ZANCO Journal of Pure and Applied Sciences
The official scientific journal of Salahaddin University-Erbil
https://zancojournals.su.edu.krd/index.php/JPAS

ISSN (print):2218-0230, **ISSN (online):** 2412-3986, **DOI:** **http://dx.doi.org/10.21271/zjpas**

RESEARCH PAPER

Proposed Solutions for the Main Challenges and Security Issues in IoT Smart Home Technology

Ahmed Abdulfatah Abdlrazaq [1], Sapan Noori Azzez [2], Mardin Abdulla Anwer [3], Shaho Ismael Hassen [4]

1 ICT Center, Salahaddin University -Erbil, Kurdistan Region, Iraq

2 Erbil Electricity Distribution Directorate Ministry of Electricity

3.Department of Software Engineering and Informatics, College of Engineering, Salahaddin University-Erbil, Kurdistan Region, Iraq

4.Department of Chemical, College of Engineering, Salahaddin University-Erbil, Kurdistan Region, Iraq

ABSTRACT:
The IoT has become a trend in recent years, and the smart home system has achieved great interest due to its need and requirement from consumers around the world. Smart home technology refers to the devices that are connected over the internet to monitor, support, and control the home in order to make our life easier. The revolution in technology has made homes more convenient, efficient, and even simpler. However, there are some challenges and obstacles that need to take into consideration when using a smart home system. Based on a comprehensive survey, this study aims to provide an overview of the critical security issues for IoT smart home systems and propose potential solutions to mitigate these risks by understanding vulnerabilities and applying security measures to ensure that the IoT system is more reliable and safe. The challenges and security issues highlighted with an emphasis on providing solutions, as well as smart home approaches and IoT layers.

KEY WORDS: Home Automation, Internet of Things (IoT), Smart Home Technology, Security Issues, Security Challenges
DOI: http://dx.doi.org/10.21271/ZJPAS.35.4.08
ZJPAS (2023) , 35(4);84-96

1. INTRODUCTION:

The Internet of Things (IoT) has revolutionized the way people interact with their homes. Smart home technologies have become increasingly popular, offering users the ability to automate and monitor their homes using connected devices and applications. This paper provides an overview of the state of the art of IoT Smart Home Technology and examines the challenges and security issues associated with its use.

All humans aspire to lead a comfortable lifestyle that is conducted safely. In many countries that are developed and have long cold winters, people may use their phones to turn on their kitchen appliances while they are away at work so that they can have a hot meal ready when they arrive home (Hamdan et al., 2021).

In a smart home environment, users can control and monitor items such as lights, temperature, climate, doors, and windows. Whilst smart homes provide greater convenience, their Internet connectivity and dynamic nature make them vulnerable to cyber-attacks (Touqeer et al., 2021). The heterogeneous nature of IoT architecture further increases their susceptibility to security breaches, with wireless network security being the most pressing issue to be addressed (Touqeer et al., 2021). Figure 1 illustrates the component and implementation of an IoT environment. This depiction demonstrates how the technology is being used in various settings and applications.

* **Corresponding Author:**
Ahmed Abdulfatah Abdlrazaq
E-mail: ahmed.abdulfatah@su.edu.krd

Article History:
Received: 18/03/2023
Accepted: 06/07/2023
Published: 30/08/2023

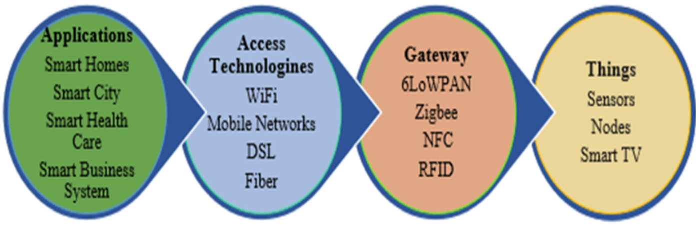

Figure 1: Components of IoT (Touqeer et al., 2021)

The integration of cloud computing and the Internet of Things has been widely discussed in recent literature. This combination can be used to show how cloud technology can expand the potential of IoT. IoT can be used to control home appliances, while machine learning techniques can be developed to ensure the security of a smart home. Additionally, sensors can be used to detect fires in real-time with a high level of accuracy (Ojha et al., 2021).

Smart home technology combines the use of networking with modern technology to promote better life quality. There is a variety of emerging technologies related to smart homes, such as automation, security, and home entertainment. Various trends are emerging as well, which will continue to shape the way smart homes are used (Stolojescu-Crisan et al., 2021).

Smart technology has revolutionized the way we interact with our environment. It has the ability to acquire data from its surroundings and respond accordingly, making it incredibly useful. In recent years, smart home tech has advanced quickly, making it more widely accessible to a variety of user groups (Marikyan et al., 2019). Smart homes are a crucial aspect of the European Union's plans for strategic energy investments. The UK's Office of Gas and Electricity Markets has declared that smart homes and businesses are critical to their mission to reduce carbon emissions and introduce more effective demand response initiatives (Sovacool et al., 2020).

In the coming sections, we clarify the methodology used in this work, then highlight the related work in the literature review, and explain the IoT components and layers. Then explain the security issues and challenges and come up with a discussion and present the most critical security issues with solutions in a framework and finally conclusion and future work.

