Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

An Intelligent IoT-Based Smart Door Lock System with Remote Access and Status Display

Anita Patil, Bibi Atiya, K Sai Sri, Rashmi G N,Sudha C Parimala
Department of Computer Science and Engineering (Artificial Intelligence)
Ballari Institute of Technology and Management
Ballari, India

***Abstract* - Traditional mechanical door lock systems provide limited security and lack intelligent features such as automation, remote monitoring, and user authentication. With the increasing demand for smart home security solutions, there is a need for door locking systems that offer enhanced safety, convenience, and real-time interaction. This paper presents an intelligent Internet of Things based smart door lock system with remote access and status display, designed using the ESP32 microcontroller. The proposed system integrates face recognition for secure and contactless authentication, along with an OLED display to provide real-time access status and system messages. Facial images are captured using a camera and processed for detection and recognition using deep learning techniques to ensure reliable user authentication. Upon successful verification, the door lock mechanism is activated automatically, while unauthorized access attempts trigger alert mechanisms and warning messages. In addition, a web-based interface enables remote locking and unlocking of the door, improving accessibility and control. Experimental results demonstrate that the system operates effectively in indoor environments and offers improved security and user convenience compared to conventional locking mechanisms. The proposed solution is suitable for smart homes and office environments, with scope for future enhancements to improve scalability and real-world deployment.**

Keywords - Internet of Things, Smart Door Lock, ESP32, Face Recognition, Remote Access, OLED Display, Home Security.

I. INTRODUCTION

Traditional mechanical door locking systems rely on physical keys and manual control, offering limited security and flexibility. Such systems are prone to key loss, duplication, and unauthorized access, making them insufficient for modern residential and commercial security requirements. As safety concerns increase, there is a growing demand for intelligent access control systems that can provide enhanced protection, automation, and user awareness.

The rapid development of the Internet of Things (IoT) has enabled interconnected devices capable of real-time monitoring and remote control. When combined with artificial intelligence techniques, IoT-based security systems can offer intelligent decision-making and reliable user authentication. Among various biometric methods, facial recognition has gained popularity due to its contactless nature, ease of use, and improved accuracy in identifying authorized users.

Despite numerous advancements, many existing smart door lock systems suffer from limitations such as the absence of robust authentication mechanisms, restricted remote accessibility, or lack of real-time user feedback. Additionally, several systems fail to provide intuitive visual indications regarding access status, reducing usability and situational awareness for users.

To overcome these challenges, this paper presents an intelligent IoT-based smart door lock system with remote access and status display. The proposed system integrates biometric authentication with automated locking control and real-time visual feedback to enhance security and convenience. Designed for smart home and office environments, the system demonstrates reliable performance in controlled indoor conditions and highlights the potential for future scalability and real-world deployment.

II. LITERATURE SURVEY

In recent years, Internet of Things (IoT)–based smart door lock systems have gained significant attention due to their ability to enhance security, automation, and remote accessibility. Alsayaydeh *et al.* presented a biometric IoT-based smart lock system incorporating fingerprint authentication, real-time monitoring, and alert mechanisms to improve access control security [1]. Although the system demonstrated reliable performance and low false acceptance rates, it primarily relied on fingerprint authentication and required continuous network connectivity, which could affect usability in unstable network environments.

With the growing demand for advanced authentication methods, Kumar *et al.* proposed a smart biometric door lock system integrating facial recognition and fingerprint authentication for multi-factor security [2]. The system improved protection against unauthorized access and supported mobile-based remote monitoring. However, the inclusion of multiple biometric modules increased system complexity and cost, limiting its suitability for low-cost residential applications.

Sonamoni *et al.* developed an IoT-based smart remote door lock and monitoring system using an ESP32-CAM and an Android application [3]. The system enabled homeowners to remotely view visitors and control door access in real time, along with alert mechanisms for intrusion attempts. Despite its improved convenience, the system depended heavily on user intervention and lacked intelligent authentication mechanisms for automated access decisions.

Premanand *et al.* introduced an IoT-enabled door lock system utilizing cognitive abilities to improve adaptive access control [4]. The proposed approach emphasized intelligent decision-making and automation to enhance security. However,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

the system required higher computational resources and complex implementation, making it less feasible for cost-sensitive smart home deployments.

