www.revistageintec.net
ISSN: 2237-0722
revista GEINTEC
Gestão, Inovação e Tecnologias

Assessment of Smart Home: Security and Privacy

Akshat Goyal[1]; Mugdha S Kulkarni[2*]

[1]Symbiosis Centre for Information Technology, Symbiosis International (Deemed University), Pune, Maharashtra, India.

[2*]Symbiosis Centre for Information Technology, Symbiosis International (Deemed University), Pune, Maharashtra, India.

[2*]mugdha@scit.edu

Abstract

Home automation is now extremely common in Internet of things services and devices with a range of assurances to improve health, lifestyle, and customer wellbeing. In terms of its success and apparent utility for humans, intelligent homes possess various safety concerns resulting from the diversified, vast-range, and nuanced nature of IoT. Previous studies have talked about security and privacy issues. However, we observe that they have not addressed the risk assessment of each smart home component and corresponding security objective along with additional factors that affect a smart home security posture. In this study, we have proposed a framework defining a standard level of security and then analyzing each component concerning it. There are so many vulnerabilities, but all cannot be assessed due to the heterogeneity of devices and their connection in a small network. IoT can support a wide range of technologies and programs in various domains, including smart cities and smart houses. For monitoring, data exchange, and other operations in the given service, IoT smart objects communicate with other elements such as proxies, mobile devices, and data collectors. While such components help solve various social issues and provide consumers with modern advanced services, their restricted computing capacities render them vulnerable to well-known protection and privacy risks.

Key-words: IoT, Security, Smart Home System, Home Automation, Data Exchange.

1. Introduction

Smart home technology also referred to as home automation, provides house owners with safe, affordability, power conservation, and comfort while encouraging them to monitor homes, usually through a mobile application. In reality, a smart home is a system that provides a mobile application to track it from your smartphone or laptop. It can monitor home appliances such as lights,

Received: 19.07.2021 – Accepted: 18.08.2021

ventilation, air conditioning, smart door doors, etc. Bluetooth or Wi-Fi is used to monitor devices remotely [1]. Smart home emphasizes the automated regulation of home appliances such as intelligent lighting, ventilation, and heating. Although industry strives to manufacture specified goods, such as the thermostat, smart lights, work has tried to understand the wide spectrum of solutions introduced at home. The devices inside the system are configured to the main hub that governs the movement of information among them, controlled and operated by end-user through mobile or web applications [2].

While it is evident that potentially numerous IoT devices and applications seem to be currently active in the smart home market, they usually come into one of the following categories: Entertainment, Monitoring and Safety, Household Maintenance, Lighting, Fitness, and Power & Resource Management. Over the last few years, rapid development or shift has witnessed voice technology adaptation in many computing applications. One of the most significant innovations that use voice technology is Smart Home Personal Assistants (SPA), e.g., Amazon Echo, Google Home, etc. Connected home systems can be categorized into two major categories: remotely operated or locally controlled systems [3]. The local system uses an in-house controller to operatee. A smart home device is interconnected via the Internet, enabling users to monitor operations like home protection, temperature, lighting, etc. Users can install anything in the home that uses electricity on your home network and at your command [4]. It includes various devices that have hit the market that regulate and control all devices such as Zigbee, Z-wave, Lutron, and Wink. So, the design of the Smart local system, the reality is that it is still linked with the external world through the back door by extracting data from homeowners and the Internet, poses a range of security issues. They are systems that integrate most users' digital devices and offer them a portal to control anything. However, generally, they come along with a mobile application, and that you can access them from wherever you want. Present Smart home systems include cloud-based Samsung Smart Things and Amazon AWS, and also several other IoTs. An example, in which a home device sensitizes the surrounding atmosphere and submits the overall collected data directly to the cloud or else from a central hub [5]. The smart house is packed with hundreds of sensors that are doing measurements in conjunction with several other evidence, including smart devices that will be used for customization, automatic services, and enhancing the quality and usability of the occupants. Technically speaking, the smart home model consists of five essential elements: device control, sensors and actuators, network controllers, the controller, and the remote-control devices. A smart home provides various security, childcare, healthcare, eldercare, energy efficiency, and management [6]. However, this smart home model has essential aspects of information protection and privacy.

The unprecedented growth in the number of linked devices has not only provided criminals new access points it also allows more of our knowledge to be captured and eventually exchanged than ever before. Based on many principles and criteria, lots of equipment manufacturers provide a wide variety of devices (meters, actuators, cameras, etc.) embedded in a household setting. The device diversity increased security issues in Smart Homes are directly impacted. Land and consumers and the knowledge they produce are an important portion of the smart house automation environment. As the occupants gradually welcome them, these network structures started attracting more attention from several other business markets [7]. The growing need for these kinds of technologies can be seen from the fact that the worldwide smart home market has been estimated to value nearly $24000 million in 2016. The figure is expected to rise as more and more people begin to adopt smart home technology to the extent of $53500 million by 2020. The following are some key safety criteria when working with protection in IOTs, which are also steps to analyze the performance of multiple protected systems [8].

Confidentiality: This applies to preventing the transmission of data to unauthorized individuals, organizations, and mechanisms.

Integrity: It applies to avoiding falsification and manipulation of data transmitted through the network by unauthorized individuals or devices.

Availability: It aims at ensuring that unauthorized individuals or programs can not restrict authorized users from accessing the network resources.

