© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716954

Smart Home Security with Voice Commands using IOT

VIVEKANANDA REDDY BONGARAM[1], SURESH GOUD BAKARAM[2], RAHUL PATEL PINGIDI[3], DEVENDER VOODARA[4]

[1]*Electronics and Communication Engineering, Institute of Aeronautical Engineering* Hyderabad, India

[2,3,4]*Assistant Professor, Electronics and Communication Engineering, Institute of Aeronautical Engineering Hyderabad, India*

Abstract- ***This project outlines the design and execution of an IoT-driven smart home security system that incorporates voice control and real-time alert features to improve residential safety and user convenience. The system employs a NodeMCU (ESP8266) microcontroller linked to a Passive Infrared (PIR) sensor for motion detection and potential intrusion identification. Upon detecting movement, the system triggers a buzzer and lights through a relay module, while also capturing images with an ESP32-CAM module. These images are transmitted to the user via a Telegram-based alert system, facilitating real-time remote monitoring. Furthermore, users can easily control appliances using voice commands through platforms like Google Assistant. The proposed system is not only cost-effective and energy-efficient but also straightforward to implement, making it ideal for contemporary smart home applications. Experimental results indicate dependable performance in motion detection, alert transmission, and voice-controlled functionality.***

Keywords - NodeMCU, smart home automation, residential security system, Internet of Things (IoT), motion-based intrusion detection, PIR motion sensor, intelligent home systems, voice-activated control

I. INTRODUCTION

The rapid evolution of smart technologies has greatly affected residential security, moving traditional systems towards more intelligent and flexible designs. Conventional security solutions were based on manual monitoring and wired installations, which limited flexibility, delayed responses, and offered minimal user interaction. With the advent of the Internet of Things (IoT), these shortcomings are being resolved through networks of interconnected sensors, cameras, and embedded controllers that enable real-time data exchange and automation. As a result, modern home security systems provide enhanced situational awareness, timely alerts, and convenient remote access.Despite these advancements, existing systems still face challenges in user interaction, system integration, and efficient control mechanisms. In particular, many IoT-based security platforms rely on smartphone interfaces or web dashboards, which may introduce delays or require active manual engagement. This creates a need for more natural, intuitive, and hands-free modes of communication, especially in emergency scenarios where rapid response is essential. Voice-controlled smart assistants have emerged as a promising solution, offering seamless interaction through speech commands while maintaining system accessibility and user flexibility.

This research presents a home security model enabled by IoT technology, which integrates voice-based control for enhanced usability and automation. The proposed system employs PIR motion sensors, ESP32 camera modules, and MQTT communication protocols to detect activity, capture visual evidence, and notify users in real time. By integrating IoT connectivity with voice interfaces, the system aims to elevate user experience, reduce response latency, and provide a more practical solution for modern residential security. The design, algorithmic framework, and implementation specifics are discussed in detail. Experimental evaluations highlight its superior performance in recommendation precision and user engagement compared to traditional approaches. This research enriches the field of intelligent real estate solutions, shedding light on avenues for improving digital property marketplaces through machine intelligence.

II. RELATED WORK

The rise of IoT technology has paved the way for the advancement of smart homes. The advantages for

consumers encompass home automation, enhanced convenience, energy efficiency, and better security. Smart homes operate through a system of interconnected sensors, cameras, and actuators that communicate via the internet to handle tasks associated with monitoring, controlling, and automating household activities. A network of devices that can communicate with each other, as demonstrated in IoT [1], processes data to offer self-service and intelligent solutions for automating a home using IoT.

Additionally, remote sensing simplifies compliance and standardization in end-user applications, making comfort, convenience, security, and energy management easier. It also enables the monitoring and control of home appliances and systems.

IoT technology has played a significant role in transforming modern home environments by enabling automation, remote access, and improved control over connected devices [1]. Smart home systems integrate various components such as sensors, controllers, and communication networks to enhance convenience, security, and energy efficiency. Several studies have highlighted that IoT-based home automation allows users to monitor and manage appliances in real time, making everyday living more efficient and responsive [2]. Furthermore, recent research has focused on integrating safety mechanisms such as fire and smoke detection within smart homes. These systems are capable of identifying hazardous conditions and generating instant alerts through interconnected networks, thereby improving emergency response and overall safety [3]. Such developments demonstrate the growing importance of IoT in designing reliable, intelligent, and scalable home security solutions.

