Publishing Excellence
Inspiring Progress
ARISTON
PUBLICATIONS

CompSci & AI
Advances

ISSN: xxxx-xxxx https://aristonpubs.com/computers-ai-advances https://doi.org/10.69626/cai.2024.0158

RESEARCH ARTICLE

Cost Effective IoT Based Smart Home Automation System: Design, Implementation, and Security Features

M. Senthil [1,*], G. Navaneetha Krishnan [2], P. Anitha [1], S. K. Heena [1], T. Jaya Sri [1]

ABSTRACT: The increasing adoption of Internet of Things (IoT) technologies has paved the way for smart home automation systems that provide efficient and user-friendly solutions for controlling household appliances and gadgets. This study proposes a cost-effective IoT-based smart home automation system designed to address affordability and ease of use for small businesses and regular users. The system enables seamless control of appliances through voice commands, physical activity sensors, and a mobile application interface. The proposed system connects home devices and appliances via Wi-Fi and utilizes a central processing unit to manage Internet of Things (IoT) operations. It features a software development kit (SDK) that simplifies the connection, configuration, and control of both new and existing appliances. The SDK also supports third-party device integration, providing flexibility for future expansions. To enhance security and reliability, the system employs 256-bit Advanced Encryption Standard (AES) encryption for end-to-end communication between the central control hub, device controllers, and the cloud. Automated device inactivity detection and power shutdown capabilities are integrated to optimize energy efficiency. The mobile application allows users to customize scripts for automated tasks and supports real-time monitoring of appliance performance. This smart home automation system combines affordability, simplicity, and robust security measures, making it a versatile solution for domestic and commercial eco-systems. The platform's scalability and customizable features highlight its potential to revolutionize modern living environments while addressing user demands for seamless control and energy efficiency.

Keywords: Internet of Things (IoT), Smart Home Automation, Wi-Fi Connectivity, Home Security Encryption.

Received: 22 April 2024; Revised: 05 June 2024; Accepted: 13 July 2024; Published Online: 28 July 2024

1. INTRODUCTION

The Internet of Things (IoT) is a network of interconnected devices that utilize electronics, sensors, software, networking, actuators, and other components to gather, process, and exchange data. This revolutionary technology connects various devices through networks, enabling them to communicate and make autonomous decisions. IoT systems typically send information to cloud storage, process the gathered data on remote servers, and issue commands to control devices efficiently. As a result, IoT has become a vital technology for monitoring and managing devices based on real-time sensor readings [1].

The rapid expansion of IoT applications in recent years has transformed various industries, including healthcare, agriculture, transportation, and smart home systems. These devices use diverse communication technologies, such as Bluetooth, Near Field Communication (NFC), Wi-Fi, Radio Frequency Identification (RFID), Li-Fi, and Z-Wave, to transfer collected data and make control decisions based on server responses [2]. IoT's ability to connect devices and analyze data has significantly boosted productivity and efficiency across industries. Moreover, IoT security systems enhance business safety by integrating technologies like

[1] Department of Computer Science and Engineering, QIS College of Engineering and Technology, Ongole, Andhra Pradesh, India
[2] Department of Mechanical Engineering, QIS College of Engineering and Technology, Ongole, Andhra Pradesh, India

[*] Author to whom correspondence should be addressed: qispublications@qiscet.edu.in (M. Senthil)

artificial intelligence (AI) and deep learning, as well as assigning unique identities to connected devices, thus ensuring secure data exchange [3].

Figure 1 illustrates the overall architecture of IoT, where sensors are linked to various communication and transmission channels. These channels include Wi-Fi, Bluetooth, wireless networks, low-power wide-area networks (LPWAN), satellite networks, and wide-area networks (WAN). The data collected by the sensors is transmitted to cloud storage or remote servers for processing. A database using a non-structured query language (NoSQL) stores the data to manage large volumes of real-time information. The processed data is then utilized to issue control signals to IoT hardware through an internet gateway, enabling modifications to real-world objects such as adjusting the temperature of heaters and air conditioners within acceptable ranges [4]. The development of IoT architecture has paved the way for integrating next-generation networking technologies like 5G. These advancements offer numerous opportunities for automation and enhanced quality of life. The high-speed connectivity provided by 5G enables real-time communication between devices, facilitating rapid decision-making and improving the performance of automated systems. For instance, virtual assistants like Google Assistant and Amazon Alexa utilize IoT to provide real-time control over home automation devices [5]. By leveraging 5G and other advanced technologies, IoT systems are becoming increasingly efficient, reliable, and versatile. IoT architecture typically involves three key layers, i.e. perception layer, network layer and application layer. The perception layer includes sensors and actuators that gather data from the physical environment. These components are crucial for collecting real-time information, such as temperature, humidity, and motion. The network layer manages the transmission of data from the perception layer to the cloud or servers. Communication technologies like Wi-Fi, Zigbee, and LoRaWAN are commonly used at this stage. Moreover, the application layer focuses on processing and analyzing the data to provide actionable insights. It also includes user interfaces, such as mobile applications, that allow users to control and monitor devices [6]. Smart home automation is one of the most prominent applications of IoT.

