Security Aspects of the Internet of Things

Dominik Hromada
ESTG, Polytechnic of Leiria Leiria,
Portugal
2192206@my.ipleiria.pt

Rogério Luís de C. Costa
CIIC, Polytechnic of Leiria
Leiria, Portugal
rogerio.l.costa@ipleiria.pt

Leonel Santos
CIIC, ESTG, Polytechnic of Leiria
Leiria, Portugal
leonel.santos@ipleiria.pt

Carlos Rabadão
CIIC, ESTG, Polytechnic of Leiria
Leiria, Portugal
carlos.rabadao@ipleiria.pt

Abstract - The Internet of Things (IoT) comprises the interconnection of a wide range of different devices, from Smart Bluetooth speakers to humidity sensors. The great variety of devices enables applications in several contexts, including Smart Cities and Smart Industry.

IoT devices collect and process a large amount of data on machines and the environment and even monitor people's activities. Due to their characteristics and architecture, IoT devices and networks are potential targets for cyberattacks. Indeed, cyberattacks can lead to malfunctions of the IoT environment and access and misuse of private data.

This chapter addresses security concerns in the IoT ecosystem. It identifies common threats for each of IoT layers and presents advantages, challenges, and limitations of promising countermeasures based on new technologies and strategies, like Blockchain and Machine Learning. It also contains a more in-depth discussion on Intrusion Detection Systems (IDS) for IoT, a promising solution for cybersecurity in IoT ecosystems.

Keywords: IoT security, IoT threats, security countermeasures, Intrusion Detection Systems

I. Introduction

Internet of Things (IoT) as a term was used for the first time in 1999 by Kevin Ashton, a British technology pioneer (Farooq, Waseem, Khairi, & Mazhar, 2015). He defines IoT as the system of physical objects in the world that connects to the internet via a sensor. This ecosystem is full of intelligent machines interacting with each other, with objects, environments, and infrastructures. This new technology has impacted the whole population from everyday people's lives to industry solutions, helping people to work smarter and efficiently, and giving them more control over monitored environments, objects, and infrastructures.

In several market areas, IoT became an essential part of business activities, e.g., providing real-time data about operation activities or measuring the performance of supply chain machines and logistic operations. The data collected by IoT devices can be analyzed later, and provide decision-makers with invaluable insights into their processes with the help of Business Intelligence (BI) to make business processes even more efficient, faster, environmentally friendly, and less expensive. Therefore, IoT opened new opportunities for data analysis and knowledge discovery (Gubbi, Buyya, Marusic, & Palaniswami, 2013). Main IoT applications areas include transportation and logistics, Smart Healthcare, Smart Environments, and City Information Modeling (Ullah, Ahmad, Ahmad, Ata-ur-Rehman, & Junaid, 2019).

On the other hand, the data collected are a double-edged sword. It may be a significant help, but also a threat to people's privacy and security, as their activity can be monitored everywhere and anytime (Neisse et al., 2015). Also, poorly secured devices may lead to attacks on other systems and lead to personal information leaks and misuses due to unauthorized access.

Some of the main security concerns in the context of IoT are related to basic processes (for example, identification, authentication, and access control), data integrity, data confidentiality, data privacy, and data availability (Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015; Farooq et al., 2015). But the layered architecture of IoT is also subject to several attacks and threats, each of them being most common in or targeted to a specific layer (Weyrich & Ebert, 2016; Swamy, Jadhav, & Kulkarni, 2017).

Some of the *traditional* security countermeasures (e.g., the use of security protocols, authentication controls, and privacy by design) may fit in the IoT context. But the new solutions for IoT security include the use of Fog Computing, Blockchain Technology, Edge computing, and Machine Learning-based techniques (Baouya, Chehida, Bensalem, & Bozga, 2020; Ozay, Esnaola, Yarman Vural, Kulkarni, & Poor, 2016).

The use of Intrusion Detection Systems (IDS) in IoT networks is subject to some additional challenges. Deep packet inspection (DPI) and stateful packet inspection (SPI) are computationally expensive and not adequate for the IoT network. An alternative solution in IoT ecosystems may go through an IDS based on IP flow analysis. Additional challenges related to an efficient IDS for IoT networks include aspects related to chosen incident detection methodology, the IDS implementation strategy, and IDS's intrusion detection capabilities.

In the following section, we present the main aspects related to the IoT processing cycle. Then, Section III presents the main security concerns in the IoT context. The IoT layered architecture and the most common threats of each layer are described in Section IV. Section V discusses some current countermeasures based on *nontraditional* solutions and Section V presents open issues and future directions. Finally, Section VII concludes the chapter.

II. Aspects of IoT Network Processing Cycle

The IoT opened several new opportunities in a wide range of applications. Figure 1 presents the main components of a processing cycle in the IoT.

A. Recognition

All the involved objects in the network must have unique identification and must be recognized accordingly. That means that two entities present in the network cannot have a similar identification representation. Hence, the two main components of successful recognition are addressing and naming. Each entity is assigned a particular address and name, where their combination is unique for it. The allocating address task uses IPv6 as the number addressing scheme of 128 bits. The naming process can use several methods, such as IP-based codes, electronic products codes (EPC), and ubiquitous codes (Al-Fuqaha, Guizani, Mohammadi, Aledhari, & Ayyash, 2015).

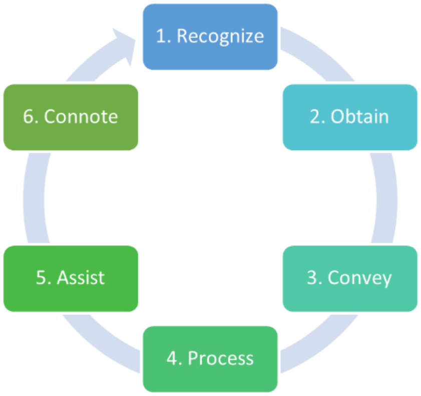

Fig. 1. Processing cycle in IoT networks

B. Obtaining

IoT obtains and collects data from different devices via sensing utilities, such as RFID (radio-frequency indicators) tags, actuators, wearables, etc. These data are further transported via gateways and stored in areas such as cloud storage (Sehrawat & Gill, 2019).

C. Conveyance

Responsibilities of reference of information from one point to another are assigned to ensure data transportation, which is essential for the proper functioning of IoT. In other words, all the communication, including messages, conversations, files, and other data, is transmitted through this component, which uses specific protocols, such as z-wave, Zigbee and 6LoWPAN (Low power Wireless Personal Area Networks) (AlSarawi, Anbar, Alieyan, & Alzubaidi, 2017).

