Securing the Connected Home: Addressing IoT Privacy and Security Challenges with Comprehensive Strategies

Mahmoud Younis Mohmmed[1], Almabruk Sultan[2]

[1]Master's Degree in Computer Science, Academy of Postgraduate Studies Libya
[2]Assistant Professor of Computer Science, University of Benghazi

Abstract:
The paper focuses on the security and privacy concerns of Internet of Things (IoT) -based smart homes, which have numerous advantages but also raise significant security and privacy concerns. These concerns stem from the sensitivity of the data collected, the heterogeneity of application components, dynamic communication patterns, and limited resources. The study aims to increase knowledge, keep pace with development, and contribute to solving these problems by studying research, studies, articles, and references that address these concerns.
The methodology of this study consists of three stages: systematic review of relevant studies, designing an evaluation model for security solutions, and proposing a security solution that addresses these concerns. The third phase proposes a security solution that consists of security tools, protocols, and procedures in a multi-layered architecture implemented in the middleware operating environment. This solution offers advantages that are missing from many other solutions proposed in previous studies, such as interoperability and scalability. The study aims to contribute to the development of integrated solutions to address these security and privacy concerns in smart home applications based on the Internet of Things.

Keywords: IoT, security, privacy concerns, security solutions, heterogeneity, interoperability, scalability

1. Introduction

1.1 preface:

- **What is the meaning of Internet of Things (IoT)?**

The IoT refers to the billions of objects and physical devices, around us that are now connected to the internet, all collecting and sharing data. Thanks to the arrival of super-cheap computer chips and the ubiquity of wireless networks, it's possible to turn anything, from something as small as a ring to something as big as an airplane, into a part of the IoT [1]. Connecting up all these different objects and adding sensors to them adds a level of digital intelligence to devices that would be otherwise dumb, enabling them to communicate real-time data without involving a human being. The IoT is making the fabric of the world around us smarter and more responsive, merging the digital and physical universes.

- **Smart Home based on IoT**

"Smart home Term " is used to define internet-connected home systems that intelligent and automate the things homeowners will use every day. They may improve energy economy, security, comfort, and style, all from a single device[2].

We leave work after exerting effort and need to relax, take a bath, eat a good meal, and sleep in a cool and dim environment to reduce job-related stress. All these needs necessitate preparation time and effort. However, when everything in our environment is inanimate or alive, intelligent, and interconnected, it participates in the exchange of data and information, evaluates, and analyzes it, determines what is needed, and makes decisive decisions without any human intervention. Yes, all the necessities will be ready and waiting for us as make our way home. According to forecasts by statista.com, this market is expected to grow at a compound annual growth rate (CAGR) of 11.43% in 2023–2028, resulting in a projected market volume of US$231.6 billion by 2028, with global corporations like Google, Amazon, and Samsung Electronics joining the industry[3].

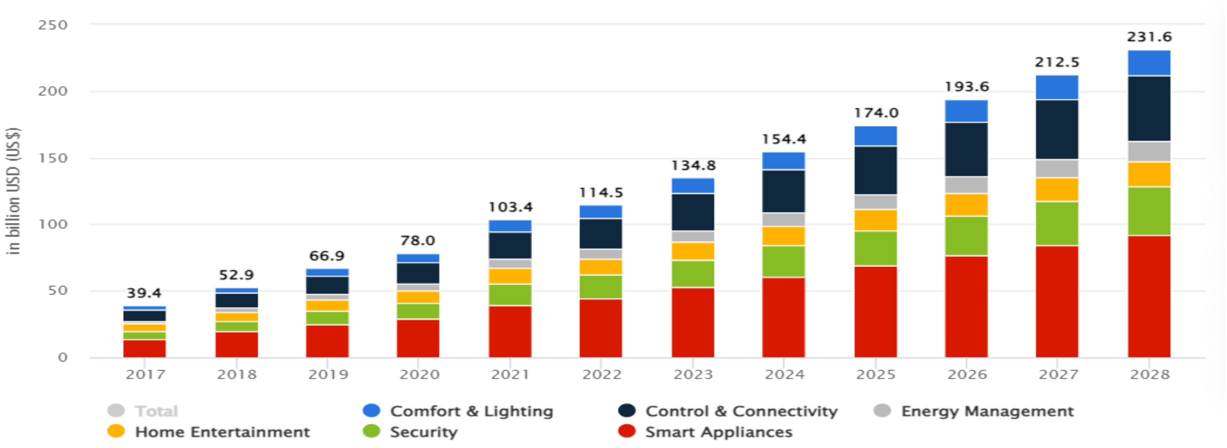


Figure 1.1 The forecast and current numbers between 2018 and 2028

1.2 Research Motivations:

The (IoT) is revolutionizing sectors like smart homes, offering opportunities for studying advanced innovations in home automation, sensors, and data analytics[4]. Studying smart home technology can position individuals for future success in the employment market. The interdisciplinary nature of smart home and IoT combines computer science, electrical engineering, data analysis, user experience design, and cybersecurity[5]. Studying smart homes offers practical applications in improving convenience, comfort, security, and energy efficiency. The industry is thriving due to increasing customer demand, offering skills in home automation, electronics manufacturing, and energy management[6]. Smart homes also promote efficiency and sustainability, contributing to climate change mitigation.

