LockMate: Artificial Intelligence-Based Dual Biometric Authentication System For Door Access

Janvi Pokharkar[1], Shrawani Nawale[2], Gayatri Shelke[3], Prof.Thorat Prajkta [4]

Abstract- *Security and privacy have become critical concerns in modern smart environments where traditional door locking mechanisms, such as keys and PIN-based systems, are no longer sufficient to ensure robust access control. To overcome these limitations, this paper presents LockMate, an Artificial Intelligence-based Dual Biometric Authentication System that integrates facial recognition and fingerprint verification for secure door access. The system is implemented using a Iot. AI algorithms perform real-time facial detection and recognition, while the fingerprint sensor provides a secondary layer of authentication. This multi-level verification framework significantly enhances system reliability, reduces the risk of unauthorized entry, and ensures that only authenticated users gain access. The inclusion of IoT-based remote monitoring and access logging further strengthens the system's adaptability for smart homes and commercial environments. The proposed system demonstrates how AI-driven biometrics and embedded hardware can collaboratively achieve an intelligent, scalable, and secure access control solution.*

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

I. INTRODUCTION

Conventional door locking mechanisms, such as traditional locks and keypads, have long been the standard for securing residential and commercial spaces. However, these methods present notable security vulnerabilities, including the risk of lost or stolen keys and the potential for passwords to be guessed or shared. As security threats have evolved, so too has the need for more robust access control solutions.

Multi-factor authentication (MFA) has emerged as a powerful method to mitigate these limitations by requiring multiple, independent credentials for access. In response to the growing demand for enhanced security, this research proposes LockMate—an artificial intelligence-based, dual-biometric authentication system designed for secure door access. LockMate integrates three levels of authentication: a user-entered password, fingerprint recognition, and facial recognition. This hierarchical approach ensures that only authorized individuals can gain entry, even if one security factor is compromised.

The LockMate system leverages the capabilities of the Internet of Things (IoT), utilizing components such as a Raspberry Pi or Arduino microcontroller, fingerprint sensor, and camera to implement a seamless and intelligent access control process. The system is designed to be user-friendly, cost-effective, and adaptable for various environments, including homes, offices, and restricted facilities.

This paper presents the design, implementation, and evaluation of the LockMate system. It aims to demonstrate how the integration of multi-level authentication and AI-driven biometrics can significantly enhance the security and reliability of modern door access control systems.

II. LITERATURE SURVEY

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

In[1]2024,Mohamed abdulal Rami qahwaiA 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.

In[2]2023,Ketan GuptaSmart 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 IoTconnectivity.It forms the base for integrating biometrics in advanced smart lock mechanisms.

In [3],2022 NAKANDHRAKUMAR. R. SDesign and Development of IoT Based Smart Door Lock System: This 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.

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 arethe 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.

4.1 RASPBERRY PI

The Raspberry Pi 4 serves as the main processing and control unitof the LockMate system. It operates as a mini-computer capable of running Python-based AI algorithms and interfacing with peripheral devices. Equipped with a quad-core ARM Cortex-A72 processor, onboard Wi-Fi, and multiple GPIO pins, it efficiently handles sensor inputs, processes biometric data, and controls the door lock mechanism. It also facilitates communication with cloud or IoT platforms for remote monitoring and logging access data.

4.2RASPBERRY PI CAMERA

This module is responsible for capturing facial images of users during authentication. Integrated with the OpenCV library, it performs face detection and recognition using machine learning models. The high-resolution camera ensures accurate image acquisition under various lighting conditions. It connects directly to the Raspberry Pi via the CSI (Camera Serial Interface) port, enabling high-speed data transfer for real-time processing.

4.3 R307 FINGERPRINT SENSOR

The R307 is a high-precision optical fingerprint sensor that captures, processes, and matches fingerprint images. It contains an internal DSP (Digital Signal Processor) for feature extraction and template matching. The module communicates with the Raspberry Pi using UART serial communication and can store multiple fingerprint templates in its internal memory. It provides reliable and fast identification, forming the first layer of authentication in the LockMate system.

4.4 KEYPAD MATRIX

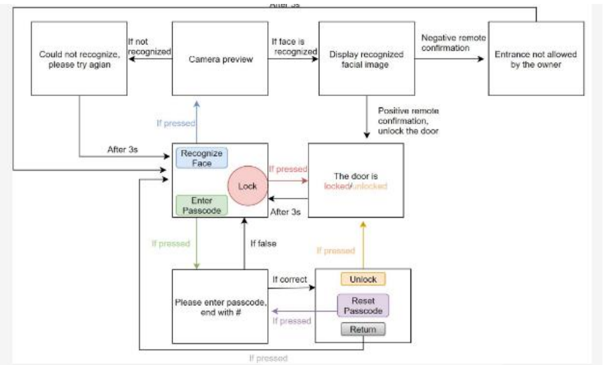
The 4x4 matrix keypad serves as a manual input interface between the user and the system. It can be used for password entry, system configuration, or additional control commands. The keypad sends signals through row and column connections to the Raspberry Pi's GPIO pins, allowing the software to detect which key is pressed. It enhances system flexibility by supporting manual overrides or administrative functions.