Several studies have focused on ESP32-based IoT smart door lock systems to achieve remote access and monitoring. Kondamu *et al.* designed an IoT-based smart door lock system using ESP32-CAM and mobile application support [5]. While the system provided remote control and improved accessibility, it did not include real-time local feedback mechanisms such as visual status displays for immediate user awareness.

IEEE researchers proposed multiple IoT-based smart door lock solutions incorporating biometric authentication and cloud connectivity to replace traditional mechanical locks [6], [7]. These systems improved security through authorized access control and remote monitoring. However, many of them were sensitive to environmental conditions such as lighting and network latency and lacked integrated status display units at the access point.

Earlier works explored Wi-Fi–enabled door lock systems using ESP32-CAM and mobile applications for remote access control. Prathapagiri and Eethamakula proposed a Wi-Fi door lock system that allowed users to unlock doors remotely after verifying visitor images [8]. Although the system enhanced convenience, it relied on manual user decisions and did not support intelligent or automated authentication.

Foundational research in biometric door access systems highlighted the effectiveness of facial recognition and fingerprint-based authentication for enhancing security [9], [10]. These systems reduced dependency on physical keys but faced challenges related to accuracy, scalability, and user privacy. Additional IoT-based locker and security systems further demonstrated the feasibility of biometric authentication but introduced concerns related to network dependency and system reliability [11], [12].

From the reviewed literature, it is evident that existing smart door lock systems have addressed various aspects such as remote access, biometric authentication, and IoT connectivity. However, limitations including system complexity, lack of real-time status display, dependence on continuous internet connectivity, and restricted adaptability remain. These research gaps motivate the development of an intelligent IoT-based smart door lock system with integrated remote access and real-time status display, as proposed in this work.

III. Comparative Analysis of Existing and Proposed System

To highlight the limitations of existing approaches and justify the need for the proposed system, a comparative analysis between existing smart door lock systems and the proposed system is presented in Table I. The comparison is based on key features such as authentication method, remote accessibility, user feedback mechanisms, system complexity, and scalability.

TABLE I. Comparison of Existing and Proposed Smart Door Lock System

Feature	***Existing Systems***	***Proposed System***
Locking Mechanism	Mechanical or semi-automated	Fully automated smart locking
Authentication	PIN, RFID, fingerprint, or manual	Face recognition
Remote Access	Limited or application-dependent	Web-based remote access
Status Display	Not available	Integrated OLED display
Unauthorized Access Alert	Limited or absent	Buzzer alert with warning display
User Interaction	Manual or semi-automatic	Intelligent and automated
System Complexity	High due to multiple modules	Compact and integrated
Cost Effectiveness	Higher for advanced systems	Cost-effective
Scalability	Limited	High

IV. PROPOSED SYSTEM

A. System Overview

The proposed system is an intelligent IoT-based smart door access solution designed to provide secure, automated, and contactless entry control. The system follows a layered architecture consisting of input, processing, and output stages to ensure reliable real-time operation and enhanced security.

In the input stage, facial images are captured using a camera module, along with user commands received through a web-based interface. These inputs are forwarded to the processing layer, where artificial intelligence–based face recognition is performed. The processing unit analyzes the captured facial data and determines whether the user is authorized to access the system.

Based on the authentication result, appropriate control signals are transmitted to the ESP32 microcontroller, which acts as the central control unit. For authorized users, the microcontroller activates the door locking mechanism and updates the system status on the OLED display. In the case of unauthorized access attempts, the system immediately triggers an audible alert and displays a warning message. This integrated design ensures secure access control while providing real-time user feedback and remote monitoring capability.

B. System Architecture

The system architecture illustrated in **Fig.1.** the interaction between the software modules and hardware components involved in the smart door access system. The architecture follows a layered design, where facial data acquisition, processing, decision-making, and actuation are clearly separated to ensure modularity and reliability.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

The input layer consists of a camera module used to capture facial images and a web interface for receiving user commands. The processing layer performs face detection and recognition using an artificial intelligence–based model. Authentication results are forwarded to the control layer, where the ESP32 microcontroller executes access decisions. The output layer includes the servo motor for door control, an OLED display for status updates, and a buzzer for alert generation. Communication between software and hardware components is achieved through serial communication and secure network tunneling.