1.3 Problem Statement:

Smart home components, consisting of hardware, physical equipment, sensors, network components, and processing components, collect sensitive data about residents. These components, are heterogeneous and diverse in resources. These components are divided into four layers: hardware, network, processing components, and components of monitoring, control, and operation for the components that make up a smart home system. To protect this data, a large number of cybersecurity mechanisms, technologies, and solutions are needed. However, these solutions can create conflicts and vulnerabilities, allowing unauthorized access to the system and resulting data, and posing privacy and security concerns. Research is crucial for understanding threats, developing safe use rules, assessing user attitudes, and evaluating policies. Comprehensive strategies are needed to address all security threats and vulnerabilities. The study aims to find comprehensive and integrated solutions to cover all security vulnerabilities and cyber threats causing security and privacy concerns for users of smart home applications based on the IoT. This research issue aims to educate users about privacy rights, data protection duties, and best practices for securing devices and networks. It also aims to understand potential risks and vulnerabilities from security breaches or privacy violations. The research can also improve smart home security protocols, safeguard networks, and implement encryption for personal information protection.

The study is divided into sections, covering literature review, methodology, results, conclusion, and future directions for a research problem. It discusses the chosen methodology, source collection, and evaluation strategy, and proposes a comprehensive security framework. The text uses the Mendeley program to organize and define sources, following the IEEE citation style.

2. Literature Review:

This section explores relevant studies in two ways: examining the research issue's scope, risk assessment methods, security concerns, privacy concerns, and solutions, and an in-depth discussion of relevant studies sorted by research issue elements and taxonomy to comprehend all components and contribute to its resolution.

D. Mocrii et al, H. Verma et al, M. Jyotsna et al, T. Malche et al[7][8]–[10]. They discuss key technologies for IoT-based smart homes, focusing on safety, security, energy efficiency, user functions, suggested architectures, software solutions, and system administration components, emphasizing the importance of addressing security and privacy issues. B. Ali et al[11], used the OCTAVE Allegro method to assess security risks in IoT-based smart homes, identifying 15 vulnerabilities both inside and outside the homes. This helps understand the impact of threats on the system, procedures, and solutions. The review aims to resolve challenges by analyzing selected studies and providing comprehensive insights into security and privacy issues.

And the security concerns aspect, Talal Abdullah et al 2019[12], analyzed vulnerabilities in smart home design and cybersecurity threats, highlighting weak encryption, storage limitations, and false authentication. Recommendations are provided for effective security mechanisms. also, F. Schuster et al 2020[13] discussed IoT basics, smart home components, communication protocols, and security challenges. It suggests adapting communication protocols and proposing architectural layers to enhance security in smart home systems. F.k.gondal et al 2021[14], assessed security and privacy risks in IoT-based smart homes, presenting mitigation strategies and emphasizing the need for further research and development to address these concerns. And, Lili Nemec et al 2022[15], surveys users of smart home devices, focusing on perceptions of application, services, and security aspects. The findings aim to contribute to developers building better devices and increasing security awareness among users.

And then, privacy concerns aspect. K. Sarwar et al 2019 [16], focused on privacy in smart home devices, analyzing privacy requirements, categorizing solutions, and addressing issues related to open search. It classifies privacy concerns and interests, particularly in context-oriented and content-oriented privacy, and analyzes privacy implications of technological developments. Keyang Yu et al 2020[17], explored user privacy concerns and proposed a low-cost, open-source defense system called Privacy Guard, aiming to reduce privacy leakage in smart homes. However, the system introduces additional hardware and traffic expenses, potentially increasing costs for users. The technical details of the proposed technology are limited in the paper. T. Yung et al 2022[18], addressed privacy leakage in IoT-based smart home applications by analyzing network traffic. The authors introduce IoT event, a semi-automated tool for detecting vulnerable smart home devices, considering both hacker and system attacker perspectives. The study provides a comprehensive view of the topic, evaluating the tool's effectiveness on different cloud platforms.

Review Solutions for concerns, by Jose Costa et al[19], Salem Aljanah et al[20], Mohammad Ali et al[21], and Vipin Kumar et al[22], the preliminary vision suggests that there is no single solution for protecting IoT devices from threats, but common strategies can mitigate risks. Researchers, companies, and manufacturers agree on the need to find comprehensive solutions for security and privacy. These strategies include algorithms, neural networks, identity-based encryption, identity and access management, and blockchain.

The literature review reveals that the diverse technologies and dynamic communication in IoT-based smart homes raise security and privacy concerns. It calls for a unified architecture, meeting security requirements, standardizing security standards, and considering interoperability, resource constraints, data volumes, and scalability in all solutions.

