48]. This attack is mainly made to gain the computational power of the nodes so that the basic cryptographic algorithm is not possible to execute. In an IoT network, privacy also needs to be maintained to build trust among the node. Internal attack in paper [49] and Access control attack in paper [50] are discussed in details. Wormhole attack is taken place at the 6LoWPAN layer, where the attacker makes a tunnel between two nodes that are connected [51]. The Side channel security attack in cloud-based IoT application along with the security challenges are explained in paper [52]. Similarly, Distributed Dos attack is the process where the server is unreachable so that smart nodes in the network cannot get the services it desires to get [53]. Man-in-the-middle attack, where the attacker relays the message or change the message during the transmission in the insecure channel, explained in Li et al. [54] IoT-Fog network. Active attacks are explained in Zhang et al. [55] and its corresponding solution in the physical layer of the IoT network. There are different types of active attacks possible in IoT, where attackers make changes in the target node. The authors in Raoof et al. [56] explained the Routing attacks in routing protocol lossy network based on IoT application. The Sybil attack is one most common types of attack in IoT. The authors in Zhang et al. [57] and Mishra et al. [58] study the phases of Sybil attacks and their countermeasures in the internet of things. The Deceptive attack in La et al. [59] and Spoofing attack in Zhang et al. [60] authors have addressed the corresponding attacks and their security analysis in the internet of things applications. The Buffer overflow attacks is the process of writing the program in a block of memory where the memory space is insufficient. The A IoT network, when nodes execute the different programs in the devices for processing or computation purpose attackers, can capture that and perform memory overflow attack. The detecting buffer overflow attack and providing appropriate security design in explained in Xu et al. [61]. In a large IoT network where heterogeneous devices are connected and communicate with each other. The trust is one of the major issues in the network. The Impersonation [62] attacks where a fake node behaves like a genius node in the network and tries to gain the information from other nodes. This is one of the most challenging issues in IoT applications where smart devices are heterogeneous and low-end devices.

Learning methods for IoT security have been grouped into ML, DL and RL methods. ML methods consist of supervised and unsupervised approaches. The supervised

approaches are further categorised into DT, SVM, NB, KNN, RF, AR and EL. Moreover, the unsupervised method only consists of two methods, which are K-means and PCA. DL methods are also grouped into supervised, unsupervised and hybrid approaches. Supervised approaches consist of CNN and RNN methods. Unsupervised approaches also consist of AE, RBMs and DBNs methods. Lastly, hybrid approaches consist of GAN and EDLNs methods. No further categorisation was found under RL methods.

1.5. Machine Learning

Machine learning (ML) refers to intelligent methods used to optimize performance criteria using example data or past experience(s) through learning. More precisely, ML algorithms build models of behaviours using mathematical techniques on huge data sets. ML also enables the ability to learn without being explicitly programmed. These models are used as a basis for making future predictions based on the newly input data. ML is interdisciplinary in nature and inherits its roots from many disciplines of science and engineering that include artificial intelligence, optimization theory, information theory, and cognitive science [54]. Machine learning is utilized when human expertise either do not exist or cannot be used such as navigating a hostile place where humans are unable to use their expertise, for instance robotics, speech recognition etc. It is also applied in situations where solution to some specific problem changes in time (routing in a computer network or finding malicious code in a software or application). Furthermore, it is used in practical smart systems, for instance Google uses ML to analyse threats against mobile endpoints and applications running on Android.