2.Methodology

This section accounted for the methodology used in this study. This study used a systematic review methodology as our target to answer the main questions of the paper. Also, this methodology provides a shred of quality evidence for the readers and follows the standard structured process. The first step is to identify the research question. In this review paper, we have identified the research question, which is:

-What are the security issues and challenges facing the smart home from IoT? What is the security gap in current research with providing the solutions?

Then, provide the criteria of inclusion and exclusion based on the paper question. This is introducing the reason for reviewing this study. After identifying the research question and the factor of reviewing this paper, we started searching for the most relevant article/study related to smart homes, security issues, and challenges for IoT.

By using the Google Scholar (GS) online search service we started searching the literature. The GS is similar to other resources like Scopus, instead, the GS is easier to use and contain a huge amount of references with citation (Paul et al., 2021).

The publications between the years 2019 and 2022 were considered. Several expressions were used for the search such as IoT, Smart Home, Home Automation, Security Issues, Challenges, and the Internet of Things. Moreover, four query forms performed by using Expression1, Expression2, and Expression3. The total number of searched references in Google Scholar and the queries are shown in Table 1.

Table 1: Publication numbers found by searching over GS with different queries

Query	Expression1	Expression2	Expression3	Retrieved No.
Query1	IoT	Smart Home	Security Issues	17600
Query2	Internet of Things	Home Automation	Challenges	17800
Query3	IoT	Home Automation	Challenges	19100
Query4	Internet of Things	Smart Home	Security Issues	18300

We considered the first 10 results per query to analyze more. And we selected only the 29 best relevant papers from the result by below two steps:

First, we considered the title and abstract from the selected references and decided on those references that are potential for this study. Second, looking at each selected reference closely and screening the texts. Overall, the methodology for research on IoT smart home technology involves a rigorous process of defining research questions, determining scope, selecting appropriate research methodology, collecting and analyzing data, drawing conclusions, and recommending solutions. By following this methodology, researchers can gain a comprehensive understanding of IoT smart home technology and its associated challenges and security issues.

3.Literature Review

An overview of various research works proposed in the field of IoT, covering systems, models, security issues, and challenges. These studies encompass a wide variety of research in the IoT domain. Additionally, the implications of these studies are discussed with respect to the current state of IoT. Sovacool (Sovacool et al. 2020) found that the smart home revolution is rapidly gaining traction in Europe and the UK. In (Stolojescu-Crisan et al., 2021), developed qToggle, a system that is designed to provide multiple home/building automation services, such as access control, security, appliance control, irrigation, and power and energy management. Ojha (Ojha et al., 2021) has developed an innovative security system that can be managed remotely. This system combines the two intelligent devices of adjusting light settings and room temperature into one interface. Shahjalal (Shahjalal et al., 2020) presented a LoRa-based Smart Home (SH) system, a proprietary LP-WAN technology developed and commercialized by Semtech Corporation. Modulating the signal in the sub-GHz Industrial, Scientific, and Medical (ISM) frequency band. In (Mulcahy et al., 2019) posit that trust and risk play a pivotal role in households' interactions with technology. In line with prior research, our conceptual framework also suggests that trust and risk will be influential in determining outcomes. In (Touqeer et al., 2021), discussed the advantages of IoT systems, which can be applied to various applications such as smart industries, smart cities, and smart homes. Taiwo (Taiwo et al., 2021) developed the iHOCS system, a comprehensive home control, monitoring, and security system, with IoT hardware and software tools. Also, (Marikyan et al., 2019) stress the importance of understanding the role of different stakeholders in the acceptance of smart homes. Hamdan (Hamdan et al., 2021) proposed a framework and set of tools to facilitate communication between user agents and home sensors. Furthermore, they developed a practical risk valuation model to minimize attack risks and provide the house owner with greater control over security. Tawalbeh (Tawalbeh et al., 2020) stated that the security network of IoT is based on a configuration that depends on employees with a lack of training. This will affect security and make development more difficult. In addition, the integration of smart home systems has a major problem which is security; this is stated by (Shakya et al., 2022) after conducting a survey that explores the security risks and provides the main solutions when integrating the smart home system with cloud computing. In another research by (Thilakarathne et al., 2020), several solutions were provided for the smart home system to be more secure and they are: authentication, authorization, confidentiality, integrity, and non-repudiation. There is a study by (Nyangaresi et al., 2022) which is designed to develop a secure protocol for smart home systems. This was an attempt for solving the security problems that might happen in the smart home system including lack of encryption and authentication.

In (Fazion et al., 2020), proposed a secure framework for IoT devices related to controlling the security of passwords through AI and robots in a new way by creating and controlling access. This framework requires less time, little energy consumption, and limited data processing. In (Stoyanova et al., 2020), stated that the growth of

IoT technology and its development has an impact on security, still researchers work to settle the security issues and propose solutions. Therefore, researchers with the collaboration of business organizations should unite to mitigate the security risks and challenges. In (Mohanta et al., 2020), recent researches focus on IoT challenges and security issues. And the vision of smart homes centres on privacy, reliability, and the integration of smart homes from the threats and vulnerabilities to IoT.