3. Methodology:

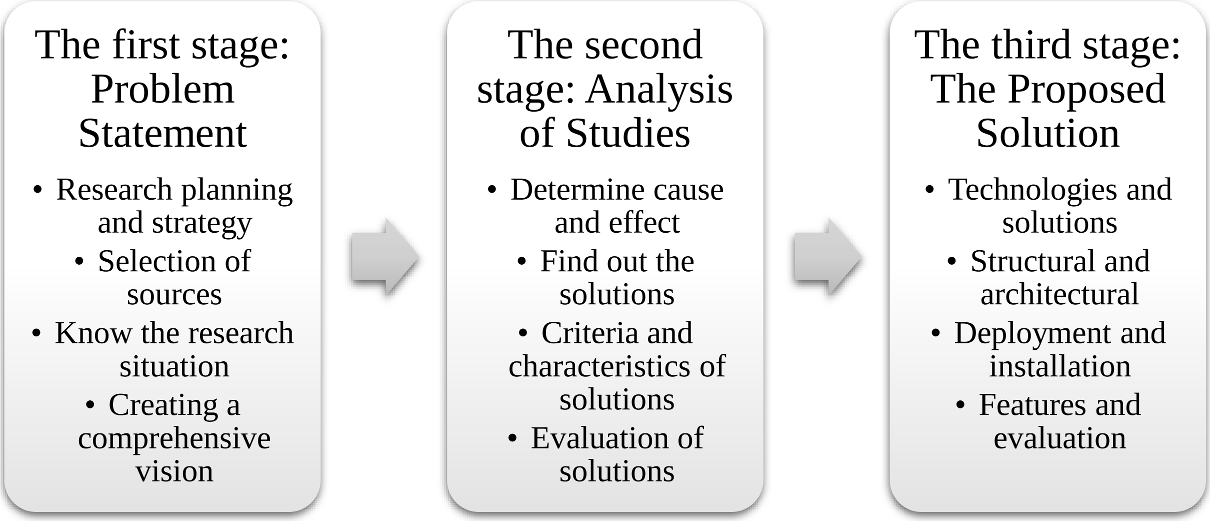
The study aims to address security and privacy concerns in smart homes based on IoT by addressing several key questions. These questions include understanding the causes, effects, and current and future measures to address these concerns, why these measures have not completely resolved them, and the most crucial question how to find comprehensive solutions to these concerns and threats. The problem statement and research questions indicate that the study is qualitative secondary research. Will use a three-stage methodology, each stage has its procedures, mechanisms, and results. These stages are described as follows:

1. The first stage: This stage will build an understanding of the basis of the research problem by knowing the current and future research status it, using the systematic review methodology (SLR) to form a complete picture of the problem statement and extract evidence and results that can be used in the advanced stages of research. (SLR) is divided into three phases[23][24]. The planning phase involves developing a strategy for gathering studies and research, defining research questions, and identifying current problems. Searches were conducted on various indexing sites, focusing on terms like "Internet of Things and Smart Home Application," "IoT-Based Smart Home Challenges," "Concerns - Issues - problems," "Addressing - Solutions - Protection," and "Security and Privacy" for the Smart Home. The review stage involves selecting sources, evaluating their quality, and extracting knowledge. The research is critically analyzed, examining the abstract, problem statement, hypothesis, technique, discussion, and conclusion. The final selection of the study comes after the initial selection and completion of the read the full text. The Al-Rayyan tool was used in the evaluation and filtering process, allowing to creation and collaborate of systematic reviews[25]. The final stage of screening involves reading the full text and selecting studies that address the issue, with 35 sources involved.

2. The second stage (Analysis of studies): Smart home users suffer from data loss due to cyber-attacks targeting IoT-based systems. The main attacks include Malware - Man-in-the-middle (MITM) and Social Engineering - Denial of Service (DoS), compromising data confidentiality, availability, and integrity. A study explores security solutions for smart homes, including encrypting data, using blockchain technology, implementing AI-based security mechanisms, and using Identity and Access Management (IAM) techniques. The aim is to propose a comprehensive security framework that addresses all security threats in a single package. The study aims to address the interoperability, scalability, and usability features of smart home security solutions. It will focus on the ability of the security solution to effectively interact with various smart home devices and platforms, support communication protocols used by these devices, and support data exchange between system components. It will also examine the security solutions, through an evaluation model consisting of questions that check whether solutions possess the required characteristics, these questions are extracted from the system environment. They verify the solution's ability to handle increased data traffic and processing demands without compromising performance or latency. The model will also examine the security solution's flexibility to accommodate a growing network infrastructure and its ability to integrate with cloud-based services or platforms to offload processing and storage needs. The focus will be on the security solution's ease of installation and configuration, its easy-to-use interface for configuration and management, and its multi-user support, allowing different family members to have their accounts and access controls.

3. The third stage: Developing a comprehensive security framework proposal that covers all security vulnerabilities and cyber threats and meets the standards that were produced from the

previous stage to give the proposal characteristics that achieve its goal, which is an integrated and comprehensive solution to security and privacy concerns that cause the loss of system security requirements.



