Journal Of Harmonized Research (JOHR)

Journal Of Harmonized Research in Engineering
8(1), 2020, 16-22

ISSN 2347 – 7393

Original Research Article

STUDY ON SECURITY ISSUES, CHALLENGES AND SOLUTIONS OF INTERNET OF THINGS (IOT)

Manoj Verma[1] and Dr. Jitendra Sheetlani[2]

[1]Research Scholar, Sri Satya Sai University of Technology and Medical Sciences, Sehore
[2]Associate Professor, Sri Satya Sai University of Technology and Medical Sciences, Sehore

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. 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, IoT

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

For Correspondence:
Manoj.verma1511@gmail.com.
Received on: March 2020
Accepted after revision: March 2020
Downloaded from: www.johronline.com

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.

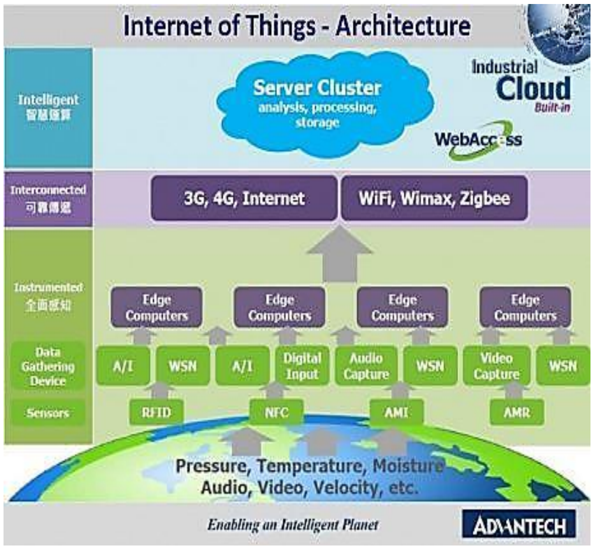

Fig.1 Architecture of Internet of things

A. Security Requirements: Security goals of Confidentiality, Integrity and Availability (CIA) are also applied to IoT. However, due to IoT restrictions and limitations in terms of the components and devices, heterogeneity and low resources, additional concerns can be added. In this section, we will present the general security requirements that the IoT must have, then we will discuss the security issues specific to each layer of the IoT. The main IoT security requirements are:

1) Confidentiality: It is very important to ensure that the data is secure and only available to authorized users by protecting information against unauthorized access and [20].

2) Integrity: To assure consistency and accuracy of data, and that it is not tampered during the transmission due to intended or unintended interference. This feature can be imposed by maintaining end-to-end security in IoT communication, and by using hash functions and digital signatures to ensure the integrity of data.

3) Availability: Data, devices and services must be available and reachable whenever users need it in. The attacks on IoT devices may hinder the provision of services through the conventional denial-of-service attacks [16].

4) Authentication: Each object in the IoT must be able to clearly identify and authenticate other objects. However, this process can be very challenging because of the nature of the IoT; many entities are in interaction in this process [20] (devices, people, services, service providers and processing units) which makes it very challenging.

B. Application of IoT: IoT solutions are widely used in numerous companies across industries. Some most common IoT applications are given below in figure 2 and brief description of applications of IoT in table 1.

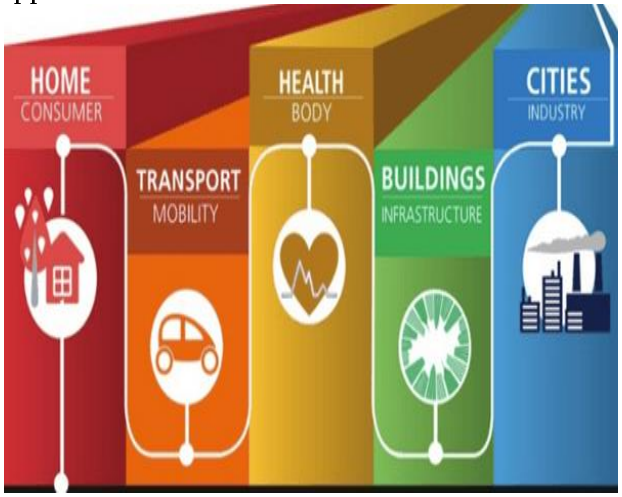

Fig.2 Applications of IoT

Table 1 Description of IoT applications

Application type	Description
Smart Thermostats	Helps you to save resource on heating bills by knowing your usage patterns.
Connected Cars	IOT helps automobile companies handle billing, parking, insurance, and other related stuff automatically.
Activity Trackers	Helps you to capture heart rate pattern, calorie expenditure, activity levels, and skin temperature on your wrist.
Smart Outlets	Remotely turn any device on or off. It also allows you to track a device's energy level and get custom notifications directly into your smartphone.
Parking Sensors	IOT technology helps users to identify the real-time availability of parking spaces on their phone.
Connect Health	The concept of a connected health care system facilitates real-time health monitoring and patient care. It helps in improved medical decision-making based on patient data.
Smart City	Smart city offers all types of use cases which include traffic management to water distribution, waste management, etc.
Smart home	Smart home encapsulates the connectivity inside your homes. It includes smoke detectors, home appliances, light bulbs, windows, door locks, etc.
Smart supply chain	Helps you in real time tracking of goods while they are on the road, or getting suppliers to exchange inventory information.

