International Journal of Management, IT & Engineering
Vol. 9 Issue 3, March 2019,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

INTERNET OF THINGS (IOT): SECURITY ISSUES AND CHALLENGES

Aashaq Hussain Najar[*]

Keywords:

Internet of Things, security issues in IoT; security; home automation; healthcare; intrinsic vulnerabilities

Abstract

The Internet of things aspires to connect anyone with anything at any point of time at any place. Internet of Things is an emerging technology across the world, which helps to connect sensors, vehicles hospitals, industries and consumers through internet connectivity. As Internet of Thing is of three-layer architecture, IoT security principles should be enabled at each layer for the proper and efficient working of these applications. Internet of Things has so many applications in today's day to day life like Home automation, Healthcare, Smart grid, Smart car etc. The intrinsic vulnerabilities of IoT devices, with limited resources and heterogeneous technologies, together with the lack of specifically designed IoT standards, represent a fertile ground for the expansion of specific cyber threats. This paper briefs the motivation for IoT, privacy, threats, challanges, IoT applications, security issues with various security solutions and challanges and opportunties for IoT.

[*] **M.Tech Student(Computer Science and Engineering),Uttarakhand Techinical University, PremNagar , Sudhowala, Dehradun, Uttarakhand ,India**

1. INTRODUCTION

Internet of Things (IoT) has attracted considerable attention during the past few years. The concept of IoT was firstly proposed by Kevin Ashton in 1999. Internet of things as the name suggests, is the connectivity of everyday devices with each other[1]. The Internet of Things (IoT) is a concept that describes a future where every day physical objects can be connected to the Internet and also be able to identify themselves to other devices [7]. According to estimation of surveys, by the year of 2020, we would be connected between 20 and 50 billion devices[2]. Thus there is a severe need to standardise it to ensure that the privacy of the user is not invaded [13]. IoT includes, for example, Cameras connected to internet that allow you to post pictures online with a single click, changing the lane while driving safely, switching off the lights automatically in a room when no one is around [8]. Nevertheless, in the past decade, this concept has been extended because of new IoT network applications such as e-healthcare and transport utilities [9]. With the advancement in technology, numerous devices are using sensors, actuators, embedded computing and cloud computing. This has enabled communication between devices. Due to rapid advancements in mobile communication, Wireless Sensor Networks (WSN), Radio Frequency Identification (RFID), and cloud computing, communications among IoT devices has become more convenient than it was before. IoT devices are capable of co-operating with one another. The World of IoT includes a huge variety of devices that include smartphones, personal computers, PDAs, laptops, tablets, and other hand-held embedded devices. The IoT devices are based on cost-effective sensors and wireless communication systems to communicate with each other and transfer meaningful information to the centralized system. The information from IoT devices is further processed in the centralized system and delivered to the intended destinations. With the rapid growth of communication and internet technology, our daily routines are more concentrated on a fictional space of the virtual world. Internet of Things is the collection of many interconnected devices, objects, services, a human which can communicate through wired/wireless mode and share data, information to achieve a particular goal or applications. Internet of Things provides Virtual connectivity through the Internet Protocol to Real life objects. Internet of Things provides the connectivity between objects timelessly. The IoT devices are heterogeneous which includes wireless sensors to less resource-constrained devices. These devices are prone to hardware/software and network attacks. If not properly secured, it may lead to security issues like privacy and confidentiality , Reliable Network and Secured Data

Transmission and Privacy are the main Concern for any Internet of Things applications. As the Internet of Things is a complex, Heterogeneous interconnected system of Smart devices, communication of such devices is associated with the shared Infrastructure and common standard. We should pay more attention to the research issues for confidentiality, authenticity, and integrity of data in the IOT[10],so privacy Protection is the main challenge for any of the Internet of things application. There are many application layer protocols for the different Internet of things applications. Depending upon the application and rate of data transmission time, heterogeneous infrastructures and smart devices available, particular protocols selected. The main aim of these protocols is to identify, track, monitor and manage the smart devices present in the network. We can find many applications of the Internet of things in almost all fields of life. Internet of things is an Intelligent network of different smart devices which can be identified, positioned, tracked, monitored and managed remotely. The applications of the Internet of things includes as; Smart parking systems, Electro Magnetic level detection system, Structural Health monitoring system, Urban noise maps, Smartphone Detection, Traffic congestion, Smart lighting system. Waste Management system, Smart Roads,Smart Homes, Smart Cars.A generalized view of Internet of Things is shown in figure 1 below.

