Engineering Universe for scientific Research and Management
ISSN (Online): 2319-3069
Vol. XV Issue VI
June 2023

Green IoT Security, Issue, Challenges and Proposed Solutions: A Study

Dr. Narendra Sharma[1], Sangram Keshari Nayak[2]
Associate Professor, Dept. of CSE, SSSUTMS, Sehore[1]
Research Scholar, Dept. of CSE, SSSUTMS, Sehore[2]

Abstract

Internet of Things (IoT) is an innovative automation and analytics system which exploits networking, sensing, artificial technology and big data to provide comprehensive system for product or services. An IoT offers better transparency, performance, and control when smeared to whichever Industry or system. The IoT system aspires to link anyone with anything at anywhere. IoT typically has a three layers architecture consisting of Perception, Network, and Application layers Due to unique flexibility and suitability to work in any environment it is widely used for many applications. Security is the major issues in this because of their flexible behavior. It also does not fulfill the security requirement of the network as Cisco said this system will be used extensively in forthcoming years. Green IoT foreshadows an exciting future in which green networks intimately integrate our physical environment. Green networks in IoT with sustainable designs are guaranteed to reduce operating costs and energy consumption and reduce environmental pollution. IoT will have a significant influence on how we approach certain challenges in our everyday lives, and it will undoubtedly make our lives easier and better. This paper presents the survey on security issues challenges and their solution at each layer of the IoT..

Keywords: *Internet of Things, Security, Challenges, threats,Green IoT*

1. Introduction

The emerging technical space is growing with the Internet of Things (IoT). IoT is bringing about a paradigm shift in services, infrastructure, and consumer industries [1,5]. While this paradigm shift is happening, trust and security are necessary requirements to tackle different kinds of attacks, threats, malfunctions, and devastating impacts to society. The responsibility of securing IoT lies with device manufacturing companies and companies that use the devices. Having a complete set of security terms is a priority to organize the threat and overcome all security challenges in IoT. Some security requirements for IoT have been proposed, including encryption, hashing, and other forms of secure communications [2, 3]. Yet, more is needed to secure this infrastructure from threats and attacks as well as other concerning interests. Advancing the technology to secure the IoT environment is the motivation of this research work. With increased commercialization of IoT devices, society is becoming more and more connected with the IoT infrastructure - making society more susceptible to the vulnerabilities of the current IoT environment. IoT will increasingly touch our lives in more ways than before. Hence, research community must tackle and resolve security aspects of IoT. Compromised IoT devices present the risk of misusing personal information, compromising other connected systems, and safety risks [4]. Due to the lack of security features in IoT devices across the environment, a security dashboard is needed to find what type of security controls are required to stop threats and attacks in the IoT environment. This IoT security dashboard is a step in the right direction to organize and standardize devices across the IoT global network. Through the use of these steps, the IoT industry can seek to better improve upon the security that is needed in these devices. In the future, more devices can be inputted by the correct domain and type of device to understand what security is necessary to make the device secure for use in the IoT environment.

Green IoT is an energy-efficient process (hardware or software). This means connected devices in an energy-efficient process for the purpose of reducing power consumption, the greenhouse effects, and minimizing the emission of CO_2. By using green computational units, communication protocols, and network-based architectures with maximum utilization of bandwidth and relatively low energy utilization. The essential element of Green IoT is sustainable design and energy-efficient. Green IoT has three concepts, namely, enabling technologies, leverage technologies, and design technologies. Design technologies refer to interconnections, network architectures, communications protocols, and the energy efficiency of devices.

To get a green IoT product, it must go through a closed process including green design, green production, green utilization, and green disposal/recycling

