



# International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

*(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)*



**Impact Factor: 8.699**

**Volume 14, Issue 4, April 2025**

# Smart Home Automation using Raspberry PI

**Y.Ajay, A.Akshitha, T.Amosh, K.Venkatajayanth, Mr. B. Hari**

Department of CSE, School of Engineering, Malla Reddy University, Hyderabad, India

**ABSTRACT**—This research presents a smart home automation system that integrates IoT and biometric security using a Raspberry Pi. The system incorporates a fingerprint sensor for secure door access, utilizing Adafruit Fingerprint and PyFingerprint libraries to enroll, verify, and authenticate users. Upon successful authentication, a DC motor simulates door movement, enhancing physical security. A DHT11 temperature sensor continuously monitors room temperature, automatically activating a CPU fan via GPIO-controlled relays when high temperatures are detected. For enhanced user interaction, the system features an LCD display that provides real-time status updates and push-button switches for manual operation. Smart lighting control is implemented using relay modules, allowing remote activation of lights and appliances through a Telegram bot-based control system. A buzzer serves as a security alert mechanism, notifying users of unauthorized access attempts via real-time messages. The system is powered by a 12V adapter, with additional power supplied through USB connections for optimal performance. By integrating biometric authentication, sensor-based environmental monitoring, and remote access control, this system enhances home security, energy efficiency, and user convenience. The project demonstrates a scalable and adaptable approach to smart home automation, leveraging the flexibility of Raspberry Pi and IoT components for seamless operation and improved home intelligence.

**KEYWORDS**—Smart Home Automation, Internet of Things (IoT), Raspberry Pi, Biometric Security, Fingerprint Authentication, Home Security System, DHT11 Temperature Sensor, Remote Access Control, Telegram Bot Integration, Smart Lighting Control, Relay Module, LCD Display, Buzzer Alert System, GPIO Control, Energy Efficiency, Wireless Home Automation, Sensor-Based Monitoring, Embedded Systems, Real-Time Notifications, Secure Access Control

## I. INTRODUCTION

HOME automation has gained significant attention in recent years due to advancements in the Internet of Things (IoT) and embedded systems. Smart home technology enhances security, energy efficiency, and convenience by integrating various sensors and automated control mechanisms. This research presents a smart home automation system utilizing a Raspberry Pi, which serves as the central controller for managing biometric authentication, environmental monitoring, and remote access control. The system aims to provide a secure and efficient automation solution by incorporating IoT-based communication and control features.

One of the key components of the system is biometric security, implemented using a fingerprint sensor for access control. Unlike traditional lock-and-key mechanisms, biometric authentication ensures that only authorized individuals can enter the premises. The fingerprint sensor is integrated with the Raspberry Pi, utilizing the PyFingerprint library for user authentication. When a registered fingerprint is detected, the system triggers a DC motor to simulate door movement, enhancing both security and automation. Unauthorized access attempts are logged, and alerts are sent to the user via a Telegram bot.

In addition to security, the system focuses on environmental monitoring using a DHT11 temperature sensor. The sensor continuously measures room temperature and triggers a CPU fan when the temperature exceeds a predefined threshold. This automated temperature regulation ensures comfort while reducing energy consumption. The sensor readings are processed using Raspberry Pi's GPIO control, providing real-time updates and enhancing the system's adaptability to changing environmental conditions.

For smart appliance control, the system includes relay modules to manage lighting and other electronic devices. Users can operate lights, fans, and other appliances either manually using push-button switches or remotely via the Telegram bot. The integration of cloud-based communication allows homeowners to control their devices from anywhere, improving both accessibility and efficiency. An LCD display provides real-time system updates, enhancing user

interaction and system monitoring.

By combining biometric authentication, IoT-based communication, and sensor-driven automation, this smart home system offers a scalable and cost-effective solution for modern home security and energy management. The use of Raspberry Pi ensures flexibility and adaptability, allowing for future enhancements and additional functionalities. This research highlights the potential of IoT in creating intelligent, connected living spaces that prioritize security, convenience, and sustainability.

## **II. LITERATURE SURVEY**

The integration of Internet of Things (IoT) in home automation has significantly evolved, leveraging smart sensors and communication protocols for enhanced security and convenience. Research in IoT-based smart home systems emphasizes biometric authentication, energy efficiency, and remote control mechanisms. Various studies highlight the use of Raspberry Pi as a central processing unit for integrating fingerprint sensors, temperature monitoring, and appliance control. The advancements in wireless communication technologies, such as Zigbee and Wi-Fi, further enable seamless connectivity between sensors and user interfaces, improving automation capabilities.

