JCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol. 9, Issue.4, April 2021 E-ISSN: 2347-2693

A Literature Survey on Security & Privacy Issues in IoT

Kamaljit Kaur[1], Ramanjot Kaur[2]

[1]M.Tech (Scholar), [2]Assistant Professor

[1,2,] Department of Computer Science Engineering/IT, DIET, Kharar, Punjab India

**Corresponding Author: kamaljeet.kaur798@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v9i4.6064 | Available online at: www.ijcseonline.org

Received: 16/Apr/2021, Accepted: 20/Apr/2021, Published: 30/Apr/2021

***Abstract*—** In the 21st century IoT plays a major role in all domains The Internet of Things (IoT) is the network of billions of devices, people and services to Interconnect and exchange information and useful data. The IoT applications are highly affirming to increase the level of comfort, efficiency and automations for the user. Due to rapid increase of devices, people, vehicles connecting with the IoT network from anywhere and anytime which causes security and privacy issues.The high level of security and privacy, authentication and recovery from the attacks is required to implement an IoT automated world. All the IoT security threats including DoS, Man-in-the-middle, Tempering, jamming etc. are discussed in the survey

***Keywords*—**Internet of Things, characteristics of IoT, IoT security, IoT future development. Security; Authentication; Attacks;

I. INTRODUCTION

Nowadays IoT is a fast growing new industry and almost all experts believe that in the coming years IoT will be used in many different aspects. However, this phenomenon, like many other IT-related phenomena, faces different challenges[1].

The IoT is a world where billions of objects can communicate and share information, all of these objects are connected over the Internet protocol (IP). These connected objects generate huge amounts of data regularly which is collected, analysed and used to perform actions, providing intelligence for decision making[2].

The number of connected devices with the IoT environment is increasing every day. The reason for this rapid increase is; connected devices provide comfort and produce good results compared to humans.The number of connected devices is increasing with enormous speed[3]. The concept of the Internet that we have in mind is a global network in which personal computers, cell phones, etc. are connected, and humans are communicating with each other using these connected devices everywhere. Now consider a world in which the Internet goes beyond its current concept and includes the objects/things around us. The Internet of Things is an emerging technology in which each “Thing” can send and receive data through various communication networks. Specifically, a “Thing” in IoT has the ability to collect data, control, or communicate remotely. A smart lock connected to your mobile phone, CCTV cameras which can be controlled remotely or a sprinkle in your garden that can be programmed are all examples of IoT devices[4].

It can be said that the Internet of Things is a network of networks in which a large number of things, sensors and devices are connected through the communication and information infrastructure to provide value-added services through intelligent data processing and management for various applications.

Along with the tremendous benefits of the Internet of Things, this technology faces some challenges. One of the main challenges of the IoT is the security of these devices. Unauthorized access, data hijacking, data manipulation, network penetration, eavesdropping, etc. are among the IoT security challenges. Therefore, new standards and protocols are always required to solve sustainability, reliability, service quality, confidentiality and integrity. Smart home and smart cities are also in need of these updates. In order to achieve this goal, it is very important to examine the protocols and standards of IoT. Actually, by using these surveys, we can provide better protocols and standards to address the challenges and limitations that currently exist[6][7].

It is very important that IoT devices have adequate security. At the moment, given the fact that manufacturers are rushing to introduce new smart devices to the market, so the security of these devices is usually not the first priority for them. Consumers and businesses are often unaware of how their devices’ security affects their lives or business. This will increase the risk of data breach or hacking these devices[5].

The survey paper is structured as follows: Section two highlights the related work in the field of IoT security & Privacy. Section three describes the problem statement and Section four the summary of the survey in the form of conclusion.

II. RELATED WORK

A. Internet of Things (IoT)

It is essential to comprehend the concept and definition of IoT (Internet of Things) as specified by many scholars to obtain a whole picture of IoT devices. Having an easy and understandable definition for IoT that can state all of its features can help researchers and scholars to do more research and can help us to understand the IoT concept much better.

