Security Issues in a Smart Home: A Review

Navpreet Kaur
Assistant Professor
Baba Farid College, Bathinda

Amandeep Kaur
Assistant Professor
Baba Farid College, Bathinda

ABSTRACT
Smart home is the latest and ultra-modern technology nowadays. It has become indispensable part of our lives. Smart homes devices are smart and talented. It can be controlled with the help of mobile but still there are shortcomings of these devices. In this paper, we have discussed issues and countermeasures of the smart home environment.

Keywords
Smart Home, Automation, Threats, centralized system, confidentiality

1. INTRODUCTION
Smart Homes consist of intelligent home appliances to make our live more straightforward and comfortable. It is also referred to as Home automation where it provides security to the users. These devices are interlinked with each other's and can be controlled from a remote location.

A smart home defines those homes consists of advanced automation systems and intelligent devices that authorizes the house owner with timely monitoring and control over the house in his absence. In these Smart homes, lights are smart and talented. It can be controlled with the help of mobile phones. Smart homes wisely exploit the innovation of technology for smooth actions in the household. It depends on a home automation technology solution to subordinate every single device to collect, examine and define decisions based on the evidence [1].

1.1 Need for Smart Homes
This technology has brought us in the past 30 years in the term of saving energy, money, time, etc. In many parts of the world, where adopters of technology are adopted with the rapid speed logy, have already started building their dream homes with proper wiring so that it can be accessed and monitored as smart homes whereas, old houses can be modified by installation and placing sensors. It provides a secure environment where you can access and control your home within few clicks. It is the energy efficient method too. It helps to save our non-renewable resources.

It provides us an effective way to save energy and enables us to focus on our work without any concern [2].

1.2 Smart home devices
There are different smart home gadgets which can fit well into the family of Internet of Things family. The vital point is the scope of the gadgets is always expanding step by step concerning automation control and sensors. Every day as new devices flood the market, it also opens up the new pathway, a new roadmap for better innovation and better strategy which can altogether help the IoT industry cross the toughest hurdle of nascent stage [3]. Some of the smart home devices are:

1. Smart Refrigerator: Refrigerator is an intelligent device which apart from controlling the temperature, also makes a menu of the available food items, notifies the user about stock replenishment and recommends healthy food with particular nutritional value.

2. Amazon Echo: It is a hands-free speaker which can be utilized and controlled by the voice recognition system. You can command it to perform multiple tasks at the same time.

3. Amazon Cloud Cam: It is an affordable security camera that captures live videos at 1080p resolutions. It can be installed in any room to get the real time motion notification and also offer free around the clock clip storage.

2. REVIEW OF LITERATURE
The IoT has gained popularity in the recent years. But this approach still has some issues and challenges. Rakesh Roshan and Abhay K Ray [2] explained many IoT challenges in Indian Scenerio like cost, availability. Maintenance issues and its purpose are clearly defined in this paper. They also discussed the frameworks to sort out issues related to this platform. Menal Dahiya [3] discussed various challenges and issues present in the smart home network environment. This system is adopted widely day by day. Therefore, it is a need to provide end-to-end solution to the user to secure their valuable data. Ali et.al [4] defined the OCTAVE methodology to handle all the challenges and issues faced by the Smart Home Environment. This method mainly focuses on the information and consider different to handle all the issues related to it. Huichen Lin and Neil W. Bergmann [8] has explained privacy and security challenge faced in the internet of things environment. To handle these devices, there is a need of advancement of the technology to cater the needs of the technology. This paper identifies the key features requirements for the trusted smart home system. A Smart Home gateway architecture supported by web-services for automatic device and network configuration and automatic system updates is the solution for this technology.

3. SECURITY ISSUES OF THE SMART HOME
Everything have two aspects positive and negative. In the same way, smart homes also have some security risks. These are [4]:

3.1 Threats
Smart homes are responsible for severe perils too, such as blackmail, theft, etc. Therefore, there is a need to take practical steps to stop these menaces. Hacking are, denial of services, eavesdropping, buffer overloading, malicious modifications, password based attacks, the man in the middle attack, phishing etc. As hackers are new in this technology, mainly security loss and data loss for the home owner and vendors are the main threats that are possible in smart homes. Authentication threats, access threats and confidentiality

threats all come under this issue.

3.2 Attacks

It is found that these smart devices have some privileges which lead to the hacker to hack the system or trigger attacks. It is possible due to smartphones as they have opportunities to perform some operation on the devices such as turn on and off the TV etc. Thus, it demands the accessing of the camera and location and hackers can easily hack it.

3.3 Insecure messaging system

Smart Apps can communicate with anyone with the help of instant messaging. These devices send which contain sensitive information such as pin code of locker etc. if you are sharing this information with someone over the phone and someone read your messages and hacks your phone thus locking information is revealed, and there is no protection left [4].