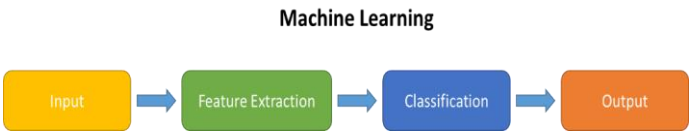

Fig.2. Machine Learning process

It is also used for identifying and removing malware from infected handsets. Likewise, Amazon has launched a service Macie that uses ML to sort and classify data stored in its cloud storage service. Although ML techniques perform well in many areas; however, there is a chance of false positives and true negatives. Therefore, ML techniques need guidance and modification to the model if inaccurate prediction is made. On the contrary, in Deep Learning (DL), a new breed of ML, the model can determine the accuracy of prediction by itself. Due to self-service nature of DL models, it is rendered as more suitable for classification and prediction tasks in innovative IoT applications with contextual and personalized assistance. Although traditional approaches are widely used for different aspects of IoT (e.g. applications, services, architectures, protocols, data aggregation, resource allocation, clustering, analytics) including security, the massive scale deployment of IoT however, advocates for intelligent, robust, and reliable techniques. To this end, ML and DL are promising techniques for IoT networks due to several reasons, e.g. IoT networks produce a sheer amount of data which is required by ML and DL approaches to bring intelligence to the systems. Furthermore, the data generated by the IoT is better utilized with the ML and DL techniques which enable the IoT systems to make informed and intelligent decisions. ML and DL are largely used for security, privacy, attack detection, and malware analysis. DL techniques can also be used in IoT devices to perform complex sensing and recognition tasks to enable the realization of new applications and services considering real-time interactions among humans, smart devices and physical surroundings.

Using ML and DL techniques in IoT applications on the other hand bring multi-faceted challenges. For instance, it is challenging to develop a suitable model to process data from diverse IoT applications. Similarly, labelling input data effectively is also a cumbersome task. Another challenge is using minimum labelled data in the learning process. Other challenges stem from the deployment of these models on resource-constrained IoT devices where it is essential to reduce the processing and storage overhead [55]. Similarly, critical infrastructure and real-time applications cannot withstand the anomalies created because of ML or DL algorithms. In the above context, it is imperative to systematically review the security solutions of IoT that leverage ML and DL techniques.

1.6. Deep Learning

Deep Learning (DL) is a subset of machine learning techniques, based on artificial neural networks, mirroring the information processing of real biological nervous systems, made of various perceptrons layers. Artificial neural networks have been devised in the past century, but they have recently come back to the limelight thanks to the developments in the computational power of computers, fostering the adoption of DL architectures, made of several related layers, each one composed, in turn, of hundreds or thousands of neurons. More precisely, each layer receives input data and abstracts and organizes them into a sort of hierarchy, useful to learn features as well as to classify different patterns. Compared to traditional machine learning techniques, DL algorithms are considered much more suitable in contexts featuring a high level of complexity, i.e., having several features and a huge

number of data, and being capable of achieving very high performance. The training phase of a deep neural network training has a particular feature: it can be split into two main steps, namely the forward and the backward propagation. In the former, the activation of the internal nodes, representing neurons or perceptrons, is performed according to a certain activation function, layer after layer, from the network input to its output [52]. Conversely, the latter allows for the refinement of the network performance by means of updated weights and bias values to be assigned, if necessary, to the single nodes.

Fig.3. Deep Learning process

There exist various types of deep neural networks, each one with its own main characteristics in terms of number of layers, types of operations performed in the layers, connections across the layers, etc. However, a first rough classification can pertain to the deep supervised, unsupervised, hybrid, and reinforcement learning approaches.

The supervised DL approaches ground their own predictions or classifications on the basis of a particular learned mapping between an instance and a certain label or class generating a discriminative model [53]. In other words, these methods are able to relate the input parameters (features) and the required output (the class) thanks to a priori knowledge of the label of a certain instance. The initial stage of supervised approaches provides that learning examples train the algorithms, then used to predict or classify a novel unlabelled input instance [54]. These approaches usually encompass Convolutional Neural Networks (CNN) as well as Recurrent Neural Networks (RNN). On the other hand, the unsupervised DL approaches can learn important representations of the input without the necessity of pre-labelled training data [55], creating a so-called generative model. These approaches generally intend to: (i) analyse unlabelled data to find previously unknown similarity relationships within the training instances and then (ii) to categorize new unlabelled instances into distinctive groups by exploiting the similarities found in the training set. Some representative members of these approaches are deep Auto Encoders (AE), Restricted Boltzmann Machines (RBM), and Deep Belief Networks (DBN). The hybrid DL approaches are a combination of the aforementioned, combining both discriminative and generative models. Examples of such DL approaches can be seen in Generative Adversarial Networks (GAN) and Ensembles of Deep Learning Networks (EDLN). Finally, deep reinforcement learning provides entities that learn according to a trial-and-error procedure, involving how their actions can affect the surrounding context. A certain reward is estimated after each action, which moves the whole learning system towards a new state accordingly. Entities will get rewarded for good actions and penalized for bad actions [56]. An example of this category is surely Deep Q-learning (QL). In the following subsections, we will summarize the main types of deep neural networks, that we found in performing the systematic review we carried out.

