ACADEMICIA: An International Multidisciplinary Research Journal
ISSN: 2249-7137 Vol. 11, Issue 11, November 2021 SJIF 2021 = 7.492
A peer reviewed journal

AN OVERVIEW OF PRIVACY AND SECURITY OF IOT BASED SMART HOME

Dr. Pavan kumar Singh*

* Faculty of Engineering,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, INDIA
Email id: pavan.engineering@tmu.ac.in
DOI: 10.5958/2249-7137.2021.02548.9

ABSTRACT

The smart home is an environment in which disparate electronic gadgets and appliances are networked together to offer smart services to people in a ubiquitous way. Smart home applications are being accepted and used by a broad range of organizations and individuals. This may be due to the numerous benefits offered by the growing internet of Things (IoT) technologies and gadgets, which are connected with sensors, cameras, or actuators and capable of gathering information from the environment or performing certain activities. Real-time monitoring, remote control, intruder protection, gas/fire alarm, and other amenities are common in smart houses. Because sensitive and personal data is handled in smart homes, security and privacy solutions should be implemented to safeguard users'/businesses' data from unauthorized access while still ensuring the provision of dependable services. The study's results and suggestions add to a wider understanding of consumers' changing attitudes about privacy in smart homes as IoT home devices grow more prevalent.

KEYWORDS: *Internet of Things (IoT), Monitoring, Privacy, Security, Smart Home.*

1. INTRODUCTION

The advancement of information and communication technology in the globalization age is a phenomena that poses a significant challenge to the company's ability to expand and flourish(1). The implementation of a good security system, as well as the availability of many security technologies, both pro and anti, provide a challenge to the development of system vulnerability. In addition, network quality and data transmission medium may have a role in information integrity and availability vulnerability(2). To compete in their individual markets, many businesses continue to change their goods, services, and marketing tactics. In the area of telecommunications services, the business must continue to offer the finest service in order to preserve the company's stability as well as maximize profits. In the future, computers will control human labor and overcome human computing skills such as remote use of electronic equipment, usage of Internet media, and Internet of Things (IoT) (Internet of Things)(3–5).

This enables users to manage and optimize Internet-connected electrical devices. This implies that computers and electrical devices will be able to communicate information via these channels in the near future, eliminating the need for direct human contact. With different Internet facilities and services, this will also boost the number of Internet users. The primary issue in the Internet of Things is to bridge the gap between the physical and digital worlds, such as how to handle

data received from electronic equipment through a user-equipment interface(6). The emerging IoT framework has come up against critical requirements for influencing it to be safe. Many security problems have become a difficulty for the IoT industry. Since the IoT idea was originally proposed in the late 1990s, security experts have warned about the potential danger of huge numbers of unprotected devices connected to the Internet(7–10). A code layer, perception layer, network layer, middleware layer, application layer, and business layer are all part of the Six Layer IoT Architecture. All of these layers can be used in a smart home.

The perception layer, network layer, and applications layer are the three layers that make up the architecture of a typical IoT system. On a wireless network, an attacker may gain access to or infiltrate a smart device(11). The security needs for a secure smart home service, such as integrity, availability, and authentication, are discussed in this research. The goal of the Internet of Objects is to enable things to connect with each other at anytime, anywhere, and with anybody via routes, networks, and services. The Internet of Things is a new Internet revolution. Goods will become readily identifiable, and they will gain intelligence by creating or permitting circumstances that are linked to their ability to convey information about themselves. This coincides with the development of a cloud system or cloud computing that handles constrained capacity by transitioning from the Internet to IPv6(12).

Digital devices can efficiently interact with each other using Internet Protocol (IP) addresses, and IoT smart home services are growing day by day. In a smart home setting, all smart home gadgets are linked to the internet. The risks of malicious assaults rise as the number of devices in the smart home environment grows. Malicious assaults are less likely when smart home gadgets are controlled autonomously. Smart home gadgets may now be accessible over the internet from anywhere at any time. As a result, malicious assaults on these devices are more likely. The service platform, smart devices, home gateway, and home network are the four components of a smart home. Many gadgets are linked in the smart home, and information is shared intelligently through a home network. As a result, there is a home gateway that manages the flow of data between smart devices linked to the internet. The service platform makes advantage of a service provider's offerings to provide various services to the home network(13).