Authenticity: It involves the conservation of the authentic self of a system user or organization and linking the existing identity to the system-embedded principal to make sure the system acknowledges this user.

Authorization: Authorization is the role of defining access rights/resource privileges relevant to information security and data security in general and access control in particular.

The idea of the “Internet of Things” is no longer a subject of science fiction but an integral part of our life. One of the most common examples of IoT in action includes technologies and applications designed to support devices and Smart house systems [9]. However, the fact that irrespective of smart home design, it will still be linked with the external environment through an internet connection, also the accessible back door protection extracted by the family members, pose a range of security issues, observes Mantas et al. Smart homes face unique challenges in terms of security, safety, and usability because they are multiple users, multiple devices networks, which has an impact on the cognitive experience of most household occupants. Current Smart home hardware is not well configured for many applications, often ignoring simple access control and other ways of

Received: 19.07.2021 – Accepted: 18.08.2021

making the device intelligible and accessible to all applications [10]. To promote the introduction and acceptance of home automation technologies, it is indeed vital to explore the user's view also, the current smart home conditions. There is a significant necessity to reassess the theories and concepts considering the rapid growth rate of studies in this field.

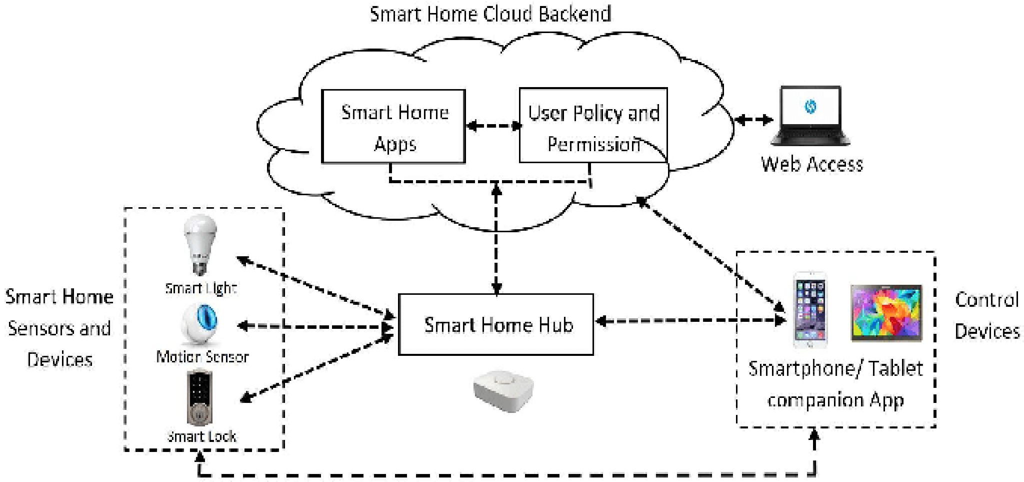
The project discusses privacy and security issues related to smart home systems and their components and segregating them based on Confidentiality, Integrity, Availability, Authenticity, and Authorization, which are also the security objectives of a Smart Home system. Lastly, we will give an overview of the mitigation options that can be implemented for developing a more secure home network [11].

The rest of the paper is structured, as Section 2 will be explaining the objective, Section 3 will be Literature Review. Section 4 is a conceptual model of how a smart home system looks. Section 5 is a research methodology, and Section 6 will be the analysis part, which discusses the conclusion and limitations.

2. Conceptual Model

A smart home environment and its major components are discussed in this section. These layers communicate with each other through signals to carry out operations. The conceptual model reference is taken from [12].

Figure 1 - Smart Home System Elemental Structure



Smart Home Systems, shown in Figure 1, are usually hardware modules composed of cameras, smart objects, gateways, and sensors. The separate one component categories are:

Received: 19.07.2021 – Accepted: 18.08.2021

- **Devices**

Smart Home Systems are usually hardware modules composed of cameras, smart objects, gateways, and sensors. The separate one component categories are:

Sensors: - Tests the electrical characteristics of the atmosphere or the actual object. They may vary from movable like wristbands to immovable, for example, CCTV.

Actuators: - They perform acts like clicking ON/Off, dimming lights, closing gates, warnings, etc.

Gateway: This is a home access point that usually helps owners or other individuals remotely track, operate, and handle home electrical appliances and even detectors. It serves as an integration node to transmit test value with an outside system, like the service providers.

Smart devices:- are networks made up of sensors and/or actuators. They are linked with the smart home web. Examples here involve automated devices like a smart speaker that reacts to the buzzer's sound and delivers access control based on real-time [13].

- **Communication**

Classic smart, wired home uses several protocol connectivity solutions. They range from wired to wireless communication protocols. Sensors typically connect using home security protocols, such as Zigbee, Z-Wave, and WPA2, and networking procedures that include Bluetooth, IEEE 802.15.4/.11ah, Wi-Fi, low-WPAN, also option of mobile technologies. GPS and RFID are also used for tracking purposes.

Smart Hub

Wiring (if applicable)

- **Services**

Services are mobile programs deployed in the cloud or in the home setting responsible for scheduling system services that are mobile programs deployed in the cloud or the home setting responsible for scheduling, system control, decision-making, etc. Usually, households run these applications over their smartphones or tablets to communicate with the computer locally or remotely [14].

