IOT ARCHITECTURE, SECURITY CONCERNS AND CHALLENGES: A COMPREHENSIVE REVIEW

Abstract

Internet of Things (IoT) is a novel paradigm that has emerged in the past recent years and has found path into our lives by automating our routine tasks through smart devices and applications but this comfort has brought with it certain security challenges and attacks. The communication of our personal data between smart devices and applications has provided a ground for cyber intruders to carry out malicious actions. Though IoT has made our lives comfortable, our personal and sensitive information are consistently exposed to attacks by cybercriminals. This paper depicts the elements, architecture and security concerns of IoT system. Moreover this paper also highlights the biggest attack on IoT so far which is Mirai botnet and explains how it is still upsetting the IoT security.

Keywords*:* Internet of Things, IoT, security, network protocols, DDoS, layered architecture

Authors

Sangita Vishwakarma
Assistant Professor
Computer Applications Department
DPGITM
Gurgaon, India
sangita.rit18@gmail.com

Dr. Payal Jindal
Assistant Professor
Computer Applications Department
DPGITM
Gurgaon, India
bhavayapayal@gmail.com

Megha Gupta
Assistant Professor
Computer Applications Department
DPGITM
Gurgaon, India
megha08in88@gmail.com

I. INTRODUCTION

Internet of things (IoT) has gained a lot of attraction by researchers in the past few years. With remarkable growth in internet technology, we have become dependent on several devices for our day-to-day tasks. Our lives are operating in two dimensions – fictional or virtual space and real world. IoT has successfully blurred the boundary between these two dimensions. When several physical devices embedded with sensors and microchips are interconnected to each other through a single platform, it is termed as Internet of Things. IoT platform collects data from these interconnected devices and analyses them in order to assist in decision making or research process. It can be decided thereafter which data is useful and which is not [1]. The term "Internet of Things" was first used by Kevin Ashton, MIT's Executive Director of Auto-ID Labs, who used this term as the title of his presentation for Procter & Gamble and this term got a place in Oxford English Dictionary in 2013. Since then, its definition has evolved continuously.

Wearable fitness and trackers (Fitbits) and IoT healthcare applications, voice assistants (Siri and Alexa), smart cars (Tesla), and smart appliances are some of the examples of IoT in our daily life. The concept of IoT states that any physical device which is connected to the internet has an identity in the global infrastructure of IoT network [2]. With the accessibility of internet at low cost, a large number of devices have become available to be connected to an IoT platform. In just over a decade, we have seen considerable progress in regard to handling devices that is moving from using fingers to communicate with devices, to being able to speak to them to now where the devices can communicate with each other with very little human intervention.

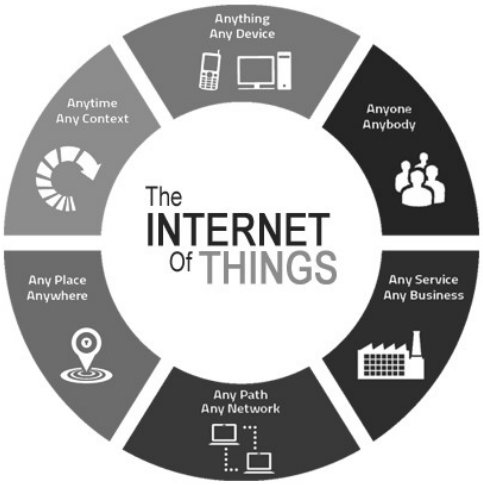

Figure 1: IoT

Internet and the entities connected to it have always been open to security attacks and since IoT's infrastructure and operation is dependent on the physical devices, the security in IoT relies heavily on these devices but sadly these devices are not capable to handle these attacks and hence poses certain threats to data integrity, authentication, data privacy, etc. [3]. These devices are continuously vulnerable to privacy attacks and with the emergence of new IoT devices and new businesses adopting this technique has resulted into the requirement of an effective mechanism to handle these attacks.

