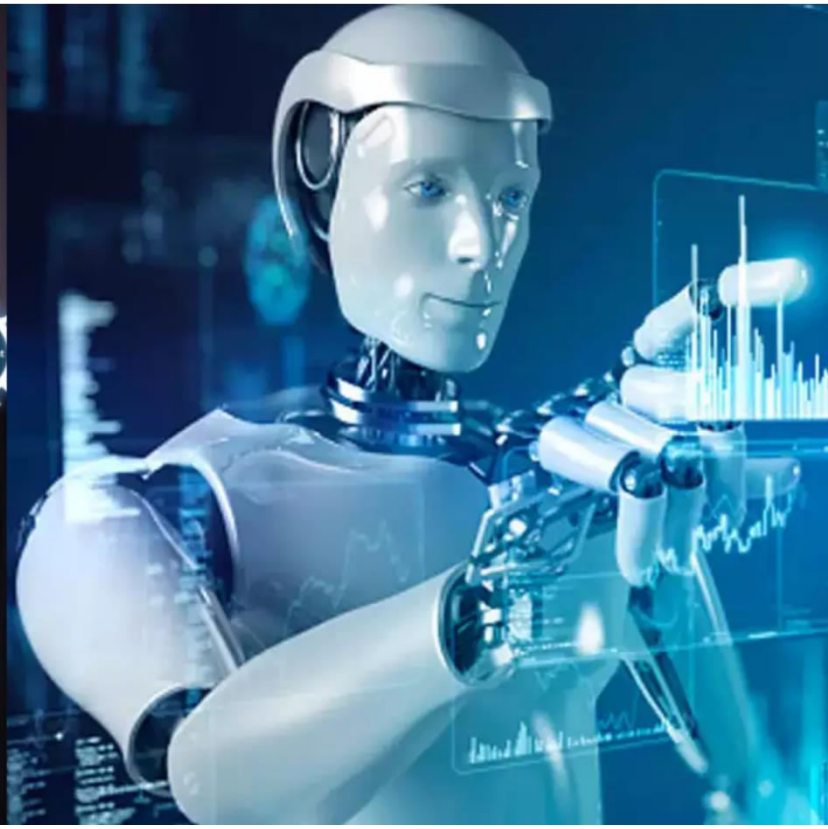
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

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

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

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404632|

Raspberry Pi-Based Smart Building Security with Multi-Module Automation

Shaikh Parvez Lalabhai[1], Prof. S. G. Joshi[2]

Student, VACOE, Ahmednagar, India[1]

Professor, VACOE, Ahmednagar, India[2]

ABSTRACT: The proposed Raspberry Pi-based smart building security system is designed to integrate multiple automated modules, providing comprehensive safety and convenience for residents. The system features an RFID-based gate control, allowing only authorized individuals to access the building by automatically opening and closing the gate upon recognizing a valid RFID tag. Additionally, a PIR sensor-based motion detection module monitors human or vehicle movement, automatically turning on lights when motion is detected and turning them off when no movement is sensed, conserving energy. The system also includes a keypad-based door access module, where users can enter a personalized password to unlock doors, adding an extra layer of security. For enhanced home security. To ensure fire safety, an MQ3 sensor-based fire detection module is implemented, which sends real-time alerts via a GSM module to notify the user of potential fire hazards. Another important feature is the suspicious activity detection module, which utilizes sensors and possibly camera systems to identify unusual movements or behaviors around the premises, sending alerts to the user to take timely action. By combining RFID, motion detection, keypad access, fire alerts, fingerprint authentication, and suspicious activity detection, the Raspberry Pi-based system offers a robust and integrated smart security solution for modern homes and buildings.

