AN INTELLIGENT FRAMEWORK FOR SMART HOME SECURITY AND AUTOMATION

A. Barkat[1], W. Azeem[2], and A. A. Malik[3]

[1]Department of Data Science, Lahore Garrison University, Lahore, 54000, Pakistan
[2]Department of Software Engineering, Lahore Garrison University, Lahore, 54000, Pakistan
[3]Department of Forensic and Criminology, Lahore Garrison University, Lahore, 54000, Pakistan

ABSTRACT: Smart home automation, security, and energy efficiency have all been transformed by the quick adoption of the Internet of Things (IoT). However, there are a number of issues with current smart home solutions, such as weak AI-driven automation, limited interoperability, dependence on third-party cloud services, and cybersecurity concerns. Through a hybrid IoT architecture that combines edge and cloud computing, end- to-end encryption, biometric authentication, and decentralized data storage, this research suggests a full smart home security and automation application that overcomes these constraints. Moreover, Predictive security measures and AI-driven automation are being used to improve threat detection and optimize energy use. Multi-platform compatibility, enhanced robustness, and increased user control over data privacy are all guaranteed by the suggested framework. This study supports the goal of sustainable and cyber-resilient smart cities by filling in the gaps and advancing the creation of a safe, intelligent, and scalable smart home ecosystem.

Index Terms: IOT, smart home, home automation, home security, AI driven Automation, Internet of things.

(Received 11.07.2024 Accepted 01.09.2024)

INTRODUCTION

The "2023 Global Smart Home Market Report" projects that the worldwide smart home market will generates US$139.3 billion in revenue overall in 2023 and will expand at a 50.01% annual rate over the following four years to reach US$222.9 billion in 2027 [1]. With these characteristics serving as stepping stones to introduce the notion, the smart home concept is continually evolving. Although this idea has more potential for the future, the primary query is why it hasn't been applied more widely yet.

There are multiple answers to this question [2]. The first reason is that most of the time, the bulk of people cannot afford the adoption of smart gadgets. The second problem stems from the implementation's frequent lack of flexibility or portability in the event that the user wants to move any of the devices. The third issue is because the device's durability is strongly correlated with its cost [3][4].

The integration of the Internet of Things (IoT) in smart homes and smart cities has significantly enhanced convenience, automation, and security. Smart home applications enable users to remotely control appliances, monitor security, and optimize energy consumption. However, as these systems become more interconnected, they are increasingly vulnerable to cyber threats, unauthorized access, and device interoperability issues. Ensuring secure and reliable communication between IoT devices while maintaining user privacy remains a key challenge in smart home development. This research focuses on designing a comprehensive smart home security and automation application that addresses the limitations identified in existing studies. Other studies explore smart home solutions using Android applications, Firebase, and cloud-based security mechanisms, yet they face issues such as weak encryption, network dependency, and limited cross-platform integration. Additionally, while some systems incorporate artificial intelligence (AI) for automation, machine learning-based decision- making remains underdeveloped. The proposed application aims to overcome these challenges by integrating end-to-end encryption, biometric authentication, and decentralized data storage to enhance security. Additionally, it leverages machine learning algorithms for energy- efficient automation and predictive security measures. A hybrid IoT architecture combining cloud and edge computing will be explored to reduce reliance on third- party platforms while improving system resilience.

A. Motivation and Scope: The motivation behind this research stems from the increasing cyber security threats targeting smart homes. Many existing solutions rely on cloud services such as Firebase and Google Assistant, creating vulnerabilities related to unauthorized access and data breaches. Additionally, smart home users often lack awareness and control over their data, further exacerbating security risks. This research aims to bridge these gaps by developing an intelligent, adaptive, and secure smart home application that integrates multi-platform interoperability, AI- driven decision-making, and enhanced privacy controls. The scope of this research includes designing, implementing, and evaluating a cost-effective, scalable smart home security and automation system that can operate efficiently across various IoT devices and communication protocols. By addressing the security, privacy, and automation challenges identified in previous studies, this research contributes to the development of a more resilient and intelligent smart home ecosystem, ultimately supporting the vision of secure and sustainable smart cities.

LITERATURE REVIEW

Jacobsson and Davidsson (2015) propose a security and privacy model for smart homes based on a systematic risk analysis. The study identifies human factors, software vulnerabilities, and network communication risks as key concerns. Their model suggests integrating security and privacy measures from the design phase rather than as an afterthought [5]. The paper provides a theoretical model but lacks practical implementation or real-world testing. Additionally, while the study acknowledges human factors, it does not provide specific solutions for enhancing user awareness and control over their data. S. Sarkat *et al.* discussed a smart home security system leveraging an Android application, Firebase, and IoT technology. The system includes PIR motion, flame, and smoke sensors to detect intrusions and hazards, sending alerts to Firebase, which then notifies users via an Android app. The study highlights affordability and flexibility but points out challenges like network dependency and the need for improved data security [5]. V. D. Vaidya *et al.* compares different smart home technologies, including GSM, Bluetooth, IoT, and PIC microcontrollers with ZigBee. Each technology has unique advantages: GSM allows remote control via SMS, Bluetooth is cost-effective but range-limited, and IoT enables real-time automation through cloud services. The study concludes that IoT- based solutions offer the best balance of automation and security, though sensor failures remain a concern [7]. T. Chaurasia *et al.* focuses on improving smart home security and automation by reducing computational overhead. It integrates authentication mechanisms and machine learning-based automation to predict user preferences. The system eliminates the need for a local gateway, using cloud-based authentication and Google security mechanisms. While enhancing security, the system still requires improvements in encryption techniques and AI-driven automation [8]. There are some security concerns about above mentioned papers:

