International Journal of Innovations & Research Analysis (IJIRA)
ISSN :2583-0295, Impact Factor: 5.449, Volume 03, No. 03(I), July- September, 2023, pp 18-24

SECURITY AND PRIVACY CONCERNS IN SMART HOMES: AN INDIAN PERSPECTIVE

Priyanka Nama*
Prof. Reena Dadheech**

ABSTRACT

The objective of this paper is to introduce Smart Homes, which are intelligent systems that integrate smart devices and sensors to provide management, monitoring, support, and responsive services. Although Smart Homes offer convenience in controlling home appliances, they face security and privacy issues due to the limitations in computing power and the heterogeneous nature of IoT devices. Moreover, the market's focus on product usefulness rather than safety has created numerous security vulnerabilities for Smart Home devices. Users are exposed to serious risks, such as the loss, theft, or misuse of personal data, in exchange for an improved quality of life. This paper aims to summarize the security threats and privacy concerns associated with Smart Homes.

Keywords: *Internet of Things (IoT) Security, Smart Home Security, Security Threats, Vulnerabilities.*

Introduction

The Internet of Things (IoT) is frequently used to refer to a concept that integrates technology and devices for networking. It has become practical as a result of a number of recent advancements in various technologies such as access to low-cost, low-power sensor technology, cloud computing platforms, machine learning and analytics, and artificial intelligence. IoT technology has now been rapidly adopted in the development of smart home systems. The smart home represents [1] smart devices and sensors that are integrated into an intelligent system, offering management, monitoring, support and responsive services and embracing a range of economic, social, health related, emotional, sustainability, and security benefits [2].

The smart home market has grown quickly as communication and network technology have advanced. According to the Statista report [3], the Indian smart home market is expected to generate US$4.87 billion in revenue in 2022 and globally [4] it is expected to grow to US$103.30 billion. Consumers have currently accepted smart home technology to a large extent, and their number is growing quickly. However, the market economy's quick expansion encourages the manufacturing sector to focus on product usefulness rather than product safety, which creates a lot of security vulnerabilities [5] for smart home devices. The trade-off for improved quality of life is that it exposes users to serious risks because personal data can be lost, stolen, or used improperly, leading to a host of issues[6].

Smart Home Technology

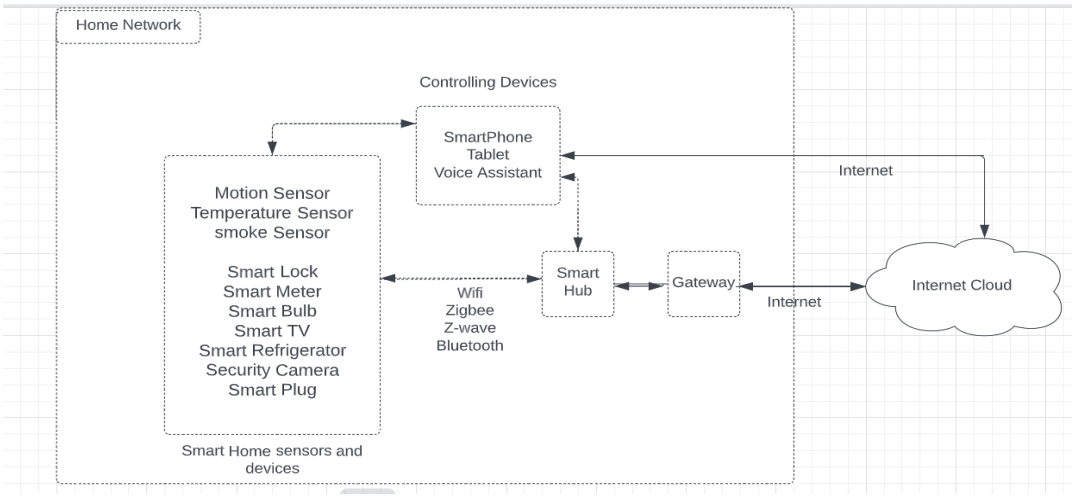
The term "Smart Home" has gained popularity in recent years. Additionally, a variety of other terms, including electronic homes, digital houses, home automation, domotics, connected homes, and others, are used synonymously with the term "smart home." Serving users' needs, enhancing their quality of life, and enhancing home efficiency in terms of energy use, security, and other factors [7] are some of the objectives of Smart Home technology services.

* Government PG College, Bandikui, Dausa, Rajasthan, India.
** University of Kota, Kota, Rajasthan, India.