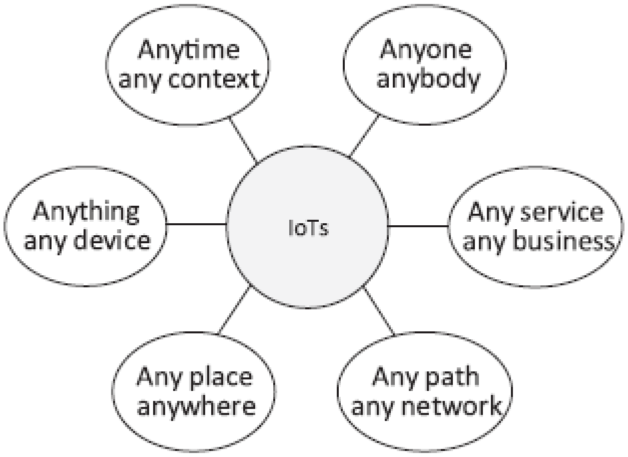


Figure 1.

2. IOT APPLICATIONS

The main objectives of IoT are the configuration of a smart environment and self-conscious independent devices such as smart living, smart items, smart health, and smart cities among others. As per the survey conducted by the IoT-I project in 2010[6] indicated IoT's circumstance applications could be grouped in 14 domain viz; Transportation, Smart home, Smart city, Lifestyle, Retail, Agriculture, Smart factory, Supply chain, Emergency, User Interaction, Healthcare, Culture and tourism, Environment and Energy[5].The applications of IoT in industries, the medical field, and in home automation are discussed in the following section.

I. IoT in Industries:

The IoT has provided a fair opportunity to build significant industrial systems and applications, in an intelligent IoT transportation system, the authorized person can monitor the existing location and movement of a vehicle. The authorized person can also predict its future location and road traffic. In the earlier stage, the term IoT was used to identify unique objects with RFID. Latterly, the researchers relate the term IoT with sensors, Global Positioning System (GPS) devices, mobile devices, and actuators. The acceptance and services of new IoT technologies mainly depend upon the privacy of data and security of information. The IoT permits many things to be connected, tracked and monitored so meaningful information and private data collected automatically. In IoT environment, privacy protection is a more critical issue as compared to traditional networks because numbers of attacks on IoT are very high.

II. IoT in Personal Medical Devices

The IoT devices are also widely used in healthcare systems for the monitoring and assessment of patients[3]. To monitor the medical condition of a patient, Personal Medical Devices (PMDs) are either planted in patients body or it may attach to patients body externally. PMDs are small electronic devices that are becoming very common and popular. The market value of these devices is projected to be around 17 billion dollars by 2019. These devices use a wireless interface to perform communication with a base station that is further used to read the status of the device, medical reports, and change parameters of the device, or update status on the device[11]. Wireless interface causes a lot of security and privacy threats for the patient. The wireless interface of such devices is very easy to cyber-attacks that may jeopardize the patients' security, privacy, and safety. In the case of health care, the primary goal is to ensure the security of the network in order to prevent the privacy of patient from malicious attacks. When attackers attack mobile devices, they have their predefined goals[12]. Usually, their aim is to steal the information, attack on devices to utilize their resources, or may shut down some applications that are monitoring patients condition. There are many types of attacks on medical devices that include eavesdropping in which privacy of the patient is leaked, integrity error in which the message is being altered, and availability issues which include battery draining attacks. Some cybersecurity threats related to security, privacy, and safety of medical data of the patient are discussed as follows:

1) PMDs are critical to any task that uses battery power.
Hence these devices must support limited encryption. If the device is a part of different networks then confidentiality, availability, privacy, and integrity will be at high risk.
2) As PMDs have no authentication mechanism for wireless communication. So the information stored
in the device may be easily accessed by unauthorized persons.
3) The absence of secure authentication also uncovers the devices to many other security threats that may lead
to malicious attacks. A hostile may launch Denial of Service (DoS) attacks.
4) The data of the patient is sent over transmission medium which may be altered by unauthorized parties, as result privacy of a patient may lose.

III. IoT in Smart Home:

The IoT smart home services are increasing day by day [4], digital devices can effectively communicate with each other using Internet Protocol (IP) addresses. All smart home devices are connected to the internet in a smart home environment. As the number of devices increases in the smart home environment, the chances of malicious attacks also increase. If smart home devices are operated independently the chances of malicious attacks also decreases. Presently smart home devices can be accessed through the internet everywhere at any time[14]. So, it increases the chances of malicious attacks on these devices. A smart home consists of four parts: a service platform, smart devices, home gateway, and home network as shown in Fig. 2. In the smart home, many devices are connected and smartly shares information using a home network. Consequently, there exists a home gateway that controls the flow of information among smart devices connected to the external network[15]. Service platform uses the services of a service provider that deliver different services to the home network.