II. IOT ARCHITECTURE

There has not been any defined standard for architecture of IoT devices because of their consistently changing nature and wide range of sensors. But still some components act similarly in all IoT projects. The IoT architecture is built keeping scalability in mind as more and more data will be captured in a long course of time and the architecture should be able to handle those massive data. As per the perspective of IoT, the architecture consists of definition of physical components, network protocols and configuration and data formats [4]. Since IoT deals with real time data, its architecture is expected to adjust according to recurrent changes. These changes may be some upgradation in the businesses or some advancement in the architecture.

1. **Four Stages of Iot Architecture:** IoT is much more than some devices connected through internet. It consists of sensors that collects data, which are pre-processed and then sent to data centres for final analysis. There is actually a flow of data from the IoT devices to data servers that happens over a four-stage process – Data collection from sensors and actuators, Data Acquisition, Pre-processing of data and Cloud and Data centre analytics *[5]*.

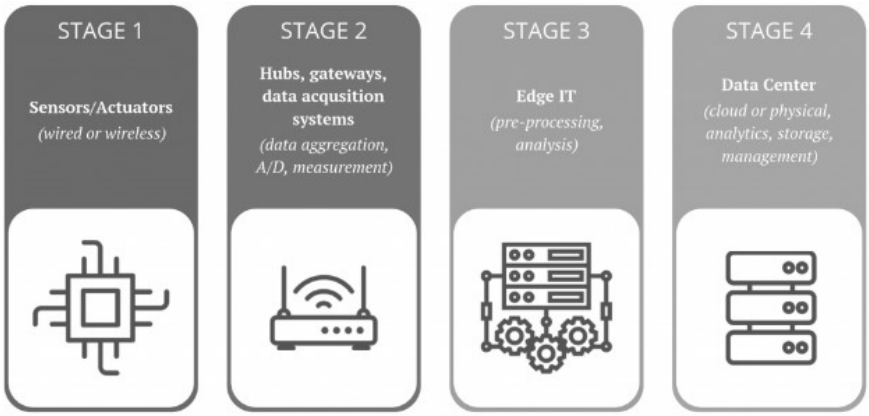

Figure 2: Four Stages of IoT System

- **Sensors and Actuators:** The very first step involves creation of physical environment where sensors and actuators are established. The main task of sensors is data capturing and collection from the devices. Apart from data collection, sensors are also responsible for transforming data into meaningful set of information that will facilitate further analysis. Based on the data sensed by sensors, actuators determine what actions to be taken in order to perform an immediate remedial action in some cases which do not require extensive processing and where a round trip from the data servers can cause delay.

- **Internet Gateway & Data Acquisition:** The raw data collected from the sensors is analog in nature and is received in massive volume as hundreds and thousands of sensors capture data simultaneously. These data need to be aggregated before further transmission so that the data stream can be filtered and compressed to optimal size. Moreover, the timing and structure compatibilities are also adjusted at this stage in order to make the further data representation uniform.

- **Edge Information Technology:** Not all data received from the sensors are of utmost importance and since they are collected in analog form, they are already in bulk amount. These data get digitized in the second stage. This stage is responsible for pre-analysis and selection of the required data received so that the bandwidth of LAN and the storage space at data centre do not get burdened by its direct transmission to data centres. Machine Learning may be used at this stage to serve feedback in a continuous manner without being dependent on the commands sent back from the data centre. Edge IT infrastructures are always located somewhere near to the location like as in an on-site wiring closet.

- **In-depth Analysis at the Cloud or Data Centre:** The last stage deals with in-depth analysis of the pre-processed data received from Edge IT. This analysis can happen at a physical server or at a cloud-based server which uses certain applications to securely analyse and store the data. The executions carried out at this stage do not get affected by the nature of the platform, i.e., cloud-based or physical. The analysis obtained at this stage are used to gain significant understandings of the IoT system that may trigger some actionable consequences to explore and recognize various patterns or to identify the loopholes if any in order to improvise the IoT operations and carry out possible or feasible optimisations.

2. **IoT Layered Architecture:** IoT systems are not limited to specific devices, domains or geographical locations, which gives a necessity of dependency on platforms & services. This dependency requires an intelligent framework which can handle wide range of IoT devices acting as a centralized controller of four stages of an IoT system [6]. Therefore, IoT architecture is designed as a sequence of different layers to manage the overall system across protocolsand gateways.

