A review on security threats in Smart Home technology using IOT

[1]Dr Venkatadri Marriboyina
[1]Professor
[1]Dept of Computer Science and Engineering
[1]Amity University Madhya Pradesh, Gwalior, India

Abstract: Internet of Things (IoT) become an emerging technology to establish smarter and connected world. IoT become very popular now a days among the researchers due to the advancements in Information communication Technology and sensor devices. IoT supports various applications and services in different domains, such as smart cities and smart homes. With this technology, our life becomes more comfortable and convenient in our day to day operations. Smart home provides fully automotive, intelligence, smart and innovative services to residential users through Information Communication Technology (ICT). Since 5G communication technology enables the IoT in a more efficient and effective way to smart home, to provide security, authentication and privacy. In this paper, we will discuss various security issues and their solutions in the smart home environment.

IndexTerms **- Internet of Things, Smart City, Smart Home, Security Issues, Wireless technology.**

I. INTRODUCTION

Advancements in information technology, Wireless communication, Internet and 5G communication creates our world as a global connected world. The advanced technologies transform our cities in to Smart Cities. IoT [1] is key enabler to convert our city in Smart city. A smart home or connected home is a highly advanced automatic system is a component of a smart city. Smart home become more popular to enhance the quality of living life by IoT and networking technologies to monitor, control various things like lighting system, home appliances, security devices irrespective of time and location barriers. Remote communication through internet, sensor technology and Machine to machine communication with the help of networking home automation creates new avenues for smarter life, same time security issues are the major concerns.

Smart home application built on top of IoT infrastructure [2]. Smart home performs various functions like smart lighting, smart monitoring, intelligent home appliances. Security is our primary concern to serve these functions most effectively. The smart home with security with proper sensor devices and network communications among various devices will automatically alert the whole system in case of security breach [3]. The smart monitoring and advanced smart automation system enable alert facility to send an alarm upon the user's discretion in case of critical situation. The provision of the security alarm is built in the system with sensor and a micro controller device. Privacy & security are essential requirement for operation of a system that is trusted in IOT [4]. Smart home threats and effective solutions are very crucial for betterment of advanced automation smart homes.

.

II. Threats related Smart Home

Rapid development of internet technologies, 5G Communication and urbanization leads to smart city implementation. IoT becomes ubiquitous and deeply interwoven in our daily lives and societies especially in smart home design and implementation [5]. The security threats and attacks against IoT devices and services increases nowadays due to the widespread use of technology. Today internet has become as the fundamental utility instead of a research tool. If there are too many resources that are available to the user to make their research easy then there are also many crimes that are seeking to gain value. The interconnectivity of the internet means that attacks to any system to anywhere from anywhere in the world and this interconnectivity is the key issue to the security in connected homes [6].

Cyber security has three basic themes [7]:

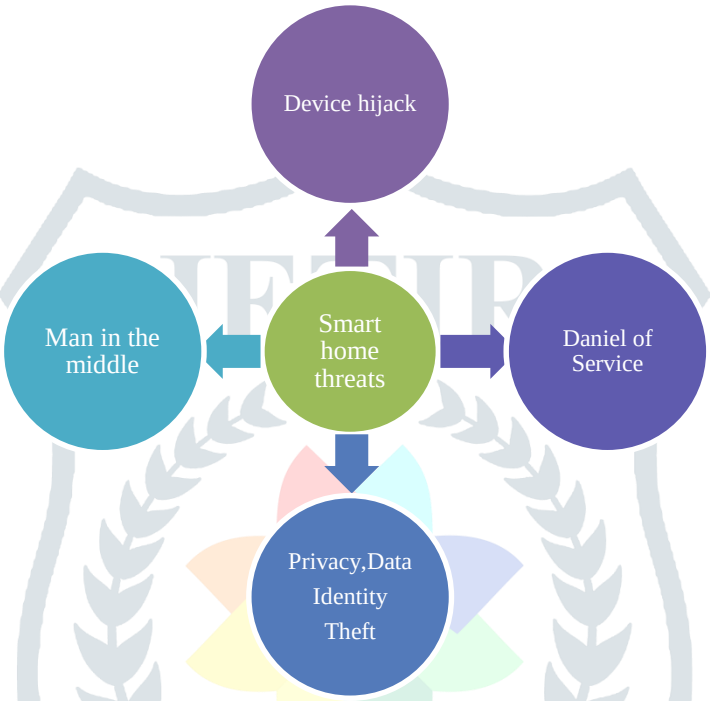
- Confidentiality
- Authentication
- Access

a. Confidentiality: Confidentiality is all about the security of the data or to keep the data private so that the authorized user can only access the data. Cryptography is a key method to achieve confidentiality. Cryptography is associated with the process that the plain original text is converted into encrypted text and sent in the network for the intend users, further this encrypted data converted to decrypted text with the help of decrypted key by the authorized user.

b. Authentication: Authentication is all about verifying that the data that is going to transferred is safe or not. Another thing is to verify the data is going to share to the claimed owner. Here one thing is considered separately that is non –repudiation (avoiding the denial by a sender).

c. Access: Access refers to only allow the authorized user can access the data, sharing the network, computing the resource or to ensure that there is no prevention from such kind of access.