Smart Apps

Web access

3. Objective

The core objective behind conducting research is to give an overview of the privacy and security issues in the IoT-based Smart home system. Due to vulnerabilities of the existing smart home systems and the multiple attacks on these systems, we have challenged security [15]. Therefore, the security of these systems is an important issue that requires analysis. The major emphasis is on highlighting the security vulnerability and risks distributed among major portions, like human-related, network, hardware, software, and information. It is accompanied by finding out the most and least vulnerable components installed within the house setting based on types of attack, likelihood, and risk score [16]. Also, keeping into consideration internal and external factors, The research would be useful for manufacturers of home automation devices, components, and reviewers and to develop a more secured smart system based on the risk assessment carried out. From the end-user and provider perspective, it will be useful as they know what factors affect smart home security and make them aware and, in turn, increase overall security posture [17].

4. Literature Review

Research attempts have been made to analyze vulnerabilities in IoT products in a smart home setting, where security issues are addressed and attack classifications are identified. Homes are the areas where secrecy is supposed to be preserved. IoT (Internet of things) has emerged as a reliable technology to enhance the lives in today’s digital homes by offering a variety of automated, interactive, and convenient services. However, maintaining safety and adequate protection for these necessary IOT offered services are key problems within a smart home setting [18]. A study by Bugeja et al. also speaks similarly that IoT services and devices are becoming widely attractive among smart homes, including many attempts to raise the standard of living of individuals. However, the stratified, complex, and web-related complexity for such space raises additional issues since personal information is obtainable, often without the knowledge of the householder. However, the privacy and protection need of vital technical infrastructure plus any important commercial activities turn out to be somewhat distinct from the demands of the domestic Smart Home community, observed Lin & Bergmann [19]. Another study states that homes are especially vulnerable to malware and data breaches at the highest degree of smartness. So, paradoxically, the better digital a house becomes, the more defenseless you get to be. Recent technology professionals speak on how only basic appliances, e.g., coffee machines, can also be an intruder's gateway to the whole house, which provides

Received: 19.07.2021 – Accepted: 18.08.2021

vulnerable digital underbelly, which criminals might manipulate. IoT's core deployment area is a home, an integrated place, where many things connect through the Internet. Hence, according to a study, this fast-technical development of IoT poses ample threats [20]. For example, in what way smart home users can get reliable utilities to maintain their account and privacy and a way to operate their houses effectively beneath managed conditions and quite enough confidentiality and prevent abuse of sensitive information.

The emergence of smart gadgets, which systematically gathers classified data, becomes evident mostly because of the expansion of everyday activities. In addition to that, a study says that insufficient protection protocols and specialized outlier analysis mechanisms systems are sometimes present [21]. Such a diverse system renders it susceptible to various threats like information theft, unknown connection, service disturbance, power wastage, and unsafe portals. Another study states that with a wide range of electronic devices and sensors, smart homes can be installed, controlled from remote areas, making it impossible for the average person to uphold safety levels. Since smart devices are connected to the Internet, the vectors used by attackers are increasing significantly [22]. It also makes it more difficult for forensic analysts to use the tool and appoint the person. The development and implementation of complex, linked operating domains, such as intelligent public transport, buildings, and cities, are on the rise [23]. The complexity of the threat area of automated homes is increasingly growing. Many vulnerable bugs got added, setting a stage for a not so stable dangerous environment.

[24] In a study, the author has attempted to present the definition of smart home system, the term privacy and security in perspective of smart home, security, vulnerabilities area, and existing security initiatives to counter these security and privacy threats [25]. The diversity of IoT devices has been the most critical problem to discuss on a high-priority basis. The product comes with various networking requirements, and different app update features often come from different manufacturers. A study describes and addresses the threat that those might influence the organization classifying them into an external threat as well as internal in order to address the issue that since home automation is a section of everyday lives, many folks wish they can keep a check on his/her residence by just tapping on mobile but are afraid to risk anonymity or personal details that may lead to a lack of protection or even financial loss [26].

A further study says IOT is also perceived as a common issue area, accompanied by potential approaches to be implemented through applications of a broad variety. However, the online security requirements for essential technical systems and important business activities were somewhat distinct in the smart house of a traditional setting. The first time IoT was created, security was just an afterthought [27]. However, this is no longer appropriate due to the high demand for IoT devices in consumer homes. Attacks on IoT systems may occur with or without human intervention, like the Mirai botnet. Ann effective IoT attack can also result in significant financial, reputational, and, worse, life-threatening losses to customers. A study states that security is crucial to the proper development and implementation of home automation systems. It also gives the inhabitants of a home a sense of security and puts their minds at ease. As it is now, much vulnerability exploits the smart home network, but no strong defensive mechanism has yet been developed [28]. One more recent study states that multi-user smart homes face particular protection and privacy issues, such as supporting a wide variety of access control priorities and handling consumer pressures and disputes. Smart homes face particular problems in terms of protection, privacy, and accessibility, as they are multi-user, multi-device networks, which have an impact on all individuals in general experience living in the house, but unfortunately, modern smart homes are not yet intelligently built for connectivity with and use by several users [29]. A similar study shows that risk quantification for smart homes is difficult because of its diverse environment with wired devices, appliances, and networks. Its design poses multiple safety concerns as well as vulnerabilities in a suburban neighborhood. It is, therefore, necessary to control the risks to smart homes. They also find out that many of the in-store apps had an extra benefit or rights because of their ability to behave as a complex system. Furthermore, after the application has been enabled, complete access to the device is given to the Smart App. It states that only partial access to the device is necessary [30].