Architecture of IoT has always been a hot topic of debate among many researchers but not a single proposal has got clear consensus as there is a lot of dynamicity in IoT system which has to work together to make the IoT operate as it is intended to. Even with non-existence of a single standard for IoT architecture, the three-layer architecture is the basic and dominant form. The three layers comprises of Perception layer, Network layer and Application layer.

- **Perception Layer:** This is the layer that actually generates the data for the IoT systems by gathering them from number of sensors installed on connected devices. Actuators also constitute a part of this layer.

- **Network Layer:** This layer is responsible for the movement and transmission of data across IoT platform by connecting IoT devices to networking components and back-end servers.

- **Application Layer:** This layer provides user interface for IoT systems in order to serve application specific services to the user.

Though the three-layer architecture covers the major concepts of IoT but still it lacks in explaining the finer and the in-depth attributes of IoT which are majorly of research concern [11]. So, two additional layers were proposed – Business and Processing.

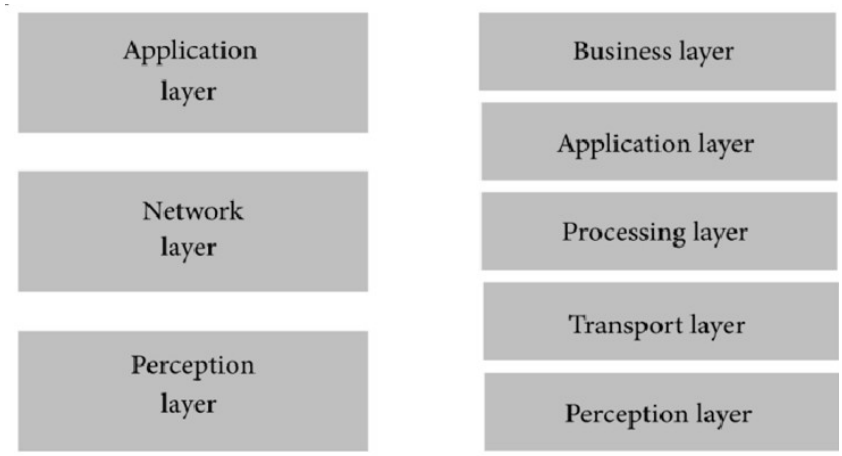

Figure 3: Layered Architecture of IoT

Perception And Application Layer Has The Same Working In Five-Layer Architecture Also. The Roles of Other Layers Are Outlined As Follows:

- **Transport Layer:** The sensor data gets transmitted from the perception layer to processing layer and vice versa by the transport layer through networks such as SDN/NFV, 5G, wireless, local area networks, RFID, Bluetooth, and NFC.

- **Processing Layer:** It serves as middleware that receives data from the transport layer and provides facility for storage, analysis and pre-processing of those data. It also involves extraction of useful information and discarding meaningless data by making use of big data analytics. Data accumulation and data abstraction are the two main tasks of this layer. Data accumulation deals with providing efficient storage solution to the data collected from transport layer. Data abstraction prepares the data for end applications to derive meaningful insights. Both the steps cover hardware details, thus increasing the efficiency of interoperability of devices.

- **Business Layer:** The data generated at all previous layers are of zero importance if they do not add any value or contribution to enhance the productivity of business or provide optimized solution to the encountered problems. The decision making process is executed by certain models which are managed by this layer along with the management of overall IoT system as well as the user's privacy. Each user's privacy has to be managed separately without conflicting with each other, also each user will have its own role in decision making due to which business layer has a separate definition from other layers.

III. IOT SECURITY ISSUES

Diversity in range of devices in IoT is its key feature which provides consumers with so many options to choose from but in turn it makes the security a bigger issue to handle in IoT. The portability of IoT devices also poses a major threat as well as absence of a single defined standard provokes compatibility concerns which also muddles the security challenge in IoT [10]. With the quick pace of technological advancements, demand for IoT app development is increasing around the world. There has been a surge in usage of IoT devices in the past decades. Presently, around 23 billion IoT devices are in use worldwide which, as per statistics, can grow up to over 41 billion by 2027. Manufacturing companies are into cut throat competition on delivering latest products to the consumers. But only handful of them are concerned regarding the security of IoT connected devices as well as privacy of the users. In the current scenario, almost every domain is utilizing the benefits of IoT whether it is corporate or healthcare firms or entertainment industry or enterprises or industrial bodies [17]. Since IoT has to involve the networking infrastructure which acts as an entry point for attacks by hackers or intruders and stretches the field of attack surface.