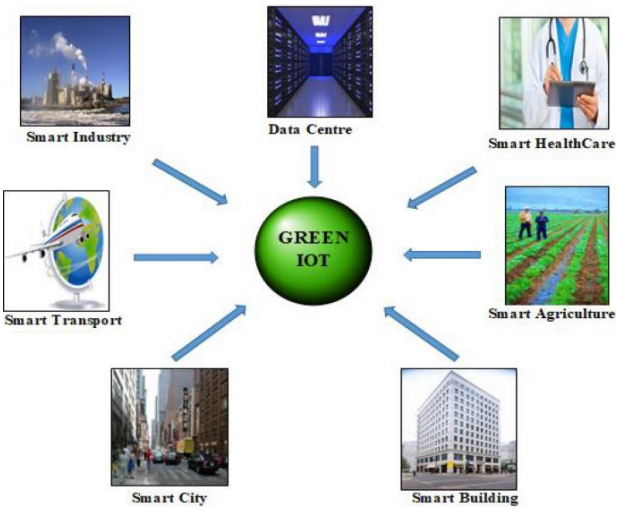

Fig.1 Architecture of Green Internet of things

2. Literature Review

Mahmoud A. M. Albreem, et al., (2017) Internet of Things (IoT) connects everything in the smart world, and thus, energy consumption of IoT technology is a challenge and attractive research area. Motivated by achieving a low power consumption IoT, a green IoT is proposed. This paper provides an overview regarding green IoT. It also discusses the life cycle of green IoT which contains green design, green production, green utilization, and green recycling. Furthermore, green IoT technologies such as green tags, green sensing networks and green internet technologies are discussed. In addition, studies of IoT in 5G and IoT for smart cities are presented. Finally, future research directions and open challenges about green IoT are presented.[6]

Rushan arshad, et al., (2017) Internet of Things (IoT) is an emerging concept, which aims to connect billions of devices with each other. The IoT devices sense, collect, and transmit important information from their surroundings. This exchange of very large amount of information amongst billions of devices creates a massive energy need. Green IoT envisions the concept of reducing the energy consumption of IoT devices and making the environment safe. Inspired by achieving a sustainable environment for IoT, we _rst give the overview of green IoT and the challenges that are faced due to excessive usage of energy hungry IoT devices. We then discuss and evaluate the strategies that can be used to minimize the energy consumption in IoT, such as designing energy efficient datacenters, energy efficient transmission of data from sensors, and design of energy efficient policies. Moreover, we critically analyze the green IoT strategies and propose have principles that can be adopted to achieve green IoT. Finally, we consider a case study of very important aspect of IoT, i.e., smart phones and we provide an easy and concise view for improving the current practices to make the IoT greener for the world in 2020 and beyond.[7]

Nitasha Khan, et al., (2020) Internet of Things (IoT) is an idea and theory of connecting billions of devices and enable them to exchange a massive amount of information. Green IoT visualize the theory of IoT with improved energy efficiency. We first give the overview of green IoT and the challenges that are faced due to excessive usage of energy hungry IoT devices. This paper presents research on energy efficiency in IoT. Authors presented some challenges, existing works, opportunities, and future directions. of green IoT [8]

Waleed Ejaz, et al., (2017) The drastic increase in urbanization over the past few years requires sustainable, efficient, and smart solutions for transportation, governance, environment, quality of life, and so on. The Internet of Things offers many sophisticated and ubiquitous applications for smart cities. The energy demand of IoT applications is increased, while IoT devices continue to grow in both numbers and requirements. Therefore, smart city solutions must have the ability to efficiently utilize energy and handle the associated challenges. Energy management is considered as a key paradigm for the realization of complex energy systems in smart cities. In this article, we present a brief overview of energy management and challenges in smart cities. We then provide a unifying framework for energy-efficient optimization and scheduling of IoT-based smart cities. We also discuss the energy harvesting in smart cities, which is a promising solution for extending the lifetime of low-power devices and its related challenges. We detail two case studies. The first one targets energy-efficient scheduling in smart homes, and the second covers wireless power transfer for IoT devices in smart cities. Simulation results for the case studies demonstrate the tremendous impact of energy- efficient scheduling optimization and wireless power transfer on the performance of IoT in smart cities. we first present an overview of energy management in smart cities, and then present a unifying framework for IoT in smart cities. Energy management has been classified into two levels: energy-efficient solutions and energy harvesting operations. We cover various directions to investigate energy-efficient solutions and energy harvesting for IoT devices in smart cities. Furthermore, two case studies have been presented to illustrate the significance of energy management. The first case study presents appliance scheduling optimization in smart home networks where the objective is to reduce the electricity cost. The second case study covers efficient scheduling of dedicated energy sources for IoT devices in smart cities. Simulation results are presented to show the advantage of energy management in IoT for smart cities.[9]

Saurabh Singh, et al., (2016) Green Internet of Things (IoT) is the study and practice of eco-friendly sustainable computing. The basic goal of green computing is to reduce the use of materials and maximize energy efficiency with

reliable and secure communications. The paper presents various technologies and issues regarding green IoT. It also studies the green Information and Communication Technology (ICT) such as green M2M, green Cloud Computing (CC), and green Data Center (DC). In addition, this paper mentions about the reliability in IoT Communication and and issues to achieve green IoT communication by applying efficient activity scheduling technique for energy saving. Finally, we propose the green IoT-Home Service (GIHS) model which provides efficient energy management in home automation system.[10]