IoT can be characterized as a set of things in an interworking network that can be made smart if they can be identified, named and addressed. IoT is also defined as a "dynamic global network infrastructure with self-configuration and interoperable communication" [8]. It is also stated that the IoT means every device around us are supposed to be connected to the Internet in a way that it can behave intelligently and can pay attention to the existence of the kind of autonomy and privacy [7]. IoT, Internet of things, is an interrelated network of devices such as mechanical and digital machines, objects, animals or people which can transfer data over a network without any need to human-to-human or human-to-computer interaction (IoT, 2019). A general and simple definition is that IoT is the network of devices, vehicles, and home appliances that contain electronics, software, actuators, and connectivity which allows these things to connect, interact and exchange data (Internet of things, 2018).

B. Security Challenges

Basic Security: One of disputes about IoT devices is that "it is believed that IoT devices are being manufactured rapidly without giving much attention to security challenges and the requisite threats"[9]. Although security is one of the most important aspects of using IoT smart devices, it has not been paid much attention to.

Privacy: Privacy is another challenge in using IoT devices. By using IoT devices billions of devices across the globe are connected to each other and interact with each other and the privacy issue should be managed somehow. General privacy and security threats like internal and external attacks should also be covered in IoT studies [10]. And also "a lack of intrinsic security measures makes IoT vulnerable to privacy and security threats" [11]. Schurgot et al., (2015) states that "well-known security and privacy problems have been shown across devices and networks, from pacemakers that can be made to deliver a fatal charge to networked light bulbs that can provide back doors into WiFi networks, to smart TVs that listen to conversations, to refrigerators that are enlisted into denial of service attacks." According to Gartner (Connected Things, 2014) the number of connected IoT devices in use by 2020 will be nearly 25 billion, and by using such a big number of interconnected IoT devices there would be new types of security and privacy threats and hackers would use security gaps to use these devices for their personal benefits [11] categorizes privacy in IoT devices in three different aspects:

data collection privacy, data sharing and management privacy and data security issues;

He believes that more research should be done on each of these aspects to find their vulnerabilities in order to have a more secure network for IoT devices.

Data Management: Managing the huge amount of data produced by IoT devices is also another security challenge for spreading IoT. Recent studies show that many of the current methods of information management are ineffective in cloud computing because these methods are not able to manage and control the massive amounts of information generated by IoT smart devices [12]. In IoT devices, data management should be as a layer between the devices that generate data and the applications that have access to this data. The data that is provided by IoT devices should be available to the network of IoT devices, depending on the level of privacy desired by the owners; Thus, communication, storage and process are the key factors in the design of data management solutions for IoT devices [13]. Besides, data which is collected from all IoT devices in a smart city must be securely protected to decrease the risk of data theft that can cause other significant problems such as identity fraud or financial damage[14]

C. Communication Protocols

Current communication protocols can also be a challenge for IoT devices. Experts believe that there are many barriers to establishing secure connections between IoT device elements and sensors and a Wi-Fi network. Moreover, there are vulnerabilities in current WiFi technology that can increase the security risk of using WiFi technology in sensitive IoT devices such as those that are used in military places. These vulnerabilities can allow attackers to intercept network traffic and steal data transmitted over a WiFi network. Since billions of devices will connect to each other by IoT devices in near future the current WiFi technology weaknesses must be resolved. In addition, some new characteristics of IoT devices cannot be implemented securely by current security protocols that are used on the Internet because most of these protocols are designed to work with desktop and laptop computers not IoT devices. Z-Wave and ZigBee are the different "languages" that IoT smart devices can use to talk with each other. Each of these protocols has weaknesses and strengths that will be referred to in this research, but the main focus is on weaknesses and strengths in terms of security issues of these protocols.

