Real Time Face Recognition Security System

Kamalakar L[1], Maheswaran T[2]. Dinesh M[3], Guhan S[4], Mohammed Abdulla[5].
[1,3,4,5] *Student, Electronics and Communication Engineering Sri Shakthi Institute of Engineering and Technology*
[2] *Professor, Electronics and Communication Engineering, Sri Shakthi Institute of Engineering and Technology*

***Abstract*—This project presents a real-time smart door unlocking system using facial recognition and keypad-based authentication, powered by a Raspberry Pi 3B. The system integrates a USB camera, solenoid lock, 4x4 keypad, and PIR motion sensor to enhance security and usability. Facial recognition is implemented using OpenCV and pre-trained models, allowing contactless user verification. A secure passcode serves as a backup authentication method. A web-based interface built with Ruby on Rails enables remote access monitoring and logging of entry attempts. The system ensures minimal response delay, reliable performance under various lighting conditions, and low power consumption. Designed for small-scale environments, it offers a scalable and efficient alternative to commercial smart locks by combining machine learning, IoT, and embedded systems.**

***Index Terms*—Facial Recognition, Raspberry pi, Keypad Authentication, IoT Monitoring.**

I. INTRODUCTION

In today's smart security landscape, traditional key-based systems are increasingly being replaced by automated, contactless solutions. This project introduces a facial recognition-based door unlocking system using a Raspberry Pi 3B, offering enhanced security and user convenience. The system combines biometric authentication with a keypad-based backup for dual-mode access. A USB camera captures real-time facial data, while a solenoid lock physically controls entry. A PIR motion sensor detects movement near the door to activate the system efficiently. The use of OpenCV and pre-trained models enables accurate and fast recognition. A web-based interface allows remote monitoring and logging of access attempts. This solution is ideal for small offices or homes, providing a scalable and modern alternative to conventional locks.

II. LITERATURE REVIEW

Traditional mechanical locks paved the way to modern electronic and biometric-based technologies in the development of door security systems. The method that Deepak et al. [1] suggested allowed users to unlock doors using text messages, and other early versions frequently relied on GSM and SMS technology for remote access. Despite being useful, these methods lacked strong user authentication procedures, which left them open to manipulation.

Biometric authentication techniques, notably facial recognition, have been thoroughly studied to overcome identity verification concerns. Yadav and Verma [2] showed how machine vision could enhance security by using OpenCV on a Raspberry Pi for developing a facial recognition-based smart door system. However, their system was sensitive for remote monitoring and was susceptible to variations in lighting conditions.

Home security systems have gained significantly greater capabilities through IoT connectivity. Using MQTT protocols for communication, Kumar et al. [3] created a fingerprint-based access system which can communicate with cloud services. This method was highly dependent upon consistent internet connectivity, even though it enabled real-time access control and monitoring.

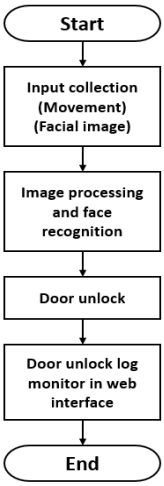
III. METHODOLOGY

The proposed system has been developed by utilizing a modular design approach with a focus on affordability, reliability, and ease of integration. The development process was divided into distinct phases from hardware selection and facial recognition setup to authentication logic and remote monitoring capabilities. The process ensures that each component

functions in synchronization with the others, resulting in a Raspberry Pi 3B smart door unlocking system that is completely operational.

IV. SYSTEM ARCHITECTURE

The architecture of the proposed smart door unlocking system is designed to ensure secure access through real-time authentication and hardware control. It integrates motion sensing, face recognition, PIN-based fallback authentication, and solenoid lock actuation into a compact, efficient setup. A Raspberry Pi 3B senses input, handles recognition processes and web-based monitoring.