D. Processing

The data collected via sensors are then processed with the help of a variety of operating systems, such as Android and TinyOs, using a range of hardware platforms like Intel Galileo and Audrino (Basha & S A K, 2016).

E. Assistance

IoT applications can provide several types of assistance. The most helpful is the assistance related to identity. The next is the assistance associated with data aggregation, which can be done without any communication channel, and unifies different technologies in a single application. The following assistance deals with the aggregated information to perform task decisions and actions needed. The fourth assistance is the ability to be omnipresent that provides the services of IoT ubiquitously without the strictness of time and location (Gigli & Koo, 2011).

F. Connotation

The whole cycle ends with this component, which acts as the brain of the IoT process. All the devices can get the response as all the data and decisions are connoted here (Basha & S A K, 2016).

III. IoT Security Concerns

The use of IoT devices has an unmediated impact on users' lives, hence high priority to the security measures must be given together with well-defined security guidelines consisting of new systems and protocols to ensure that the possible threats related to security and privacy will be limited. Specifically, the processes of authentication, integrity, data confidentiality, and data privacy are among the main elements of IoT security (Farooq et al., 2015). Other important concerns include identification, trust and access control (Sicari et al., 2015), and data availability (Atzori, Iera, & Morabito, 2010).

A. Identification

The identification process is crucial for the network to decide whether the smart device can be trusted or not. Serious threats may arise from permitting an intruder to enter the secured network (Sicari et al., 2015). Despite this fact, we must prevail a system that can detect these possible security threats but is still able to provide its device identity to other qualified devices. Therefore, devices interacting with their users must know their identity and can distinguish them too (Atzori et al., 2010).

B. Authentication

In the case of IoT, authentication is quite challenging as it usually requires appropriate authentication infrastructures and servers to be secure, such as two-factor authentication. As in IoT passive utilities are used, such as RFID tags or sensor nodes, the standard procedures commonly used in other IT sectors cannot be used, as these passive utilities cannot exchange too many messages with the authentication servers (Atzori et al., 2010), (Farooq et al., 2015), (Sicari et al., 2015).

C. Data Integrity

The data transmission can be disrupted by plenty of factors that cannot be controlled by the nodes involved. For example, data changes during transmission, server outages, or electromagnetic interference (Riahi Sfar, Natalizio, Challal, & Chtourou, 2018). Hence, data integrity is preserved with the help of common surveillance methods to protect the data transmitted from cyberattacks and to avoid external interference during the communication itself. For this purpose, methods like checksums and cyclic redundancy checks (CRC) are used to guarantee data accuracy and reliability with the help of error detection mechanisms (Sicari et al., 2015), (Atzori et al., 2010).

D. Trust

Trust is a very broad term covering many disciplines beyond security, hence it is more difficult to be established (Atzori et al., 2010). Nitti et al. (Nitti, Girau, & Atzori, 2014) conducted a study that had as main objective to explore how users accept the IoT objects around them. Interestingly, 43% of respondents say they are worried about their data, therefore are afraid to use the IoT utilities. 18% think that IoT objects used are not operational and 8% believe they are not reliable. Users are concerned with the fact that they cannot always determine when, whether, and to whom the personal information could and could not be exposed (Riahi Sfar et al., 2018). It is believed that as soon as the users gain certainty that the IoT objects are secured enough by the manufacturer and their data cannot be misused, the IoT technologies will be most likely better adopted by their users (Sicari et al., 2015).

E. Data Confidentiality

User is secured by data confidentiality which ensures that confidential information is trusted. This process is done by various mechanisms to prevent any exposure against the user's will. These security mechanisms ensure data privacy work with the help of data encryption, two stage authentication, and biometric authentication mechanisms which protect data from unauthorized access. In the case of IoT devices, these mechanisms ensure that sensor networks maintain their sensor nodes hidden from unauthorized neighboring nodes as well as their communication from unauthorized readers (Farooq et al., 2015).

F. Access Control

Access control is associated with permissions in the usage of resources that are assigned to different entities connected to the IoT network. These permissions specify whether the user is granted access and the user's authorizations to perform specified tasks. Access Control List (ACL) is used to specify a device used and the user's access level. Here the administrator of the network must be careful with access granting as a mistake can result in serious threats (Riahi Sfar et al., 2018).

G. Data Privacy

In the IoT environment, the amount of data collected and stored is rapidly increasing and users cannot be sure that this data will be used only for the purposes they gave consent to or will not be misused in the nearest future. Hence, protecting stored data has the same priority as securing its transmission. The IoT environment is full of devices, readers, sensors, and applications that might collect data on multiple levels that together can expose user's habits, their actual or most common locations, where the user lives and goes to work, does shopping, or even their diet via smart fridges. As nowadays we can evaluate many aggregated data with the help of Business Intelligence, the data leak may result from useful insight from market sectors to unwanted surveillance by the cyber attacker or even the government. As data are stored on centered cloud services and they are not anonymous and collected all the time, their privacy should be given high priority (Farooq et al., 2015; Gubbi et al., 2013; Riahi Sfar et al., 2018).

H. Data Availability

IoT gathers, analyses, and provides data to its users. Data availability ensures that the data is provided to its user when needed without necessary delays. This state is supposed to be maintained even under unfavorable conditions, such as cyberattacks, by implementing appropriate secure measurements, such as firewalls preventing denial of service attack (DoS) or its advanced version - distributed denial of service attack (DDoS). Moreover, this should be facilitated by the corresponding hardware infrastructure which is supposed to be well secured as well. In the case of data loss prevention, data should be sufficiently backed up, which helps to ensure system components replication in the case of system failure, providing reliability and availability (Atzori et al., 2010).

IV. IoT Security and Layers Architecture

Internet of Things can be broadly defined in four layers. Going top-down, it begins with the *application layer*, followed by the *middleware layer* (or *data processing layer*) (Sikder, Petracca, Aksu, Jaeger, & Uluagac, 2018) and by the *network layer* (also known as *transport layer*). The *perception layer* (or *sensing layer*) is the last one. Figure 2 represents this layered architecture.