Recent research has explored the role of Intrusion Detection Systems (IDS) in IoT environments, focusing on different techniques, system architectures, and challenges involved in securing connected devices. In smart home applications, IoT-based security systems commonly use technologies such as motion sensors and facial recognition to detect and identify unauthorized individuals. These systems rely on advanced sensing and processing mechanisms to improve accuracy and response time. Additionally, IoT enables users to remotely monitor and manage home security systems through connected platforms, increasing accessibility and control [4]. Beyond residential use, IoT-based biometric systems are also being studied in sectors like education, where they are used for identity verification and automated attendance management. Such systems enhance security while simplifying administrative processes for students, staff, and visitors.

An exploratory study has been carried out on the development of IoT-based intelligent home automation systems aimed at improving control and efficiency in residential environments. These systems utilize a combination of interconnected IoT devices to enhance safety, comfort, and energy management within smart homes. By integrating multiple devices over a unified wireless network, users can monitor and control home appliances more effectively. Platforms such as Arduino-based controllers are widely used along with internet-enabled applications to implement such automation systems [5]. Further research in this area focuses on improving system reliability and performance by ensuring seamless communication between devices and optimizing the overall productivity of smart home solutions.

IoT technology enables seamless communication between devices within a home, allowing automated monitoring and improved security systems [6]. Smart home automation solutions built using Arduino microcontrollers and IoT platforms are designed to be efficient, affordable, and scalable, enabling users to remotely control appliances such as lighting, security devices, and other household systems. Due to their flexibility and low cost, Arduino-based systems are widely adopted as a central component in home automation applications [7]. Recent developments have also introduced advanced features such as voice-based control and energy monitoring, where users can operate devices through speech recognition while simultaneously tracking power consumption to improve efficiency and safety [8]. In addition to home environments, IoT-based surveillance systems have been developed for high-security areas, integrating multiple sensors and communication protocols to provide continuous real-time monitoring. These systems enhance reliability and overall

performance by enabling accurate detection and efficient data transmission across connected networks [9].

III. SYSTEM DESIGN AND ARCHITECTURE

4.1 Block Diagram

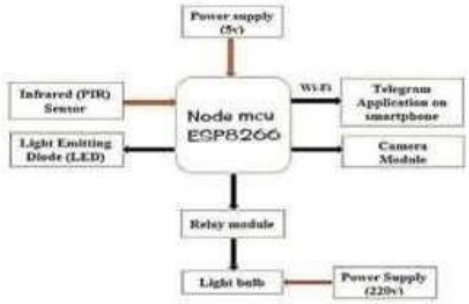


Figure 1. Block diagram of the system

The proposed smart home security system is designed using components such as a PIR motion sensor, NodeMCU (ESP8266), relay module, buzzer, ESP32-CAM, and a smartphone interface. In this setup, the NodeMCU acts as the main controller that processes all incoming signals. When the PIR sensor detects movement near the entrance, it sends a signal to the NodeMCU, which then triggers the relay module to switch on connected devices like lights and a buzzer to indicate a possible intrusion. At the same time, the ESP32-CAM captures an image of the detected person and sends it to the user through a Telegram notification using Wi-Fi, allowing real-time monitoring. The system also supports voice-based control using virtual assistants such as Google Assistant or Amazon Alexa, enabling users to operate devices remotely without manual interaction. The controller and sensors are powered using a 5V supply, while high-voltage devices such as lights operate on 220V AC through the relay, ensuring safe and efficient operation of the system.

4.2 Hardware Description

The hardware components used in this project are listed below:

1. NodeMCU (ESP8266)
2. ESP8266 Wi-Fi Module
3. Light Emitting Diode (LED)
4. Passive Infrared (PIR) Sensor
5. Relay Module
6. Buzzer
7. ESP32-CAM Module

4.3 Hardware specifications

4.3.1 Node MCU (ESP8266)

NodeMCU is an open-source development board based on the ESP8266-12E Wi-Fi module, widely used for Internet of Things (IoT) applications. It can be programmed using either the Lua scripting language or the Arduino IDE, making it suitable for both beginners and advanced users. The board enables easy Wi-Fi connectivity and input/output configuration with minimal coding effort. It supports direct USB-to-TTL programming and can operate in both station mode and access point mode for flexible network communication. With built-in Wi-Fi capabilities, the NodeMCU can host web servers and communicate with cloud platforms, making it a cost-effective and efficient solution for IoT-based system development.