- Most systems rely on cloud-based security but lack robust encryption mechanisms.
- Vulnerabilities exist due to reliance on third-party plat- forms like Firebase and Google Assistant
- Potential risks from unauthorized access and hacking remain unaddressed.
- Limited integration of different IoT devices and platforms across the reviewed solutions.
- Most systems focus on single-platform solutions, reducing flexibility in device compatibility.
- While some papers introduce AI for automation, ma- chine learning-driven decision-making remains underdeveloped.
- Lack of adaptive learning for user behavior and energy consumption optimization.
- Solutions relying on Wi-Fi or mobile networks may suffer from latency and outages, affecting reliability.
- GSM-based systems experience delays due to weak mobile signals.

Then Dik *et al.* (2020) explore the vulnerabilities in smart home systems due to the growing reliance on IoT devices. The study highlights critical security threats such as unauthorized access, weak encryption mechanisms, lack of soft- ware updates, and device interoperability issues. The paper also discusses existing security measures and best practices recommended by organizations like ENISA and the Cloud Security Alliance to mitigate these threats. [9] While the paper comprehensively outlines security challenges, it lacks empirical validation through case studies or practical implementation of the proposed security measures. Additionally, it does not address user behavior and awareness as a factor influencing security vulnerabilities.

A cost-effective home automation and security system using NodeMCU, Google Assistant, and IFTTT cloud services is presented by K. S. S. Javvaji *et al.* It integrates temperature, humidity, and light sensors while providing security through motion detection and automatic door locking. Voice commands via Google Assistant control various appliances. The system is energy-efficient, reducing power wastage by turning off unused appliances. The study emphasizes affordability and ease of implementation but lacks advanced AI-driven automation.

[10] Kabir *et al.* (2021) propose an IoT-based smart home automation and security system integrated with a mobile application and an assistant robot. The system enhances security and automation by providing remote monitoring, voice- controlled features, and real-time alerts. The study focuses on affordability and applicability in developing countries. [11] Although the study presents an innovative approach integrating mobile applications and robotics, it does not comprehensively address cybersecurity risks associated with IoT-based smart home automation. Additionally, scalability and interoperability challenges in multi-device environments are not explored.

People have successfully integrated the Internet of Things and smart houses in the field of intelligence in an era of rapidly advancing science and technology, as well as the emergence of the Internet of Everything [12]. Many issues with the smart home devices that are now in use remain unresolved, including how to adequately safeguard the security and privacy concerns brought on by the advancement of Internet technology [13], as well as the intricate issue of older people's discomfort with smart devices [14]. Uncertainty surrounds the success factors of smart home technologies in helping senior citizens who have dementia, cognitive decline, or decreased everyday activities in their daily lives [15]. As a result, in order to handle the sensitive aspects of the senior population's lives, specialized smart devices must be implemented [16]. Some of the more advanced systems created with smart home platforms at the moment include Zhu's design of a quick and effective smart home environment design scheme using wireless sensors and artificial intelligence technology [10], Dong *et al*.'s indoor smart home system for aging houses based on IoT sensors [17], and Yan's IoT-based smart home products for senior families [18]. Data transmission via wireless networks is made possible by the ongoing advancement of communication technology, which enhances system security and dependability, lowers maintenance costs, and improves user experience [19]. With the growth of smart houses, security systems are also progressively maturing [20]. Consequently, a security system ought to be a part of an advanced smart home system. For instance, Hardyan M *et al*. created an Arduino-based biometric smart house security system [21], Salay *et al*. created an IoT-based adaptive intrusion detection smart home system [18], and Aminu M *et al*. created an IoT-based smart home monitoring system based on NodeMCU [22].

To address the research gaps future research should be focused on:

- Implementing end-to-end encryption, biometric authentication, and decentralized data storage.
- Developing cross-platform standards for seamless integration of IoT devices.
- Leveraging machine learning for energy-efficient and context-aware automation.
- Exploring hybrid systems that combine IoT with local processing to reduce reliance on cloud services.
- Future research should focus on empirical studies assessing the effectiveness of proposed security strategies.

Additionally, user education and behavioral studies can be explored to improve security adoption among smart home users.

