International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

Intelligent Lock System with Facial Recognition and Fingerprint-Based Authentication Applications

Gandrathi Navya jyothi[1*], Thaduka Varun[2], Suram Akshith[2], Konda Sai Vardhan[2], Thotakuri Ganesh[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Electronics & Communication Engineering

[1,2]Vaagdevi Engineering College, Bollikunta, Warangal, 506005, Telangana, India.

*Correspondence: Gandrathi Navya jyothi (navyakits@gmail.com)

Abstract

In practical scenarios such as smart homes, offices, research laboratories, and restricted access facilities, there is a critical requirement for systems that provide secure, automated, and real-time access control. These environments demand reliable authentication mechanisms, continuous monitoring, and immediate alerts to prevent unauthorized entry. Traditional locking systems based on keys, PINs, or passwords are prone to theft, duplication, and hacking, while lacking real-time monitoring and remote accessibility. Furthermore, conventional systems do not integrate biometric verification or intelligent analytics, reducing their effectiveness in modern security applications. To address these challenges, the proposed Facial Lock Drive 2.0 utilizes the ESP32 microcontroller to develop a robust and intelligent access control system. The system integrates an ESP32-CAM for facial recognition and a fingerprint sensor for multi-factor biometric authentication, ensuring high security and accuracy. Upon successful verification, the ESP32 activates a DC motor to control the door locking mechanism, while an LCD display provides real-time system status and authentication feedback. Unauthorized access attempts trigger buzzer alerts, enhancing security awareness. IoT integration enables remote monitoring, access log management, and real-time notifications through cloud platforms. This smart system enhances security, eliminates the limitations of traditional locking methods, and provides a scalable, reliable, and intelligent solution for modern access control applications.

Keywords: Access Control System, Biometric Authentication, Facial Recognition, Fingerprint Sensor, Internet of Things, Smart Door Lock, Smart Home Security, Surveillance Systems

1. Introduction

The increasing demand for advanced security systems in residential, commercial, and high-security environments has grown rapidly due to rising safety concerns and technological advancements [1]. The global security systems market is expected to exceed 200 billion USD, while biometric authentication technologies are witnessing growth rates above 15% annually, driven by the need for reliable and tamper-proof access control [2]. Incidents involving unauthorized access—often caused by key duplication, password breaches, and weak authentication mechanisms—continue to increase, highlighting vulnerabilities in traditional systems. In environments such as smart homes, offices, research laboratories, and restricted facilities, there is a critical need for solutions that provide secure, automated, and real-time access control with high accuracy and reliability [3].

Traditional locking systems rely on keys, PINs, or password-based authentication methods, which are inherently prone to security risks. Physical keys can be lost or duplicated, while passwords and PINs can be guessed, shared, or hacked. These systems typically lack real-time monitoring and remote accessibility, making it difficult to track access or respond to unauthorized attempts [4].

Received: 03-03-2026 | Accepted: 06-04-2026 | Published: 13-04-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

Additionally, conventional systems do not incorporate biometric verification or intelligent analytics, limiting their ability to ensure identity authenticity [5]. As a result, they are insufficient for handling modern security requirements, especially in sensitive or high-risk environments.

In real-time scenarios, these limitations lead to several critical challenges that compromise safety and control. Unauthorized access attempts may go undetected or unrecorded due to the absence of continuous monitoring systems [6]. Delayed alerts and lack of real-time notifications prevent timely intervention during security breaches. Furthermore, reliance on single-factor authentication increases vulnerability to identity theft and unauthorized entry [7]. The inability to maintain access logs and analyze patterns reduces system transparency and accountability. These challenges highlight the need for an intelligent, IoT-based access control system that integrates multi-factor biometric authentication, real-time monitoring, and instant alert mechanisms, ensuring enhanced security, improved reliability, and efficient management of modern access control environments.