D. IoT security vs traditional IT security

There are several differences between IoT and conventional wireless networks in terms of dealing with security and privacy. Frustaci, Pace, Aloi and Fortino (2018) explains That the devices in the IoT system has limited hardware and software resources (i.e., sensor or RFID), whereas traditional IT is mostly based on resource rich devices. So, IoT devices only use lightweight algorithms to find a right balance between higher security and lower capabilities. Hassija et al. (2019) explains that without a trusted IoT ecosystem, IoT applications may lose all their potential along with the security issues faced generally by the Internet, cellular networks, and WSNs, alongside these issues IoT has its own security challenges such as privacy issues, authentication issues, management issues, information storage and so on.

*E. **IoT vulnerabilities***

IoT is the network of a large number of devices and they are also at the high security risks. Bertino and Islam (2017) explains that IoT systems are higher security risks for several reasons

i) these systems don’t have well defined perimeters

ii) these systems are highly heterogeneous with respect to communication medium and protocols

iii) smartphone applications require permissions for installations and other user interactions but in IoT devices these permissions might not be possible due to the large number of devices etc. Li Tryfonas and Li (2016) explains the data security and privacy issues are very important, but the risks associated with the IoT will reach new levels due to this communication and autonomous decision making begin to embed complexity, security loopholes, and potential vulnerability. Similarly, Moscholios (2019) explains that the interconnections and the similarity of devices and technologies in the IoT generate possible cyber-physical security vulnerabilities that can be exploited by various cyber attackers

Insecure web interface Inability to change default password and username, exposed credential, weak passwords, lack of robust password recovery etc. Insufficient authentication/authorization Privilege escalation (design flaw or configuration error in an application or operating system) Insecure network services DoS, buffer overflow, fuzzing attacks etc. Lack data encryption and verification Transmission of unencrypted data and credential Privacy concerns Collection of unnecessary user data; exposed personal data and insufficient controls on who has access to user data Insecure cloud interface Account enumeration, no account lockout, credentials exposed in network traffic Insecure mobile interface Insufficient authentication, lack of transport encryption and account enumeration Insecure security configuration Weak password policies, no security logging and lack of data encryption option Insecure software/firmware Lack of secure update mechanism, update files not verified before upload Poor physical security Device easy of disassemble, access to software via USB ports, removable storage media

In order to achieve trust among the systems, an important part is to secure them. The approach to securing these systems relies on threat and risk analyses. The solutions of these risks consist of many different kinds of security architectures. The process of securing IoT environments is a difficult task since there will be many different scenarios and each scenario consists of different kinds of devices. Each security solution looks different from the other since these systems may contain entities which are constrained in different ways.

F. IoT Security Issues

Node capture attacks: IoT applications are the combination of several low power nodes. These nodes are vulnerable to a variety of attack. The attacker can capture the node and get all the information and data.

Malicious code Injection attack: In this type of attack the attacker can inject some malicious code in the memory of the node. By injecting this type of code, the attacker may force the node to perform some unintended functions.

False Data injection attack: Once the attacker captures the node, he can inject erroneous data onto the IoT system. This leads the false results and they can use this method to cause a DoS attack (Hassija et al., 2019).

Tampering: The attacker can get the physical access of the sensors. By using this method, the attacker can access sensitive information like encryption/decryption keys (Cerullo et al., 2018).

Eavesdropping and interference: IoT applications consist of various nodes deployed in the open environment, this exposed the IoT applications to eavesdropper.

Jamming: This attack disturbs the radio channel, the attacker sends useless information to corrupt or lose the message[23]. This kind of attack can be divided into four categories: constant jamming, deceptive jamming, random jamming and reactive jamming (Radoglou et al., 2019)

Flooding attack in cloud: This attack has a big impact on the cloud system by increasing the load on the cloud services. This attack works the same as the DoS in the cloud and affects the quality of service (QoS). The attacker continuously sends multiple requests to a service.

SQL Injection Attack: In such attacks, attackers can embed malicious SQL statements in a program. The attacker can obtain private data of any user and can even alter records in the database.

De-Synchronization: An attacker forwards some fake sequence number for de-synchronizing the endpoints and producing the data retransmission [22].

