A General Overview of The Internet of Things and Its Future Applications

Sandy Montajab Hazzouri

Faculty of Informatics Engineering , Albaath University, Syria

Email: Samonhaco1994@gmail.com

Abstract

With the great acceleration in the world of digital technology and communications, the globe has turned into a virtual world connected, A new term has appeared, namely the Internet of Things, which refers to a kind of network to connects anything to the Internet based on the protocols prescribed Sensors conduct information exchange and communication to realize intelligent identification, Positioning, Tracking, Monitoring, and management. In this paper, we briefly discussed what the Internet of Things is, its applications, characteristics, and structure.

Keywords: Internet of Things; communication; monitoring; identification

1. Introduction:

The vision of the Internet of Things is to use smart technologies to connect things anytime, anywhere, for anything. The Internet of Things appeared in 1998, and the term Internet of Things was first coined by Kevin Ashton and Kevin Ashton in 1999. As shown in Figure 1, studies show that in 2011 the number of internet-connected devices exceeded the population of the Earth, and in 2020 the number was between 26 and 50 billion users [1]

The Internet of Things (LOT) refers to the use of intelligently connected devices and systems to take advantage of data collected by sensors and actuators embedded in

Machines and others. The Internet of Things is expected to spread rapidly over the coming years, and this convergence will unleash a new dimension of services that improve the quality of life of consumers and the productivity of enterprises, It is a new revolution of the Internet[2]. It allows people and things to be connected anytime, anywhere, anywhere, and anyone, ideally using any network and any service, as shown in Figure (2).

The common definition of the Internet of Things is a network of physical objects. But the internet is not only a network of computers, it has evolved into a network of devices of all types and sizes; such as vehicles،

And smartphones, household appliances, toys, cameras, medical instruments and industrial systems, animals, people, and buildings [4] [3]

In this article, we will shed light on the concept of the Internet of Things, and this article is organized as follows, We will review the applications of the Internet of Things in various fields of life, such as city applications

Then we will address the characteristics of the Internet of Things that you enjoy, and then we will provide an explanation of the layers that make up the Internet of Things, and conclude this article with the concept of security in the Internet

Doi: https://doi.org/10.54216/PMTCS.020103
Received: January 09, 2023 Revised: April 08, 2023 Accepted: July 05, 2023

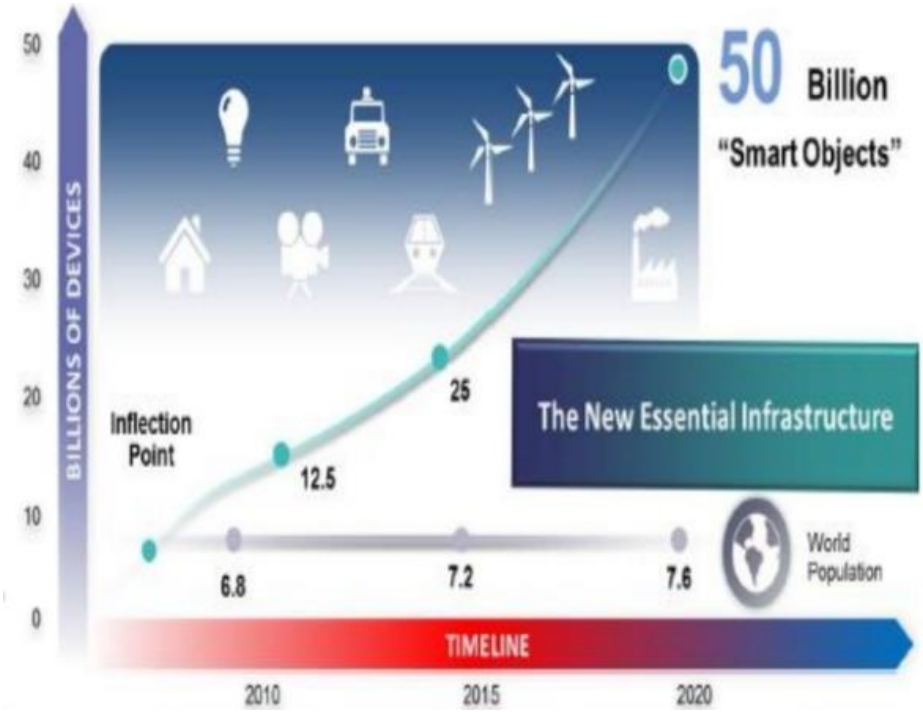


Figure 1: The Internet of Things revolution

2. Internet of Things applications: II.

There are a lot of applications, that can be classified as IoT applications, We mention some of them [3]