A smart home is an application of the IoT environment; Smart lighting, smart heaters, smart refrigerators, smart washing machines, smart locks, and smart televisions are IoT-based smart home appliances. Although smart homes are more convenient to use and control all home appliances. However, due to the limitations in computing power and the heterogeneous nature of IoT devices, smart homes [6] are facing different security issues.

The hub and IoT devices often communicate wirelessly using several protocols that vary depending on the manufacturer of the device [8] Some of them are Bluetooth, Wi-fi, Zigbee, Z-wave. In order to link the IoT devices with the outside world, the hub is next connected to the smart home's router by either an Ethernet or a Wi-Fi interface, depending on its capabilities.

Users can control their smart home and connect with IoT devices using PCs, smart phones [9], tablets and voice assistants. There are two main types of interaction: 1) communicating with them directly through the hub's connectivity and services; 2) accessing Internet cloud services that communicate with the hub and the connected IoT devices.



Smart Home Environment

Smart Home Market Segments in India

In recent years, India's smart home market has seen rapid expansion [10]. The country's smart home industry has grown as a result of factors such as increased urbanization, rising disposable incomes, technical improvements, and growing public awareness of energy conservation and home automation. The market, which is still in its infancy, exhibits tremendous growth potential [11] . The smart home market in India can be divided into the following segments:

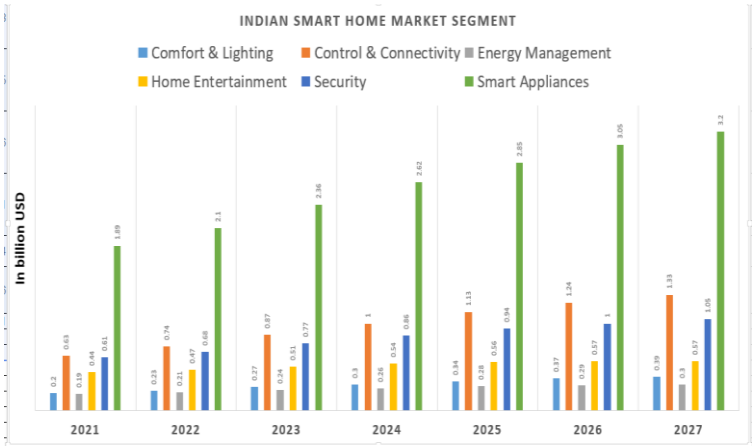


Fig 2: Smart home market growth in India

Source: www.statistica.com

- **Energy Management**

This segment focuses on technological innovations that can monitor and manage household energy use. Users can control their energy consumption and electricity expenses by using technologies like smart thermostats, smart lighting systems, and energy monitoring equipment.

- **Comfort & Lighting**

This section focuses on smart lighting items, such as smart bulbs, switches, and fixtures, which provide capabilities like remote control, scheduling, dimmer control, and colour customization. These solutions enhance energy efficiency and also provide convenience and ambiance control in homes.

- **Home Entertainment**

This market sector consists of smart TVs, streaming devices, home theatre setups, and audio systems that can communicate with and be controlled by other smart devices. These devices frequently offer voice commands, streaming services, multi-room audio, and personalized content recommendations.

- **Control & Connectivity**

The key components of an intelligent home network (hubs, switches, smart speakers, and plugs) are included in the Control & Connectivity category. Smart speakers are the market leader in this sector.

- **Security**

This category comprises smart sensors, video doorbells, smart locks, and smart security cameras that give households improved security and surveillance capabilities. These gadgets frequently have functions like motion detection, remote access, and live video streaming.

- **Smart Appliances**

This market sector consists of intelligent washing machines, refrigerators, air conditioners, and other home appliances that can be managed and operated remotely via smartphone apps or voice assistants.

