World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

IoT based smart doorbell with face recognition and remote alerts

Akshay S. Kadam * and Aurangjeb Khan

School of Science and Computer Studies, CMR University, Bengaluru, Karnataka, India.

World Journal of Advanced Research and Reviews, 2025, 27(01), 755-763

Publication history: Received on 30 May 2025; revised on 05 July 2025; accepted on 08 July 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.27.1.2580

Abstract

Smart doorbells are the requirement in the houses, especially in the city for the security of the members where most of the people are outside home for work or study and only few members are inside home, sometimes only children or elderly people. Our effort is to provide a solution to this problem with a robust and cost-effective smart doorbell system that combines computer vision, Internet of Things (IoT), and cloud-based messaging to enhance residential security. When a visitor presses the doorbell button, the system captures an image using a connected webcam, performs facial recognition using a pre-trained model, rings a buzzer, and sends a real-time photo alert with the identified name via Telegram. The camera then powers down to conserve resources. The system then switches to a Blynk-controlled interface, allowing the user to remotely unlock or lock the door using two buttons on the Blynk mobile or web dashboard. The system runs on a Raspberry Pi, integrating hardware-level GPIO interaction with cloud-based APIs, offering a hybrid edge-cloud security solution.

Keyword: Intelligent Entry Notification System; Facial Verification-Based Access Control; Embedded IoT Home Security; Raspberry Pi–Driven Automation; Cloud-Connected Blynk Interface; Real-Time Alerts Via Telegram Messaging

1. Introduction

Traditional doorbells are limited in functionality, as they demand the homeowner's physical presence and fail to provide any insight into the visitor's identity. As the need for smarter and more secure home access systems grows, integrating technologies like IoT, computer vision, and mobile alerts offers a powerful upgrade. This project transforms the conventional doorbell into an intelligent system by employing face recognition to identify individuals at the door, enhancing access control. It utilizes the Telegram Bot API to send real-time image alerts to the user, enabling instant remote awareness. The Blynk IoT platform further enhances usability by allowing users to monitor and control the system through a mobile app. Additionally, the Raspberry Pi's GPIO pins manage a servo motor for door unlocking and a buzzer for audio notifications, creating a comprehensive, responsive, and secure smart doorbell solution. This research presents the development of a smart doorbell system using IoT technologies to enhance home security with minimal human interaction. The system uses an ESP32-CAM module to detect human presence, capture images, and send real-time notifications via the Blynk app. It supports both manual and automated modes, with automation achieved through face recognition using Python and OpenCV. Key hardware includes a solenoid lock, push button, and voltage regulator. The project consists of three main phases: data gathering, face detection, and face recognition, offering both control and security through mobile integration [1]. According to [2] introduces a IoT-based smart doorbell system using a Raspberry Pi, focusing on enhanced security and remote monitoring. The system captures images and audio when a visitor presses the doorbell and sends them via Gmail, allowing users to monitor from anywhere. It includes a display screen to show messages to visitors and uses MAC encryption for secure data transmission. The project demonstrates a wireless, internet-connected door system that enhances home security. Future improvements aim to reduce transmission delays and further strengthen security protocols.

* Corresponding author: Akshay S Kadam

2. Material and Methods

2.1. Manual Process

When a visitor presses the doorbell button, it triggers the camera to capture an image of the person at the door. This image undergoes face recognition to identify whether the visitor is known or unknown. A real-time notification, along with the captured image and identification result, is sent to the homeowner via the Telegram app. Simultaneously, the owner can open the Blynk IoT mobile app, where they are provided with control options. By tapping the "Unlock" or "Lock" button in the app, the homeowner can remotely control the door lock mechanism based on the visitor's identity. This integration of facial recognition, Telegram alerts, and Blynk IoT app control enhances both security and convenience.