Smart Cities (Smart Cities A).

The Internet of Things plays a big role in making cities smart, see Figure (3), through several applications such as monitoring parks in the city, monitoring vibrations and physical components of buildings and bridges, monitoring noise in sensitive places, monitoring the movement of vehicles and linking it to traffic lights, as in Figure (4), and smart street lighting adapted to weather changes [5]

Doi: https://doi.org/10.54216/PMTCS.020103
Received: January 09, 2023 Revised: April 08, 2023 Accepted: July 05, 2023

Figure 2: Smart city applications

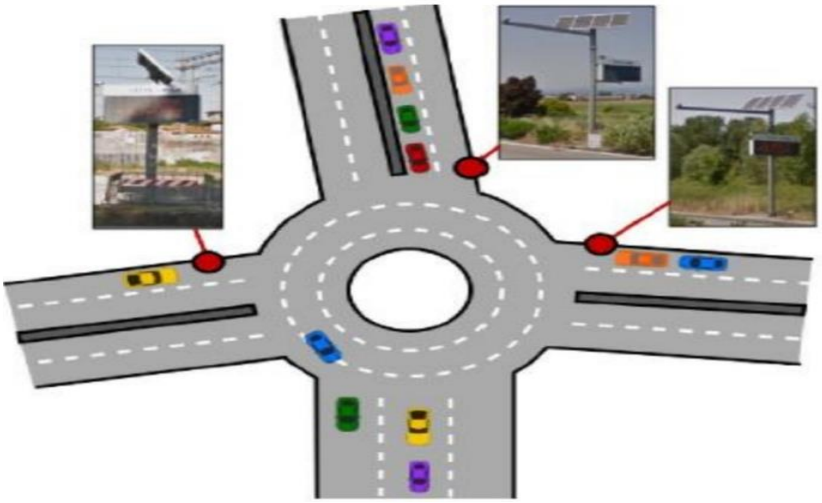
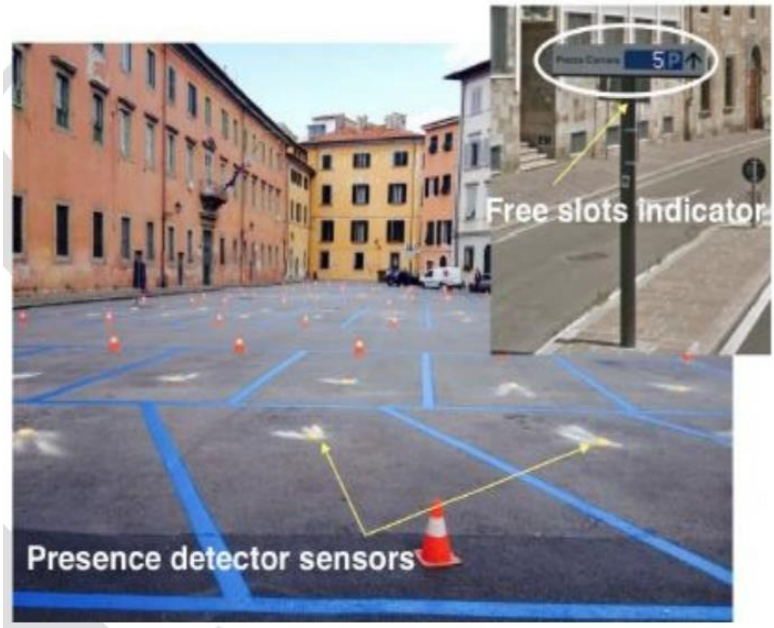