The first stage: Problem Statement

- Research planning and strategy
- Selection of sources
- Know the research situation
- Creating a comprehensive vision

The second stage: Analysis of Studies

- Determine cause and effect
- Find out the solutions
- Criteria and characteristics of solutions
- Evaluation of solutions

The third stage: The Proposed Solution

- Technologies and solutions
- Structural and architectural
- Deployment and installation
- Features and evaluation

The figure3.1shows the stages of the methodology applied in the study and its main steps

4. Result:

This research aims to find complete and integrated solutions to security and privacy concerns in IoT-based smart homes. Four cybersecurity technical solutions were chosen to address multiple security threats simultaneously, work within multiple architectural layers, and secure more than one component of the system. These solutions have been developed based on criteria derived from reviewing studies and their feasibility in a smart home system environment. The results of the evaluation were as follows:

Table 4.1 Evaluation of selected technologies for security solutions that meet the requirements of the required characteristics

	Encryption Techniques	Blockchain Technology	Security Mechanisms based on AI	IAM Techniques
Interoperability	100%	100%	100%	100%
Scalability	50%	50%	100%	100%
Usability	33%	33%	66%	66%
Result	61%	61%	88.60%	88.60%

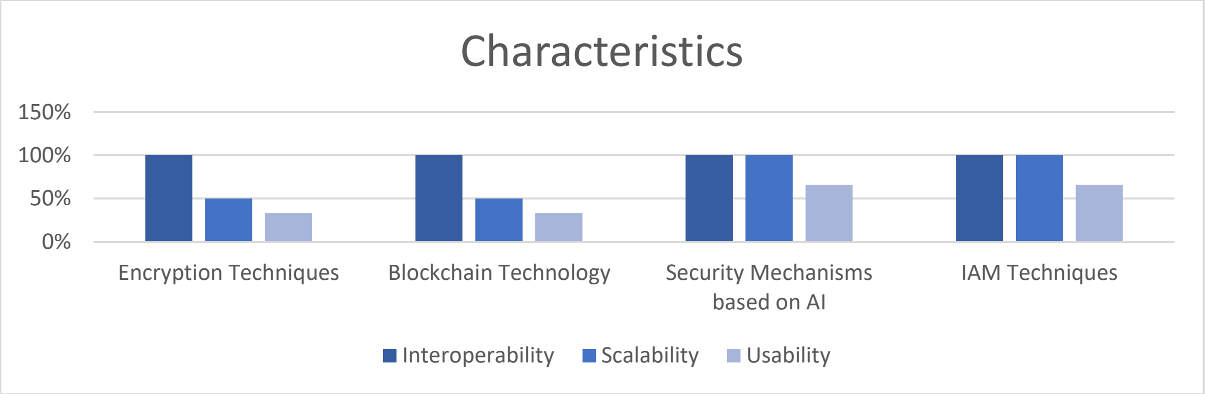


Figure 4.1 The percentage of security solutions achieving the required characteristics according to the selected studies

Looking at the evaluation results, it became clear that all security technical solutions cannot work alone to address all threats and all stakeholders' security concerns, for the reasons and criteria mentioned previously, which are related to the system environment and characteristics. Furthermore, the differences in these solutions' possession of the characteristics required in the system environment make it impossible to use a single security solution; however, by integrating, they can provide the system with the necessary security requirements and gain user confidence.

This is the main reason and real motivation for our study, which is to find a comprehensive and integrated solution to all these vulnerabilities and threats that raise concerns among stakeholders interested in implementing an IoT-based smart home.

4.1 The Need for Comprehensive and Integrated Solutions:

An integrated solution is a comprehensive security system that integrates various technologies and processes, such as firewalls, intrusion detection systems, antivirus software, and access control systems, to create a seamless and effective security posture against various threats. This approach uses a standardized collection of settings, rules, policies, and procedures to protect all network security workloads. The system provides a single solution for each service type and technology, including on-premises, hybrid resources, and cloud-based services like IaaS or container hosting. This eliminates the cost and hassle of providing, administering, and scaling security software for each specific task, ensuring the latest security technology and updates are delivered quickly and consistently[26][27]. A comprehensive security strategy should include policies for handling incidents, regular assessments to identify vulnerabilities, and employee training to promote good security hygiene. Combining an integrated solution with a broader strategy allows organizations to create a holistic approach to security, better addressing the constantly evolving threat landscape[28].

4.2 The Proposed Integrated Solution:

An integrated solution is a comprehensive security approach that combines various security technologies and processes into a single system, ensuring a more effective defense against various threats. This includes firewalls, intrusion detection systems, antivirus software, and access control systems. The integrated solution uses a standardized collection of settings, rules, policies, and procedures to protect all network security workloads. It offers a single solution for each service type and technology, including on-premises and hybrid resources, as well as cloud-based services like IaaS or container hosting environments. This eliminates the need for supplying, administering, and scaling security software for each specific task, resulting in faster and more consistent security technology and upgrades. However, an integrated solution is only one aspect of a broader security strategy that should include policies for handling security incidents, regular security assessments, employee training, and awareness programs. Combining an integrated solution with a broader security strategy allows organizations to create a more holistic approach to security, better addressing the constantly evolving threat landscape.

The proposed integrated solution for smart home security and privacy consists of a multi-layered system that includes hardware and software components. The Getaway Layer is responsible for connecting devices and systems within the home and to the external network, ensuring privacy and integrity. Key components of this layer include firewalls, secure communication protocols, authentication and authorization, and Virtual Private Networks (VPNs).

The Data Layer manages and secures data generated by various devices and systems within the home, storing, processing, and transmitting it while ensuring its CIA triad. Security technologies in the Data Layer include data encryption using cryptographic algorithms such as AES & RSA, hash functions like SHA-256, SHA-3, or MD5, key exchange protocols like Diffie-Hellman, and secure hashed password storage. Access control management is crucial in data layer security, ensuring that only authorized individuals or devices can access and modify data.