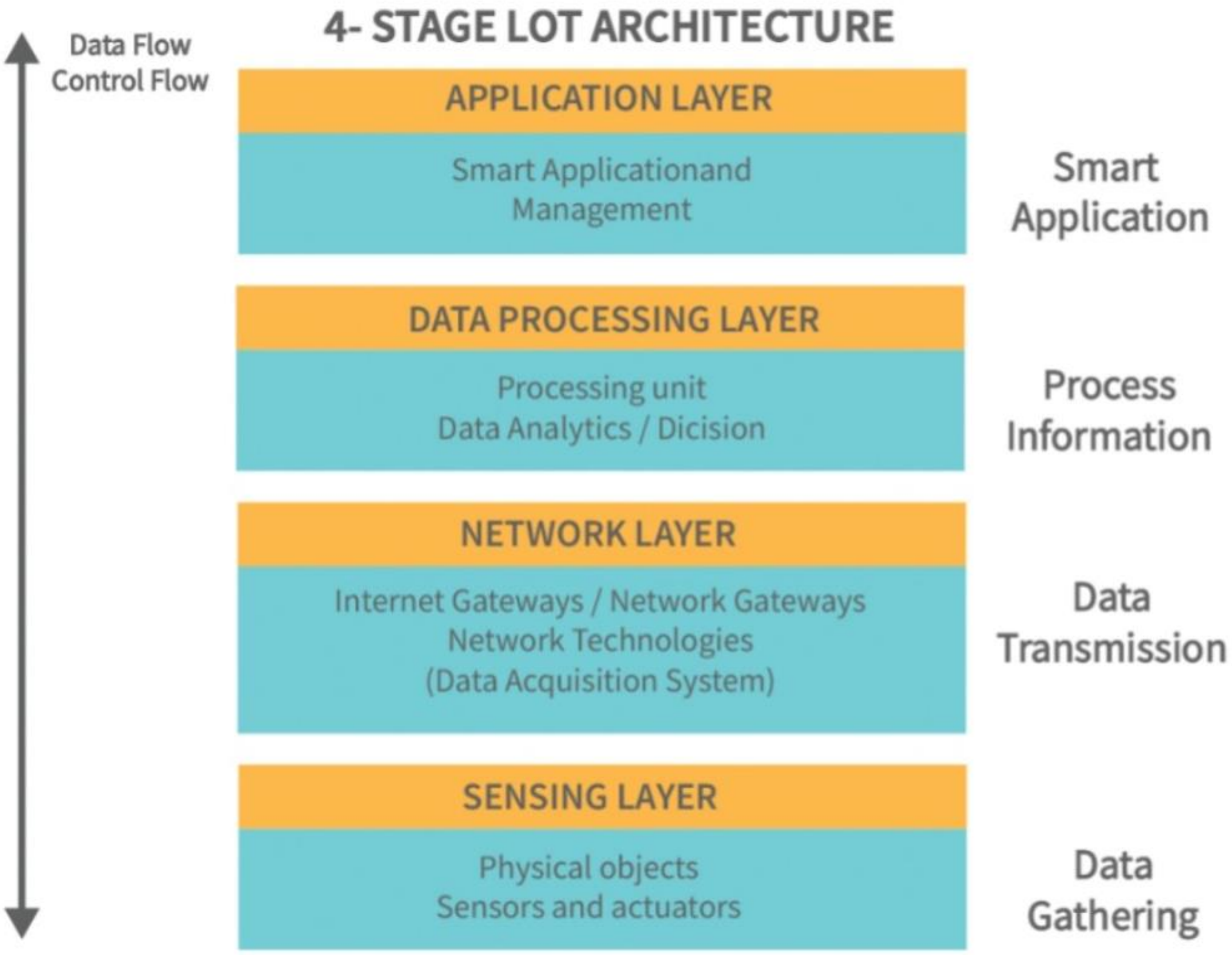

Fig. 1. Architecture of IoT.

It enables users to control various household devices, such as lights, thermostats, and security cameras, through mobile apps or voice commands. The proposed IoT-based smart home automation system leverages Wi-Fi connectivity to link devices and utilizes a central processing unit (CPU) for managing IoT operations. This system also integrates a software development kit (SDK) that simplifies the connection and configuration of devices, supporting the seamless addition of third-party appliances [7]. The scalability of IoT in smart home automation is enhanced by its compatibility with various platforms, including Android, iOS, and web-based applications. Users can customize the system by creating scripts for automated tasks, such as scheduling lights to turn on or off at specific times. Additionally, the system incorporates energy-efficient features like automated device shutdown and inactivity detection, which reduce energy consumption and contribute to sustainable living practices [8]. Ensuring the security of IoT systems is a critical challenge, given the vast amount of data exchanged between devices. The proposed system addresses this issue by employing 256-bit Advanced Encryption Standard (AES) encryption for end-to-end communication between the central control hub, device controllers, and the cloud. The encryption keys are regularly updated based on user preferences to strengthen security further [9]. Moreover, the system uses a lightweight encryption technique to minimize latency and improve efficiency. A mesh emergency network is also introduced to ensure continuous operation during network failures. This network acts as a backup, taking over the ecosystem and maintaining its functionality in case of connectivity issues [10].

The future of IoT holds immense potential for innovation and growth. Emerging technologies like edge computing and machine learning are expected to play a pivotal role in enhancing the performance and scalability of IoT systems. Edge computing, for example, reduces latency by processing data closer to the source rather than relying solely on cloud storage. Machine learning algorithms can analyze data patterns to predict user behavior and optimize system performance [11]. In the context of smart home automation, future developments may include advanced voice recognition systems, integration with renewable energy sources, and the ability to manage complex ecosystems comprising hundreds of connected devices. The use of blockchain technology in IoT is also gaining traction, offering a decentralized approach to data security and reducing the risk of cyberattacks [12].

This paper explores the design, implementation, and evaluation of a cost-effective IoT-based smart home automation system. Section 2 provides an in-depth analysis of existing home automation methods. Section 3 introduces the proposed smart automation paradigm, detailing its architecture and functionality. Section 4 presents the results of the system implementation, followed by a discussion of its performance and limitations. Finally, Section 5 outlines the key contributions of this study and suggests potential areas for future improvement.