In (Shouran et al., 2019), stated that because of the lack of security equipment IoT, and smart home devices purchase easily and timely targeted by hackers. This does not guarantee patient knowledge. In (Hassan et al., 2021), stated that cloud computing and big data have their role and impact on the development of smart cities by having a huge dimension of information and capabilities. However, still, there are gaps in this new technology when implementing smart cities. Both (Sepasgozar et al., 2020) and (Singh et al., 2019), agreed that in the cyber-physical system vulnerability and privacy issues could be found, for instance the smart home system and other IoT systems. In this case, the hackers may start attacking since having vulnerabilities and security issues. Thus, using hashing and encryption algorithms will achieve the solution for smart home networks. In (Almusaylim et al., 2019), another critical challenge is sensitive data, those data are collected by the sensors and might include sensitive private information. The protection and privacy for these sensitive data crash the users legally, and it is considered the most critical challenge in smart homes.

In addition, (Abdulla et al., 2020) proposed a dynamic security model for smart home systems using Arduino and the IoT sensors to secure the smart home devices when transferred over the wireless into the cloud. And (Ibrahim et al., 2022), stated that (DDoS) attack is a significant threat to smart home devices, to prevent this threat proposed a blockchain model for detecting DDoS attacks toward IoT systems.

4. IoT & Smart Home Technology

In recent years, the Internet of Things (IoT) paradigm has become increasingly popular and is comprised of various hand-held devices such as smartphones, tablets, laptops, personal computers, and other embedded devices, including smart watches, smart doors, and smart locks (as demonstrated in Figure 2) (Touqeer et al., 2021). In the IoT framework, devices can communicate without human interaction and can send and process data automatically according to different situations; for example, when a fire is detected, fire sensors will sense the fire and trigger an alarm to activate any other relevant devices to extinguish the fire. For the IoT to be successful, its environment must be organized in such a way that all devices operate effectively, despite the heterogeneity of the system. This can lead to various issues, such as formalization problems, standardization problems, data problems, and security issues. To ensure a successful transaction, all smart nodes and Radio Frequency Identifier (RFID) equipment must be connected properly. In terms of formalization, users tend to focus on reliability (which should cover all aspects), optimality (which should utilize the minimum number of nodes), and redundancy (which should be fault-tolerant, portable, and able to facilitate easy recovery from any mishaps). In the IoT, every single node or protocol should be standardized to overcome the heterogeneous nature of the IoT environment, with a worldwide standard being implemented across the network to ensure smooth operation with other equipment. As data is essential to the IoT network, it is necessary to ensure the integrity and availability of the data, which must be circulated from legitimate devices and sensor nodes, and ensure that there are no pirated devices within the premises of the IoT network. Below is Figure 2 showing the IoT structure.

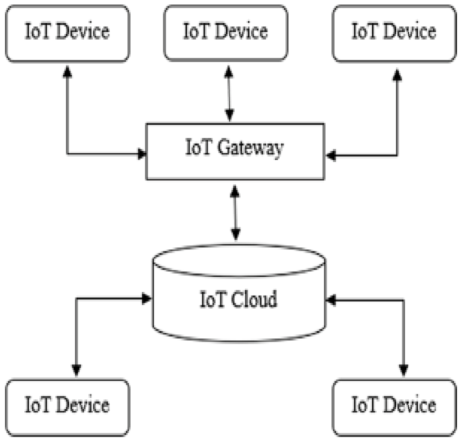

Figure 2: IoT Structure (Touqeer et al., 2021)

4.1Structure of IoT Layers:

Figure 3 illustrates the layers of the architecture of the Internet of Things (IoT) environment, which allow for the accomplishment of the objectives of IoT. The main layers that are instrumental in realizing these objectives are outlined below (Touqeer et al., 2021).

1. Application layer:

    The application layer of the Internet of Things (IoT) is one of its most integral components, providing access to a wide range of applications and services such as smart cities, smart homes, smart hospitals, and intelligent transportation. Consequently, it is essential for ensuring the smooth operation of the IoT platform.

2. Perception layer:

    The perception layer is a component of scholarly architecture that encompasses the various technologies and devices that capture input from the environment. It is responsible for gathering and processing basic information, often referred to as a fragment of knowledge.

3. Network layer:

    The Network Layer is an essential component of communication systems, as it encompasses both software and hardware components that facilitate communication between different devices.

4. Physical layer:

    The physical layer of the Internet of Things (IoT) comprises a variety of hardware devices and components, such as power supplies, smart appliances, and smartphones, which act as the foundation of the IoT world. In Figure 3 the IoT layers are presented.

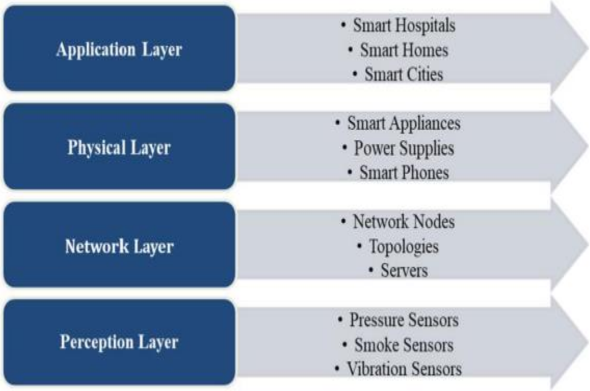

Figure 3: IoT Layers (Touqeer et al., 2021)

4.2 Smart Home System:

The term "smart home" widely refers to a dwelling that utilizes a home controller to link together the house's multiple home automation systems (Stolojescu-Crisan et al., 2021). Figure 4 illustrates the smart home automation system.