User authentication involves authentication methods such as passwords, biometrics, or two-factor authentication (2FA) to verify the identity of clients and control access to APIs. Device authentication involves assigning a unique identifier or token, and authentication mechanisms like cryptographic keys or certificates are used to verify the device's identity before granting access. Access control policies specify permissions and privileges assigned to smart home ecosystem users or entities, with fine-grained access control techniques like role-based access control (RBAC) or attribute-based access control (ABAC) implemented.

Smart contracts are self-executing agreements with pre-defined rules and conditions encoded on the blockchain. These contracts determine who can access specific data, under what conditions, and for what purposes. Maintaining access logs and auditing mechanisms within the data layer helps track data accesses, modifications, and user activities, enabling the detection of unauthorized access attempts, suspicious behavior, and potential security breaches.

Data anonymization refers to the act of deleting or obscuring personally identifiable information (PII) from acquired data to maintain privacy and preserve individuals' identities. Differential privacy techniques can be applied to add noise or randomness to computations or queries performed on the data, providing a mathematical guarantee of privacy. Secure Multi-Party Computation (SMPC) protocols can be used to perform computations on encrypted data without revealing the underlying sensitive information, preserving privacy.

Data backup and recovery are essential for data availability and resilience. Blockchain can provide specific data backup and recovery methods, such as immutable data storage, which ensures data is resistant to tampering or accidental loss.

The proposed integrated solution for smart home security and privacy combines hardware and software components to address various vulnerabilities and mitigate cyber-attacks. By implementing these security measures, the system can provide a comprehensive and effective solution for protecting users' personal and sensitive data in the context of smart home technology.

4.3 Installation of Integrated Solution:

The integration of security technologies and solutions in a smart home system requires a common working platform that allows them to work together, eliminate differences, complement each other's shortcomings, and enhance their capabilities[29]. This results in a strong security posture that enhances system deployment and user adoption. The middleware layer, which consists of several security technologies and tools, is crucial in deploying integrated security solutions. By deploying middleware technologies, integrated security solutions can provide a layer of abstraction between different components of the security system, enabling them to communicate and exchange data in a standardized and flexible way.

Middleware technologies provide a set of common interfaces, protocols, and standards that enable different components of the security system to work together seamlessly, regardless of their underlying technology or platform. It also offers advanced features and capabilities that enhance the security system's effectiveness and efficiency.

Some essential middleware layers for integrating smart home security solutions include Application Programming Interfaces (APIs) [30], Data Access Middleware, Message-Oriented Middleware (MOM), and Service-Oriented Architecture (SOA) [31]. APIs enable seamless communication and interoperability between different software applications and hardware devices in a smart home security system, while MOM facilitates reliable and effective communication between various hardware and software components. SOA can be used to expose security services as APIs, enabling other applications to access these services and make decisions based on real-time data[32].

Smart home integrated security solutions in the middleware layer provide a common platform for communication and interoperability among various software applications, hardware devices, and platforms, enabling a unified and seamless security solution that protects against a broad range of security threats. By employing middleware technologies, smart home integrated security solutions can improve protection and detection capabilities, reduce the risk of security breaches, and protect critical information and resources[33][34].

4.4 Features of the Proposed Solution:

The proposed solution provides operational and technological advantages for smart homes, including[35][36], [37]:

- Centralization of management.
- Flexibility and interoperability.
- Scalability.
- Multi-layered security solutions.
- Comprehensive security posture.
- Severe consequences of breaches.
- Provides a centralized platform for device administration, security management, and event management.

4.5 Architecture for Implementation and Operation:

The middleware layer in an IoT-based smart home architecture can be implemented in various locations, depending on the system's design and needs. Cloud-based middleware allows for centralized management and scalability, while edge-based middleware allows local data processing and real-time decision-making on IoT devices at the network's edge. This method reduces dependency on cloud or centralized services. Another option is to place the middleware layer within a gateway device, which acts as a central hub in the smart home, linking IoT devices to the external network. This allows communication, data processing, and other middleware functions.

In the security solution, we proposed that deploying gateway-based middleware is preferred, since adopting gateway-based middleware in the smart home architecture gives several advantages over alternative deployment options, the most important of which is having an easy-to-use and familiar user interface, here are some of the main advantages:

- Centralized administration
- Improved Communication and Integration
- Localized Processing and Reduced Latency
- Offline Functionality
- Reduced Network Traffic
- Scalability and Flexibility
- Improved Privacy and Security