Figure 1 Manual Flow Chart

2.2. Automation Process

The smart doorbell system eliminates the need for manual supervision by combining facial recognition, IoT, and real-time messaging. Once the Raspberry Pi initializes, it sets up all required GPIO pins and loads facial data for recognition. When a visitor presses the doorbell button, the system immediately captures an image using a webcam. It then processes the image using facial recognition to determine whether the visitor is known or unknown. Simultaneously, a buzzer is triggered to notify people inside the house, and the captured image along with the identified name is sent to the homeowner via the Telegram app. After sending the image, the camera is turned off to save power. The user is then alerted on their smartphone and can open the Blynk IoT app, which provides buttons to either unlock or lock the door remotely. If the visitor is trusted, the owner taps "Unlock" to open the door using a servo motor. If the visitor is unknown or suspicious, the door remains locked. This process ensures real-time visitor detection and secure access control, offering a reliable and efficient alternative to traditional doorbells.

2.3. Experiments and Design

2.3.1. Hardware components

Raspberry Pi 3B+, USB Webcam, SG 90 Servo Motor, Buzzer, Push Button.

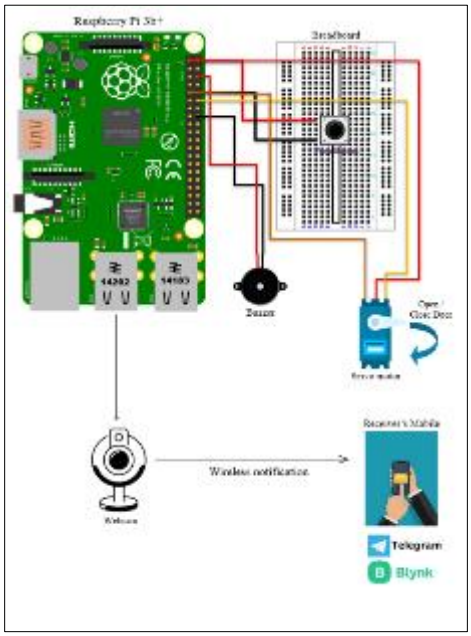

Figure 2 Circuit diagram

2.3.2. Implementation Process

The implementation of the smart doorbell system is structured into several logical stages, combining hardware setup and software development to achieve a fully automated visitor recognition and control system.

Hardware Setup

- **Step 1: Raspberry Pi Initialization**

The hardware setup begins with flashing the Raspberry Pi OS onto a microSD card, which is then inserted into the Raspberry Pi board. Essential peripherals such as a keyboard, mouse, and HDMI display are connected to perform the initial boot. Once operational, system configurations are adjusted to enable SSH for remote access, I^2C for sensor communication, and the camera interface, if applicable, ensuring the board is fully prepared for hardware and software integration.

- **Step 2: Component Connections**

The hardware components were interfaced with the Raspberry Pi through its GPIO pins to enable input and output functionality. A push button was wired to GPIO23 with a 10kΩ pull-down resistor to detect user interaction. The SG90 servo motor, responsible for door control, was connected via GPIO18 for signal, 5V for power, and GND for grounding. For audio feedback, a buzzer was linked to GPIO24 and grounded appropriately. Additionally, a USB webcam was connected through a USB port to capture visitor images for facial recognition.

Software Dependencies

The system's software stack begins with installing essential Python libraries using pip, including OpenCV-python, face-recognition, python-telegram-bot, nest, asyncio, and requests. These packages enable facial recognition, image processing, and cloud-based messaging. To support face identification, user images are captured and encoded using the face recognition library, with the resulting data stored in a serialized format as encodings. Pickle for use during real-time visitor verification.

2.3.3. Telegram Bot Setup

To enable real-time message alerts, a Telegram bot is created using **@BotFather**, which provides a unique **BOT Token**. The user initiates a chat with the bot and retrieves the **Chat ID** using tools like **@userinfobot**. Both credentials are then embedded into the system's Python script, allowing the Raspberry Pi to send instant notifications to the user's Telegram account upon doorbell activation.