Figure 3: Monitoring the movement of wagons

Smart city applications also fall under the intelligent management of parking lots, which is a big problem in major cities that suffer from congestion, which contributes to reducing traffic in areas

In which all parking lots are occupied. In Figure (5), an example of Intelligent Parking Management is shown where the status of each parking lot is monitored through a dedicated Center for sensing and periodically collected information, and then the collected data is used to create a real-time map of the parking area that can be provided to drivers, through a specific application on their smartphones. In this way, drivers are guided to the nearest (free) parking lot, which saves time and reduces fuel consumption and air pollution [6].



Smart agriculture (Smart Agriculture B).

The Internet of Things can help improve agriculture by monitoring soil moisture, controlling microclimatic conditions to increase the yield and quality of fruits and vegetables, studying weather conditions in them

To predict ice, drought, snow or wind changes information and control humidity and temperature levels to prevent fungus and other microbial contaminants. The role of the Internet of Things in water management includes

Doi: https://doi.org/10.54216/PMTCS.020103
Received: January 09, 2023 Revised: April 08, 2023 Accepted: July 05, 2023

Studying the suitability of rivers and seawater for agriculture and potable uses and monitoring water level changes in rivers, dams, and reservoirs. Figure 6 shows an example of smart farming applications.

Figure 4: Example of smart agriculture applications

Smart health care (Smart health C).

The technologies that the Internet of Things brings to the healthcare field are classified into two basic categories: 1. Tracking objects, employees, and patients, e.g. patient monitoring status to improve workflow in

Hospitals .2 Identification and authentication of persons and includes identification of the patient to reduce accidents harmful to patients and others. Figure 7 shows examples of LOT applications in

The field of health care.

Figure 5: Example of healthcare applications

Smart Environment (Smart environment D).

Nature-related applications include air pollution monitoring to control the CO2 released by factories, automobile exhaust, forest monitoring to detect fires early, and monitoring

Climatic conditions of humidity, heat, and pressure. Figure 6 shows an example illustrating one of the applications of the smart environment.

Doi: https://doi.org/10.54216/PMTCS.020103
Received: January 09, 2023 Revised: April 08, 2023 Accepted: July 05, 2023

Figure 6: Automobile exhaust air pollution monitoring application

Smart Energy (Smart energy E).

Applications that make monitoring energy consumption a goal, such as monitoring and analyzing the flow of energy from turbines and in homes, include controlling the amount of energy required and improving energy efficiency with losses

Less power sources are related to computers and other electronic devices.

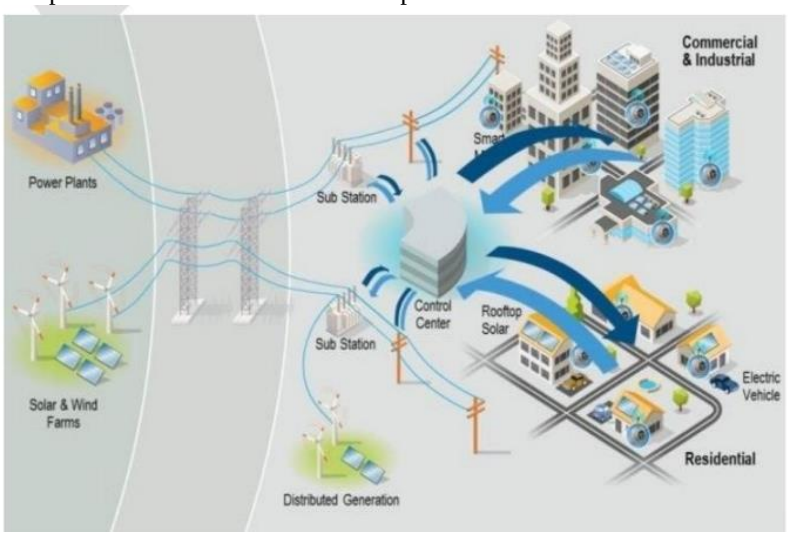


Figure 7: Intelligent power flow monitoring and analysis application

3. Characteristics of the Internet of Things III.

The Internet of Things has many characteristics, some of which are listed below [4] [3]

1) Interconnectivity (Interconnectivity)

The Internet of Things ensures that anything is connected to the global information and communication infrastructure.