Man-in-the-Middle attack: This is the form of eavesdropping attack in which the target of attack is the communication channel. The unauthorized party can monitor the communication between two parties without identification.

Data thefts: IoT applications deal with a lot of data which is critical and private. The data in transit is more vulnerable than the data at rest. The users are always reluctant to transmit their private data on the IoT system [21].

Malicious codes such as viruses, spy-ware, worms etc. are the possible attacks in this layer. The malicious codes can alter the data collected by the sensors, the receiver will receive the wrong data and perform wrong actions.

Sniffing attacks: The attackers may use sniffer applications to monitor the network traffic in IoT applications. This may allow the attackers to gain access to confidential user data.

Denial-of-Service attack: These type of attacks stop the authenticated users to use the IoT application by artificially making the servers or networks too busy to respond.

Malicious code injection attacks: Attackers can inject the malicious code in a script because this is the simplest way to break the security. Due to these attacks the attackers can hijack an IoT account and paralyze the IoT system.

G. System Ports

The network ports supported by the Transport layer, it is a number which serves endpoint communication between two connected machines. Each port number has a distinct value that support one serves, Usually those values are predefined to be used by a known service[8]. SSL stands for Secure Sockets Layer is to establish secure connection and stand as a safeguard for the connection between client-server or server-server it encrypts the transferred data between the machines to make sure the data being shared is fully safe. TLS stands for Transport Layer Security; it is an enhanced version of SSL and does the same thing[8]. HTTPS HyperText Transfer protocol operates in the application-layer and it’s a secure version of HTTP, allowing users to transmit sensitive data over the internet using authentication and encryption that comes with an SSL issues certificate [8].

The rapid increase of IoT devices and communication led to increase in security and privacy issues. Security issues include malicious code attacks, inability to receive security patches, hacking into smart meters, eavesdropping, sniffing attacks and DoS attacks etc. [19]. The current devices of IoT have limited power and computational resources. Therefore, a lightweight encryption algorithm and key management protocols are needed for IoT devices. Cryptographic techniques can 52 be used to protect, store and process data and keeping information as local as possible using decentralized computing and key management [20]. The privacy issues are also very critical for the IoT environment. The private information of any user can be leaked because anyone can connect with his device. The privacy issues can be addressed in two ways. Firstly, the user’s device ignores the query that need the private data. Secondly, construct the network architecture in which the use device returns only the requested data without including protected data attacks.

III. CONCLUSION AND FUTURE SCOPE

In this survey we have studied about IoT securities issues and its Privacy issues to mitigate with these issues. The high level of security and privacy required. The IoT faces various security and privacy issues due to rapid increase of devices, people, vehicles connecting with the IoT network from anywhere and anytime which causes security and privacy issues. All the IoT security threats including DoS, Man-in-the-middle, Tempering, jamming etc. are discussed in the survey. This literature review is expected to be a valuable resource to understand the security issues at each layer of IoT. Finally, a lot of research is available in different areas of IoT but security and privacy is still considered the weakest part of it. Different researchers have proposed many different kinds of adaptations to lightweight protocols and authentication methods for IoT which makes it very difficult to identify the best solution. Therefore, IoT requires structured guidelines in the form of standardisation in order to interconnect all kinds of devices, protocols, applications, etc.

REFERENCES

[1] Ray, Partha Pratim. "A survey of IoT cloud platforms." *Future Computing and Informatics Journal* 1.1-2 (2016): 35-46.

[2] Tank, Birju, Hardik Upadhyay, and Hirenc Patel. "A survey on IoT privacy issues and mitigation techniques." *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*. 2016.

[3] Samie, Farzad, Lars Bauer, and Jörg Henkel. "IoT technologies for embedded computing: A survey." *2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ ISSS)*. IEEE, 2016.

[4] Lee, Suk Kyu, Mungyu Bae, and Hwangnam Kim. "Future of IoT networks: A survey." *Applied Sciences* 7.10 (2017): 1072.