1.1 Security Issues in Smart Homes:

The word "security" refers to the state of not being afraid. Security is concerned with secure communication channels that protect the secrecy, authenticity, and integrity of messages. IoT devices gather and analyze a large quantity of very sensitive personal data. Biometric identity recognition systems, such as fingerprint matching, voice identification, and face recognition, are included in the home security system, as are RFIDs and smart cards, which offer access control to guests. Furthermore, this system incorporates alert systems that prompt quick action. In a Smart Home, a CCTV surveillance mechanism is an essential component of the Home Security system for monitoring and detecting an intruder(14). Finally, this system includes health monitoring for handicapped and elderly individuals, as well as children. Confidentiality, Availability, Integrity, Authentication, Authorization, and Non-repudiation are the seven key security goals of the Smart Home Environment. Confidentiality is a network security feature that prevents unauthorized users from accessing data produced in a smart home environment.

A symmetric cryptographic method may be used to do this(15). The availability of network services and resources indicates that they are accessible and secure against malicious assaults.

Because of its Internet connectivity, the Smart Home internal network is particularly susceptible to direct denial of service (DDOS) assaults (16–20). Integrity is a kind of security service that protects data against unauthorized changes. It ensures that data hasn't been tampered with, deleted, or lost. Integrity, in other terms, guarantees that data is consistent and accurate. Malicious attackers who eavesdrop on communications to or from a Smart Home's internal network may undermine its integrity. Authentication is a security service that confirms an individual's actual identity using a password or secret key given by the communicating parties. Authentication is the process of one entity confirming the identity of another. The process of authorizing someone to do something is known as authorization. It defines the user's network and device access privileges and what they are permitted to perform in the Smart Home environment.

Non-repudiation is a security feature that protects against denial of association in a transaction. Non-repudiation prevents both the sender and the recipient from rejecting a message or access that has been sent. Digital signatures based on public keys may provide non-repudiation.

1.2 Privacy in Smart Homes:

Privacy is a broad word whose meaning varies according to culture, period, and age. Privacy, according to Brandeis, is the right to be left alone. Privacy may also be described as a condition of not being watched or bothered by others. In a nutshell, privacy focuses on safeguarding a user's personal information, which may include a person's identity, location, movements, or any other information about a person (that the individual does not wish to share with others). Sensitive data, such as personal photographs, movies, and digital information, is stored in a smart home. Images and videos may be accessed from anywhere using smart devices that run remotely active IP cameras.

Additionally, feature microphones may be used to listen in on private talks. New gadgets, such as Amazon Alexa and Google Home, are designed to respond to voice instructions. As a result, stringent security measures are required to safeguard private information. There are two major kinds of threats: data privacy and context aware privacy. When it comes to sharing vital information about anything, data privacy is a major issue. Because everything will be linked and accessible through the internet, hackers will have an easy time breaking into the network. The hacker learns everything about a person simply by accessing a portion of the network. Context aware or situational privacy is the second option. Context awareness entails identifying, detecting, and finding users' movements, activities, and behaviors, and then utilizing that knowledge to offer services that the user may find useful. Context Awareness is the capacity to detect and react when the context of a Thing changes, such as when it is relocated to a new place or when the surrounding environment changes. Context aware technology is a valuable tool in the corporate sector, particularly in mobile business, since it offers substantial understanding of the situation or data, but it also raises security risks owing to possible abuse of identity, location, mobility, and behavior. As a result, both security and trust must be thoughtfully handled.