2) Heterogeneity (Heterogeneity)

The devices that make up the Internet of Things are heterogeneous because they depend on different hardware platforms and networks, they may be wireless sensors, cellular devices, or others.

Doi: https://doi.org/10.54216/PMTCS.020103
Received: January 09, 2023 Revised: April 08, 2023 Accepted: July 05, 2023

3) Dynamic changes (Dynamic changes)

The state of the devices changes dynamically, for example, the change between sleep and wake States, connection and disconnection, it may also be the location and speed relative to moving devices. Moreover, the number of connected devices can be dynamically variable.

4) Enormous size (abnormal scale)

The number of devices that need to be managed and communicate with each other will be an order of magnitude larger than those that are currently connected to the internet. Here the importance of managing the data exchanged between these devices is shown

And process and utilize them according to the application.

The structure of the Internet of Things (IOT ARCHITECTURE)

It consists of several layers supporting LOT technology, we will list below the most common LOT structure [7], which consists of 4 layers as shown in Figure (10):

Smart/ sensitive device layer.

It is the lowest layer in the structure of the Internet of Things, consisting of smart equipment integrated with sensors. Sensors ensure the interaction between the digital world and the physical world, making it possible by

Processing and collection of information in real-time. The sensor can measure the physical property and convert it into a signal that can be understood by the devices. There are several types of sensors for different goals and objectives. The sensors can take measurements such as temperature, air quality, humidity, and pressure

Sensors can be classified by a single target such as environmental sensors, body sensors, and vehicle sensors. Most sensors need to connect with other sensors that work as gateways, this can be in the form of a LAN network such as Ethernet (wired) wireless such as WiFi, or a PAN network such as Zigbee or Bluetooth.UWB some sensors do not need bundled nodes but communicate with the server or application

Sensors that use low power and a low data connection rate form one of the most common types of networks, which are WSN wireless sensor networks, which have gained great popularity by being able to handle a large number of nodes while retaining battery life and covering large areas.

Network/ gateway layer (Gateway/Networks Layer B).

The large volume of data generated by the information captured by the sensors requires a high-performance infrastructure capable of handling it, whether the transmission medium is wired or wireless. The networks

Current ones are constrained by a very different set of protocols, which have been used to support machine-to-machine (M-2-M) networks and their applications. So with the need to serve a wide range of LOT services and applications such as high-speed transport services, there is a need for multiple networks with various technologies and access protocols to work with each other. These networks can be of the private, public, or hybrid model to support communication requirements such as latency, packet width, and security.

Service management layer (Management Service Layer C).

Service management makes information processing possible through process modeling, equipment management, analysis, and security control. One of the important features of the management service is the engines of business rules and processes. The Internet of Things combines communication and interaction between objects and systems to provide information in the form of events or data such as the temperature of goods, current location, and data traffic. Some of these events such as periodic allergic data capture need to be filtered or routed to post-processing systems،

While the other requires a response to urgent situations such as emergencies related to the patient's health conditions.

In terms of analysis, several analysis tools can be used to analyze additional interrelated amounts of information from a large data flow, and these data can be processed at a high speed.

For example, the use of memory analysis reduces the time of data request and increases the speed of decision-making, and flow analysis occurs in real-time, as a result, decision-making is within seconds.

Doi: https://doi.org/10.54216/PMTCS.020103
Received: January 09, 2023 Revised: April 08, 2023 Accepted: July 05, 2023

The higher layer of applications can be protected from the need to process unnecessary data and reduce the risk of revealing the privacy of the data source, since filtering technologies such as data anonymization, integration, and data synchronization, are used to hide the basic information used in related applications. Security should be imposed on the entire LOT architecture directly from the smart device layer down to the application layer. System security prevents hacking or control of the system by unauthorized individuals, as a result minimizing the likelihood of danger.