Table I. Comparative Analysis of Smart Home Security and Automation Solutions

Feature	**Proposed Framework**	**Jacobsson & Davidsson (2015) [4]**	**Sarkar *et al.* (2018) [5]**	**Vaidya *et al.* (2018) [6]**	**Chaurasia *et al.* (2019) [7]**	**Dik *et al.* (2020) [8]**	**Javvaji *et al.* (2020) [9]**
Security Mechanisms	End-to-end encryption, biometric authentication, blockchain	Privacy-focused security model	Cloud-based security (Firebase, Android)	GSM, IoT, Bluetooth security	Cloud authentication, Google Security	Identifies key vulnerabilities	Motion detection, door locking, IFTTT
Automation & AI	AI-driven predictive automation	No AI-based automation	Basic automation, no ML	IoT-based real-time automation	ML-based automation	No AI integration	No AI-driven automation
Interoperability	Multi- protocol support (Wi- Fi, Zigbee, LoRa)	Not addressed	Limited cross-platform support	GSM, Bluetooth, IoT integration	Requires cloud authentication	Discusses interoperabilit y issues	Limited IoT device support
Data Privacy	Blockchain- based data security	Theoretical model, no practical validation	Firebase- based security with vulnerabilities	IoT cloud-based storage	Improved encryption, no blockchain	Identifies privacy risks, lacks implementation	Cloud-based storage, no blockchain
Cloud Dependency	Hybrid cloud-edge computing	Cloud-dependent	Fully cloud-based system	IoT cloud storage	Cloud authentication dependency	Cloud vulnerabilities discussed	Uses IFTTT cloud services
Threat Detection	AI-based IDS for real-time monitoring	Identifies risks but lacks empirical testing	Alerts via Firebase, motion detection	Sensor failures remain a concern	Enhanced security mechanisms	Theoretical security measures	Motion detection, Google Assistant alerts
Scalability	Modular, easy device addition	No scalability discussion	Limited scalability, network-dependent	IoT-based, but device failures impact scalability	No cross-platform standards	Scalability issues remain unaddressed	Cost- effective, limited scalability
Energy Efficiency	AI-driven optimization based on usage patterns	Not addressed	No AI for energy management	IoT-based real-time automation	No focus on energy optimization	No energy-saving discussion	Energy efficiency through appliance control

Future studies should assess the security vulnerabilities of such systems and propose robust cybersecurity measures. Furthermore, evaluating the scalability of the proposed system in larger smart home environments could be an important area for exploration.

Proposed IoT Framework for Comprehensive Smart Home Security and Automation: The proposed IoT framework is designed to address the limitations and challenges identified in literature review section. It integrates advanced security measures, cross-platform interoperability, and AI-driven automation to create a resilient, scalable, and user-friendly smart home ecosystem. Below is a detailed explanation of the framework, including its components, technologies, and methodologies.

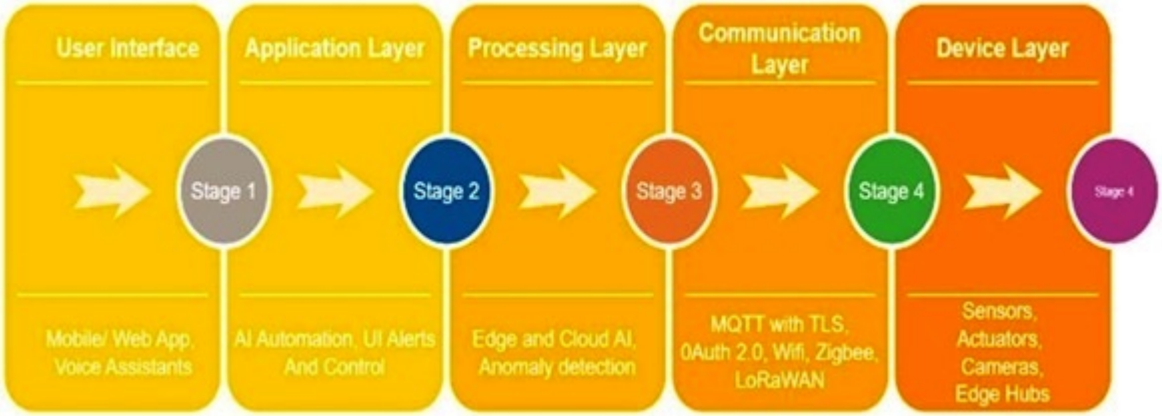
User Interface
Application Layer
Processing Layer
Communication Layer
Device Layer
Stage 1
Stage 2
Stage 3
Stage 4
Stage 4
Mobile/ Web App, Voice Assistants
AI Automation, UI Alerts And Control
Edge and Cloud AI, Anomaly detection
MQTT with TLS, 0Auth 2.0, Wifi, Zigbee, LoRaWAN
Sensors, Actuators, Cameras, Edge Hubs

Figure 1: Block Diagram of proposed IOT Framework indicating various layers that are used in this framework

A. **Framework Architecture:** The framework adopts a hybrid IoT architecture that com- bines edge computing and cloud computing to balance performance, security, and scalability. It consists of the following layers:

1) Device Layer:

- **IoT Devices:** In smart homes and buildings, a variety of sensors— including motion, temperature, humidity, smoke, gas, and water leak sensors—are essential for keeping an eye on the environment and guaranteeing safety. These sensors identify changes in their environment and cause linked IoT devices to take automated action. To create a responsive and automated living space that improves convenience, energy efficiency, and safety, these sensors integrate effortlessly with smart locks, smart lights, motorized curtains, smart plugs, and smart appliances.

