Journal of Advanced Multidisciplinary Research Studies and Development

ISSN : 2583-6404
Jul - Aug 2024

# AN ANALYSIS OF THE RISKS ASSOCIATED WITH IOT-BASED SMART HOME SYSTEMS AND THEIR POSSIBLE SOLUTIONS

**Dr. Surendra Kothari**
*Assistant Professor, University of Science & Technology, Meghalaya.*

**Abstract**
Due to its affordability, ease of use, and ease of installation, Internet of Things (IoT) technology has quickly acquired popularity and is currently utilized everywhere. We now use IoT devices on a regular basis; they have simplified our lives and decreased our workload. The smart home environment is a real-world example of an Internet of Things application. Smart home systems are becoming a significant part of our daily lives because they offer a variety of features and benefits, but they also present significant challenges because they rely on the internet for connectivity, making them susceptible to cyberattacks. When using IoT devices, privacy and security are the main concerns. An overview of smart home systems, their architecture, environmental hazards and vulnerabilities, and remedies are covered in this paper.
**Keywords:** Internet of Things (IoT), Smart Home System, Cyber Threats.

► *Corresponding Author: Dr. Surendra Kothari*

## Introduction

There is no need to introduce Internet of Things technology in this digital age. Since its introduction to the globe, smart devices that run on the internet have become an essential part of our everyday lives. The ease of use, ease of installation, and cost-effectiveness of IoT devices are key factors in their success. IoT devices are simple to use, but because they are connected to the Internet, they are susceptible to cyberattacks. Since its introduction, privacy and security have been the main concerns. Cybercriminals are taking advantage of the weaknesses in the current IoT ecosystem to compromise the owner's security and privacy, gain access to the device, and use it anyway they choose.

IoT technology is demonstrated in the real world via smart home appliances and applications. Because these gadgets are less secure and are therefore simple targets for hackers, cybercriminals exploit them as victims.

The significance of self-automated and controlled devices and technologies has grown, making them an integral part of our daily lives due to their easy installation, user-friendly nature, and remote accessibility via the internet. Smart home technologies have recently surged in popularity due to their ability to minimize human effort and their user-friendly interface. A smart home refers to an environment equipped with electronic devices that can be easily managed by the owner, thus reducing the need for manual effort. In a traditional home setting, the owner must physically access the switchboard to turn the fan or light bulb on or off, whereas in a smart home, these devices can be controlled using a remote or mobile phone. Smart home applications lessen the need for human effort and enhance convenience. The smart home environment surpasses the constraints of traditional homes. Users have the ability to manage and communicate with every device in the smart home setting using a mobile app or laptop. These devices utilize wired or wireless connectivity mediums such as Bluetooth, ZigBee, or Wi-Fi connections. As a result, homeowners can effortlessly control, monitor, and engage with these devices at their preferred time and location.

ISSN : 2583-6404
Jul - Aug 2024

This survey paper has addressed the vulnerabilities, security threats, and privacy concerns found in real-world IoT applications, specifically the Smart Home Environment. The paper is structured into the following sections: Section II provides a brief overview of smart home architecture. Section III covers the threats to smart home environments, and Section IV offers guidelines and preventive measures to mitigate the threats in the current IoT-based Smart Home System, concluding with discussions in Section V.

**IoT Based Smart Home Architecture**

The Smart Home differs from the traditional home setting because the household appliances are interconnected through wired or wireless means, allowing the homeowner to easily control them. This type of home environment is typically diverse, with various devices equipped with programmable sensors communicating with each other and being managed by the homeowner using a remote device such as a smartphone, laptop, or tablet. The user can conveniently oversee and regulate the devices within the smart home.

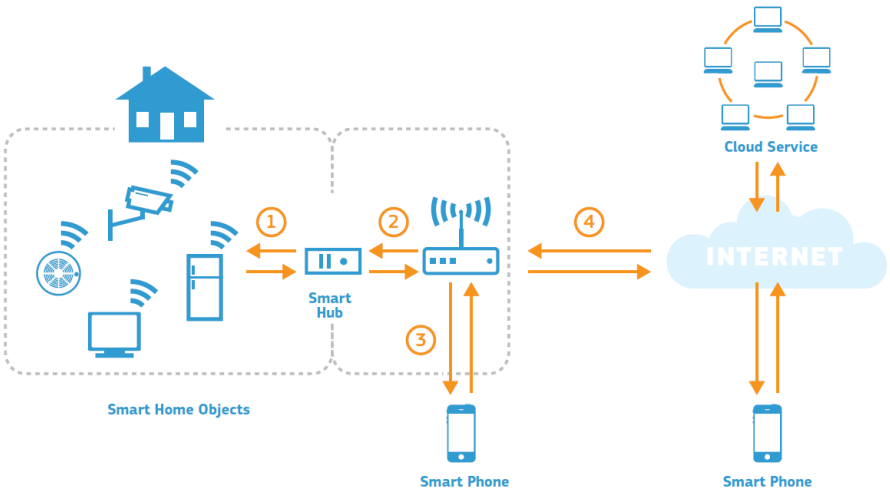


Figure1. Smart home architecture

FIGURE 1. shows the smart home architecture and explain how the devices are connected and controlled by the remote device.