1.6.1. Supervised deep neural networks DNN

1.6.1.1. CNN

A first type of supervised DNN is the CNN, which has been originally devised to shrink the number of parameters in image recognition tasks, replacing traditional artificial neural networks. The reduction of the parameters, by means of sparse interaction, parameter sharing and equivariant representation [9], allows the simultaneous cutting down of the connections between layers, thus augmenting the scalability as well as improving the overall training time complexity. Basically, a CNN is made of two types of layers, which are usually interchanged, namely, convolutional layers and pooling layers. The former are in charge of convoluting data parameters using multiple equal-sized filters [57]. The latter reduce the sizes of the following layers by means of max pooling (division into non-overlapping clusters and selection of the maximum value per cluster) or average pooling operations, which act as a sort of down-sampling. The reduction of the parameters can be seen when a CNN is extensively applied to the training set, thus permitting the automatic learning of features from raw data with high performance. Notwithstanding, the disadvantage of a CNN is the high computational cost; thus, its implementation on resource-constrained devices, such as those present in an IoT environment, is challenging and often requires the help of edge computing devices.

1.6.1.2. RNN

Another type of supervised DNN is the RNN, which has been introduced to manage sequential input data, e.g., speech, text, sensor data, etc., thus considering, in the prediction about the current sample, the associations of several previous samples as well. In summary, the output of an RNN depends both on present and past inputs; therefore, the traditional feed-forward scheme is not suitable in this context, whereas the back-propagation technique fits perfectly [58]. The main feature of an RNN is a temporal layer, getting sequential input data and learning multifaceted variations thereof. This is performed

by using hidden units of a recurrent cell [59], which elaborate the current state of the network by means of an estimation of the following state as an activation of the previous state. However, the main disadvantage of an RNN is the so-called vanishing or exploding gradient [60], which prevents the weights of the network from being correctly updated. RNNs can be used for IoT security by analysing the great quantity of sequential data produced by IoT smart objects, namely by detecting time series-based threats.

1.6.2. Unsupervised deep neural networks

A first type of unsupervised DNN is made of an AE, which, as the name may suggest, aims to reproduce the input into the output. Usually, AE have only one hidden layer joining its two main parts: an encoding function h = f (x), abstracting the input into a so-called code, and a decoding function r = g(h), which tries to replicate the input with minimum reconstruction error [9,61]. One of the advantages is that an AE can give priority to some input feature in the copying process; thereby, it is normally very effective in extracting a reduced set of useful characteristics out of the input data. A disadvantage may be the fact that an AE cannot reconstruct the input perfectly, as it only reproduces an approximation thereof, by simply copying the inputs being similar to the training data having already been processed. Moreover, an AE requires a high computational time and it could only make the learning process more complicated in case the considered training dataset has no significant relationships with the testing dataset. Other types of unsupervised DNN are deep generative models such as RBMs, wherein no links between any two nodes belonging to the same layer are present.

An RBM is made of two main types of layers, namely the visible and hidden layers, in order to understand hierarchically features from the input data themselves. The former encompass known inputs, while the latter entail latent variables, i.e., the features captures in the initial visible layer, spread into further multiple layers. The main issues with RBMs concern the accurate follow-up of the evolution of the training data over time, as well as the limited capability to represent features. However, RBMs can be improved by stacking two or more of them in order to create another type of generative DNNs, i.e, a DBN [55]. The stacked RBMs perform greedy layer-wise unsupervised training in order to enhance the robustness and the performance of the whole training procedure. This objective is achieved by training each RBM layer, one layer after the other, executing the operations of each layer on top of the formerly trained layer and applying a SoftMax layer during the fine-tuning phase of the features with respect to the labeled samples [63]. Indeed, after the pre-training phase, a DBN turns out to be a feedforward network that fine-tunes the weights with contrastive convergence [59]. Moreover, although contrastive convergence may lower computational time, these types of DNN are still not very much applicable to resource-constrained devices.