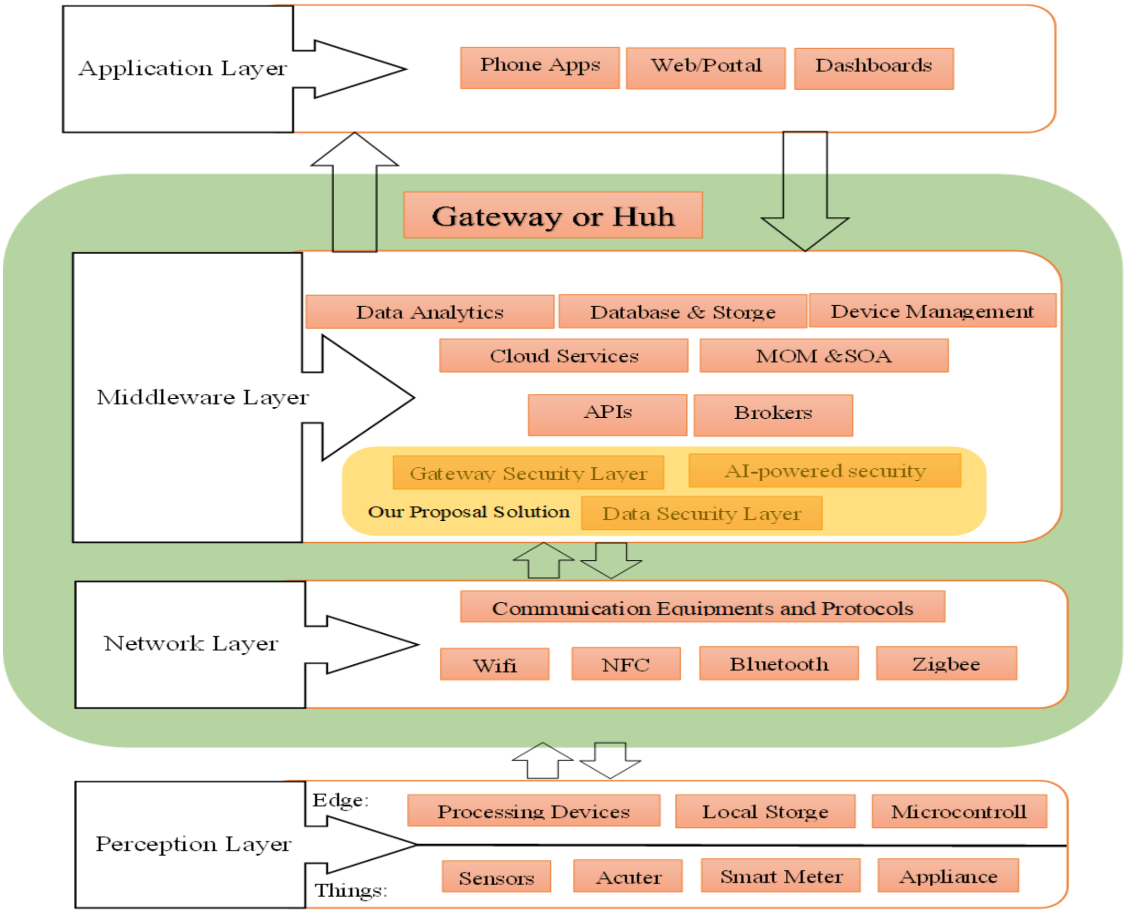


Figure 4.2 shows the smart home's architectural design, demonstrating where the proposal security solution was installed via the middleware layer.

Figure 4.2 The smart home's architectural design and our proposal Solution

5. Conclusion & Future Directions:

5.1 Conclusion:

The study delved into a critical research problem by reviewing relevant studies, identifying concerns, their types, classifications, causes, and impact, and the solutions and procedures used to prevent, mitigate, and evaluate these issues that hinder the adoption of IoT-based smart home applications by users. The summary of what was realized from our study is that:

- The diverse nature of IoT-based smart home technologies and equipment, as well as the dynamic nature of connections and data sharing between them, are important reasons for security and privacy issues.
- Create a unified architecture that encompasses procedures and technology that aid in the protection of privacy and security.
- All solutions must meet to Security requirements (confidentiality, availability, and integrity).
- Standardization of security standards to ensure the application's trustworthiness.
- Interoperability, resource limits, big data, usability, and scalability must all be considered in all solutions.
- All the security solutions and procedures put in place to protect stakeholders' privacy cannot operate alone since they cannot cover all risks without integrating with other solutions and procedures.
- The necessity of legislators in countries to create and enforce regulations, including international law, to prevent huge corporations and service providers from exploiting user data in their commercial operations and policies.
- The end user is one of the most crucial pillars of the system's success, and must be cyber-educated to protect himself and hence the system's success.

To address security concerns, an integrated security environment is needed, integrating software and physical components. A multi-layered security framework is proposed, allowing interoperability and scalability. This system consists of mechanisms and procedures compatible with various components, making system management easier. Modern technologies, such as artificial intelligence, are used to manage vulnerabilities and threats, and data encryption through blockchain and access management policies. This solution provides a unified user face for system management.

5.2 Future Directions:

The development of IoT-based smart homes has raised security and privacy concerns. Future studies should explore these areas to understand their impact and potential solutions. This will help anticipate challenges and opportunities, ensuring smart homes continue to enhance our lives, provide convenience, and contribute to a sustainable and connected future. Examining technologies, procedures, and mechanisms can help.

Threat modeling and risk assessment are crucial in identifying potential vulnerabilities and prioritizing security solutions in smart home environments. Blockchain technology can enhance security and privacy by developing decentralized authentication mechanisms, secure data-sharing protocols, and tamper-proof audit trails. This technology can provide a transparent and immutable record of smart home operations, ensuring data integrity and enabling secure interactions between devices and users. However, the scalability problem and storage size of this data pose challenges to its use.