2. Literature Survey

Pecolt et al. [8] proposed a Raspberry Pi-based face recognition system for personal identification using embedded processing and image analysis techniques. George et al. [9] proposed EdgeFace, an efficient face recognition model optimized for edge devices with reduced computational complexity. Chaiyarab et al. [10] proposed an authentication system using Histogram of Oriented Gradients (HOG)-based face recognition integrated with a web-based interface for medical dispenser machines.

Rosebrock [11] proposed a Raspberry Pi-based face recognition implementation using image processing libraries and pre-trained models for real-time detection. Rana et al. [12] proposed a real-time deep learning-based face recognition system using Raspberry Pi that integrated neural network models for improved accuracy. Madhavan et al. [13] proposed a survey on incremental methods in face recognition, analyzing adaptive learning techniques for continuous model improvement.

Selvaganesan et al. [14] proposed a comprehensive evaluation of deep learning models for face recognition along with a novel ensemble approach using hyperparameter tuning. Li et al. [15] proposed a survey on deep facial expression recognition, analyzing models for emotion detection using facial features. The study highlighted advancements in feature extraction techniques. Prasad [16] proposed an Internet of Things (IoT)-based door access control system using face recognition for secure authentication.

Eddine et al. [17] proposed a real-time face recognition system using Raspberry Pi 4 with optimized algorithms for embedded deployment. Shi et al. [18] proposed the LighterFace model for community face detection and recognition using a lightweight deep learning architecture. Chamikara et al. [19] proposed a privacy-preserving face recognition system using differential privacy techniques to protect user data.

3. Proposed System

Figure 1 illustrates the architecture of Facial Lock Drive 2.0; an advanced smart security system built around the ESP32. The system integrates biometric authentication modules such as ESP32-CAM for facial recognition and a fingerprint sensor for identity verification. A regulated power supply ensures stable operation of all components. The ESP32 processes biometric inputs and controls output devices including an LCD display for status messages, a buzzer for alerts, a DC motor for door locking/unlocking, and IoT connectivity

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

for remote monitoring. This system provides a secure, automated, and intelligent access control mechanism.

Step 1: Power Supply Initialization: The regulated power supply converts input voltage into stable DC voltage required for the ESP32 and all connected modules, ensuring reliable system operation.

Step 2: Facial Recognition using ESP32-CAM: The ESP32-CAM captures real-time facial images of the user and compares them with stored authorized images to verify identity.

Step 3: Fingerprint Authentication: The fingerprint sensor scans the user's fingerprint and matches it with stored templates to ensure that the person is authorized.

Step 4: Data Processing by ESP32: The ESP32 processes both facial and fingerprint data to perform multi-factor authentication, improving system security and reliability.

Step 5: Door Control using DC Motor: If authentication is successful, the ESP32 activates the DC motor, which controls the locking mechanism and opens the door.

Step 6: LCD Display Output: The LCD displays real-time messages such as "Access Granted" or "Access Denied," providing clear user feedback.

Step 7: Buzzer Alert System: If authentication fails or unauthorized access is detected, the buzzer is activated to alert nearby individuals and enhance security.

Step 8: IoT-Based Remote Monitoring: The ESP32 transmits access logs and system data to a cloud platform via IoT, enabling users to monitor entry activity and receive alerts remotely.

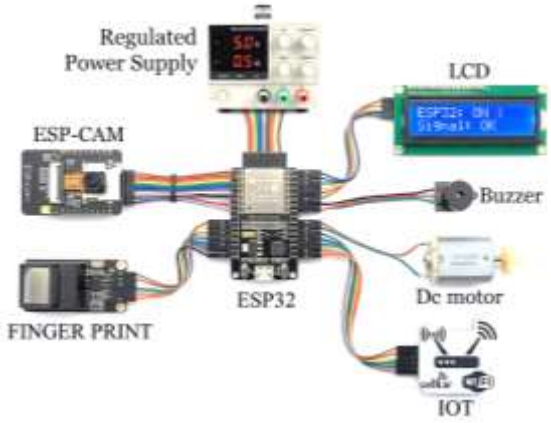


Figure 1. Facial Lock Drive 2.0 – Smart Biometric Access Control System.