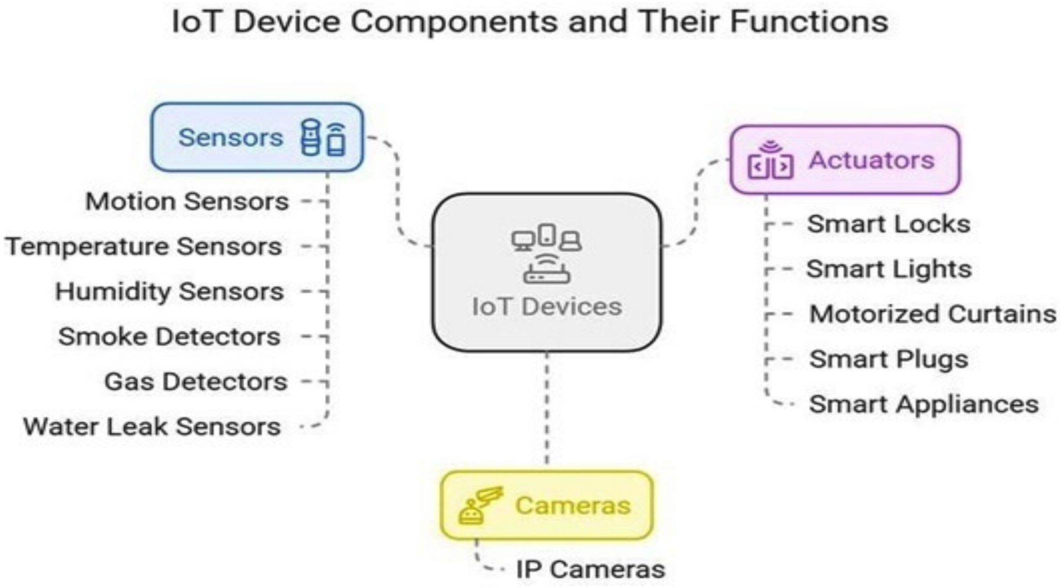

Figure 2: IOT Devices and their Functionalities

- **Communication Protocols:** Supports multiple protocols (Wi-Fi, Zigbee, Z-Wave, Bluetooth, LoRaWAN) to ensure interoperability across diverse devices.

2) Communication Layer:

Secure Communication: End-to-end encryption (e.g., AES-256) and MQTT with TLS for secure data transmission is used to Implements OAuth 2.0 for secure authentication and authorization. Moreover, in order to safeguard IoT connections, Secure MQTT (SMQTT) improves MQTT by incorporating authentication, encryption, and additional security features.

A dedicated security flag is used in SMQTT to indicate whether encryption, authentication or integrity mechanism is used. In certain implementations, brokers can enforce varying security levels according to policies by adding a security policy field.

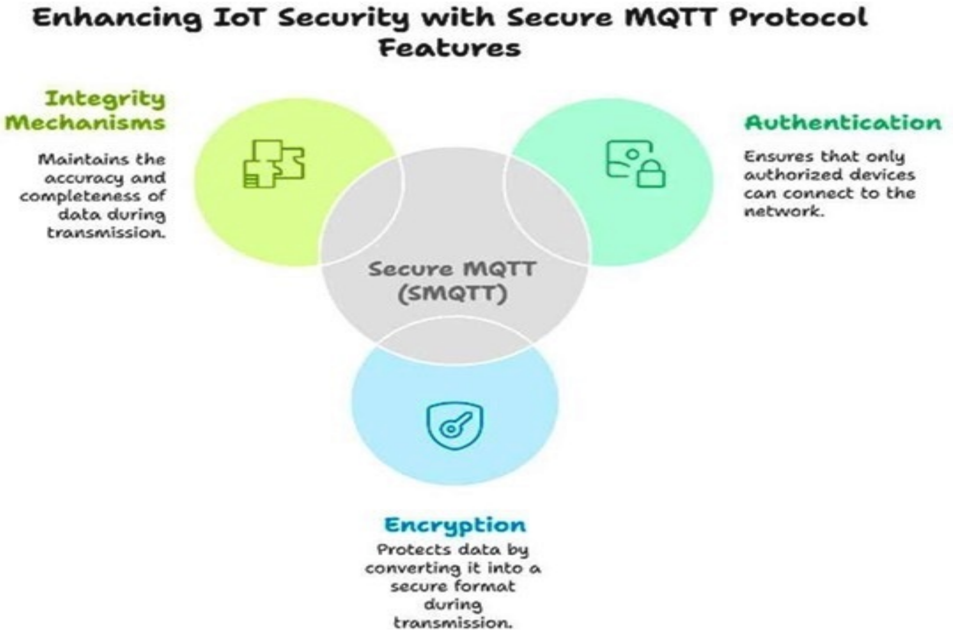
Enhancing IoT Security with Secure MQTT Protocol Features
Integrity Mechanisms
Maintains the accuracy and completeness of data during transmission.
Authentication
Ensures that only authorized devices can connect to the network.
Secure MQTT (SMQTT)
Encryption
Protects data by converting it into a secure format during transmission.

Figure 3: SQMTT Protocol features enhancing IOT security.

3) Processing Layer:

- **Edge Computing:** Local processing of critical data (e.g., motion detection, intrusion alerts) to reduce reliance on the cloud. Implements AI-based anomaly detection at the edge for real-time threat mitigation. Edge Devices. Local hubs (e.g., Raspberry Pi, NodeMCU) for preprocessing data and reducing latency. Local network (Wi-Fi, Zigbee) and cloud-based communication are combined for redundancy and reliability.

4) Application Layer:

- **Mobile/Web Application:** A cross-platform app for remote monitoring and control. Features include real-time alerts, device control, and energy consumption reports.

- **Cloud Computing:** Handles non-critical tasks (e.g., long-term data storage, user analytics) and provides scalability. Uses machine learning models for predictive automation and energy optimization.

