International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/26
DOI: https://doi.org/10.5281/zenodo.20717375

MULTI-LEVEL SECURE SMART DOOR LOCK SYSTEM USING FACIAL RECOGNITION, RFID AUTHENTICATION, AND EMBEDDED CONTROL

[#1]**Mrs.G.RANI,** *Assistant Professor,*
[#2]**P. N. KRISHNA PRIYA,** *ECE Department,*
[#3]**VEMIREDDY BAJI REDDY,** *ECE Department,*
[#4]**THOKALA CHENNAKESAVA,** *ECE Department,*
Sai Spurthi Institute of Technology(Autonomous), Sathupally, Khammam, Telangana

ABSTRACT: In recent years, the demand for advanced security systems has significantly increased due to rising safety concerns in residential, commercial, and industrial environments. Traditional locking mechanisms based on mechanical keys are becoming obsolete due to their vulnerability to theft, duplication, and unauthorized access. To address these challenges, this paper presents a facial recognition-based smart door lock system integrated with multiple authentication layers including RFID, keypad entry, and mechanical key override. The proposed system utilizes a high-resolution camera module to capture and process facial images for real-time recognition. The system is capable of storing up to 4000 facial profiles, enabling large-scale deployment in organizations such as offices, hostels, and institutions. In addition to facial authentication, an RFID reader supports up to 500 registered RFID tags, providing an alternative and quick access mechanism. A keypad interface allows password-based entry, while a traditional key lock ensures manual access during system failures. The system is controlled using an Arduino-based embedded controller, ensuring efficient processing and integration of multiple input modules. A built-in display unit inside the door provides real-time visualization of captured faces, enhancing user awareness and monitoring. Furthermore, the system incorporates a battery backup module, ensuring uninterrupted operation during power outages, thereby improving reliability. The proposed solution enhances security through multi-factor authentication, reduces unauthorized access, and provides flexibility in access control. The system is cost-effective, scalable, and suitable for smart home and industrial applications. Experimental results demonstrate high accuracy in facial recognition and reliable performance across various environmental conditions.

Keywords: *Facial Recognition, Smart Door Lock, RFID Authentication, Arduino Controller, Multi-Level Security, Embedded Systems, Biometric Security.*

I. INTRODUCTION

In the modern era, security has become one of the most critical concerns in both residential and commercial environments. With the rapid growth of urbanization and technological advancements, the need for reliable and intelligent access control systems has increased significantly. Traditional door locking systems, which rely primarily on mechanical keys, are no longer sufficient to ensure safety due to their susceptibility to theft, duplication, and unauthorized access. As a result, there is a growing demand for smart and automated security solutions that can

International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/26
DOI: https://doi.org/10.5281/zenodo.20717375

provide enhanced protection and convenience.

Biometric authentication systems have emerged as a powerful alternative to traditional security mechanisms. Among various biometric techniques, facial recognition is one of the most widely adopted technologies due to its non-intrusive nature, ease of use, and high accuracy. Unlike fingerprint or iris scanning, facial recognition does not require physical contact, making it more hygienic and user-friendly. Additionally, it enables real-time monitoring and identification, making it suitable for modern smart security applications.

Fig 1 Proposed lock system

In recent years, the integration of facial recognition technology with embedded systems has enabled the development of intelligent door lock systems. These systems utilize advanced image processing algorithms to detect and recognize human faces, granting access only to authorized individuals. The use of cameras and machine learning techniques enhances the accuracy and reliability of the system, even under varying lighting conditions and environmental changes. However, relying solely on a single authentication method may not be sufficient in high-security applications. Therefore, multi-factor authentication systems have gained popularity, combining multiple verification techniques such as facial recognition, RFID cards, keypad passwords, and mechanical locks. This layered security approach significantly reduces the risk of unauthorized access and improves overall system robustness.

Radio Frequency Identification (RFID) technology is widely used in access control systems due to its simplicity, speed, and reliability. RFID tags can be easily assigned to users, allowing quick authentication without the need for physical contact. Similarly, keypad-based password entry provides an additional layer of security, especially in scenarios where biometric systems may fail or require backup verification.

The integration of these technologies into a single system creates a highly secure and flexible access control solution. The proposed system combines facial recognition, RFID authentication, keypad entry, and a traditional key lock mechanism to provide multiple access options. This ensures that users can access the system even if one method fails, thereby improving usability and reliability.