[5] Hassan, Wan Haslina. "Current research on Internet of Things (IoT) security: A survey." *Computer networks* 148 (2019): 283-294.

[6] Ishaq, Isam, et al. "IETF standardization in the field of the internet of things (IoT): a survey." *Journal of Sensor and Actuator Networks* 2.2 (2013): 235-287.

[7] Gilchrist, Alasdair. *IoT security issues*. Walter de Gruyter GmbH & Co KG, 2017.

[8] Shah, Sajjad Hussain, and Ilyas Yaqoob. "A survey: Internet of Things (IOT) technologies, applications and challenges." *2016 IEEE Smart Energy Grid Engineering (SEGE)*. IEEE, 2016.

[9] Deogirikar, Jyoti, and Amarsinh Vidhate. "Security attacks in IoT: A survey." *2017 International Conference on I-*

SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC). IEEE, 2017.

[10] Schurgot, Mary R., David A. Shinberg, and Lloyd G. Greenwald. "Experiments with security and privacy in IoT networks." *2015 IEEE 16th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. IEEE, 2015.

[11] Safdar, Noreen, Hala Asif, and Fatima Farooq. "Energy Use and Human Health Nexus in Pakistan." *Review of Economics and Development Studies* 6.3 (2020): 661-674.

[12] Gravely, Shannon, et al. "Discussions between health professionals and smokers about nicotine vaping products: Results from the 2016 ITC Four Country Smoking and Vaping Survey." *Addiction* 114 (2019): 71-85.

[13] Abu-Elkheir, Mervat, Mohammad Hayajneh, and Najah Abu Ali. "Data management for the internet of things: Design primitives and solution." *Sensors* 13.11 (2013): 15582-15612.

[14] Bohli, Jens-Matthias, et al. "SMARTIE project: Secure IoT data management for smart cities." *2015 International Conference on Recent Advances in Internet of Things (RIoT)*. IEEE, 2015.

[15] Zhang, PeiYun, MengChu Zhou, and Giancarlo Fortino. "Security and trust issues in fog computing: A survey." *Future Generation Computer Systems* 88 (2018): 16-27.

[16] Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." *IEEE Access* 7 (2019): 82721-82743.

[17] Bertino, Elisa, and Nayeem Islam. "Botnets and internet of things security." *Computer* 50.2 (2017): 76-79.

[18] Grammatikis, Panagiotis I. Radoglou, Panagiotis G. Sarigiannidis, and Ioannis D. Moscholios. "Securing the Internet of Things: Challenges, threats and solutions." *Internet of Things* 5 (2019): 41-70.

[19] Ramotsoela, Daniel, Adnan Abu-Mahfouz, and Gerhard Hancke. "A survey of anomaly detection in industrial wireless sensor networks with critical water system infrastructure as a case study." *Sensors* 18.8 (2018): 2491.

[20] Abomhara, Mohamed, and Geir M. Køien. "Security and privacy in the Internet of Things: Current status and open issues." *2014 international conference on privacy and security in mobile systems (PRISMS)*. IEEE, 2014.

[21] Hassija, Vikas, et al. "A survey on IoT security: application areas, security threats, and solution architectures." *IEEE Access* 7 (2019): 82721-82743.

[22] Cerullo, Gianfranco, et al. "Iot and sensor networks security." *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks*. Academic Press, 2018. 77-101.

[23] Tang, Xiao, Pinyi Ren, and Zhu Han. "Jamming mitigation via hierarchical security game for iot communications." *IEEE Access* 6 (2018): 5766-5779.

AUTHORS PROFILE

Er. Kamaljit Kaur is presently working as an Analyst in a Multinational Company, India. She received the degree of Bachelor of Technology(B.Tech.) in Computer Science and Engineering from the PTU. She is presently pursuing her M.Tech in Computer Science & Technology at DIET ,Kharar, Punjab India. Her research interests include NLP, Network Security, SDN, Big Data and Computer Applications.