Features:

- Open-source platform
- Low cost
- Arduino-compatible hardware
- Onboard status LED
- Micro-USB interface for programming and power
- Reset and flash buttons
- Built-in Wi-Fi support
- Easy to program and configure

Figure 2. Node MCU Module

4.1.1 ESP8266 Wi-Fi Module (USB to UART Converter)

The ESP8266 Wi-Fi module is a low-cost and efficient solution that enables wireless

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716954

communication for microcontroller-based systems. It can function either as a standalone device capable of executing programs or as a Wi-Fi interface module connected to another microcontroller. The module supports booting from external flash memory and includes internal memory features that enhance performance during operation.

It can communicate with microcontrollers using serial (UART) communication, allowing devices without built-in Wi-Fi to access the internet. The ESP8266 also provides multiple GPIO pins, enabling easy interfacing with sensors and other hardware components. Due to its high level of integration, it includes essential components such as antenna circuitry and power management units within a compact design, reducing the need for additional external hardware. This makes the ESP8266 a space-efficient and reliable choice for IoT applications.

Figure 3. ESP8266 Wi-Fi Module

4.3.3 Light Emitting Diode (LED)

A Light Emitting Diode (LED) is a semiconductor device that produces light when an electric current flows through it. It operates based on the principle of electroluminescence, where electrical energy is directly converted into light energy. With advancements in semiconductor technology, modern LEDs have become more efficient, offering higher brightness while consuming less power. Due to their low energy consumption, long lifespan, and reliability, LEDs are widely used in electronic circuits, indicators, and lighting applications.

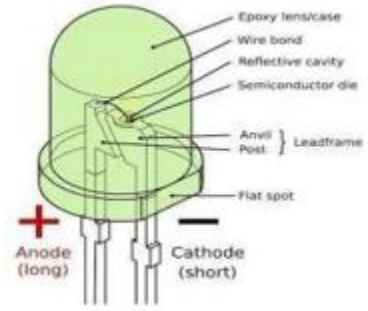


Figure 4. LED Pin Configuration

4.3.4 Passive Infrared (PIR) Sesnsor

A Passive Infrared (PIR) sensor is a widely used device in motion detection systems that detects infrared radiation emitted by objects within its sensing range. It operates using a pyroelectric material that produces a small electrical signal when there is a change in infrared energy. The sensor consists of multiple sensing elements arranged in segments, which helps it identify variations in heat patterns when a moving object passes through its field of view. These changes are processed as motion signals, allowing the system to detect human or object movement effectively.

PIR sensors are commonly used in security systems, automatic lighting, and smart home applications due to their low power consumption, quick response, and affordability. However, their performance can be affected by environmental factors such as temperature variations, and they typically require a clear line of sight for accurate detection.

Figure 5. Passive Infrared (PIR) Sensor

Internal Working Principle:

A PIR sensor is built using a pyroelectric material arranged in one or more sensing elements, often referred to as pixels. In many designs, two sensing elements are connected in a differential

configuration. When there is no movement, both elements receive similar levels of infrared radiation, and the output remains stable. However, when a moving object such as a human pass across the sensor's field of view, there is a change in infrared energy between the two elements. This difference generates an electrical signal, which is interpreted as motion.

The differential arrangement helps eliminate false triggering caused by uniform temperature changes in the environment, such as sunlight or room heating. It also improves immunity to disturbances like electrical noise and lighting variations. Although PIR sensors do not measure absolute temperature, they are highly effective in detecting motion based on changes in infrared radiation patterns.

4.3.5 Relay Module

A relay is an electromechanical switching device that allows a low-power signal to control high-voltage or high-current circuits. It works by providing electrical isolation between the control side and the loadside, ensuring safe operation of connected devices. When a control signal is applied, the relay coil gets energized and generates a magnetic field. This magnetic action moves the internal switching contacts, causing them to either open or close, thereby turning the connected devices ON or OFF.

Relays are widely used in automation systems, control circuits, and IoT applications where it is necessary to operate electrical loads such as lights, fans, or alarms using a microcontroller. In this project, the relay is used to control high-voltage devices safely through the NodeMCU.

Figure 6. Relay Module

4.1.1 Buzzer

A buzzer is an audio signaling device used to generate sound alerts in electronic systems. It can be classified into electromechanical, piezoelectric, and electronic types, depending on its operating mechanism. In modern applications, piezoelectric buzzers are commonly used due to their compact size, low power consumption, and ease of integration with microcontrollers.