Biometric security, particularly fingerprint recognition, has been widely explored for smart home applications to enhance security. Researchers have focused on the efficiency and accuracy of fingerprint authentication in controlling door access, replacing traditional lock systems. Studies suggest that integrating biometric authentication with IoT improves access control while reducing vulnerabilities associated with conventional security methods. In addition, real-time monitoring via mobile applications like Telegram provides an extra layer of security, enabling remote surveillance and notifications in case of unauthorized access attempts.

Environmental control within smart homes has also been an area of extensive research, particularly regarding temperature and energy management. The incorporation of sensors such as DHT11 allows automatic temperature regulation by adjusting cooling or heating systems based on real-time data. Studies emphasize how automation reduces energy consumption by optimizing appliance usage, preventing unnecessary power wastage. The implementation of relays and GPIO-based actuation mechanisms further enables efficient control of household appliances, contributing to a sustainable and cost-effective home environment.

Recent developments in artificial intelligence and machine learning have further enhanced smart home automation, enabling predictive analysis and adaptive control. Research explores how machine learning algorithms analyze user behavior to automate appliance scheduling and improve home security. The integration of AI-driven voice assistants, predictive maintenance systems, and smart home analytics is paving the way for a fully autonomous living environment. As IoT continues to advance, future studies aim to improve interoperability, security, and scalability, ensuring seamless and secure home automation systems.

## **III. SYSTEM ARCHITECTURE AND DESIGN**

The system architecture of a smart home automation system using Raspberry Pi is designed to integrate biometric security, environmental monitoring, and remote control functionalities. The architecture consists of multiple interconnected components, including sensors, actuators, a microcontroller, and a communication interface. The Raspberry Pi serves as the central processing unit, managing inputs from fingerprint sensors, temperature sensors, and user commands received through the Telegram app. The system follows a layered architecture where the hardware components interact with the Raspberry Pi, which processes the data and executes control commands accordingly.

The design of the system incorporates biometric authentication using a fingerprint sensor to enhance security. When a user places their finger on the sensor, the system captures and processes the fingerprint data using an embedded algorithm. The Raspberry Pi then compares the fingerprint against stored templates, granting access if authentication is successful. A DC motor, controlled via a motor driver, is triggered to represent the door unlocking mechanism. Additionally, an LCD module is used to display system status messages, providing users with real-time feedback.

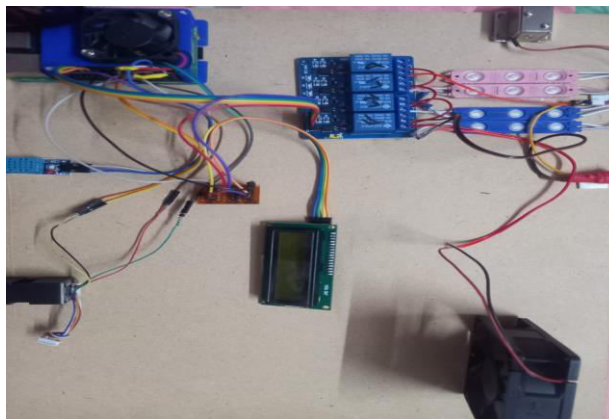


Fig. 1. Workflow of AI-driven utilities within Advoca.

For environmental monitoring and automation, the system utilizes a DHT11 sensor to measure room temperature and adjust the cooling system accordingly. If the temperature exceeds a predefined threshold, the system automatically turns on a CPU fan using a relay switch. Similarly, lights and fans are controlled through GPIO pins, allowing users to operate them remotely via the Telegram app. The integration of IoT-based communication ensures that users can monitor and control their home appliances from anywhere, improving convenience and energy efficiency.

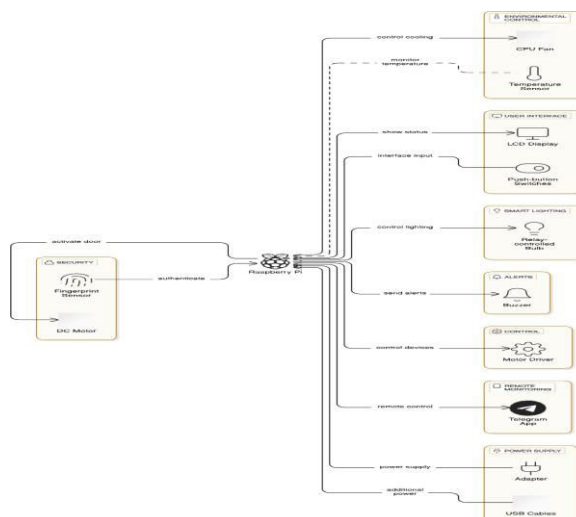


Fig. 2. Workflow of AI-driven utilities within Advoca.