Application layer (Application Layer D).

Applications include the field of smart environments in several sectors such as transport, construction, City, Agriculture, Lifestyle, Commerce, Industry, emergency, healthcare, education, culture, tourism, environment, and energy.

Security in the Internet of Things V.

Security is defined as the procedural protection of the source from physical damage, unauthorized access, or theft, by maintaining the confidentiality and integrity of information and ensuring authentication and non-leakage

Information. Since the Internet of Things depends on the connection of a myriad of devices for its operation, there is a very high probability of being subjected to a security attack. In Information Technology, an attack is

An attempt to destroy, expose, alter, disable, steal, or gain unauthorized access to a source. The Internet of Things attack is not new, but what is new is the scale and relative simplicity of attacks in the Internet of Things (LOT), millions and billions of devices can be potential victims of traditional cyber-attacks [8]

For example, an analysis conducted by researchers in [9] showed that 13% of 156,680 connected devices were vulnerable to a security vulnerability.

Security requirements in LOT networks VI.

Security must be considered throughout the LOT lifecycle, from the initial design to the operation of services. The main security requirements in LOT scenarios include authentication, authorization, confidentiality, and reliability, and we explain each of these requirements:

Data reliability (Data confidentiality A).

The data sent or received by the node must be reliable and this is achieved by combining safety and reliability by encryption. For example, in wireless body networks

The represented value of the sugar meter must be sent so that it is guaranteed to arrive without being subjected to a sudden change or being seen by an unauthorized person to maintain confidentiality

Patient data is done using encryption, although there are challenges related to the application of encryption techniques such as limited memory and limited processor capacity [10].

Confidentiality (Privacy B).

Maintaining confidentiality in the Internet of Things is still a major challenge [11-12]. Confidentiality includes the security of personal information as well as the ability to control what happens to this information. The problems of

Confidentiality with LOT systems is complicated because the system is more than a set of parts. Confidentiality considerations for low-level devices may differ from what is at the level of

Application or data analysis. But at the same time, violations of confidentiality at any level in the system will affect the entire system.

Collecting a lot of private information from smart devices, and controlling this information is weak in current LOT technologies. In many cases, the data is collected in such a way that

Violations of confidentiality occur unnoticed for a long time.

In some cases, the user may not be aware that the LOT device is collecting data about the individual and may share it with third parties. This type of data collection is becoming more and more popular in

Doi: https://doi.org/10.54216/PMTCS.020103
Received: January 09, 2023 Revised: April 08, 2023 Accepted: July 05, 2023

Consumer devices such as smart TVs and smart personal assistants.

Authentication and authorization C.

Authentication and access control technologies are of great importance in the Internet of Things. Without an appropriate access control mechanism, the entire LOT architecture can be hacked, since internet devices

Things largely depend on the reliability of other components associated with them. As a result, an appropriate access control mechanism is crucial to mitigate the flaws in the existing LOT infrastructure [13]

The control mechanisms of the Internet of Things consist of two basic stages: 1. Authentication .2 license, as in Figure (11)

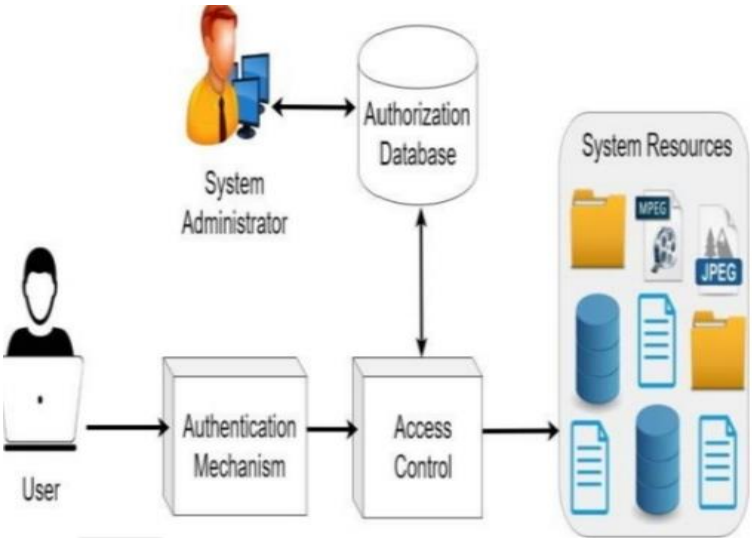


Figure 8: LOT control mechanism system

(**Authentication:** is the process of verifying the identity of an entity[14]. The entity to be verified can be