2.3.4. Blynk IoT Setup

To enable remote control of the door lock system, a project is created on Blynk Cloud, where two virtual buttons are configured—one assigned to **Unlock (V0)** and the other to **Lock (V1)**. Upon setup, the platform generates an **authentication token (Auth Token)**, which is securely embedded into the Python code to authorize communication between the Raspberry Pi and the Blynk mobile application interface. This integration allows seamless, real-time access control from a smartphone.

2.3.5. Code Integration

The Python script performs real-time video frame capturing and facial recognition by comparing detected faces with pre-stored encodings. Upon doorbell button activation, the system captures an image, triggers the buzzer, sends the captured image with an alert via Telegram, and then disables the camera to conserve power. Additionally, it continuously monitors virtual buttons on the Blynk IoT platform to control the door locking mechanism using a servo motor.

2.3.6. System Execution

The system execution begins by running the Python script using the command python3 smart_doorbell.py. Once initiated, the system continuously monitors the push button input. Upon pressing the button, the buzzer is activated to provide an audible alert, and the connected webcam captures an image of the visitor. The captured image is then processed using the face recognition algorithm to identify known individuals. Following the recognition process, the image along with the identification result is transmitted to the predefined Telegram chat for remote notification. After completing this sequence, the system powers down the camera module to conserve energy and enters a standby mode, waiting for further commands via the Blynk IoT platform. The Blynk mobile application allows remote control of the door lock mechanism by interacting with virtual buttons configured for locking and unlocking operations through the servo motor. The proper functioning of the system is validated through multiple channels: monitoring the Raspberry Pi terminal for real-time status logs, confirming receipt of face identification alerts in the Telegram application, and testing the door locking and unlocking actions through the Blynk mobile interface.

3. Results and Discussion

The smart doorbell system was implemented and tested under real-world home conditions to validate its functionality, responsiveness, and accuracy. The results obtained from various experiments are summarized below:

Using OpenCV, the system detects known or unknown faces, sends their image via Telegram, and controls door access remotely through the Blynk IoT app.

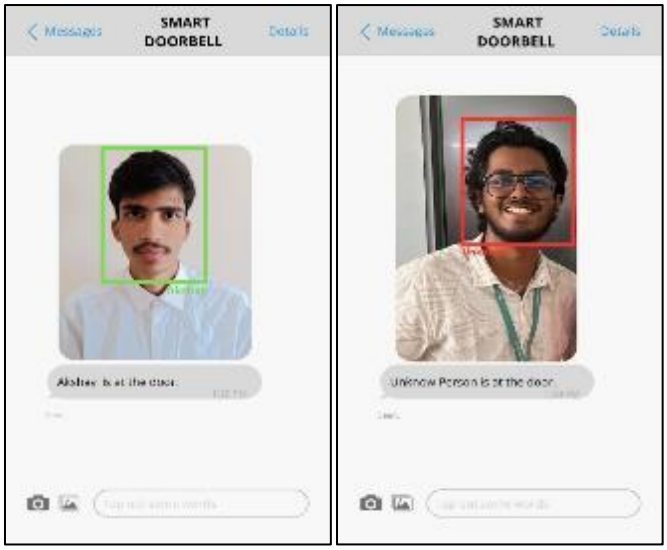

Figure 3 Face Recognition for Identifying Known and Unknown Individual

Figure 4 Blynk IoT App

Table 1 Face Recognition and Accuracy

Test Scenario	Outcome	Accuracy
Known person directly in front of camera	Face correctly identified	95%
Known person with partial face visible	Partially recognized or unknown	70%
Unknown person (not in dataset)	Marked as "Unknown"	100%
Poor lighting conditions	Reduced detection accuracy	~60–70%