Xilong Liu and Nirwan Ansari, (2019) With the ongoing worldwide development of IoT, an unprecedented number of IoT devices imperatively consume a substantial amount of energy. IoT devices have been predicted to be the leading energy guzzler in Information and Communications Technology by 2020. In considering the finite amount of brown energy sources along with their potential harmful impacts to the climate and environment, we propose to leverage "free" green energy to power IoT devices and revolutionarily enable wireless charging of these devices. Specifically, we propose to green IoT in three steps, namely, ambient green energy harvesting, green energy wireless charging and green energy balancing, in which the latter step reinforces the former step to ensure the availability of green energy. We lay out the basic design principles for these three steps, shed some light on the solutions and present the corresponding challenges individually.[11]

Vinita Tahiliani and Mayuri Digalwar, (2018) The Internet of Things (IoT) is an emerging paradigm that has gained popularity in recent years. The large number of high performance and sophisticated devices connected to the IoT system consumes huge amount of energy. Thus, the issue of energy consumption in IoT based systems is an important research focus. Green IoT represents the issue of reducing energy consumption of IoT devices which achieves a sustainable environment for IoT systems. This paper presents the current state of the art research on energy optimization in IoT. We investigated the literature, categorized the existing energy efficient techniques and presented the open challenges and research opportunities that can assist the research community. The main contribution of this paper is that it systematically summarizes and analyzes the existing energy aware techniques in tabular form on the basis of different layers and components of IoT.[12]

Faris., et al., (2021) The development of the Internet of Things (IoT) technology and their integration in smart cities have changed the way we work and live, and enriched our society. However, IoT technologies present several challenges such as increases in energy consumption, and produces toxic pollution as well as E-waste in smart cities. Smart city applications must be environmentally-friendly, hence require a move towards green IoT. Green IoT leads to an eco-friendly environment, which is more sustainable for smart cities. Therefore, it is essential to address the techniques and strategies for reducing pollution hazards, traffic waste, resource usage, energy consumption, providing public safety, life quality, and sustaining the environment and cost management. This survey focuses on providing a comprehensive review of the techniques and strategies for making cities smarter, sustainable, and eco-friendly. Furthermore, the survey focuses on IoT and its capabilities to merge into aspects of potential to address the needs of smart cities. Finally, we discuss challenges and opportunities for future research in smart city applications. This survey studied the strategies and techniques to improve our life quality by making the cities smarter, greener, sustainable, and safer. In specific, we highlighted the green IoT for efficient resource utilization, creating a sustainable, reducing energy consumption, reducing pollution, and reducing e-waste. This survey provided a practical insight for anyone who wishes to find out research in the field of eco-friendly and sustainable city- based on emerging IoT technologies. Based on the critical factors of enabling technologies, the smart things in smart cities become smarter to perform their tasks autonomously. These things communicate among themselves and humans with efficient bandwidth utilization, energy efficiency, mitigation of hazardous emissions, and reducing e-waste to make the city eco-friendly and sustainable. We also identified the challenges and prospective future research direction in developing eco-friendly and sustainable smart cities.[13]

3. Architecture of IOT

The IoT environment should be capable of interconnecting large number of heterogeneous objects through the Internet. So, there is a need for elastic and adjustable layered architecture. The general IoT architecture is divided into three layers such as Perception layer, Network Layer and Application layer. Figure.2 shows the three-layer IoT architecture.

- Perception Layer

This layer collects information through the sensing devices such as RFID, Zigbee and all kinds of sensors. Radio Frequency Identification (RFID) technology enables the design of microchips for wireless data communication and helps in automatic identification of anything they are attached to, acting as an electronic barcode [14]. The collected data are transmitted only through wireless network transmission (WSN). Some common attacks that occur in this layer are: Node capture, Fake node or malicious data, Denial of Service attack, Reply attack etc. [15].