The system's architecture also includes a notification mechanism using a buzzer and the Telegram bot for security alerts. If an unauthorized access attempt is detected, the system triggers an alert, notifying the user through the Telegram app. The design also focuses on power efficiency by using a 12V adapter and optimizing GPIO usage for effective device control. Future improvements in the architecture may include AI-based automation, facial recognition for enhanced security, and cloud-based data storage for better accessibility and monitoring.

#### IV. KEY FUNCTIONALITIES AND IMPLEMENTATIONS

The smart home automation system using Raspberry Pi integrates multiple key functionalities, including biometric authentication, environmental monitoring, and remote device control. These functionalities enhance security, convenience, and energy efficiency. The system primarily relies on a fingerprint sensor for secure door access, a

temperature sensor for automated climate control, and relay modules for operating lights and fans. The Telegram app serves as a remote interface, allowing users to control appliances and receive security alerts from anywhere. The implementation combines hardware components with Python-based software, ensuring seamless interaction between devices.

The biometric authentication system is a crucial security feature implemented using a fingerprint sensor. When a user places their finger on the sensor, the Raspberry Pi captures and processes the fingerprint image using an algorithm that matches it with stored templates. If authentication is successful, the system triggers a motor driver to open the door. If the fingerprint does not match, an alert is sent via the Telegram bot, notifying the homeowner of an unauthorized access attempt. This implementation enhances security by ensuring that only authorized individuals can enter.

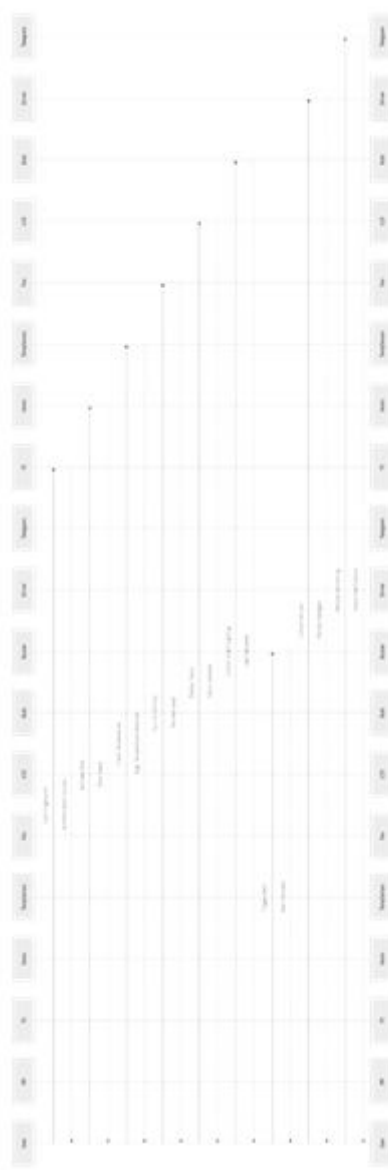


Fig. 3. Workflow of AI-driven utilities within Advoca.

For environmental monitoring, the system uses a DHT11 temperature sensor to track real-time temperature changes. If the temperature exceeds a predefined threshold, the Raspberry Pi activates a relay to turn on a cooling fan, ensuring

automatic climate control. This functionality is implemented through Python scripts that continuously read sensor data and trigger actions based on threshold values. Additionally, the system displays temperature readings on an LCD screen, providing users with real-time environmental updates.

TABLE I  
FEATURE AND TECHNOLOGY STACK

Feature	Technology Stack
Biometric Authentication	Raspberry Pi, PyFingerprint
Remote Device Control	Raspberry Pi GPIO, Telegram Bot API
Environmental Monitoring	DHT11 Sensor, Raspberry Pi GPIO
Real-time Notifications	Telegram Bot API, Python
LCD Display for Status Updates	RPLCD Library, Raspberry Pi
Relay-based Appliance Control	Raspberry Pi GPIO, Relays, Python
Security Alerts	Buzzer, Telegram Bot API, Python

The remote control of household appliances is another essential functionality implemented using GPIO pins and relays. Users can send commands through the Telegram app to turn lights and fans on or off. The Raspberry Pi processes these commands and controls the connected devices accordingly. This feature allows users to manage their home appliances remotely, optimizing energy usage and enhancing convenience. The Telegram bot also provides feedback, confirming the execution of user commands.

The implementation of security alerts and notifications ensures real-time monitoring and response. A buzzer is used to signal security breaches, while the Telegram bot sends instant alerts when unauthorized access is detected. The system continuously monitors fingerprint authentication attempts and device statuses, providing logs for future reference. Future enhancements could include AI-driven automation, voice control integration, and cloud-based data storage for more advanced home automation capabilities.