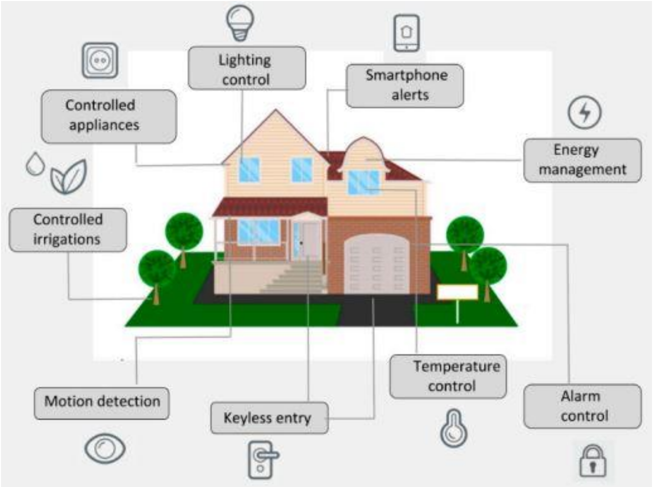

Figure 4: Smart Home Technology Automation (Stolojescu-Crisan et al., 2021)

The appliances and devices within a system are designed to receive commands, while transmitters, such as remote controls or keypads, are used to control the system. For instance, if you wish to turn off a lamp in another room, the transmitter will send a message encoded in numerical code to the receiver (Stolojescu-Crisan et al., 2021).

Several smart home technology approaches are commonly used, and they are:

A.Z-Wave:

Z-Wave utilizes a Source Routing Algorithm to establish the most efficient path for messages to travel. Each device in the Z-Wave system has a unique code embedded within it. (Marikyan et al., 2019).

B. ZigBee:

The name ZigBee reflects its mesh networking approach, where messages from the transmitter travel along multiple paths, similar to how bees move, to find the most efficient route to the receiver (Stolojescu-Crisan et al., 2021).

C. Insteon:

Wireless networks offer more freedom in terms of device placement, but may also encounter interference issues. The Insteon provides a solution by allowing communication over both electrical wires and radio waves, creating a dual mesh network. This ensures that if a message is unable to be transmitted through one platform, it will automatically attempt to transmit through the other (Stolojescu-Crisan et al., 2021).

4.2.1 Smart Home Categories:

Popular Smart Home Systems can be grouped into several sub-categories based on the functions, devices, and hardware/software combinations they offer.

1-Smart Home System Based on DTMF Technology:

The concept of controlling appliances remotely in a home setting originated with the use of Dual-Tone Multi-Frequency (DTMF) tones via mobile phone (Hasan et al., 2018). The system employed specific signals generated by the digits on a mobile phone's keypad to execute specific tasks.

2-Smart Home System Based on GSM:

A GSM-based home automation system utilizes a mobile phone, a GSM module, a microcontroller board, and a control circuit to control appliances (Hasan et al., 2018). The user sends commands as SMS messages to the GSM module, which receives the message and forwards it to the microcontroller board for execution.

3-Smart Home System Based on Voice Recognition:

When it comes to voice recognition-based automation, Zigbee-based smart home systems are the most widely used. These systems are comprised of three main modules: a microphone module, a Zigbee coordinator, and Terminals (Stolojescu-Crisan et al., 2021).

5. Challenges and Security Issues

The key components of cyber security are confidentiality, authentication, non-repudiation, and access to ensure that data is shielded from alteration and unwanted access. To achieve secrecy, cryptography is a must. Data integrity is checked during authentication to make sure it hasn't been changed and that the source of the data can be positively identified (Nacer et al., 2017).

5.1 Security Issues:

5.1.1 Threats:

Smart Home settings confront identical security risks as other domains. When confidential information is disclosed without permission, confidentiality hazards arise. For instance, the disclosure of medical information from home monitoring devices may constitute a significant violation of confidentiality. Even seemingly unimportant information, like a home's interior temperature, can be utilized to identify occupancy and could even result in a break-in. This is so that a denial-of-service assault known as an energy depletion attack, which is a sort of denial-of-service, won't occur on the network. Several Smart Home gadgets may be wirelessly networked with a low operating duty cycle (Tawalbeh et al., 2020).

5.1.2 Vulnerabilities:

Given that Smart Home systems are linked to the Internet, network accessibility is a big worry when it comes to network security. Remote assaults can be executed by installing malware on targets or by directly accessing networked control interfaces. Physical accessibility might also be a concern because networks can be accessed even if a property is safely closed from the outside (Almusaylim et al., 2019). The majority of modern Smart Home gadgets lack efficient security measures, despite certain proprietary systems having well-designed security requirements. The complexity of a Smart Home network requires a dedicated security specialist to maintain it (Ibrahim et al., 2022).