A. System Activation and Data Captured

The Passive Infrared (PIR) sensor is the first component of the smart door system to detect motion in front of the entrance. Upon activating the PIR sensor, the Raspberry Pi 3B receives a signal to initiate image capturing using the attached USB camera. Continuous surveillance is maintained and rapid system response is ensured by this real-time picture acquisition procedure. Preprocessing techniques like scaling and grayscale conversion are used to captured frames in order to maximize the facial recognition capabilities. With the aim to save energy, the system automatically switches to a low-power standby state if no motion is detected. This approach strikes a compromise between system readiness and economical power use.

B. Face Recognition and Verification Module

The OpenCV and Dlib libraries, that utilize reliable computer vision algorithms for face detection and encoding, are used to process the collected image frames. Algorithms including deep learning-based embeddings and Histogram of Oriented Gradients (HOG) are used to extract facial features. Later, these encodings are compared with a locally saved dataset of Raspberry Pi authorized users. A similarity score is used to determine a match, and access is provided if the score is higher than the predetermined threshold. The system initiates a backup method for manual authentication in the event of the face cannot be recognized or the score drops below the threshold. This multi-layered verification technique enables strong security and increases accuracy.

C. Fall Back Authentication: Keypad Based PIN Entry

The system prompts the user to utilize the 4x4 matrix keypad for fallback authentication in case face recognition is unsuccessful or the person isn't in the approved database. It requires the entry of a 4-digit PIN code that is cross-checked against the securely stored data on the Raspberry Pi. If the entered PIN matches the stored credentials, the system grants access just as it would for a recognized face. However, the system initiates a temporary lockout as a security mechanism if the user enters the incorrect PIN three times in a row. To assure accountability and enable administrator review, all such efforts are logged.

D. Access Control and Solenoid Actuation

The Raspberry Pi activates a specific GPIO pin those powers the solenoid lock during authentication—either by facial recognition or PIN entry—is successful. As a result, the lock can disengage and the door can be physically unlocked for a short period of time—typically three to five seconds. The lock automatically re-engages to keep the door secure after the specified amount of time. While reducing mechanical wear, this mechanism ensures rapid and seamless access. With its close integration with the system's authentication logic, the solenoid lock provides a safe yet electronically operated solution.

V. RESULT AND ANALYSIS

Using a multi-modal authentication method, the suggested smart door unlocking system—which was set up on a Raspberry Pi 3B and was assessed for its capacity to offer safe, convenient access. The system incorporates motion detection, keypad input, facial recognition, and stepper motor-driven locking, all of which are controlled through a web-based interface. Five main categories are used to examine the results: facial recognition accuracy, keypad reliability, lock

control response, PIR-based system activation, and remote monitoring through the web interface.

Facial Recognition Accuracy

The face recognition the library was used to build the face recognition module which uses deep learning methods to identify registered users. To assess the system's dependability in the real world, it was tested in a variety of settings and lighting circumstances.

In illuminated and typical interior settings, the identification accuracy was high, accurately recognizing authorized individuals in less than two seconds. The success rate slightly decreased under challenging conditions, such as dim lighting, partial obstruction (such as masks or glasses), or non-frontal facial angles. The result was in line with the known limitations of lightweight models on embedded platforms. Keypad input and other backup alternatives, however, maintained general usability. In addition to optimizing resource utilization, the PIR sensor's ability to solely activate the camera in response to motion events ensured the recognition efforts were initiated whenever necessary.

VI. CONCLUSION

This paper successfully demonstrates the implementation of a smart, secure door unlocking system using the Raspberry Pi 3B. Dual-factor authentication is provided by the system, which combines computer vision for facial recognition with a 4x4 matrix keypad for human PIN entry, guaranteeing convenience and improved security. The system is more efficient and secure since local decision-making and real-time processing don't involve external servers.

The GPIO-controlled solenoid lock operated dependably across each test scenario. Its mechanical stability and rapid activation demonstrated the robustness of the hardware-software integration. Furthermore, the PIR sensor-based motion-triggered camera configuration ensured system resources were utilized solely when required, which improved responsiveness and power efficiency.

