Middle East Research Journal of Engineering and Technology

ISSN: 2789-7737 (Print) ISSN: 2958-2059 (Online)
Frequency: Bi-Monthly
DOI: https://doi.org/10.36348/merjet.2025.v05i06.003

KUWAIT SCHOLARS PUBLISHER

Website: http://www.kspublisher.com/
Email: office@kspublisher.com

Improved Home Automated System Using Arduino Controller with Two-Way Security

Diponkar Sharker[1]*, Nandon Kumar Singha[2], Anselem Onyejuruwa[3], Engr. Satta Chandra Pramanik[4], Arman Mohammad Nakib[5]

[1]Nanjing University of Information Science and Technology, Artificial Intelligence, Nanjing, Jiangsu, China
[2]Chang'an University, School of Electrical Engineering, Xi'an, Shaanxi, China
[3]Nanjing University of Information Science and Technology, School of Ecology and Applied Meteorology, Nanjing, Jiangsu, China
[4]Associate member of the Institution of Engineers Bangladesh, Electrical and Electronics Engineering, Dhaka, Bangladesh
[5]East China Normal University, Shanghai, China

Abstract: This paper addresses the growing need for home security and energy management by proposing a GSM- and Bluetooth-based Home Automation System (HAS). Current automation systems often lack proper security measures, such as specific digital interactions and safety bridges. To address this gap, the study aims to develop a robust solution that integrates dual off-site access control with a security alert system. The system is designed using an Arduino Uno microcontroller with GSM and Bluetooth modules for remote SMS command processing and secure local connections via encrypted communication. The proposed system ensures double security verification through a key password and a one-time password (OTP) for remote access. Additionally, it facilitates local access using a long-range Bluetooth device in case of GSM network disruptions. Overall, this technology enhances smart communication protocol integration, improves home appliance management, and strengthens safety and smart living conditions.

Keywords: Home Automation System (HAS), GSM Technology, Bluetooth Communication, Arduino Microcontroller, Two-Factor Security Authentication.

Research Paper

***Corresponding Author:**
Diponkar Sharker
Nanjing University of Information Science and Technology, Artificial Intelligence, Nanjing, Jiangsu, China

How to cite this paper:
Diponkar Sharker *et al* (2025). Improved Home Automated System Using Arduino Controller with Two-Way Security. *Middle East Res J. Eng. Technol, 5*(6): 158-169.

Article History:
| Submit: 24.11.2025 |
| Accepted: 22.12.2025 |
| Published: 29.12.2025 |

INTRODUCTION

The concept of the so-called smart home, which involves the use of interconnected devices allowing precise control of various aspects of home life including lighting, temperature, and security has inspired numerous researchers and potential consumers. More households are beginning to adopt smart home technologies, which enhance energy management, security, and comfort levels (M. A. Abubakar *et al*., 2020)(Matura & Kunal, 2024). As a result, smart home systems have become a primary focus for development in both academia and industry. However, it is essential to note that despite the rapid advancement of smart home technology, existing infrastructure and systems require improvement in terms of security and multi-access control(Santos *et al*., 2014; T[1] *et al*., 2016).

Advancing existing smart technology is crucial to ensuring the efficient use of communication protocol systems. This study proposes a novel Home Automation System (HAS) control technology that integrates GSM and Bluetooth technologies. GSM provides a reliable communication platform, enabling users to control their home environment using text messages alone(Jivani, 2014)(Reza, 2022). Meanwhile, Bluetooth offers a secure and dependable method for local interactions within the dwelling, as the transmitted information is shielded from unauthorized external intrusions(Teymourzadeh *et al.*, 2013). Smart home systems gain robust security through the implementation of multiple communication methods according to recent studies(Yuneela & Sharma, 2022)(Santos *et al*., 2014).

The integration of these two technologies into a comprehensive home automation system represents a significant step toward addressing the limited access to smart environments caused by the reliance on a single communication device in current home automation systems. The specific aim of this study is to design a HAS that enhances remote interaction and strengthens security measures beyond the standard methods used in smart homes[9-10]. This approach involves a complex structure based on an Arduino Uno microcontroller, which oversees the operation of both GSM and Bluetooth modules to create a harmonized network for managing

home appliances (Okubanjo *et al*., 2021). Previous research demonstrates how Arduino microcontrollers excel in smart home applications because of their flexible programming features and user-friendly systems(Jagdalpur, 2018)(Hamidi *et al*., 2021).

The method proposed in this research effectively addresses issues of security and limited access, which are commonly identified as key challenges in the literature (Arijit Pal *et al*., 2015)(R. kingsly Stephen, 2020). The goals of the study are: first, to demonstrate that practical SMS command processing combined with a local Bluetooth system satisfies the highest standards of security and efficiency for smart home systems; and second, to propose the use of a two-factor authentication system requiring a static password and a dynamic OTP, which minimizes the risk of unauthorized intrusions(Maniam *et al*., 2019). Experts confirm that the addition of two-factor authentication boosts the security measures for smart home technology(Hossain Shawon *et al*., 2022).

The implications of this research are substantial, extending beyond enhancing security and power efficiency. This study aims to open new avenues for integrating GSM and Bluetooth technologies into smart homes and sustainable living arrangements, providing a secure and efficient platform. By doing so, it seeks to inspire future advancements that will augment the functionality and capability of smart home systems, paving the way for more robust, integrated, and practical solutions(Stolojescu-crisan *et al*., 2021)(T[1] *et al*., 2016). The proposed system offers an adaptable framework that enables the integration of upcoming technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI) to enhance existing capabilities(H. A. Abubakar *et al*., 2022)(Rani, 2024).

LITERATURE REVIEW

Different innovations in mobile communication and wireless technologies, including the integration between GSM and Bluetooth, have impacted the development of HAS systems in general convenience and ease of accessing home automation, but there are still some issues of reliability, security, and energy utilization.

GSM Technology in Home Automation

Many home automation systems have relied on this technology for its capability to allow remote control/monitoring. In the view of Okubanjo(Okubanjo *et al.*, 2021), GSM can control home appliances using SMS or voice commands and has enhanced user convenience and reduced energy consumption. This remote capability is advantageous for users with different requirements for controlling the environment of their homes from distant places; therefore, it provides much-needed flexibility. However, a critical limitation pointed out by (Reza, 2022) is that GSM-based indoor positioning is dependent on network coverage. Message delivery response issues can undermine the effectiveness of the overall system and real-time responsiveness in quite many countries with low-standard cellular networks. This issue illustrates the need for supporting communication paradigms for high availability and timeliness, particularly for mirror activities.