2. RELATED WORKS

This section presents a comprehensive analysis of recently developed smart automation systems for office and household appliances, highlighting their advantages and limitations. The integration of real-time control techniques for managing home and office equipment via mobile devices and general radio services has been extensively explored. A transport-based message queuing telemetry protocol (MQTT) has been proposed for developing an Internet of Things (IoT) authorisation system, establishing a structured framework for access control. The architecture is built on the principles of open authorization (OAuth), a standard widely utilized in online applications for secure resource access [13].

The IoT is a transformative technology with immense potential to revolutionize various domains, including e-governance, environmental management, military applications, infrastructure maintenance, energy management, smart homes, health monitoring, and transportation systems [14]. In the realm of home automation, frameworks have been proposed to address critical challenges. One study presented a prototype system known as IoT@HoMe, designed to automate the control of home appliances and monitor environmental conditions. This system employed multiple sensors connected via a NodeMCU, a microcontroller unit functioning as a Wi-Fi-based gateway. The architecture utilized EmonCMS software for recording and simulating controlled data, enabling remote operation of household appliances [15].

Numerous businesses, from tech giants like Google, Amazon, and Microsoft to smaller firms, have developed home automation systems for managing domestic appliances. These systems leverage Bluetooth technology to connect with devices, allowing users to configure and control them via mobile applications. Products such as Amazon Alexa and Google Assistant exemplify the integration of IoT into daily life by supporting vendor-specific smart devices like smart bulbs. However, these solutions often fall short when it comes to traditional household appliances, which are more cost-effective and easier to replace but lack built-in IoT compatibility [16]. Current automation systems like Alexa or Google Assistant are not equipped to manage such appliances, creating a gap in the market for universal solutions.

Some initiatives have attempted to address this issue by enabling internet-based control of home appliances. However, these systems often require the allocation of a static IP address to the home network, a feature that is uncommon among average consumers [17]. The need for an affordable, user-friendly solution to automate traditional appliances remains unfulfilled. This gap highlights the potential for systems that provide a convenient and cost-effective means to remotely control household environments using mobile applications or voice commands over the internet, regardless of geographic location. While the current advancements are promising, several challenges persist. According to findings from various studies, the following key aspects should be prioritized to enhance the effectiveness of existing systems:

Automation of Traditional Appliances**:** Current solutions focus predominantly on smart appliances, neglecting the automation of traditional devices. Addressing this gap would significantly broaden the reach and utility of home automation systems [18].

Offline Functionality**:** Systems should be capable of functioning without internet connectivity, ensuring reliability even during network outages [19].

User-Friendly Configuration**:** Simplifying the setup process for traditional appliances via mobile applications can make automation accessible to a wider audience [20].

Cost-Effectiveness**:** The high cost of existing systems poses a barrier to adoption. Developing budget-friendly solutions is crucial for widespread implementation, especially in small-scale applications [21].

Custom Scripting**:** Allowing users to create and execute custom scripts for their devices can enhance system flexibility and personalization [22].

In addition to these challenges, security concerns have emerged as a critical area of focus. The communication between device controllers and central hubs must be encrypted to prevent unauthorized access and data breaches. Advanced encryption standards, such as 256-bit AES, are commonly used, but the development of lightweight encryption techniques for resource-constrained IoT devices is essential [23].

Furthermore, addressing interoperability issues among devices from different vendors is vital for seamless integration and operation. Solutions that work across various platforms, including iOS, Android, and web-based interfaces, can significantly improve user experience and system versatility [24]. Another area of improvement is the creation of a mesh emergency network to maintain ecosystem functionality during network failures, ensuring uninterrupted operation [25]. The literature underscores the potential of IoT in transforming home automation but also highlights the need for innovative solutions to overcome existing limitations. By addressing these challenges, future systems can achieve greater efficiency, security, and accessibility, paving the way for the widespread adoption of smart automation technologies.

3. PROPOSED SYSTEM

The proposed system introduces a versatile smart automation framework that functions as a general-purpose vendor, offering enhanced connectivity and convenience for users. While existing systems can be controlled through voice assistants such as Google Assistant or Alexa, the current proposal aims to transcend limitations like rigid schedules and incompatibility with certain technologies. The core components of the system leverage a sophisticated yet energy-efficient Raspberry Pi device running Java, which serves as the central processing unit for the smart automation ecosystem. This device is interconnected to the system's local network, forming the backbone of the automation infrastructure.

The system is designed to respond dynamically to user voice commands received within the home or remotely via internet connectivity. Upon detecting a command, the system processes it, identifies the requested action, and executes the task seamlessly. This enables users to remotely adjust their surroundings and control devices, making life significantly more convenient and adaptable. The system architecture is optimized for speed and efficiency, and its integration with widely used voice assistants like Google Assistant and Alexa enhances its usability and compatibility. These assistants act as the backbone for managing connected applications, providing a smooth and interactive user experience.

Figure 2 illustrates the flow diagram of the proposed system, demonstrating the sequence of operations from receiving user commands to executing the desired actions. The system's design emphasizes safety, user-friendliness, and adaptability, making it feasible to transform a conventional home into a fully automated smart home. To ensure reliable communication and connectivity, the system employs Wi-Fi technology, which offers superior bandwidth, extended range, and fast transmission of control messages. The cloud platform serves as the foundation for managing user preferences and data, utilizing a secure storage space that can be accessed from anywhere in the world. This storage is integrated with real-time database capabilities, enabling instant synchronization between user commands and device actuation. The Firebase Real-Time Database plays a critical role in the system, acting as the central data repository for storing and processing user preferences. Through its real-time data triggers, the database ensures instantaneous actuation of connected devices upon receiving control signals. The system architecture also includes mechanisms for secure cloud subscriptions and publications, further enhancing its reliability and responsiveness.