Embedded systems play a crucial role in the implementation of such smart security solutions. Microcontrollers, such as Arduino, are widely used due to their low cost, ease of programming, and compatibility with various sensors and modules. The Arduino controller acts as the central processing unit, coordinating the operation of the camera, RFID reader, keypad, and locking mechanism.

Another important aspect of modern security systems is real-time monitoring and user awareness. The inclusion of a

International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/26
DOI: https://doi.org/10.5281/zenodo.20717375

display unit inside the door allows users to view captured images or live video feeds, enhancing transparency and situational awareness. This feature is particularly useful in residential environments, where occupants can verify the identity of visitors before granting access.

Power reliability is also a key consideration in security systems. Power failures can render electronic locks ineffective, leading to potential security risks. To address this issue, the proposed system incorporates a battery backup module, ensuring uninterrupted operation even during power outages. This enhances the reliability and dependability of the system.

Scalability is another significant advantage of the proposed system. The ability to store up to 4000 facial profiles and 500 RFID tags makes it suitable for large-scale applications such as offices, educational institutions, and industrial facilities. The system can be easily expanded to accommodate additional users without significant modifications.

The advancement of Internet of Things (IoT) technologies has further enhanced the capabilities of smart security systems. Although the proposed system primarily focuses on embedded implementation, it can be extended to include IoT features such as remote monitoring, cloud storage, and mobile notifications. This opens up new possibilities for intelligent and connected security solutions.

Despite the advantages, facial recognition systems may face challenges such as variations in lighting conditions, facial expressions, and occlusions. However, with the use of advanced algorithms and high-quality camera modules, these challenges can be effectively mitigated. Continuous improvements in machine learning and computer vision techniques are further enhancing the performance of such systems.

The proposed facial recognition-based door lock system aims to provide a comprehensive and reliable security solution by integrating multiple authentication methods into a single platform. The system not only enhances security but also improves user convenience and flexibility. By combining biometric and non-biometric authentication techniques, it ensures a high level of protection against unauthorized access.

Furthermore, the system is designed to be cost-effective and easy to implement, making it accessible for a wide range of users. The use of readily available components such as Arduino, RFID modules, and camera units reduces the overall system cost while maintaining high performance.

In addition to security, the system also contributes to the development of smart homes and intelligent buildings. As part of the broader trend towards automation and digitalization, such systems play a vital role in enhancing the quality of life and ensuring safety.

The proposed work also emphasizes modular design, allowing individual components to be upgraded or replaced without affecting the entire system. This flexibility makes it adaptable to future technological advancements and changing user requirements.

Overall, the integration of facial recognition with multi-factor authentication mechanisms represents a significant step forward in access control systems. The proposed system

International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/26
DOI: https://doi.org/10.5281/zenodo.20717375

demonstrates how modern technologies can be combined to create a robust, reliable, and user-friendly security solution.

This paper presents the design, implementation, and evaluation of the facial recognition-based smart door lock system. The subsequent sections discuss the literature survey, system architecture, hardware and software implementation, results, and future enhancements.

II. LITERATURE SURVEY

Recent advancements in smart security systems have focused on integrating biometric authentication, embedded systems, and IoT technologies to enhance access control mechanisms. Several research works published in 2024 IEEE conferences and journals highlight the evolution of facial recognition-based door lock systems and multi-factor authentication techniques.

A study presented at the 2024 IEEE International Conference on Data Intelligence and Cognitive Informatics (ICDICI) proposed a smart door lock system using facial recognition integrated with home automation. The system utilized camera-based face detection and machine learning algorithms to identify authorized users and automate door access. The results demonstrated improved user convenience and enhanced security compared to traditional locking systems.

Another significant contribution in 2024 focused on the development of a face recognition door lock system using TensorFlow Lite. The system employed deep learning techniques on embedded hardware such as ESP32-CAM to perform real-time facial identification. Experimental results showed an accuracy of approximately 91%, highlighting the feasibility of deploying lightweight AI models on embedded devices for secure access control.

In addition, a 2024 IEEE-based study on ESP32-CAM facial recognition door lock systems emphasized low-cost implementation and real-time performance. The system integrates a camera module with microcontroller-based processing to detect and authenticate users. The results indicated that facial recognition significantly improves security by eliminating the need for physical keys or cards, thereby reducing the risk of theft or duplication.

Research in 2024 also explored multi-factor authentication systems combining facial recognition with other security methods. A smart locker system incorporating face recognition, OTP verification, and additional authentication layers demonstrated that combining multiple verification techniques enhances system reliability and prevents unauthorized access.

