IJCSN - International Journal of Computer Science and Network, Volume 9, Issue 3, June 2020
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

A Detailed Study of Security and Privacy of Internet of Things (IoT)

[1] Mohan Krishna Kagita; [2] Madda. Varalakshmi

[1] School of Computing and Mathematics,
Charles Sturt University,
Melbourne, Australia.

[2] Department of Computer Science and Engineering,
Vasireddy Venkatadri Institute of Technology,
Guntur, Andhra Pradesh, India.

Abstract - The (IoT) "Internet of Things" is a comprehensive notion that entirely depend on the network configuration that connects a huge number of programs whose prime objective is to assemble data and to impart among one another in an attempt to improve their decision-making efficiency. The growth of technology simplifies individual's life in different ways. At the same time, it also dispenses some threats and attacks as well. The assurance of security and privacy necessity plays an important role. Such mandates consist of data concealment and verification, access authority within the "IoT" network, privacy and trust between users and things, and the implementation of security and privacy policies. General security and remedies can't be straightway applied to "IoT" technologies because of the distinct standards and communication scads connected.

Keywords - Internet of Things, Security issues of IoT, Sensors, security guidelines, countermeasures, security attacks

1. Introduction

Internet of Thing is the new era of technology that we are living in. Objects and people are interconnected with the internet on "Internet of Things". A vast number of innovative applications have got amazing prospects; that is why the Internet of Things have got extensive consideration. Our lives have got advance quality with this new paradigm. It has made a huge effect on agriculture, tracking of locations, Supply Chain system, analyzing finances, energy efficiency, remote monitor and its maintenance, business process and its management and so on. Physical devices that are all around the world and are now connected to the internet and are connected and sharing the data and information are known as "Internet of Things". It has now become possible to turn something as small as a pill and as big as aero-plane into the part of "Internet of Things" with the arrival of cheap computer chips and universal wireless Network. All the dumb things are now able to communicate real-time data without the help of human beings only because when all these devices are connected, and sensors are added to them it gives them the level of digital intelligence to these dumb devices and makes them work. The "Internet of Things" is merging digital and physical things and making them smarter and more responsive. Any object that can be connected to the internet to be controlled to communicate information can be transformed into an "IoT" device.

The word "Internet of Things" is majorly used for those devices that would not be normally predicted to have an internet connection and can communicate without the need for human action. Hence a computer or a smartphone is not called an "IoT" device, despite the fact that the fact smartphones are jammed with sensors. "IoT" device can be a smartwatch, a fitness band or any other wearable device. Swiftness and efficiency are the top considerations for the benefit of business if "IoT" is applied. Ability to make changes and have better access to data and information about products and internal system of an enterprise is the idea of "Internet of Things". The lifestyle of human beings has been changed totally with the speedy growth of advanced technology and have moved to the system, which is known as "always connected". Wide variety of objects are connected in such a way that they can communicate with each other and called as "Internet of Things" which is a rapidly emerging paradigm. The research and innovation team of "Internet of Things" describes it as a high powered global network structure with self-configuring efficacy based on accustomed and interoperable communication guidelines where physical and virtual things have identities. Making a smart city with smart healthcare and smart transportation can be the goal of the Internet of Things".

Application of "IoT" is possible in several areas, but many security and privacy issues are seen with the rapid growth of "IoT."

High risk for several reasons is seen in the "Internet of Things" system. Continuous changes due to high mobility, highly dynamic and due to fewer parameters do are very risky. The system of "Internet of Things" is highly diversified with reference to communication mode and its codes, stages and devices. A portion of the "IoT" system can be controlled by different parties and can be physically unprotected. Against attacks, there are officially recognized security methods in reference to the prevailing information system and mobile locality. Several exciting opportunities and new applications have been introduced by "IoT" technology. Without much effect on performance, usability and adaptability, proper security measures should be adopted to ensure security and privacy. Although the computer and network security system has presented several essential skills and methods reevaluating and expanding these practices and methods so as to address the relevance of IoT system involve several technical and engineering provocations. Where consumers are worried about the security and privacy of their data and information at the same time sales of "Internet of Things" devices are rising high. People want to have control over the personal information and data which these devices collect and as per the survey, they are very much concerned about the privacy.

