International Journal of Computing and Artificial Intelligence

Advanced door protection system using AI

G Sai Ram, M Nikitha Goud, G Uday Kiran and K Bhavitha

DOI: https://doi.org/10.33545/27076571.2025.v6.i2b.191

E-ISSN: 2707-658X
P-ISSN: 2707-6571
Impact Factor (RJIF): 5.57
www.computersciencejournals.com/ijcai
IJCAI 2025; 6(2): 144-147
Received: 25-06-2025
Accepted: 29-07-2025

G Sai Ram
Assistant Professor, Department of ECE, Siddhartha Institute of Engineering and Technology, Ibrahimpatnam, India

M Nikitha Goud
UG Student, Department of ECE, Siddhartha Institute of Engineering and Technology, Ibrahimpatnam, India

G Uday Kiran
UG Student, Department of ECE, Siddhartha Institute of Engineering and Technology, Ibrahimpatnam, India

K Bhavitha
UG Student, Department of ECE, Siddhartha Institute of Engineering and Technology, Ibrahimpatnam, India

Corresponding Author:
G Sai Ram
Assistant Professor, Department of ECE, Siddhartha Institute of Engineering and Technology, Ibrahimpatnam, India

Abstract

The Advanced Door Protection System using AI is designed to provide enhanced security through a combination of biometric, visual, audio, and person detection technologies. This system utilizes a Raspberry Pi 4 as the central controller and incorporates a webcam for facial recognition, a microphone for sound detection, an IR sensor for person sensing, a fingerprint sensor for biometric authentication, and a servo motor for controlling the door lock. It also includes a buzzer for local alerts and a GSM module for sending remote notifications via SMS. The power supply ensures stable operation of all components. The system's architecture enables multi-factor authentication and remote monitoring, thereby significantly improving access control and threat detection. Its modularity and affordability make it suitable for modern smart security deployments.

Keywords: Psychiatric disorders, suicide, suicide attempt, first admission, recurrent admission, schizophrenia, bipolar disorder, depression, substance abuse disorder

1. Introduction

In earlier times, security systems for residential and commercial doors were predominantly mechanical, relying heavily on conventional locks and keys. While these systems were simple and inexpensive, they suffered from several inherent limitations. With technological advancements, electronic security systems were introduced, including PIN-based door locks, RFID card access systems, and remote-controlled locks. Although these systems offered improved control and convenience, they still faced significant issues such as password leakage, card theft, and limited adaptability to dynamic threat environments. Moreover, these systems typically relied on a single layer of authentication, making them susceptible to breaches by determined intruders. Additionally, most of them lacked remote alert capabilities and did not provide comprehensive real-time monitoring. To overcome these limitations and meet the growing demand for intelligent, secure, and adaptable door protection solutions, this project proposes the Advanced Door Protection System Using AI. The system is built around a Raspberry Pi 4, serving as the brain of the system and interfacing with multiple advanced components including a webcam, microphone, IR sensor, fingerprint sensor, servo motor, buzzer, and a GSM module. Each of these components plays a crucial role in achieving a secure, responsive, and smart access control system. The webcam captures real-time images for facial recognition, allowing the system to identify authorized users without the need for physical keys or access cards. The fingerprint sensor adds a second layer of biometric security, ensuring only pre-approved users can unlock the door. The IR sensor detects any movement near the entrance, acting as a motion-based trigger to activate the system. A microphone captures ambient audio to detect suspicious activity or enable voice-based interaction. The servo motor automates the locking and unlocking mechanism of the door, while the buzzer provides immediate audio alerts in case of unauthorized access attempts. Most importantly, the GSM module is used to send real-time SMS alerts to the homeowner, enabling remote monitoring and immediate awareness of any security breach. Artificial Intelligence plays a central role in this system, especially in facial recognition, anomaly detection, and learning from access patterns over time. This makes the system not only reactive but also proactive in improving its accuracy and response to potential threats.

2. Literature Survey

This paper presents the design and implementation of an access control system using RFID technology. The system is based on Arduino and operates by reading RFID cards or tags to grant access to users. It offers a low-cost and simple solution for secure entry and is often used in offices and hostels. However, the authors highlight several limitations, including the ease with which RFID cards can be cloned, misplaced, or stolen. Furthermore, the system lacks the ability to monitor real-time access logs or trigger alerts in case of unauthorized attempts. It does not support any form of veriationutomation biometric fic. Our proposed system addresses these shortcomings by integrating biometric fingerprint sensors and AI-based facial recognition, providing more secure and personalized authentication. Moreover, we incorporate real-time alerting through GSM and intelligent access decisions based on multiple inputs.