**Vunerablities and Threats in Smart Home System**

Smart Home system rapidly gained popularity as they are cheap, easy to use and easy to install in nature but the IoT Base Smart Home System are vulnerable to cyber threats and hacker can gain access on the devices easily. Security and Privacy related issues are major concern in present Smart Home.

Devices presents in the smart home system are connected in heterogeneous way so the security and maintaining the privacy of each device is quite tough task. If hacker gets the access or control on any one of the connected devices, they can attack the whole smart home network.

Few Security concepts are need to be applied in present Smart home system to mitigate the security threats, privacy issues and vulnerabilities. Smart Home system are vulnerable due to its heterogeneous architecture.

ISSN : 2583-6404
Jul - Aug 2024

**1. Main Vulnerabilities in Smart Home System: -**

Research in discussed that around 85% of the IoT systems are vulnerable to wide range of threats and cyber-attacks. Attacker might exploit the present vulnerabilities and get access to the smart home environment. IoT System have three layers that are application layer, perception layer and last one is network layer. IoT system are vulnerable to attack at each layer. In this section we have discussed about the main vulnerabilities present in Smart Home Systems.

**A. Heterogeneous Architecture: -**

To turn traditional home into smart home we need different smart devices that are connected to each other. Architecture in smart home system is dynamically heterogeneous and it will be built through these three layers which we have discussed above. Smart Home system consists of nodes that have Heterogeneous devices, technology and protocols. Heterogeneous architecture and dynamic environment of smart home comes up with many challenges, IoT manufacturing companies need to figure out new methods to mitigate the challenges.

**B. Obsolete Protocols: -**

Since the Internet is introduced few protocols are not updated by the time and few outdated protocols are still in use and hackers/attackers can compromise them for their evil intentions. In IoT devices security protocols are limited hence the many security and privacy related issues arises.

**C. Poor Encryption: -**

Encryption is a technique to secure the data packets by assigning a key to the packets and only authorized user can decrypt the data packets using the decryption key. this technique helps to prevent attackers to tamper the data during transmission. If any data packet is unencrypted, then the data packets will be tampered easily by the attacker. Furthermore, some of the IoT devices use poor encryption that make these devices vulnerable to the attacks. IoT based smart home system contains delicate information about the owner's daily life. Thus strong encryption key need to be used its very easy and essential method for the security and privacy of the owner.

**D. Using Insecure application: -**

IoT Based smart home system can be controlled by mobile application or web platform. These applications are vulnerable to threats, attacker can easily hack the application and gain access to the devices that are controlled by that application. Using insecure application will lead to major loses.

**E. Weak Authentication Techniques: -**

Authentication is a technique or method having credential that will be used to identify and validate the User s identity in a system. A weak authentication may lead to many security risks. Default credentials need to be changed before using the IoT devices. Main risk of the risk is primarily because of weak authentication process.

**F. Outdated or Failure of Firmware: -**

In Smart home system smart devices face a major problem due to outdated firmware and there is no possibility to upgrade the firmware. Majority the low cost IoT devices that are used in Smart Home system doesn't have method for validating firmware during setup, execution or upgrade. Most of the IoT devices have same firmware that increase the chances of a successful exploitation. Thus firmware became the major problem in IoT devices [22]. As the firmware on an IoT devices is constant and outdated so hacker can easily utilize this vulnerability and perform the attacks to that device.

ISSN : 2583-6404
Jul - Aug 2024

**2. Threats on Smart Home System: -**

Smart Home Systems are vulnerable to active and passive attacks. Hackers can easily attack on any layers of the Smart Home System and gain the access. Most Common attacks are Eavesdropping, distributed denial-of-service (DDoS), Using Malicious software or application. Hacker gain the access easily as the devices use outdated protocols, weak encryption and don't have any authentication system to avoid impersonation. In this section we have discussed the threats on smart home system.