A further study states that cybercrime and information security challenges are far closer to the reality of wired home environments than has ever been anticipated. Much of the work initiative focuses on the protection systems of collaboration and essential services. Failing to recognize a few out of several delicate ties within the system emerges because of smart equipment wired today and the future. A study depicts that because of the absence of a safety procedure for smart components, most of which are easy preys; however, it is not in the subject's experience about being compromised. Considering the significance of protection among smart devices, a prevention methodology based on smart devices and wireless connections is necessary. Also, while safeguarding against hackers or network attacks, it is quite often advised that the device's original or out-of-box password should not be used and read the device's security specifications before using them for the first time. Another study states that even if the Internet of Things delivers enormous benefits, it is prone to various security threats in our everyday lives. The bulk of vulnerabilities were linked to the disclosure of data and disruption in businesses. Cyber-attacks in IoT devices directly affect the risk of general security. Applying IOT technologies to smart homes creates both opportunities and security risks. Homes integrated with the Internet of things smart homes seem particularly unsafe for a range of security hazards in and around the house. In case the protection of the home or device got breached. The security, private details, in addition to the protection of the user, will be at risk.

Necessary steps must be followed to move towards safer homes and all the more acceptable for living inside. Supporting the research with a study that shows why smart home security is the new challenge is quite evident. In the current situation, the use of IoT & its support technologies and strategies for deployment in a smart home is one of several major fields, wherein a lot of major corporations like Google, Amazon, etc., are spending a quite great deal of money also initiated work for enhancing security and health at home. A recent study shows that, up to date, the risk analyses of IoT systems were not all-included. However, in certain instances, include best-known products or vendors. Recent tests have shown IoT devices are quite prone to several cryptographic, system, network and physical, network attacks. At present, there are no health standards for IoT devices. Therefore, the consequence is that safety defects are found during usage, which ensures IoT health hazards are not well understood or investigated. Vulnerability checks are conducted to assess if IoT applications can be abused. It is crucial for security vulnerabilities experiments to be well-rounded across all areas of attack vectors.

5. Research Methodology

The research question identified for this paper is an addition to the existing research. It adds to more knowledge about the associated security issues related to a smart home.

Q1. Are the current smart home environment security problems and privacy issues well addressed?

Q2. Do the smart home system components meet or fulfill the proposed security standards?

Systematic Literature Review has been carried out in conjunction with current exploration to address research questions. The intention is to start by phases of the organizing, implementation, and documentation of the evaluation to support the execution of the literature review.

5.1. Selection of Primary Studies

Key findings have been outlined by entering tags for a particular journal or web search service. Relevant keywords are chosen along with conditional 'and' and 'or' operators to help find better results. So, the threads in the sample were:

("Smart home" or "Home automation") AND ("Security" OR "Cybersecurity").

5.2. Inclusion and Exclusion Criteria

Studies to be included in this SLR report empirical findings and could be papers on Smart home security, privacy and security issues of IoT-based smart home, challenges implementing smart home. **The inclusion criteria were:** English Paper, Paper having relevant information related to smart home, smart home cybersecurity. **The exclusion criteria were:** Non-English paper, a paper that is unclear and duplicate, paper related to the connection between a smart home and a smart city.

5.3. Selection Results

The original searches for the selected keyword for the topic identified 90 articles, conference papers, and chapters. Upon elimination of redundant findings, this was limited to 70**.** From remaining, the articles left to be read upon applying inclusion/exclusion criteria were 50 with the review, a risk assessment/analysis is also going to be carried out that will contain Risk, Vulnerability, Threat vector, Impact, risk score under which security requirement (Confidentiality, Integrity, Availability, Authenticity, Authorization) the risk identified will fall in the defined security requirements needed for the securing functioning of a smart home are used later during risk assessment part so that we can group which risks impact which requirement.

6. Data Interpretation and Analysis

The smart home concept is modeled on convenience by connectivity and the automation of efficiency processes. When homeowners choose the idea of clever home, they must also be aware of the threats posed by the clever home as cybercriminals trawl the Internet and build hacks directed at a clever property. In response, the desired intelligent homeowner must take a security measure. Smart home protection will begin with understanding and take the appropriate measures to protect your home network's integrity.