4.5LCD DISPLAY

A 16x2 LCD display with an I2C communication interface is used to display system messages, authentication prompts, and status notifications. The I2C module minimizes the number of GPIO pins required, simplifying circuit design. It provides real-time feedback such as "Enter Fingerprint," "Face Verified," or "Access Denied," ensuring clear interaction between the system and the user.

V. SYSTEM ARCHITECTURE

The system architecture of LockMate is designed to provide a secure, efficient, and intelligent door access mechanism by integrating artificial intelligence with dual biometric authentication. The architecture consists of hardware and software modules that work collaboratively to ensure accurate identification and robust control over door operations.


After 3s
Could not recognize, please try agian
If not recognized
Camera preview
If face is recognized
Display recognized facial image
Negative remote confirmation
Entrance not allowed by the owner
If pressed
Positive remote confirmation, unlock the door
After 3s
Recognize Face
Lock
Enter Passcode
If pressed
The door is locked/unlocked
After 3s
If pressed
If false
If pressed
Please enter passcode, end with #
If correct
Unlock
Reset Passcode
If pressed
Return
If pressed

The process begins when a user approaches the door. The camera module captures the user's facial image and processes it using AI-based facial recognition algorithms. If the face is successfully recognized, the system prompts the user to enter a passcode through the keypad interface. The entered passcode is verified against a stored database in the Raspberry Pi's memory.If both authentication stages are validated, the Raspberry Pi triggers the relay module to activate the solenoid lock, thereby unlocking the door. In the case of incorrect credentials or unrecognized faces, the system denies access and displays an appropriate message on the LCD. Additionally, the system includes remote confirmation functionality, allowing the owner to permit or deny entry through connected IoT services.

This architecture ensures robust, multi-layered security while maintaining operational simplicity and user convenience. It also logs each access attempt for future analysis, enhancing traceability and accountability.

VI. CONCLUSION

The LockMate: Artificial Intelligence-Based Dual Biometric Authentication System enhances traditional door security through the integration of AI-driven facial recognition and passcode verification. By combining these two authentication layers, the system minimizes vulnerabilities associated with single-factor methods such as keys or standalone passwords. The use of Raspberry Pi as the central controller ensures efficient processing, real-time decision-making, and smooth hardware coordination.

This intelligent system not only provides high security but also improves user convenience with automation and remote monitoring capabilities. In essence, LockMate demonstrates how AI and IoT technologies can be effectively applied to modern access control systems, offering a reliable, scalable, and secure solution for both residential and commercial environments.

REFERENCES

[1] M. Castelli, L. Manzoni, and A. Popovič, ''An artificial intelligence system to predict quality of service in banking organizations,'' Comput. Intell. Neurosci., vol. 2016, May 2016, Art. no. 9139380.

[2] F. Gideon, M. A. Petersen, J. Mukuddem-Petersen, and B. De Waal, ''Bank liquidity and the global financial crisis,'' J. Appl. Math., vol. 2012, May 2012, Art. no. 743656.

[3] L. Sun, S. Wu, Z. Zhu, and A. Stephenson, ''Noninterest income and performance of commercial banking in China,'' Sci. Program., vol. 2017, Feb. 2017, Art. no. 4803840.

[4] K. Riad and M. Elhoseny, ''A blockchain-based key-revocation access control for openbanking,'' Wireless Commun.MobileComput.,vol.2022, Jan. 2022, Art. no. 3200891.

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

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

[7] 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.

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

[9] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, You only look once: Unied, 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

[10] 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.

[11] 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.

[12] 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

[13] 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.

[14] 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.

[15] 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.

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

[17] M. L. Gavrilova and M. M. Monwar, ''Current trends in multimodal bio metric system-rank level fusion, in pattern recognition,'' in Machine Intel ligence and Biometrics. Berlin, Germany: Springer, 2011, pp. 657–673.

[18] J. Jeong, "A Study on the IoT Based Smart Door Lock System BT - Information Science and Applications (ICISA) 2016," 2016, pp. 1307–1318.

[19] K. Patil, N. Vittalkar, P. Hiremath, and M. Murthy, "Smart Door Locking System using IoT," Int. J. Eng. Technol., vol. 7, pp. 56 2395, May 2020.

[20] Y. T. Park, P. Sthapit, and J. Pyun, "Smart digital door lock for the home automation," in TENCON 2009 - 2009 IEEE Region 10 Conference, 2009, 10.1109/TENCON.2009.5396038. pp