At the heart of the proposed automation system is a central hub device that efficiently manages communication between the cloud, user commands, and the connected devices. This hub not only facilitates seamless control but also minimizes the cost and complexity of integrating multiple devices into the ecosystem. By leveraging a streamlined and scalable architecture, the system ensures that both traditional and modern appliances can be automated and controlled with ease.

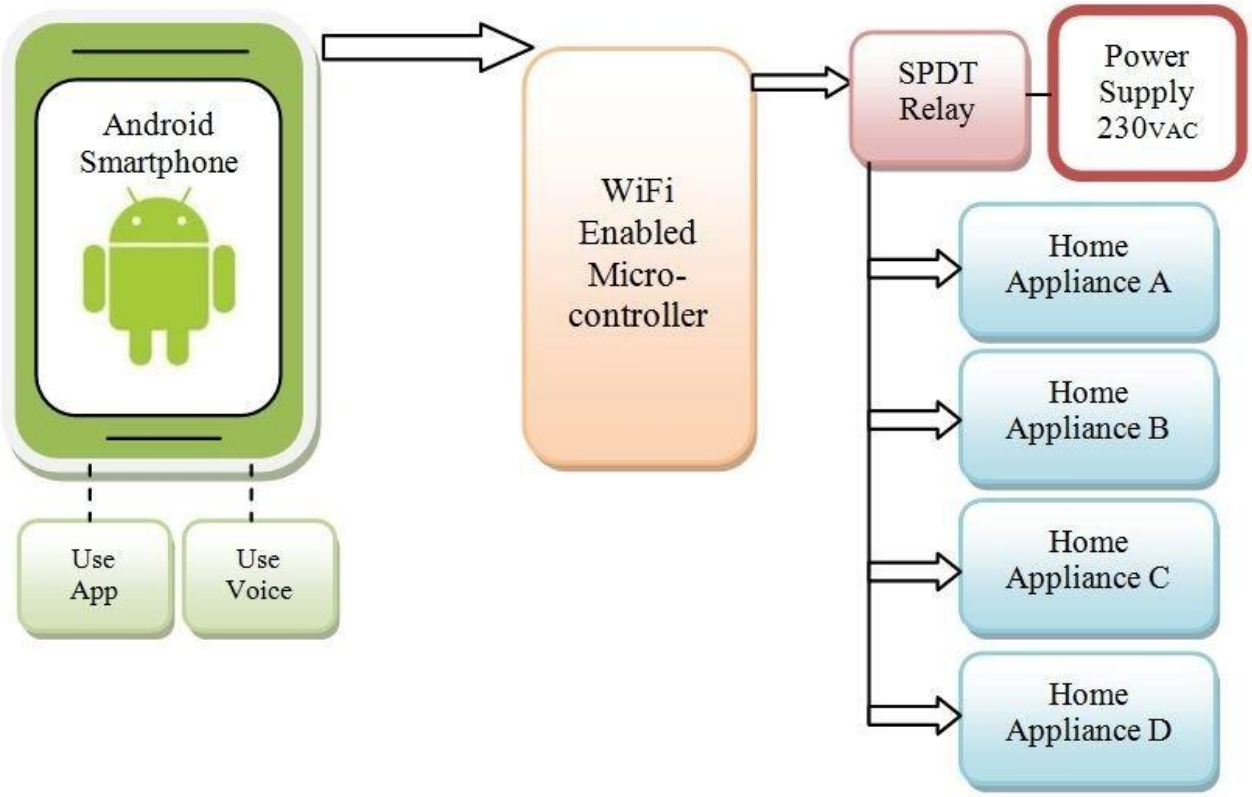

Fig. 2. Flow diagram illustrating the operation of the proposed smart automation system, from receiving user commands to device actuation.