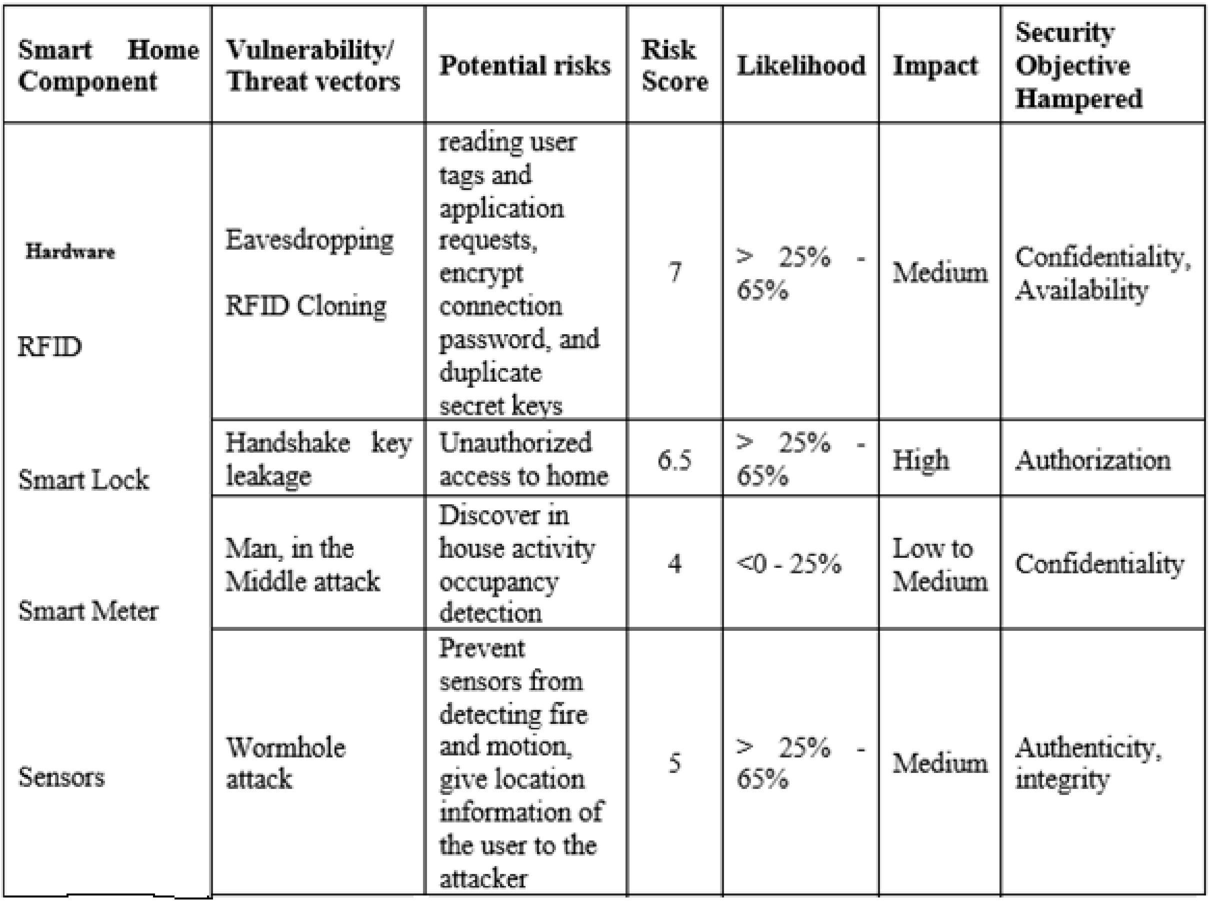
Potential security risks include eavesdropping, Distributed Denial of Service (DDoS) attack, data spill, etc. Home automation is also under threat of unauthorized access.

To fulfill the research question goals, we agreed to develop a risk evaluation methodology to perform a risk assessment for crucial components of smart home systems probably to be the target of attacks. The below risk evaluation reference table is created based on the data acquired from an institute risk analysis and management framework. It is then customized according to the project need. The scale selected here is a three-scale factor for the ease of doing risk assessment is shown in Table 1.

Table 1 - Range of Risk Assessment Factors

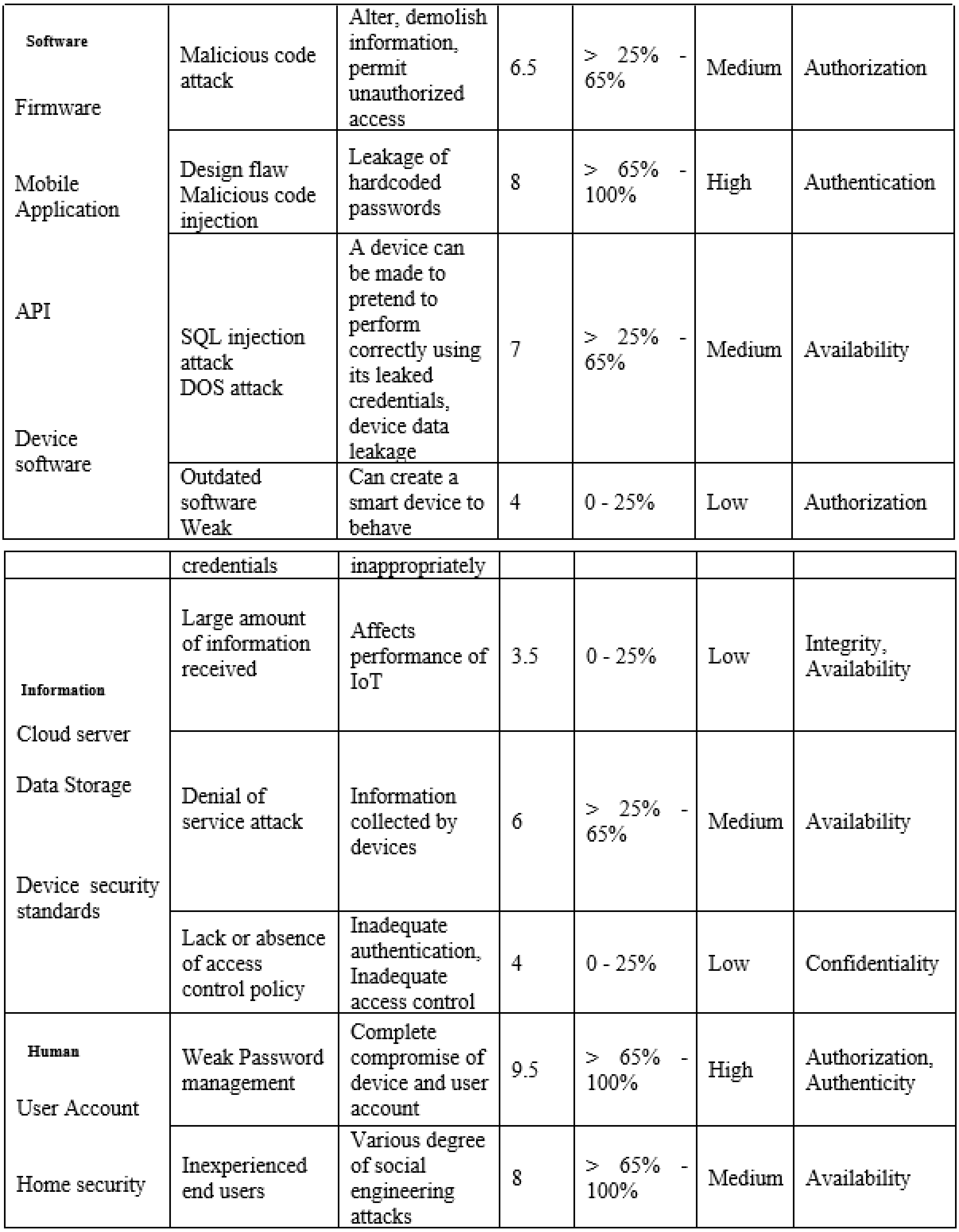
Risks Score	**Impact**	**Likelihood**
7.5<Score<=10	High	> 65% - 100%
4<Score<=7.5	Medium	> 25% - 65%
1<Score<=4	Low	0 - 25%