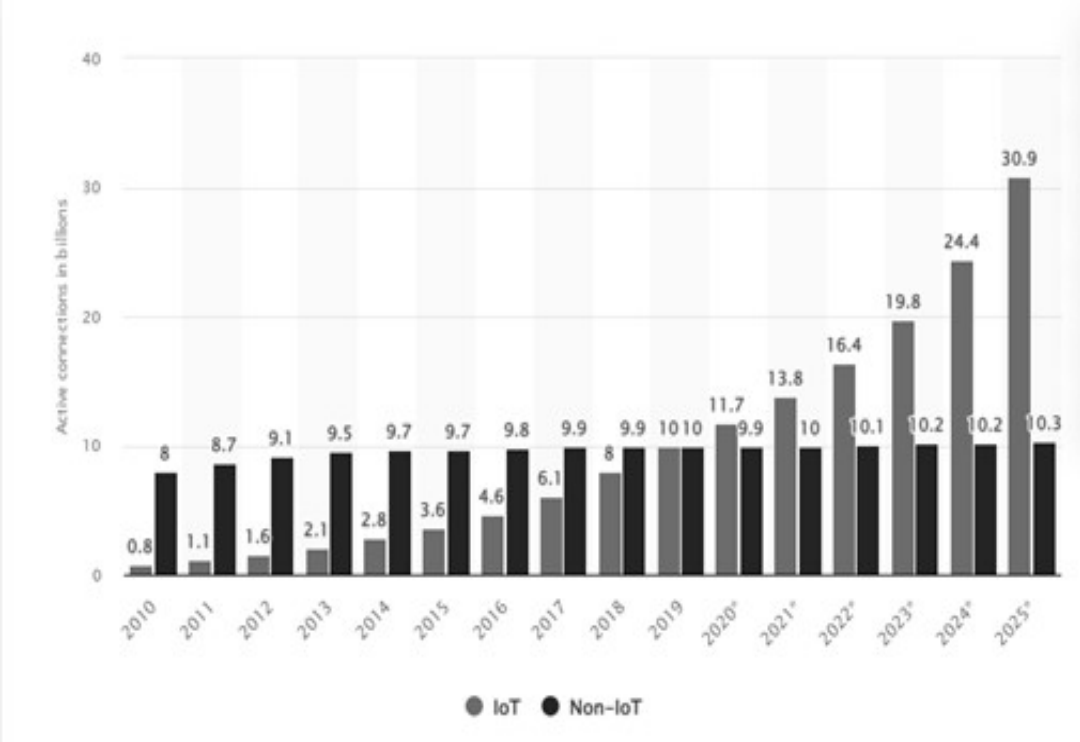

Figure 4: Iot Connections Over Past Decade And Prediction in Coming Years

Some common concerns are always felt and expected when we deal with transmission of data in a network and they are:

- **Integrity of Data :** The data transmitted between two nodes should always be accurate.
- **Confidentiality Data :** None other than the designated entities should be able to access the data.
- **Authenticity of Data:** Data should reach the destined entity in its original form, no unauthorized modifications should be done to the data while being transmitted.

- **Availability of data :** Data should always be available to the users when required.

Mentioning the IoT's layered architecture, each layer is vulnerable to security attacks. For example, if correct and appropriate encryption mechanisms are not implemented for the transmitted data then it makes the overall communication doubtful. Perception, Network and Application layers form the basic layers in IoT system. The following table explains the different types of attack that each layer of IoT architecture can be encountered with.