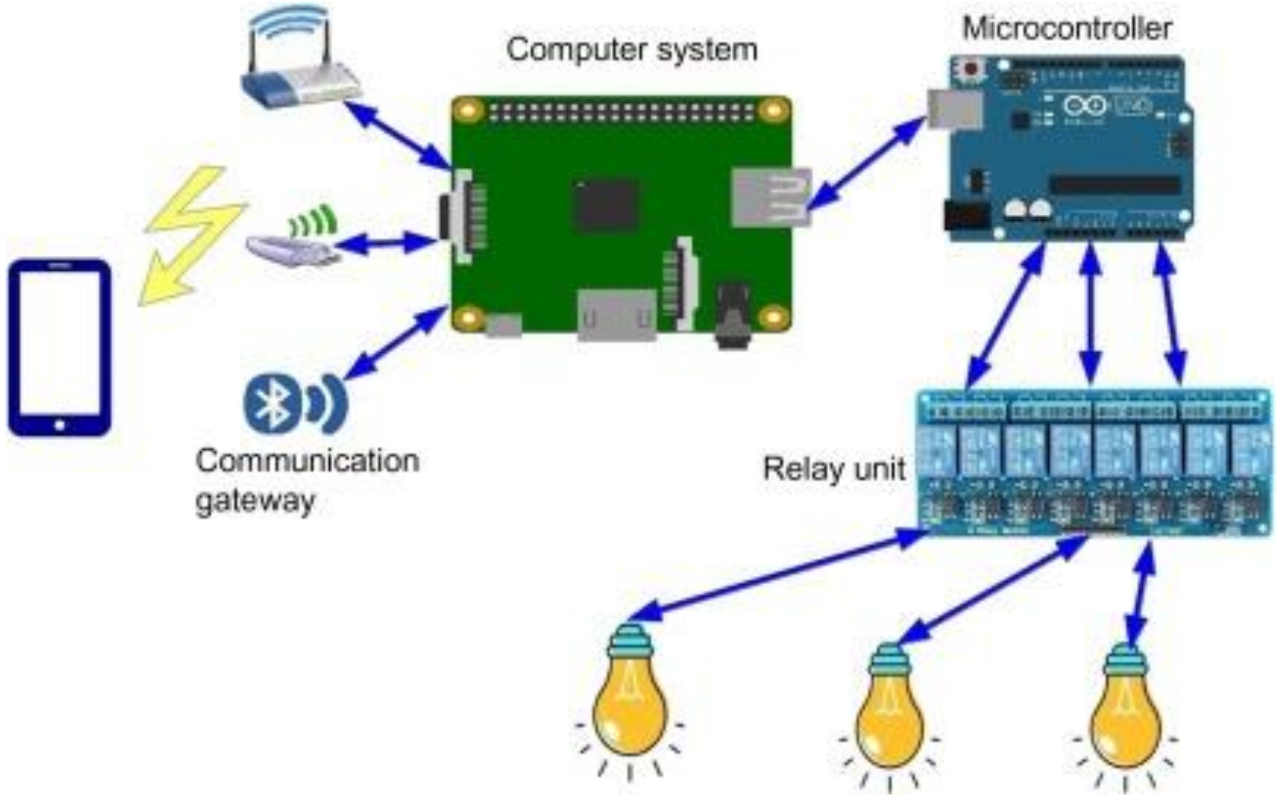

Fig. 3. Generalized architecture of the proposed home automation system, highlighting the integration of devices, cloud storage, and user interfaces for seamless operation.

The proposed design aims to address the shortcomings of existing home automation systems, such as the inability to automate conventional appliances, the need for costly infrastructure, and the lack of flexibility in device integration. By focusing on user-centric features such as affordability, offline functionality during network downtimes, and compatibility with mobile applications, the system offers a comprehensive solution for smart home automation. Figure 3 shows the generalized architecture of the proposed home automation system, highlighting the integration of devices, cloud storage, and user interfaces for seamless operation.

4. RESULTS AND DISCUSSION

The results of the proposed smart automation system demonstrate its efficacy in addressing modern-day needs for flexible, user-friendly, and secure automation in home environments. The system's modular implementation, benchmarked through eight distinct modules, delivers enhanced functionalities for users, catering to both technical and non-technical individuals. Each module plays a vital role in achieving the overarching goals of seamless communication, ease of configuration, security, and personalization. The discussion below provides an in-depth analysis of the results and elaborates on the design and operation of each module, supplemented by detailed interpretations of the associated figures.

4.1. Device Configuration

This module focuses on simplifying the setup process for devices in the smart home ecosystem. Through intuitive Android and iOS applications, users can quickly configure devices wirelessly. Two configuration modes are provided: auto-configured, which minimizes user intervention, and manual configuration for advanced customization. A key highlight is the secure cloud storage feature that retains device configuration data. This enables effortless restoration of settings even after reinstallation of the app or transitioning to a new device. The system ensures that device data is encrypted, safeguarding user information while maintaining accessibility. This is particularly beneficial for non-technical users, as it minimizes technical barriers and promotes user-friendly operation.

4.2. Device Communication

Device-to-device communication is central to the functionality of the smart automation system. By leveraging the Wi-Fi network, devices interact with each other through a central control hub. This interaction ensures that user commands are efficiently executed across the ecosystem. Figure 4 illustrates this communication mechanism, emphasizing the seamless exchange of control signals. The module addresses critical challenges, including device identification, authentication, and reliable signal transmission. Additionally, the system supports scalability, allowing for the addition of new devices without compromising existing communication protocols. Figure 4 represents the device-to-device communication framework, showing how devices transmit data via the central hub. It highlights the architecture's robustness and flexibility in managing multiple devices simultaneously.

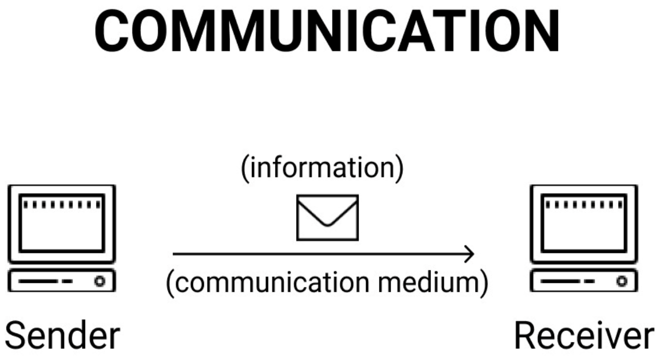

Fig. 4. Communication between devices.

4.3. Local Network Connection

The local network connection module ensures uninterrupted connectivity between devices and the control hub. Wi-Fi is utilized as the backbone for its high bandwidth, reliability, and wide coverage, ensuring rapid communication. This module not only establishes device connections but also maps devices to specific locations within the home for precise control. A location-based mapping strategy is implemented, ensuring that commands are routed to the correct devices. For example, a lighting command intended for the living room will only activate the specified lights, avoiding interference with devices in other areas. Figure 5 showcases the network architecture, emphasizing how devices communicate with the control hub and with each other to create a cohesive automation ecosystem. Figure 5 details the connections within the local network, highlighting the flow of data between devices and the central hub. It underscores the system's capability to maintain stable and efficient communication even in complex setups.