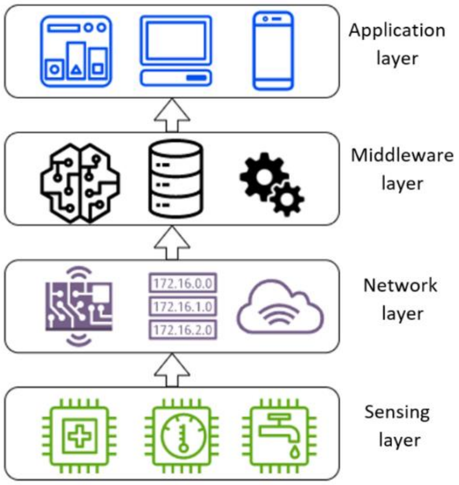

Fig. 2. IoT Layers and Components (Adapted from Sikder, Petracca, Aksu, Jaeger, & Uluagac, 2018)

The first two layers represent the utilization of data in the application, the following two where data are captured (Weyrich & Ebert, 2016). Some authors (e.g., Antão, Pinto, Reis, & Gonçalves, 2018) refer to a *business layer* as a layer above the application layer, which is supposed to manage the whole IoT system, including applications, business models, and users' privacy. Discussing such a business layer is out of the scope of this chapter.

Each IoT layer has its objectives and characteristics and may suffer distinct types of threats. Figure 3 presents some of the most common threats of each layer. In the following, we identify the main components of each layer and the threats which may occur on the layer.

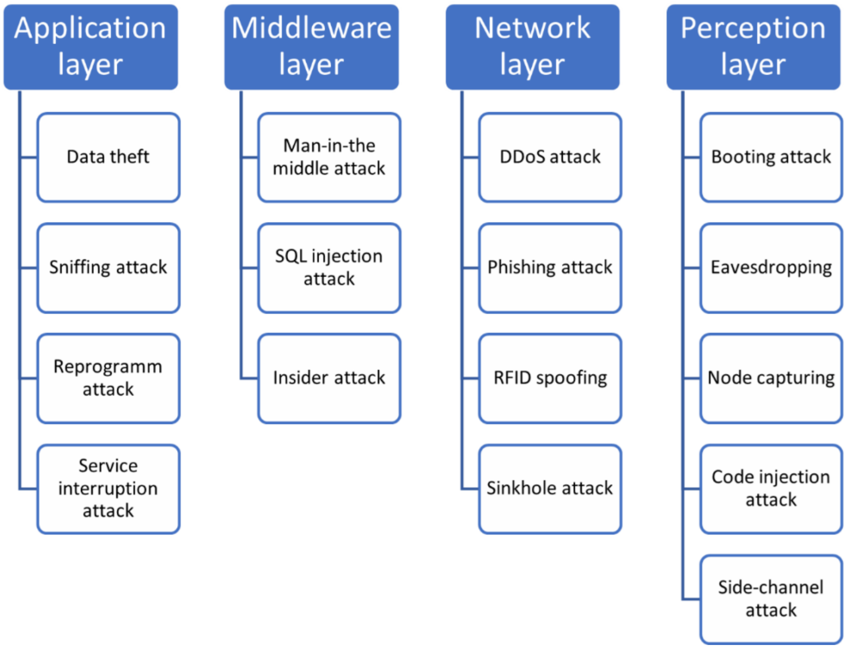

Fig. 3. Common threats in IoT layers

A. Perception layer

The perception layer represents the physical layer of IoT and is responsible for data collection and its transmission. Utilities working on this layer include sensors (e.g., camera sensors, temperature sensors, chemical sensors, detection sensors, and humidity sensors), and wireless sensors networks (WSNs), global positioning systems (GPS), RFID systems, and electronic data interfaces (EDI). Hence, this layer provides most of the data collection. The attacks on utilities working on this layer are mainly aimed at the sensors. In the following, we list the most common attacks (Tukur, Thakker, & Awan, 2019).

1) Booting attack: Usually, all the security services are enabled when a device is in working mode. But between the booting, or startup, and working mode there is a window when the security services are not fully enabled. Hence, at this moment a device is vulnerable to possible attacks. Moreover, edge devices due to power savings are in constant sleep-wake modes. Therefore, they are more likely to be vulnerable to these attacks.

2) Eavesdropping: An interloper can get in the communication stream between nodes within a closed network to listen to the data transmitted. For example, this often happens with poorly secured baby cameras, smart TVs, etc.

3) Node capturing: This type of attack is executed via replacement of the original node with the intruder's one which enables him to get access to parts or, in the worst case, to the entire network.

4) Code injection attack: As the software of the IoT nodes is usually updated OTA (over the air), the opportunity to inject a malicious code during this activity by the assailer might give him unauthorized access to the system, which can lead to the execution of unwanted actions.

5) Side-channel attacks (SCA): A data leak can happen due to a side-channel attack which involves gaining delicate information from the processor chips by so-called electromagnetic attacks, timing attacks, radiation emitted by a computer screen to view the information before its encryption.

B. Network layer

The main function of the network layer is data handling, which includes data preparation and transmission, message routing, publishing, and managing the messages. The data are obtained from the perception layer and then sent further to the middleware layer by divergent communication channels as GSM (Global System for Mobile), WiFi (Wireless Fidelity), and Ethernet (Weyrich & Ebert, 2016). As Weyrich et al. (Weyrich & Ebert, 2016) mentioned, the network layer transmits data between perception and middleware layers, hence plenty of attacks here can be experienced (Mao, Kawamoto, Liu, & Kato, 2019).

1) DDoS attack (Distributed denial of service): Attackers using DDoS attacks try to disrupt the normal traffic functioning of a targeted server resulting in overflooding the server with unwanted requests, thus making the service unavailable for other users. The DDoS attack is like DoS (Denial of service attack), but it is used for attacking other compromised devices, such as poorly secured infected IoT. Such a group of devices is known as a botnet.

2) Phishing attacks: This technique is used to gain full access to a particular IoT network with the help of the human factor. The basic principle is that the attacker sends an e-mail containing a link to some page that requires the user to enter his credentials, in most cases e-mail and password. Either for registration into a fake internet game, where the user can win a prize, or into a page that looks like a login page of a social network or online payment service website (e.g. PayPal), asking for the user's credentials. As this e-mail is sent to thousands of e-mail addresses, the attacker relies on somebody entering his credentials. As users usually have only one password and e-mail for all their accounts, after this action the attacker can gain access to all their sensitive data, including full access to a particular IoT network.

3) RFID spoofing and cloning: Even though RFID tags use plenty of security measures, such as different operational frequencies and different protocols, they can still be compromised. First, they can be cloned, which is a process of duplication of the original RFID tag. Therefore, they can be used for spoofing, which means to use a cloned RFID tag to gain access somewhere. Hence, it is used in access or asset management operations.

4) Sinkhole attack: It is a type of routing attack where false routing details are forwarded to nodes in a network causing a huge amount of network traffic. The attack is initiated from a compromised node that has been compromised by the attacker which infiltrated into the network. Besides false routing attacks, this can be used to issue a variety of other attacks.