1.7. Blockchain

A Blockchain is a distributed public database that keeps a permanent record of digital transactions. The distributed ledger records the transactions of Blockchain blocks, and every block is related with a hash function to preserve the chain with its previous block [14]. The network elements/nodes will receive a pair of the public key and private key upon registering to the network. Public key works as a unique identifier for each element. Private key also helps to sign transactions in the network and is used for encryption and decryption. The transactions are received by all the nodes and are validated. They are grouped into a timestamped block by few nodes designated as miners [14]. Blockchain is a “No Central Authority,” consensus algorithm used to select a block, among the number of blocks created by the miners, added to the Blockchain network. For making any changes to the existing block of data, all the nodes present in the network run algorithms to evaluate, verify, and match the transaction information with Blockchain history. If the majority of the nodes agree in favour of the transaction, then it is approved, and a new block gets added to the existing chain. Implementing Blockchain comes with benefits such as securing data, reducing errors, ensure reliability, and improve integrity and effectiveness

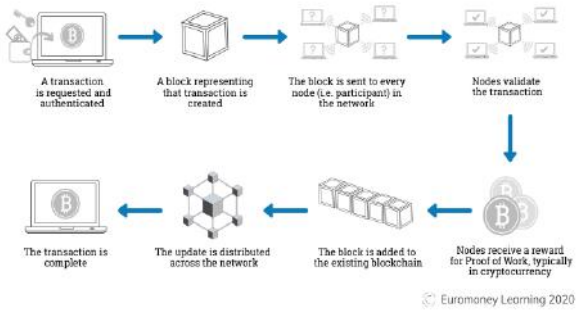

Fig.4. Blockchain Process

IV. CONCLUSION

In this paper, we tried to give an overview of IoT technology and its application domains study various security challenges that can be faced by IoT applications then we have described some existing AI approaches that can enhance IoT security. From the survey, it was found that some research has already been done in various technology like Machine learning, Artificial intelligence,

and Blockchain technology, which are capable of addressing the existing security issue. So, in detail study has been made in three technology machine learning, artificial intelligence and Blockchain technology, and their integration with IoT. Security is an important issue that needs to address. In this survey, we have focused on the emerging Artificial intelligence technologies like DL, MI, and Blockchain and their integration with IoT to make the system more secure.

REFERENCES

[1] A. ˇColakovi ´c , M. Hadžiali ´c , Internet of things (IoT): a review of enabling technologies, challenges, and open research issues, Comput. Netw. 144 (2018) 17–39 .

[2] D. Mocrii , Y. Chen , P. Musilek , IoT-based smart homes: a review of system architecture, software, communications, privacy and security, Internet Things 1 (2018) 81–98 .

[3] Q. Jing , A.V. Vasilakos , J. Wan , J. Lu , D. Qiu , Security of the internet of things: perspectives and challenges, Wirel. Netw. 20 (8) (2014) 2481–2501 .

[4] A.H. Ngu , M. Gutierrez , V. Metsis , S. Nepal , Q.Z. Sheng , Iot middleware: a survey on issues and enabling technologies, IEEE Internet Things J. 4 (1) (2016) 1–20 .

[5] A. Mosenia , N.K. Jha , A comprehensive study of security of internet-of-things, IEEE Trans. Emerg. Top. Comput. 5 (4) (2016) 586–602 .

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

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

[8] F.A. Alaba , M. Othman , I.A.T. Hashem , F. Alotaibi , Internet of things security: a survey, J. Netw. Comput. Appl. 88 (2017) 10–28 .

[9] P.I.R. Grammatikis , P.G. Sarigiannidis , I.D. Moscholios , Securing the internet of things: challenges, threats and solutions, Internet Things 5 (2018) 41–70 .

[10] A.K. Das , S. Zeadally , D. He , Taxonomy and analysis of security protocols for internet of things, Future Gener. Comput. Syst. 89 (2018) 110–125 .

[11] B. Di Martino , M. Rak , M. Ficco , A. Esposito , S. Maisto , S. Nacchia , Internet of things reference architectures, security and interoperability: a survey, Internet Things 1 (2018) 99–112 .

[12] V. Hassija , V. Chamola , V. Saxena , D. Jain , P. Goyal , B. Sikdar , A survey on IoT security: application areas, security threats, and solution architectures, IEEE Access 7 (2019) 82721–82743 .