4.4. Offline Control of Remote Devices

The addition of offline remote control capabilities addresses scenarios where an internet connection is unavailable.

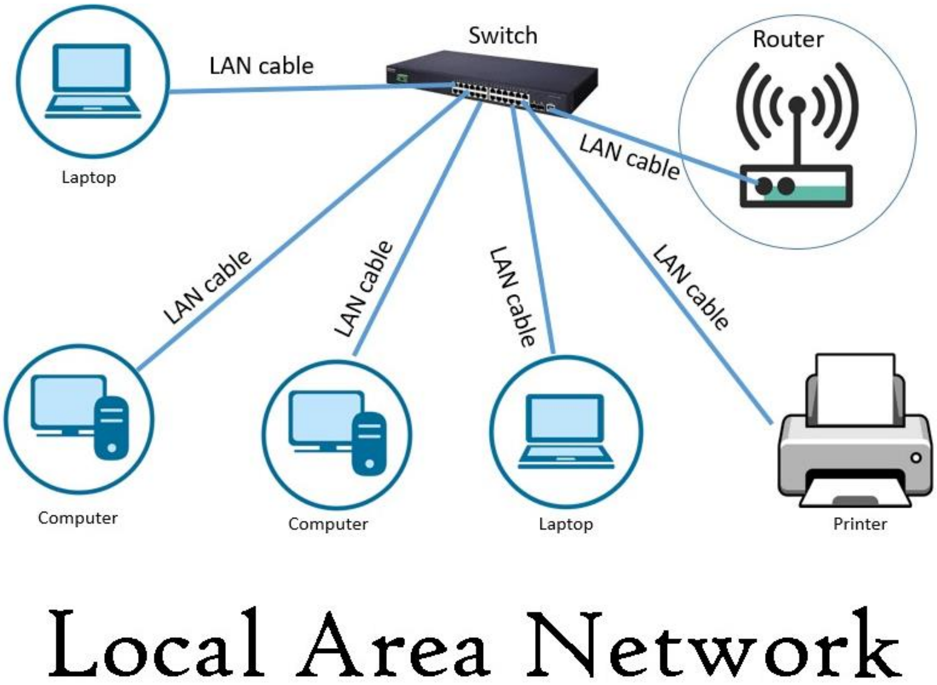

Fig. 5. Local network connection.

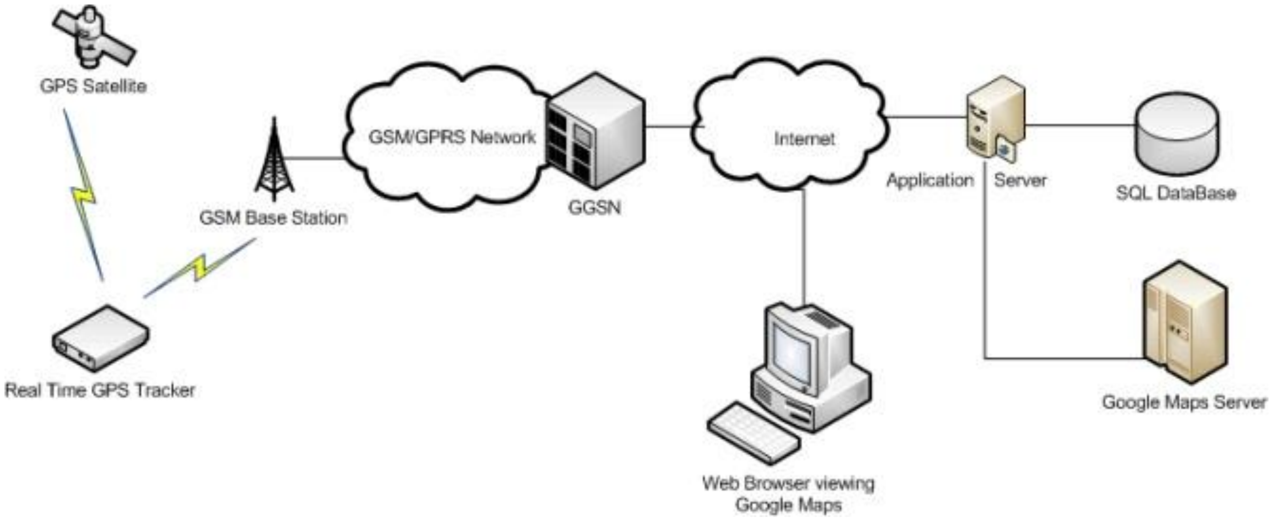

Fig. 6. Online remote control and mapping.

This module enables the Android app to function within the local Wi-Fi network, ensuring users can still manage devices without external dependencies. The offline mode is especially useful in areas with limited internet access, making it a practical solution for diverse user environments. This functionality is achieved through user-friendly remote-control techniques embedded within the Android app, allowing users to perform tasks such as device configuration and maintenance. Figure 5 illustrates how the offline mode operates, showcasing data transmission from the app to devices through the local network. Figure 5 demonstrates the process of offline remote control, highlighting the interaction between the app and devices within the local network. It emphasizes the system’s ability to maintain core functionalities without internet connectivity.

4.5. Online Control of Remote Devices

The online control module enhances flexibility by enabling remote access to devices via the internet. This functionality allows users to control and monitor devices from any location, significantly improving the system's utility. A mapping strategy is employed to associate devices with specific locations and appliances, ensuring precise and reliable control. Figure 6 depicts the connections between devices in the online mode, highlighting how control signals are routed through the cloud platform to designated devices. This figure showcases the routing of control signals in the online mode, emphasizing the integration of cloud-based mapping strategies for location-specific device control.