C. Middleware layer

This layer provides software utilities that make the communication between IoT components possible by data filtering, analysis of data semantic, management, and discovery of the device and access control (Weyrich & Ebert, 2016). Hence, the middleware layer has two main tasks. The first one is confirming the authenticity of the user, and the second is data transfer. The main tasks of this layer (Hu, Zhang, & Wen, 2011) are listed below.

1) Man-in-The-Middle attack: In this type of attack, the perpetrator pretends to be the legitimate user of an IoT system being in between the communication of two users who are communicating within their network with each other. As their communication goes through the cyber attacker, he can interact with both participating sides, impersonates them both trying to gain access to the information they are trying to send to each other. Thus, the perpetrator can control and manipulate the conversation.

2) SQL injection attack: A very serious threat to any system may result in unauthorized access, confidential data loss or even exploiting the whole network or individual machines. An intruder inserts a particular malicious SQL statement in the vulnerable web applications, which are connected to the backend databases, resulting in their compromising.

3) Insider attack: During this attack, the cyber attacker appears to be an authentic member of the network. Hence, it is very difficult to identify attacks like these. The perpetrator can be a present or former member with access to the details of the system resulting in the ability to launch different types of attacks within the network. Hence, it is very important to keep ACL up to date at any time.

D. Application layer

The application layer is the topmost one in this architecture responsible for providing services and establishing the sets of protocols used for messages passing at the application layer. It is the interface bridge between the IoT devices and the network. For instance, the end IoT device is a computer with a browser as an application layer using protocols such as HTTP, HTTPS, DNS, SMTP, and FTP. This layer can be further divided into two sub-layers (Weyrich & Ebert, 2016):

- Application service sub-layer: Its main function is to span the connection between the end-user and applications; hence it is over the application layer of IoT.
- Data management sub-layer: Tasks performed by this sub-layer include machine-to-machine (M2M) services, Quality of Service (QoS), data process, and directory services. As this layer is in this architecture considered as the final one where the end-user has a direct connection to, plenty of threats are possible to occur.

1) Data theft: The data which are collected by IoT devices with their sensors are most vulnerable while in transit. Intruders can steal the data easily and misuse them for personal use or resell it to another person if proper security protocols are not applied and followed.

2) Sniffing attack: If the data packets are poorly encrypted or without encryption at all, they can be caught, and sensitive data can be extracted with the use of sniffers during its transmission.

3) Reprogram attacks: If the IoT device's programming process is not secured, an intruder can remotely reprogram the IoT device easily resulting in making another infected device in his growing botnet, misusing collected data, etc.

4) Service interruption attack: Due to artificially making the services of an application's network too busy to access to the legitimate users, the network becomes unavailable resulting in its significant slowdown or denial of service.

V. Countermeasures

The whole IoT ecosystem contains three major elements: users, hardware, and software. Hence, to ensure a secure environment within a network, designers and developers must focus on all of the elements involved. Focusing on the users and their behavior within the network can give the designers and developers valuable insights, and enable them to understand better the problems of the whole system, resulting in the enhancement of overall IoT security, and protecting users' privacy and minimizing their risks by educating them to be more aware of their surroundings. Furthermore, to observe how the users interact with the system can be useful to implement appropriate security countermeasures. Some of the *traditional* countermeasures include security protocols, single sign-on, access, and authentication controls, security awareness, establishing trust and privacy by design (Ogonji, Okeyo, & Wafula, 2020).

In this section, we present some new technologies, strategies, and architectures that have gained popularity over the years for being very helpful in enhancing security, including Fog Computing, Blockchain Technology, Edge computing, and Machine learning (Baouya et al., 2020; Ozay et al., 2016). We also present the main challenges related to the creation of an Intrusion Detection System (IDS) for IoT.

A. Fog Computing

Internet of Things and cloud computing are powerful technologies that can work together. IoT facilitates utilizing and incorporating smart applications and cloud computing provides needed space and functionalities that can help manage, store and process the data (Rahman et al., 2019). As IoT gathers a lot of data in real-time using all sorts of devices, services, and technologies, there is a need for storage of this gathered data for possible future analyses and processing. Hence, the cooperation between both technologies has become a beneficial solution which leads to better efficiency in organization and security of the stored data. As the technologies evolve, the attacks and threats become more sophisticated as well. Hence, it was found that cloud computing itself lacks some features. Therefore, the fog computing was introduced to aid the drawbacks of cloud computing itself and make it more efficient and secure.

The basic principle of fog computing is that the fog extends the cloud enabling it to be closer to the things which interact with IoT data. The fog can be described as an additional layer between the end nodes and the cloud. It provides additional detection, invalidation, and reporting of malicious activities. The fog works as a smaller inner cloud within the big cloud, and, thus, the fog also provides isolation from the major cloud to be infected and deals with the security incidents on its own.

Figure 4 represents how the fog can extend the cloud. Devices with computing, network connectivity, and storage, known as fog nodes, can be deployed anywhere with a network connection, such as in a vehicle, water reservoir, or traffic systems. Examples are switches, routers, embedded servers, and video surveillance cameras.

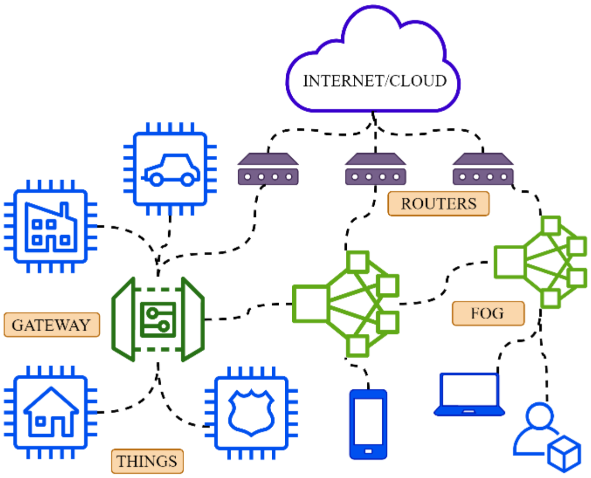

Fig. 4. The Fog extends the Cloud closer to the devices producing data

The major advantages of fog computing for IoT security are:

- Whenever the IoT system is attacked, this attack must go through the fog layer where it can be identified and mitigated. This layer acts as a middleman between the end-user and the cloud.
- As the data is stored in the fog rather than on the devices, the risk of attacks to a great extent has been reduced. Moreover, as the fog is a smaller unit than the cloud unit, it can identify these issues faster and react accordingly preventing the broader part of the network to be compromised.
- Fog computing facilitates discovering malicious activities, such as malware, by being able to red flag them when a problem appears.
- As fog computing is a relatively closed unit, the information transmitted is transported within the fog network rather than through the whole network, if possible. Hence, the chances of eavesdropping are minimized as the network traffic is reduced (Rahman et al., 2019).