3. IOT SECURITY, PRIVACY, THREATS AND CHALLENGES

The era of IoT has changed our living styles. Although the IoT provides huge benefits, it is prone to various security threats in our daily life. The majority of the security threats are related to leakage of information and loss of services[1]. In IoT, the security threats straightforwardly are affecting the physical security risk. Cyber attacks are recorded almost every day, mainly due to the poorly secured applications, services, and devices [16]. The IoT consists of different devices and platform with different credentials, where every system needs the security requirement depending upon its characteristics. The privacy of a user is also most important part because a lot of personal information is being shared among various types of devices. Hence a secure mechanism is needed to protect the personal information. Moreover, for IoT services, there are multiple types of devices that perform communication using different networks. It means there are a lot of security issues on user privacy and network layer[17]. User privacy can also be uncovered from different routes. Some security threats in the IoT are as follows:

a) E2E Data life cycle protection: In order to ensure the security of data in IoT environment, end-to-end data protection is provided in a complete network. Data is collected from different devices connected to each other and instantly shared with other devices. Thus it requires a framework to protect the data, confidentiality of data and to manage information privacy in the full data life cycle.

b) Secure thing planning: The interconnection and communication among the devices in the IoT vary according to the situation. Therefore, the devices must be capable of maintaining the security level. For example, when local devices and sensors used in the home-based network to communicate with each other safely, heir communication with external devices should also work on the same security policy.

c) Visible/usable security and privacy: Most of the security and privacy concerns are invoked by misconfiguration of users. It is very difficult and unrealistic for users to execute such privacy policies and complex security mechanism. It is needed to select security and privacy policies that may apply automatically.

4. Security Threats in Smart Home

Smart home services can be exposed to cyber-attacks because the majority of the service provider does not consider security parameters at early stages. The possible security threats in a smart home are eavesdropping, Distributed Denial of Service (DDoS) attacks and leakage of information, etc. Smart home networks are threatened by unauthorized access[18]. The possible security threats to smart home are discussed as follows;

a) Trespass: If the smart door lock is effected by malicious codes or it is accessed by an unauthorized party, the attacker can trespass on smart home without smashing the doorway. The result of this effect could be in the form of loss of life or property[19]. To get rid of such attacks, passwords should be changed frequently that must contain at least ten characters because it is very difficult for attackers to break the long password. Similarly, the authentication mechanism and access control may also be applied.

b) Monitoring and personal information leakage: Safety is one of the important purposes of a smart home. Hence there are a lot of sensors that are used for fire monitoring, baby monitoring, and housebreaking, etc. If these sensors are hacked by an intruder then he can monitor the home and access personal information as shown.In order to avoid such attacks, data encryption must be applied between gateway and sensors or user authentication for the detection of unauthorized parties may be applied.

c) DoS/DDoS: Attackers may access the smart home network and send bulk messages to smart devices such as Clear To Send (CTS) / Request To Send (RTS)[20]. They can also attack targeted device by using malicious codes in order to perform DoS attacks on other devices that are connected in a smart home. As a result, smart devices are unable to perform proper functionalities because of draining resources due to such attacks. For avoidance from this attack, it is very important to apply authentication to block and detect unauthorized access.

d) Falsification: When the devices in smart home perform communication with the application server, the attacker may collect the packets by changing routing table in the gateway. In this way, the attacker can misinterpret the contents of data or may leak the confidentiality of data. In order to secure the smart home, it is very important to block unauthorized devices that may try to access smart home network. The IoT helped to build connections from human to human, human to physical objects and physical object to other physical objects. As per appraisal from IDC, there will be 30 billion internet-connected devices by 2020. This rapid growth of internet data needs a more valuable and secure network.

5.Cyber Resistance Radio(CRR):

There are almost two million to the CRR. In this, we take about the information security threats to 2017, what we can expect from 2017 and what types of security threats and attacks we expect from 2017.

