International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

LockMate: Intelligent Dual Biometric Authentication System for Door Access

Miss. Shrawani Maruti Nawale
Artificial Intelligence & Machine Learning Engineering
Samarth College Of Engineering & Management , Belhe Pune, India

Miss. Janvi Santosh Pokharkar
Artificial Intelligence & Machine Learning Engineering
Samarth College Of Engineering & Management , Belhe Pune, India

Prof. Prajakta Thorat Tanaji
Artificial Intelligence & Machine Learning Engineering
Samarth College Of Engineering & Management , Belhe Pune, India

Miss. Gayatri Vikas Shelke
Artificial Intelligence & Machine Learning Engineering
Samarth College Of Engineering & Management , Belhe Pune, India

***Abstract* - Security in modern environments requires more reliable solutions than traditional locks and passwords. This paper presents LockMate, an Artificial Intelligence-based multi-factor authentication system for secure door access. The system integrates three authentication layers: PIN verification, fingerprint recognition, and facial recognition to enhance security and prevent unauthorized entry. Facial recognition is implemented using OpenCV and deep learning-based encoding techniques, while fingerprint authentication ensures high accuracy through biometric verification. The system is built using Raspberry Pi, enabling efficient hardware-software integration and real-time processing. Additionally, IoT-based features allow access logging and alert notifications for failed attempts. Experimental results show high accuracy, low false acceptance rate, and fast response time, making the system reliable and efficient. The proposed system provides a cost-effective, scalable, and robust solution for smart homes, offices, and high-security areas, addressing the limitations of conventional access control systems.**

***Keywords*— Artificial Intelligence (AI), Dual Biometric Authentication, Raspberry Pi, Internet of Things (IoT), Smart Security, Access Control System, Solenoid Lock, Embedded Systems.**

I. INTRODUCTION

In the modern era of smart technologies, ensuring secure and reliable access control has become increasingly important for residential, commercial, and industrial environments. Traditional door locking mechanisms such as keys, passwords, and keycards are widely used but suffer from significant security limitations, including the risk of loss, duplication, and unauthorized sharing. These vulnerabilities highlight the need for more advanced and intelligent security solutions.

Biometric authentication has emerged as a promising approach for enhancing security by utilizing unique human characteristics such as fingerprints and facial features. However, systems relying on a single biometric modality may still face challenges such as spoofing, sensor errors, or environmental variations. To address these issues, dual biometric authentication systems have gained attention as they combine multiple biometric factors to improve reliability and reduce the chances of unauthorized access.

This paper presents **LockMate**, an Artificial Intelligence-based dual biometric authentication system designed for secure door access. The system integrates facial recognition and fingerprint verification as two primary authentication layers, supported by an optional PIN-based mechanism for additional security. Facial recognition is implemented using computer vision and deep learning techniques, enabling real-time detection and identification, while fingerprint recognition ensures accurate user validation through unique biometric patterns.

The proposed system utilizes a Raspberry Pi as the central processing unit, enabling seamless integration of hardware components such as the fingerprint sensor, camera module, and door locking mechanism. Additionally, the system incorporates IoT-based features for access logging, monitoring, and alert generation in case of unauthorized attempts. By combining artificial intelligence with embedded systems, LockMate provides a cost-effective, scalable, and highly secure solution suitable for smart homes, offices, and restricted environments.

II. LITERATURE SURVEY

A brief overview of existing work in various papers, which have been referred for implementation:

In [1],2022 NAKANDHRAKUMAR. R. S Design and Development of IoT Based Smart Door Lock System: This

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

work designs an IoT-controlled door lock using microcontrollers and sensors. It enables remote monitoring and secure digital access for users. The paper focuses on reliability, cost-effectiveness, and real-time alerts. It provides groundwork for future biometric-based IoT security innovations.

In[2] 2023,Ketan Gupta Smart Door Locking System Using IoT:This study presents an IoT-enabled door lock operated via smartphone and Bluetooth. It automates acces control, improving convenience and reducing key depenency.The system demonstrates efficient real-time control through IoT connectivity.It forms the base for integrating biometrics in advanced smart lock mechanisms.