Although the environment of a smart home is very different, and its threats of security are very similar to another domain. Confidentiality threats shows the unwanted release of the private information or the information that is private. For ex: Its infringed monitoring system in home which lead to unwanted or accidental release of data for ex home temperature along with all details of ac system parameter are also used to check whether there is occupied or not. Authentication to threats can lead to the sharing of information or control of system confuse authentic user that there is something going on makes the whole system uncertain. This can be through unseemly secret key and key administration, or it could be by unapproved gadgets associating with the system. Regardless of whether control can't be picked up, an unapproved association with a system can take organize transmission capacity or result in a disavowal of administration to authentic clients. Since present day Smart Home frameworks are associated with the Internet, assaults can be led remotely, it either can be direct access to organized control interfaces or can be download malware to gadgets. The following figure shows the popular threats in association with the smart home [8,9]



Smart home IoT Threats

III. Available Solutions smart home Threats

Smart home threats can be handled very effectively through the available technology, but always a scope to improvise the system in a most efficient way. The security threat Device hijacking can be effectively handled through Device identification and Access control mechanism. The threat Daniel of Service can be handled through the authentication and encryption, further it also can be handled through access control and application level Daniel of service. Man in the middle attack can be effectively through security life cycle management. Most IoT gadgets are low vitality, utilize Low-End Microcontroller (LEM) and have restricted memory. Such controllers are very much coordinated to the prerequisites of independent controllers in a clothes washer or climate control system. Through the implanted IoT gadgets threats can be limited. A few (Internet Engineering Task Force) IETF working gatherings have been made to handle these issues.

IV. Conclusion

IoT is a domain of single application and the application that are used as domestic smart home ‘s security system is basically quite different from those application that are afforded to the (MCA)Mission Critical Application in industry or for other uses. This paper presents the importance of IoT to design an efficient Smart home and also elaborate various threats associated with smart home IoT devices, further it also provides some basic solutions to these threats. Further to this the author will work on an efficient multipurpose solution to handle all these threats.

REFERENCES

[1] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, Internet of Things (IoT): A vision architectural elements and future directions, Future Generation Computer Systems (Elsevier), pp. 1645-1660, 2013
[2] Timothy Malche, “Internet of Things (IoT) for building smart home system” , 2017 International Conference on I- SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), https://ieeexplore.ieee.org/document/8058258.
[3] Gaurav Tripathi, Dhananjay Singh, and Antonio J. Jara, "A survey of Internet-of-Things: Future Vision, Architecture, Challenges and Service", IEEE World Forum on Internet of Things (WF-IoT), 2014, pp. 287-292.
[4] Ming Wang, Guiqing Zhang, Chenghui Zhang, Jianbin Zhang, and Chengdong Li, "An loT-based Appliance Control System for Smart Homes", Fourth International Conference on Intelligent Control and Information Processing (lCICIP) June 9 - 11, 2013, pp. 744-747
[5] Vittorio Miori, and Dario Russo, "Domotic evolution towards the loT", 28th International Conference on Advanced Information Networking and Applications Workshops, 2014, pp. 809-814
[6] Sarita Agrawal, and Manik Lal Das, "Internet of Things - A Paradigm Shift of Future Internet Applications", International Conference on Current Trends in Technology, December, 2011
[7] Qingping Chi, Hairong Yan, Chuan Zhang, Zhibo Pang, and Li Da Xu, "A Reconfigurable Smart Sensor Interface for Industrial WSN in loT Environment", IEEE Transactions on Industrial Informatics, vol. 10, no. 2, May 2014
[8] Moataz Soliman, Tobi Abiodun, Tarek Hamouda, Jiehan Zhou, and Chung-Horng Lung, "Smart Home:Integrating Internet of Things with Web Services and Cloud Computing", IEEE International Conference on Cloud Computing Technology and Science, 2013, pp. 317-320
[9] Kang Bing, Liu Fu, Yun Zhuo, and Liang Yanlei, "Design of an Internet of Things-based Smart Home System", The 2nd International Conference on Intelligent Control and Information Processing, July 2011, pp. 921-924