[13] A. Al-Hasnawi , S.M. Carr , A. Gupta , Fog-based local and remote policy enforcement for preserving data privacy in the internet of things, Internet Things 7 (2019) 10 0 069 .

[14] K.-C. Chen , S.-Y. Lien , Machine-to-machine communications: technologies and challenges, Ad Hoc Netw. 18 (2014) 3–23 .

[15] V. Casola , A. De Benedictis , A. Riccio , D. Rivera , W. Mallouli , E.M. de Oca , A security monitoring system for internet of things, Internet Things 7 (2019) 10 0 080 .

[16] S. Siboni , V. Sachidananda , Y. Meidan , M. Bohadana , Y. Mathov , S. Bhairav , A. Shabtai , Y. Elovici , Security testbed for internet-of-things devices, IEEE Trans. Reliab. 68 (1) (2018) 23–44 .

[17] R. Nawaratne , D. Alahakoon , D. De Silva , P. Chhetri , N. Chilamkurti , Self-evolving intelligent algorithms for facilitating data interoperability in IoT environments, Future Gener. Comput. Syst. 86 (2018) 421–432 .

[18] K. Bing , L. Fu , Y. Zhuo , L. Yanlei , Design of an internet of things-based smart home system, in: 2011 2nd International Conference on Intelligent Control and Information Processing, 2, IEEE, 2011, pp. 921–924 .

[19] U. Satapathy , B.K. Mohanta , D. Jena , S. Sobhanayak , An ECC based lightweight authentication protocol for mobile phone in smart home, in: 2018 IEEE 13th International Conference on Industrial and Information Systems (ICIIS), IEEE, 2018, pp. 303–308 .

[20] S.S. Panda , D. Jena , B.K. Mohanta , A remote device authentication scheme for secure communication in cloud based IoT, in: 2019 2nd International Conference on Innovations in Electronics, Signal Processing and Communication (IESC), IEEE, 2019, pp. 165–171 .

[21] R.K. Kodali , V. Jain , S. Bose , L. Boppana , IoT based smart security and home automation system, in: 2016 International Conference on Computing, Communication and Automation (ICCCA), IEEE, 2016, pp. 1286–1289 .

[22] K. Jaiswal , S. Sobhanayak , B.K. Mohanta , D. Jena , IoT-cloud based framework for patient's data collection in smart healthcare system using raspber- ry-pi, in: 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), IEEE, 2017, pp. 1–4 .

[23] S.R. Moosavi , T.N. Gia , A.-M. Rahmani , E. Nigussie , S. Virtanen , J. Isoaho , H. Tenhunen , Sea: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways, Procedia Comput. Sci. 52 (2015) 452–459 .

[24] Y. Mehmood , F.Ahmad , I.Yaqoob , A.Adnane , M.Imran , S. Guizani ,Internet-of-things-based smartcities:recent advancesand challenges,IEEE Com- mun. Mag. 55 (9) (2017) 16–24 .

[25] H. Arasteh , V. Hosseinnezhad , V. Loia , A. Tommasetti , O. Troisi , M. Shafie-Khah , P. Siano , IoT-based smart cities: a survey, in: 2016 IEEE 16th Interna- tional Conference on Environment and Electrical Engineering (EEEIC), IEEE, 2016, pp. 1–6 .

[26] A.J. Neto , Z. Zhao , J.J. Rodrigues , H.B. Camboim , T. Braun , Fog-based crime-assistance in smart IoT transportation system, IEEE Access 6 (2018) 11101–11111 .

[27] L.F. Herrera-Quintero , J.C. Vega-Alfonso , K.B.A. Banse , E.C. Zambrano ,Smart ITS sensor for the transportation planning based on IoT approaches using serverless and microservices architecture, IEEE Intell. Transp. Syst. Mag. 10 (2) (2018) 17–27 .

[28] S. Muthuramalingam , A. Bharathi , N. Gayathri , R. Sathiyaraj , B. Balamurugan , et al. , IoT based intelligent transportation system IoT-ITS for global perspective: a case study, in: Internet of Things and Big Data Analytics for Smart Generation, Springer, 2019, pp. 279–300 .

[29] M.R. Dey , U. Satapathy , P. Bhanse , B.K. Mohanta , D. Jena , Magtrack: detecting road surface condition using smartphone sensors and machine learning, in: TENCON 2019-2019 IEEE Region 10 Conference (TENCON), IEEE, 2019, pp. 2485–2489 .