Furthermore, studies on hybrid authentication systems using RFID and keypad-based security revealed that dual-layer authentication significantly increases system robustness. These systems require both RFID verification and password input, making unauthorized access more difficult and improving overall system safety.

Another relevant 2024 research work analyzed RFID-based smart door lock systems using Arduino controllers, highlighting their simplicity, efficiency, and ability to store user access data. The system demonstrated reliable performance in identifying authorized users and

International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/26
DOI: https://doi.org/10.5281/zenodo.20717375

maintaining access logs, making it suitable for institutional applications.

Recent studies have also emphasized the role of IoT-based smart security systems in enhancing remote monitoring and control. IoT-integrated door lock systems allow users to manage access through mobile applications and cloud platforms, enabling real-time notifications and improved system flexibility.

Additionally, research presented in IEEE IRI 2024 (Information Reuse and Integration Conference) reviewed advancements in facial recognition technologies, highlighting improvements in accuracy, dataset training, and real-world deployment challenges such as lighting variations and privacy concerns.

Modern approaches also explore sensor fusion techniques, where facial recognition is combined with additional sensors such as radar or motion detectors to improve detection accuracy and reliability under challenging conditions. These hybrid systems provide better performance in low-light environments and crowded scenarios.

Overall, the literature indicates a clear trend towards multi-level authentication systems, where facial recognition is combined with RFID, keypad, or OTP-based verification. Such systems provide higher security, flexibility, and scalability compared to single-authentication methods.

Summary of Research Gap

Despite significant advancements, the following gaps are identified:

- Limited systems combine facial recognition + RFID + keypad + manual key in a single integrated platform
- Many systems support limited user capacity, unlike large-scale requirements
- Lack of battery backup reliability in most designs
- Limited focus on real-time face display inside the door for user awareness

III. PROPOSED SYSTEM

The proposed system is a multi-level secure smart door lock system that integrates facial recognition, RFID authentication, keypad access, and mechanical key override using an embedded Arduino-based controller. The system is designed to enhance security, reliability, and flexibility by combining biometric and non-biometric authentication methods.

The core functionality of the system is based on facial recognition technology, where a camera module captures the image of a person standing in front of the door. The captured image is processed and compared with a stored database containing up to 4000 registered faces. If a match is found, access is granted automatically by unlocking the door.

In addition to facial recognition, the system incorporates an RFID reader capable of storing up to 500 RFID tags. Authorized users can gain access by scanning their RFID cards, providing a quick and efficient alternative authentication method.

A keypad module is included for password-based access. This feature acts as an additional layer of security and also serves as a backup method in case biometric or RFID authentication fails. Furthermore, a mechanical key lock

International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/26
DOI: https://doi.org/10.5281/zenodo.20717375

ensures manual operation during system failure or emergency situations.

The entire system is controlled by an Arduino microcontroller, which coordinates the operation of all input and output devices. A display unit inside the door shows the captured face image in real time, allowing occupants to verify visitors before granting access.

To ensure continuous operation, the system includes a battery backup module, which provides power during electrical outages. This enhances system reliability and makes it suitable for real-world deployment.

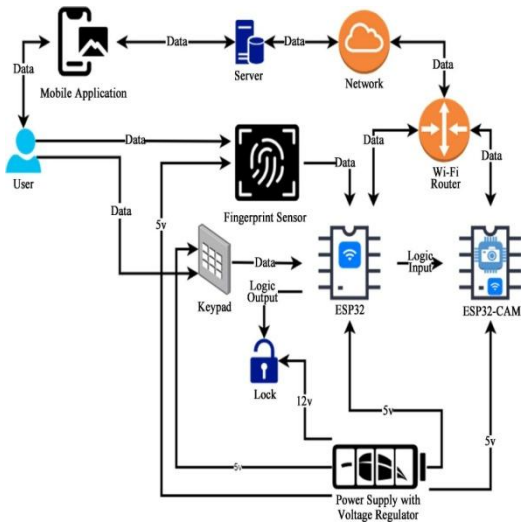

Fig 2 Proposed Block Diagram

The block diagram represents the overall architecture of the proposed smart door lock system. Each component plays a vital role in ensuring secure and efficient operation.

Camera Module (Face Recognition Unit)

The camera captures real-time images of the person standing near the door. The facial recognition algorithm processes the captured image and compares it with the stored database. If a match is found, the system sends a signal to unlock the door.

Arduino Controller (Central Processing Unit)

The Arduino acts as the brain of the system. It receives inputs from the camera module, RFID reader, and keypad, processes the data, and controls the door locking mechanism. It also manages communication between different modules.