Bluetooth Technology for Secure Communication

Unlike GSM, Bluetooth technology is especially appreciated for enabling safe and immediate connections within home networks. Teymourzadeh (Teymourzadeh *et al*., 2013)also proves that Bluetooth supports whisper technology and gives more secure facilities than Wi-Fi or infrared-authorized systems. This encryption capability makes Bluetooth suitable for applications where short-range, close-quarters communication is highly sensitive. Bluetooth is useful in device authentication locally and in performing key exchanges; this, according to Jivani (Jivani, 2014), is critical in ensuring that only authorized devices are allowed to communicate within the home automation system. Nevertheless, Bluetooth has a limited range of coverage and cannot cover a large home and network, so it is only good for local coverage compared to GSM.

Integration of GSM and Bluetooth Technologies

The implementation of GSM and Bluetooth enhances home automation systems; however, each technology has its drawbacks: GSM is remotely controllable but has weak connectivity, while Bluetooth is secure and has good connectivity within a limited radius.(Matura & Kunal, 2024) Matura and Kunal, the authors propose a GSM/Bluetooth model where both GSM and Bluetooth systems are used for home automation systems where GSM will be remotely accessible but have low connectivity, and the Bluetooth is locally networked but has high connectivity in limited coverage. Thus, this approach helps to overcome many limitations, including a low level of security measures and a lack of opportunities for remote control. Aparna Gira (Aparna Gira, 2022) also agrees with this integration and notes that integrating both technologies makes the system more solid, adjustable, and secure. By combining both GSM and Bluetooth, a huge advantage can be felt in terms of remoteness, at the same time ensuring that everything in the local environment stays unhampered and secure.

Security Concerns and Solutions

This is still an important issue in home automation systems design even with the current advancement in technology. Vulnerabilities described by Sarmah, Bhuyan, and Bhuyan (Sarmah *et al*., 2019) and Pal, Singh, and Bijoy Rai (Arijit Pal *et al*., 2015) are, therefore, threats such as. To counter these threats, they propose multi-factor authentication (MFA) that uses elements like one-time passwords (OTPs) and dynamic passwords. These methods of authentication come as an added security measure, cutting down the probability of code break-ins. MFA integrated into the system increases

the security level, improves the satisfaction level of the users, and guarantees the safety of home automation.

Implications for Future Research

Although there have been notable strides in home automation, there are some significant categories that even today need to be worked upon more, and that includes system integration, energy, and security. As recommended by Maniam (Maniam *et al*., 2019), future research should be directed at the advancement of more elaborate energy management strategies for a smart grid infrastructure as well as better forms of prognosis maintenance. Some of these developments could enhance the optimum utilization of energy and develop methods for detecting faulty home appliances, hence cutting energy consumption and maintenance costs. Furthermore, the combination of Internet of Things (IoT) devices with GSM and Bluetooth systems can also open up a lot of possibilities to offer even more intelligent and more responsive smart homes. The combination of these devices may enhance the possibility of creating very effective interactive systems that not only react to inputs from a user but also predict the needs of a user and enhance the overall performance of each function in the interactive system, as well as its efficiency in satisfying the needs of users. Using GSM with Bluetooth to control home automation offers a balanced scheme of the system where GSM facilitates remote control, while Bluetooth ensures secure local communications. Whereas GSM enhances the capability of handling long-distance communication, Bluetooth ensures that near-device communications are secure and efficient. Proposing concrete security measures for stringer identification and validation, as well as significantly enhancing encryption mechanisms, provided a high level of security, convenience, and usability to these systems.

However, there are weaknesses mainly in the dependency on network reliability and a call for additional and enhanced energy management systems. Further research in these areas should be done to improve the system's efficiency and user satisfaction, and questions concerning IoT and prediction algorithms should be further investigated.

METHODOLOGY

The methodology involves the conception and construction of a secure as well as energy-efficient home automation entity.

The following is a systematic approach to constructing and implementing a safe and low-power home automation system (HAS) through GSM and Bluetooth. This system intends to enable people to control all their household appliances safely from a distance as well as use energy-efficient appliances.

System Architecture Overview

The system's main fundamental is based on Arduino Uno, which can be viewed as the main control unit. The microcontroller interfaces with two communication modules: a GSM module (SIM900) for SMS-based remote control and a Bluetooth module (HC-12) for local control. Such modules enable the provision of a user interface to the system, whether local or remote (Fig. 1).

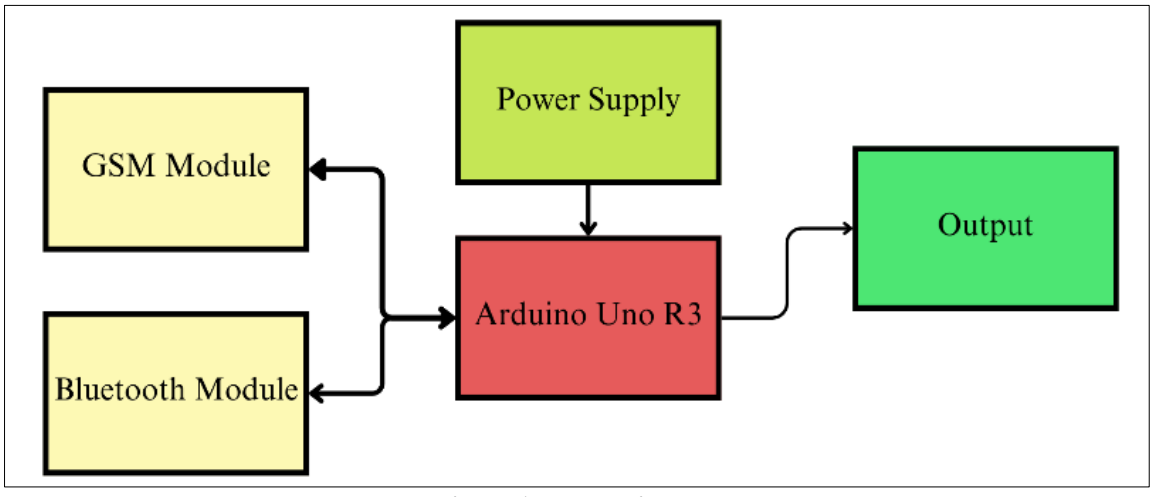

Figure 1: Block Diagram

Components and Communication Setup

The home automation system is built using several key hardware components, each crucial in ensuring the system operates effectively and securely. The following components are integrated into the system (Fig. 2).