"Internet of Things" devices which are secured and private are demanded by the customers, but very less information is available about the same. IoT device creators are being called by the regulators and have been asked to implement security safeguards and also supply information about the security and privacy of devices. Standardized Labels highlighting security and privacy rules should be mentioned on the "Internet of Things" devices. Security and privacy are of great importance when modern-day smart city applications are considered. Industries like governance, education, transportation and healthcare will use wireless communication, and mobile computing applications will be used as "Internet of Things" devices to generate and store sensitive data and information. However, challenges related to diversity, adaptability, flexibility, potency and most important privacy and security has been well acknowledged. Securing data from intruders is the key requirement from any "Internet of Things" application as the number of modern technological application are increasing across various domains. For the increased demand for more security and privacy, several attempts have been made to furnish the same. Such proposals include machine learning-based methods to contradict zero-day attacks, intelligent attack exposure and escape system, the application of bio-inspired methods and the implementation of context-aware privacy maintenance plans. New features adopted technologies and innovations keep "Internet of Things" as fresh and new, yet this is not a new paradigm. Because of so many facilities and advantages, thousands of new devices join this family of massive technology every day. The two main players of "Internet of Things" are wireless sensor network and "RFID". "RFID" being cheap and potential play a major role in "IoT". An owner can track the information and data of an individual; hence this is the main issue with "RFID" with reference to privacy. Without any special configuration, it is very easy to locate an individual inside of clothing. To be used by military and to forecast weather and it ranges from tiny home sensors and has a size of millimetres to a big one's Wireless sensor network (WSN) is the next major player in this race. Sensors assemble a lot of information and data in several situations; they may be home, office and can be used even for measuring Blood pressures.

2. Literature Review

Vijayalakshmi and Arockiam (2016) found that in the usage of Internet "Internet of things" has made a lot of changes and have also given a lot of opportunities for the research. There are still security and privacy issues with "Internet of Things" although a lot of research has already been carried out in this reference. It is obvious that there is no limit to the protection in case of "Internet of Things". With a huge effect on social and business life "Internet of Things" is going to become a very necessary and important element. In most of the application domains "Internet of things" applications and services have found to be unsecured. A secured technology is required urgently for these applications to get "Internet of Things" secured from all security and privacy issues. The major issues with "Internet of Things" are the privacy, secrecy, certification and purity of data.

Ghani and Konstantas (2019) studied that to provide unlimited services and solutions in systems such as cars, homes, offices, hospitals etc. a lot of "Internet of Things" devices are being used, and they are tightly involved with human beings. However, there is a big risk of security and privacy by using devices of "Internet of Things". Researchers first identified the requirement for "Internet of Things" and then its stakeholders. Security and privacy guidelines list are also being made by the researchers. Investors who are going to get boosted by these guidelines

and build "Internet of Things" objects that are secured have also be stated. To implement the proposed guidelines, there is a set of proper countermeasures that can be used at each level. To address security and privacy issues, there are two developing technologies that are coming up; they are known as block-chain and SDN. All possible attacks and threats have been investigated by the researcher, and the security goals like secrecy, privacy and data quality that are violated have also be stated.

Maras (2015) revealed that information about lifeless and living things is being shared with the help of the "Internet of Things" devices. "Internet of Things" is involved in everything it can be household appliances or medical devices. New and changed demonstrations of weakness exist with the use of "IoT" devices and its extensiveness in society. Security and safeguarding of "Internet of Things" devices are diverse and complicated procedure. Urgent actions in legal analysis and new approaches in legislation are required for the existing risk of an inadequate legal framework. A complete analysis of existing legal framework needs to be undertaken to deal effectively with existing weaknesses of "Internet of Things" at the same time new principles need to be developed to look after the risks associated with the usage "Internet of Things".

Joshitta and Arockiam (2016) studied the security and privacy issues and challenges with reference to "Internet of Things" devices. Round the clock people will be involved in the world of internet-only if there is proper control mechanism is developed. A car order to fill its oil tank or a refrigerator asking for milk without a middleman will be the scenario. Hence, it will be secured and smart environment for everyone. If we think "Internet of Things" as a reality, then security is the key to resolve all the issues such as standards, mobility support, traffic classifications, authentication of QoS, data quality etc. Connectivity will be there for anyone, anytime and at anyplace. Wide variety of usage of "IoT" is brought by the pattern of "Internet of Things". Concerns about privacy and security and even the whole "IoT" system is brought by the same pattern of "Internet of Things". Elements like secrecy, confidentiality, authentication and authorization need to be ensured for the whole "IoT" system in order to guarantee the security of "Internet of Things".