In[3] 2024,Mohamed abdulal Rami qahwai A Novel Approach to Enhancing Multi-Modal Facial Recognition: This paper integrates CNN, PCA, and SNN to improve facial recognition accuracy.
It combines deep learning and feature reduction for robust multi-modal recognition. The hybrid approach enhances performance under varying lighting and pose conditions.This concept supports AI-based biometric authentication in smart security systems.

III. EXISTING SYSTEM

The Traditional and modern door access control systems have evolved to address the need for security in residential, commercial, and institutional environments. The most commonly used systems include **mechanical lock-and-key systems** are the oldest and most widely used form of access control. While simple and cost-effective, they suffer from significant drawbacks, such as the risk of lost, stolen, or duplicated keys. Unauthorized duplication of keys and lock-picking techniques further compromise. Electronic locks that use keypads require users to enter a numeric or alphanumeric password to gain access. While these systems are more flexible than traditional keys, they are vulnerable to several attacks:

- Most conventional systems rely on a single authentication factor, making them vulnerable if that factor is compromised.
- Many lack comprehensive monitoring, logging, or alert mechanisms for unauthorized access attempts.
- Biometric data in some systems may not be securely stored, raising privacy concerns.

These limitations highlight the need for more robust access control solutions that combine multiple authentication factors and intelligent monitoring motivating the development of advanced systems like LockMate.

IV. PROPOSED SYSTEM

The proposed system, LockMate, is designed to enhance physical security using an Artificial Intelligence (AI)-based dual biometric authentication mechanism. It integrates two powerful biometric modalities—fingerprint recognition and facial recognition—to establish a multi-level verification framework that ensures only authorized individuals gain access. This approach overcomes the limitations of traditional password or single-biometric systems, which are often susceptible to duplication, spoofing, and hacking.The inclusion of AI algorithms enables accurate and efficient facial recognition even under varying lighting conditions or minor changes in the user's appearance. Additionally, IoT connectivity can be implemented to allow remote monitoring, access logging, and real-time notifications through Wi-Fi or a mobile application. In case of multiple failed authentication attempts, the system can trigger an alarm or send alerts to the authorized user's device for enhanced security.

V. SYSTEM ARCHITECTURE

The proposed Lockmate Door Access System follows a client-server architecture consisting of two main components: a Laptop Application (client) and a Raspberry Pi Hardware Controller (server). The system implements a three-layer multi-factor authentication mechanism including PIN verification, fingerprint recognition, and face recognition to ensure high security.

The Laptop Application acts as the main controller and provides a Tkinter-based GUI for user interaction. It performs face recognition using OpenCV and the face_recognition library, manages user data using an SQLite database, maintains access logs, and generates email alerts for unauthorized access attempts.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

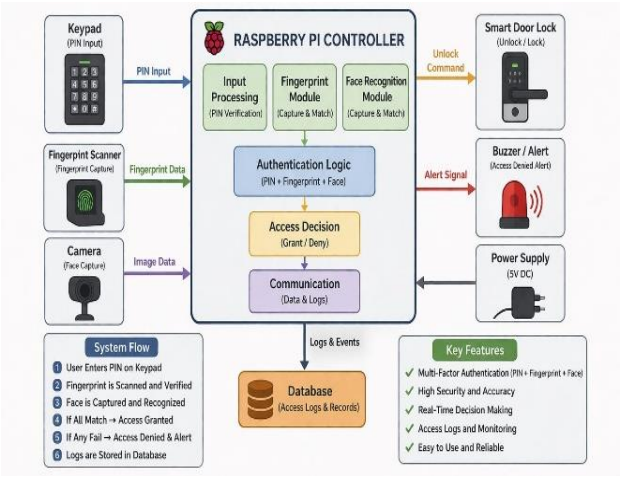

Fig: System Architecture

The Raspberry Pi functions as a hardware controller using a Flask REST API. It interfaces with the R307S fingerprint sensor for biometric verification, controls the servo motor for door locking/unlocking, and activates the buzzer for audio alerts. Communication between the laptop and Raspberry Pi is achieved through HTTP-based REST APIs over a local network using JSON data format.