1.3 Existing studies of smart home security:

In today's world of technology, the internet of things is a relatively new concept. The Internet of Things, on the other hand, is expected to be a huge trend in the future. The past efforts relating to security and privacy in the smart home are examined in this part. Applications for security and privacy. Other works are divided into separate groups depending on the security activities and

efficiency in IoT-based smart home systems. These projects are focused on IoT-based security systems and applications for smart homes. Security improvement in smart home systems and apps ,and network system security and privacy control for home intelligence and IoT devices are all examples of secure data management in different devices. Other papers discuss secure healthcare architecture and node communication in a Constrained Application Protocol (CoAP; an application layer protocol prepared for use in Internet devices in IoT smart homes, such as wireless sensor network nodes) network, as well as security challenges between heterogeneous devices and different smart home applications. Password security and applications for IoT smart home systems are the subject of several research. Secure software updates in smart home devices, and security system equipment (such as surveillance cameras) and their usage in smart houses Threats to home automation and security are also defined.

In smart energy management systems, a novel approach is proposed to address risk reduction in instances of privacy breaches. Proposed that radio frequency identification (RFID) tags be used to effectively identify different products within a smart refrigerator. This method may be used to enhance house security, but it necessitates the use of RFID tags on most objects within the home, including the residents, which is unpleasant and difficult to execute given human nature's proclivity for forgetfulness. Proposes a privacy-enhanced security architecture, which is implemented in a smart home context. Personal information hijacking and burst assaults between an attacker and gadgets in a smart home setting are protected by architecture. Encryption, access control, digital signature, authentication, and logging are all included in the study's suggested security architecture for a smart home setting. The suggested framework is built on the open source framework ‘AllJoyn.' Device, AllJoyn Core, permission module, ACLs, and policy certificate trust anchor are all part of it. Critical data is transferred between devices following authentication in the framework. The end-user security manager is in charge of device security provisioning and maintenance(21–23).

For data transfer, a session is created between the apps of devices. A group key and a certificate are used to authenticate the user. Authenticated devices send communications that are encrypted according to a policy. encrypts a message using smart device authentication and a lightweight lattice-based homomorphic cryptosystem. It is split into two phases: setup and reading aggregation. The control center may decode an encrypted message to enhance device secrecy and privacy since the method allows for monitoring authentication between smart devices, control centers, smart meters, and communication between APs. utilizes an encryption technique and a hash function to securely authenticate cellphones and transmit communications in a smart home setting. AES256, ephemeral Diffie-Hellman key exchange, and an RC4-based hash function are used in the method. All messages to transmit are monitored via the usage of a central hub, and messages transmitted by smartphones travel through the central hub for transmission.

A hash value is produced when a message is encrypted using three methods. In 2014, the concept of the Internet of Things evolved in tandem with technological advancements and the incorporation of several technologies, ranging from wireless communication to the Internet, embedded systems to microelectromechanical systems (MEMS), implying that all fields around the world will contribute to the development of the Internet of Things. Although IoT-based smart homes have many advantages, they are vulnerable to a variety of threats. An interconnection device (e.g., gateway) or field device may be directly attacked via its network or local communication interface (i.e., assaulting the device), and a device can be impersonated using its

defective certificate. The home gateway can link household appliances to a wired or wireless network. Because it is the place where an outside connection may be established, an assault on the home gateway can quickly lead to an attack on the whole household network.

2. DISCUSSION

In the Smart Home setting, the security system is a system that may assist security personnel and inhabitants in monitoring the surrounding environment. This aims to reduce the risk of criminal intervention from both outside and inside the environment. The smart home is a branch of ubiquitous and pervasive computing in and of itself. Smart Home introduces automation of home equipment and household helpers, resulting in a more practical quality of life. Automation is based on a context-aware model derived from the outcomes of home environment monitoring. Users may manage their home appliances remotely, such as turning on the air conditioner to chill the room, controlling the water heater for bathing, and so on, while still on their way home. One of the security issues with IoT devices is that the default password cannot be changed simply by the user. In a DDoS attack, this enables a hacker to take control of the device. Mirai is a bundle of malware that was used to control the device. The software's source code was released to the public earlier this month, but the culprits remain unknown. The Mirai virus was originally posted on a hacking forum by a hacker called Anna-senpai. Mirai is said to have infected millions of IoT devices across the globe since then. One worry was that the Mirai botnet will launch another DDoS assault, crippling the internet. Furthermore, since Mirai is difficult to trace, hackers will feel comfortable utilizing it. Girai is a botnet that is especially intended to target Internet-connected IoT devices such as routers, CCTV cameras, and printers. The Mirai botnet can automatically scan a variety of IoT devices. The objective is an IoT device with a shoddy security mechanism, particularly those with usernames and passwords that haven't been updated in a long time.