Agarwal et al. (2015) found that still there are many "IoT" devices that do not use encoded communications or proper authentication due to which there are so many media reports every day regarding cyber-attacks hacking incidents. It is important to use mutual authentication and encryption for smart home devices or any other "Internet of Thing" device for that matter. Usually, embedded software is installed in "Internet of Thing" devices, but as this software are device-specific, it is difficult to update, so this is one of the problems with embedded software. To make these software bugs free, it is an important responsibility of these software makers to take extra care in developing and testing these software and updates should be issued on a regular basis. Lack of strong encryption cannot be an excuse as due to less memory and slow CPU's they may not be able to use same encryption methods as conventional computers. "Elliptic Curve Cryptography" (ECC) are efficient cryptographic techniques developed for small scale devices. Currently, it is difficult to install multiple smart devices in a secure manner due to all these security and privacy issues on a different level. The more hardware and software will get more costly as more and more security measures get implemented in the same. As compared to hardware protection, software-based security measures are cheap.

Razzaq et al. (2017) studied the security attacks and its countermeasures and highlighted the major security and privacy issues with reference to "Internet of Things" devices. Many of the "IoT" devices become the soft target, and even the victims do not have any knowledge about it because of inefficient security mechanism. Researchers studied the security requirements like confidentiality, integrity and authentication. There are different categories of attacks like low-level attacks, medium-level attacks, high-level attacks and extremely high-level attacks. It is very necessary to install security mechanism in "IoT" and communication network devices considering the importance of security in "Internet of Things". It is recommended to read security requirements and not to use default passwords when using a device for the first time in order to protect them from security threats and intruders. Chances of security threats can be decreased by disabling the features that are not of use.

Al–Sharekh and Al-Shqeerat (2019) studied the architecture of "IoT" based on five layers. Crucial aspects with regards to security requirements that should be examined in "Internet of Things" have also been mentioned. The limitation with reference to the security and privacy of "IoT" as well as security challenges have been discovered. With reference to security challenges and restrictions of "IoT" a questionnaire was prepared and was distributed to the faculty of various universities in Saudi Arabia. Research opportunities in future have also been discovered. Developing security measures of "Internet of Things" by the researchers is a significant contribution. To overcome security threats practical solutions needs to be

provided and issues like Vulnerabilities and threats should be followed for future research. Jindal et al. (2018) revealed different attributes of what future "Internet of things" will look like. The situations can be made better if we try to eliminate the chain of myths that always hold our future with uncertainty. Making use of the data wisely that is possessed by the sensors, reliance of "Internet of Things" on the mobile network, the influence of data that is collected by different devices, the value of network along with data centres, the requirement of a secured service framework with the option of remote control, development of interactivity standards, diverseness and vulnerability are few of the issues that need to look after, security and privacy of information and data are going to play a key role in showing the picture of "IoT" in the near future. There is also a threat to the success of "Internet of Things" due to the challenges faced by this technology. The success rate of "Internet of Things" is opposed by factors like technology, business, society and law. At the time of development of these technologies, people are not very fond of using gadgets and smart devices should also be considered as well as their acceptance because they might have difficulties in using devices as they are quite complex.

Iqbal et al. (2016) studied the overview of "Internet of Things", and its issues related to security and privacy challenges and have also found out the security measures and solutions that can be taken to secure communication data and information. Traditional security measures cannot be applied because of the diversified nature of the sensors, low reserves and the system structure in "Internet of Things". The strong security framework is needed to protect the unauthorized use of data of users, to protect their privacy and to control security and privacy threats. Spying on sensitive data or vicious inflaming of harmful tasks can be stopped by successive data protection and authentication. Users should be restricted to utilize "Internet of Things" based applications for any unauthorized data and information. The present system is determined on pre-deployed and pre-shared keys while certified authentication is usually thought to be impossible.

Sedrati and Mezrioui (2018) found that there are a lot of challenges, but still "Internet of Things" is an amazing and exciting thing. "Internet of Things" has been defined formally and its specifications have been discovered. "Internet of Thing" is different from the traditional internet. To identify the areas of challenges that "Internet of Thing" is going to face, it is important to understand those key differences. To analyze the security of "Internet of Things" a reference model was suggested after the presentation of those challenges. Security issues that were hanging out have been able to exhibit with the help architecture of that model. The future plans of the researchers are to find out the lightweight security solutions. Study on future lightweight cryptography algorithms is necessary because objects in "Internet of Things" do not support complicated computing system and cryptography is important for the securitization of data and information.