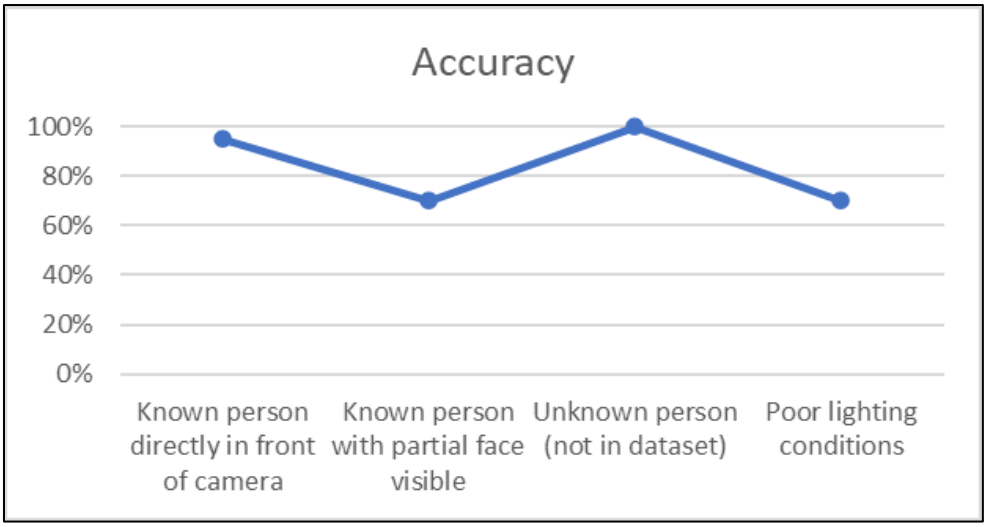

Figure 5 Accuracy graph

The system achieves optimal performance under good lighting conditions and when the face is viewed from the front. As shown in **Figure 5**, accuracy decreases under low lighting or when faces are captured from side angles. **Figure 3** illustrates OpenCV successfully detecting a known individual from the trained dataset, while it demonstrates detection of an unknown person

Table 2 Telegram Notification

Metric	**Result**
Time from button press to alert	3–5 seconds (avg.)
Image quality in Telegram	High
Caption clarity	Properly labelled

Real-time alerts are delivered quickly and reliably via Telegram with both the image and identity caption.

Table 3 Buzzer Activation

Trigger	**Behaviour**
Doorbell button pressed	Buzzer rings for 1 second
Response time	Immediate (<1 sec)

Buzzer provides immediate audible feedback upon button press, confirming input to both visitor and owner

Table 4 Servo Motor

Action	**Response**	**Delay**
Unlock via Blynk (V0)	Door unlocks (servo turns)	1–2 sec
Lock via Blynk (V1)	Door locks (servo resets)	1–2 sec

Using the interface shown in **Figure 4,** the Blynk IoT app enables door locking and unlocking. It responds with minimal delay and consistently actuates the servo motor to control the door mechanism efficiently.

Table 5 Camera Behaviour and Resource

Event	Camera State
On program start	Activated
After button press + photo sent	Deactivated (to save resources)
During face processing	Real-time face capture

Efficient resource use. The camera is only active during the recognition phase, conserving power on Raspberry Pi.

From the result discussion, it is evident that the IoT-based smart doorbell system successfully integrates a Raspberry Pi circuit with OpenCV for real-time face detection and recognition. The system is capable of identifying both known and unknown visitors by comparing captured facial images with pre-stored data. Upon pressing the doorbell button, the system activates the buzzer, captures the visitor's image, and accurately processes it to identify the person. The identified name along with the captured image is then sent to the homeowner via Telegram, ensuring immediate notification and enhancing situational awareness. Additionally, the system effectively utilizes the Blynk IoT platform for remote door access control. Users can securely lock and unlock the door using the Blynk mobile application, which communicates with the Raspberry Pi to operate the servo motor connected to the door mechanism. The testing results confirm that the system operates reliably, providing accurate face recognition, prompt Telegram alerts, and smooth door control through the Blynk app. Overall, the system demonstrates an efficient and practical solution for home security, combining computer vision, IoT, and cloud-based messaging technologies.