Even if they are linked to the Internet network, devices infected by Mirai will continue to search for IP addresses from other IoT devices. The private network and IP addresses of various departments in America, as well as some businesses, are among the IP addresses that will not be affected by Mirai. Mirai waited for a command from the hacker to activate the IoT device after successfully locating the target. Mirai will transmit an anonymous data packet to the server that is the target of the assault after it has been started. Although the data packet is tiny, if it is transmitted by hundreds of millions of IoT devices at the same time, it will result in a DDoS assault that will not be stopped. Hundreds of thousands of IoT devices are susceptible to malware since they utilize default settings. The device will connect to the command and control server after being infected, which will display the attack's target. By restarting the machine, the Mirai attack may be avoided. Experts, on the other hand, claim that restarting Mirai did not eliminate it, but simply halted assaults for a short time. Because Mirai can re-deploy his soldiers in a matter of minutes. Changing the default password on IoT devices is another way to prevent Mirai attacks. Mirai's creator claimed that the botnet was created in anticipation of different institutions' increased security awareness. It was blamed on the rising degree of security awareness. A Bricker Bot attack is also included, in addition to Mirai and key installation (KRACKs).

Bricker Bot made headlines a few weeks ago when it was found to be responsible for taking an unprotected IoT device down rather than hijacking it and utilizing it for DDoS assaults, as was

the case with DYN last year. This is the third botnet to target untrustworthy IoT devices, but it is the only one that is malicious. The second, called Hajime, damages IoT devices, but instead of bricking them, it disables internet remote access to them. Mirai is the first, but it has the same aim as previous botnets: to enslave IoT devices and utilize the computing power of the botnet's collection for whatever the threat actors behind it want. While a Bricker bot may not be a mass-adoption worm, it may be a sign of things to come. Because it has greater appeal, ithas all the early signs of becoming very hazardous (much more so than today). There are millions of unprotected devices ready to be hacked, and hundreds of thousands being added to the network every day. Because so many of these gadgets are insecure, they represent a significant threat to the digital economy. Because of their broad deployment, deploying them to participate in assaults like a major DDoS attack last autumn would almost likely put a significant section of the Internet to a halt, disrupting commerce, impairing services, and possibly damaging vital infrastructure.

3. CONCLUSION

Internet of Things (IoT) applications will have a significant impact on human existence. With accelerating innovation, IoT applications will move from a spectacular house to sharp human services. IoT applications are crucial to consider. The general public need innovative, adaptive, flawless, and secure solutions for both the administration of the constantly expanding, unpredictable Internet of Things and the support of various plans of action. Many IoT devices become soft targets due to a lack of security mechanisms, and the victims are unaware that they have been infected. Confidentiality, integrity, and authentication are the security criteria. According to the data survey, there are four kinds of assaults: low-level attacks, medium-level attacks, high-level attacks, and very high-level attacks, as well as their nature/behavior and recommended methods for dealing with these attacks.Given the significance of security in IoT applications, installing security mechanisms in IoT devices and communication networks is critical.

Furthermore, it is advised not to use default passwords for devices and to understand the security requirements for devices before using them for the first time to safeguard against intruders or security threats. Disabling features that aren't in use may help to reduce the risk of security breaches. Furthermore, various security protocols utilized in IoT devices and networks should be studied. IoT devices, particularly smart home and healthcare devices, have gathered, transmitted, and utilized more sensitive data, resulting in increased privacy concerns. New IoT devices and protocols are more likely to include security flaws, necessitating more efforts to address these issues. As previously stated, the main reason of inadequate security configurations and insecure cloud and online services is a lack of security awareness. Furthermore, despite the fact that security research on IoT operating systems and mobile applications has decreased in recent years, owing to the “constrained” and “interdependence” IoT characteristics, more attackers will discover and exploit possible system and application vulnerabilities in the future. These results inspire a number of suggestions for device manufacturers, academics, and industry standards to better match device privacy features to smart homeowner expectations and preferences.