The system captures real-time images and matches them against a trained dataset to determine access eligibility. The advantage of this system is its non-contact nature and ease of use. However, it is heavily dependent on lighting condition, nor does it include remote monitoring or a Ons and camera angles

In this study, the authors developed a facial recognition-based door access system using a Raspberry Pi 3. Any deviation in the user's facial features due to aging, glasses, or poor lighting can lead to false rejections. Additionally, there is no second layer of authentication, which makes it vulnerable to spoofing via printed photos or video feeds. Our system enhances the facial recognition approach by adding fingerprint verification and an IR sensor to detect physical presence. This multi-layered authentication strategy significantly increases security and reduces the chances of unauthorized access. Furthermore, by using Raspberry Pi 4 and integrating a GSM module, we introduce real-time communication and alert features absent in the original system.

This paper introduces a smart door locking system that connects to a mobile application via the Internet of Things (IoT). Users can control door access through their smartphones and monitor access history through cloud services. The system uses simple password protection or app authentication to unlock the door. While convenient and modern, it is susceptible to security vulnerabilities such as hacking or password leaks. The lack of biometric verification also means that physical identity is never truly confirmed. Additionally, the system depends on a stable internet connection and lacks local autonomy in case of network failures our proposed model, we not only enable IoT features through the GSM module for message-based alerts but also incorporate strong local authentication using fingerprint and face recognition. This makes our system more secure, even in the absence of internet connectivity, and ensures access identity rather than just app credentials.

In this research, the authors developed an AI-based surveillance system for homes using computer vision. The system uses cameras connected to a processor (like Raspberry Pi) to detect human presence and send alert notifications to homeowners. The major advantage of this setup is that it provides non-intrusive, automatic monitoring. However, the system is passive—it does not provide access control or actively prevent unauthorized entry. Furthermore, it typically lacks real-time feedback mechanisms like alarms or physical locking components, and does not use multi-modal authentication methods. Our proposed system builds upon this by offering both surveillance and access control. The AI component not only monitors but also makes access decisions based on visual and biometric input. The servo motor actively locks or unlocks the door, while the GSM module sends out alerts. In essence, our system moves from passive observation to active protection, which is more effective in modern-day security applications.

3. Related Methodologies

The Advanced Door Protection System using AI integrates several methodologies for enhanced security, including AI, various biometric technologies, multi-factor authentication, IoT, embedded systems, computer vision, and sound detection. Related methodologies and concepts in these areas include:

Advanced Threat Detection AI systems use anomaly detection, behavioral analytics, and signature less detection to identify unusual patterns that indicate potential threats. Predictive Analysis AI can anticipate security issues by analyzing existing data and patterns. Real-time Analysis and Proactive Monitoring AI enables continuous monitoring and analysis of data, allowing for immediate identification and response to threats .Security Automation and Orchestration AI streamlines security operations, automates responses to incidents, and coordinates security processes for complex threats.AI-Enhanced Access Control AI improves access control beyond traditional methods by analyzing entry attempts and preventing unauthorized access. Biometric Authentication Method Beyond facial recognition and fingerprint scanning, other methods include: Physiological Biometrics This category includes iris recognition, palm or finger vein patterns, and finger geometry, which analyze unique biological markers. Behavioral Biometrics this involves analyzing patterns in human activities such as keystroke rhythm, walking gait, and mouse movements for continuous authentication. Biometric systems function through identification (comparing input to a database) and verification (confirming user identity against a specific profile).

4. Multi-Factor Authentication (MFA)

MFA enhances security by requiring at least two verification factors from different categories:

- **Knowledge-based factors:** Something the user knows, such as a password or PIN.
- **Possession-based factors:** Something the user has, like a security token, smartphone for OTPs (One-Time Passwords via SMS/email), or an authenticator app.
- **Inherence-based factors:** Something the user is, such as biometrics (fingerprints, facial recognition, voice, retina, or iris scanning).
- **Hardware Security Keys:** FIDO2/Web Authn security keys offer strong phishing resistance by using cryptographic keys.
- **Password less Authentication:** This eliminates passwords entirely, relying solely on biometrics or security keys for authentication.

