IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125234

Cyber Security Of Embedded Iot's In Smart Homes: Challenges, Requirements, Countermeasures And Trends

Veena S , V K Bhavyadha

Sri Jagadguru Chandrashekaranatha Swamiji Institute of Technology,Chikkaballapur,India.

Abstract: Connected computers and sensors transmit data across the Internet to solve problems and generate new services (IoT). Smart homes use IoT, for example. Smart home technology can monitor temperature, detect smoke, regulate lighting automatically, and install smart locks. It also poses additional security and privacy problems, such as accessing user data through surveillance equipment or false fire alarms. Smart homes are vulnerable to numerous sorts of assaults. This survey emphasizes IoT. We discuss IoT's design, objects, and standards. We also address the tiered Internet of Things framework and smart home security concerns. In this article, researchers examine IoT-based smart home difficulties and offer solutions.

1. INTRODUCTION

The Internet of Things (IoT) is defined as "An open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data, and resources, reacting and acting in face situations and changes in the environment" IoT is a cutting-edge technology that is changing the way we live. An autonomous smart home is equipped with embedded devices that are designed to detect and respond to a person's presence and needs such as light detection devices, fingerprint readers, gas detection systems, smoke sensors, temperature monitoring devices, motion detection systems, home surveillance cameras, etc. These devices are connected together for many purposes such as saving energy consumption, reducing the bill costs, and security of home occupants Users are using interface devices such as a remote control, computer, or smartphone to manipulate different sensors and devices in these systems. The use of IoT-enabled smart home systems is significantly growing around the world to allow residents to live more comfortably, easily, and smoothly.

According to IoT Analytics' latest reports "In 2021, IoT analytics expects the global number of connected IoT devices to grow by 9% to reach 12.3 billion active end points. By 2025, there will likely be more than 27 billion IoT connections. With this huge increase in the number of connected devices, the spectrum of attack surface increases accordingly, and any security flaws can represent the weakest link thus becoming an attack entry point. Moreover, these devices communicate directly, or indirectly, with each other using several protocols such as Bluetooth, Wi-Fi, Zigbee etc and they are connected to the home internet service. Securing such communications, devices and applications becomes in the past few years an increasingly complex and leading-edge challenge for IoT network designers.

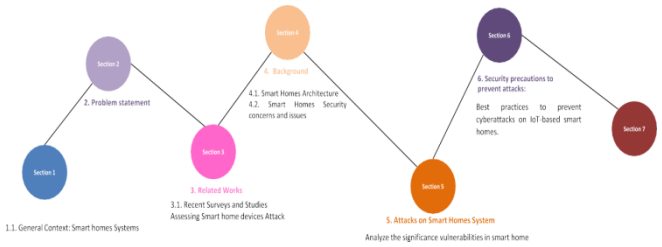

Fig1: Organization of the review paper.

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125234

2. TECHNOLOGY

Several threats result in the unwanted release of sensitive information. For instance, a confidential breach in a smart home system can result in the release of the sensitive medical data of a certain house. Several threats also include unauthorized access to a system controller at an administrator level, which makes the entire system insecure. Moreover, these connected devices have several attack surfaces and could have several vulnerabilities. Many attacks can be carried out remotely, either by direct access to the control interface or by installing malware in the system.

This paper focuses on the main serious cyber-security challenges of IoT devices used in smart connected homes. We will introduce a taxonomy related to vulnerabilities, threats and attacks on IoT devices. Moreover, we will highlight several recommended and countermeasures security solutions that can be used to keep IoT devices, networks, and applications cyber-safe and protect them against cyber-attacks.

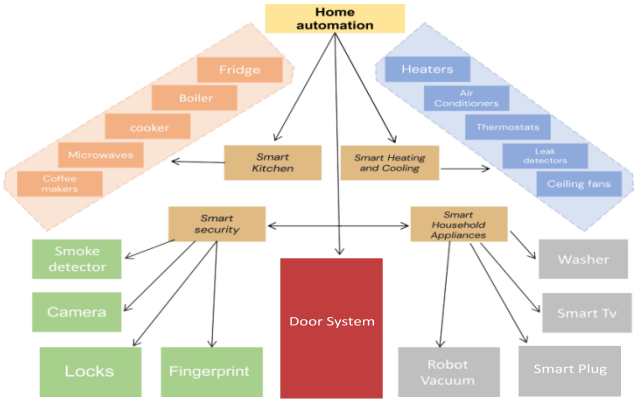

Fig2: Smart home devices communications.