3.1 Working Procedure

The proposed system as shown in Figure 2, Facial Lock Drive 2.0, is an advanced smart security system designed to provide secure and intelligent access control using biometric authentication and IoT technology. The system aims to enhance security by integrating facial recognition and fingerprint authentication to verify the identity of individuals attempting to access a secured area. Unlike traditional locking mechanisms that rely on keys or passwords, the proposed system uses biometric features that are unique to each individual, making unauthorized access extremely difficult.

The system is built around the ESP32 microcontroller, which acts as the central processing unit responsible for controlling all connected modules. The ESP32 collects input data from biometric devices such as the ESP-CAM module and the fingerprint sensor. These modules are used to capture facial images and fingerprint patterns of individuals attempting to unlock the door.

The ESP-CAM module performs facial recognition by capturing images and comparing them with previously stored authorized user images. If the captured face matches the stored database, the system identifies the user as authorized. In addition to

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

facial recognition, the system also integrates a fingerprint sensor, which scans the fingerprint of the user and compares it with stored fingerprint templates for authentication.

Once the authentication process is successfully completed, the ESP32 sends control signals to activate a DC motor, which operates the door locking mechanism. This allows the door to open for authorized users. If authentication fails, the system does not activate the motor and instead triggers an alert mechanism.

To provide real-time system information, the system includes an LCD display, which shows messages such as "Access Granted" or "Access Denied." A buzzer is also included in the system to provide audible alerts during unauthorized access attempts or system errors.

Additionally, the system incorporates IoT connectivity, allowing authentication data and system logs to be transmitted to remote monitoring platforms via Wi-Fi. This feature enables users to monitor door access activity remotely and receive notifications whenever unauthorized access attempts occur.

By combining facial recognition, fingerprint authentication, automated locking mechanisms, and IoT communication, the proposed system significantly improves security and provides a modern solution for smart home and office access control system.

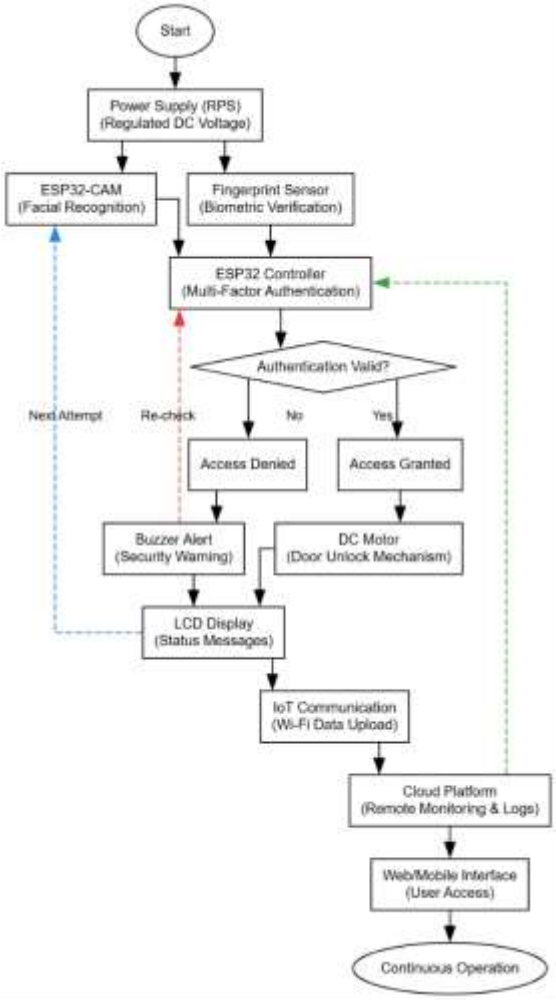


Figure 2. Proposed Flowchart.