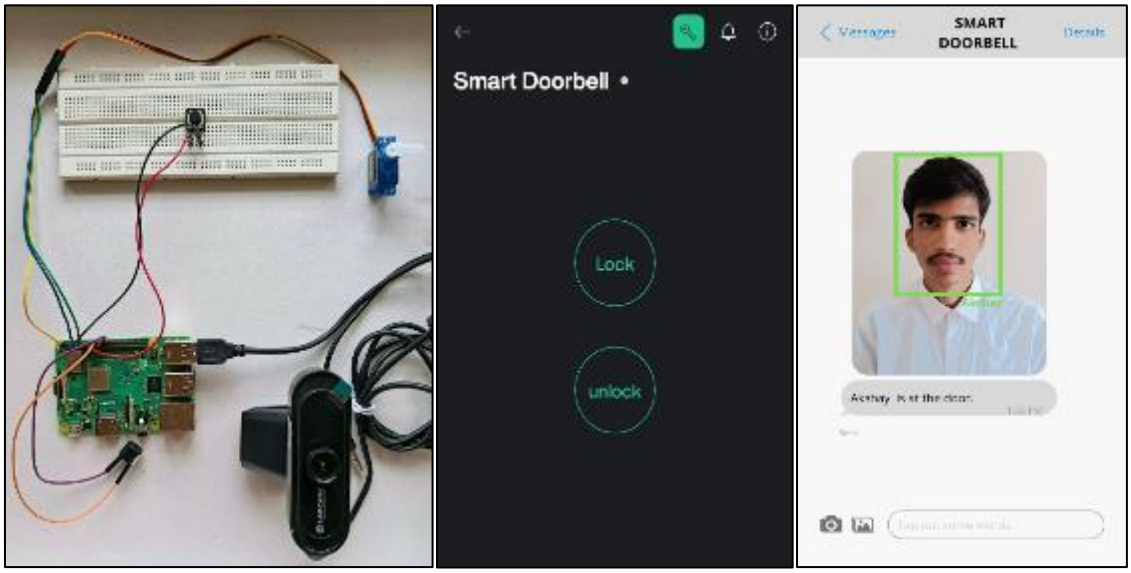

Figure 6 Circuit Integration with Blynk IoT and Telegram Alert System

4. Conclusion

This study presents the successful development of a smart doorbell system that addresses the limitations of traditional doorbells by integrating advanced technologies such as computer vision, IoT platforms, and real-time messaging services. The system enhances home security by enabling automated visitor identification, remote monitoring, and convenient door lock control.

The proposed design, as shown in Figure 6, utilizes a Raspberry Pi as the core controller, effectively managing image capture, face recognition, buzzer activation, servo motor control, and cloud communications. The face recognition module accurately detects and identifies known visitors while alerting the homeowner through Telegram, regardless of their location. Additionally, the Blynk IoT platform enables secure, remote door access through a mobile app, providing flexible control over locking and unlocking functions. The system's energy-efficient design further ensures sustainable operation without excessive resource consumption.

In summary, this smart doorbell system demonstrates a practical, cost-effective, and scalable solution that integrates hardware, software, and cloud services into a unified platform. It empowers users with real-time awareness and control over home access. This study will benefit society by promoting affordable, intelligent home security solutions and can serve as a foundation for future advancements in smart home automation technologies.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Madhu Shree S. M., & Swarnamugi M. (2021). Smart Doorbell System Using Internet of Things.NavaJyoti, International Journal of Multidisciplinary Research, 5(2), February 2021.

[2] Suprita Das, S.R.N. Reddy, & Ila Kumar (2017). Raspberry Pi Based Smart Doorbell System with Advanced Encryption Scheme. International Journal of Advanced Computational Engineering and Networking (IJACEN), 5(9), September 2017. ISSN: 2320-2106.