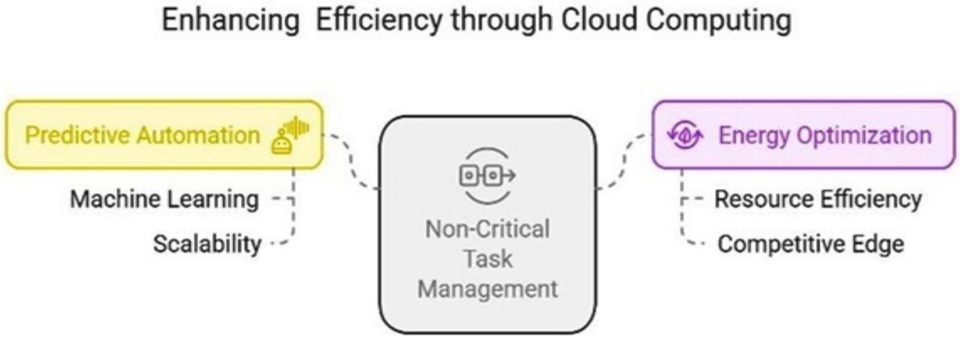

Figure 4: Cloud Computing enhancing Efficiency of Secure and Smart Automation

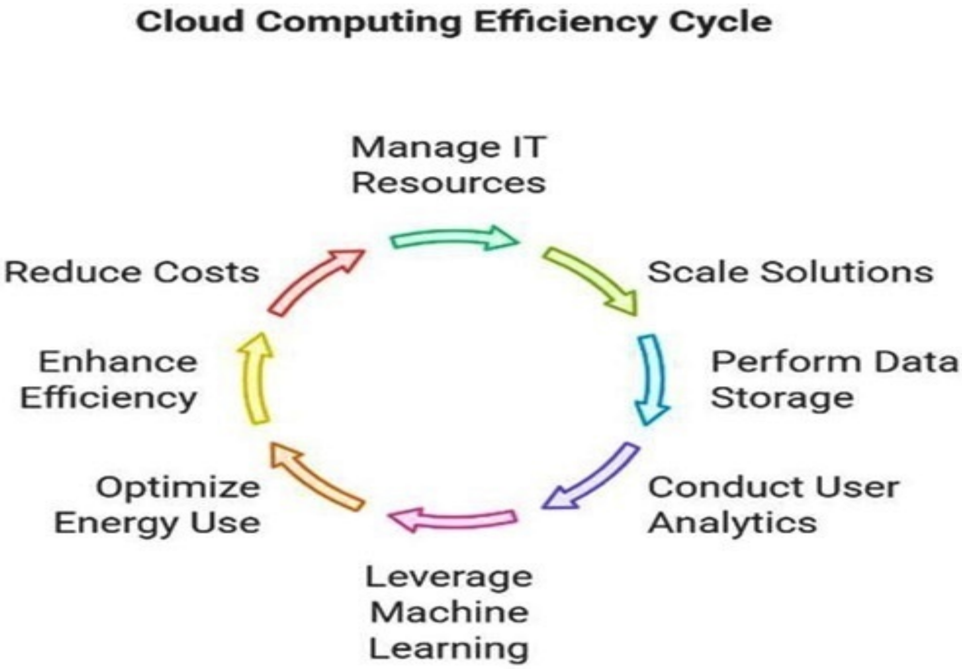

Figure 5: Cloud Computing Efficiency Cycle through multiple levels.

- **API Integration:** It allows multiple applications, services, or systems to communicate by exchanging data and functionalities. The application layer enables APIs to send and receive HTTP(S) requests between client and server applications. Integration with Google Assistant, Amazon Alexa, and Siri for voice commands is also provided. AI-Driven Automation Machine learning algorithms for predictive automation (e.g., adjusting thermostat based on user behavior) are used. Context-aware automation (e.g., turning off lights when no one is in the room) is also implemented.

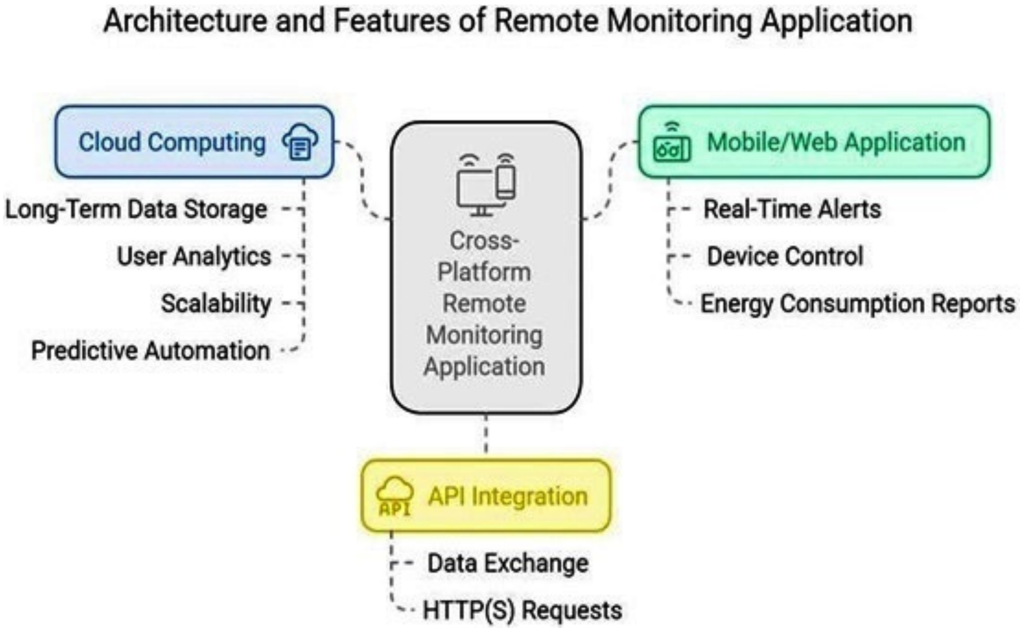

Figure 6: Remote Monitoring Application representing Architecture and Features.