It's either a human or a machine. Authentication is the first stage of any access control mechanism that can determine the exact identity of the accessing party to establish System Trust.

In most cases, **the man-machine authentication procedure begins with logging** into the online services portal and entering authentication data.

Licensing: is the process of imposing limits and granting privileges to certified entities [15]. In simple terms, this is the determination of the capabilities of an entity in the system. For an entity to be allowed to perform any action, the identity of this entity must first be verified through authentication. According to Figure 11, the administrator usually configures the license database to grant access and rights to system resources. Assigns different rights to each resource such as reading, writing, and execution. Depending on the level of authorization (authorization) that is set by the administrator, each certified entity can perform different actions on resources.

Security risks in the Internet of Things VII.

Security risks in the Internet of Things can be classified into:

A. Typical risks that occur in any internet system: what is meant by security practices

Traditional methods such as locking open ports on appliances, for example, may use a refrigerator

Connected to the internet to send alerts about product inventory and temperature SMTP server is insecure and vulnerable to hacking.

Risks specific to LOT devices B.

Issues specifically related to IoT devices include, for example, they may compromise secure device information, and some IoT devices are too small to support proper asymmetric encryption.

Doi: https://doi.org/10.54216/PMTCS.020103
Received: January 09, 2023 Revised: April 08, 2023 Accepted: July 05, 2023

Safety to ensure no damage C.

Misuse may cause damage to the network, for example, misuse of triggers may cause damage to these triggers and as a result to the network as a whole.

Attacks on LOT networks VIII.

The attack itself may come in many forms, including active network attacks to monitor unencrypted traffic in search of sensitive information; or passive attacks such as monitoring unprotected network connections to decrypt poorly encrypted traffic and obtain authentication information; etc., We mention the common types of cyberattacks are:

Physical attack (Physical Attack A).

The attacker in this attack messes with solid components. This is due to the distributed and unattended nature of the Internet of Things, as devices operate in an open environment [16].

Reconnaissance attack (Reconnaissance Attack B).

It is an attack that results in unauthorized detection and mapping of the network and services or identification of vulnerabilities. An example is scanning network ports, and analyzing traffic.

DOS (Denial of Services Attack)denial of Services attack C.

It is one of the most widespread and easiest attacks to implement in LOT networks, The goal of this type of attack is to try to make network resources unavailable to users, which is

Helping the attacker to easily achieve his goal is the low memory capabilities and limited processing capacity of most devices of LOT networks. It can appear in several forms, for example, for any network

Wireless, "jamming" the channel with an interrupt signal promises an effective DOS attack.

Access attack (Access Attack D).

Unauthorized persons gain access to the network or devices, and they do not have access to them. This attack has two types: The first type is physical access when the attacker can

That accesses the physical device, remote access, and occurs when an attacker manages to gain access to the IP address of a connected device.

Cyber espionage (Cyber Espionage E).

The use of hacking techniques and malware to spy on or obtain confidential information of individuals, organizations, or governments.

Analysis attack (Cryptanalysis Attacks F).

It consists of the attacker who obtained the ciphertext trying to analyze it to reach a cryptographic crack.

Man-In-the-middle MITM(Man-In-the-Middle) attack G.

The concept of a man-in-the-middle attack is an attack in which an attacker or hacker interrupts and penetrates communications between two separate systems. It can be a serious attack because it is an attack

In it, the attacker secretly intercepts and transmits messages between two parties while the parties think that they are communicating with each other directly because the attacker has the original connection, so he can trick the recipient into thinking that he is still receiving a legitimate message.