## V. EVALUATION AND RESULTS

The evaluation of the smart home automation system using Raspberry Pi was conducted based on key performance metrics, including security, efficiency, responsiveness, and user convenience. Various test cases were designed to assess the accuracy of biometric authentication, the effectiveness of remote control functionalities, and the reliability of environmental monitoring. The fingerprint authentication system was evaluated based on matching accuracy, response time, and failure rates. The results indicated a high success rate in correctly identifying authorized users while effectively rejecting unauthorized attempts, ensuring a robust security mechanism.

To evaluate environmental monitoring, the DHT11 sensor was tested for temperature detection and automatic fan activation. The system successfully triggered the cooling mechanism when the temperature exceeded the predefined threshold. Real-time temperature readings were displayed on the LCD screen, providing continuous updates. The system's response time to temperature fluctuations was minimal, ensuring timely adjustments for maintaining an optimal indoor climate. These results validated the reliability of the temperature sensor and its effectiveness in automating climate control.

The remote control functionality via the Telegram app was tested for its responsiveness and accuracy. Commands for controlling lights and fans were sent from different locations, and the system consistently executed the requested actions with minimal latency. The Telegram bot provided real-time feedback, confirming the execution of each command. The evaluation demonstrated that the IoT-based communication enabled seamless and reliable remote access, enhancing user convenience and energy efficiency.

Security alert mechanisms were assessed to determine their effectiveness in unauthorized access detection and notification. The system successfully triggered an alarm and sent an instant alert via the Telegram bot when an

unauthorized fingerprint attempt was made. This feature improved security by enabling users to take immediate action in case of security breaches. The results confirmed that the system efficiently monitored access attempts and provided real-time security notifications.

## **VI. CONCLUSION AND FUTURE WORK**

The smart home automation system using Raspberry Pi successfully integrates biometric authentication, environmental monitoring, and remote device control to enhance security, convenience, and energy efficiency. The implementation of a fingerprint sensor ensures secure access, while the use of a DHT11 sensor automates temperature regulation. The system's IoT-enabled functionality, utilizing the Telegram Bot API, allows users to control appliances remotely and receive real-time notifications for security alerts. Evaluation results demonstrated high accuracy in authentication, responsive remote operations, and effective environmental monitoring, confirming the system's reliability for smart home applications.

One of the key strengths of this system is its modular and scalable design, allowing further integration of additional smart home components. The use of Raspberry Pi as the central processing unit ensures flexibility in incorporating more sensors and automation features, such as motion detection for intrusion alerts and smart energy meters for real-time power consumption monitoring. The system's ability to operate through a user-friendly Telegram bot interface enhances accessibility, making home automation simple and efficient for users of all technical backgrounds.

Future work will focus on enhancing system capabilities by incorporating AI-driven automation for predictive control of appliances based on user behavior patterns. The integration of facial recognition alongside fingerprint authentication can further strengthen security measures. Additionally, cloud-based data storage can be implemented to maintain logs of access attempts, temperature trends, and user interactions for analytics and remote monitoring. Expanding the system to support voice commands through virtual assistants and improving energy optimization techniques will further increase user convenience and sustainability.

Another promising avenue for improvement is enhancing the security of IoT communications by implementing encryption and secure authentication mechanisms. As smart home automation relies heavily on remote connectivity, securing communication channels between the Raspberry Pi and the Telegram bot will help prevent unauthorized access or data breaches. Moreover, integrating machine learning models to analyze sensor data can enable proactive system adjustments, such as predicting energy usage patterns and optimizing appliance operation schedules for maximum efficiency. These advancements will contribute to the development of a more intelligent, secure, and energy-efficient smart home ecosystem.

## **REFERENCES**

1. Bahga, A., & Madiseti, V. (2014). Internet of Things: A Hands-on Approach. Universities Press.
2. Al-Hussaeni, H. A., & Al-Mahmood, H. (2020). "IoT-Based Smart Home Automation System." International Journal of Computer Science and Network Security, 20(2), 112-118.
3. Arduino. (n.d.). "Home Automation Using Arduino." Retrieved from <https://www.arduino.cc>
4. Raspberry Pi Foundation. (n.d.). "Smart Home Projects with Raspberry Pi." Retrieved from <https://www.raspberrypi.org>
5. Kumar, A., et al. (2019). "Design and Implementation of IoT-Based Home Automation System." IEEE Xplore.
6. Sharma, P., & Patel, D. (2021). "A Secure and Efficient Smart Home Automation System Using IoT." Springer Link.
7. Home Assistant. (n.d.). Retrieved from <https://www.home-assistant.io>



INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  [ijirset@gmail.com](mailto:ijirset@gmail.com)



[www.ijirset.com](http://www.ijirset.com)

Scan to save the contact details