This solution also presents some challenges and limitations such as the guarantee of privacy between the fog and IoT devices, the software update capabilities of IoT devices need to handle remote security updates, and the scalability and efficiency of IoT solutions need to be designed to overcome the limitations of resource constrained IoT devices.

B. Blockchain technology security solution

From a security point of view, the IoT applications and platforms lack the security feature in the decentralization of information collected as all data are stored on a centralized cloud. Hence, this issue may be solved by implementing blockchain technology into the centralized cloud system (Kshetri, 2017). Moreover, blockchain technology prevents data duplicity, sensors' data tracking, and offers safe data transfer. With the help of various cryptography techniques, continuously growing blocks containing lists of records are made forming a circulated ledger known as blockchain.

The advantages of implementing blockchain technology in IoT are:

- As blockchain is a distributed system, when a particular part of a system is attacked and its security fails, the entire system is not affected.
- Blockchain can be implemented in every layer of IoT as a suitable utility for data transport.
- Being a decentralized system with cryptographic hash functions for data encryption, it is much harder for the attacker to perform successful cyber theft as data are not centralized on one cloud.
- Based on smart contracts (as represented in Figure 5), data in blockchain can be only accessed by authorized users. Even if the node in a network is infected, the data cannot be read as they are encrypted with appropriate keys.
- IP spoofing and IP address forgery attacks are more difficult due to blockchain-based identity and access management systems as the blockchains cannot be altered. Hence, devices can't be connected to a network using a fake identity and fake signatures.

As presented in the previous list, blockchain technology can be part of IoT security solutions. However, blockchain technology in itself poses research challenges to be tackled with regards to its scalability, efficiency, arbitration/regulations, and key collision.

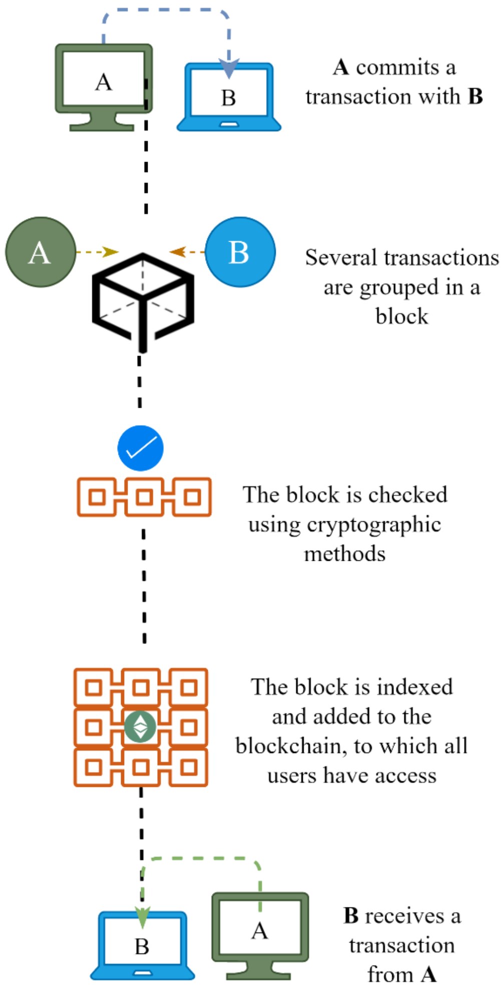
A
B
A commits a transaction with **B**
A
B
Several transactions are grouped in a block
The block is checked using cryptographic methods
The block is indexed and added to the blockchain, to which all users have access
B
A
B receives a transaction from **A**

Fig. 5. Smart contracts

Some examples of challenges and limitations in this field are blockchain vulnerabilities, such as the consensus mechanism depending upon the miner's hashing power can be compromised, and the private keys with limited randomness, which attackers exploit to compromise the blockchain accounts.

C. Edge computing security solutions

Edge computing takes the storage of data and computation much closer to the location of use, thus saving the bandwidth of the network and improving response time (Sodhro, Pirbhulal, & de Albuquerque, 2019). It is very similar to fog computing, but the main difference is that fog computing processes data within a fog node or IoT gateway situated within LAN, whereas edge computing processes the data on the devices or sensors themselves without transferring them. Figure 6 represents the main differences between fog and edge computing.

Hence, edge computing is a fast-processing utility that has multiple positive effects of implementation in IoT applications:

- As data can be processed at the edge, only necessary data can be sent to the cloud for further processing and storage. Therefore, it leads to saving the cost of bandwidth and faster processing of basic tasks.
- Unlike in fog computing, data are stored at the local internet or within the device itself. This reduces the possibility of data theft during its transmission due to lowering the amount of data transported.
- One of the most notable advantages of edge computing is the ability to respond very quickly as the data are processed in the device or nearby. Moreover, with a combination of fog computing and edge computing, we can achieve even better results in terms of response time and security of the system, which can even save lives. For instance, consider an Ambient Assisted Living (AAL) application in which an elderly person has a smart wearable device monitoring their heart rate or other life functions. As the wearable device would be the edge, it can detect a sudden life-threatening change in the elderly person's body and send this information to the caregiver. Without the fog layer, there might be a possibility that the cloud is under DDoS attack, hence the caregiver would not receive the information and do necessary steps to save the person's life. But as the fog would be implemented as the processing middle layer, the possibility of dysfunction is lowered, hence the alert can be processed by fog itself without the cloud involvement resulting in a convenient and quicker response.

We have introduced some positive effects on using edge computing in IoT security but there are still many challenging and open research issues that include: securing the edge layer, dealing with untrusted edge layer, lightweight protocols for end device-edge communications, as well as secure operating systems and lightweight virtual machines.

D. Machine learning security solutions

Machine learning (ML) is part of the Artificial Intelligence (AI) discipline and can make devices and machines infer knowledge from the data (Hussain, Hussain, Hassan, & Hossain, 2020). Some well-known applications of ML in IoT devices include Google Assistant, Amazon Alexa, or Apple Siri. As machine learning has plenty of advantages in other disciplines, some of the ones applicable for IoT are:

- Use of machine learning can enhance the security in terms of malware and DDoS attack detection and, with the use of Deep Learning (DL), it can effectively find patterns in the previously made attacks. Hence, potentially future attacks can be predicted, identified, and mitigated faster and more efficiently.
- The following point is coherent with the previous one in terms of attack detection. As machine learning algorithms can detect possible attacks, they can also mitigate false attack alerts and false error alerts by using various techniques of machine learning, such as Support Vector Machines (SVM) (Hussain et al., 2020).
- Utilization of machine learning properties can lead to cost and energy consumption reduction, improvement of customer care, and efficiency.