5. IoT in Smart Home Security

Interconnected Devices: IoT systems connect various devices and services to collect, exchange, and process data, dynamically adapting to smart home environments. Remote Management: Users can remotely control and monitor smart home security functions, including appliance control, security monitoring, and intrusion alerts, through internet connectivity. Sensor Integration: IoT security systems integrate various sensors, such as motion, door/window break, gas leak, and smoke detectors, to gather data and trigger alerts. Voice and Button Controls: Enhanced user interaction can be achieved through voice commands and physical buttons for system control.

6. Embedded Systems for Access Control

Dedicated Functionality: Embedded systems are specialized computer systems designed for specific tasks, often integrated into larger mechanical or electrical systems like door access controls. Security Lifecycle Workflows: Securing embedded systems involves a comprehensive process including risk assessment, threat modeling (e.g., STRIDE, DREAD), and implementation of security controls, continuous monitoring, incident response, and system restoration. Computer Vision for Surveillance and Access Control Real-time Video Analysis: Computer vision transforms traditional surveillance systems into intelligent monitoring tools by analyzing video feeds in real time to detect threats and unusual activities. Object and Facial Recognition: It can identify and track object, recognize faces, and analyze human behavior for security purposes. Anomaly Detection: Computer vision systems are capable of spotting off-pattern or suspicious behavior within a live feed, such as lingering in restricted areas or unauthorized access attempts. Biometric Integration: It is extensively used in biometric authentication, including facial, iris, and fingerprint recognition. Sound Detection for Security Systems. Complementary Monitoring: Audio surveillance complements video surveillance and access control by providing real-time monitoring of sounds. Threat Identification: It can detect specific suspicious sounds like breaking glass, gunshots, or aggressive behavior, which can precede or indicate security incidents. False Alarm Reduction: Audio detection provides an additional layer of verification, helping to confirm the veracity of alarm events and reduce false alarms.AI-Powered Sound Analysis: Advanced algorithms can analyze audio data to identify specific threats or unusual audio patterns, enhancing proactive security measures.