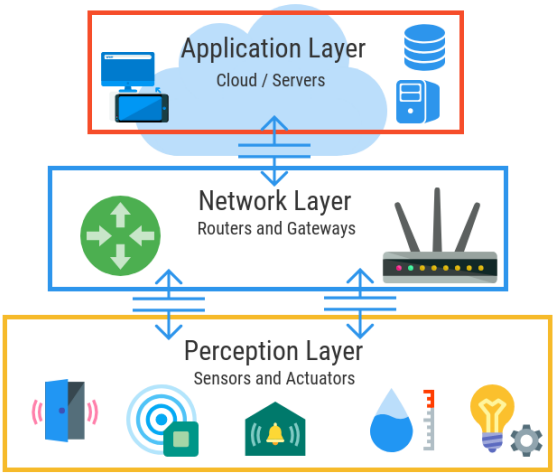

Fig.2 Three-layer IoT Architecture

- Network Layer

This layer supports secure data transfer over the sensor networks and responsible for routing. It transfers the information through wireless technology such as Wi-Fi, Bluetooth, and Infrared etc. [16]. Hence, this layer is mainly responsible for transferring the information from perception layer to upper layer. There are some common security problems in LAN, Wi-Fi, and Internet. They are: illegal access network, eavesdropping information, confidentiality and integrity damage, DoS attack, Man-in-the-middle attack etc.

- Application Layer

This layer is the topmost layer of the IoT architecture that provides the delivery of all services in various fields. It includes cloud computing, intelligent transportation, environmental monitoring etc. Application layer has some security problems such as data security, cloud platform security, data protection and recovery etc. To solve the security problems of this layer, authentication and privacy protection are needed. Particularly, password management is very important for data security [17].

4. Issues and Challenges in IOT

The Internet of Things faces many issues and challenges which is described below:

A. IoT Security Issues

- *Unsecured Devices:* The role of the consumers in the IoT industry has been upgraded and the consumer now plays an integral part in Security. Manufacturers upon launching a device should equip it with a strong default password. They should also advise consumers on how to make their lives with smart gadgets more secure. Most consumers are not well-informed about the significance of changing the default password on their devices. Thus, the responsibility falls on the manufacturers to maintain a more secure network and to educate the consumers of the necessary steps they need to take.[18]
- *Data Privacy:* Nowadays, power plants, manufacturing processes and healthcare devices are connected to IoT. These critical infrastructures constitute IoT a treasure trove of data. One mistake in security and precious confidential data might end up in the hands of criminals. One leak in Privacy and hackers can gain access to confidential, private data. Data transmission and reception as well as maintaining the privacy of the users must be a top priority of the IoT industry. With so many applications, gadgets and processes connected, even lives can be at stake. This is one of the reasons why Security-by-design is a great solution, particularly for Enterprise IoT.[18]
- *Insufficient Testing and Updating:* As the number of connected devices is in constant rise, one of the major IoT security issues is keeping the devices updated. Though IoT is a highly-digitised industry, it is amazing to see that the devices used, do not receive many updates. All the gadgets, applications and devices need to be sufficiently tested before launched. Then, they should be updated frequently, with patches and releases enhancing their security.[18]
- *IoT Malware and Ransomware:* Some digitised appliances and some gadgets too, have the same computing power as a tablet. This means that they can be compromised by hackers. Then, they can become a powerful weapon which hackers can use to compromise the system in many ways. This is one of the reasons why security cannot be achieved by obfuscation; on the contrary, it should be Open-Source where knowledge of operations is shared and put to good use.

B. Challenges

- *Identification and Localizing and Tracking*

The evolving features and technologies of the IoT along with the emerging systems of the IoT interaction have led to specific privacy and security challenges. One of the privacy and security challenges of the IoT is related to identification with regard to the risk of associating an identifier such as an address with the individual and related data [6]. In this case, the main challenge is related to associating the identity to a particular context that violates the individual's privacy by providing the identifying information to entities outside the user's personal sphere, increasing the possible cyber attack vectors. Another privacy and security challenge linked to

the IoT is localizing and tracking. In this case, the threat is related to the determination and recording of the individual's location across space and time. While localization and tracking are already possible through various means such as internet traffic and mobile phone GPs location, many users may perceive it as a violation of privacy if the data is used inappropriately or if they do not have any control of the sharing of their location data [6]. As such, the IoT faces a challenge in ensuring awareness of tracking and control of the localization data.