4.6. User Profiling and Cloud Configuration Storage

The user profiling module tailors the system to individual preferences by analyzing user behavior and interactions. Personalized profiles are created and securely stored in the cloud, enabling seamless synchronization across devices. This feature ensures a consistent user experience, even when switching devices or accessing the system remotely. The cloud configuration storage facilitates easy restoration of settings and profiles, eliminating the need for repeated manual configurations. Figure 7 illustrate this module, highlighting the secure flow of data to and from the cloud. The figure demonstrates the process of user profiling and cloud storage, showcasing the system's ability to deliver a personalized and secure experience.

The integration of these modules results in a robust and efficient smart automation system that combines ease of use, security, and flexibility. The system's modular design allows for scalability and adaptability, accommodating future technological advancements and user needs. The system simplifies automation for users, regardless of technical expertise, through intuitive apps and streamlined processes. It secure storage and communication protocols ensure user data and device interactions are protected. Offline and online control modes provide flexibility, making the system suitable for various environments. In addition, user profiling creates tailored experiences, increasing satisfaction and engagement.

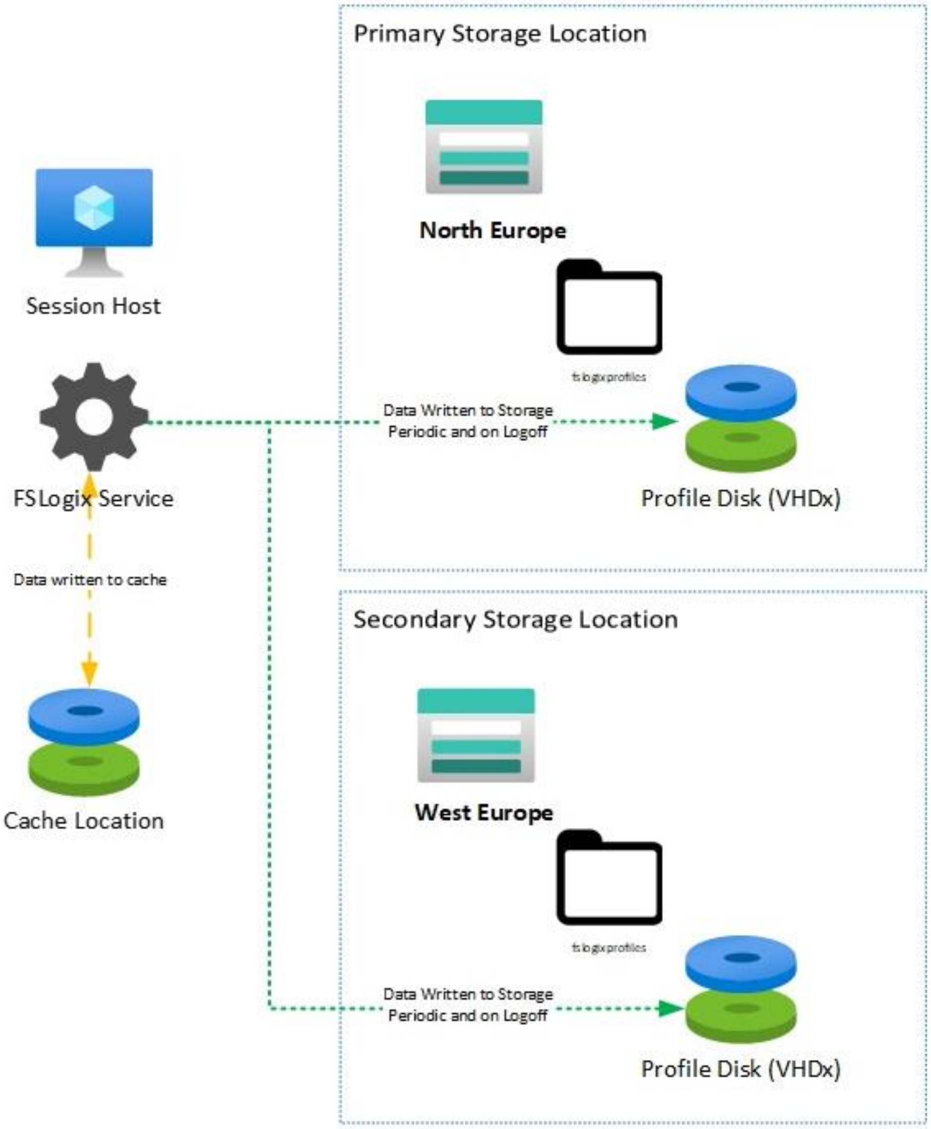

Fig. 7. Cloud configuration storage and user profiling.

5. CONCLUSION

The proposed IoT-based smart home automation system presents a cost-effective, scalable, and user-friendly solution for modern households and small businesses. By leveraging Wi-Fi connectivity and a central processing unit, the system enables seamless control of home appliances and gadgets through voice commands, activity sensors, and a dedicated mobile application. This integration of technologies ensures that the system is accessible to users with varying technical expertise. The system's affordability is achieved without compromising its functionality. The incorporation of a software development kit (SDK) simplifies the connection and configuration process, allowing users to integrate new devices and manage third-party appliances effortlessly. The flexibility offered by this feature enhances the system's adaptability for future upgrades and expansions. A key highlight of the system is its focus on robust security measures. Communication between the central control hub, device controllers, and the cloud is secured using 256-bit Advanced Encryption Standard (AES) encryption, ensuring the safety of user data and system integrity. The system also supports regular updates to encryption keys based on user preferences, further strengthening its defense against potential cyber threats. Energy efficiency is another crucial aspect of the system. Features such as automated device shutdown and inactivity detection minimize unnecessary energy consumption, contributing to sustainable living practices. Additionally, the system provides real-time consumption monitoring through a cloud-integrated eco-power management system. The introduction of a lightweight encryption technique and a mesh emergency network ensures reliable operation during network failures. Users can also create custom scripts for specific tasks, adding to the system's versatility. These features collectively position the proposed system as a comprehensive solution for smart home automation, addressing the needs of modern households for affordability, security, and convenience.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interests.