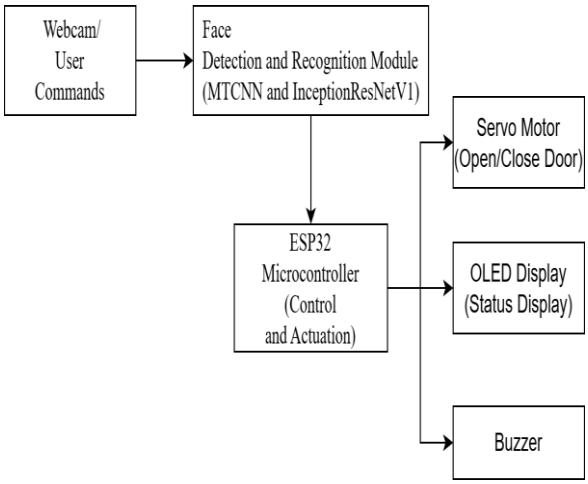

Fig. 1. System Architecture

C. *Proposed Methodology*

The objective of the proposed methodology is to implement an intelligent access control mechanism using real-time facial recognition integrated with IoT-based hardware control.

1) Data Acquisition and Preprocessing

Facial images of authorized users are captured using a camera under varying lighting conditions and facial orientations to improve recognition robustness. The captured images undergo preprocessing steps including facial region detection, normalization of pixel values, and face alignment to ensure consistent input to the recognition model. These steps enhance recognition accuracy and reduce false detections.

2) Face Recognition Model

A deep learning–based facial recognition model is employed to generate unique facial embeddings for each authorized user. A pre-trained model is utilized to reduce computational complexity and improve execution speed. During system operation, real-time facial embeddings are generated and compared with the stored embeddings to determine user authenticity.

3) Hardware Integration

The ESP32 microcontroller is responsible for executing lock control operations and managing peripheral devices such as the servo motor, OLED display, and buzzer. The hardware components are interfaced using appropriate GPIO connections, and the control logic is implemented using embedded firmware.

4) Communication Between Software and Hardware

Efficient communication between the facial recognition module, web interface, and microcontroller is achieved through serial communication and secure network tunneling. Authentication decisions generated by the processing module are transmitted to the ESP32, enabling rapid execution of lock or unlock actions.

5) Real-Time Authentication Process

The system continuously monitors the camera feed for facial presence. When a face is detected, it is analyzed and compared with stored authorized profiles. If a match is found, the door is unlocked and a confirmation message is displayed. In the absence of a valid match, the system triggers an audible alert and displays an access denial message.

6) Remote Access and Control

Remote locking and unlocking functionality is provided through a web-based interface. User commands are securely transmitted to the system, allowing authorized users to control the door remotely without the need for a static IP address.

7) Testing and Validation

The system was tested under different lighting conditions, facial angles, distances, and unauthorized access scenarios. System latency, recognition response time, and remote command execution were evaluated to ensure reliable real-time performance.

V. HARDWARE IMPLEMENTATION

The hardware implementation of the proposed smart door access system is centered around the ESP32 microcontroller, which functions as the primary control and communication unit. Multiple peripheral components are integrated to enable automated door operation, real-time status indication, and alert generation. All hardware modules are interconnected using GPIO pins, ensuring synchronized operation and reliable signal transmission.

The hardware implementation of the proposed smart door access system is centered around the ESP32 microcontroller, which functions as the primary control and communication unit. Multiple peripheral components are integrated to enable automated door operation, real-time status indication, and alert generation. All hardware modules are interconnected using GPIO pins, ensuring synchronized operation and reliable signal transmission.

The complete hardware setup was assembled using jumper wires, allowing flexibility during development and simplifying testing and modifications. Fig. 2 gives the initial hardware setup and the hardware components used are listed in Table II.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

TABLE II. HARDWARE COMPONENTS USED

Component	*Role*
ESP32 Microcontroller	*Central control unit for lock control and communication*
SG90 Servo Motor	*Controls the mechanical locking and unlocking mechanism*
0.96" OLED Display	*Displays real-time system status messages*
Buzzer	Generates audible alerts during unauthorized access