Table 1: Security Attacks On Different Layers

Layer	Attacks	Technology	Explanation
Perception Layer	Node Duplication	WSN	The key node gets attacked and all the sensitive data, key for protected transmission and data storage get leaked. The key IoT node is cloned to initiate further attacks.
	Eavesdropping	WSN	A real-time attack where confidential communications or messages get unauthorized access by the intruder.
	Jamming attack	RFID	The intruder keeps transmission medium busy by sending interfering signals or packets which results into reduction of signal-to-noise ratio at receiver's end. As a consequence of this the network performance degrades.
	Relay attack	WSN	The IoT nodes get replaced by relay nodes that captures the communication between two entities and forwards it to other relay node or to the destined entity without harming it.
	Timing attack	WSN	The intruder continuously monitors the network and as soon as it realizes that the device is in a weak state and observes its low response time, it attacks.
	Replay attack	RFID	Also known by the term playback attack. The hacker keeps monitoring the communication between two parties and intercepts the data sent by the sender and simply forwards it to the receiver who considers it to be coming from the

			legitimate sender but it is actually not.
Network Layer	Man-in-the-middle attack	RFID	In this attack, the communication between two parties is accessed and modified in an unauthorized manner and in such a way that both the sender and receiver think that they are in constant communication with each other. It triggers serious security hazard to the whole communication.
	Routing attack	WSN	This attack increases the response time by redirecting the route which results into formation of noisy nodes causing huge traffic in the network.
	DoS (Denial of Service) attack	RFID	The device and the networking resources are drowned with repeated requests and messages so much that they first of all become less responsive to valid requests and then ultimately stop responding. This attack prevents authentic users to use the resources and devices.
	Sybil attack	WSN	This attack exhausts networking resources in which a node functions as multiple fake nodes to weaken the influence by growing its own authority.
	Sinkhole attack	WSN	In this attack, a node is hijacked and is completely controlled by the intruder and draws all the traffic towards itself which may lead to selective forwarding of data packets, modification of packets or completely discarding for the transmission process.
Application Layer	Phishing attack	RFID	In this attack the users are trapped into believing that the information is coming from a trusted source which in fact is a fraudulent replica of the authentic source to gain access to user's sensitive data like login credentials, credit card information, etc.
	Malicious code attack	RFID	The application contains some intentionally written infected code that

			causes detrimental damage to the system. Even the antivirus software are not able to control or stop them from threatening the security.
	Session hijacking attack	RFID	User's online web session is targeted with the intention of hijacking the confidential data.
Processing layer	Resource Exhaustion attack	RFID	Main targets of this attack are the networking resources mainly memory storage and power consumption. It is the consequence of attacks such as DoS. It does not make much harm to the security but disrupts the normal functioning of IoT system.

IV. IOT SECURITY CHALLENGES

1.51 billion breaches were reported between January and June 2021. Taking the security concern too lightly while designing IoT system is intolerable. Moreover in the absence of a standard security infrastructure in IoT, companies continue to create devices without considering security as a crucial element. Certain challenges exist in thecurrent IoT approach which are ruining the IoT system.

- **Insufficient Testing And Updating**: Companies manufacturing IoT devices don't give enough attention to its security matters. Most of the devices do not receive security updates regularly or receive for very short duration of time.

- **Gap In Iot Skills:** IoT needs skilled professionals but there has been a broad gap because of lack of proper training or up-gradation programs.

- **Iot Malware And Ransomware:** With increase in number of IoT devices, a surge has been recorded in the number of malwares and ransomwares and in unpredictability of the type of their attacks.

- **AI And Automation:** IoT is consistently entering in our routine life, companies are dealing with millions of IoT devices as well as with massive data generated from them which are already being filtered with the help of AI tools. AI tools help in developing autonomous systems that apply data-specific instructions and discover unusual or suspicious data transmission patterns. But using autonomous systems may impose some risks as a single error in the algorithm can destroy the whole infrastructure.

- **Home Invasions And Remote Vehicle Access:** We are witnessing the emergence of the concept of home automation. This has obviously changed our life but also has put our homes at a huge security risk as it can leak our IP address which can be used to get

to our residential address. Apart from this, car hijacking is also a potential security threat with the arrival of smart car feature. Getting access to cars through remote access can leave us exposed to lethal crimes.

- **Untrustworthy Communication:** Certain IoT devices are involved in insecure and unencrypted communication which each other. This is right now the biggest challenge companies are facing today.