The system operates sequentially: the user first enters a PIN, followed by fingerprint verification, and finally face recognition. If all three authentication layers are successfully validated, access is granted and the door is unlocked; otherwise, access is denied and an alert is generated. This architecture ensures secure, real-time, and efficient access control.

VI. IMPLEMENTATION

The Lockmate Door Access System is implemented using a modular approach, where each functionality is developed as an independent module to ensure scalability, maintainability, and efficient performance.

Module 1: User Registration

This module is responsible for enrolling new users into the system. It captures user details such as user ID, name, age, and phone number. A 4-digit PIN is created and securely stored using SHA-256 hashing. The system also enrolls the user's fingerprint using the R307S sensor and captures facial images through the camera to generate a 128-dimensional face encoding, which is stored in the SQLite database.

Module 2: Access Verification

This module handles the core authentication process using three layers. First, the user enters a PIN, which is verified against the stored hash. If valid, the system proceeds to fingerprint verification via the Raspberry Pi. Upon successful fingerprint matching, the system performs face recognition by capturing a live image and comparing it with stored encodings. Access is granted only if all three layers are successfully verified.

Module 3: Face Recognition Engine

This module performs face detection, encoding, and matching. It uses OpenCV and the face_recognition library to detect faces and generate 128-dimensional feature vectors. The system calculates the Euclidean distance between stored and captured encodings, and if the distance is below a defined threshold, the face is recognized as valid.

Module 4: Raspberry Pi Hardware Controller

This module manages all hardware operations through a Flask REST API. It controls the fingerprint sensor for enrollment and verification, operates the servo motor to lock/unlock the door, and activates the buzzer for alerts. It communicates with the laptop application using HTTP requests and JSON responses.

Module 5: Email Alert and Logging System

This module is responsible for security monitoring. It logs all access attempts with details such as timestamp, user ID, and authentication status. In case of failed authentication, it sends an email alert with a snapshot image of the user, specifying the reason for failure. This enhances system security and traceability.

VII. RESULT & DISCUSSIONS

The proposed LockMate Door Access System demonstrates efficient performance in providing secure and intelligent access control through the integration of software and hardware components. The system interface, as shown in the User Registration and Access Verification modules, operates smoothly and allows users to interact with the system effectively.

The registration module successfully captures user details such as user ID, PIN, fingerprint, and facial data. The fingerprint enrollment process using the R307S sensor is reliable and accurately stores biometric templates in the database. The face enrollment module initializes the camera and captures facial features efficiently for further recognition.

During the access verification process, the system performs multi-factor authentication in a sequential manner. The PIN verification stage responds quickly, followed by fingerprint verification, which provides consistent and accurate results. The face recognition module activates the camera in real time and matches the captured face with stored encodings effectively.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

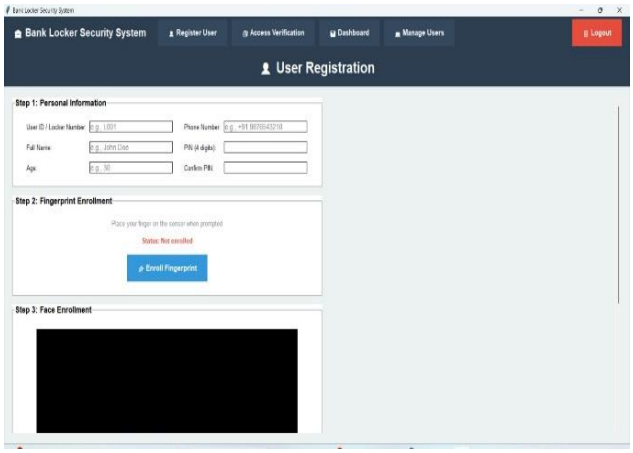

Fig: Dashboard

From the hardware perspective, the Raspberry Pi 4 acts as the central controller, efficiently managing all connected components. The R307S fingerprint sensor performs fast and accurate biometric verification within one second. The camera module captures real-time images for facial recognition, while the servo motor operates reliably to control door access upon successful authentication. The buzzer provides immediate feedback during authentication success or failure. All components are interconnected and powered through the Raspberry Pi, ensuring stable operation.