The working principle of a buzzer is based on the conversion of electrical energy into sound energy. In piezoelectric buzzers, an applied voltage causes mechanical deformation of the piezoelectric material, resulting in the generation of audible sound waves. Buzzers are widely employed in alarm systems, household appliances, and embedded systems to provide real-time auditory feedback. In IoT-based applications, they are often used as warning or alert devices to indicate specific events such as intrusion detection or system status changes.

Figure 7. Buzzer

4.1.1 ESP32-CAM

The ESP32-CAM is a compact and low-cost camera module built around the ESP32-S chip, widely used in IoT-based image and video processing applications. It is equipped with an OV2640 camera sensor and supports both Wi-Fi and Bluetooth connectivity, enabling wireless communication and remote monitoring. The module also includes a microSD card slot for storing captured images and videos locally. Owing to its small size, integrated features, and affordability, the ESP32-CAM is commonly utilized in smart home systems, surveillance applications, and embedded vision-based projects.

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716954

Figure 8. ESP-32 CAM Module

IV. IMPLEMENTATION

5.1 Methodology

The proposed smart home security system is developed using components such as a PIR sensor, NodeMCU (ESP8266), relay module, buzzer, and camera module to enhance residential safety. The PIR sensor continuously monitors the surroundings and detects motion near the entrance. Once movement is identified, it sends a signal to the NodeMCU, which processes the input and activates the relay to switch on connected devices such as lights and a buzzer, thereby alerting the user.

Simultaneously, the camera module captures an image of the detected individual and transmits it to the user through a Telegram-based notification system, enabling real-time monitoring. In addition, the system supports voice-based control through platforms such as Google Assistant or Amazon Alexa, allowing users to operate devices remotely. This approach ensures an efficient, cost-effective, and automated security solution suitable for smart home environments.

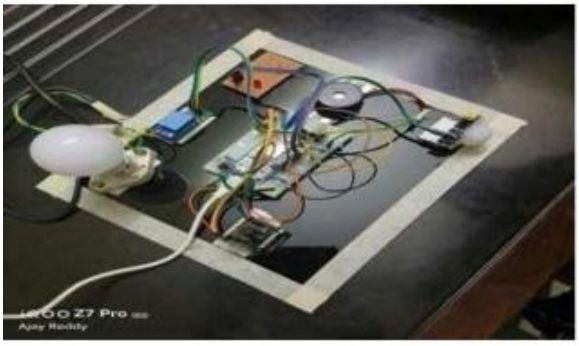
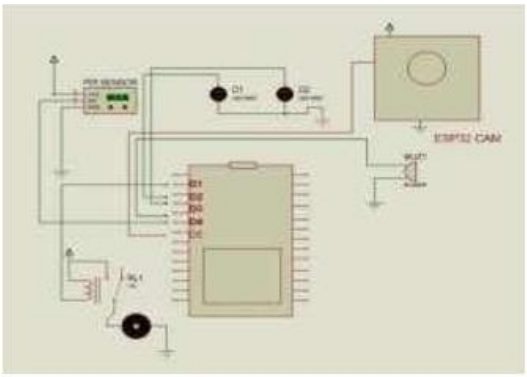


Figure 9. System Setup

5.1 Circuit Diagram



The circuit is designed by interfacing a PIR motion sensor with the digital input pin of the NodeMCU, while the relay module is connected to a digital output pin to control electrical loads such as lights and a buzzer. The camera module operates with a separate power supply and uses Wi-Fi communication to transmit captured images. A common ground is maintained across all components to ensure stable and reliable operation. The relay provides electrical isolation between the low-voltage control circuit and high-voltage load devices, thereby ensuring safe switching and protecting the system.

V. RESULTS AND DISCUSSION

5.1 Functional Results

1. Motion Detection and Activation

The PIR sensor successfully detects motion near the entrance and sends a signal to the NodeMCU. Upon detection, the system activates the relay, which in turn switches on the lights and buzzer. This provides immediate alerts, indicating the presence of a person near the door.

2. Voice Command Control

The system is integrated with voice assistants such as Google Assistant and Amazon Alexa, enabling users to control the connected devices through voice commands. This feature enhances user convenience and allows hands-free operation of the system.

3. Photo Capture and Telegram Integration

When motion is detected, the camera module captures an image of the individual at the entrance. The captured image is then transmitted to the user via a Telegram bot, providing real-time visual confirmation and improving overall security monitoring.