- *Profiling and Authentication*

The IoT also poses significant privacy and security challenges related to profiling as well as interaction and presentation that violate privacy. In relation to profiling, the IoT poses a risk in the compilation of data about users so as to determine their interests through correlation with other sources of data and profiles [7]. In this case, profiling methods may be used in e-commerce for consumer personalization as well as for internal targeting and optimization on the basis of the customers' interests and demographics. However, profiling could lead to privacy violations if the data is used for unsolicited ads, price discrimination, and social engineering. Moreover, the gathering and sale of user profiles in the data marketplace without the individual's consent is considered as a privacy violation. In turn, the IoT may also pose privacy and security challenges where private information on the individual user is conveyed inadvertently through the public media, thus disclosing the data to unwanted audiences. Various applications used in the IoT such as healthcare, transportation, and retail are reliant on significant user interactions. Majority of the mechanisms used to interact with the user and present feedback information are inherently public in nature, posing a threat to the individual's privacy in case other people can observe the data [8]. Thus, the IoT must solve the challenge posed by the easy visibility of personal user data.

- *Lifecycle Transitions and Inventory Attacks*

Finally, IoT poses privacy and security challenges with regard to lifecycle transitions and inventory attack. In this case, the users' private information collected during the IoT device's lifetime may be disclosed during changes to the gadget's control spheres during their lifecycle [9]. The smart devices interact with numerous services and persons and amass the data on such interactions in their history logs. Considering that the lifecycle of most consumer goods is based on the customer owning the products forever, the sale or sharing of such devices could result in the buyer accessing sensitive data about the previous owner, thus violating the individual's privacy. In turn, the privacy and security of the IoT are challenged by the threat of an inventory attack. As the IoT interconnection capacities evolve with the development of end-to-end vision, the smart devices can be queried over the internet by both legitimate and non-legitimate parties. When the IoT gadgets are queried by the non-legitimate entities, the latter may exploit the device to collect unauthorized information regarding the characteristics and existence of the user's personal effects [10]. Thus, the IoT can allow for the disclosure of comprehensive data about the users' life and belongings, posing a threat to their security and privacy.

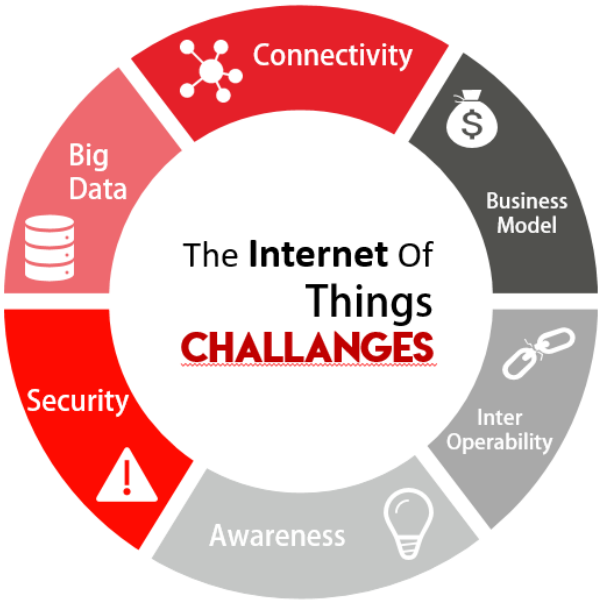

Fig. 3 Challenges in IoT.

5. Security Measures of IOT

Security measures used in IOT are:

• **Use a Trusted Platform Module (TPM) for authentication**. A TPM is a dedicated microprocessor that integrates cryptographic keys into devices to uniquely identify and authenticate them.[18]

• **Use the Trusted Network Connect (TNC) standards to check for malicious software or firmware**. The TNC standards offer a way to check devices for malicious software or firmware whenever they try to access networks or other devices.

• **Isolate and remediate infected devices with security software and protocols**. If a device is infected with malware or other malicious programs, it needs to be quarantined.

• **Layered security can limit the damage a hacker can do once device is hacked.** A Mandatory Access Control system limits access to certain functions or files on a device for a given user.

• **Data encryption is a must**. This should go without saying, but data needs to be encrypted when stored on a device or in transit.

• **Secure legacy systems through industrial control systems**. To reach their full potential, IoT devices and systems have to be integrated with legacy machines or

appliances that were never built to be connected or secured against hacking.

6. Conclusion

It is estimated that the IoT is now an emerging technology for the connection and accessing of devices from anywhere and anytime which is more cost effective but due to their flexible and work on any environment it is more prone to security issues. So it becomes more essential that this IoT technology offers more security and confidentiality of information for any applications. In this paper, we present the various security issues and challenges face by the internet of things (Iot) technology and discuss the layered architecture of it with security threats at each layer of IoT technology, also discusses some security measures for this technology. After study it is found that we need to use code signing ability with much more encryption technique to the devices for enhancing the security level of internet of things.