Such attacks can be very dangerous in the Internet of Things, due to the nature of the "things" that penetrate. For example, such devices can be anything from industrial tools or

Machines or carts to harmless "things" such as smart TVs, smart refrigerators, or motors that are responsible for opening and closing the garage.

Doi: https://doi.org/10.54216/PMTCS.020103
Received: January 09, 2023 Revised: April 08, 2023 Accepted: July 05, 2023

Authentication of devices in LOT networks involves the exchange of possible device identities, so a man-in-the-middle attack would be possible through identity theft [10]

4. Conclusion

The Internet of Things with its applications will change the face of the world. Many research teams have been established from all over the world to conduct research related to the Internet of Things. All this is intended to enable communication with and between intelligent objects, providing communication "anytime, anywhere, any media, anything. So in this article, we presented the most important aspects of the Internet of Things, the various applications of the Internet of Things, and its components. The last part of this paper also highlighted the issue of security in the Internet of Things.

References

[1]. O. Vermesan, P. Friess, "Internet Of Things -from *research and innovation to market deployment*", River Publisher Series communication, 2014.

[2]. V. Bhuvaneswari, and R Porkodi "The Internet of Things (IoT) Applications and Communication Enabling Technology Standards: An Overview," IEEE. Computer Science, International Conference on Intelligent Computing Applications, 2014.

[3]. K. K Patel, S. M Patel, "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges", May 2016.

[4]. G. D. Amane, ‘‘An Overview of Internet of Things’’, 13th international conference on recent innovations in science, engineering and management, February 2018.

[5]. A. Grizhnevich (2021), ‘‘IoT for Smart Cities: Use Cases and Implementation Strategies’’, [Online]. Available:

http://www.scnsofet.com/blog/iot-fpr-smart -city-use-cases-approaches-outcomes.

[6]. F. Righetti, C. Vallati, G. Anastasi*, "IoT Applications in Smart Cities: A Perspective Into Social and Ethical Issues",* IEEE International Conference on Smart Computing, 2018.

[7]. (2021), [Online] Available:

https://www.ida.gov.sg/~/media/Files/Infocomm%20 Landscape/Technology/Technology Roadmap/Internet OfThings.pdf

[8]. J. Anca, R. Pasika and X. Lina. "Introduction to IoT Security". ch2 in the book: IoT Security: Advances in Authentication, Publisher: John Wiley Sons Ltd. 2019.

[9]. M. Abomhara and G. M. Koien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," Journal of Cyber Security and Mobility, vol. 4, no. 1, pp. 65–88, 2015.

[10]. M. Gloukhvtsev," IOT Security: Challenges, Solutions & Future Prospects", DELLEMC, 2018.

[11]. R. Williams, E. McMahon, S. Samtani, M. Patton, and H. Chen, "Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach", 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), 2017.

[12]. X. Lu, Z. Qu, Q. Li, and P. Hui, Privacy Information security Classification for Internet of Things based on Internet Data". International Journal of Distributed Sensor Networks. 11(8), 2015.

[13]. J. Kannaiappan and B. Rajendran, "Privacy in the Internet of things". In Lee (ed.). The Internet of Things in the modern environment. IGI. Global. 2017.

[14]. F. Alaba, M. Othman, I. Hashem and F. Alotaibi, "Internet of Things security: A survey", Journal of Network and Computer Applications, 88, pp.10-28, 2017.

[15]. M. Stamp, Information security, 2nd ed. Hoboken, N.J.: Wiley, 2011, pp. 227-278.

Doi: https://doi.org/10.54216/PMTCS.020103
Received: January 09, 2023 Revised: April 08, 2023 Accepted: July 05, 2023

[16]. S. Ansari, S. Rajeev, and H. Chandrashekar, "Packet sniffing: a brief introduction," Potentials, IEEE, vol. 21, no. 5, pp. 17–19, 2002.

Doi: https://doi.org/10.54216/PMTCS.020103
Received: January 09, 2023 Revised: April 08, 2023 Accepted: July 05, 2023