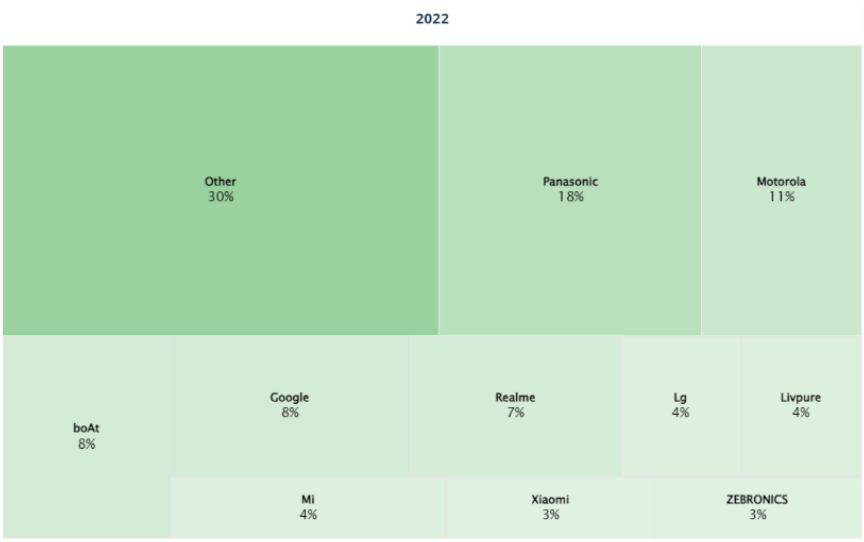


Fig. 3: Smart home market share in India by different companies

(Source:www.statistica.com)

Smart Home Privacy and Security Concerns

Smart Home vulnerabilities are a common fear of consumers. Because of the flaws in the security mechanisms that are already in place, smart technology increases the likelihood of cyber-attacks. Smart home systems include multiple layers [10] that add to the difficulty of security, including device, controller, cloud, and mobile application. Each of these levels uses a separate technology and set of communication protocols, which could result in security flaws, infringements of protocol specifications,

and logical flaws in automation programs, if they are not properly implemented. Security attack is the capacity to exploit the premises' weaknesses and cause a significant loss for the company. Smart home users are exposed to various security risks as new ways have emerged to control and access the information remotely due to internet connectivity of smart home devices. [11]

The research discussed in [12] classifies attacks in four categories- Physical, Network, Software and Encryption. Under the category of physical attacks the hardware of an IoT device or system is attacked such as node tampering, node jamming in wireless sensor networks, malicious node injection, physical damage and malicious code injection. Network attacks launched on the IoT network [13] are traffic analysis, man-in-the-middle, sinkhole, denial of service, stealing routing information, and sybil attack. By using malicious software, such as worms, viruses etc., software attacks exploit the system. Some of the software attacks are phishing attacks, malicious script, denial of service, trojan horse, adware, spyware etc. In Encryption attacks [13], attackers compromise the encryption technology employed by an IoT system. Based on the literature we identified some of the most prevalent security and privacy breaches in Smart home devices. The proposed work sheds light on the security and privacy problems with smart homes and also outlines the solutions for these problems.

Node Tampering

Malicious rootkits are installed once hackers get control of the device nodes. According to [14], when an attacker makes physical changes to the device or the communication link, this is referred to as tampering.

To avoid tampering, devices should be made tamper proof to detect any changes done at the hardware or software level. Units

MITM Attack

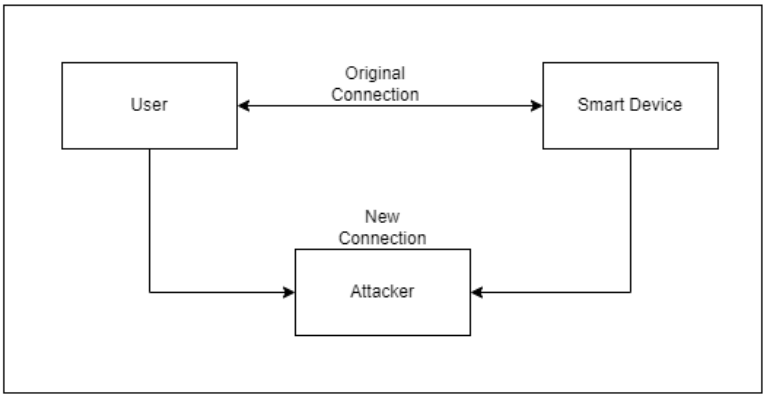
In such types of attacks, the attacker interferes or spoofs the communication between devices. In [15], [16] authors explain how messages are relayed unknowingly between bluetooth devices. In a successful attack, the user believes the pairing was successful; however, this is not the case, as the two devices are paired to the attacker [9].

In the case of WiFi devices [17] after the acquisition of the MitM position, the attacker often intercepts or modifies the Internet traffic (between the client and web server) made possible by the bridged connection.

Eavesdropping

The traffic between the smart hub and the local or remote users can be captured if the attacker is successful in connecting to the smart home network. In that situation, the adversary uses well-known tools to access the data, like tcpdump3, wireshark4, etc.

In such cases, the attacker gets access to a variety of information such as: user device's type, device's status through traffic analysis, smart hub's operating system, methods used for sending commands to hub, unique identifiers for different services offered by [8] smart home devices and many more. Encryption and authorization are possible solutions to avoid this type of security issues[11.