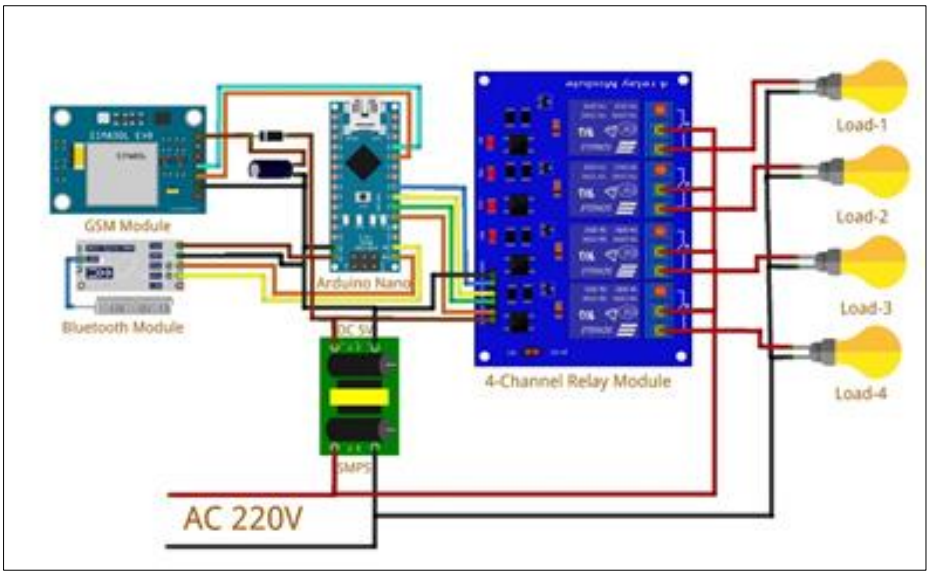

Figure 2: Circuit Diagram

Arduino Uno

The Arduino Uno is used here as the master processor of the home automation system; it operates as the system's controller. It handles the input by users and coordinates the output, which includes home appliances, among other things. This Arduino is based on the ATmega328P microcontroller that offers the facility of 14 digital I/O interfaces and 6 analog interfaces. This adaptability enables it to connect between many kinds of sensors and actuators. The Arduino is designed with a developed integrated development environment known as the Arduino IDE, which is used in the writing and uploading of codes to the Arduino board to support the command logic system needed for the automation of respective tasks(Hossain Shawon *et al*., 2022) (Fig. 3).

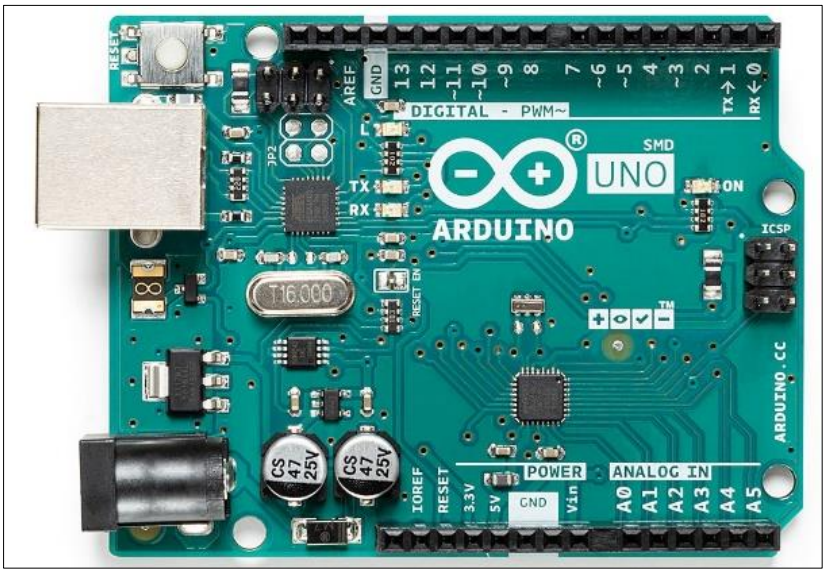

Figure 3: Arduino Uno R3 (https://store.arduino.cc/collections/black-friday/products/arduino-uno-rev3-smd)

GSM Module (SIM900)

The GSM Module (SIM900) used in the home automation system realizes SMS control, enabling the user to send commands through short messages. This particular module of the integrated system allows control of home appliances from anywhere with a mobile network by sending text messages to the system (Fig. 4). This GSM module is highly adopted due to its reliability and universal coverage to support use in home automation remote control(Aparna Gira, 2022).

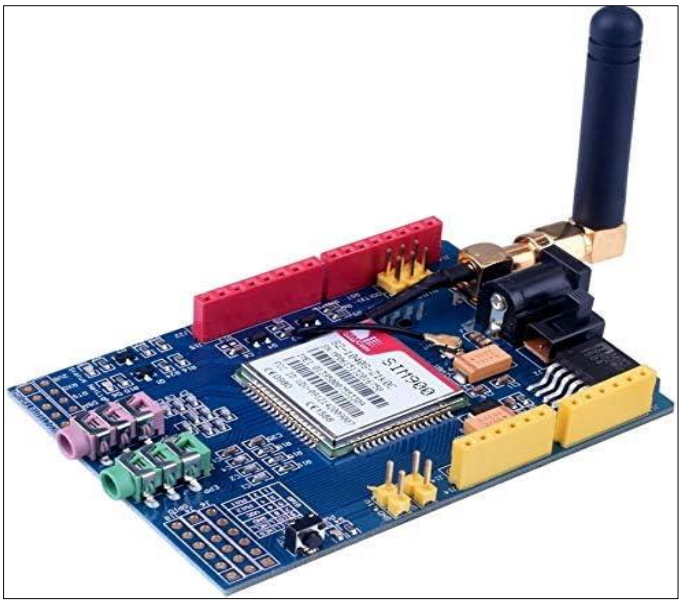

Figure 4: GSM Module (https://www.amazon.de/-/en/SIM900-Shield-Development-Quad-Band-Antenna/dp/B07FS34P84)

Bluetooth Module (HC-12)

Bluetooth communication is realized by using a Bluetooth module (HC-12) (Fig. 5), which offers secure, short-range access to the home automation system. Once the authentication by SMS has been completed, users can use Bluetooth to manage the appliance locally to great aspects of nearby appliances. Bluetooth technology is preferred in home automation systems because of easy installation and configuration as well as the security inherent in the system against unlawful interference(Aravind.S, n.d.).