[30] X.C. Yin , Z.G. Liu , L. Nkenyereye , B. Ndibanje , Toward an applied cyber security solution in IoT-based smart grids: an intrusion detection system approach, Sensors 19 (22) (2019) 4952 .

[31] A . Meloni , P.A . Pegoraro , L. Atzori , A. Benigni , S. Sulis ,Cloud-based IoT solution for state estimation in smart grids: exploiting virtualization and edge-intelligence technologies, Comput. Netw. 130 (2018) 156–165 .

[32] M. Karjalainen, S. Sarker, and M. Siponen, “Toward a Theory of Information Systems Security Behaviors of Organizational Employees: A Dialectical Process Perspective,” Inf. Syst. Res.,

[33] Z. Li , G. Liu , L. Liu , X. Lai , G. Xu , IoT-based tracking and tracing platform for prepackaged food supply chain, Ind. Manag. Data Syst. 117 (9) (2017) 1906–1916 .

[34] Y.P. Tsang , K.L. Choy , C.-H. Wu , G.T. Ho , C.H. Lam , P. Koo , An internet of things (IoT)-based risk monitoring system for managing cold supply chain risks, Ind. Manag. Data Syst. 118 (7) (2018) 1432–1462 .

[35] C. Verdouw , R.M. Robbemond , T. Verwaart , J. Wolfert , A.J. Beulens ,A reference architecture for IoT-based logistic information systems in agri-food supply chains, Enterp. Inf. Syst. 12 (7) (2018) 755–779 .

[36] L. Liu , B. Zhou , Z. Zou , S.-C. Yeh , L. Zheng , A smart unstaffed retail shop based on artificial intelligence and IoT, in: 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), IEEE, 2018, pp. 1–4 .

[37] M. Mehra , S. Saxena , S. Sankaranarayanan , R.J. Tom , M. Veeramanikandan , IoT based hydroponics system using deep neural networks, Comput. Elec- tron. Agric. 155 (2018) 473–486 .

[38] A. Goap , D. Sharma , A. Shukla , C.R. Krishna , An IoT based smart irrigation management system using machine learning and open source technologies, Comput. Electron. Agric. 155 (2018) 41–49 .

[39] C. Kamienski , J.-P. Soininen , M. Taumberger , R. Dantas , A. Toscano , T. Salmon Cinotti , R. Filev Maia , A. Torre Neto , Smart water management platform: IoT-based precision irrigation for agriculture, Sensors 19 (2) (2019) 276 .

[40] B. Keswani , A.G. Mohapatra , A. Mohanty , A. Khanna , J.J. Rodrigues , D. Gupta , V.H.C. de Albuquerque , Adapting weather conditions based IoT enabled smart irrigation technique in precision agriculture mechanisms, Neural Comput. Appl. 31 (1) (2019) 277–292 .

[41] N.K. Nawandar , V.R. Satpute , IoT based low cost and intelligent module for smart irrigation system, Comput. Electron. Agric. 162 (2019) 979–990 .

[42] M. Ayaz , M. Ammad-Uddin , Z. Sharif , A. Mansour , E.-H.M. Aggoune , Internet-of-things (IoT)-based smart agriculture: toward making the fields talk, IEEE Access 7 (2019) 129551–129583 .

[43] M. López , A. Peinado , A. Ortiz , An extensive validation of a SIR epidemic model to study the propagation of jamming attacks against IoT wireless networks, Comput. Netw. 165 (2019) 106945 .

[44] P. Patil, “Artificial intelligence in cybersecurity,” Int. J. Res. Comput. Appl. Robot., vol. 4, no. 5, pp. 1–5, 2016.

[51] S. Dilek, H. Çakır, and M. Aydın, “Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review,” Feb. 2015, doi: 10.5121/ijaia.2015.6102 [45] M. Almiani , A. AbuGhazleh , A. Al-Rahayfeh , S. Atiewi , A. Razaque , Deep recurrent neural network for IoT intrusion detection system, Simul. Modell. Pract. Theory 101 (2019) 102031 .