KEYWORDS: Raspberry Pi, Smart building security system, RFID-based gate control, Authorized access, PIR sensor, Alert System, Water Level Detection

I. INTRODUCTION

In recent years, the demand for intelligent and automated security solutions has grown significantly due to the increasing concerns over residential safety and energy efficiency. With advancements in embedded systems and the Internet of Things (IoT), smart security systems have become more accessible and customizable for a wide range of users. This paper presents a Raspberry Pi-based smart building security system designed to offer a modular, scalable, and cost-effective approach to modern home security. By integrating various technologies such as RFID, biometric authentication, motion detection, and wireless communication, the proposed system addresses key aspects of building safety and automation.

The system architecture consists of multiple independent yet interconnected modules, each tailored to handle specific security functions. These include an RFID-based gate control module that permits access exclusively to authorized personnel, a keypad-based door access system, and a fingerprint-based biometric system for high-security zones such as personal lockers. Energy-efficient operation is achieved through a PIR sensor module that automates lighting based on motion detection, ensuring illumination only when necessary. Fire hazards are proactively addressed with an MQ3 sensor that detects smoke or flammable gases and notifies users in real time via a GSM module, enabling swift preventive action.

A standout feature of this system is its capability to detect suspicious activities through sensor or camera surveillance, enhancing security by identifying potential threats before they escalate. The use of Raspberry Pi as the central control unit allows for seamless integration and communication between modules, real-time processing, and remote monitoring. The modular design not only allows easy customization and expansion but also ensures that each component can function independently, thus enhancing system reliability. This paper explores the design, implementation, and performance of each module and demonstrates how their synergy creates a comprehensive and efficient smart building security solution.

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

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404632|

II. METHODOLOGY

The proposed smart building security system is designed with a modular architecture where each component functions independently while being coordinated through a central Raspberry Pi unit. The core of the system, the Raspberry Pi, acts as the main controller and communication hub, interfacing with all sensors and modules. The choice of Raspberry Pi is strategic due to its GPIO capabilities, processing power, and support for various programming environments, making it suitable for real-time data acquisition, processing, and alert generation. Python is used as the primary programming language to control the sensors, handle input/output logic, and manage system behavior. Communication between the modules is managed using GPIO pins and serial communication protocols, ensuring synchronized and reliable operations.

The RFID-based gate control module is implemented using an RFID reader (such as RC522) connected to the Raspberry Pi via SPI protocol. Each authorized individual is provided with a unique RFID tag. When a tag is scanned, its UID is compared against a predefined list stored in the Raspberry Pi database. If the UID matches an authorized entry, the system triggers a relay to operate a gate-opening mechanism, typically a servo or motorized gate controller. This mechanism ensures that only registered individuals can gain access to the premises. The system also logs each access attempt with a timestamp for auditing purposes. The keypad-based door access system follows a similar logic, where a 4x4 matrix keypad is used to input a password, which is validated against a secure password stored on the Raspberry Pi. Only correct entries unlock the electronic lock connected through a relay module.

For areas requiring enhanced security, such as lockers or private rooms, a fingerprint-based biometric authentication system is integrated using modules like the R305 or GT511C3 fingerprint sensor. These modules communicate with the Raspberry Pi via UART, capturing and comparing fingerprints against enrolled templates stored in memory. Only a successful fingerprint match triggers the door unlock relay, ensuring biometric-level security. To enhance safety and efficiency in building illumination, a PIR sensor-based motion detection module is employed. PIR sensors installed in strategic locations detect human or vehicle movement, and based on this input, the Raspberry Pi controls lighting circuits through relays. Lights are automatically turned on when movement is detected and turned off after a predefined period of inactivity, thus promoting energy conservation.

The system also integrates safety and alert mechanisms. A fire detection module using an MQ3 gas/smoke sensor continuously monitors air quality for the presence of smoke or flammable gases. When dangerous levels are detected, the system immediately triggers an alarm and sends a real-time alert via a GSM module (SIM800L/SIM900) connected to the Raspberry Pi through serial communication. The system can send SMS alerts to the homeowner's mobile phone, ensuring prompt notification even when the user is away. Additionally, a suspicious activity detection module employs either ultrasonic sensors or basic camera-based monitoring to detect unexpected movements in restricted or sensitive areas. Unusual patterns of motion trigger alerts that are logged and sent to the user. This proactive approach allows the system to serve not only as a reactive but also a preventive security solution. All modules are tested independently and then integrated into the final setup to ensure smooth interaction and reliable system performance.