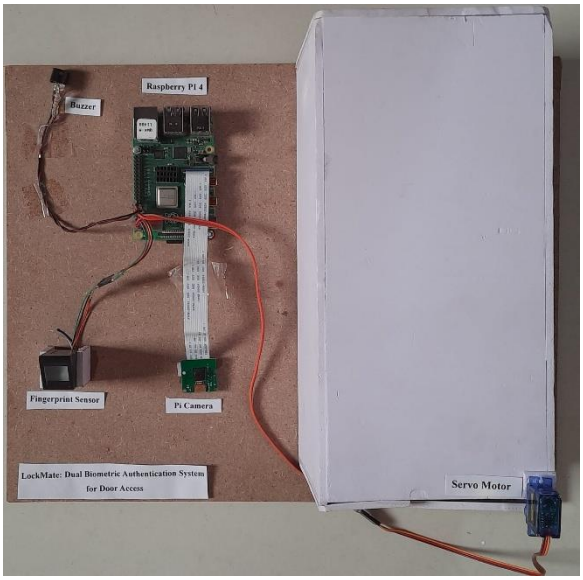

Fig: Hardware Connectivity

The communication between the software interface and hardware components is achieved through a Flask-based REST API over a local network, which ensures smooth data exchange and minimal latency. Overall, the system reduces manual effort, enhances security through multi-factor authentication, and provides a cost-effective and practical solution for modern access control applications. The integration of hardware and software ensures real-time performance and makes the system suitable for secure environments such as bank lockers and offices.

VIII. APPLICATIONS

The Lockmate Door Access System with multi-factor authentication has a wide range of applications in areas requiring secure and reliable access control. The integration of PIN, fingerprint, and facial recognition makes it suitable for both residential and commercial environments.

In banking and financial institutions, the system can be used for securing lockers, vaults, and restricted transaction areas, ensuring that only authorized personnel gain access. In corporate offices, it can be deployed to protect confidential data rooms, server rooms, and research laboratories where sensitive information is stored.

The system is also highly applicable in smart homes, providing enhanced security compared to traditional locks by preventing unauthorized entry through multiple authentication layers. In educational institutions, it can be used to restrict access to laboratories, examination control rooms, and administrative offices. Additionally, the system can be implemented in government and defense sectors where high-level security is required.Overall, the proposed system provides a scalable and efficient solution for modern security needs across various domains requiring advanced authentication mechanisms.

IX. FUTURE WORK

Although the proposed Lockmate Door Access System demonstrates high accuracy and reliability, several enhancements can be implemented to further improve its performance and scalability. One potential improvement is the integration of a mobile application that allows users and administrators to remotely monitor access logs, receive real-time notifications, and control the system.

The system can also be enhanced by incorporating cloud-based storage, enabling centralized data management, backup, and remote accessibility. Additionally, advanced deep learning models can be used to improve face recognition accuracy under challenging conditions such as low lighting, occlusions, and varying angles.

Another possible extension is the addition of voice recognition as an extra authentication layer, making the system more secure and flexible.Furthermore, implementing encryption techniques and blockchain-based security can strengthen data protection and prevent unauthorized data access. These improvements will make the system more robust, scalable, and suitable for large-scale real-world deployments.

X. CONCLUSION

The Lockmate Door Access System presents a reliable and efficient solution for modern security requirements by integrating multi-factor authentication techniques. The system combines PIN verification, fingerprint recognition, and facial recognition to provide a robust three-layer security mechanism, significantly reducing the risk of unauthorized access compared to traditional systems.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The implementation using Python, OpenCV, SQLite, and Raspberry Pi demonstrates effective hardware-software integration, ensuring real-time performance and accurate authentication. Experimental results show that the system achieves high accuracy, low false acceptance rates, and fast response time within the defined performance limits. Additionally, features such as access logging, email alerts, and user management enhance the overall functionality and usability of the system.