AI security and privacy techniques are essential for addressing security and privacy concerns in IoT applications, including smart homes. These techniques enable the analysis of sensitive data while minimizing the risk of unauthorized access, data breaches, or misuse of personal information. By incorporating privacy-preserving algorithms, federated learning approaches, or edge computing solutions, individuals can benefit from AI-driven technologies while maintaining control over their data and ensuring privacy is respected.

Usable security and privacy interfaces are essential for empowering individuals to manage the security and privacy settings of their smart home devices effectively. Research can explore innovative ways to present complex security and privacy information to users, provide clear control mechanisms, and ensure transparency in data collection and sharing practices.

Secure cloud integration is crucial for smart home systems, as it introduces security and privacy risks. Future research should focus on developing secure cloud integration mechanisms, including end-to-end encryption, secure data transmission protocols, and secure data storage practices.

Wearable sensors in the smart home context present an avenue for future exploration, with a particular focus on enhancing security and privacy measures. Advanced sensor technologies offer promising avenues for improved accuracy and reliability in the smart home environment. For example, optical sensors can facilitate precise monitoring of heart rates, while ultra-low-power sensors can extend battery life. Researchers may also consider integrating wearable sensors with other smart home devices to foster a more intelligent living space.

Ethical and legal considerations are necessary as smart home technologies become more widespread. Research could investigate issues such as data ownership, consent, algorithmic bias, and the potential impact of smart home systems on individuals and society. This research can contribute to the development of ethical frameworks and guidelines for the dissemination and responsible use of smart home technologies.

6. Reference:

1. R. A. Radouan Ait Mouha, "Internet of Things (IoT)," *J. Data Anal. Inf. Process.*, vol. 09, no. 02, pp. 77–101, 2021, doi: 10.4236/jdaip.2021.92006.
2. J. Singh, M. Kumar, A. Sharma, G. Pandey, K. Chae, and S. Lee, "We are IntechOpen, the world ' s leading publisher of Open Access books Built by scientists, for scientists TOP 1 %," *Intech*, vol. 11, no. tourism, p. 13, 2019, [Online]. Available: https://www.intechopen.com/books/advanced-biometric-technologies/liveness-detection-in-biometrics
3. statista, Ed., "Smart Home - Worldwide," 2023. https://www.statista.com/outlook/dmo/smart-home/worldwide
4. L. K. Ramasamy and S. Kadry, "Internet of things (IoT)," *Blockchain Ind. Internet Things*, no. May, 2021, doi: 10.1088/978-0-7503-3663-5ch1.
5. F. ZARO, A. TAMİMİ, and A. BARAKAT, "Smart Home Automation System," *Int. J. Eng. Innov. Res.*, no. 04, pp. 1785–1789, 2020, doi: 10.47933/ijeir.781091.
6. R. Hassan, F. Qamar, M. K. Hasan, A. H. M. Aman, and A. S. Ahmed, "Internet of things and its applications: A comprehensive survey," *Symmetry (Basel).*, vol. 12, no. 10, pp. 1–29, 2020, doi: 10.3390/sym12101674.
7. D. Mocrii, Y. Chen, and P. Musilek, "IoT-based smart homes: A review of system architecture, software, communications, privacy and security," *Internet of Things (Netherlands)*, vol. 1–2, pp. 81–98, 2018, doi: 10.1016/j.iot.2018.08.009.
8. H. Verma, M. Jain, K. Goel, A. Vikram, and G. Verma, "Smart home system based on Internet of Things," *Proc. 10th INDIACom; 2016 3rd Int. Conf. Comput. Sustain. Glob. Dev. INDIACom 2016*, pp. 2073–2075, 2016, doi: 10.5772/intechopen.84894.
9. M. Jyotsna, P. Gabhane, M. Shradha Thakare, and M. Craig, "Smart Homes System Using Internet-of-Things: Issues, Solutions and Recent Research Directions," *Int. Res. J. Eng. Technol.*, 2017, [Online]. Available: www.irjet.net
10. T. Malche and P. Maheshwary, "Internet of Things (IoT) for building smart home system," *Proc. Int. Conf. IoT Soc. Mobile, Anal. Cloud, I-SMAC 2017*, no. February 2019, pp. 65–70, 2017, doi: 10.1109/I-SMAC.2017.8058258.