- **Pub/Sub Architecture:** Publisher Creates events and messages, then forwards them to a central broker. Broker (Event Bus/Message Queue): Gets messages from publishers and forward them to the right subscribers. Subscriber pays attention to and interprets pertinent communications.

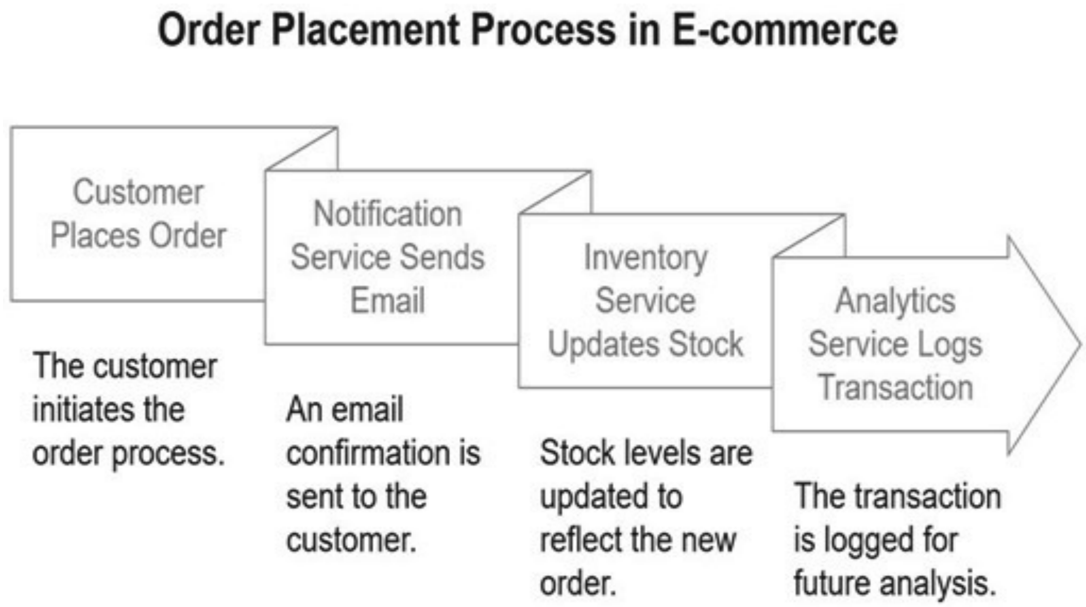
Order Placement Process in E-commerce
Customer Places Order
Notification Service Sends Email
Inventory Service Updates Stock
Analytics Service Logs Transaction
The customer initiates the order process.
An email confirmation is sent to the customer.
Stock levels are updated to reflect the new order.
The transaction is logged for future analysis.

Figure 7: A PUB/SUB Architecture Application representing the order placement process in E-Commerce

5) **Security Layer:** Only authorized users can access critical systems thanks to biometric authentication, which includes facial and fingerprint recognition. It is a very safe and easy way to manage access. By spreading data over several nodes and lowering the possibility of a single point of failure, decentralized data storage employing blockchain technology helps shield private data from unwanted access and manipulation. In order to stop possible security breaches, an AI-powered Intrusion Detection System (IDS) also continuously analyzes system activity and network traffic, identifying and thwarting cyberthreats in real-time. Regular software upgrades are carried out using automated systems to maintain a strong security posture. This guarantees that vulnerabilities are quickly fixed and that system security is continuously enhanced against changing threats.

Although both DES (Data Encryption Standard) and AES (Advanced Encryption Standard) are symmetric encryption algorithms used to protect data, they differ greatly in terms of application, security, and efficiency. While DES is antiquated and susceptible to assaults, AES is the current encryption standard because of its high security and effectiveness. AES is the recommended option for applications that need strong security.

B. Key Feature

1) ***Enhanced Security**:* **E**nd-to-End Encryption ensures data privacy during transmission. Biometric Authentication adds an extra layer of security for user access. Blockchain for Data Integrity stores logs and sensitive data in a decentralized manner to prevent tampering. AI- Based Intrusion Detection monitors network traffic and device behavior to detect anomalies.

2) ***Interoperability**:* Multi-Protocol Support ensures compatibility with various IoT devices and platforms. Cross- Platform Integration provides Seamless integration with Android, iOS, and web applications.

3) **Scalability and Resilience**: Hybrid Architecture combines edge and cloud computing to ensure system resilience and reduce latency. Modular Design allows easy addition of new devices and features.

C. **Implementation and Work Flow**

– **Device Setup:** Install IoT devices (sensors, actuators, cameras) and connect them to the local hub.

– Configure communication protocols (e.g., Wi-Fi, Zigbee).

– **Secure Communication Setup:** Implement end-to-end encryption and secure communication protocols (MQTT with TLS).

– Set up biometric authentication for user access.

– **AI and Automation Setup:** Train machine learning models using historical data for predictive automation.

– Implement AI-based intrusion detection and energy optimization algorithms.

– **Application Development:** Develop a cross-platform mobile/web app for remote monitoring and control.

– Integrate voice assistants for hands-free control.

– **Testing and Evaluation:** Test the system for security, reliability, and performance.

– Conduct user trials to evaluate usability and effectiveness.

D. **Addressing Research Gaps**

– **Security:** End-to-end encryption, biometric authentication, and blockchain-based storage address vulnerabilities in existing systems.