Table 2 - A Risk Assessment Matrix Describing Component Vulnerabilities/Threat Vector Together with their Likelihood, Potential Risk, Risk Score, Security Objective, and Impact



Smart Home Component	**Vulnerability/ Threat vectors**	**Potential risks**	**Risk Score**	**Likelihood**	**Impact**	**Security Objective Hampered**
Hardware RFID	Eavesdropping RFID Cloning	reading user tags and application requests, encrypt connection password, and duplicate secret keys	7	> 25% - 65%	Medium	Confidentiality, Availability
Smart Lock	Handshake key leakage	Unauthorized access to home	6.5	> 25% - 65%	High	Authorization
Smart Meter	Man, in the Middle attack	Discover in house activity occupancy detection	4	<0 - 25%	Low to Medium	Confidentiality
Sensors	Wormhole attack	Prevent sensors from detecting fire and motion, give location information of the user to the attacker	5	> 25% - 65%	Medium	Authenticity, integrity

Smart Appliances	Port scanning Device hardware exploitation	Leakage of personal information into hands of attackers, Malfunctioning results in fire or monitoring.	3.5	<0 - 25%	Low	Confidentiality
Smart hub	Man, in the middle attack	Full access to central and peripheral devices, creation of SSH backdoor	5	> 25% - 65%	Medium	Confidentiality, Authorization
Biometrics	Sensor output interception	Captured sample is replayed and falsely accepts by the individual.	6.5	> 25% - 65%	Medium	Authenticity
Network Wi-Fi Telnet Smart home server WSN Gateway	Duplicating access point Replay attack	Smart home devices password leakage leading to a cyber-attack.	9	> 65% - 100%	High	Integrity
	Dictionary attack	Credentials could be used to connect and use smart devices as a botnet.	5.5	> 25% - 65%	Medium	Authentication
	Denial of Service attack	User unable to use the home network service	8	> 65% - 100%	High	Availability
	Eavesdropping	Access to sensitive information flowing between two devices	3.5	<0 - 25%	Low	Confidentiality
	Inadequate physical security	Impersonation of the device can happen by using just its compromised certificate, Home network under attack	5.5	> 25% - 65%	Medium	Integrity



Software Firmware Mobile Application API Device software	Malicious code attack	Alter, demolish information, permit unauthorized access	6.5	> 25% - 65%	Medium	Authorization
	Design flaw Malicious code injection	Leakage of hardcoded passwords	8	> 65% - 100%	High	Authentication
	SQL injection attack DOS attack	A device can be made to pretend to perform correctly using its leaked credentials, device data leakage	7	> 25% - 65%	Medium	Availability
	Outdated software Weak credentials	Can create a smart device to behave inappropriately	4	0 - 25%	Low	Authorization
Information Cloud server Data Storage Device security standards	Large amount of information received	Affects performance of IoT	3.5	0 - 25%	Low	Integrity, Availability
	Denial of service attack	Information collected by devices	6	> 25% - 65%	Medium	Availability
	Lack or absence of access control policy	Inadequate authentication, Inadequate access control	4	0 - 25%	Low	Confidentiality
Human User Account Home security	Weak Password management	Complete compromise of device and user account	9.5	> 65% - 100%	High	Authorization, Authenticity
	Inexperienced end users	Various degree of social engineering attacks	8	> 65% - 100%	Medium	Availability

NOTE: Smart lock is an exception; the impact is high because if attacked, the whole smart home system and users are compromised.