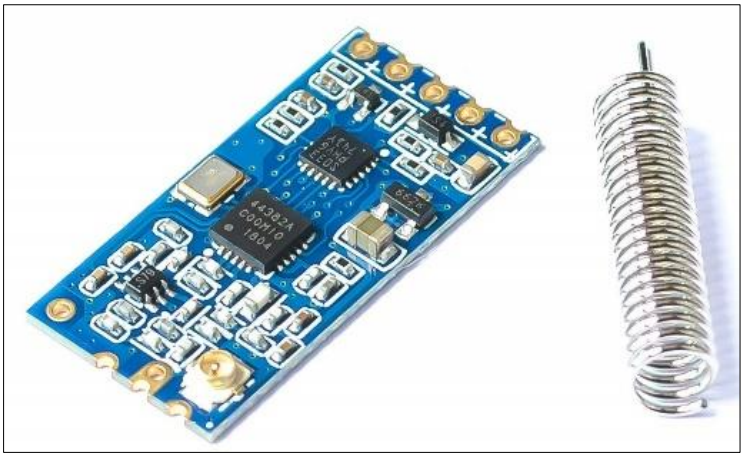

Figure 5: Bluetooth module HC-12 (https://www.amazon.in/SI4463-wireless-serial-consumption-bluetooth/dp/B01MUCVL67)

Relay Modules

Relay modules are important pieces in the home automation system for turning appliances on and off wherever it has been instructed to do so by the GSM module or the Bluetooth module(s). Fig. 6 shows a picture of a Relay modules device, which is useful in the management of high-power loads, for example, light bulbs, fans, and air conditioners. They serve the function of electrically operated switches that can control the amount of current needed in these appliances. These relays are connected to the Arduino Uno to enable the microcontroller to switch on/off the appliances following the command given on the system(Kumar & Devachandra Singh, 2021).

When all these components are incorporated into the home automation system, the user can be afforded the convenience of managing the home appliances through an SMS or locally through Bluetooth. This approach increases user convenience while at the same time keeping the system open and running smoothly.

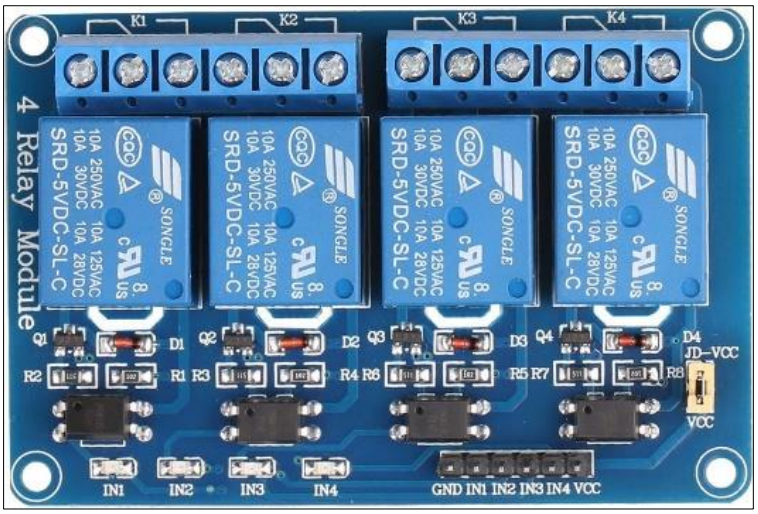

Figure 6: 4C Relay Module (https://www.amazon.com/JBtek-Channel-Module-Arduino-Raspberry/dp/B00KTEN3TM)

User Authentication Mechanism

Another important aspect of the proposed home automation system is the authentication of the user, thus restricting anyone's access to the system. It involves two main steps: password authentication and the use of a one-time password (OTP) for making transactions.

- Password Authentication: This is the first process to undertake in the process of authenticating the users of a particular product. Users are forced regularly to key in a password, which is then cross-checked in the database of the program. User authentication must be done by use of the password to authorize the user to transact on the system. In particular, if the password is entered in the wrong way, then the system may bar the user from accessing it after several tries; this is in a bid to prevent unauthorized access(M. A. Abubakar *et al*., 2020)(Okubanjo *et al*., 2021)(Saxena & Pal, 2020).
- One-Time Password (OTP): It also provides the One-Time Password (OTP) in addition to the successful password authentication. The OTP can be defined as. Temporarily valued, one-time code that is sent to the user's registered mobile number through SMS. This enhances security since even if someone has physical access to the user's password, he or she cannot sign in unless he or she also has the OTP. The user needs to input the OTP on the system to effectively complete the authentication process. This two-factor authentication method improves the security of the system several fold(Aparna Gira, 2022)(Reza, 2022)(Arijit Pal *et al*., 2015).

Energy Monitoring

The home automation system is integrated with an energy monitoring feature through which users can easily track their energy use.

- Simulation of Energy Consumption: This process mimics power utilization depending on data garnered from integrated sensors on home appliances or appended devices. This simulation enables the establishment to estimate energy usage and possibly inefficiency in energy consumption. Using the analyzed data, the system can reveal how energy is being consumed and maybe advise on how to use it more efficiently(Aparna Gira, 2022).
- Energy Data Reporting: The developed system is also equipped with energy monitoring and analysis, which displays the data to the user. This data is sent in real-time and can be accessed on a user interface on a mobile device or a web-based portal. The reporting feature has information about the energy used by a particular appliance and the energy used in the house as a whole. This assists users in making appropriate choices on energy-saving and cost-cutting mechanisms(Murugan *et al*., 2023).