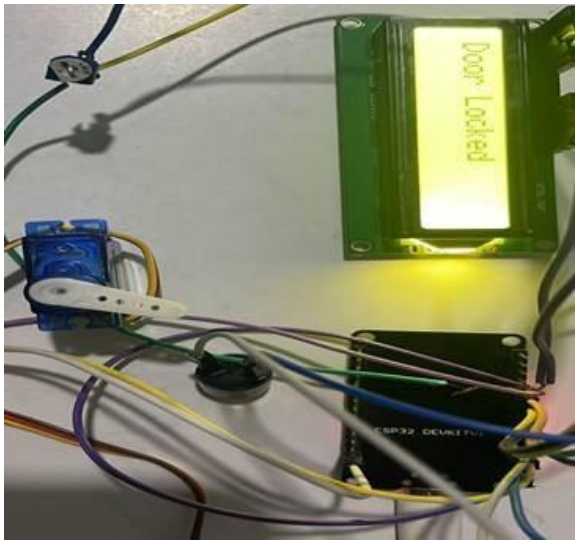

Fig. 2. Initial Hardware Setup

VI. SOFTWARE IMPLEMENTATION

The software implementation of the proposed system consists of two major modules: the facial recognition module and the microcontroller control module. The facial recognition module is developed using Python and employs deep learning techniques for accurate user authentication. The ESP32 microcontroller is programmed to execute control actions based on authentication results received from the software module.

The facial recognition pipeline uses the MTCNN algorithm for face detection, followed by the InceptionResNetV1 model for facial feature extraction and recognition. Facial embeddings of authorized users are generated during enrollment and stored locally for comparison during real-time operation. When a face is detected, its embedding is compared against the stored database to determine access validity.

Upon successful authentication, control signals are transmitted to the ESP32 through serial communication, triggering door unlocking and updating the OLED display. In case of unauthorized access, the ESP32 activates the buzzer and displays a warning message. A Flask-based web interface enables remote door locking and unlocking, while secure tunneling is achieved using ngrok for external access.

VII. RESULTS AND DISCUSSION

A. Experimental Setup

The proposed smart door access system was implemented using an ESP32 microcontroller integrated with a servo motor, OLED display, and buzzer. A USB webcam was used to capture facial images for real-time authentication. The facial recognition module was executed on a local system using Python, while control commands were transmitted to the ESP32 through serial communication. A Flask-based web interface enabled remote lock and unlock operations.

The system was tested under different scenarios, including authorized access, unauthorized access, and remote control operation, to evaluate its functional reliability and responsiveness.

B. Face Recognition and Authentication Results

The facial recognition module successfully detected and authenticated registered users using the MTCNN algorithm for face detection and the InceptionResNetV1 model for feature extraction. When an authorized user was identified, the system generated a positive authentication result and initiated the door unlocking process.

For unregistered or unknown users, the system accurately identified the access attempt as unauthorized. In such cases, the door remained locked, and appropriate alert actions were triggered. These observations indicate that the facial recognition module effectively distinguishes between authorized and unauthorized users under controlled indoor conditions. The authentication outcome is illustrated in **Fig. 3**.

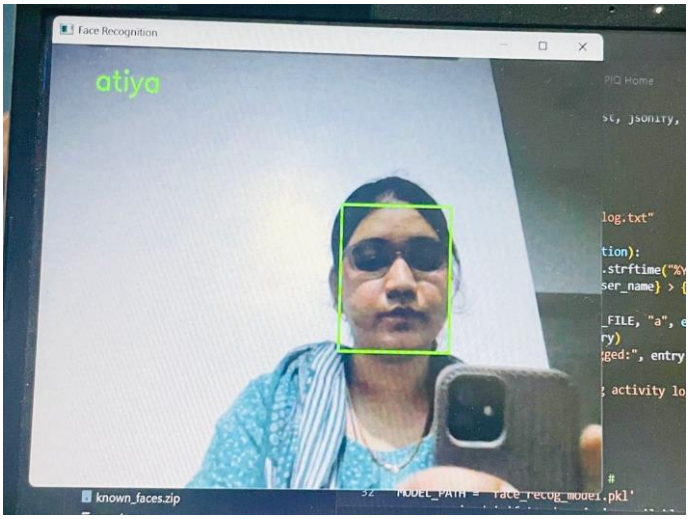

Fig. 3. Face Recognition Result (Authorized)

C. OLED Display and Actuation Results

Upon successful authentication, the ESP32 microcontroller actuated the servo motor to unlock the door, confirming authorized access, as shown in **Fig. 4**. At the same time, the OLED display provided real-time visual feedback by displaying messages such as *"Door Unlocked"*, informing the user of the system status.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

In the event of an unauthorized access attempt, the system immediately denied entry by keeping the door locked. An audible alert was generated using the buzzer, and a warning message such as *"Unauthorized User"* was displayed on the OLED screen, as illustrated in **Fig. 5**.