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.3 shows the three-layer IoT architecture.

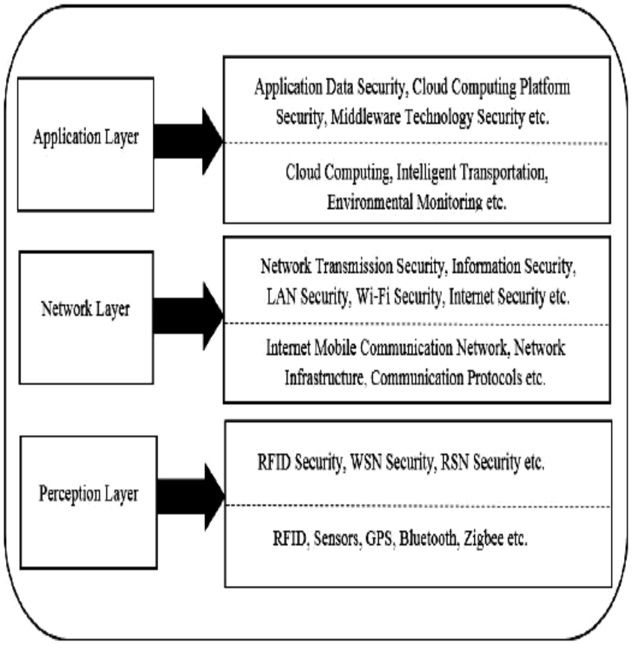
Application Layer
Application Data Security, Cloud Computing Platform Security, Middleware Technology Security etc.
Cloud Computing, Intelligent Transportation, Environmental Monitoring etc.
Network Layer
Network Transmission Security, Information Security, LAN Security, Wi-Fi Security, Internet Security etc.
Internet Mobile Communication Network, Network Infrastructure, Communication Protocols etc.
Perception Layer
RFID Security, WSN Security, RSN Security etc.
RFID, Sensors, GPS, Bluetooth, Zigbee etc.

Fig.3 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 [11]. 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. [12].

- 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. [13]. 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 [14].

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.[15]
- **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.[15]
- **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.[15]
- **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.

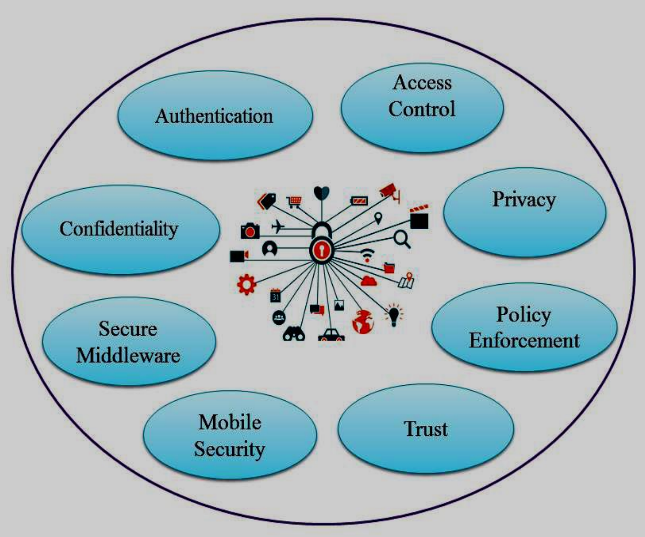

Fig. 4 Challenges in IoT

I. 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.[15]

• **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.

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] Rose, Karen et al. "The Internet of Things: An Overview." The Internet Society (ISOC), vol. 1, 2015, pp. 1-50.

[7] Abomhara, Mohamed, and Geir M. Koien. "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders, and Attacks." Journal of Cyber Security, vol. 4, no. 1, 2015, pp. 65-88.

[8] Razzaq, Mirza Abdur, et al. "Security Issues in the Internet of Things (IoT): A Comprehensive Study." International Journal of Advanced Computer Science and Applications (IJACSA), vol. 8, no. 6, 2017, pp. 383-388.

[9] Baldini, Gianmarco, et al. "Ethical Design in the Internet of Things." Science and Engineering Ethics, vol. 24, no. 3, 2018, pp. 905-925.

[10] Lin, Huichen, and Neil W. Bergmann. "IoT Privacy and Security Challenges for Smart Home Environments." Information, vol. 7, no. 3, 2016, pp. 44-54.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

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