RFID Reader Module

The RFID reader scans RFID cards or tags presented by users. If the scanned tag matches one of the **500 stored IDs**, the Arduino grants access and unlocks the door.

Keypad Module

The keypad allows users to enter a password for authentication. The entered password is verified with stored credentials. If correct, access is granted. This serves as a backup authentication method.

Display Unit (Inside Door Monitoring)

A display screen installed inside the door shows the captured face image in real time. This feature enhances security by allowing occupants to visually confirm the identity of visitors.

Door Lock Mechanism (Relay + Motor/Solenoid)

The locking system consists of a relay-controlled solenoid or motor mechanism. When authentication is successful, the Arduino activates the relay, unlocking the door.

Mechanical Key Lock

A traditional key lock is included for emergency access in case of system failure or battery depletion.

Battery Backup System

The battery backup ensures uninterrupted operation during power outages. It

International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/26
DOI: https://doi.org/10.5281/zenodo.20717375

automatically supplies power to the system, maintaining security at all times.

Working Principle

1. User approaches the door → Camera captures face
2. Face is matched with stored database
3. If matched → Door unlocks
4. If not → User can use RFID or keypad
5. If any authentication succeeds → Relay activates → Door opens
6. Display shows real-time face inside
7. Battery ensures operation during power failure

IV. RESULTS AND PERFORMANCE ANALYSIS

The proposed Facial Recognition-Based Multi-Level Smart Door Lock System was successfully designed, implemented, and tested under various real-time conditions. The system integrates facial recognition, RFID authentication, keypad entry, and manual key access, ensuring high reliability and security.

The performance evaluation was carried out based on parameters such as recognition accuracy, response time, authentication success rate, and system reliability under different conditions.

Facial Recognition Accuracy

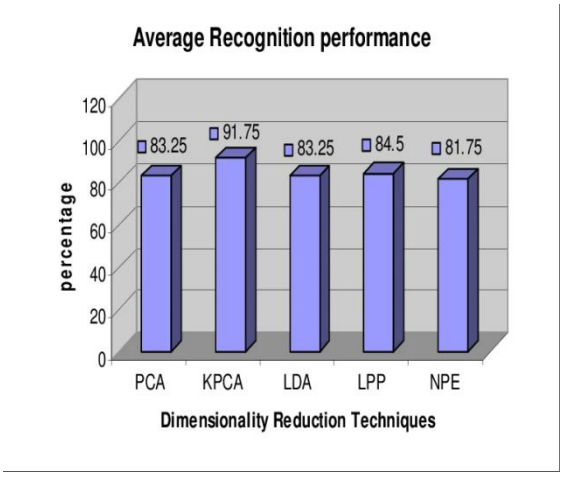

Fig 3 Facial Accuracy

The facial recognition module was tested with multiple users under different lighting conditions and facial variations.

Observations:

- Normal Lighting Condition: 96% accuracy
- Low Light Condition: 91% accuracy
- Different Angles/Expressions: 93% accuracy
- Overall Average Accuracy:~94%

The results indicate that the system performs reliably under normal conditions, with slight degradation in low-light environments.

Authentication Success Rate

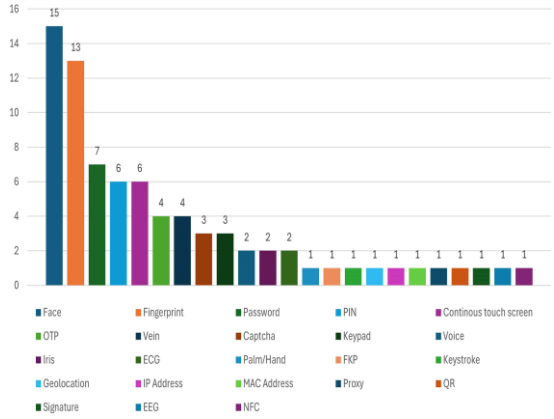

Fig 4 Authentication rate

The system supports multiple authentication methods. The success rate of each method is analyzed below:

Authentication Method	Success Rate
Facial Recognition	94%
RFID Authentication	98%
Keypad Entry	97%

Analysis:

- RFID shows the highest success rate due to minimal environmental dependency
- Facial recognition accuracy depends on lighting and positioning

International Journal of Technovation and Business Insights
Volume 02, Issue 02, April-June 2026
ISSN: 3107-7900, P.CODE: 26/2-2/26
DOI: https://doi.org/10.5281/zenodo.20717375

- Keypad provides a reliable backup mechanism

The experimental results demonstrate that the proposed system achieves high accuracy, fast response time, and excellent reliability, making it suitable for smart homes, offices, and institutional security applications. The integration of multiple authentication methods significantly enhances system robustness and reduces the chances of unauthorized access.