5.1.3 Integration Issues

A suggested trust security method has offered an effective remedy that improves communication in IoT-cloud services to overcome these problems. To secure data secrecy, an access control approach is needed (Mulcahy et al., 2019). In contrast to current methods, Xiong et al. suggested cypher text-based policy-based attribution technique decreased storage usage of public keys, as well as computational overhead and storage costs (Shakya 2022). A distance-based and fuzzy approach was developed to give an ideal solution and boost the effectiveness of IoT-based communication (Thilakarathne et al., 2020). A flexible approach to addressing security concerns was developed in an IoT-based cloud framework that makes use of Software Defined Network for effective communication with end users (Fazion 2020). Last but not least, there is a security paradigm that uses cloud computing to solve IoT security problems (Mohanta et al., 2020). In the Table 2, several security methods with the techniques and their result presented.

Table 2: Security Communication Techniques

Methods	Approach	Result
Lightweight security	E2E System communication	High security in real time applications (Shakya 2022)
Attack modeling	IoT based-Cloud	Quality of solutions improved (Abdulla et al., 2020)
Security of loT Devices	Machine tools	Secure cloud framework (Thilakarathne et al., 2020)
Authorization Structure	Services of Healthcare	Decrease secure storage. Prevent the malicious (Almusaylim et al., 2019)
Balanced incomplete block design model	Secure key management protocol	Secure E2E communication (Stoyanova et al. 2020)

5.1.4 Attacks in Terms of IoT Layers:

A. Perception Layer:

This layer, which is also known as the Devices layer, is the lowest in the IoT architecture. Using trustworthy and secure sensing equipment that can precisely collect data and connect with other levels is crucial to ensuring the effective operation of this (Stoyanova et al. 2020).

B. Gateway Layer:

This layer is located between the Perception Layer and the Cloud Layer. The main purpose is to provide reliable communication between the lower-level devices and the upper-level cloud services (Shouran et al., 2019).

C. Cloud Layer:

The IoT architecture's top layer is in charge of offering end-user services, such as an interface that enables users to manage and control their devices (Mulcahy et al., 2019). The descriptions of these security threats shown in Table 3.

Table 3: Security Threats and Their Descriptions

No.	Threat Types	Layer Type	Description and Details
1	Denial of Service Attack	Perception Layer	IoT sensing nodes have limited capacity and capabilities thus attackers can use Denial of Service attacks to stop the service. Eventually, servers and devices will be unable to provide their service to users (Ibrahim et al., 2022).
2	Hardware Jamming	Perception Layer	An attacker can damage the node by replacing the parts of the node hardware (Taiwo et al., 2021).
3	Insertion of Forged nodes	Perception Layer	An attacker can insert a falsified or malicious node between the actual nodes of the network to get access and get control over the IoT network (Fazion 2020).
4	Brute Force Attack	Perception Layer	As the sensing nodes contain weaker computational power brute force attacks can easily compromise the access control of the devices (Tawalbeh et al., 2020).

5	Denial of Service Attack	Gateway Layer	As this layer provides network connectivity by following a DOS attack, servers or devices are unable to provide the services to the user (Shouran et al., 2019).
6	Session Hijacking attacks	Gateway Layer	Attackers can hijack the session and obtain access to the network through this kind of attack (Singh et al., 2019).
7	Man in the middle attacks	Gateway Layer	The attacker can intersect the communication channel between two sensing nodes and easily obtain classified information if there is no proper encryption mechanism in place (Shakya 2022).
8	Data security in cloud computing	Cloud Layer	All the Data that is collected will be processed and stored in the cloud, Cloud service providers will be held responsible for protecting this data (Abdulla et al., 2020).
9	Application layer attacks	Cloud Layer	Most applications are hosted on the cloud as Software as a Service and delivered through web services, so the attacker can easily manipulate the application layer protocols and get access to the IoT network (Thilakarathne et al., 2020).
10	An Attack on Virtual Machines	Cloud Layer	The security of cloud virtual machines is very important and any security breach can cause the failure of the entire IoT environment (Nyangaresi et al., 2022).

5.2 IoT Challenges:

Guarantee the availability, integrity, and secrecy of IoT ecosystems, this involves protecting physical components, applications, data, and network connections (Fazion 2020). IoT systems face a large number of security issues as a result of the frequent discovery of faults in them. IoT security must be comprehensive to be effective, encompassing component hardening, monitoring, firmware updates, access control, threat response, and vulnerability patching. IoT device security must be ensured since these systems are widespread, exposed, and highly-targeted attack vectors. To avoid IoT devices acting as a backdoor into other areas of the network or leaking important information, unauthorized access to them should be blocked (Thilakarathne et al., 2020).

There are several weaknesses in IoT security, including those in linked cars, smart grids, and wearable, and smart home appliances. For instance, researchers found that webcams were easily hackable and could be used to get access to networks. Similar security flaws were discovered in smartwatches, enabling hackers to monitor wearers' whereabouts and overhear their conversations. Moreover, most consumers are unaware of the magnitude of IoT security concerns and the inherent hazards connected with IoT equipment (Tawalbeh et al., 2020). The numerous security challenges that IoT encounters include the following:

- Lack of visibility: Although IoT devices have grown in popularity over the past several years, it can be difficult to secure these devices since they are sometimes deployed without the awareness of IT departments (Abdulla et al., 2020).
- Limited security integration: Due to the variety and size of these devices, it is difficult to impossible to integrate IoT devices into security systems (Almusaylim et al., 2019).
- Open-source code vulnerabilities: Firmware for IoT devices frequently includes open-source software, which is prone to errors and weaknesses (Nyangaresi et al., 2022).
- Overwhelming data volume: The vast amount of data generated by IoT devices can make data oversight, management, and protection challenging (Thilakarathne et al., 2020).