Communication Protocols

The home automation system utilizes two primary communication protocols to facilitate user interaction and control, such as single SMS through the GSM module and multiple SMS through the HC-12 Bluetooth module. These protocols are selected based on their dependability, reachability, and appropriateness for several communication distances and contexts.

- SMS Communication (GSM Module): The GSM module is used to send messages to the user and make communication through SMS, while this way of controlling and monitoring the home automation system is easily accessible. SMS is selected for its high availability and stability, so users receive commands and notifications at any time and from any Internet source(Okubanjo *et al*., 2021). People can use their mobile phones to

text specific messages to control aspects of a home, for instance, to turn on/off lights, set/change temperature, and even watch over home security systems. Possible applications of the GSM module include its use in receiving and transmitting updates and alerts back to the user(M. A. Abubakar *et al*., 2020).

- Bluetooth Communication (HC-12 Module): After the user receives the code by SMS to confirm the authenticity of the device, short-range communication of the home appliances is by Bluetooth. Bluetooth is used in short-range connections, using individual appliances that are close to the Bluetooth module(Maniam *et al.*, 2019). One of its advantages is that it provides safety in employee-to-employee communication without exposing the organization to potential external threats from the Internet. Following the successful use of SMS-based authentication, the user can change his means of control from remote to local by simply moving his Bluetooth(Reza, 2022).

System Operation Flow

The system flow processes from the user's initial communication through the verifications protocols and finally to the end process is demonstrated as follows (Fig. 7).

Initial Command

The process starts with a user giving the home automation system a first command. An SMS, a mobile application picture, or another user interface may issue it. This first command prompts the system to enable the authorization procedure so that only appropriately credentialed actors can continue several given actions (Saxena & Pal, 2020).

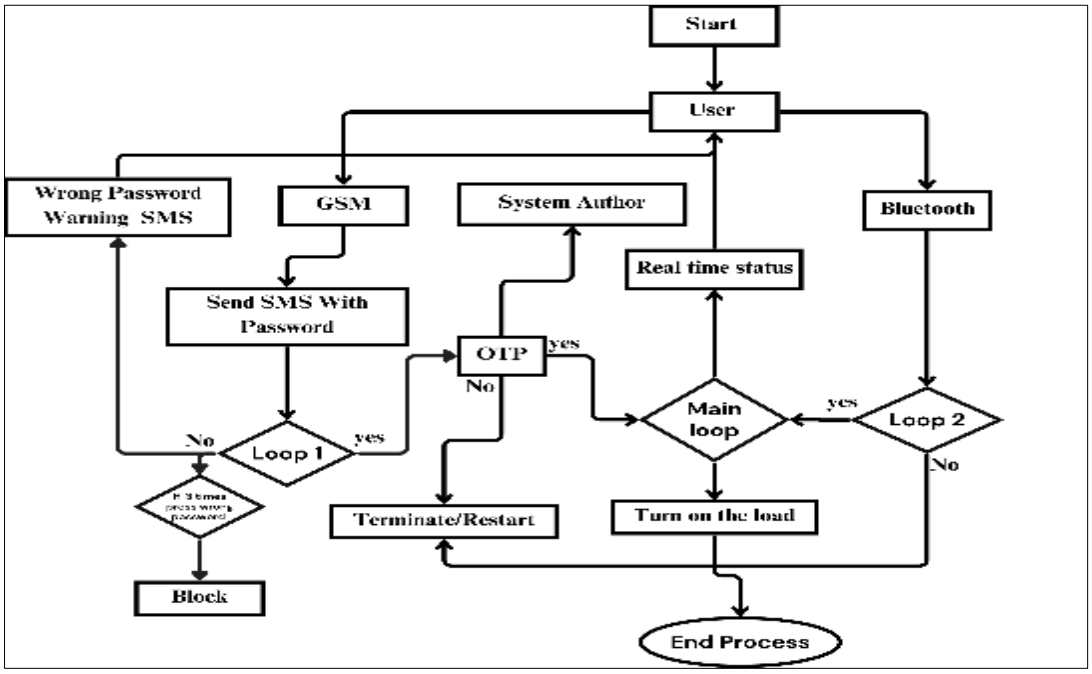

Figure 7: Flowchart of HAS circuit systems

Password Verification

When the user is given the first command, the entered password is passed through the keypad to the system database to initiate the recognition of his or her credentials. For instance, the first message that the system displayed when the user entered incorrect information would be, 'Your password is wrong. It said something like, 'Input accepted wrong; please try again,' which enabled them to re-input it. Upon entering the password on the second try, the system detects and sends a message telling the user, "Your password is wrong. You have one more try. Please try again carefully." Last of all, if the user fails to input the right password the third time, the system locks the user and outputs, 'Too many failed attempts. Access denied. This message is spelled like this: "Your number has been blacklisted." This process safeguards the system from early access by other unauthorized persons while at the same time enhancing user convenience by giving him/her several opportunities to key in the right password(Saxena & Pal, 2020).

OTP Generation

Besides, if the entered password is successfully authenticated to the system, then it then creates a One-Time Password (OTP). OTP is a one-time temporary code that is delivered to the user's registered mobile number through SMS. This brings an extra measure of security, as even when anyone knows this password, he or she cannot log into the account without this one-time password(Sarmah *et al*., 2019).

OTP Verification

The system sends the user a One Time Password (OTP) on the mobile phone, which forms a crucial part of the identification process to the system. When the OTP is received by the user, the latter is supposed to manually enter it into the system. The system then checks for the OTP that has been entered through the keyboard with that generated. If the OTP generated from the backbone server matches with the OTP generated and displayed to the user, the user is granted permission to control the linked home appliances in the system securely. This makes it possible for only those that are allowed to have access to operate on the devices. However, if the OTP entered by the user is incorrect, then the system also denies access & interrupts the process, and deletes further attempts to ensure the privacy and security of the system. This mechanism offers protection against unauthorized access and guarantees the security of the home automation system(Aparna Gira, 2022).

Appliance Control

Once the user interacts and gets authenticated, they can, in a way, manage the home appliances from a distance away. This range covers switching on appliances or off, setting, and other tasks as per the need of a particular appliance. The system interprets the user's instructions or inputs and sends out signals to the target appliances to perform the required actions(Okubanjo *et al*., 2021).