Along with the identified risks and vulnerabilities of the components in Table 2, some factors are unintentional or say, not technical/network-related, that also affects smart home security. In Table

3, some identified factors are listed out, followed by dividing them into internal, related to the device, and external, which are non-device related or actions happening outside a smart home.

Table 3 - Internal and External Factors Affecting Security Posture of Smart Home System

Internal factors	**External factors**
Constrained System resources	Lack of dedicated professionals
Failure of home devices	Moderate intake of quality standards
Power and internet malfunction	Time analysis

Talking about Internal Factors

Constrained System Resources – It is still a challenge for IoT device manufacturers to design comprehensive security measures within a constraint available memory.

Failure of Home Device – It is a situation that is unintentional and can make a device vulnerable to security attack. These happen either because of poor design flow or software failure.

Power and Internet Malfunction – A malfunction in power can also affect device security. Most IoT devices are low-powered ones; therefore, a surge could damage the device. Also, an internet malfunction can create a barrier between consumers and their connected devices.

External Factors

Lack of Dedicated Professionals – It is noted that there is a lack of professional assistance in the concept or service phases of IoT implementation in the Smart Home system. An improvement can greatly reduce security vulnerabilities.

Slow Uptake of Standards – This problem is the lack of uniform standards and appropriate certificates by manufacturers and providers, resulting in low-quality products. As a result, security is compromised.

Time Analysis – It is a side-channel attack that might not be active, but instead just watching and analyzing just how much time various computations take to perform. This factor is crucial because it happens even if the data is encrypted.

7. Results and Discussion

The serious challenges in a smart world are mainly security and privacy. Smart computers/devices are quite vulnerable to attacks, resulting in data loss and identity breaches.

Received: 19.07.2021 – Accepted: 18.08.2021

Due to the lack of security mechanisms in IoT devices, many become soft targets and even without being in victim's knowledge of getting infected. We made an effort in this paper to deliver a Risk evaluation for smart connected home surroundings constructed on IoT. Major emphasis is on highlighting the privacy, security vulnerability, risks distributed among major portions like human-related, network, hardware, software, and information. Issues discussed were in context with security and privacy objective, which is CIA triad and authorization and authenticity. For risk assessment, a framework created with the help of reference form is proposed, in which we have defined that the expected level of security for any component is 60%, which is 6 in our case, as our risk score ranges from 0 to 10, which helped us in finding out which are the least and most vulnerable components as risk score above 6 is more vulnerable and below is less vulnerable. Here, the concept of risk appetite comes into the picture, which we have integrated into our study based on the results are drawn. Coming to the hardware-related vulnerabilities, the least vulnerable are smart appliances, and one more is RFID. In network, less vulnerable is WSN, and more vulnerable is Wi-Fi. In software, the less vulnerable is Device software, and the more vulnerable one is Mobile application. Coming to information, less vulnerable is cloud server and more is data storage, including physical storage in memory cards, etc. In human-related cases, most of the security cases occur due to poor password management. The study helps in carefully addressing the security issues of each home automation component; also mentioning which security objective is breached along with identified external and internal factors that affect the smart home security. Through the proposed framework, we learned that most of the components meet the defined expected level of security. It is because of design flaws, low memory constraints, heterogeneity of sensors, appliances, and networks. It shows that the proposed method can help the manufacturers and providers develop a more secure smart home environment.

8. Conclusion

The topic of cybersecurity is much more closely related to the Smart Home Environment than is commonly assumed. People have been producing a large volume of personal data due to the increased use of smart devices, posing a significant privacy danger, particularly as this data is stored in small smart devices that are more vulnerable to privacy, mostly achieved without the user's understanding. Third parties gather and store any of this data, and in some situations, this is achieved without the user's permission. It is also crucial to consider the data after it has been obtained from the end-user. The result would remain the same if the data were stolen from an unreliable machine or

Received: 19.07.2021 – Accepted: 18.08.2021

computer. The user was duped into giving more data than he wanted. The sourced data will be repurposed or distributed to third parties by the organizations that collected it. The customer has little influence of it, and in some cases, no knowledge of it. Every safeguard taken by the recipient will only restrict the amount of data gathered. Smart device manufacturers and interface designers must resolve these concerns in order to ensure adequate protection and privacy.

9. Limitations and Future Scope

When we transition into the next generation, more and more devices will continue to connect. For future scope in smart home security, we should seek to view the local network as a whole and create a framework that can quickly detect the intruder and his actions during the attack. This paper presents opportunities for potential research work in this area. There is also the scope of examination of security of components with other devices, such as remote access from a far location and social impact of smart home security. Artificial intelligence can greatly improve smart home security and also blockchain.

References

Abdur, M., Habib, S., Ali, M., & Ullah, S. (2017). Security Issues in the Internet of Things (IoT): A Comprehensive Study. *International Journal of Advanced Computer Science and Applications*, *8*(6).

Alam, T., A. Salem, A., O. Alsharif, A., & M. Alhejaili, A. (2020). Smart home automation towards the development of smart cities. *Computer Science and Information Technologies*, *1*(1), 17–25. https://doi.org/10.11591/csit.v1i1.p17-25

Ali, B., & Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors (Switzerland)*, *18*(3), 1–17.

Almusaylim, Z. A., & Zaman, N. (2019). A review on smart home present state and challenges: linked to context-awareness Internet of things (IoT). *Wireless Networks*, *25*(6), 3193–3204.