A smart home comprises all the interconnected sensors and appliances and is monitored through one central monitoring end-point, which can be a smartphone, tablet, computer etc. The “things” that can be controlled are doors, locks, air conditioners, devices, thermostats, screens, lights, cameras, and refrigerators. Fig. 2 shows the communications between smart home devices. Frequently, smart home devices are connected online and can be controlled remotely, for instance, using a cloud and/or mobile application. This is extremely convenient for the user and can reduce costs thanks to the scalability of usage, but it can also introduce problems. Typically, users may control and manage the security of these devices using a desktop or mobile application. Users are fearful of hackers who can gain access to private and confidential data such as Health monitoring systems, but also credit card numbers for automatic retailing orders, causing damages by running Air conditioning, and decreasing the temperature of fridges.

The internet has grown a lot during the past few decades and has become a necessity. Berners-Lee played a significant role in the development of the internet and shaping the World Wide Web. According to Berners-Lee, the Internet of Things (IoT) must be open, free, and available to everyone (IoT). With 24 billion devices expected to be online in the public domain by 2025, several security vulnerabilities can lead to a variety of serious problems if they are not properly protected or configured. Different personal information is collected by a variety of connected devices such as name, date of birth, address, credit card information, etc.

3. METHODOLOGY

Smart home devices are convenient to use and relate several advantages for security and safety concerns, they are prone to Cyber security risks Indeed, due to people’s negligence and several device vulnerabilities, various cases provide evidence that intelligent home automation has been hacked on multiple occasions . This raises the risk of concern for Cyber security among individuals that greatly rely on smart home automation.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125234

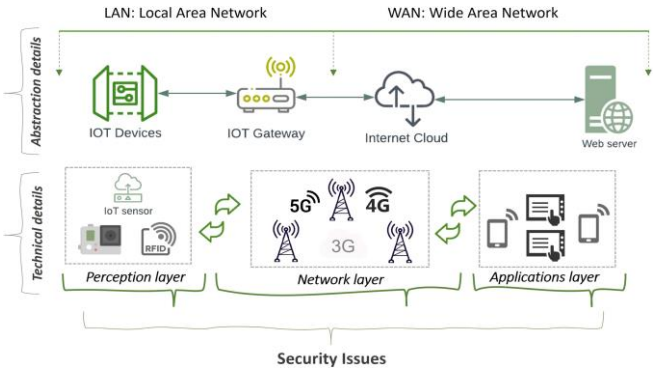

Fig 3: Architecture of IoT system.

It is essential for individuals also to stay concerned about their safety and security processes, mainly towards the relevance of smart home automation [25].

Better assessment of the Cyber security framework, analysis of the threat areas, and better evaluation of the network-based processes need to be processed. Due to the lack of clear user guidance, the poor in-built security measures can be easily hacked, leading to the infiltration of hackers into the security system, and accessing the whole network from the smart home automation system. With respect to the concept of physical attacks targeting smart home devices, it is essential to note that there is a likeliness of vulnerabilities affecting the security of the smart devices. Smart homes are also prone to physical attacks, by tampering with digital wires and installing low-quality sensors. Moreover, while the engagement of the external processes might not be seen as dangerous, the real danger is processed after firing up the gadgets. These issues with physical attacks affect the data integrity due to a lack of control and evidence entertained in the security of the hardware and software systems of the devices.

4. FUTURE SCOPE

The cyber-security of embedded IoTs in smart homes is vast and critical, considering the increasing adoption of smart home devices and the potential risks associated with them. Here are some key aspects to consider regarding the challenges, requirements, countermeasures, and trends in this field:

CHALLENGES:

- **Limited Resources:** IoT devices often have limited computational power, memory, and energy resources, making it difficult to implement robust security mechanisms.
- **Data Privacy:** Smart home devices collect and process sensitive user data, which raises oncerns about privacy and data protection. Ensuring secure data handling and preventing unauthorized access is crucial.