III. DATA COLLECTION AND SENSOR DEPLOYMENT

The deployment of sensors in the proposed system is strategically planned to ensure maximum coverage and accurate data acquisition across various security and automation modules. Each sensor is selected based on its reliability, compatibility with the Raspberry Pi, and relevance to its specific function within the building security framework. The system comprises several sensor types, each catering to a particular domain of security such as access control, intrusion detection, biometric authentication, fire hazard detection, and intelligent lighting. Data from these sensors are collected in real time and processed directly on the Raspberry Pi using Python scripts, allowing the system to respond instantly to detected events. The collected data is not only used for immediate control operations—such as unlocking doors or turning on lights—but also logged in a local or cloud-based storage system for analysis and audit purposes.

Access control data is primarily collected through the RFID reader, keypad, and fingerprint sensor modules. The RFID reader is typically mounted at entry gates or building entrances, collecting unique identification tags (UIDs) from RFID cards. These UIDs are matched against a preloaded database to grant or deny access. The keypad, usually installed beside interior doors, captures numeric input sequences entered by users attempting to gain access to specific areas.

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

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404632|

Each entry is time-stamped and logged, whether successful or failed. The fingerprint sensor is deployed in high-security zones, such as personal lockers or restricted rooms, and collects biometric data for identity verification. All access events are recorded, and unsuccessful attempts can trigger alerts or increase surveillance sensitivity. This method ensures that the system not only grants access but also maintains a robust digital footprint of all entries and exits for security auditing and incident tracing.

Environmental and safety monitoring is achieved through deployment of PIR motion sensors, MQ3 gas sensors, and optionally camera modules for visual surveillance. PIR sensors are installed in corridors, entrances, stairwells, and parking zones to detect motion and trigger lighting circuits or raise alerts. Their placement is carefully planned to avoid blind spots while minimizing false positives from small animals or heat sources. The MQ3 gas sensor is mounted in kitchen areas, near gas lines, or inside enclosed spaces where smoke or alcohol vapors might concentrate. It continuously collects air quality data and alerts the user in case of a fire or gas leak hazard. For suspicious activity detection, ultrasonic sensors or Raspberry Pi-compatible cameras can be deployed at the periphery of the premises or near entry points to detect abnormal movement patterns. The system can compare this input with predefined thresholds or behavioral templates, and upon anomaly detection, send real-time SMS alerts using the GSM module. Data from all these sensors is routed to the Raspberry Pi through GPIO pins, SPI, I2C, or UART interfaces, depending on the sensor type. This comprehensive and modular sensor deployment ensures that every critical area of the building is under constant and intelligent surveillance, supporting a proactive and responsive smart security infrastructure.

IV. HARDWARE DESIGN

The hardware design of the proposed smart building security system revolves around the Raspberry Pi, which serves as the central processing and control unit. The Raspberry Pi 4 Model B is preferred due to its superior processing power, multiple USB ports, GPIO availability, and support for wireless communication protocols such as Wi-Fi and Bluetooth. It operates on Raspbian OS and executes Python scripts to manage sensor inputs, process data, and control actuators. A 5V/3A power supply is used to ensure stable operation. GPIO pins are assigned specific roles for interfacing with various modules including sensors, actuators, and communication devices. A microSD card is used for local data storage, while optional cloud storage can be integrated for remote monitoring and analytics. The Raspberry Pi's HDMI port is used during development and debugging to connect to a display, but in regular operation, it functions as a headless device controlled via SSH or VNC.