5.2 Discussion

1. System Reliability and Responsiveness

The performance of the PIR sensor was evaluated under different environmental conditions to assess its reliability. The system demonstrated consistent detection of motion with minimal false triggering. Additionally, the response time in activating the relay, lights, and buzzer was observed to be quick, ensuring timely alerts with negligible latency.

2. User Interface and Accessibility

The integration of voice assistants such as Google Assistant and Amazon Alexa improved the usability of the system by enabling hands-free control. The interface was found to be user-friendly; however, further improvements can be made to enhance responsiveness and overall user experience.

3. Security and Privacy Considerations

The system incorporates basic security measures to prevent unauthorized access and ensure safe operation. However, since images are captured and transmitted through a Telegram bot, privacy concerns must be considered. Proper authentication and secure communication protocols are necessary to protect user data.

4. Cost-Effectiveness and Scalability

The proposed system is cost-effective compared to conventional security solutions, as it utilizes low-cost components such as NodeMCU, PIR sensors, and camera modules. Furthermore, the system can be easily scaled by integrating additional sensors or functionalities, making it suitable for larger environments and advanced applications.

VI. CONCLUSION AND FUTURE SCOPE

6.1 Conclusion

This project demonstrates the feasibility of developing an affordable and efficient smart home security system using readily available IoT components. By integrating motion detection, voice-based control, image capture, and Telegram-based notifications, the system provides effective security while maintaining ease of use and real-time monitoring capabilities. The overall performance indicates that the proposed solution is reliable and suitable for practical smart home applications. Furthermore, aspects such as system reliability, user interaction, security measures, and scalability highlight potential areas for future improvement and enhancement.

6.2 Future Scope

The future scope of the proposed smart home security system includes the integration of advanced features such as facial recognition for automatic identification of visitors. Enhancements can be made to improve sensor accuracy and optimize energy consumption, thereby increasing overall system efficiency. The use of cloud-based storage can enable secure data management and support advanced analytics for better monitoring. Additionally, the user interface can be further improved by incorporating more intuitive controls and automation features. Strengthening security protocols will also be essential to ensure safe communication and protection of user data. These improvements can significantly enhance the system's performance, reliability, and user experience, contributing to the development of smarter and more secure home environments.

REFERENCES

[1] V. Lohan and R. P. Singh, "Home automation using Internet of Things," in *Advances in Data and Information Sciences*, vol. 39, Springer, Singapore, 2019, pp. 293–301.

[2] A. Samad and F. Siddiqui, "IoT-based automation for smart sustainable homes," in *Proc. 2nd Int. Conf. ICT for Digital, Smart, and Sustainable Development*, New Delhi, India, Feb. 2020.

[3] P. Netinant, P. Vasprasert, and M. Rukhiran, "Evaluation of LWIR micro thermal camera IoT and digital thermometer for human body temperature," in *Proc. Int. Conf. E-Commerce, E-Business and E-Government*, New York, NY, USA, Apr. 2021.

[4] S. H. Ahmed and S. R. Zeebaree, "A survey on security and privacy challenges in smart home-based IoT," *J. Contemp. Archit.*, vol. 8, pp. 489–510, 2021.

[5] R. Garg and S. Gupta, "A review on Internet of Things for home automation," *Int. J. Eng. Res. Technol.*, vol. 8, pp. 80–83, 2020.

[6] K. S. Gayathri and T. Thomas, "Intrusion detection systems for Internet of Things," in *Handbook of Research on Intrusion Detection Systems*, IGI Global, Hershey, PA, USA, 2020, pp. 148–171.

[7] A. J. Majumder and J. A. Izaguirre, "A smart IoT security system for smart homes using motion detection and facial recognition," in

[8] *Proc. IEEE 44th Annual Computers, Software, and Applications Conf.*, Madrid, Spain, Jul. 2020.

[9] M. Khudhair Al-Gburi and L. A. Abdul-Rahaim, "Secure smart home automation and monitoring system using Internet of Things,"

[10] *Indones. J. Electr. Eng. Comput. Sci.*, vol. 28, p. 269, 2022.

[11] P. Netinant, M. Rukhiran, and P. Rattanakorn, "Development of smart light control and intruder detection with voice and motion based on Internet of Things using Raspberry Pi," in *Proc. 6th Int. Conf. Business and Information Management*, Guangzhou, China, Aug. 2022.