- Poor testing: The majority of IoT developers do not prioritize security, which frequently prevents them from doing efficient vulnerability testing to find flaws in IoT systems (Sepasgozar et al., 2020).
- Unpatched vulnerabilities: IoT devices frequently have flaws that go unpatched for a variety of reasons (Tawalbeh et al., 2020).
- Vulnerable APIs: act as entry points for attacks like SQL injection, distributed denial of service, man-in-the-middle, and network intrusions that are launched from command-and-control centres (Ibrahim et al., 2022).
- Weak passwords: A significant security risk is the pervasive usage of default passwords in IoT devices (Fazion 2020).

6.Discussion

It is crucial to mention that smart home devices that are connected to the internet are vulnerable and fit for attacks. It is important when developing this technology to consider the security issues and how to prevent them. In this case, the companies and engineers have a huge responsibility to take care of the security and apply the security methods and certificates to mitigate the security risks (Ibrahim et al., 2022).

The merging of three seemingly disparate concepts such as linked components, smart homes, and the IoT is the subject of this discussion. We highlight the individual advantages and benefits of each component, as well as the potential synergies that can be achieved by integrating them. By doing so, we unlock additional advantages of the overall system, resulting in a more comprehensive and powerful solution. The cloud computing component is also an important part of this integration, and we explore its role in enabling seamless communication and data exchange among the various components (Ojha et al., 2021). Since the advantages of this technology are not without matching concerns, it is crucial to identify any potential obstacles and dangers related to smart houses such as privacy difficulties, security problems, and hacker possibilities. By examining these dangers, it will be feasible to create technologies and mitigation measures that will make users of smart homes safer and more secure (Sovacool et al., 2020).

With the increasing interconnection of smart household appliances to Smart Home networks, technical support is expected to become a major challenge in the household environment. As a result, householders may face tedious and error-prone manual tasks for adding and managing these smart devices on their home network, which can lead to significant security risks. Therefore, a secure auto-configuration approach should be studied further for the successful implementation of a Smart Home. This approach not only simplifies Smart Home device installation and maintenance, but also enhances security during the auto-configuration process. As Smart Home networks continue to expand, it is crucial to address the technical challenges and security risks associated with these interconnected devices (Abdulla et al., 2020).

Hence, it is critical to maintain the most recent version of the firmware on smart devices to resolve security flaws, improve functioning, add new features, and handle any other problems. Smart home users generally lack such resources, in contrast to enterprise-scale setups that have specialized IT departments or technical teams in charge of software upgrades and implementation (Abdulla et al., 2020).

In addition, security is still a serious issue, though, because intruders and third parties might access IoT networks. Investigating potential solutions is important to solve these security concerns. Reviewing the literature for this study looks at several security issues and suggests solutions for preventing security problems when integrating IoT with cloud computing. Confidentiality, integrity, availability, authentication, authorization, and accountability are the six categories that make up the security core and are shown in Figure 5.

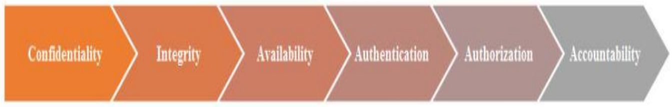

Figure 5: Security Core (Shakya 2022)

To address security concerns in the integration of IoT with cloud computing, confidential information is disclosed without permission, confidentiality hazards arise such when keys and passwords are lost; there is a risk of unauthorized access. The absence of frequent software updates to repair security vulnerabilities in Smart Home appliances is another concern, due to the lack of incentive for devices that cost merely a few dollars. Unauthorized access, particularly at the administrator level, poses the most hazards since it can render the system vulnerable as a whole. An unwanted connection to the network might deny service to authorized users or deplete the battery of Smart Home devices even if control is not taken. This is so that a denial-of-service assault known as an energy depletion attack, which is a sort of denial of service, won't occur on the network. Several Smart Home gadgets may be wirelessly networked with a low operating duty cycle. Network accessibility is a big worry when it comes to network security

Remote assaults can be executed via installing malware on targets or by directly accessing networked control interfaces. Physical accessibility might also be a concern because networks can be accessed even if a property is safely closed from the outside.

Another weakness in the field of smart homes is the sluggish adoption of security standards. The majority of modern Smart Home gadgets lack efficient security measures, despite certain proprietary systems having well-designed security requirements.

A suggested trust security method has offered an effective remedy that improves communication in IoT-cloud services to overcome these problems. To secure data secrecy, access control approach is needed. Cryptosystems were also implemented, introducing secret encryption and decryption keys based on a time encoding scheme. The datagram transport layer security protocol was established and offered secure communication appropriate for UDP- and TCP-based applications. A flexible approach to addressing security concerns was developed in an IoT-based cloud framework that makes use of Software Defined Network for effective communication with end users. Last but not least, there is a security paradigm that uses cloud computing to solve IoT security problems. Moreover, considering the attacks in IoT layers such as perception, gateway, and cloud layer may lead to protect the IoT system.