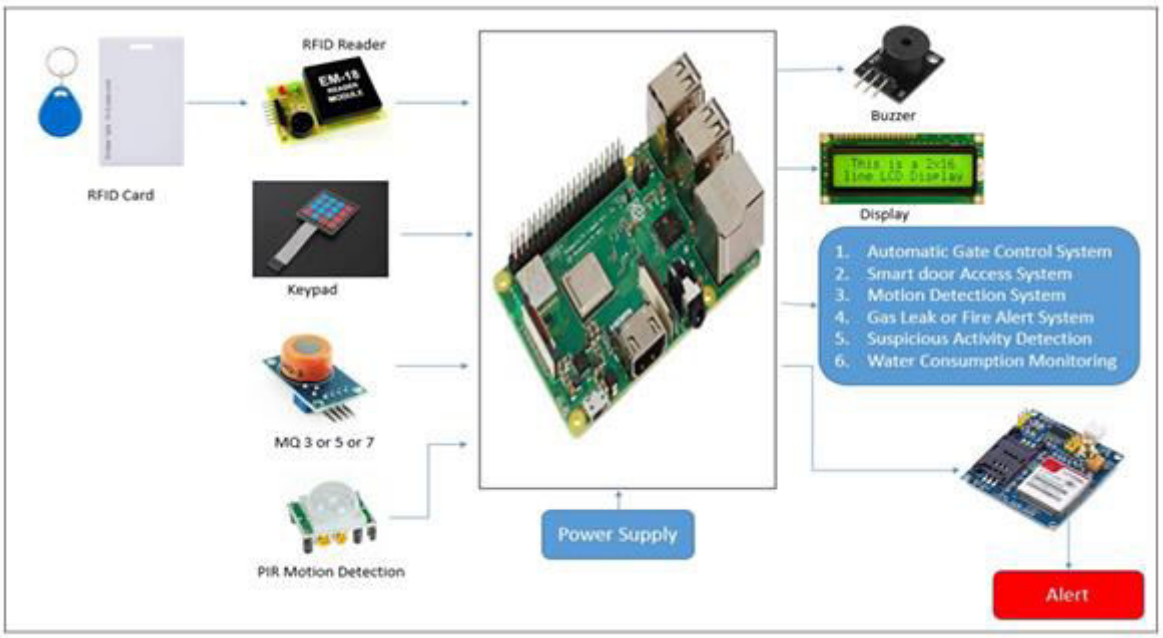


Fig: System Architecture

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

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404632|

The RFID module (RC522) is interfaced using the SPI protocol, with specific connections made to the Raspberry Pi's MOSI, MISO, SCK, and SDA pins. A 3.3V supply from the Raspberry Pi powers the RFID module. The RFID reader is mounted at the main gate and configured to trigger a servo motor or relay that controls the physical gate barrier. The 4x4 matrix keypad is connected to digital GPIO pins and used for indoor access control. Each keypress generates a digital signal that the Raspberry Pi interprets using a keypad scanning algorithm. A relay module is used to control door locks or electronic latches based on successful code entry. For biometric access, the fingerprint sensor (R305 or GT511C3) is connected via UART pins and requires an additional 5V power source. It is mounted on lockers or doors and captures fingerprint data, comparing it with previously stored templates to determine access permission.

The PIR motion sensors are deployed in multiple locations and connected to GPIO pins configured as input with interrupt handling. Each sensor is powered by the Raspberry Pi's 5V and GND pins and set to detect human presence within a 5–7 meter range. Upon detecting motion, the sensor sends a HIGH signal to the Pi, which then triggers corresponding outputs—such as turning on an LED or activating a relay-controlled light bulb. The MQ3 gas/smoke sensor is used for fire detection and connected to an analog-to-digital converter (like MCP3008), since the Raspberry Pi lacks native analog input. The sensor continuously samples the environment for alcohol, smoke, or combustible gases and sends digital data through the ADC to the Raspberry Pi, which triggers an alert when threshold levels are exceeded. A buzzer is also included in the design to provide immediate audio alerts for critical events like gas leaks or unauthorized access.