3.4. Poor Product Design

The whole appliance is based upon the centralized system. The security of this system is based upon the products which are used in various applications or used in the devices those connect the smart home systems. Several product designs are unsuccessful to integrate the basic requirements of the security into the main products. Thus, these devices are not up to the mark to maintain the privacy and other safety concerns that are specific to the home only. All the devices are connected to a single device. Therefore, if the central system fails, all other dependent devices also get fails [5].

3.5. Limited Software Updates

A variety of software updates can be outlined using software patches. According to the survey, 97% of security incidents can be recognized due to patch vulnerabilities failure in current software applications [6]. The use of third party components is unable to find out the problems in source components.

4. COUNTERMEASURES FOR A SECURE SMART HOME ENVIRONMENT

These issues have some solution too. These solutions are [4]:

4.1. Tool: To overcome serious threats always use surveillance tool which helps to alert the owner when the garage door opened or closed when an owner is not in the house. The other way to keep smart home privately is to ensure that a home doesn't have any ports opened in its router. If the owner does decide to have a remote access to his home, then always make use of virtual private network (VPN) rather than opening ports in your router [1].

2. Protocols: To over the attacks, use popular ZigBee protocols which helps to detect and prevent the attacks.It is the one of the secure protocols which is used to protect your data from major risks [3].

3. Acknowledge based system: Acknowledge based system must be used to create a Pin code for the doors by sending a confirmation message to the network.

4. Uninterruptible Power Supply: One of the best solutions to avoid design issues is the use of an uninterruptible power supply (USP) so that in the event of a power cut your system still runs. In addition to it, a an additional mini-server acts as a backup, arrange emergency lighting and circuits and always attached an SD card with these devices. So in case of application fault a live install take place from the vendor side [5].

5. Regular updates: With the advent of technology, everything is changing day by day at the rapid speed. So it is necessary for all of us and for our security, that technology is always up to date. Therefore, carry out regular update for smart home [7].

Table 1. Issues and Countermeasures

Sr. no	Issues	Counter measures
1.	Threats	Surveillance tool
2.	Attacks	ZigBee Protocol
3.	Insecure messaging system	Acknowledge Based System
4.	Poor Product Design	Uninterruptible Power Supply
5.	Limited Software Updates	Regular Updates

5. CONCLUSION

There is no doubt; smart homes are one of the biggest innovations of the century. It makes our life simpler, easier and hassle free. It helps to save our money too. But, these systems have some security issues such as threats, attacks and insecurity. In this paper we have discussed all the security issues and their pragmatic solutions to provide security to the users so that they can enjoy this innovation without any doubt.

6. REFERENCES

[1] Tyrsina, R. (2013). *Best 20 Internet of Things Devices.* Retrieved from,http://techpp.com/2013/10/16/best-internet-of-things-devices/

[2] Roshan, R., & Ray, A. K. (2016). Challenges and risks to implement IOT in smart homes: an Indian perspective. *Int J Comput Appl*, *153*, 16-19.

[3] Dahiya, Menal. (2017). Issues and Countermeasures for Smart Home Security. International Journal of Innovative and Emerging Research in Engineering. 4. 124-126.

[4] Ali, B., & Awad, A. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors*, *18*(3), 817.

[5] Zheng, X., Cai, Z., & Li, Y. (2018). Data linkage in smart internet of things systems: A consideration from a privacy.perspective. *IEEE Communications Magazine*, *56*(9), 55-61.

[6] Ricquebourg, Vincent & Menga, David & Durand, David & Marhic, Bruno & Delahoche, Laurent & Logé, Christophe. (2007). The Smart Home Concept : our immediate future. 2006 1st IEEE International Conference on E-Learning in Industrial Electronics, ICELIE. 23 - 28. 10.1109/ICELIE.2006.347206.

[7] Chin, J., Callaghan, V., & Allouch, S. B. (2019). The Internet-of-Things: Reflections on the past, present and

future from a user-centered and smart environment perspective. *Journal of Ambient Intelligence and Smart Environments*, *11*(1), 45-69.

[8] Lin, H., & Bergmann, N. (2016). IoT privacy and security challenges for smart home environments. *Information*, *7*(3), 44.

[9] Kumar, Sathish & Vealey, Tyler & Srivastava, Harshit. (2016). Security in Internet of Things: Challenges, Solutions and Future Directions. 5772-5781. 10.1109/HICSS.2016.714.

[10] Radoglou-Grammatikis, Panagiotis & Sarigiannidis, Panagiotis & Moscholios, Ioannis. (2018). Securing the Internet of Things: Challenges, Threats and Solutions. 10.1016/j.iot.2018.11.003.