ML algorithms could be used to improve the IoT security domain, although they have some limitations in the IoT environment, such as scalability, complexity, latency, compatibility, and vulnerability. Learning efficiency, response time, automatic feature selection and parameter tuning strategies are also challenging in such context.

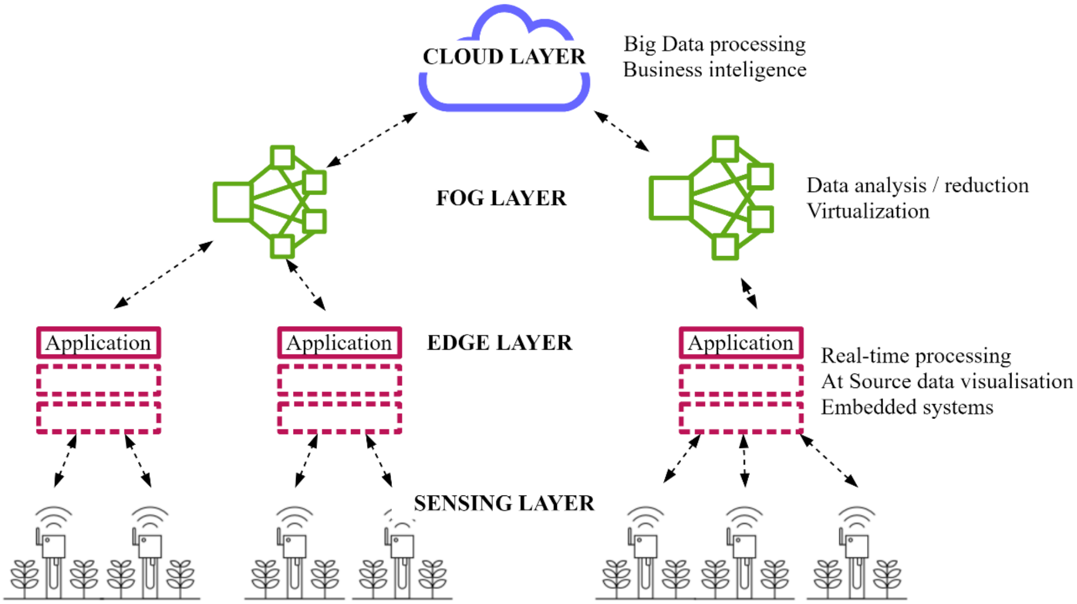

Fig. 6. Data process within network

E. Intrusion Detection Systems

Conventional intrusion detection systems use techniques based on packet capture and analysis to detect intrusions or attacks. *Deep packed inspection* (DPI) techniques scan packet headers and examine the content in the application data field, looking for any evidence of attack (Abuadlla, Kvascev, Gajin, & Jovanovic, 2014). However, the use of DPI-type IDS is impractical for high-speed connections and inspection is not possible when the contents of the packet data field are encrypted (Husak, Velan, & Vykopal, 2015). In *stateful packet inspection* (SPI) techniques, the semantics of the protocol are checked and any record outside the defined is considered an intrusion or anomaly. However, this technique is oriented towards known protocols and does not affect unknown protocols.

Also, it does very little when it comes to malicious code as it does not analyze the payload of packages. Finally, both techniques are computationally expensive and can create a bottleneck in the network (Koch, 2011; Liao, Lin, Lin, & Tung, 2013).

Considering the limitations of techniques based on packet analysis, DPI, and SPI, and considering the less computational and resource requirements of the approach based on flow analysis, an alternative solution against intrusions and attacks in IoT ecosystems may be using an IDS based on IP flow analysis (Santos, Rabadão, & Gonçalves, 2019). This type of IDS has as a strong point in its favor: the lower need for computational resources to operate, as they only analyze the flow records that contain aggregated information from packet headers, reducing the amount of data that needs to be processed. In this way, they can provide an answer almost in real-time, low implementation cost, fewer privacy concerns, and that can be used with traffic consisting of packages that have their encrypted payload. A weakness of these IDS is the difficulty in detecting some attacks using only information from the packet header, so many of the known attacks are not detected. When compared to IDS based on packet detection, with the cryptographically unprotected payload, the detection of network attacks hidden in the packet payload is not as accurate as packet-based detection. However, the increasing use of end-to-end encryption in distributed applications, such as web portals, mobile applications, and e-mails, has left limited space for the application of payload-based intrusion detection systems and opens the way for the IDS based on flow analysis.

Recently, there has been a huge increase in research on IDS for IoT, especially concerning the application of ML techniques (especially deep learning) (Dutta & Granjal, 2020). However, ML-based techniques face the challenge of the low availability of realistic, high-quality datasets that contain diverse attacks for the IoT. In Dutta & Granjal (2020), the authors also identify a strong effort in the optimization of existing algorithms for implementation in IoT, and in the development of nodes with high computational performance to perform the tasks of IDS in IoT, through the adoption of fog and edge computing. Implementing an IoT IDS using edge and fog computing would allow the detection of intrusions in IoT ecosystems with less resource consumption. (Chaabouni, Mosbah, Zemmari, Sauvignac, & Faruki, 2019). However, most of the existing proposals detect a low number of attacks and focus mostly on attacks on routing and DoS and, less frequently, on attacks related to the source of the data (Dutta & Granjal, 2020).

VI. Future Directions

The use of Intrusion Detection Systems (IDS) in the context of IoT is still an open and promising issue. Despite considerable progress in the development of IDS solutions designed specifically for IoT ecosystems, existing solutions still have numerous limitations. Also, some solutions require considerable computational overhead or modification of the software of IoT devices that, in an environment of limited computational resources, turns out to be a weakness.

Regarding the detection methodology, and although there is no consensus on which of the methodologies will be the most appropriate, the solutions that use the methodology based on anomalies are the ones that consume more computational and energy resources, while the methodologies based on signatures or specifications are the ones that require fewer resources. However, anomaly-based detection is the one most often proposed in studies, in part because of its potential to detect unknown attacks. For this, it is necessary to develop, analyze and compare lighter and optimized anomaly detection algorithms, mainly based on ML (especially deep learning) for IoT networks (Dutta & Granjal, 2020).