Energy Monitoring

The home automation system keeps track of the energy consumption of the appliances all the time. It records energy consumption and displays information for the user via the monitor, having controls on the front side. This lets the user monitor the energy being used regularly, make proper decisions on overcoming energy wastage, and make proper management on how the energy is used for payment efficiency and the general welfare of the environment(Reza, 2022).

Testing and Validation

In order to increase the reliability, security, and efficiency of the home automation system, testing and validation procedures were performed. This process addressed the main components of the system interacting with the user, such as authentication, remote and local control, and energy display.

Authentication Process

Access control in the home automation system is a process that is intended to prevent unauthorized access to the system. It uses both password and OTP (one-time password) authentication. The system was duly checked, and through it, the capability of the system to authenticate the users and also generate and authenticate the OTPs was confirmed. The above testing proved very vital as far as avoiding any access to the system by unauthorized personnel and making sure that the system is very secure(Saxena & Pal, 2020).

Remote Control via GSM

To check the efficiency of the system's ability to function as a remote control, the GSM module's ability to receive and process SMS commands was effectively tested. The testing concentrated on the correctness of receiving SMS commands as well as the correct execution of the home automation system command according to the module's parameters. This made sure that users can control appliances from a distance and in the most effective manner(Okubanjo *et al*., 2021).

Local Control via Bluetooth

During the Bluetooth integration phase, the system's local control functionality was tested by enabling users to manage appliances through a secure Bluetooth connection. SMS-based authentication was utilized as an additional layer of security to authorize the activation of the Bluetooth module. The MIT App Inventor platform was used to develop the smartphone application for Bluetooth communication, allowing users to input encrypted credentials. To enhance Bluetooth security, AES encryption was implemented for password validation and data exchange, ensuring that all communications between the system and the user's smartphone were secure. A final assessment confirmed that the system successfully established secure Bluetooth links with the user's smartphone, enabling reliable local control of appliances without requiring internet connectivity(Arijit Pal *et al*., 2015).

Energy Data Transmission

Energy consumption data transmission accuracy was verified to confirm that the system could give real-time feedback to the user. Their efficiency in gathering as well as transmitting only accurate info on energy consumption was established as a way to inform users of energy use. This testing was important for helping users make decisions about energy savings(Reza, 2022).

User Blocking Mechanism

Thus, to improve security from brute-force attacks, the system contains a user-blocking mechanism that temporarily disables the user after several attempts to enter the wrong password. To make hacking or guesses to accounts, the system disables user log-ins for a short time after certain tries are complete. This mechanism enhances the security of an account since attempts to crack an account will take a very long time to offer a level of protection to prevent unauthorized access to the database(Nivethika *et al*., 2023).

Why We Use this System

The system utilizes Bluetooth in addition to the GSM technology to afford high security and multiple access. This feature makes it functional in one-handed

mode, as well as using the frequent dual-system approach, which guarantees dependability, even in cases when there is a problem with a network. In such cases, users can easily switch to Bluetooth to gain access to the system. Bluetooth is more beneficial when users of a device are nearby, within a specific room, or Nigeria has an operating range of up to a hundred meters. It is an inexpensive solution because it gains outside access without requiring extra operational expenses for security and access assurance. The integration of Bluetooth with GSM is that the best of both worlds of each technology is that both are flexible, inexpensive, and reliable for both short- and long-range communication.

RESULTS

The implementation and testing of the secure home automation system (HAS), integrating GSM and Bluetooth technologies, produced the following key results:

GSM-Based Remote Control Possibilities:

- Functionality: The use of the GSM module that is SIM 900 allowed for controlling the appliances through SMS. Accessing the option, where the predefined password and the OTP are entered, the user could send commands for the operation of devices such as lights and ANSYS fans.
- Response Time: Average response times remained at high levels with 5-10 seconds during the normal traffic. Some lags were experienced when there was traffic congestion in the network.
- Reliability: A stable performance was carved throughout the sessions whereby several testing locations possessed a good cellular signal.

Local Control via Bluetooth

- Functionality: For local control, the device with the Bluetooth module (HC-12) allowed easy control through Bluetooth-enabled devices. The users were required to sign on through an SMS and then sync their mobile phones to the system to give commands.
- Security: No such things as a man at the bathroom door happen in the testing, proving that secure communication prevails after authentication.
- Range (Novel Contribution): The HC-12 Bluetooth module increased the range of local control up to around 100 meters, which greatly increases the flexibility compared to the standard Bluetooth, which has a maximum range of around 10 meters for the standard Bluetooth modules. Perhaps the most notable of these is the newly available greater range of distance beaters can now deliver for medium to large homes.

Energy Monitoring

- Simulation: Actual real-time energy consumption data in the simulation was relayed through SMS after every appliance control command.
- Accuracy: A view was created to mimic real energy usage and provide appropriate feedback using standard appliance utilization parameters.
- User Awareness: They were given prompt reports of their energy consumption to allow them to make informed choices and enhance energy conservation.
- Identification and Authentication of a System
- Two-Factor Authentication (Novel Contribution): The system used a proven two-factor authorization method that included an option to use a password and an OTP.
- Password Authentication: Real-time verification prevented unauthorized users from gaining access to the web application, while three consecutive attempts locked out the user.
- OTP Authentication: OTPs were generated as well as delivered in less time and validated OTPs within the given time frame; OTP added an extra layer of security.
- Enhanced Security: The adoption of this two-fold approach to authentication makes it a step up from the historically used one-layer systems and consequently eliminates risks of actual threats like brutal force attacks.

System Usability and User Experience

- Ease of Use: Users interfaced with the system with simple text commands via SMS and an accessible Bluetooth control system.
- Feedback and Error Handling: The system also gave clear messages through the SMS and the actions performed successfully and messages that there were wrong inputs made by the user.

DISCUSSION

The home automation system that has been proposed to use GSM and Bluetooth enables users to efficiently control their home appliances using a secure platform. The insights generated from the findings that are presented below will highlight the use as well as the limitations of integrating these communication technologies.