The proposed system is cost-effective, scalable, and suitable for deployment in various high-security environments such as banks, offices, and smart homes. Overall, the system successfully meets the objectives of providing secure, efficient, and intelligent access control, making it a practical solution for real-world applications.

XI. REFERENCES

[1] Nakandhrakumar. R. S , Ramkumar Venkatasamy Design and Development of IOT based Smart Door Lock System DOI: 10.1109/ ICICICT54557.2022.9917767

[2] K. Gupta, N. Jiwani, N. Afreen, and Mehmood Ali Mohammed.,Smart Door Locking System Using IoT in January 2023 DOI: 10.1109/ICACCM56405.2022.10009534

[3] H Khan,S Uzir,F. Khan Utilizing Bio Metric System for Enhancing Cyber Security in Banking Sector:A Systematic Analysis https:// www.researchgate.net/publication/372646377_Utilizing_Bio_Metric_ system_for_enhancing_Cyber_security_in_banking_sector_A_Syste maticAnalysis DOI10.1109/ACCESS.2023.

[4] K. AL-Dosari, N. Fetais, and M. Kucukvar, ‘‘Artificial intelligence aC. F. Gaitán,

[5] T.-H. Chen, ‘‘Do you know your customer? Bank risk assessment based on machine learning,’’ Appl.SoftComput.,vol.86,Jan.2020,Art. no. 105779.

[6] A. Jain, D. Arora, R. Bali, and D. Sinha, ‘‘Secure authentication for bank ing using face recognition,’’ J. Informat. Electr. Electron. Eng. (JIEEE), vol. 2, no. 2, pp. 1–8, Jun. 2021.

[7] A. Krizhevsky, I. Sutskever, and G. E. Hinton, ImageNet classi cation with deep convolutional neural networks, in Proc. Adv. Neural Inf. Pro cess. Syst., 2012, pp. 10971105.

[8] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, You only look once: Uni ed, real-time object detection, in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), May 2016, pp. 779788. [Online]. Available: https://www.cv-foundation.org/openaccess/content_cvpr_2016/papers/Redmon_You_ Only_Look_CVPR_2016_paper.pdf

[9] S. W. Shah and S. S. Kanhere, Recent trends in user authentication A survey, IEEE Access, vol. 7, pp. 112505112519, 2019, doi: 10.1109/ACCESS.2019.2932400.

[10] K. M. Renuka, S. Kumari, D. Zhao, and L. Li, Design of a secure password-based authentication scheme for M2M networks in IoT enabled cyber-physical systems, IEEE Access, vol. 7, pp. 5101451027, 2019, doi: 10.1109/ACCESS.2019.2908499.

[11] H.-J. Mun, Biometric Information and OTP based on authentication mechanism using blockchain, J. Converg. Inf. Technol., vol. 8, no. 3, pp. 8590, 2018, doi: 10.22156/CS4SMB.2018.8.3.085

[12] X. Li and H. Niu, ‘‘Feature extraction based on deep-convolutional neural network for face recognition,’’ Concurrency Comput., Pract. Exper., vol. 32, no. 22, p. 1, 2020.

[13] N. Radha and A. Kavitha, ‘‘Rank level fusion using fingerprint and iris biometrics,’’ Indian J. Comput. Sci. Eng., vol. 2, no. 6, pp. 917–923, 2012.

[14] G. Amirthalingam and G. Radhamani, ‘‘A multimodal approach for face and ear biometric system,’’ Int. J. Comput. Sci. Issues (IJCSI), vol. 10, no. 5, p. 234, 2013.

[15] D.T.MevaandC.K.Kumbharana,‘‘Comparativestudyofdifferentfusion techniques in multimodal biometric authentication,’’ Int. J. Comput. Appl., vol. 66, no. 19, pp. 16–19, 2013.