3. Conclusion

Both benefits and risks are associated with the variable and investigating the structure of technology and consequently "Internet of Things" and so many individual users are on risk. With the help of "Internet of Things" sharing and collecting data and information has become very easy and transferable, but at the same time, there are a lot of security and privacy issues. Hence protection and security measure should also be taken into account for a better and safe future. The security issues that have been regularly seen with the "IoT" devices is because of the weak passwords. Configuration of these devices is mostly done remotely as "IoT" devices very often do not have keyboards. It is recommended to put security and privacy fact labels because there is an increased number of security attacks and many poorly manufactured devices do not offer protection to their users. Manufacturers and researchers are busy in designing the system to control the flow of data and information without the leak of privacy by getting motivated by the increased number of security attacks and are trying to provide full security and privacy to user's information.

With the speedy growth of "Internet of Things" cyber-crimes and attacks are also growing rapidly. Hence it is very important for the manufacturers and researchers to develop strong security countermeasures and safeguard the end-users. Security considerations with reference to Information Technology is not a new context. The new and exclusive security issues and challenges are presented by the implementation of many new features of "internet of Things" devices. As "IoT" technology and devices are have become common and blended in our daily lives, it is necessary for the users to trust the "IoT" devices and that their data is safe from getting exposed and leaked. It is important to develop strong security measures as soon as possible to safeguard user information and data.

The lack of certainty and business risks always exist in new technology. With reference to "internet of Things," many dangers are not physically present and sometimes slightly misrepresented. Assets of hardware and software

are may be available in less quantity or are under development. At the time of developing the "Internet of Things" devices, its security and privacy are the major concerns and addressing these concerns is very important. There is always a scope of abuse for new technologies, so before the issues of security and privacy get influenced, it is smarter to work on it beforehand. Hence, it is important to develop security countermeasures and safeguards the data from getting attacked by the hackers and to have a better future for "Internet of Things" devices.

Reference

[1] Vijayalakshmi, A. and Arockiam, L. (2016) A study on security Issues and Challenges in IoT, International Journal of Engineering Sciences & Management Research, Vol. 3(11), Pp. 34-43

[2] Ghani, H. and Konstantas, D (2019) a Comprehensive Study of Security and Privacy Guidelines, Threats, and Countermeasures: An IoT Perspective, Journal of Sensor and Actuator Networks, doi: 10.3390, Pp. 1-38

[3] Maras, M. (2015) Internet of Things: Security and privacy Implications, International Data Privacy Law, Vol. 5, No. 2, Pp. 99-104

[4] Joshitta, R. and Arockiam, L. (2016) Security in IoT Environment: A Survey, Int. Journal of Information Technology & Mechanical Engineering, Vol.2 Issue. 7, Pp. 1-8

[5] Agarwal, S., Majumdar, S., Maiti, A., Nath, A. (2015) Security and privacy issues of Internet of Things: challenges and threats, International Journal of Advanced Technology in Engineering and Science, Vol. 3, Issue – 4, Pp. 89-98.

[6] Razzaq, M., Qureshi, M., Gill, S., Ullah, S (2017) Security Issues in the Internet of Things (IoT): A Comprehensive Study, International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, Pp. 383-388

[7] Al-Sharekh and Al-Shqeerat (2019) Security Challenges and Limitation in IoT Environment, International Journal of Computer Science and Network Security, VOL.19 No.2, Pp. 193-199

[8] Jindal, F. and Jamar, R and Churi, P (2018) Future and Challenges of Internet of Things, International Journal of Computer Science & Information Technology (IJCSIT) Vol 10, No 2, Pp. 13-25

[9] Krishna Kagita, M. (2019). Security and Privacy Issues for Business Intelligence in a loT. In Proceedings of 12th International Conference on Global Security, Safety and Sustainability, ICGS3 2019 [8688023]

[10] Iqbal, M., Olaleye, O and Bayoumi, M. (2016) A Review on Internet of Things (IoT): Security and Privacy Requirements and the Solution Approaches, Global Journal of Computer Science and Technology: E Network, Web and Security, Vol-16, Issue – 7

[11] Sedrati, A. and Mezrioui, A. (2018) A Survey of Security Challenges in Internet of Things, Advances in Science, Technology and Engineering Systems Journal Vol. 3, No. 1, Pp. 274-280.