– **Interoperability:** Multi-protocol support and cross- platform integration ensure compatibility with diverse

IoT devices.

– **Resilience:** Hybrid architecture reduces reliance on cloud services and improves system reliability.

E. **Future Enhancements:** Applications can incorporate AI-powered user education modules to raise security awareness. These modules use machine learning algorithms to adapt training according on user behavior and possible threats. More adaptable and context-aware automation is made possible by advanced AI, especially reinforcement learning, which enables systems to dynamically modify operational settings and security procedures in response to real-time data analysis. By offering quicker and more dependable communication, seamless connectivity for IoT devices, and real-time data processing, the integration of 5G networks further improves AI-driven applications. In order to effectively power IoT networks, AI may also manage energy use by examining usage trends and incorporating renewable energy sources, like solar panels. Systems can become more intelligent, flexible, and sustainable by utilizing AI and ML in these areas.

F. **Feasibility:** The proposed framework is feasible due to multiple reasons. Increasing user knowledge is essential for security, and integrating AI-powered learning modules into apps can assist users in comprehending best practices and possible risks. Intelligent automation that dynamically adapts to changing situations is made possible by advanced AI, especially reinforcement learning, which makes systems more flexible and context-aware. These capabilities are further improved by the inclusion of 5G networks, which offer quicker and more dependable connectivity, guaranteeing smooth data flow for AI-powered apps and Internet of Things devices. Using renewable energy sources, such solar panels, to power IoT ecosystems can further increase sustainability by lowering environmental effect while preserving efficiency.

Architecture of our proposed framework can pe represented through a pictorial Diagram given below:

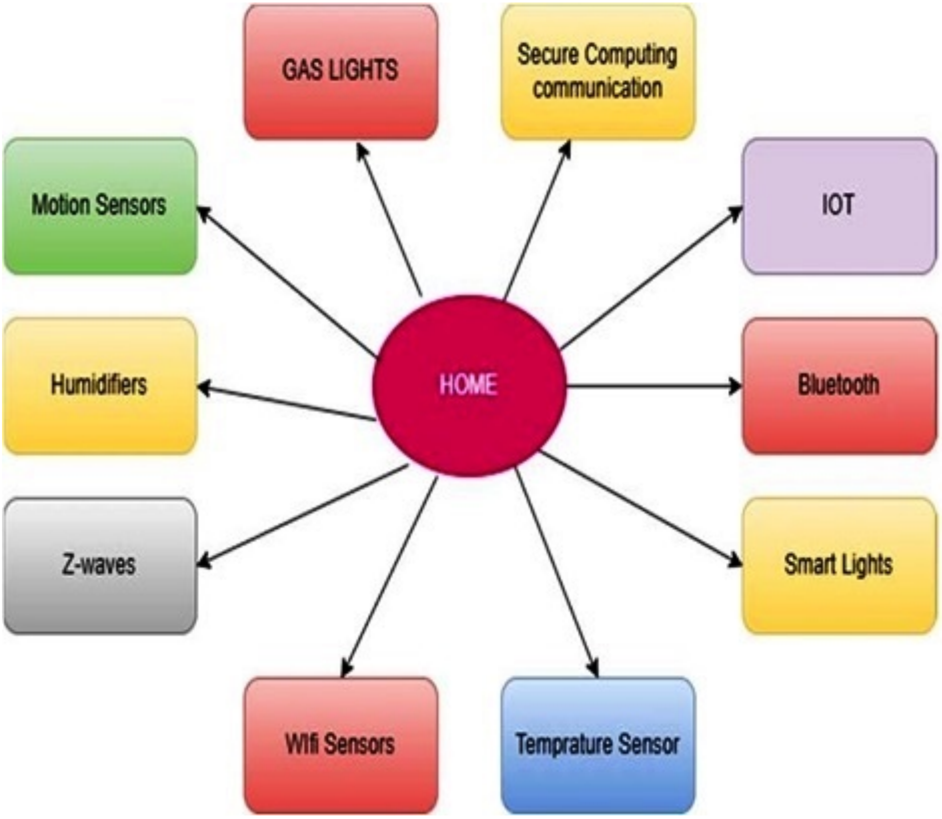

Figure 8: Architecture of proposed Framework representing A SMART Home Devices

Conclusion: This paper presents a robust and scalable IoT-based system that integrates edge and cloud computing, AI-driven automation, and enhanced security measures to optimize smart environments. By leveraging multi-protocol sup- port, AI-powered predictive automation, and blockchain for secure data storage, the proposed architecture ad- dresses key challenges in interoperability, security, and system resilience. The combination of edge and cloud computing ensures low-latency decision-making while maintaining scalability for future expansions. Through a modular approach, the system can easily adapt to new devices and evolving technologies, making it a viable solution for real-world IoT applications.

A. Future Framework: Future enhancements will focus on improving system intelligence, security, and efficiency. Key directions include:

- Developing interactive user education modules within the mobile application to enhance security awareness and best practices.
- Exploring reinforcement learning techniques for more adaptive and context-aware automation based on real-time user behavior.
- Integrating 5G technology to enhance communication speed and reliability, enabling real-time processing at the edge.
- Incorporating renewable energy sources, such as solar- powered IoT devices, to improve energy efficiency and reduce carbon footprint.
- Further investigating blockchain-based decentralized storage to enhance data privacy and integrity while minimizing reliance on centralized cloud services.