[46] L. Liu , Z. Ma , W. Meng , Detection of multiple-mix-attack malicious nodes using perceptron-based trust in IoT networks, Future Gener. Comput. Syst. 101 (2019) 865–879 .

[47] J. Moon , I.Y. Jung , J.H. Park , IoT application protection against power analysis attack, Comput. Electr. Eng. 67 (2018) 566–578 .

[48] Y. Niu , J. Zhang , A. Wang , C. Chen , An efficient collision power attack on AES encryption in edge computing, IEEE Access 7 (2019) 18734–18748 .

[49] N. Tariq , M. Asim , Z. Maamar , M.Z. Farooqi , N. Faci , T. Baker , A mobile code-driven trust mechanism for detecting internal attacks in sensor node-pow- ered IoT, J Parallel Distrib. Comput. 134 (2019) 198–206 .

[50] H. Yan , Y. Wang , C. Jia , J. Li , Y. Xiang , W. Pedrycz , IoT-FBAC: function-based access control scheme using identity-based encryption in IoT, Future Gener. Comput. Syst. 95 (2019) 344–353 .

[51] S. Deshmukh-Bhosale , S.S. Sonavane , A real-time intrusion detection system for wormhole attack in the RPL based internet of things, Procedia Manuf. 32 (2019) 840–847 .

[52] H. Yi , Z. Nie , Side-channel security analysis of UOV signature for cloud-based internet of things, Future Gener. Comput. Syst. 86 (2018) 704–708 .

[53] D. Yin , L. Zhang , K. Yang , A DDoS attack detection and mitigation with software-defined internet of things framework, IEEE Access 6 (2018) 24694–24705 .

[54] C. Li , Z. Qin , E. Novak , Q. Li , Securing SDN infrastructure of IoT–fog networks from MitM attacks, IEEE Internet Things J. 4 (5) (2017) 1156–1164 .

[55] N. Zhang , R. Wu , S. Yuan , C. Yuan , D. Chen , RAV: relay aided vectorized secure transmission in physical layer security for internet of things under active attacks, IEEE Internet Things J. 6 (5) (2019) 8496–8506 .

[56] A . Raoof , A . Matrawy , C.-H. Lung , Routing attacks and mitigation methods for RPL-based internet of things, IEEE Commun. Surv. Tutor. 21 (2) (2018) 1582–1606 .

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

[58] A .K. Mishra , A .K. Tripathy , D. Puthal , L.T. Yang , Analytical model for Sybil attack phases in internet of things, IEEE Internet Things J. 6 (1) (2018) 379–387 .

[59] Q.D. La , T.Q. Quek , J. Lee , S. Jin , H. Zhu , Deceptive attack and defense game in honeypot-enabled networks for the internet of things, IEEE Internet Things J. 3 (6) (2016) 1025–1035 .

[60] P. Zhang , S.G. Nagarajan , I. Nevat ,Secure location of things (SLOT): mitigating localization spoofing attacks in the internet of things, IEEE Internet Things J. 4 (6) (2017) 2199–2206 .

[61] B. Xu , W. Wang , Q. Hao , Z. Zhang , P. Du , T. Xia , H. Li , X. Wang , A security design for the detecting of buffer overflow attacks in IoT device, IEEE Access 6 (2018) 72862–72869 .

[62] A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, and Y. Weiss, Andromaly': a behavioral malware detection framework for android devices," J. Intell. Inf. Syst., vol. 38, no. 1, pp. 161–190, 2012.

[63] I. Kotenko , I. Saenko , A. Branitskiy , Framework for mobile internet of things security monitoring based on big data processing and machine learning, IEEE Access 6 (2018) 72714–72723 .

[64] E. Hossain , I. Khan , F. Un-Noor , S.S. Sikander , M.S.H. Sunny , Application of big data and machine learning in smart grid, and associated security concerns: a review, IEEE Access 7 (2019) 13960–13988 .

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

[66] E. Anthi , L. Williams , M. Słowi ´nska , G. Theodorakopoulos , P. Burnap , A supervised intrusion detection system for smart home IoT devices, IEEE Internet Things J. 6 (5) (2019) 9042–9053 .

[67] N. Wang , T. Jiang , S. Lv , L. Xiao , Physical-layer authentication based on extreme learning machine, IEEE Commun. Lett. 21 (7) (2017) 1557–1560 .