Also, integration of detection techniques based on rules, anomalies, and specifications should be used, to avoid their weaknesses and obtain their benefits. To this end, it will be necessary to dedicate greater effort to the refinement of this integration, namely by improving the modeling of the behavior of IoT ecosystems to allow a better definition and parameterization of network parameters to detect intrusions (Cervantes, Poplade, Nogueira, & Santos, 2015; Bostani & Sheikhan, 2017; Fu, Yan, Cao, Kone, & Cao, 2017).

At the level of the IDS implementation strategy, given the computational limitations of the IoT devices and the privacy and confidentiality requirements of the information collected, the solution may include the exploration of hybrid detection solutions, using edge and fog computing (Chaabouni et al., 2019). This approach will allow decision making close to the perception layer, improving the privacy and confidentiality issues of the information collected and minimizing the need for necessary network resources between the perception layer and the cloud, making use of the computing power of the cloud, during the training phase of machine learning algorithms.

Regarding the intrusion detection capability, the existing solutions are limited concerning the diversity of attacks they detect. Most of the intrusions detected are located at the perception layer of the IoT architecture, at the DoS level, and at the network layer, at the level of routing attacks, possibly due to the use of existing generalist datasets, which do not represent the particularities of IoT systems and applications, leaving other types of intrusions, internal and external, and from other layers, without specific solutions for some IoT protocols. Although some works propose datasets more suited to the reality of IoT (e.g. (Moustafa & Slay, 2015; Sivanathan et al., 2017; Bezerra et al., 2018; Verma & Ranga, 2019)), there is a need to intensify this work, in the sense of creating public datasets that include the different IoT protocols and their threats/attacks, to be able to develop IDS solutions adapted to the diversity of threats to which the IoT ecosystems are subject.

These datasets, specifically suitable for IoT, must be public and serve as a reference for the validation of solutions proposed by the scientific community, and must be properly labeled and support a wide variety of attacks and protocols used in IoT ecosystems. In this way, it will be possible to improve the IDS validation strategy, as it will be possible to compare, in a clear, practical, and convenient way, the different IDS developed.

At the level of IoT technologies and protocols, the vast majority only cover perceptual layer protocols such as 6LoWPAN and RPL, which means support, interoperability, and expandability with other technologies and protocols, used at the network layer or application, are not addressed in the analyzed proposals.

Besides, only a few solutions refer to aspects or features related to the privacy of network traffic and the management of the communication of internal messages and IDS alerts. This is an important topic, because if the internal messages between the various components of an IDS or the intrusion alert messages are intercepted and tampered with it will result in the loss of the reliability and effectiveness of the IDS.

Finally, it should be noted that most solutions presented make use of packet capture, and respective payloads, to develop their intrusion detection processes. Intrusion detection solutions based on the analysis of IP traffic flows can be considered, reduce the use of resources, such as the processing and storage of network packets, which is especially important when using devices with limited resources at the computational level.

VII. Conclusion

In this chapter, the authors identified the main security aspects of the Internet of Things. and identified possible attacks, threats, and vulnerabilities of IoT.

The authors characterized the IoT in terms of its processing cycle. Then, the authors identified the processes and features that are the most common security concerns in IoT networks, namely identification, authentication, data integrity, trust, data confidentiality, access control, data privacy, and data availability. The authors described the IoT layers and architecture, and the attacks and threats that are the most common for each layer.

Then, the authors presented a set of countermeasures based on new technologies, strategies, and architectures to enhance IoT security, namely security solutions based on Fog and Edge Computing, Blockchain Technology, Machine learning, and Intrusion Detection Systems (IDS) for IoT. Each of such solutions has its advantages and application challenges, but the limitations of resource constrained IoT devices impose constraints on the scalability and efficiency of most proposed IoT cybersecurity solutions.

The IDS for IoT is the authors' main research direction in terms of countermeasures for IoT. Such IDS should use lighter and optimized anomaly detection algorithms, mainly based on machine learning. Also, integrating detection techniques based on rules, anomalies, and specifications would increase the IDS efficiency. Computational limitations of the IoT devices and privacy and confidentiality requirements of collected data lead to hybrid solutions, which use Edge and Fog computing.

Datasets specifically suitable for IoT must be created and turned public to serve as a reference for the validation of proposed solutions. Such datasets must be labeled and support a wide variety of attacks and protocols used in IoT ecosystems. Also, the use of intrusion detection solutions based on the analysis of IP traffic flows can be considered, reducing the use of resources, such as the processing and storage of network packets, which is especially important when using devices with limited resources at the computational level.

As future work, the authors intend to advance the study of IDS for IoT, mainly with the application of machine learning techniques in this context. The authors also plan to prepare data sets of the IoT context for benchmarking solutions of the literature.

Acknowledgment

This work was partially funded by National Funds through the FCT (Foundation for Science and Technology) in the context of the project UIDB/04524/2020.

References

Abuadlla, Y., Kvascev, G., Gajin, S., & Jovanovic, Z. (2014). Flow-based anomaly intrusion detection system using two neural network stages. *Computer Science and Information Systems*, *11*(2), 601–622.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys Tutorials*, *17*(4), 2347-2376. doi: 10.1109/COMST .2015.2444095

Al-Sarawi, S., Anbar, M., Alieyan, K., & Alzubaidi, M. (2017). Internet of Things (IoT) communication protocols: Review. In *2017 8th International Conference on Information Technology (ICIT)* (p. 685690). doi: 10.1109/ICITECH.2017.8079928

Antao, L., Pinto, R., Reis, J. P., & Gonçalves, G. (2018).˜ Requirements for testing and validating the industrial Internet of Things. In *2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)* (p. 110-115). doi: 10.1109/ICSTW.2018.00036

Atzori, L., Iera, A., & Morabito, G. (2010, 10). The Internet of Things: A survey. *Computer Networks*, 2787-2805. doi: 10.1016/j.comnet.2010.05.010

Baouya, A., Chehida, S., Bensalem, S., & Bozga, M. (2020). Fog computing and blockchain for massive IoT deployment. In *2020 9th Mediterranean Conference on Embedded Computing (MECO)* (p. 14). doi: 10.1109/MECO49872.2020.9134098

Basha, S., & S A K, J. (2016, 03). An intelligent door system using raspberry pi and amazon web services IoT. *International Journal of Engineering Trends and Technology*, *33*, 84-89. doi: 10.14445/ 22315381/IJETT-V33P217

Bezerra, V. H., da Costa, V. G. T., Martins, R. A., Junior, S. B., Miani, R. S., & Zarpelao, B. B. (2018). Providing IoT host-based datasets for intrusion detection research. In *Anais do XVIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais* (pp. 15–28).

Bostani, H., & Sheikhan, M. (2017). Hybrid of anomaly-based and specification-based IDS for Internet of Things using Unsupervised OPF based on Map-Reduce Approach. *Computer Communications*, *98*, 52–71.