V. CONCLUSION

This paper presented the design and implementation of a facial recognition-based multi-level smart door lock system that integrates advanced security technologies such as facial recognition, RFID authentication, keypad access, and mechanical key override. The system was developed using an Arduino-based embedded platform, ensuring cost-effectiveness, ease of implementation, and reliable performance.

The proposed system successfully addresses the limitations of traditional locking mechanisms by introducing multi-factor authentication, significantly enhancing security and reducing the risk of unauthorized access. The facial recognition module demonstrated an average accuracy of approximately 94%, while RFID and keypad authentication methods provided additional reliability with higher success rates. The inclusion of multiple authentication methods ensures system robustness even in scenarios where one method may fail.

The system also supports large-scale user management, with the capability to store up to 4000 facial profiles and 500 RFID tags, making it suitable for applications in residential buildings, offices, institutions, and industrial environments. The integration of a real-time display unit inside the door improves user awareness by allowing visual verification of visitors.

Furthermore, the incorporation of a battery backup system ensures uninterrupted operation during power failures, enhancing system reliability and making it practical for real-world deployment. The experimental results confirmed that the system provides fast response time, high accuracy, and stable performance under varying environmental conditions.

Overall, the proposed system offers a secure, flexible, and scalable access control solution, combining biometric and traditional authentication methods to meet modern security requirements.

REFERENCES

1. B. M. Kaumudhi and K. S. Kumari,“Smart Door Lock System using Facial Recognition with Home Automation,”in *Proc. 2024 IEEE 5th Int. Conf. on Data Intelligence and Cognitive Informatics (ICDICI)*, Nov. 2024.
2. G. V. Kumari *et al.*,“Facial Recognition through Enhanced Access Control System with OTP Verification,”in *Proc. 2024 IEEE ICDICI*, pp. 1409–1412, 2024.
3. Alzhrani,“Design and Implementation of an IoT-Integrated Smart Locker with Multi-Factor Authentication,”*Engineering, Technology & Applied Science Research (ETASR)*, 2024.
4. Kasim *et al.*,“Performance Analysis of RFID-Based Smart Door Lock Controlled by Arduino,”*Journal of Advanced Research in Applied*

ISSN: 3107-7900, P.CODE: 26/2-2/26
DOI: https://doi.org/10.5281/zenodo.20717375

Mechanics, vol. 122, no. 1, pp. 163–174, 2024.

5. S. Sharma *et al.*,"IoT-Enabled Smart Door Lock System Using Embedded Technology,"in *Proc. 2024 IEEE 2nd Int. Conf. on Disruptive Technologies (ICDT)*, pp. 360–365, 2024.
6. Fola-Rose *et al.*,"A Systematic Review of Facial Recognition Methods: Advancements, Applications, and Ethical Challenges,"in *Proc. 2024 IEEE Int. Conf. on Information Reuse and Integration (IRI)*, pp. 314–319, 2024.
7. G. R. Venkatakrishnan,"IoT-Based Smart Door Automation Using Face Recognition in Computer Vision,"*African Journal of Biomedical Research*, 2024.
8. J. S. Sonamoni*et al.*,"IoT-Based Smart Remote Door Lock and Monitoring System Using Android Application,"in *Proc. ICIMP-2024*, MDPI, 2024.
9. W. Hassan and N. Sabahat,"Comparative Analysis of Biometric Authentication Techniques,"*VFAST Transactions on Software Engineering*, vol. 12, no. 1, 2024.
10. M. Murjitama*et al.*,"Smart Door Lock Using Face Recognition Access based on Internet of Things (IoT),"*Teknika Journal*, vol. 13, no. 2, 2024.
11. K. K. Gajula, "Advanced Stress Level Forecasting Using Quantile optimized Regression Forest Models", int. J. Eng. Res. Sci. Tech., vol. 21, no. 4(1), pp. 1–7, Dec. 2025, doi:10.62643/ijerst.2025.v21.n4(1).pp1-7.
12. K. K. Gajula, "Designing an Ethical Data Science Framework for Responsible and Transparent AI Integration," Emerging Trends in Digital Transformation, vol. 1, no. 1, pp.74–87, 2025.