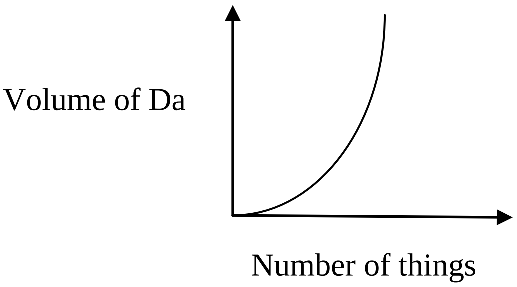
One of the major threats and disastrous waling to happen has to do with the mass increase in the internet of things devices. The manufacturers of these devices barely take security into consideration when developing these devices. In 2016, we have seen coordinated by e.g: security cameras connected to the internet. These devices are amongst D-DOS attacks in history. If you are interested just check out “SHODAN”, this is a search in for the internet of things, at least devices connected to the internet have little or no security. You can log on to webcam sometimes even network attached storage devices. You will be amazed at how many devices are open to you as a user. Nowadays manufacturers of the devices, who offer products with internet connectivity, we apparently all want to control the devices very conveniently not only for you but also for the outside world have security cameras and refrigerators are always connected to the internet, again convenient for you as a user switching on the light one united home but it is also convenient for manufacturers again acts the information and let its big data team loose on the data plus it is also very interesting for hackers. All these devices have chips inside them, a hardware and simple software to make away do things. This software can be manipulated and used for the attacks on the website all part of the internet architecture. Most of these devices have network capability and that is this problem. These devices can take part of the coordinating attacks without the owner even not knowing it if you have internet of devices at home check it if you can update the software or at least place the devices in the different Virtual Lane (V- Lane). Your television will be held hostage, another development is the more and more television is smart, some of them have software on them and internet connect capability expect more and more Malware attacks on these televisions. There is already a Malware that can break your television, rendering it useless. Sometimes attacks even go on for as to as many to break your television again. Basically holding your television as a hostage, that is a blizzard. The only good thing is the malware looks another type of smart television and no to do the type in the market, of course, that is only temporary. If there is money involved and attacks find new ways to then access to devices it is a concern especially when manufacturers do not really take security into account when they are developing these television sets and its software.

Moving on next to the television, your car also gets more connected to the internet. You have software to control your car and the ECU for your instance and you have software for an entertainment system for your audio, locks, navigation, telephone and right settings. To colour big storage shots the car has an entry point for communication either through the fallopian 4g pana 9(Balmain 4g pana) and GSM system for mobile telephone calls, audio infrared receiver on your door system. We live in an era where almost everything gets connected to the internet connection, we need to be careful and realize that exposes the threats as well. Many convenient things are possible with the connectivity, devices that are connected to the internet but always understand the risks as well when concerned about the internet security rights, these deceive you could have a little more faith in the technology until just be careful.

When you look at your house or apartment, it might be very well possible to connect your house and have a lock management system on your phone or laptop in future. With this Appprogram, you could check if your house is locked down when you are on way. I am sure the traditional lock system will be connected to the internet in the near future. Again offering convenience but also adding an external threat in the form of new bread burglars. How crazy would it get if your phone security system that is probably connected to the internet became part of the BOTNET that D-DOS or a network I think it is crazy, but it have already might be happening right now?

6. Internet of Things: Challenges and Opportunities

The Internet of Things digitizes physical assets, sensors, devices, machines, gateways on the network. It connects people to things and things to things in real time. A typical IoT now working go rapidly resulting in an exponential increase in providing; variety, velocity and overall volume of the data.



This structure open opportunities for significant time equation and revenue generation but the real challenges for IoT environment has to analyze for information from last resources and take action in real time what this means to you, the complexity of the IoT combined with the high expectation created by the internet mobile devices and 24x7 IT environment. It made the need for new analytic approaches and technologies more urgent. Achieving desired business objectives is required the ability to act in real time to take advantage of opportunities and address problems quickly.

In the pre IoT era, the issues of the typical supply chain scenario are addressed in the two to three-day cycles for satisfactory results. But in the IoT, time to act is in minutes, seconds or microseconds, 30 minutes to visualise the problem, 30 seconds to act on information on devices, 5 milliseconds to address the security breach. This explosion of data at a high expectation of IoT environment is the reliable data will slip away quickly. The importance of time to act for the internet of things is that the application could be seen in the wide reliable application in these cases. Broadly speaking these applications can be grouped in the three categories:

1. Operations and fulfilment
2. Customer focused cells and marketing
3. Innovation in products and services

Theses provide predictive maintenance, demands and supply optimization, predictive to marketing outage management addressing the critical time to action requirement in the case and application demands an advanced analytics solution.