REFERENCES

[1] Ashton, K., 2009. That 'internet of things' thing. *RFID journal*, *22*(7), pp.97-114.

[2] Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M., 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), pp.1645-1660.

[3] Sicari, S., Rizzardi, A., Grieco, L.A. and Coen-Porisini, A., 2015. Security, privacy and trust in Internet of Things: The road ahead. *Computer networks*, *76*, pp.146-164.

[4] Atzori, L., Iera, A. and Morabito, G., 2010. The internet of things: A survey. *Computer networks*, *54*(15), pp.2787-2805.

[5] Perera, C., Zaslavsky, A., Christen, P. and Georgakopoulos, D., 2013. Context aware computing for the internet of things: A survey. *IEEE Communications Surveys & Tutorials*, *16*(1), pp.414-454.

[6] Palattella, M.R., Accettura, N., Vilajosana, X., Watteyne, T., Grieco, L.A., Boggia, G. and Dohler, M., 2012. Standardized protocol stack for the internet of (important) things. *IEEE Communications Surveys & Tutorials*, *15*(3), pp.1389-1406.

[7] Da Xu, L., He, W. and Li, S., 2014. Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics*, *10*(4), pp.2233-2243.

[8] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M., 2015. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials*, *17*(4), pp.2347-2376.

[9] Fernández-Caramés, T.M. and Fraga-Lamas, P., 2018. A Review on the Use of Blockchain for the Internet of Things. *Ieee Access*, *6*, pp.32979-33001.

[10] Li, S., Xu, L.D. and Zhao, S., 2015. The internet of things: a survey. *Information Systems Frontiers*, *17*, pp.243-259.

[11] Dastjerdi, A.V. and Buyya, R., 2016. Fog computing: Helping the Internet of Things realize its potential. *Computer*, *49*(8), pp.112-116.

[12] Christidis, K. and Devetsikiotis, M., 2016. Blockchains and smart contracts for the internet of things. *IEEE Access*, *4*, pp.2292-2303.

[13] Tightiz, L. and Yang, H., 2020. A comprehensive review on IoT protocols' features in smart grid communication. *Energies*, *13*(11), p.2762.

[14] Perwej, Y., Haq, K., Parwej, F., Mumdouh, M. and Hassan, M., 2019. The internet of things (IoT) and its application domains. *International Journal of Computer Applications*, *975*(8887), p.182.

[15] Jabbar, W.A., Kian, T.K., Ramli, R.M., Zubir, S.N., Zamrizaman, N.S., Balfaqih, M., Shepelev, V. and Alharbi, S., 2019. Design and fabrication of smart

home with internet of things enabled automation system. *IEEE Access*, *7*, pp.144059-144074.

[16] Huang, D.Y., Apthorpe, N., Li, F., Acar, G. and Feamster, N., 2020. Iot inspector: Crowdsourcing labeled network traffic from smart home devices at scale. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *4*(2), pp.1-21.

[17] Liu, C., Zha, X.F., Miao, Y. and Lee, J., 2005. Internet server controller based intelligent maintenance system for information appliance products. *International Journal of Knowledge-based and Intelligent Engineering Systems*, *9*(2), pp.137-148.

[18] Aheleroff, S., Xu, X., Lu, Y., Aristizabal, M., Velásquez, J.P., Joa, B. and Valencia, Y., 2020. IoT-enabled smart appliances under industry 4.0: A case study. *Advanced Engineering Informatics*, *43*, p.101043.

[19] Irugalbandara, C., Naseem, A.S., Perera, S., Kiruthikan, S. and Logeeshan, V., 2023. A secure and smart home automation system with speech recognition and power measurement capabilities. *Sensors*, *23*(13), p.5784.

[20] Han, J., Yun, J., Jang, J. and Park, K.R., 2010. User-friendly home automation based on 3D virtual world. *IEEE Transactions on consumer electronics*, *56*(3), pp.1843-1847.

[21] Mustofa, A.A., Dagnew, Y.A., Gantela, P. and Idrisi, M.J., 2023. SECHA: A Smart Energy-Efficient and Cost-Effective Home Automation System for Developing Countries. *Journal of Computer Networks and Communications*, *2023*(1), p.8571506.

[22] Shvaika, D.I., Shvaika, A.I. and Artemchuk, V.O., 2024. Advancing IoT interoperability: dynamic data serialization using ThingsBoard. *Journal of Edge Computing*, *3*(2), pp.126-135.

[23] Mehmood, M.S., Shahid, M.R., Jamil, A., Ashraf, R., Mahmood, T. and Mehmood, A., 2019, November. A comprehensive literature review of data encryption techniques in cloud computing and IoT environment. In *2019 8th International Conference on Information and Communication Technologies (ICICT)* (pp. 54-59). IEEE.

[24] Perumal, T., Ramli, A.R. and Leong, C.Y., 2011. Interoperability framework for smart home systems. *IEEE Transactions on Consumer Electronics*, *57*(4), pp.1607-1611.

[25] Messina, F., Santoro, C. and Santoro, F.F., 2024. Enhancing Security and Trust in Internet of Things through Meshtastic Protocol Utilising Low-Range Technology. *Electronics*, *13*(6), p.1055.