IoT devices rely on various communication protocols, such as Wi-Fi, Bluetooth, and cellular networks. Weak encryption, unencrypted data transmission, and insecure network configurations can expose sensitive information to interception and tampering. Physical access to IoT devices can compromise their security. Inadequate physical protection, tampering, or unauthorized device modifications can lead to unauthorized control or data manipulation.

In addition, IoT security must be comprehensive in order to be effective, encompassing component hardening, monitoring, firmware updates, access control, threat response, and vulnerability patching.

Most consumers are unaware of the magnitude of IoT security concerns and the inherent hazards connected with IoT equipment. The numerous security challenges that IoT encounters includes (lack of visibility, limited security integration, unpatched vulnerabilities, poor testing, weak password and etc.).

Along with identifying the security risks and challenges, providing a proper solution is a must to protect the IoT ecosystem. Strong authentication mechanisms need to be implemented, such as two-factor authentication to enhance the security. Also, Access controls should also be implemented to restrict unauthorized access to sensitive data. Another critical solution is securing communication, the transmitted data between the network and devices should be encrypted and the standard communication protocols need to be applied to protect data integrity. Upgrading firmware and providing security patch to identify vulnerabilities and improve the security of the devices is a major point that needs to be considered. Physical security measures are another solution as IoT devices should be protected physically from unauthorized access, by applying a mechanism to detect physical tampering attempt. In addition, sensitive data collected by IoT devices should be encrypted during transmission and storage. Access controls, data anonymization, and regular security audits should be implemented to protect user privacy and prevent unauthorized data access.

Finally, after reviewing the literature in this review study, we propose a security framework to consider when implementing and using the smart home system. The solutions that may be used to successfully handle the security issues with IoT devices are presented. These methods can be used for one or more functions of an IoT device and are not mutually exclusive. They operate together as a platform and make use of complicated network theory, statistics, and encryption techniques, among other things, to enhance IoT security continuously (Fazion 2020). The security issues and the affected side of IoT systems with their solutions are provided in Table 4 after reviewing the literature and according to the security framework of this work.

Table 4: Security Issues and Their Solutions

Security Problem	Impacted side	Solutions
eavesdropping	Between two point of IoT device	Using VPN to encrypt the data between two points and using HTTPS for all communication channels (Thilakarathne et al., 2020).
Identity Spoofing	Identification, Interface	Well-organized physical layer for attack detection using two step detection schemes (Shouran et al., 2019).
Data Tampering	Processor, Sensing, Communication	Using a firewall in a smart home system to control the traffic over the network and defense against any unauthorized access (Fazion 2020).
Malicious code	Actuating, Sensing, Identification	Creating a proper input validation before processing any request. And applying a security certificate to the API gateway. Also, lock down the environment to minimize security risks. Moreover, using ML techniques (Tawalbeh et al., 2020).
Sniffing and encryption cracking	IoT Network	Most Wi-Fi routers use WEP which causes it to be reused. This repetition makes it vulnerable. More secure options are WPA2 & WPA3 (Singh et al., 2019).
DDoS	IoT devices, Server and Network	Using a blockchain model to mitigate/prevent the DDoS attack toward IoT system. Also, tracing IP addresses from malicious gadgets in the middle of the blockchain to stop the attacks from communicating with IoT network (Ibrahim et al., 2022).
Interoperability/ Gateways	Cooperation, Communication	Using the MI method to confirm the deportment of the patterns. Also, improving the security of network over identity verification & deviation detection (Shakya 2022).
Phlashing (PDoS)	IoT devices	It's recommended to change the default password of the manufacturer to secure the devices. Also, the best way is to apply multi-factor authentication (Abdulla et al., 2020).

7.Conclusion and Future Work

As the IoT ecosystem continues to expand, it is crucial to address the security challenges associated with interconnected devices. By implementing strong authentication, encryption, regular updates, and physical security measures, the risks associated with IoT can be mitigated. Collaboration among manufacturers, policymakers, and end-users is vital to establishing a secure and trustworthy IoT environment.

The main contribution is addressing smart home security issues and their expectation when integrating with IoT. A complete IoT framework suggested including different portions proposed in the literature review to incorporate a smart home with an IoT environment properly. Although several researchers are working on IoT security issues, there are still many areas under development as there are still many significant issues that remain unsolved. As a second contribution, this paper provides comprehensive security solutions challenges toward smart homes in order to have a reliable and safe IoT system.

The current situation is that smart home devices are still target for hackers and security problems, and the best solution according to the proposed security framework is to use a firewall to manage the security levels of connected IoT devices.

For future work, a new model is to be introduced called a trust management model. This model will increase IoT and smart system security when integrated into the network.

Conflict of interest

I certify that I have no connections to or participation in any organization or entity that might have a financial interest (such as an honorarium, educational grants, speaking engagements, membership, employment, consultancies, stock ownership or other equity interest, expert testimony, or patent-licensing arrangements) or non-financial interest (such as connections, affiliations, knowledge, or beliefs) in the topic or materials discussed in this manuscript.

Reference

Hamdan, Y.B., 2021. Smart home environment future challenges and issues-a survey. Journal of Electronics, 3(01), pp.239-246.

Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F., & Bilal, M. (2021). Smart home security: challenges, issues and solutions at different IoT layers. The Journal of Supercomputing, 77(12), 14053-14089.