The combination of visual indications and audible alerts improves system usability and enhances security by clearly communicating access outcomes to users.

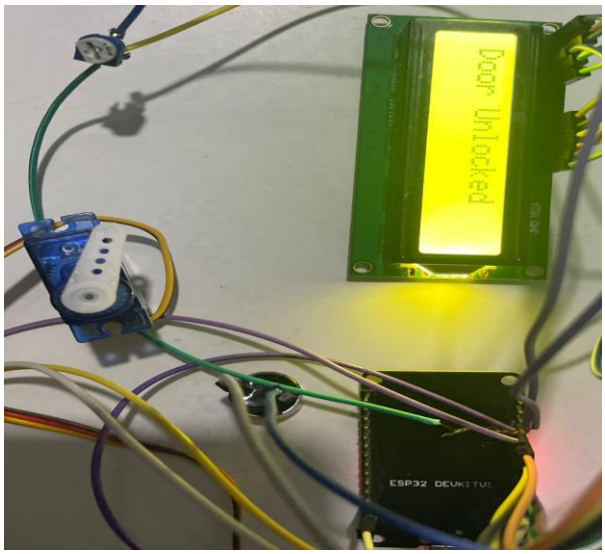

Fig. 4. Servo motor actuation during door locking and unlocking

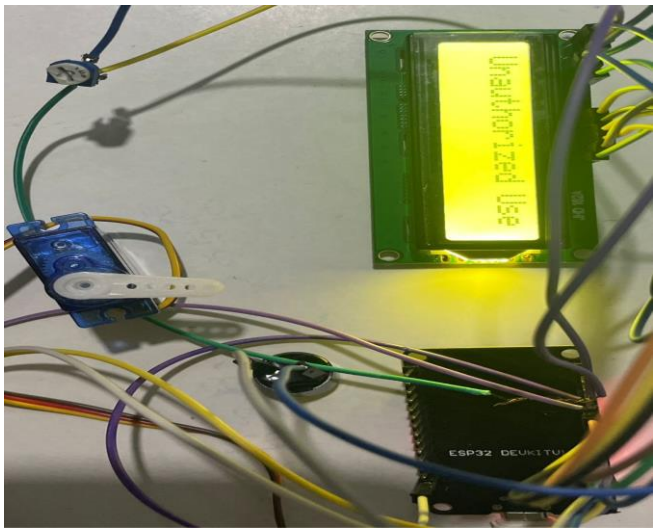

Fig. 5. OLED display showing access status during system operation

D. Web Based Remote Access Results

The web-based control interface enabled authorized users to remotely lock and unlock the door through a browser-based application. The interface also allowed users to send custom messages, which were displayed on the OLED screen in real time. Communication between the web interface and the ESP32 was stable and responsive during testing.

The remote access functionality demonstrated the IoT capability of the system and allowed convenient door control without physical interaction as shown in Fig. 6.

E. Discussion

The experimental results demonstrate that the proposed system effectively integrates facial recognition, IoT-based control, and real-time status display into a unified smart door access solution. Compared to conventional locking systems, the proposed approach offers improved security through biometric authentication and enhanced user interaction through visual feedback and remote accessibility.

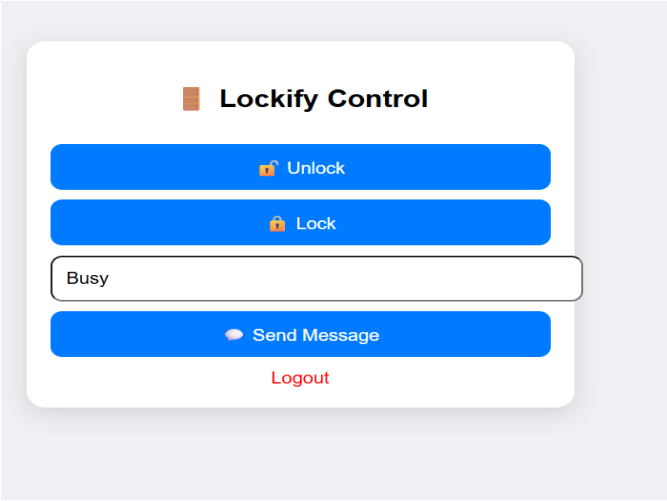

Fig. 6. Web-based remote access control dashboard

Although the system performs reliably in controlled environments, its performance can be influenced by lighting conditions and network availability. These limitations do not affect core functionality and can be addressed in future enhancements through improved camera modules, optimized models, and cloud-based processing.
Overall, the results validate the feasibility, effectiveness, and practicality of the proposed smart door locking system for indoor security applications.