An important layer of control and transparency was provided for the administrator through the implementation of a web interface for logging and monitoring using on Ruby on Rails. Successful and unsuccessful login attempts were all recorded and shown on a clear, useful dashboard. In addition to improving security tracking, this makes it possible to scale in the future and integrate with larger IoT systems.

Overall, the project succeeds in creating a door access control system which is both economical and efficient. Workplace entrance systems, and remote access monitoring are a few of the small-scale security applications that can be accommodated by its modular architecture and low component requirements.

VII. FUTURE WORK

Although the existing system uses PIN authentication and facial recognition to provide reliable and secure door entry, there are few enhancements that could further improve its functionality. Efficiency, security, and user experience can be enhanced by further developments in hardware and software. Integrating new technologies will also support broader deployment scenarios. The system's intelligence, scalability, and dependability are the goals of these upcoming improvements.

Multi-Modal Authentication

Future iterations of the system might include RFID or NFC technology however it currently offers face and PIN-based identification. This would enable users to use smartphones or keycards to unlock the door. In settings with multiple users, such as offices or hostels, this is extremely helpful. Security will be increased by combining two or more techniques (e.g., facial + RFID). Additionally, it increases flexibility by providing customers with alternative options in case one approach fails. Minor software updates and new hardware would be required for the implementation

Cloud Integration and Remote Access

Currently, the Raspberry Pi is used to store all logs and data locally. In the future, logs can be remotely accessed and backed up using cloud storage services. This ensures the longevity of data and enables managers to keep track on access activities remotely. A web interface linked to the cloud might provide remote user administration, dashboards, and warnings. AWS, Firebase, and Azure integration would provide scalable infrastructure. The system would become more remotely controlled and robust.

REFERENCES

[1] Deepak, A., Kumar, N., & Sharma, P. SMS Based Door Locking System Using GSM. International Journal of Engineering Research and General Science, vol. 3, no. 2, 2015.
[2] Yadav, R., & Verma, A. Face Recognition Based Smart Door. International Journal of Engineering Research & Technology (IJERT), vol. 9, no. 5, 2020.
[3] Kumar, P., Singh, D., & Raj, M. IoT Based Smart Lock System Using Fingerprint and Cloud Integration. International Journal of Scientific Research and Engineering Development (IJSRED), vol. 3, no. 4, 2020.
[4] Bhatt, S., & Patel, N. Dual Authentication System Using RFID and Password. International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), vol. 6, no. 3, 2018.
[5] Mishra, R., Soni, S., & Sharma, R. Design and Implementation of Raspberry Pi Based Security System Using RFID and Camera. International Journal of Research in Engineering, Science and Management, vol. 1, no. 5, 2018.
[6] Sahu, A., & Panda, R. Smart Door Lock System Using Face Recognition. International Journal of Computer Science and Mobile Computing, vol. 7, no. 4, 2018.
[7] Rajesh, V., Kumar, M., & Balamurugan, P. Facial Recognition Based Door Lock System Using GSM and Keypad. International Journal of Engineering and Techniques (IJET), vol. 4, no. 2, 2018.
[8] Patel H., & Sharma, S. Web-based Smart Home Automation System Using Raspberry Pi. International Journal of Research in Engineering, Science and Management, vol. 2, no. 4, 2019.
[9] Patel, R., Mehta, K., & Shah, D. Smart Surveillance System Using PIR Sensor and Raspberry Pi. International Journal of Scientific and Research Publications, vol. 7, no. 12, 2017.
[10] Chakraborty, S., Das, T., & Ghosh, A. Review of Smart Locking System in IoT. International Journal of Scientific & Engineering Research, vol. 10, no. 5, 2019.
[11] Sharma, A., & Thakur, R. Multi-Factor Authentication Door Locking System. International Research Journal of Modernization in Engineering Technology and Science (IRJMETS), May 2023.