- **Botnet Attack:** IoT is a network of connected devices which makes the task of automating a hijack easier for cybercriminals. Botnet is a network of malware affected IoT devices that is designed to create, automate and speed up attack in a short span of time. Botnet attracted a lot of attention after Mirai botnet attack in 2016.

Apart from all above challenges, covid-19 pandemic has given rise to work from home culture around the world which has increased the dependence on home automation. This arrangement has made the companies realize to reassess the security routines in IoT. In addition to this, with the transition to 4g and 5g connectivity, people have been continuously switching to smart mode of living. Security threats in IoT have much more dangerous consequences than can be thought of. Iot devices are consistently being in use in homes and in medical fields also. If a hacker gets access to a baby monitor or thermostat or to the devices that keeps monitoring the patients remotely, it may even risk someone's life.

V. MIRAI BOTNET ATTACK

Mirai is a malware that has been a constant threat to IoT security since its surge. In 2016, a series of DDoS attacks was launched from thousands of infected IoT devices that got converted into botnetsby Mirai malware. The creators of Mirai botnet, Paras Jha and Josiah White, wrote the source code for Mirai to shake down his university's system, afterwards targeted the servers of a popular video game Minecraft.

These attacks targeted small audience but in September 2016, this duo attacked the French Company OVH that hosted tool against DDoS attacks against a popular video gaming company, Minecraft. This attack assaulted about 1,45,000 devices at around 1Tbps peak speed. After this attack, Brian Krebbs's website was targeted by flooding over 600 GB of data as this cybercrime investigative journalist was considered a threat to the creators of Mirai. In order to make their identity anonymous, this pair leaked the source code of Mirai botnet online to get plausible deniability. The other intruders and cybercriminals copied the code, modified the code and used it for own malicious intentions. Attack on Dyn, a company which offered domain registration services to various popular websites such as Amazon, PayPal, Verizon, The New York Times and Netflix, was a consequence of these waves of attacks. Though the originators got caught and found guilty the damage was done by then as the code was already out there and it continues to be in existence and is still causing damages. Since its release into the online community, several variants of Mirai have been created like Okiru, Satori, Masuta and PureMasuta that have compromised the IoT security in different forms.

For example, the PureMasata variant can explode HNAP error in D-Link devices and there is an OMG variant that grant anonymity to the intruders by creating IoT proxies. IoTrooper and Reaper are some of the newly discovered variants that are much faster and powerful than Mirai botnet. Security of IoT devices is not given sufficient importance by the manufacturers and also by the users. As per a Cisco report, by the end of 2022 about 72% of mobile devices will be smart devices and 99% of the data traffic will initiate from these devices. In addition to this, 5g connectivity will boost this traffic by almost 2.6 times than an average 4g connection.

VI. CONCLUSION

In this paper we have reviewed various security concerns and challenges that have come with IoT and IoT enabled smart devices and applications. Some of these attacks are so dangerous that they can risk someone's life. This paper also described the basic architecture and elements of IoT along with certain security breaches that each layer of the architecture is exposed to. The main objective of this paper is to highlight the current challenges or challenges that still exist in IoT system irrespective of certain efforts that has been put into securing IoT infrastructure. Much work is to be done in this area as IoT has become an integral part of our day-to-day life. Heterogeneity of IoT devices and lack of end-to-end encryption and access control are some of the reasons behind insecure communication in IoT system. It is high time that manufacturers give priority to consider security as a major aspect in designing IoT devices.