A study of GSM & Bluetooth Communications for Secure Home Automation

- Remote Control with GSM: One application was the use of GSM technology in remote control using the method of SMS, with the advantage of its operation at great distances (M. A. Abubakar *et al.*, 2020). However, network congestion sometimes affects the delivery of the message, which sometimes offends the user experience(H. A. Abubakar *et al.*, 2022).

Possible enhancements to extend such limitations in the future include using better athletic communication in LTEs or 5Gs (Chiranjivi1 *et al*., n.d.).

- Local Control with Bluetooth: Bluetooth allows secure local control following SMS-based authentication. For a 100-meter range, Bluetooth was effective with its HC-12 history(Rakib *et al*., 2021). However, they might be a little limited, especially in large-scale homes. Architectural Digest has a smaller range than other sites. That could be improved by switching to more contemporary protocols like Zigbee, Wi-Fi, or Bluetooth Low Energy (BLE)(Reza, 2022).

Security and Authentication Mechanisms

- Password Authentication: Static passwords however as much as they may improve security can become compromised in the long run. Implementations of Strong Passwords: While risks were helped with regular personnel password updates, future versions may include dynamic passwords, or biometric authentications(Murugan *et al*., 2023).
- OTP Authentication: To implement the recommendations made on the recommendations page, the following observations should be made:(Aparna Gira, 2022)As for reducing the level of security threat, encrypted messaging protocols or secure applications could be used(Matura & Kunal, 2024).

Energy Monitoring and Efficiency

- The fake energy monitoring feature of the system, where the researchers monitored actual electronic energy, showed that the system had the possibility of fostering energy-efficient behaviors when users had a way of monitoring reliability in real-time energy use(Rakib *et al*., 2021). The real interaction with connected IoT meters for tracking and detailed analytics in the cloud for additional precision(Singh *et al.*, 2016) can add a level of deeper analysis of energy utilization.

Usability and User Experience

- This was achieved through the development of the interface, which was made simple such that a regular user of the internet would not have any trouble at all using the system. Perhaps a specific application on the user's smartphone could simplify his or her interactions with the system by including features such as scheduling an appliance, checking on the status of a particular appliance, and controlling these devices through voice commands through such programs as Alexa or Google Assistant(Singh *et al*., 2016).

System Limitations

- SMS Delays: Network congestion in the delivery of SMS also leans performance. Besides, going to higher protocols, for instance, Wi-Fi or Zigbee, would contribute to overcoming these limitations(Teymourzadeh *et al*., 2013).
- Simulated Energy Monitoring: Although the use of simulators with energy metering devices helped show possibilities, real integration of the program with the actual energy metering devices is important for precise tracking and data that can be used in problem-solving.

Future Enhancements

- Cloud Integration: Expanded cloud-based storage and analysis would improve energy management, give clients more distant access to their data, increase sophistication, and improve control of planetary energy consumption.
- IoT Integration: This was due to the integration of IoT protocols, including MQTT, that might provide a more accurate means of tracking real-time energy monitoring and efficient device compatibility(Singh *et al.*, 2016).
- Advanced Security: To additionally discourage capers to the databases, shifting toward biometric verification and using encrypted communication methods can also be of utter use.
- Smart Ecosystem Compatibility: Connecting the system with other intelligent home platforms such as Amazon Alexa and Google Home would be more convenient for the users; at the same time, the system would have the opportunity to connect with the other smart devices, and so the flexibility of the system would be provided.
- Bluetooth Range: Because Bluetooth is limited to short distances, this suggests that there is a fresh need for enhanced methods of connection in larger homes or areas that Bluetooth may not cover signals well. This could be done using other broader technologies like Zigbee or Wi-Fi integrated to perform additional functions.

CONCLUSION

An effective use of GSM and Bluetooth technologies to design a home automation system shows a safe way towards the implementation of the modern smart home application. The features successfully implement remote and local management of household appliances with a strong emphasis on security, which requires a password and OTP.

Key achievements of the system include:

- Reliable remote control via GSM enables users to manage appliances virtually anywhere.

- Secure local control using Bluetooth, offering seamless operation within range.
- Simulated real-time energy monitoring, promoting conscious energy consumption.

Some drawbacks were identified, which include the following: The system was successful, but some drawbacks include that there was some delay in sending the SMS, Bluetooth has a limited range, and the power data was dummy. The features can be added in future releases to overcome these difficulties, including Wi-Fi, Zigbee, or 5G communication; IoT-based energy meters in real time; and cloud analytics for better energy control.

In conclusion, this work offers a good research platform for future smart home solutions further using traditional and novel communication technologies. Still, it is possible to continue the development of such a system: improve the security features, combine them with IoT appliances, adjust to the existing smart environment, and make other improvements, which would make it a comprehensive, scalable platform for the advanced home automation system of the future.