Figure 3 illustrates the circuit diagram of the Facial Lock Drive 2.0 system, an advanced IoT-enabled smart access control solution that integrates facial recognition and biometric authentication. The system is powered by a regulated power supply unit comprising a step-down transformer, bridge rectifier, filter capacitors, and a 7805-voltage regulator to provide a stable +5V output. The ESP32 microcontroller serves as the central processing unit, interfacing with a keypad for manual input, a motor for lock/unlock actuation, and a fingerprint sensor for biometric verification. An IoT camera module enables facial recognition and real-time monitoring, enhancing security through AI-based authentication. The system also includes a 16×2 LCD to display user status and access

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

messages, along with a buzzer for alert notifications during unauthorized access attempts. This integrated design ensures multi-layered security, combining facial recognition, fingerprint authentication, and IoT connectivity for smart and secure access control applications.

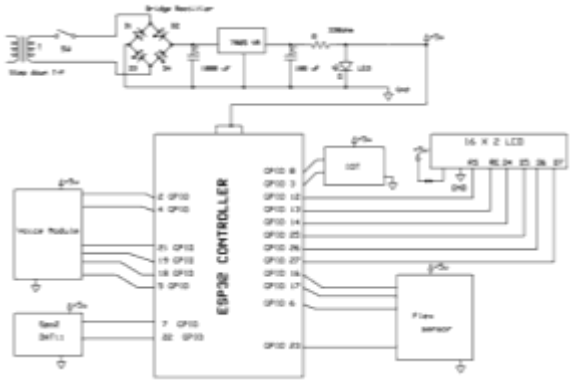


Figure 3. Circuit Diagram of Facial Lock Drive 2.0.

4. Results and Discussion



Figure 4. Hardware Implementation of Facial Lock Drive 2.0

Figure 4 shows the hardware prototype of the Facial Lock Drive 2.0 system built using the ESP32 microcontroller. The system integrates modules such as ESP32, ESP-CAM, LCD display, buzzer, fingerprint sensor, and DC motor driver to implement biometric-based smart door locking and access control.

Figure 5 shows the facial recognition output captured through the ESP-CAM module and displayed on a computer interface. The system detects and analyzes the user's face in real time, enabling secure authentication before granting access to the door locking mechanism.

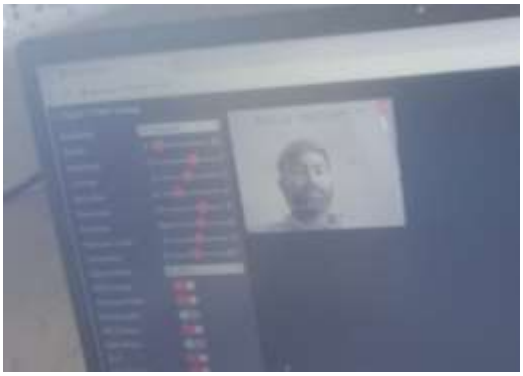


Figure 5. Facial Recognition Monitoring Interface

5. Conclusion

The proposed Facial Lock Drive 2.0 system presents a highly secure and intelligent access control solution by integrating multi-factor biometric authentication, automation, and IoT connectivity. By combining facial recognition using ESP32-CAM with fingerprint verification, the system ensures accurate and reliable user authentication, significantly reducing the risks associated with traditional key or password-based systems. The automated door locking mechanism using a DC motor enhances convenience, while the LCD display provides real-time feedback to users. Unauthorized access attempts are immediately detected and alerted through a buzzer, improving security responsiveness. Additionally, IoT integration enables remote monitoring, access log management, and real-time notifications, allowing better control and oversight of entry activities. This system effectively overcomes the limitations of conventional security methods by offering a

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

robust, scalable, and smart solution, making it suitable for applications in homes, offices, laboratories, and other restricted environments.