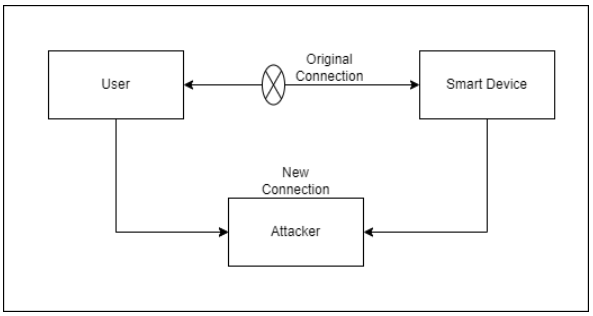


Fig. 4: Eavesdropping

MITM Attack

- **DoS (Denial of Service)**

A DoS attack's main goal is [18] to flood the victim's device with traffic in order to prevent the user from using that device or its services, not to gain unauthorized access or steal sensitive data. Devices like smart cameras, for instance, may be employed for physical security in IoT enabled smart homes.

Attackers may use DoS [18]to disable a camera, clearing the way for physical entrance to a home without leaving behind digital forensic evidence. Authors [19] proposed that network-level security solutions be added to device-level defenses so they can monitor network activity and identify suspicious activity.

- **Malicious Code Injection**

Malicious codes are computer software that harm the internal network of smart homes by taking advantage of its vulnerabilities. Authors in [20] suggested a security framework for smart home devices to provide defense against security threats such as data alteration, malicious code, and information leakage.

- **Impersonation**

Impersonation is a significant security issue in smart homes. Smart homes are equipped with a variety of internet-connected devices that can be controlled through a central hub or mobile application. If an attacker gains access to the smart home's network, they may be able to impersonate the legitimate user and control their devices. There are several ways that attackers can gain access to a smart home's network, including weak passwords, unsecured Wi-Fi networks, and unpatched software vulnerabilities [8].

Attackers who impersonate legitimate users can gain access to sensitive information such as usernames, passwords, credit card information, and other personal data. Additionally, they can take control of smart home devices such as locks, cameras, and thermostats, using them for malicious purposes, such as breaking into the home or conducting surveillance [11].

- **Privacy Violations**

Smart home devices collect and store data, since it is unclear how this data is being stored, who has access to it, and what are the data retention regulations among devices, this raises certain dangers for the privacy of the individual. All of these problems have the potential to cause financial losses, identity theft, and privacy violations. Some of the time this data is sold to third parties.

Another concern for privacy is about collecting browsing or viewing behavior information about users and later using it to customize online advertising. The lack of user choice and control over data collection, storage, and distribution reduces user control and poses privacy risk.

Conclusion and Future Work

The benefits that smart homes bring to its owners also make their houses vulnerable to known attacks. Smart home devices need to handle weaknesses that weren't previously thought of. Due to their limited computing power and reliance on heterogeneous network architectures, these devices increase the attack surface of the service they provide.

In future, we plan to expand our analysis to show in more depth the effects of the various risks on users and the smart home infrastructure. We also plan to present the proper solutions for enhancing smart home security.