REFERENCES

1. A. Jacobsson and P. Davidsson,”Towards a model of privacy and security for smart homes,” 2015 IEEE 2nd World Forum on Internet of Things (WF- IoT), Milan, Italy, 2015, pp. 727-732, doi: 10.1109/WF-IoT.2015.7389144.
2. Internet of things. [Online]. Available: https://en.wikipedia.org/wiki/Internet of things.
3. IOT based Theft Preemption and Security System.[Online]. Available: https://www.ijirset.com/upload/2016/march/229-IOT.pdf
4. Rana , G.M.S.M., Khan, A.A.M., Hoque, M.N. and Mitul, A.F. (2013). Design and Implementation of a GSM Based Remote Home Security and Appliance Control System. Proceedings of the 2nd International Conference on Advances in Electrical Engineering, Dhaka, 19-21 December 2013, 291-295.
5. S. Sarkar, S. Gayen and S. Bilgaiyan, ”Android Based Home Security Systems Using Internet of Things(IoT) and Firebase,” 2018 International Conference on Inventive Research in Comput- ing Applications (ICIRCA), Coimbatore, India, 2018, pp. 102- 105, doi: 10.1109/ICIRCA.2018.8597197
6. V. D. Vaidya and P. Vishwakarma, ”A Comparative Analysis on Smart Home System to Control, Monitor and Secure Home, based on technologies like GSM, IOT, Bluetooth and PIC Microcon- troller with ZigBee Modulation,” 2018 International Conference on Smart City and Emerging Technology (ICSCET), Mumbai, India, 2018, pp. 1-4, doi: 10.1109/ICSCET.2018.8537381.
7. T. Chaurasia and P. K. Jain, ”Enhanced Smart Home Automation System based on Internet of Things,” 2019 Third International conference on I- SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2019, pp. 709-713, doi: 10.1109/I-SMAC47947.2019.9032685.
8. D. Dik, Y. Adamenko, E. Polyakova and A. Chelovechkova, ”Key Issues of Information Security of Smart Home Systems,” 2020 International Multi- Conference on Industrial Engineering and Modern Technologies (FarEastCon), Vladivostok, Russia, 2020, pp. 1-7, doi: 10.1109/FarEastCon50210.2020.9271347.
9. K. S. S. Javvaji, U. R. Nelakuditi and B. P. Dadi, ”IoT Based Cost Effective Home Automation and Security System,” 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020, pp. 1-5, doi: 10.1109/ICCCNT49239.2020.9225557.
10. A. Z. M. T. Kabir, A. M. Mizan, P. K. Saha, K. M. M. R. Songlap, A. J. Ta-Sin and N. A. Chisty, ”IoT Based Smart Home Automation and Security System Using Mobile App With Assistant Robot for Developing Countries,” 2021 Inter- national Conference on Electronics, Information, and Commu- nication (ICEIC), Jeju, Korea (South), 2021, pp. 1-4, doi: 10.1109/ICEIC51217.2021.9369770.
11. W. Changhui, X. Miaomiao, Indoor environment design education and smart home under the background of internet[J], Int. J. Web Based Learn. Teach. Technol. (IJWLTT) 19 (1) (2024) 1–15.
12. S. Turkyilmaz, E. Altinda, Analysis of smart home systems in the context of the internet of things in terms of consumer experience[J], Int. Rev.Manag. Market. (2022) 12.
13. R.J. Heon, J.H. Ma, S. Joonoh, *et al*., Review of

applications and user perceptions of smarthome technology for health and environmental monitoring[J], J. Comput. Des. Eng. (3) (2022) 3.

14. W. Moyle, J. Murfield, K. Lion, The effectiveness of smart home technologies to support the health outcomes of community-dwelling older adults living with dementia: a scoping review[J], Int. J. Med. Inform. 153 (2021) 104513

15. J.Y. Baek, S.H. Na, H. Lee, *et al.*, Implementation of an integrated home internet of things system for vulnerable older adults using a frailty-centered approach, Sci. Rep. 12 (2022) 1922.

16. J. Zhu, D. Wang, Y. Zhao, Design of smart home environment based on wireless sensor system and artificial speech recogni- tion[J], Measurement: Sensors 33 (2024) 101090.

17. X.C. Dong, C. Wonjun, Interior design of aging housing based on smart home system of IOT sensor[J], J. Sens. 2023 (2023).

18. J. Yan, W. Lin, X. Tu, *et al.*, IoT-based interaction design of smart home products for elderly families[J], Appl. Math. Nonlinear Sci. 9 (1) (2024).

19. N. Mehrbakhsh, R.A. Ali, S. Sarminah, *et al.*, Factors impacting customer purchase intention of smart home security systems: so- cial data analysis using machine learning techniques[J], Technol. Soc. 71 (2022).

20. Y. Pu, Smart home security design based on STM32 microcon- troller[J], Archit. Eng. Sci. 5 (1) (2024). [11] H. Sallay, Designing an adaptive effective intrusion detection system for smart home IoT[J], IInt. J. Adv. Comput. Sci. Appl. (IJACSA) 15(1) (2024).

21. M. H, A.F.H. Yohandri, Arduino based smart home security design using biometric recognition[J], J. Phys. Conf. Ser. 2582 (1) (2023).

22. M. Aminu, A. Yerima, A. Salisu, *et al.*, Design and implementa- tion of an IOT based smart home monitoring and control system using nodeMCU[J], J. Eng. Res. Rep. 25 (2) (2023) 78–88.