Table 1. IoT Based Smart Home Threats Overview

| **Attack Type** | **Threat/Attack** | **Effect/Impact** | **Target** |
|---|---|---|---|
| Active | Impersonation | Integrity, Availability, unauthorized Access | User and IoT |
| Active | Software exploitation | Integrity, Availability | User and IoT |
| Active | DoS | Availability | IoT |
| Passive | Software exploitation | Privacy | User |
| Passive | Eavesdropping | Confidentiality, Privacy | User and IoT |

TABLE 1. Shows the overview of threats present in smart home system. These threats are most common threats that violate security of the home automation system.

**A. Eavesdropping: -**

In Smart home system devices are connected in heterogeneous way hacker might use different tools and technique to intercept the traffic in between various parts of IoT devices. these methods are mainly depending upon the skills and location of the attacker. If the attacker/hacker is able to use the vulnerabilities of smart home devices and get connected to those devices then he will be able to compromise the security of the network components, hacker will get the access to intercept the traffic between the hub and user. Eavesdropping attack is a passive attack that can be used to target the IoT Device or User and it impacts on the confidentiality and privacy.

**B. DoS Attacks: -**

Denial of Service attack or DoS attack is an active attack that impacts on the availability of the devices. With the help of Eavesdropping attack attacker already knows the IP address of the smart hub so he can easily launch a DoS (denial of service) attack by flooding the targeted system by numerous request to it, these unnecessary requests overload the targeted system and the system will not be able to respond to the legitimate request thus the system will be in an unviability state.

**C. Impersonation: -**

Impersonation is an active attack that impacts on Integrity of the user, availability between user and IoT devices and lead to unauthorized access on IoT devices. In Impersonation attack hacker try to impersonate the authorized owner and acts as an authorized owner to violate the security and privacy. For this purpose, attacker need to obtain the credentials like User name and passwords and it can be easily obtained by social engineering techniques or by capturing the network traffic.

ISSN : 2583-6404
Jul - Aug 2024

**D. Software Exploitation: -**

Software Exploitation can be done by active or passive attack and the attacks impacts on confidentiality of User and IoT devices, integrity, privacy of the user and availability of the IoT devices. Malicious software(Malwares) can easily affect the IoT devices. These malwares are designed to get unauthorized access to private system or network. Since the IoT devices comes up with a lightweight autonomous popular operating system hacker will search for the vulnerabilities present in that operating system and exploit them using these malicious software to get the personal information.

**Suggested Solution for Threats Present in Smart Home Environment**

As the Smart Home System contain private information and it's directly connected to us, so the question arises How far we are safe while using these devices present in the smart home? We can't take security and privacy for granted we must understand the threats using these systems as these devices are vulnerable to cyber threats. Many researchers have suggested some precaution and safety measures to reduce the risk of security breach and violation of Privacy. In this section we have provided the techniques and methods to prevent the threats.

**1. Updating the Software**

We must regularly check for any required updates for the software, firmware and also update the firewall system. Firewall system is the key and basic safety system to prevent the outer threats. it helps to blocks the attacks from the outside. A Firewall acts as a safety wall and a filter between the system interface and the internet. It helps to prevent any malicious software and external threats. Firewall system also detects and issues alerts to the user and invoke strategy to counter that particular threat. Thus its very essential to update the firewall and devices software to avoid vulnerabilities. Outdated Software and firewall have flaws that allows the hacker utilize the vulnerability and intrude to the system. Issues related to security present in smart home system can be fixed by an updated firewall system.

**2. Using Strong Encryption**

As the Smart Home System consists of different components and it's easy to violate any one of them and get the access on the whole home automations system to prevent the threat we can use strong encryption technique and deploy them to each components. Encrypted data communication can prevent the threats on the system and it will reduce the risk of unauthorized access to the system components. By Encrypted Data risk of any security and violation of privacy due to malicious code/attack and unauthorized access will be reduced.

**3. Use of Secure Network**

Using A secure communication network is most popular and effective method to protect and prevent the threats in IoT Device as it prevents unauthorized access. Secure communication network uses secure VPN that will limit the network traffic and will give access only to the authorized users.

**4. Apply Updated Protocols**

IoT devices still use the same protocols and by the time these protocols became outdated hence these protocols are vulnerable and can be compromised easily by the hacker thus It's very important to use updated protocols for protecting the IoT devices. Protocols are the main part in IoT system. Protocols are set of rules that are used for transmission between the devices and that need to establish in a uniform way. IoT manufactories should consider this point as well to ensure the security of the IoT devices.

ISSN : 2583-6404
Jul - Aug 2024

**5. Updating Credential Regularly**

IoT Device manufacturers should make IoT system in such a way that if a User doesn't change the factory-set credentials into difficult credentials; IoT device will not work. By this User will set a unique credential. Password should be regularly changed by the user. User must use different credentials to different devices and avoid the use of same passwords for all. Updating credentials regularly prevent the hackers to guess the credentials hence the system will be hard to intrude.