Anthi, E., Williams, L., Slowinska, M., Theodorakopoulos, G., & Burnap, P. (2019). A Supervised Intrusion Detection System for Smart Home IoT Devices. *IEEE Internet of Things Journal*, *6*(5), 9042–9053.

Banham, R. (2017). *Cyber Scorekeepers*. Rmmagazine. http://www.rmmagazine.com/2017/11/01/cyber-scorekeepers/

Batalla, J. M., Vasilakos, A., & Gajewski, M. (2017). Secure Smart Homes: Opportunities and challenges. *ACM Computing Surveys*, *50*(5).

Bugeja, J., Jacobsson, A., & Davidsson, P. (2016). On Privacy and Security in Smart Homes. *2016 European Intelligence and Security Informatics Conference (EISIC)*, 172–175.

Received: 19.07.2021 – Accepted: 18.08.2021

Davis, B. D., Mason, J. C., & Anwar, M. (2020). Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study. *IEEE Internet of Things Journal*, *4662*(c), 1–1.

Desai, D., & Upadhyay, H. (2014). Security and Privacy Consideration for Internet of Things in Smart Home Environments. *International Journal of Engineering Research and Development*, *10*(11), 73–83.

Doan, T. T., Safavi-Naini, R., Li, S., Avizheh, S., Muni Venkateswarlu, K., & Fong, P. W. L. (2018). Towards a resilient smart home. *IoT S and P 2018 - Proceedings of the 2018 Workshop on IoT Security and Privacy, Part of SIGCOMM 2018*, 15–21.

Edu, J. S., Such, J. M., & Suarez-Tangil, G. (2019). *Smart Home Personal Assistants: A Security and Privacy Review*. http://arxiv.org/abs/1903.05593

Gadiyar, H. M. T., Thyagaraju, G. S., Bhavya, T. P., & Ahana, R. (2018). *Privacy and Security issues in IoT-based Smart Home Applications*. *6*(15), 6–8.

J. Sturgess, J. R. C. Nurse, and J. Z. (2018). Kent Academic Repository Movement. *A Capability-Oriented Approach to Assessing Privacy Risk in Smart Home Ecosystems*, *47*, 459–469. https://kar.kent.ac.uk/69955/

Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems*, *56*, 719–733.

Karimi, K., & Krit, S. (2019). Smart home-smartphone systems: Threats, security requirements and open research challenges. *Proceedings of 2019 International Conference of Computer Science and Renewable Energies, ICCSRE 2019*, 1–5.

Kavallieratos, G., Chowdhury, N., Katsikas, S., Gkioulos, V., & Wolthusen, S. (2019). Threat Analysis for Smart Homes. *Future Internet*, *11*(10), 207.

Lamba, A., Singh, S., Dutta, N., & Muni, S. S. R. (2019). Uses of Different Cyber Security Service to Prevent Attack on Smart Home Infrastructure. *SSRN Electronic Journal*, *1*(11), 5809–5813.

Lavanya, N and Malarvizhi, T. (2008). Risk analysis and management a vital key to effective project management. *PMI Global Congress Proceedings*.

Lin, H., & Bergmann, N. W. (2016). IoT privacy and security challenges for smart home environments. *Information (Switzerland)*, *7*(3).

Mantas, G., Lymberopoulos, D., & Komninos, N. (2010). Security in a smart home environment. *Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications*, 170–191. https://doi.org/10.4018/978-1-61520-805-0.ch010

Nagarkar, S. (2019). Evaluating Privacy and Security Threats in IoT- based Smart Home Environment. *International Journal of Applied Engineering Research*, *14*(7), 75–78.

Philomin, S., Singh, A., Ikuesan, A., & Venter, H. (2020). Digital forensic readiness framework for smart homes. *Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020*, 627–636.

Ray, A. K., & Bagwari, A. (2018). Study of smart home communication protocols and security & privacy aspects. *Proceedings - 7th International Conference on Communication Systems and Network Technologies, CSNT 2017*, 240–245.

Saxena, U., Sodhi, J. S., & Singh, Y. (2017). Analysis of security attacks in a smart home network. *Proceedings of the 7th International Conference Confluence 2017 on Cloud Computing, Data Science and Engineering*, 431–436.

Shouran, Z., Ashari, A., & Kuntoro, T. (2019). Internet of Things (IoT) of Smart Home: Privacy and Security. *International Journal of Computer Applications*, *182*(39), 3–8.

Sikder, A. K., Babun, L., Aksu, H., & Uluagac, A. S. (2019). AEGIS: A Context-aware Security Framework for Smart Home Systems. *ACM International Conference Proceeding Series*, 28–41.

Sovacool, B. K., & Furszyfer Del Rio, D. D. (2020). Smart home technologies in Europe: A critical review of concepts, benefits, risks, and policies. *Renewable and Sustainable Energy Reviews*, *120*(May 2019), 109663.

Wongvises, C., Khurat, A., Fall, D., & Kashihara, S. (2017). Fault tree analysis-based risk quantification of smart homes. *Proceeding of 2017 2nd International Conference on Information Technology, INCIT 2017*, *2018-Janua*, 1–6.

Zeng, E., & Roesner, F. (2019). Understanding and improving security and privacy in multi-user smart homes: A design exploration and in-home user study. *Proceedings of the 28th USENIX Security Symposium*, 159–176.