REFERENCES

1. Malik N, Bodwade Y. Literature Review on Home Automation System. IJARCCE. 2017;
2. Sain M, Kang YJ, Lee HJ. Survey on security in Internet of Things: State of the art and challenges. In: International Conference on Advanced Communication Technology, ICACT. 2017.
3. Avizheh S, Doan TT, Liu X, Safavi-Naini R. A secure event logging system for smart homes. In: IoT S and P 2017 - Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, co-located with CCS 2017. 2017.
4. Goswami L, Kaushik MK, Sikka R, Anand V, Prasad Sharma K, Singh Solanki M. IOT Based Fault Detection of Underground Cables through Node MCU Module. In: 2020 International Conference on Computer Science, Engineering and Applications, ICCSEA 2020. 2020.
5. Mathur G, Ghai W, Singh RK. A totalitarian technique for wormhole detection using big data analytics in iot network. Int J Sci Technol Res. 2020;
6. Wlodarczak P, Soar J, Ally M. Context aware computing for ambient assisted living. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2016.
7. Jerabandi M, M Kodabag i M. Internet of Things Based Technology for Smart Home System : A Generic Framework. Int J Recent Innov Trends Comput Commun. 2017;
8. Pandey J, Singh AV, Rana A. Roadmap to Smart Campus based on IoT. In: ICRITO 2020 - IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions). 2020.
9. Hussain I, Pandey N, Singh AV, Negi MC, Rana A. Presenting IoT Security based on Cryptographic Practices in Data Link Layer in Power Generation Sector. In: ICRITO 2020 - IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions). 2020.
10. Shaurya, Som S, Rana A. IoT Based Educational Model for Better Teaching-Learning Environment. In: ICRITO 2020 - IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions). 2020.
11. Newswire PR. Global Internet of Things (IoT) Industry. LON-REPORTBUYER. 2016.
12. Newswire PR. Global Context Aware Computing (CAC) Industry. NY-Reportlinker. 2015.
13. Sandra V. B. Jardim*. The Electronic Health Record and its Contribution to Healthcare Information Systems Interoperability. Procedia Technol. 2013;
14. Committee S. IEEE Standard for Software Verification and Validation IEEE Standard for Software Verification and Validation. IEEEInstitute of Electrical and Electronics Engineers. 1998.
15. Bobaru M, Borges M, d'Amorim M, Păsăreanu CS. NASA formal methods : third international symposium, NFM 2011, Pasadena, CA, USA, April 18-20, 2011 : proceedings.

Proceedings of the Third international conference on NASA Formal methods. 2011.

16. Mishra N, Gupta N, Rana A. Air Quality Monitoring and IoT- Past and Future. In: ICRITO 2020 - IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions). 2020.

17. Abhishekh, Nishad AK. A Novel Ranking Approach to Solving Fully LR-Intuitionistic Fuzzy Transportation Problems. New Math Nat Comput. 2019;

18. Gupta D, Rana A, Tyagi S. A novel representative dataset generation approach for big data using hybrid Cuckoo search. Int J Adv Soft Comput its Appl. 2018;

19. Srivastava R, Sharma PK, Das KJM, Manjhi J. A hybrid approach for head and neck cancer using online image guidance and offline adaptive radiotherapy planning. J Radiother Pract. 2019;

20. Niladry G, Ranjit S. Biogenic synthesis of bimetallic nanoparticles using cassia tora leaf extract. Res J Biotechnol. 2020;

21. Jain UK, Bhatia RK, Rao AR, Singh R, Saxena AK, Sehar I. Design and development of halogenated chalcone derivatives as potential anticancer agents. Trop J Pharm Res. 2014;

22. Kehwar T, Chopra K, Rai D. A unified dose response relationship to predict high dose fractionation response in the lung cancer stereotactic body radiation therapy. J Med Phys. 2017;

23. Ratra S, Naseer A, Kumar U. Design, Docking, ADMET and PASS Prediction Studies of Novel Chromen-4-one Derivatives for Prospective Anti-Cancer Agent. J Pharm Res Int. 2021;