[3] Surla, S., Manepalli, N. A., Shaik, N. A., & Gurram, N. S. (2023). IoT and Face Recognition basedAutomated Door Lock System. 2023 Second International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, pp. 648–651.https://doi.org/10.1109/ICEARS56392.2023.10085609

[4] Shaout, A., & Theisen, M. (2021). State of the Art - Smart Doorbell Systems. 2021 22ndInternational Arab Conference on Information Technology (ACIT), Muscat, Oman, pp. 1–8. https://doi.org/10.1109/ACIT53391.2021.9677313

[5] Sudharsan, B., Malik, S., Corcoran, P., Patel, P., Breslin, J. G., & Ali, M. I. (2021). OWSNet: TowardsReal-time Offensive Words Spotting Network for Consumer IoT Devices. 2021 IEEE 7th WorldForum on Internet of Things (WF-IoT), New Orleans, USA, pp. 83–88. https://doi.org/10.1109/WF-IoT51360.2021.9595421

[6] Rodrigo, G., & De Silva, D. (2023). IoT-enabled Contactless Doorbell with Facial Recognition. 20234th International Conference on Innovative Trends in Information Technology (ICITIIT), Kottayam, India, pp. 1–6. https://doi.org/10.1109/ICITIIT57246.2023.10068625

[7] Antzoulis, I., Chowdhury, M. M., & Latiff, S. (2022). IoT Security for Smart Home: Issues andSolutions. 2022 IEEE International Conference on Electro Information Technology (eIT), Mankato, MN, USA, pp. 1–7. https://doi.org/10.1109/eIT53891.2022.9813914

[8] Yang, J. (2023). Real Time Object Tracking Using OpenCV. 2023 IEEE 3rd International Conference on Data Science and Computer Application (ICDSCA), Dalian, China, pp. 1472–1475. https://doi.org/10.1109/ICDSCA59871.2023.10392831

[9] Kaushik, K., Bhardwaj, A., & Dahiya, S. (2023). Smart Home IoT Forensics: Current Status, Challenges, and Future Directions. 2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT), Gharuan, India, pp. 716–721. https://doi.org/10.1109/InCACCT57535.2023.10141730

[10] Srinivasan, L., Reddy, N. K., Basavaraj, U. P., Chirag, K., & Darshan, M. E. (2023). A Review on Techniques used for Face Authentication based Smartdoor Bell System using IOT. 2023 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India,pp. 1–5 https://doi.org/10.1109/ICCCI56745.2023.10128225

[11] Khan, M., Anum, H., Batool, S. S., & Bashir, B. (2021). Smart Home with Wireless Smart Doorbellwith Smart Response. 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Mauritius, pp. 1–5. https://doi.org/10.1109/ICECCME52200.2021.9590865

[12] Salsabila, N., Siswanto, A., & Bayuaji, L. (2025). Design of a Smart Home Door Security System with Face Detection and Smart Bell using ESP32-CAM. 2025 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI), Goathgaun, Nepal, pp. 124–129.https://doi.org/10.1109/ICMCSI64620.2025.10883160

[13] Susheel, & Nayak, S. K. (2024). Knocking out Security Risks of Smart Video Doorbell Cameras. 2024 27th International Symposium on Wireless Personal Multimedia Communications (WPMC) Greater Noida, India, pp. 1–5. https://doi.org/10.1109/WPMC63271.2024.10863209

[14] Rani, T. P., Sakthy, S., Kalaichelvi, P., Vignesh, T., & Priyadarshan, M. (2022). Home Security and Anti-Theft System. 2022 1st International Conference on Computational Science and Technology (ICCST), Chennai, India, pp. 130–133. https://doi.org/10.1109/ICCST55948.2022.10040423

[15] Pilania, U., Kumar, M., Singh, S., & Mittal, V. (2023). Video Steganography in IoT: Information Embedding using OpenCV and 2LSB. 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, pp. 1067–1072. https://doi.org/10.1109/ICSCSS57650.2023.10169567

[16] Valarmathi, V., Sathya, T., Nirmala, J., Sivarajeswari, S., Prasanth, R. M., & Srihari, V. (2022). Design and Implementation of Secured Contactless Doorbell using IOT. 2022 International Conference on Computer, Power and Communications (ICCPC), Chennai, India, pp. 187–191. https://doi.org/10.1109/ICCPC55978.2022.10072073