REQUIREMENTS:

- **Data Encryption:** End-to-end encryption should be employed to secure the communication between devices and prevent unauthorized access or data tampering.
- **Secure Firmware Updates**: Implementing a secure and automated firmware update mechanism is crucial to address vulnerabilities promptly and ensure devices are protected against emerging threats.

COUNTERMEASURES:

- **Intrusion Detection and Prevention Systems (IDPS):** Implementing IDPS can help monitor network traffic, detect malicious activities, and block potential threats.
- **Behavioral Analytics:** Employing machine learning algorithms to analyze user behavior and device interactions can help identify anomalies and potential security breaches.

TRENDS:

- **Block chain for Security:** Block chain technology can provide decentralized and tamper-resistant solutions for authentication, secure device management, and data integrity in smart homes.
- **Cloud-based Security Solutions:** Cloud platforms can offer centralized security management, threat intelligence, and real-time monitoring capabilities for smart home environments.

5. CONCLUSION

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.125234

The cyber-security of embedded IoTs in smart homes presents a range of challenges that need to be addressed to ensure the safety and privacy of users. The heterogeneity of devices, limited resources, data privacy concerns, firmware updates, and human factors pose significant obstacles to establishing robust security measures. To meet these challenges, several key requirements must be met. These include implementing strong authentication and authorization mechanisms, employing data encryption for secure communication, establishing a reliable firmware update mechanism, implementing network segmentation, and integrating privacy by design principles.To mitigate the risks associated with cyber threats, various countermeasures can be employed. These include conducting regular vulnerability assessments, implementing intrusion detection and prevention systems, leveraging behavioral analytics, enforcing access control measures, and prioritizing user education. Looking ahead, several trends are shaping the future of cyber-security for embedded IoTs in smart homes. Overall, as technology continues to advance, it is crucial to prioritize the security of embedded IoTs in smart homes. By addressing the challenges, meeting the requirements, implementing effective countermeasures, and keeping up with emerging trends, we can ensure a safer and more secure environment for smart home users.

6. REFRENCES

[1] O. Taiwo, A. E. Ezugwu, O. N. Oyelade, and M. S. Almutairi, "Enhanced intelligent smart home control and security system based on deep learning model," Wireless Commun. Mobile Comput., vol. 2022, Art. no. 9307961.

[2] J. Kim, "Cloud Internet of Things for the smart environment of a smartcity," M.S. thesis, Dept. Inf. and Decision Sci., California State Univ.,San Bernardino, CA, USA, 2021.

[3] P. Mann, N. Tyagi, S. Gautam, and A. Rana, "Classification of various types of attacks in IoT environment," in Proc. 12th Int. Conf. Comput. Intell. Commun. Netw., 2020, pp. 346–35.

[4] G. E. Rodríguez, J. G. Torres, P. Flores, and D. E. Benavides, "Crosssite scripting (XSS) attacks and mitigation: A survey," Comput. Netw., vol. 166, 2020, Art. no. 106960.

[5] E. Džaferovi´c, A. Sokol, A. A. Almisreb, and S. M. Norzeli, "Dos and DDoS vulnerability of IoT: A review," Sustain. Eng. Innov., vol. 1, no. 1, pp. 43–48, 2019.

[6] A. Camphouse and L. Ngalamou, "Securing a connected home," in Proc. IEEE 10th Annu. Ubiquitous Comput. Electron. Mobile Com-mun. Conf., 2019, pp. 0250–0256.

[7] D. Mocrii, Y. Chen, and P. Musilek, "IoT-based smart homes: A review of system architecture, software, communications, privacy and secu-rity," Internet Things, vol. 1, pp. 81–98, 2018.

[8] K. Ghirardello, C. Maple, D. Ng, and P. Kearney, "Cyber security of smart homes: Development of a reference architecture for attack surface analysis," in Proc. Living in the Internet of Things: Cybersecur. IoT, 2018, pp. 1–10.

© IJARCCE This work is licensed under a Creative Commons Attribution 4.0 International License