References

1. D. Marikyan, S. Papagiannidis, and E. Alamanos, “A systematic review of the smart home literature: A user perspective,” Technol. Forecast. Soc. Change, vol. 138, pp. 139–154, Jan. 2019, doi: 10.1016/j.techfore.2018.08.015.
2. Z. B. Celik, P. McDaniel, and G. Tan, “Soteria: Automated IoT Safety and Security Analysis.” arXiv, May 22, 2018. Accessed: Jul. 30, 2022. [Online]. Available: http://arxiv.org/abs/1805.08876
3. “Smart Home - India | Statista Market Forecast,” Statista. https://www.statista.com/outlook/dmo/smart-home/india (accessed Aug. 07, 2022).
4. R. and Markets, “Global Smart Home Market Report 2022: Rising Investment in Residential Building Construction & Increasing Importance of Smart Home Healthcare Presents Growth Opportunities,” GlobeNewswire News Room, Aug. 09, 2022. https://www.globenewswire.com/news-release/2022/08/09/2494920/28124/en/Global-Smart-Home-Market-Report-2022-Rising-Investment-in-Residential-Building-Construction-Increasing-Importance-of-Smart-Home-Healthcare-Presents-Growth-Opportunities.html (accessed Aug. 15, 2022).
5. F. Loi, A. Sivanathan, H. H. Gharakheili, A. Radford, and V. Sivaraman, “Systematically Evaluating Security and Privacy for Consumer IoT Devices,” in Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, Dallas Texas USA: ACM, Nov. 2017, pp. 1–6. doi: 10.1145/3139937.3139938.
6. H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal, “Smart home security: challenges, issues and solutions at different IoT layers,” J. Supercomput., vol. 77, no. 12, pp. 14053–14089, Dec. 2021, doi: 10.1007/s11227-021-03825-1.
7. W. Li, T. Yigitcanlar, I. Erol, and A. Liu, “Motivations, barriers and risks of smart home adoption: From systematic literature review to conceptual framework,” Energy Res. Soc. Sci., vol. 80, p. 102211, Oct. 2021, doi: 10.1016/j.erss.2021.102211.
8. D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, “Security and privacy issues for an IoT based smart home,” in 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia: IEEE, May 2017, pp. 1292–1297. doi: 10.23919/MIPRO.2017.7973622.
9. E. Fernandes, J. Jung, and A. Prakash, “Security Analysis of Emerging Smart Home Applications,” in 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA: IEEE, May 2016, pp. 636–654. doi: 10.1109/SP.2016.44.
10. C. Vyas and S. Patil, “Smart Home Analysis in India:An IOT Perspective,” Int. J. Comput. Appl., vol. 144, no. 6, pp. 29–33, Jun. 2016, doi: 10.5120/ijca2016910384.
11. S. Chatterjee, A. K. Kar, and M. P. Gupta, “Alignment of IT Authority and Citizens of Proposed Smart Cities in India: System Security and Privacy Perspective,” Glob. J. Flex. Syst. Manag., vol. 19, no. 1, pp. 95–107, Mar. 2018, doi: 10.1007/s40171-017-0173-5.
12. C. K. Nkuba, S. Kim, S. Dietrich, and H. Lee, “Riding the IoT Wave With VFuzz: Discovering Security Flaws in Smart Homes,” IEEE Access, vol. 10, pp. 1775–1789, 2022, doi: 10.1109/ACCESS.2021.3138768.
13. Z. A. Almusaylim and N. Zaman, “A review on smart home present state and challenges: linked to context-awareness internet of things (IoT),” Wirel. Netw., vol. 25, no. 6, pp. 3193–3204, Aug. 2019, doi: 10.1007/s11276-018-1712-5.

I. Andrea, C. Chrysostomou, and G. Hadjichristofi, “Internet of Things: Security vulnerabilities and challenges,” in 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca: IEEE, Jul. 2015, pp. 180–187. doi: 10.1109/ISCC.2015.7405513.

14. B. D. Davis, J. C. Mason, and M. Anwar, “Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study,” IEEE Internet Things J., vol. 7, no. 10, pp. 10102–10110, Oct. 2020, doi: 10.1109/JIOT.2020.2983983.
15. P. Varga, S. Plosz, G. Soos, and C. Hegedus, “Security threats and issues in automation IoT,” in 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), Trondheim, Norway: IEEE, May 2017, pp. 1–6. doi: 10.1109/WFCS.2017.7991968.

A. Lonzetta, P. Cope, J. Campbell, B. Mohd, and T. Hayajneh, “Security Vulnerabilities in Bluetooth Technology as Used in IoT,” J. Sens. Actuator Netw., vol. 7, no. 3, p. 28, Jul. 2018, doi: 10.3390/jsan7030028.

16. T. Melamed, “An active man-in-the-middle attack on bluetooth smart devices,” Int. J. Saf. Secur. Eng., vol. 8, no. 2, pp. 200–211, Feb. 2018, doi: 10.2495/SAFE-V8-N2-200-211.

17. M. Thankappan, H. Rifà-Pous, and C. Garrigues, “Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review,” Expert Syst. Appl., vol. 210, p. 118401, Dec. 2022, doi: 10.1016/j.eswa.2022.118401.

18. E. Anthi, L. Williams, A. Javed, and P. Burnap, “Hardening machine learning denial of service (DoS) defences against adversarial attacks in IoT smart home networks,” Comput. Secur., vol. 108, p. 102352, Sep. 2021, doi: 10.1016/j.cose.2021.102352.

19. V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, “Network-level security and privacy control for smart-home IoT devices,” in 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Abu Dhabi, United Arab Emirates: IEEE, Oct. 2015, pp. 163–167. doi: 10.1109/WiMOB.2015.7347956.

20. W. M. Kang, S. Y. Moon, and J. H. Park, “An enhanced security framework for home appliances in smart home,” Hum.-Centric Comput. Inf. Sci., vol. 7, no. 1, p. 6, Mar. 2017, doi: 10.1186/s13673-017-0087-4.