REFERENCES

- Abubakar, H. A., Araoye Adegboye, B., James, T. O., Olatomiwa, L., & Dauda, U. S. (2022). Development of An Enhanced Home Automation System For Energy Saving Using GSM, Internet of Things and Bluetooth Technologies. *Proceedings of the 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development, NIGERCON 2022*, 1–5. https://doi.org/10.1109/NIGERCON54645.2022.9803133
- Abubakar, M. A., Adepoju, T. M., Okunlola, M. O., Abodunrin, F. O., & Bakare, U. (2020). Gsm Based Home Automation. *International Journal of Science, Engineering & Environmental*, *5*(6), 54–59. https://www.researchgate.net/publication/346015292
- Aparna Gira. (2022). *DEVELOPMENT OF GSM BASED ADVANCED DIGITAL DOOR LOCKING SYSTEM*. *9*(12), 356–363.
- Aravind.S. (n.d.). Arduino and HC-12 Long Range Wireless Communication Module - HowToMechatronics. *International Journal of Advanced Research in Electronics and Communication Engineering*, *4*(10). Retrieved November 15, 2024, from https://howtomechatronics.com/tutorials/arduino/arduino-and-hc-12-long-range-wireless-communication-module/
- Arijit Pal, Akanksha Singh, & Bijay Rai. (2015). GSM Based Home Automation, Safety and Security System Using Android Mobile Phone. *International Journal of Engineering Research And*, *V4*(05). https://doi.org/10.17577/ijertv4is050648
- Chiranjivi1, M., Suresh2, K., Chandranshekar3, G., & Siddarth4, M. (n.d.). AN ADVANCED LOCK SYSTEM USING NOVEL SECURITY INTEGRATION. *Journal of Nonlinear Analysis and Optimization*, *15*, 2024.
- Hamidi, E. A. Z., Effendi, M. R., Syarifuddin, F., Wildan, M., & Huda, U. N. (2021). Design and implementation of prototype smart plug at home automation based on bluetooth using Arduino Uno. *IOP Conference Series: Materials Science and Engineering*, *1098*(4), 042066. https://doi.org/10.1088/1757-899x/1098/4/042066
- Hossain Shawon, M. S., Das, C., Ahammed, M. T., Biswas, G., Mia, M. S., Akter Eva, E., & Sakib, M. N. (2022). Voice Controlled Smart Home Automation System Using Bluetooth Technology. *4th International Conference on Recent Trends in Computer Science and Technology, ICRTCST 2021 - Proceedings*, 67–72. https://doi.org/10.1109/ICRTCST54752.2022.9781967
- Jagdalpur, A. E. E. G. E. C. (2018). *Scrutiny of Commercial Automation System To Monitor &*. *7*(7), 75–86.
- Jivani, M. N. (2014). GSM Based Home Automation System Using App-Inventor for Android Mobile Phone. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, *03*(09), 12121–12128. https://doi.org/10.15662/ijareeie.2014.0309042
- Kumar, M., & Devachandra Singh, T. (2021). Design and Development of Bluetooth Based Home Automation System Using FPGA. *International Journal of Applied Engineering Research*, *16*(10), 830–838. http://www.ripublication.com
- Maniam, T. S., AMajid, H., Esmail, B. A. F., & Ibrahim, M. Y. (2019). GSM Based Automated Home Application Power Consumption Reading System. *Journal of Electrical Power and Electronic Systems*, *1*(2), 1–5.
- Matura, R., & Kunal. (2024). Secure and User-Friendly Smart Home Automation: A Mobile-Centric IoT Approach. *Journal of Trends in Computer Science and Smart Technology*, *6*(2), 180–198. https://doi.org/10.36548/jtcsst.2024.2.007
- Murugan, K., Dhanesh, R., Diliphan, R., Gowtham, S., Sabari, S. G., Suganyadevi, S., Alsalami, Z., & Gogineni, N. (2023). Enforcement in the Security of ATM Pin Entry. *International Conference for Technological Engineering and Its Applications in Sustainable Development, ICTEASD 2023*, 143–145. https://doi.org/10.1109/ICTEASD57136.2023.10585235
- Nivethika, S. D., Pandian, M. S., Parameswaran, N. G. S., Elakiya, E., Naresh, M., & Dhamodharan, S. (2023). Arduino UNO Based OTP Lock for Integrated Home Security System. *Proceedings of the 2nd International Conference on Edge*

Computing and Applications, ICECAA 2023, 1342–1347. https://doi.org/10.1109/ICECAA58104.2023.10212109

- Okubanjo, A., Okandeji, A. A., Abolade, O. R., Alao, P. O., Okubanjo, A. A., Okandeji, A. A., Abolade, O. R., & Alao, O. P. (2021). DEVELOPMENT OF GSM BASED HOME AUTOMATION SYSTEM USING ARDUINO UNO MICROCONTROLLER. In *FUW Trends in Science & Technology Journal, www.ftstjournal.com e-ISSN* (Vol. 6, Issue 2). www.iea.org
- R. kingsly Stephen. (2020). GSM based home automation system. *International Journal of Engineering Science and Computing*, *10*(6), 26324–26326.
- Rakib, M. A. Al, Rahman, M. M., Rana, M. S., Islam, M. S., & Abbas, F. I. (2021). GSM Based Home Safety and Security System. *European Journal of Engineering and Technology Research*, *6*(6), 69–73. https://doi.org/10.24018/ejers.2021.6.6.2580
- Rani, A. (2024). IoT based Home Automation Control using Feedback System. *2024 International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS)*, 464–468. https://doi.org/10.1109/ICICNIS64247.2024.10823290
- Reza, M. S. (2022). Low-cost approach plan and development of GSM-based smart home automation system. *International Journal of Research In Science & Engineering*, *31*, 1–8. https://doi.org/10.55529/ijrise.31.1.8
- Santos, D., Ad, J. A. S. B., Verlag, A. S., Lncs, G., Sendra, S., Laborda, A., Díaz, J. R., & Lloret, J. (2014). *Ad-hoc, Mobile, and Wireless Networks*. *8487*. https://doi.org/10.1007/978-3-319-07425-2
- Sarmah, R., Bhuyan, M., & Bhuyan, M. H. (2019). SURE-H: A Secure IoT Enabled Smart Home System. *IEEE 5th World Forum on Internet of Things, WF-IoT 2019 - Conference Proceedings*, 59–63. https://doi.org/10.1109/WF-IoT.2019.8767229
- Saxena, A., & Pal, R. (2020). IoT Based Security and Controlled Smart Home Automation System Using GSM. *International Journal of Research in Engineering, Science and Management*, *3*(8), 445–448.
- Singh, P., Chotalia, K., Pingale, S., & Kadam, S. (2016). A review paper on smart GSM based home automation system. *International Research Journal of Engineering and Technology (IRJET)*, *3*(04), 1838–1843. www.irjet.net
- Stolojescu-crisan, C., Crisan, C., & Butunoi, B. (2021). *Sensors-21-03784-V2.Pdf*. 1–23.
- T[1], S., B[2], S., & S[3], T. (2016). Smart control of Electronic Appliances and Digital Notice Board using GSM and Bluetooth. *International Research Journal of Engineering and Technology*, *2*, 285–290. www.irjet.net
- Teymourzadeh, R., Ahmed, S. A., Chan, K. W., & Hoong, M. V. (2013). Smart GSM based home automation system. *Proceedings - 2013 IEEE Conference on Systems, Process and Control, ICSPC 2013*, 306–309. https://doi.org/10.1109/SPC.2013.6735152
- Yuneela, K., & Sharma, A. (2022). A Review Paper on Technologies used in Home Automation System. *Proceedings - 6th International Conference on Computing Methodologies and Communication, ICCMC 2022*, *Iccmc*, 366–371. https://doi.org/10.1109/ICCMC53470.2022.9753928.