7. CONCLUSIONS

The main emphasis of this paper was to highlight major security issues of IoT particularly, focusing the security attacks and their countermeasures. Due to lack of security mechanism in IoT devices, many IoT devices become soft targets and even this is not in the victim's knowledge of being infected. In this paper, the security requirements are discussed such as confidentiality, integrity, and authentication, etc

Internet of things is a new technology which provides many applications to connect things to things and human to things through the internet. Each object in the world can be identified, connected to each other through internet taking decisions independently. Moreover, to protect from any intruders or security threat, it is also recommended not to use default passwords for the devices and read the security requirements for the devices before using it for the first time. Disabling the features that are not used may decrease the chances of security attacks. Moreover, it is important to study different security protocols used in IoT devices and networksIoT requires standardized approach for architectures, identification schemes, protocols and frequencies will happen parallels, each one targeted for a particular and specific use. By the internet of things many smart applications becomes real in our life, which enables us to reach and contact with everything in addition to facilities many important aspects for human life such as smart healthcare, smart homes, smart energy, smart cities and smart environments.

References

[1] S.Vashi, J.Ram, J.Modi, S.Verma, Dr.C.Prakash ;"*Internet of Things",*International Confrence on IoT in Social, Mobile, Analyticas abd Cloud;pg-492-96;2017.

[2] Boheung Chung, Jeongyeo, and Youngsung Jeon ;"*On Demand Security Configuration for IoT Devices"*, ICTC,IEEE Conference;pg-1082-84;2016.

[3] Sharath Anandl, Sudhir K. Routray ; “*Issues and Challenges in Healthcare Narrowband IoT”,* International Conference on Inventive Communication and Computational Technologies;pg-486-89;2017.

[4] D. Geneiatakis, I. Kounelis, R. Neisse, Igor Nai-Fovino G.Steri, and G. Baldini ; “*Security and Privacy Issues for an IoT based Smart Home”,* MIPRO 2017, May 22- 26, 2017, Opatija, Croatia;pg-1292-97;2017.

[5] Santhosh Krishna B V, Gnanasekaran T; “*A Systematic Study of Security Issues in Internet-of-Things(IoT)”,* International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud);pg-107-11;2017.

[6] Arampatzis, T., et al; “A Survey of Security Issues in Wireless Sensors Networks, in Intelligent Control”, IEEE International Symposium on, Mediterranean Conference on Control and Automation;pg- 719-24; 2005.

[7] Jun Wei Chuah ―The Internet of Things: An Overview and New Perspectives in Systems Design‖ 2014 International Symposium on Integrated Circuits 978-1-4799-4833-8/14.

[8] Sarita Agrawal, Manik Lal Das ―Internet of Things – A Paradigm Shift of Future Internet Applications‖ Institute of technology, nirma university, ahmedabad – 382 481, 08-10 december, 2011.

[9] [9] D.Geneiatakis, I.Kounelis,R.Neisse, I.Nai-Fovino,G.Steri,G.Baldini;”*Security and Privacy Issues for an IoT based Smart Home”*,MIPRO Conference;pg-1292-97;2017.

[10] Jaifu wan,Caifeng Zou, Jainqi Liu, Hui Suo ;” *Security in the Internet of Things: A Review”*,ICCSEE;pg-648-51;2012.

[11] P. A. Laplante, and N. Laplante, “*The Internet of Things in Healthcare: Potential Applications and Challenges*”, *IEEE IT Professional*;pg- 2 – 4;2016.

[12] K.-H. Yeh, “*A Secure IoT-based Healthcare System with Body Sensor Networks*,” *IEEE Access*; pg- 10288-99;2016.

[13] Ala Al-Fuqaha , Mohsen Guizani , Mehdi Mohammadi “*Internet of things: a survey and enabling technologies, protocols and application*”, IEEE Communication Surveys & Tutorials, Vol. 17, No. 4, Fourth Quarter 2015.

[14] C. Perera, C. McCormick, A. K. Bandara, B. A. Price, and B. Nuseibeh; “*Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms*”, International Conference on the Internet of Things;pg-83–92;2016 .

[15] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle; “Privacy *in the internet of things: threats andchallenges*”, Security and Communication Networks;pg-2728-42.

[16] D. Miorandi, S. Sicari, F. D. Pellegrini, I. Chlamtac; “Internet of things: Vision, applications and research challenges”, Ad Hoc Networks 10 (7) (2012) 1497.

[17] R. Roman, J. Zhou, J. Lopez,; “*On the features and challenges of security and privacy in distributed internet of things*”, Computer Networks 57 (10) (2013).

[18] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits; “*Denialof- service detection in 6lowpan based internet of things*”, IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob); pg- 600–07.

[19] A. Jacobsson and P. Davidsson; “*Towards a model of privacy and security for smart homes*”, IEEE 2nd World Forum on Internet of Things (WF-IoT); pg -727–32;2015.

[20] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle; “*Privacy in the internet of things: threats andchallenges*”,Security and Communication Networks, vol. 7, no. 12, pg-2728–42;2014.