VIII. PERFORMANCE AND ANALYSIS

The performance of the proposed system was evaluated based on recognition accuracy, response time, and system reliability. Face recognition decisions were typically generated within a short duration after face detection, enabling near real-time access control. The servo motor responded immediately upon receiving control signals from the ESP32, demonstrating minimal actuation delay.

The system maintained stable operation under moderate lighting variations and different facial orientations. Remote commands issued through the web interface were executed with negligible delay under stable network conditions, confirming the effectiveness of the communication mechanism.

IX. LIMITATIONS

Despite its effectiveness, the proposed system has certain limitations. The face recognition accuracy may decrease under extreme lighting conditions or partial face occlusions. Since the recognition module is executed on a local system, overall performance depends on system hardware capabilities. Additionally, continuous internet connectivity is required for

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

remote access functionality. Future enhancements can address these limitations by integrating edge-based processing and adaptive illumination handling.

X. FUTURE SCOPE

The proposed system can be further enhanced in several ways:

- Integration of cloud-based face recognition for improved scalability.
- Addition of a mobile application for remote access and monitoring.
- Incorporation of multi-factor authentication such as OTP or RFID.
- Use of wireless communication protocols to improve deployment flexibility.Enhancement of security using encrypted communication channels.

XI. CONCLUSION

This paper presented an intelligent IoT-based smart door locking system using facial recognition and ESP32 microcontroller. By combining deep learning-based authentication with real-time hardware control, the system provides enhanced security, automation, and user convenience. Experimental results demonstrate reliable access control for both authorized and unauthorized users. The proposed solution offers a cost-effective and scalable approach for modern smart security applications, making it suitable for residential and institutional use.

REFERENCES

[1] M. Alsayaydeh, A. Almajali, and R. Khater,"Design and Evaluation of a Biometric IoT-Based Smart Door Lock System,"International Journal of Advanced Engineering and Management Applications,vol. 6, no. 7, pp. 1–7, 2023.

[2] R. Kumar, S. Verma, and A. Sharma, "Smart Biometric Door Lock System Using Face and Fingerprint Recognition," in *Proc. IEEE Int. Conf. Smart Computing and Communication*, pp. 215–220, 2022.

[3] S. Sonamoni, R. Das, and P. Deka, "IoT-Based Smart Remote Door Lock and Monitoring System," *International Journal of Engineering Research and Technology (IJERT)*, vol. 11, no. 6, pp. 45–49, 2022.

[4] P. Premanand, A. Amune, R. Unde, S. Jangral, B. Sadmake, and K. Singh, "IoT Enabled Door Lock System Using Cognitive Abilities," in *Advances in Intelligent Systems*, Taylor & Francis Group, pp. 321–330, 2023.

[5] K. Kondamu, R. Kiran, and S. Reddy, "ESP32-CAM Based Smart Door Lock System with Mobile Application," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 4, no. 5, pp. 890–895, 2022.

[6] A. Singh and P. Jain, "IoT-Based Smart Door Lock System Using Embedded Platforms," in *Proc. IEEE Int. Conf. Internet of Things and Applications*, pp. 112–117, 2021.

[7] S. Patil and M. Kulkarni, "Design of Smart Door Lock System Using IoT and Biometric Authentication," in *Proc. IEEE Int. Conf. Communication and Signal Processing*, pp. 978–982, 2020.

[8] S. Prathapagiri and P. Eethamakula, "Wi-Fi Based Smart Door Lock System Using ESP32-CAM," *International Journal of Engineering and Technology*, vol. 9, no. 3, pp. 210–214, 2019.

[9] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, "Joint Face Detection and Alignment Using Multi-Task Cascaded Convolutional Networks," *IEEE Signal Processing Letters*, vol. 23, no. 10, pp. 1499–1503, 2016.

[10] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, pp. 815–823, 2015.

[11] S. Gupta and R. Mehta, "IoT-Based Smart Locker System Using Biometric Authentication," *International Journal of Computer Applications*, vol. 175, no. 8, pp. 20–25, 2020.

[12] Espressif Systems, *ESP32 Technical Reference Manual*, Espressif Systems Inc., 2023.