REFERENCES

[1] Wei Zhou, Yan Jia, AnniPeng, Yuqing Zhang, and Peng Liu, "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved", IEEE.
[2] Rachit, Shobha Bhatt, Prakash Rao Ragiri, "Security trends in Internet of Things: a survey", SN Applied Sciences, 12 January 2021.
[3] MirzaAbdurRazzaq, Muhammad Ali Qureshi, Sajid Habib Gill, SaleemUllah, "Security Issues in the Internet of Things (IoT): A Comprehensive Study", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017, pp 383- 388.
[4] Jari Porras, Jayden Khakurel, AnttiKnutas and JouniPankalainen, "Security Challenges and Solutions in the Internet of Things", Journal of NBICT, Vol. 1, 177–206, pp 177-205.
[5] Muhammad Burhan, Rana Asif Rehman, Bilal Khan, "IoT Elements, Layered Architectures and Security Issues:A Comprehensive Survey", Sensors, ResearchGate, August 2018.
[6] Daniel Minoli, KazemSohraby, and Benedict Occhiogrosso, "IoT Considerations, Requirements, and Architectures for Smart Buildings – Energy Optimization and Next Generation Building Management Systems", IEEE Internet of Things Journal.
[7] Husamuddin Mohammed, Mohammed Qayyum, "Internet of Things: A Study on Security and Privacy Threats", ResearchGate, March 2017.
[8] Rao Faizan Ali, AmgadMuneer, DhanapalDurai Dominic PanneerSelvam, ShakirahMohdTaib, "Internet of Things (IoT) Security Challenges and Solutions: A Systematic Literature Review", ResearchGate, December 2021.
[9] KaziMasumSadique, Rahim Rahmani, Paul Johannesson, "Towards Security on Internet of Things: Applications and Challenges in Technology", ScienceDirect, The 9th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2018), Procedia Computer Science 141 (2018) 199–206.
[10] Parushi Malhotra, Yashwant Singh, PoojaAnand, Deep Kumar Bangotra, Pradeep Kumar Singh, and Wei-Chiang Hong, "Internet of Things: Evolution, Concerns and Security Challenges", Sensors 2021, 21, 1809.

[11] Jalal Safari Bazargani, AbolghasemSadeghi-Niaraki and Soo-Mi Choi, "A Survey of GIS and IoT Integration: Applications and Architecture", Applied Sciences, 2021, 11, 10365.
[12] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, Shiuhpyng Shieh, "IoT Security: Ongoing Challenges and Research Opportunities", 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, pp 230-234.
[13] Shinsuke Tanaka, Kenzaburo Fujishima,Nodoka Mimura, Dr. Eng. Tetsuya OhashiMayuko Tanaka, "IoT Security IoT System Security Issues and Solution Approaches", Hitachi Review Vol. 65 (2016), No. 8, pp 359-363.
[14] Jee Young Lee and Jungwoo Lee, "Current Research Trends in IoT Security: A Systematic Mapping Study", HindawiMobile Information Systems Volume 2021, Article ID 8847099, 25 pages.
[15] Chakib BEKARA, "Security Issues and Challenges for the IoT-based Smart Grid",International Workshopon Communicating Objects and Machine to Machine for Mission Critical Applications (COMMCA-2104), Procedia Computer Science 34 (2014) 532 – 537.
[16] MaedeZolanvari, "IoT Security: A Survey", http://www.cse.wustl.edu/~jain/cse57015/ftp/iot_sec/index.html.
[17] MardianabintiMohamad Noor, Wan Haslina Hassan, "Current research on Internet of Things (IoT) security: A survey", Computer Networks 148 (2019) 283–294.
[18] R.Vignesh and A.Samydurai, "Security on Internet of Things (IOT) with Challenges and Countermeasures", IJEDR, Volume 5, Issue 1, ISSN: 2321-9939.
[19] LoaiTawalbeh, FadiMuheidat, Mais Ali Tawalbeh, MuhannadQuwaider, "IoT Privacy and Security: Challenges and Solutions", June 2020, Applied Sciences 10(12):4102.
[20] N Alhalafi1 and Prakash Veeraraghavan1, "Privacy and Security Challenges and Solutions in IOT: A review", IOP Conference Series: Earth and Environmental Science, Volume 322, 2019 International Conference on Smart Power & Internet Energy Systems 25–27 April 2019, Deakin University, Melbourne, Australia.
[21] Eman Shaikh; ImanMohiuddin; AyishaManzoor, "Internet of Things (IoT): Security and Privacy Threats", 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), 01-03 May 2019.
[22] FarhadMehdipour, "A Review of IoT Security Challenges and Solutions", 2020 8th International Japan-Africa Conference on Electronics, Communications, and Computations (JAC-ECC), 14-15 December 2020.
[23] Khalid Hameed Zaboon, NafeaAlhammadi, "A Review of IoT Applications, Attacks and Its Recent Defense Methods", ResearchGate, March 2020.