References

[1] Gururaj, H.L.; Soundarya, B.C.; Priya, S.; Shreyas, J.; Flammini, F. A Comprehensive Review of Face Recognition Techniques, Trends, and Challenges. IEEE Access 2024, 12, 107903–107926.

[2] Explainable AI Framework for Policy-Compliant Anomaly Detection in Data Pipelines. (2025). Inaternational Journal of Communication Networks and Information Security, 16(4). https://doi.org/10.48047/ijcnis.16.4.2111

[3] Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.

[4] Prodduturi, S. M. K. To Secure Your Paper as Per UGC Guidelines We Are Providing A ElectronicBar code.

[5] Singh, A.D.; Jangra, B.S.; Singh, R. Face Recognition Door Lock System Using Raspberry Pi. Int. J. Res. Appl. Sci. Eng. Technol. (IJRASET) 2022, 10, 1733–1735.

[6] Padhan, D.G.; Divya, M.; Varma, S.N.; Manasa, S.; C, V.; Pakkiraiah, B. Home Security System Based On Facial Recognition. In Proceedings of the Department of Electrical and Electronics Engineering, Bhubaneswar, India, 9–12 August 2023.

[7] Reddy, S. K. R. (2025). Tailoring Loyalty Rewards Systems across Industries: Cloud vs On-Prem Solutions. International Journal of All Research Education and Scientific Methods (IJARESM).

[8] Poojari, R. (2025). A Comparative Analysis of Fine-Tuning Versus Retrieval-Augmented Approaches for Enhancing Healthcare-Centric Large Language Models.

[9] George, A.; Ecabert, C.; Shahreza, H.O.; Kotwal, K.; Marcel, S. EdgeFace: Efficient Face Recognition Model for Edge Devices. IEEE Trans. Biom. Behav. Identity Sci. 2024, 6, 158–168.

[10] Patyrykin, K. (2025). CANCEL CULTURE PROBLEM. Lex Localis: Journal of Local Self-Government, 23.

[11] Purmani, S. S. R. (2025). Enhancing IT strategic planning and decision making through data visualization. International Journal of Enhanced Research in Management & Computer Applications, 14(4), 75–81

[12] Rana, M.S.; Fattah, S.A.; Uddin, S.; Rashid, R.U.; Noman, R.M.; Quasem, F.B. Real-Time Deep Learning Based Face Recognition System Using Raspberry Pi. In Proceedings of the 26th International Conference on Computer and Information Technology (ICCIT), Cox's Bazar, Bangladesh, 13–15 December 2023; pp. 1–6.

[13] Madhavan, S.; Kumar, N. Incremental Methods in Face Recognition: A Survey. Artif. Intell. Rev. 2021, 54, 253–303.

[14] Vasagam, M., Kumar, A., & Garg, A. (2026). Learning Execution Plan Embeddings for Multi-Dimensional Query Resource Prediction. IEEE Access.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

[15] Kalae, U. K. (2025). Optimizing cost-effective cloud data pipeline orchestration across multiple cloud providers. Journal of Information Systems Engineering and Management, 10(63s), e726–e741.

[16] Prasad, H.H. IoT-Based Door Access Control Using Face Recognition. Int. Res. J. Eng. Technol. (IRJET) 2019, 6, 1222–1225.

[17] Kumara, S. (2026, February). A Lightweight Deep Learning Based Classification Models for Non-Human Identity Threat Detection. In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-6). IEEE.

[18] Shi, Y.; Zhang, H.; Guo, W.; Zhou, M.; Li, S.; Li, J.; Ding, Y. LighterFace Model for Community Face Detection and Recognition. Information 2024, 15, 215.

[19] Chamikara, M.A.P.; Bertok, P.; Khalil, I.; Liu, D.; Camtepe, S. Privacy Preserving Face Recognition Utilizing Differential Privacy. Comput. Secur. 2020, 97, 101951.