Reference

[1] Z. Yan, P. Zhang and A. Vasilakos, "A survey on trust management for Internet of Things," Journal of Network and Computer Applications, vol. 42, pp. 120-134, 2014.

[2] J. Granjal, E. Monteiro and J. Sa Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," IEEE Communications Surveys & Tutorials, vol. 17, pp. 1294-1312, 2015.

[3] M. Ambrosin et al., "On the Feasibility of Attribute-Based Encryption on Internet of Things Devices," in IEEE Micro, vol. 36, no. 6, pp. 25- 35, Nov.-Dec. 2016. doi: 10.1109/MM.2016.101.

[4] V. Kharchenko, M. Kolisnyk, I. Piskachova and N. Bardis, "Reliability and Security Issues for IoT-based Smart Business Center: Architecture and Markov Model," 2016 Third International Conference on Mathematics and Computers in Sciences and in Industry (MCSI), Chania, 2016, pp. 313-318.

[5] Harsh Pratap Singh, R. P. Singh, Rashmi Singh, and Bhaskar Singh, "Internet of Things (IoT) Based on User Command Analysis and Regulator Systems", International Conference on Recent Trends in IoT and Blockchain, India, 19-20 October 2019, In proceeding of Apple Academic Press.

[6] Mahmoud A. M. Albreem, Ayman A., Muzamir Isa, Wael Salah, M. Jusoh, M.M Azizan, and A Ali (2017) "Green Internet of Things (IoT): An Overview", Proc. of the 4th IEEE International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA), https://www.researchgate.net/publication/322021467, pp-1-7.

[7] Rushan Arshad, Saman Zahoor, Munam Ali Shah, Abdul Wahid, and Hongnian Yu, (2017) "Green IoT: An Investigation on Energy Saving Practices for 2020 and Beyond", IEEE, http://www.ieee.org/publications/standards/publications/rights/index.html for more information., pp- 15667-15681.

[8] Nitasha Khan, Aznida Abu, Muhammad Alam, and M.S Mazliham, (2020) "Analysis of Green IoT", https://www.researchgate.net/publication/344217922, pp-1-15.

[9] Waleed Ejaz, Muhammad Naeem, Adnan Shahid, Alagan Anpalagan, and Minho Jo, (2017) "Efficient Energy Management for the Internet of Things in Smart Cities", Enabling Mobile and Wireless Technologies for Smart Cities: Part 1, 10.1109/MCOM.2017.1600218CM, pp-84-91.

[10] Saurabh Singh, Seo Yeon Moon, Gangman Yi and Jong Hyuk Park "Energy Consumption and Reliable Communications for Green IoT", pp- 309-312.

[11] Xilong Liu and Nirwan Ansari, (2019) "Toward Green IoT: Energy Solutions and Key Challenges", IEEE Communications Magazine, 10.1109/MCOM.2019.1800175, pp-104-110.

[12] Vinita Tahiliani and Mayuri Digalwar, (2018) "Green IoT Systems: An Energy Efficient Perspective", Proceedings of 2018 Eleventh International Conference on Contemporary Computing (IC3), pp-1-6.

[13] Faris. Almalki, S. H. Alsamhi, Radhya Sahal, Jahan Hassan, Ammar Hawbani, N. S. Rajput, Abdu Saif, Jeff Morgan and John Breslin, (2021) "Green IoT for Eco-Friendly and Sustainable Smart Cities: Future Directions and Opportunities" https://doi.org/10.1007/s11036-021-01790-w, pp-1-25.

[14] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic and Marimuthu Palaniswami, "Internet of Things (IoT)" A Vision, architectural elements, and future directions", Elsevier, Future Generation Computer Systems, 2013, pp. 1645-1660.

[15] Kai Zhao and Lina Ge, "A Survey on the Internet of Things Security", IEEE, International Conference on Computational Intelligence and Security, 2013, pp. 663-667.

[16] Gurpreet Singh Mathuru, Priyanka Upadhyay and Lalita Chaudhary, "The Internet of Things: Challenges & Security Issues", IEEE International Conference on Emerging Technologies (ICET), 2014, pp. 54-59.

[17] Hui Suoa, Jiafu Wana and Caifeng Zoua, Jianqi Liua, "Security in the Internet of Things: A Review", International Conference on Computer Science and Electronics Engineering, 2012, pp. 649-651.

[18] https://www.quora.com/What-are-security-measures-used-in-IoT