## Conclusion

In recent years IoT technology and devices gained rapid popularity in traditional home system. Most of the traditional homes are now converted into A Smart Home by adopting IoT technology. Using IoT Technology in the Home System helps to enhance the quality of our lives. However, the Privacy and security related issues are present in the smart home environment. In this survey paper we have discussed about the basic structure, main vulnerabilities, threats and prevention methods. Nowadays new threats are evolving day by day as the attacker uses different techniques to breach the security and privacy so we must apply new methods and techniques and new methods and techniques to counter the threats need to be discovered and deploy to assure the security and maintain the privacy of the User. Our Future work will be based on this analysis and we will try to deploy more security methods and techniques to increase the security and maintain the privacy in IoT Based Smart Home Environment.

## References

1. NetFormation, "8 Best Practices for Security Within the Internet of Things." [Online]. Available:https://www.netformation.com/featured/8-best-practices-for-security within-the-internet-of-things/. [Accessed: 23-Aug-2019].
2. D. Bastos et al., "Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments," In IET Conference: Living in the Internet of Things: Cybersecurity of the IoT – 2018, pp. 30 (7 pp.), 2018.
3. Rambus, "Smart Home: Threats and Countermeasures - Rambus." [Online]. Available: https://www.rambus.com/iot/smart-home/. [Accessed: 23Aug-2019].
4. D. E. Kouicem, et al., "Internet of things security: A top-down survey to cite this version: HAL Id: hal-01780365 Internet of Things Security: a top-down survey," 2018.
5. Y. Lu et al., "Internet of things (IoT) cybersecurity research: A review of current research topics," IEEE Internet Things J., vol. 6, no. 2, pp. 2103–2115, 2019.
6. iot for all, "How Encryption is Powering the Future of IoT | IoT For All," 2018. [Online]. Available: https://www.iotforall.com/future-iot-encryption/. [Accessed: 01-Aug-2019].
7. A. Jacobsson, et al., "A risk analysis of a smart home automation system," Futur. Gener. Comput. Syst., vol. 56, pp. 719–733, 2016.
8. D. Geneiatakis, et al., "Security and privacy issues for an IoT based smart home," 2017 40th Int. Conv. Inf. Commun.Technol. Electron. Microelectron. MIPRO 2017 - Proc., pp. 1292–1297, 2017.
9. W. Paper, "Cyber Security in the Era of Smart Homes," pp. 1–114.
10. G. Corser et al., "IEEE Internet Technology Policy Community White Paper INTERNET OF THINGS ( IOT ) SECURITY BEST PRACTICES," Ieee, no. February, 2017.
11. "LOIC." [Online]. Available: https://sourceforge.net/projects/loic/
12. J. M. Hatfield, "Social engineering in cybersecurity: The evolution of a concept," Comput. Secur., vol. 73, pp. 102–113, 2018.

ISSN : 2583-6404
Jul - Aug 2024

13. N. Nthala et al., “Rethinking Home Network Security,” no. April, 2018.
14. I. Krishna et al., “Intelligent Home Automation System using BitVoicer,” in 11th International Conference on Intelligent Systems and Control (ISCO), 2017, pp. 14–20.
15. R. K. Deore, et al., “Internet of Thing Based Home Appliances Control,” in International Conference on Computational Intelligence and Communication Networks (CICN), 2015, pp. 898–902.
16. Y. Mittal, et al., “A voice-controlled multi-functional Smart Home Automation System,” in Annual IEEE India Conference (INDICON), 2015, pp. 1–6.
17. M.-S. Pan et al., “Intuitive Control on Electric Devices by Smartphone for Smart Home Environments,” IEEE Sensors Journal, 2016, vol. 16, no. 11, pp. 1-14.
18. F. Steps, et al., “How to Develop an IT Security Strategy,” pp. 1–5, 2018.
19. N. Apthorpe et al., “Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic,” 2017.
20. S. Ur Rehman et al., “An approach to secure smart homes in cyber-physical systems/Internet-of-Things,” 2018 5th Int. Conf. Softw. Defin. Syst. SDS 2018, pp. 126–129, 2018.
21. T. M. Secur, “PA R A D I G M.”
22. C. Perera et al., “Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms,” pp. 83–92, 2016.
23. B. Ali et al., “Cyber and physical security vulnerability assessment for IoT-based smart homes,” Sensors (Switzerland), vol. 18, no. 3, pp. 1–17, 2018.
24. A. M. Lonzetta, et al., “Security vulnerabilities in bluetooth technology as used in IoT,” J. Sens. Actuator Networks, vol. 7, no. 3, pp. 1–26, 2018.