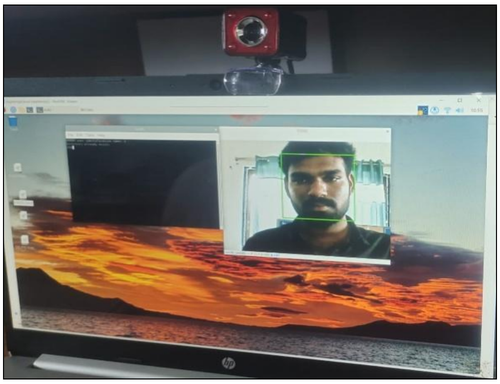


Fig (a): Face one captured

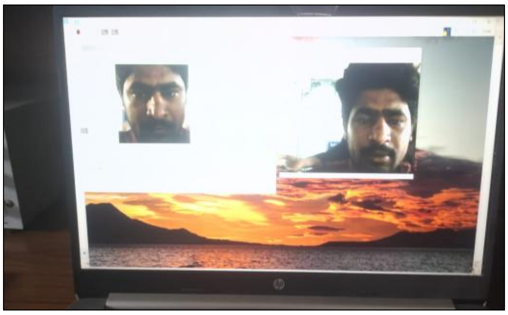


Fig b: Face two captured

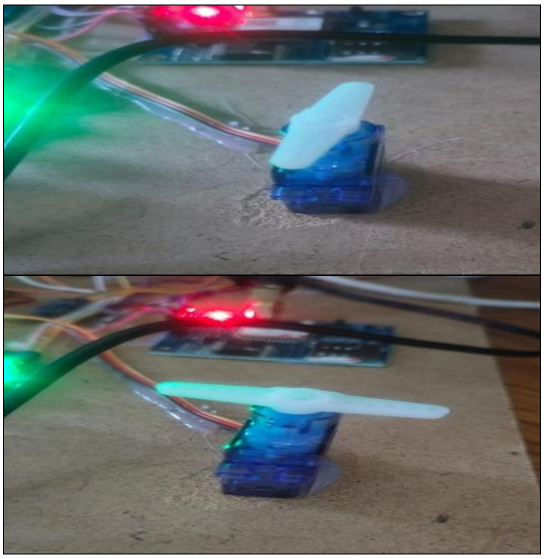
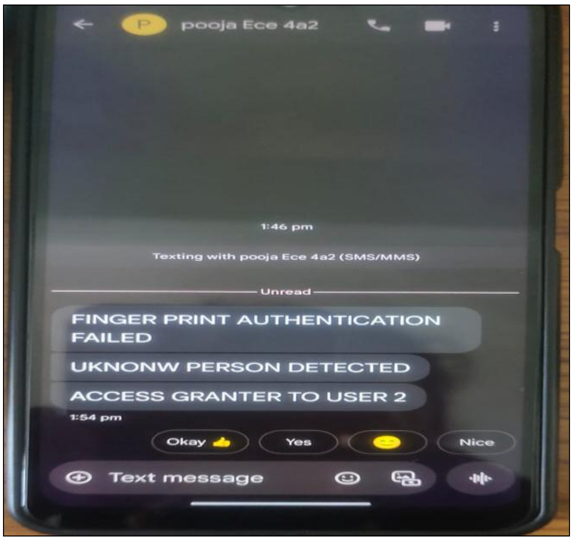


Fig c: Door closed and open condition



pooja Ece 4a2

1:46 pm

Texting with pooja Ece 4a2 (SMS/MMS)

Unread

FINGER PRINT AUTHENTICATION FAILED

UKNONW PERSON DETECTED

ACCESS GRANTER TO USER 2

1:54 pm

Fig d: Door open to send message

7. Conclusion

The Advanced Door Protection System Using AI provides a comprehensive and intelligent solution to modern-day security challenges. By integrating multiple technologies such as facial recognition, fingerprint scanning, IR motion detection, audio monitoring, and real-time GSM alerts, the system ensures a high level of security that goes beyond conventional methods. Unlike traditional locking mechanisms or single-layer electronic systems, this project offers multi-factor authentication and automated control through a servo motor, significantly reducing the risk of unauthorized access. The use of a Raspberry Pi 4 enables efficient processing of sensor inputs and AI algorithms, while maintaining low cost and flexibility. The system is especially suitable for smart homes, offices, and secure facilities, where security, convenience, and remote monitoring are essential. With its modular design and the ability to expand or upgrade, it demonstrates how modern embedded systems and AI can work together to build adaptive, real-time, and intelligent protection systems. Overall, this project successfully meets its goal of delivering an affordable, efficient, and robust security solution, making it highly relevant in today's growing demand for smart and secure environments.

References

1. Kumar A, Sharma R. RFID-based access control system using Arduino. Int J Eng Technol Innov. 2019;6(2):45-49.
2. Rahman M, Das T. Face recognition door access system using Raspberry Pi and OpenCV. In: Proceedings of the International Conference on Intelligent Systems and Applications. 2020. p. 127-132.
3. Verma P, Patel K. Smart door lock system using IoT for home automation. J IoT Smart Technol. 2021;9(1):22-28.
4. Mehta S, Raj L. Biometric fingerprint-based door locking system. In: Proceedings of the National Conference on Embedded Systems and Security. 2018. p. 34-38.
5. Singh D, Thomas V. AI-based home surveillance system with real-time notification alerts. J Artif Intell Secur Technol. 2022;11(3):78-84.
6. Reddy B, Thomas S. Design of intelligent vehicle security system using GSM and GPS. Int J Adv Res Electron Commun Eng. 2020;7(5):155-159.
7. Jadhav L, Rani V. IoT-based integrated vehicle safety and tracking system. In: Proceedings of the International Conference on Smart Systems and Applications. 2023. p. 88-93.
8. Patel A, Mishra K. Implementation of multi-factor authentication in smart door locks using Raspberry Pi. J Embed Syst Smart Appl. 2021;5(2):99-106.
9. Nair S, Bhatia R. AI and IoT-based intrusion detection and access control system. In: IEEE Int Conf Internet Things Secur. 2020. p. 213-218.
10. Gupta R, Malik H. Design and development of a low-cost AI-enabled door lock system. J Intell Embed Syst. 2022;6(4):142-148.