Ojha, M. K. (2021). AN OVERVIEW OF SMART HOME SYSTEM BASED ON INTERNET OF THINGS.

Stolojescu-Crisan, C., Crisan, C. and Butunoi, B.P., 2021. An IoT-based smart home automation system. Sensors, 21(11), p.3784.

Almaiah, M.A.; Nasereddin, Y. (2020) Factors influencing the adoption of e-government services among Jordanian citizens. Electron. Gov. Int. J. 2020, 16, 236–259.

Marikyan, D., Papagiannidis, S., & Alamanos, E. (2019). A systematic review of the smart home literature: A user perspective. Technological Forecasting and Social Change, 138, 139-154.

Sovacool, B. K., & Del Rio, D. D. F. (2020). Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies. *Renewable and sustainable energy reviews*, *120*, 109663.

Paul, J., Lim, W. M., O'Cass, A., Hao, A. W., & Bresciani, S. (2021). Scientific procedures and rationales for systematic literature reviews (SPAR-4-SLR). *International Journal of Consumer Studies*, *45*(4), O1-O16.

Mohamed Shaffril, H. A., Samsuddin, S. F., & Abu Samah, A. (2021). The ABC of systematic literature review: the basic methodological guidance for beginners. *Quality & Quantity*, *55*, 1319-1346.

Hasan, M., Biswas, P., Bilash, M. T. I., & Dipto, M. A. Z. (2018, November). Smart home systems: Overview and comparative analysis. In *2018 Fourth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)* (pp. 264-268). IEEE.

Stolojescu-Crisan, C., Crisan, C., & Butunoi, B. P. (2021). An IoT-based smart home automation system. *Sensors*, *21*(11), 3784.

Shahjalal, M., Hasan, M. K., Islam, M. M., Alam, M. M., Ahmed, M. F., & Jang, Y. M. (2020, February). An overview of AI-enabled remote smart-home monitoring system using LoRa. In *2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)* (pp. 510-513). IEEE.

Mulcahy, R., Letheren, K., McAndrew, R., Glavas, C., & Russell-Bennett, R. (2019). Are households ready to engage with smart home technology?. *Journal of Marketing Management*, *35*(15-16), 1370-1400.

Yar, H., Imran, A. S., Khan, Z. A., Sajjad, M., & Kastrati, Z. (2021). Towards smart home automation using IoT-enabled edge-computing paradigm. *Sensors*, *21*(14), 4932.

Taiwo, O., & Ezugwu, A. E. (2021). Internet of things-based intelligent smart home control system. *Security and Communication Networks*, *2021*.

Nacer, A., Marhic, B., & Delahoche, L. (2017, May). Smart Home, Smart HEMS, Smart heating: An overview of the latest products and trends. In *2017 6th International Conference on Systems and Control (ICSC)* (pp. 90-95). IEEE.

Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102.

Shakya, S. (2022). A perspective review of security issues in iot with cloud environment. *Journal of IoT in Social, Mobile, Analytics, and Cloud*, *4*(2), 84-93.

Thilakarathne, N. N. (2020). Security and privacy issues in iot environment. *International Journal of Engineering and Management Research*, *10*.

Nyangaresi, V. O., Rodrigues, A. J., & Abeka, S. O. (2022). Secure Algorithm for IoT Devices Authentication. In *Industry 4.0 Challenges in Smart Cities* (pp. 1-22). Cham: Springer International Publishing.

Fazion, M. (2020). Vulnerabilities and security issues of IoT devices. *Sikur Report*, *1022020*.

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, *22*(2), 1191-1221.

Mohanta, B. K., Jena, D., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2020). Addressing security and privacy issues of IoT using blockchain technology. *IEEE Internet of Things Journal*, *8*(2), 881-888.

Shouran, Z., Ashari, A., & Priyambodo, T. (2019). Internet of things (IoT) of smart home: privacy and security. *International Journal of Computer Applications*, *182*(39), 3-8.

Hassan, R. J., Zeebaree, S. R., Ameen, S. Y., Kak, S. F., Sadeeq, M. A., Ageed, Z. S., ... & Salih, A. A. (2021). State of art survey for iot effects on smart city technology: challenges, opportunities, and solutions. *Asian Journal of Research in Computer Science*, *8*(3), 32-48.

Sepasgozar, S., Karimi, R., Farahzadi, L., Moezzi, F., Shirowzhan, S., M. Ebrahimzadeh, S., ... & Aye, L. (2020). A systematic content review of artificial intelligence and the internet of things applications in smart home. *Applied Sciences*, *10*(9), 3074.

Singh, S., Ra, I. H., Meng, W., Kaur, M., & Cho, G. H. (2019). SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology. *International Journal of Distributed Sensor Networks*, *15*(4), 1550147719844159.

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*, 3193-3204.

Abdulla, A. I., Abdulraheem, A. S., Salih, A. A., Sadeeq, M. A., Ahmed, A. J., Ferzor, B. M., ... & Mohammed, S. I. (2020). Internet of things and smart home security. *Technol. Rep. Kansai Univ*, *62*(5), 2465-2476.

Ibrahim, R. F., Abu Al-Haija, Q., & Ahmad, A. (2022). DDoS Attack Prevention for Internet of Thing Devices Using Ethereum Blockchain Technology. *Sensors*, *22*(18), 6806.