To enhance communication and alert functionalities, a GSM module (SIM800L or SIM900A) is connected to the Raspberry Pi via UART. A dedicated power supply (typically 12V to 5V buck converter) ensures stable operation, as GSM modules are power-intensive. The module allows the system to send SMS alerts in case of security breaches or environmental hazards. Additionally, a camera module or USB webcam may be included in the design for real-time surveillance and suspicious activity detection. The camera is mounted in strategic outdoor or entry-point locations and is triggered either continuously or via PIR sensor input. Optional enhancements to the hardware design include backup power using a UPS HAT or power bank to maintain system uptime during outages, and the inclusion of a touchscreen display for direct user interaction and system status monitoring. Overall, the hardware design emphasizes modularity, reliability, and ease of integration, ensuring the system can be scaled or modified based on specific user needs and installation environments.

V. CONCLUSION

The proposed Raspberry Pi-Based Smart Building Security System with Multi-Module Automation presents a robust, scalable, and cost-effective solution for modernizing and securing residential and commercial properties. By integrating multiple independent modules—such as RFID-based gate control, keypad and fingerprint-based door access, PIR-based motion sensing for intelligent lighting, MQ3 sensor for fire detection, and GSM-based real-time alert mechanisms—the system offers a comprehensive approach to building security. Each module is carefully chosen for its reliability, ease of integration, and relevance to specific security and automation tasks, ensuring a balance between user convenience and protection. The centralized processing capability of the Raspberry Pi, combined with its versatile GPIO architecture, allows seamless communication among components while enabling real-time decision-making and response. Additionally, the modular design ensures easy scalability, allowing future upgrades such as cloud connectivity, AI-driven surveillance, and remote monitoring via mobile apps. This solution not only enhances safety through proactive detection and instant alerts but also contributes to energy efficiency and modern smart home functionality. Overall, the project demonstrates how open-source hardware and intelligent sensor integration can revolutionize building security by making it smarter, more responsive, and user-friendly.

REFERENCES

1. J. Boxall (2013). Adruino Workshop. First Edition, San Francisco: No Starch Press, 2013.
2. D. Ingole, S. Gharde, S. Lad, M., S. Lambade, "Automated system for office using Arduino and Android," 2019.
3. A. Licorish, E. Zolduoarrati, N. Stanger, "Linking User Requests, Developer Responses and Code Changes: Android OS Case Study," In Proceedings of the 22nd International Conference on Evaluation and Assessment in Software Engineering, 2018, pp 79-89.
4. Liu, Q. Zhu, K. A. Holroyd, E. K. Seng, "Status and trends of mobile-health applications for iOS devices: A

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

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404632|

developer's perspective, " Journal of Systems and Software, 84(11), 2011, pp 2022- 2033

5. Madan, S. R. N. Reddy, "GSM-Bluetooth based remote monitoring and control system with automatic light controller," International Journal of Computer Applications, 46(1), 2012, pp 20-28.
6. A. Ramlee, K.A.A. Aziz, M. H. Leong, M. A. Othman, H. A. Sulaiman, Wireless controlled methods via voice and internet (e-mail) for home automation system.International Journal of Engineering and Technology, 5, 2019, pp3580- 3587.
7. A. Radzi, M. M. F. Alif, Y. N. Athirah, A. S. Jaafar, A. H. Norihan, and M. S. Saleha, "IoT based facial recognition door access control home security system using Raspberry Pi," Int. J. Power Electron. Drive Syst., vol. 11, p. 417, Mar. 2020.
8. Mehra, A. Khatri, P. Tanwar, and V. Khatri, "Intelligent embedded security control sys tem for maternity ward based on IoT and face recognition," in Proc. Int. Conf. Adv. Comput.Commun. Control Netw.(ICACCCN), Oct. 2018, pp. 49–53
9. Ziqiang and G. Zhang, "Data science in face recognition system based on BP neural network," J. Phys., Conf. Ser., vol. 1881, no. 2, Apr. 2021, Art. no. 022029.
10. Puvaneswari, M. Ramya, R. Kalaivani, and S. B. Ganesh, "Smart home security system using facial recognition," in Proceedings of Third International Conference on Sustainable Expert Systems. 2023, pp. 239–252.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details