11. B. Ali and A. I. Awad, “Cyber and physical security vulnerability assessment for IoT-based smart homes,” *Sensors (Switzerland)*, vol. 18, no. 3, pp. 1–17, 2018, doi: 10.3390/s18030817.
12. T. Nandy *et al.*, “Review on Security of Internet of Things Authentication Mechanism,” *IEEE Access*, vol. 7, pp. 151054–151089, 2019, doi: 10.1109/ACCESS.2019.2947723.
13. G. Singh, K. Mehta, and H. Singla, “Security Concerns of Smart Homes and Its Solutions,” *Adv. Appl. Math. Sci.*, vol. 19, no. 6, pp. 543–549, 2020.
14. F. K. Gondal, “Security and Privacy Challenges for theIOT-based Smart Homes with Limited Resources and Adoption Immaturity,” *Innov. Comput. Rev.*, vol. 1, no. 1, 2021, doi: 10.32350/icr.0101.04.
15. L. Nemec Zlatolas, N. Feher, and M. Hölbl, “Security Perception of IoT Devices in Smart Homes,” *J. Cybersecurity Priv.*, vol. 2, no. 1, pp. 65–74, 2022, doi: 10.3390/jcp2010005.
16. K. Sarwar, S. Yongchareon, and J. Yu, *A brief survey on IoT privacy: Taxonomy, issues and future trends*, vol. 11434 LNCS, no. September. Springer International Publishing, 2019. doi: 10.1007/978-3-030-17642-6_18.
17. K. Yu, Q. Li, and D. Chen, “IoT Privacy Preserving in Modern Smart Homes”, [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2017/03/30/fcc
18. T. Yang, G. Zhang, Y. Li, Y. Yang, H. Wang, and Y. Zhang, “Detecting Privacy Leakage of Smart Home Devices through Traffic Analysis,” *Secur. Commun. Networks*, vol. 2022, 2022, doi: 10.1155/2022/5655314.
19. J. C. S. Sicato, P. K. Sharma, V. Loia, and J. H. Park, “Vpnfilter malware analysis on cyber threat in smart home network,” *Appl. Sci.*, vol. 9, no. 13, pp. 1–20, 2019, doi: 10.3390/APP9132763.
20. S. Aljanah, N. Zhang, and S. W. Tay, “A Survey on Smart Home Authentication: Toward Secure, Multi-Level and Interaction-Based Identification,” *IEEE Access*, vol. 9, pp. 130914–130927, 2021, doi: 10.1109/ACCESS.2021.3114152.
21. M. A. Nassiri Abrishamchi, A. Zainal, F. A. Ghaleb, S. N. Qasem, and A. M. Albarrak, “Smart Home Privacy Protection Methods against a Passive Wireless Snooping Side-Channel Attack,” *Sensors*, vol. 22, no. 21, pp. 1–21, 2022, doi: 10.3390/s22218564.
22. V. Kumar, N. Malik, J. Singla, N. Z. Jhanjhi, F. Amsaad, and A. Razaque, “Light Weight Authentication Scheme for Smart Home IoT Devices,” *Cryptography*, vol. 6, no. 3, 2022, doi: 10.3390/cryptography6030037.
23. G. Lame, “Systematic literature reviews: An introduction,” *Proc. Int. Conf. Eng. Des. ICED*, vol. 2019-Augus, no. July, pp. 1633–1642, 2019, doi: 10.1017/dsi.2019.169.
24. S. Outsourcing and R. Trust, “Systematic Literature Review Protocol for,” no. October 2015, pp. 1–40, 2020.
25. “Rayyan - {AI} {Powered} {Tool} for {Systematic} {Literature} {Reviews},” Sep. 2023.
26. “United Nations Cybersecurity in the United Nations system organizations,” 2021.
27. C. G, “What is {IoT} integration, and why is it important for {IoT} solutions?” 2022.
28. “What is {Information} {Security} {Management} {System} ({ISMS})?” Sep. 2022.
29. Z. Ali *et al.*, “A Generic Internet of Things (IoT) Middleware for Smart City Applications,” *Sustainability*, vol. 15, no. 1, 2023, doi: 10.3390/su15010743.
30. L. Hogie, “Idawi : a middleware for distributing applications in the IOT , the fog and other multihop dynamic networks,” pp. 1–36, 2022.
31. I. Gamal, H. Abdel-Galil, and A. Ghalwash, “Osmotic Message-Oriented Middleware for Internet of

Things," *Computers*, vol. 11, no. 4, 2022, doi: 10.3390/computers11040056.

32. Y. Mesmoudi, M. Lamnaour, Y. El Khamlichi, A. Tahiri, A. Touhafi, and A. Braeken, "A Middleware based on Service Oriented Architecture for Heterogeneity Issues within the Internet of Things (MSOAH-IoT)," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 32, no. 10, pp. 1108–1116, 2020, doi: https://doi.org/10.1016/j.jksuci.2018.11.011.
33. P. Agarwal and M. Alam, "Investigating IoT Middleware Platforms for Smart Application Development BT - Smart Cities—Opportunities and Challenges," S. Ahmed, S. M. Abbas, and H. Zia, Eds., Singapore: Springer Singapore, 2020, pp. 231–244.
34. Q. Alfalouji *et al.*, "IoT Middleware Platforms for Smart Energy Systems: An Empirical Expert Survey," *Buildings*, vol. 12, no. 5, pp. 1–23, 2022, doi: 10.3390/buildings12050526.
35. S. M. M. Gilani, M. Usman, S. Daud, A. Kabir, Q. Nawaz, and O. Judit, "SDN-based multi-level framework for smart home services," *Multimed. Tools Appl.*, 2023, doi: 10.1007/s11042-023-15678-2.
36. Y. Wan, K. Xu, G. Xue, and F. Wang, "IoTArgos: A Multi-Layer Security Monitoring System for Internet-of-Things in Smart Homes," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, 2020, pp. 874–883. doi: 10.1109/INFOCOM41043.2020.9155424.
37. D. Popescu, D. Rusu, L. Bacali, and S. Popescu, "Multi-layered Functional Analysis for Smart Homes Design," *Procedia - Soc. Behav. Sci.*, vol. 238, pp. 114–123, 2018, doi: 10.1016/j.sbspro.2018.03.014.