Cervantes, C., Poplade, D., Nogueira, M., & 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* (pp. 606– 611).

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

Dutta, M., & Granjal, J. (2020). Towards a secure Internet of Things: A comprehensive study of second line defense mechanisms. *IEEE Access*, *8*, 127272–127312.

Farooq, M., Waseem, M., Khairi, A., & Mazhar, P. (2015, 02). A critical analysis on the security concerns of Internet of Things (IoT). *International Journal of Computer Applications*, *111*, 1-6.

Fu, Y., Yan, Z., Cao, J., Kone, O., & Cao, X. (2017). An automata-based intrusion detection method for Internet of Things. *Mobile Information Systems*, *2017*.

Gigli, M., & Koo, S. (2011, 01). Internet of Things: Services and applications categorization abstract. *Adv. Internet of Things*, *1*, 27-31. doi: 10.4236/ait.2011.12004

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645 - 1660. doi: 10.1016/j.future.2013.01.010

Hu, C., Zhang, J., & Wen, Q. (2011). An identity-based personal location system with protected privacy in IoT. In *2011 4th IEEE International Conference on Broadband Network and Multimedia Technology* (p. 192-195). doi: 10.1109/ICBNMT.2011 .6155923

Husak, M., Velan, P., & Vykopal, J. (2015). Security monitoring of HTTP traffic using extended flows. In *2015 10th International Conference on Availability, Reliability and Security* (pp. 258–265).

Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine learning in IoT security: Current solutions and future challenges. *IEEE Communications Surveys Tutorials*, *22*(3), 16861721. doi: 10.1109/COMST.2020.2986444

Koch, R. (2011). Towards next-generation intrusion detection. In *2011 3rd International Conference on Cyber Conflict* (pp. 1–18).

Kshetri, N. (2017). Can blockchain strengthen the Internet of Things? *IT Professional*, *19*(4), 68-72. doi: 10.1109/MITP.2017.3051335

Liao, H.-J., Lin, C.-H. R., Lin, Y.-C., & Tung, K.-Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, *36*(1), 16–24.

Mao, B., Kawamoto, Y., Liu, J., & Kato, N. (2019). Harvesting and threat aware security configuration strategy for IEEE 802.15.4 based IoT networks. *IEEE Communications Letters*, *23*(11), 2130-2134. doi: 10.1109/LCOMM.2019.2932988

Moustafa, N., & 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* (pp. 1–6).

Neisse, R., Steri, G., Baldini, G., Tragos, E., Nai Fovino, I., & Botterman, M. (2015, 01). Dynamic context-aware scalable and trust-based IoT security, privacy framework. In (p. 199-224). River Publishers.

Nitti, M., Girau, R., & Atzori, L. (2014). Trustworthiness management in the social Internet of Things. *IEEE Transactions on Knowledge and Data Engineering*, *26*(5), 1253-1266. doi: 10.1109/TKDE.2013 .105

Ogonji, M. M., Okeyo, G., & Wafula, J. M. (2020). A survey on privacy and security of Internet of Things. *Computer Science Review*, *38*, 100312. doi: https://doi.org/10.1016/j.cosrev.2020.100312

Ozay, M., Esnaola, I., Yarman Vural, F. T., Kulkarni, S. R., & Poor, H. V. (2016). Machine learning methods for attack detection in the smart grid. *IEEE Transactions on Neural Networks and Learning Systems*, *27*(8), 1773-1786. doi: 10.1109/TNNLS.2015.2404803

Rahman, M. A., Rashid, M. M., Hossain, M. S., Hassanain, E., Alhamid, M. F., & Guizani, M. (2019). Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city. *IEEE Access*, *7*, 18611-18621. doi: 10.1109/ ACCESS.2019.2896065

Riahi Sfar, A., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks*, *4*(2), 118 - 137. doi: https://doi.org/ 10.1016/j.dcan.2017.04.003

Santos, L., Rabadão, C., & Gonçalves, R. (2019). Flow monitoring system for IoT networks. In *World conference on information systems and technologies* (pp. 420–430).

Sehrawat, D., & Gill, N. S. (2019). Smart sensors: Analysis of different types of IoT sensors. In *2019 3rd International Conference on Trends in Electronics and Informatics* (p. 523-528). doi: 10.1109/ICOEI.2019.8862778

Sicari, S., Rizzardi, A., Grieco, L., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146 - 164. doi: https://doi.org/10.1016/j.comnet .2014.11.008

Sikder, A. K., Petracca, G., Aksu, H., Jaeger, T., & Uluagac, S. (2018). *A survey on sensor-based threats to internet-of-things (IoT) devices and applications.* arXiv preprint arXiv:1802.02041.

Sivanathan, A., Sherratt, D., Gharakheili, H. H., Radford, A., Wijenayake, C., Vishwanath, A., & Sivaraman, V. (2017). Characterizing and classifying IoT traffic in smart cities and campuses. In *2017 IEEE Conference on Computer Communications Workshops (Infocom Wkshps)* (pp. 559–564).

Sodhro, A. H., Pirbhulal, S., & de Albuquerque, V. H. C. (2019). Artificial intelligence-driven mechanism for edge computing-based industrial applications. *IEEE Transactions on Industrial Informatics*, *15*(7), 4235-4243. doi: 10.1109/TII .2019.2902878

Swamy, S. N., Jadhav, D., & Kulkarni, N. (2017). Security threats in the application layer in IoT applications. In *2017 International Conference on I-SMAC (IoT in social, mobile, analytics and cloud) (I-SMAC)* (p. 477-480). doi: 10.1109/I-SMAC.2017 .8058395

Tukur, Y. M., Thakker, D., & Awan, I. (2019). Ethereum blockchain-based solution to insider threats on perception layer of IoT systems. In *2019 IEEE Global Conference on Internet of Things (GCIoT)* (p. 1-6). doi: 10.1109/GCIoT47977.2019.9058395

Ullah, Z., Ahmad, S., Ahmad, M., Ata-ur-Rehman, & Junaid, M. (2019). A preview on Internet of Things (IoT) and its applications. In *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMet)* (p. 1-6). doi: 10.1109/ICOMET.2019.8673468

Verma, A., & Ranga, V. (2019). Evaluation of network intrusion detection systems for rpl based 6LoWPAN networks in IoT. *Wireless Personal Communications*, *108*(3), 1571–1594.

Weyrich, M., & Ebert, C. (2016). Reference architectures for the Internet of Things. *IEEE Software*, *33*(1), 112-116. doi: 10.1109/MS.2016.20