IoT-Based Facial Authentication System

[1]Mrs. Deepali Adhyapak, [2]Aditya Bhangre, [3]Chetan Godhwani, [4]Aditya Raina
[1234]Department of Electronics and Telecommunication
[1234]Progressive Education Society Modern College of Engineering, Pune – 411005, Maharashtra, India

***Abstract*—This paper presents the design and implementation of an IoT-based facial authentication system for secure and intelligent door access control.**
The proposed system utilizes an ESP32-CAM module to capture images of individuals at the entrance and perform facial recognition for identity verification. The system is designed to enhance security by allowing only authorized access based on real-time authentication.
The system integrates multiple components, including an ESP32 microcontroller with built-in Wi-Fi for internet connectivity, an LCD display for user interaction, a speaker for audio alerts, and an ultrasonic sensor for detecting the presence of a person near the door. The ESP32 module performs image acquisition and processing, while also enabling communication with a mobile application or software interface.
For remote monitoring and control, the system sends a notification to the authorized user whenever a visitor is detected. The user can verify the visitor through the received data and remotely grant or deny access. Upon approval, the system activates the door unlocking mechanism; otherwise, access is restricted, ensuring safety and controlled entry.
The proposed system provides real-time monitoring, remote accessibility, and automated door control, making it a reliable and efficient solution for modern security needs.
The developed prototype demonstrates effective performance in facial recognition and access management, offering a cost-effective and scalable approach for smart homes and secure facilities.

***Index Terms*—Facial Recognition, Internet of Things (IoT), ESP32-CAM, Smart Door Lock System, Remote Access Control, Wireless Communication (Wi-Fi), Real-Time Monitoring, Home Security, Embedded Systems, Access Authentication**

I. Introduction

Security and access control are critical aspects of modern homes, offices, and smart buildings. With increasing concerns about unauthorized entry and safety, there is a growing need for intelligent systems that can provide reliable and real-time monitoring of entry points. Traditional security systems such as locks, keys, and password-based access methods are often vulnerable, inconvenient, and lack remote accessibility.
With the rapid advancement of embedded systems and the Internet of Things (IoT), smart security solutions have become more efficient and accessible. IoT-enabled systems allow users to monitor and control devices remotely through internet connectivity. In particular, facial recognition technology provides a secure and contactless method of authentication, reducing the risks associated with physical keys or passwords.
In this paper, an IoT-based facial authentication system for secure door access is proposed and developed. The system is built around an ESP32-CAM module, which captures images and performs facial recognition for identifying individuals at the entrance. The system integrates multiple components, including an LCD display for user interaction, a speaker for audio alerts, and an ultrasonic sensor to detect the presence of a person near the door.

For communication and remote access, the ESP32 module with built-in Wi-Fi is used to send real-time notifications to the authorized user through a mobile application or software interface. This enables the user to verify the visitor remotely and make a decision to grant or deny access. Based on the user's response, the system controls the door locking mechanism, ensuring secure and controlled entry.

The proposed system aims to provide a smart, cost-effective, and efficient solution for modern security challenges. By integrating facial recognition, IoT communication, and automated access control into a single platform, the system enhances security, improves user convenience, and reduces the need for physical presence at the entry point.

The major contributions of this work are as follows:

IoT-Based Smart Access System

A compact and efficient system is developed for secure door access using IoT technology. The system enables remote monitoring and control, making it suitable for modern smart homes and offices.

Facial Recognition Authentication

The system uses facial recognition to identify individuals, providing a secure and contactless method of access control and reducing dependency on traditional keys or passwords.

Real-Time Notification and Control

The system sends instant alerts to the authorized user when a visitor is detected. This allows real-time verification and remote decision-making for granting or denying access.

Integrated Hardware Components

Multiple components such as ESP32-CAM, LCD display, speaker, and ultrasonic sensor are integrated into a single system, enabling efficient operation and user interaction.

Automated Door Control System

The system automatically controls the locking and unlocking of the door based on user authorization, ensuring enhanced security and convenience.

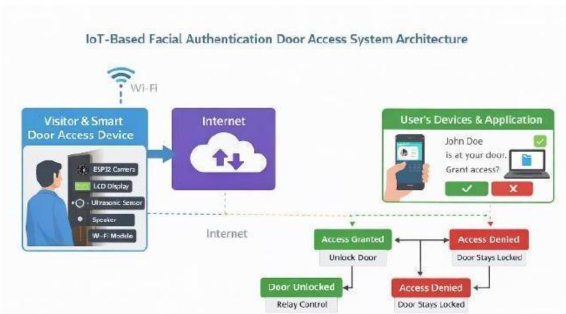

Fig. 1. System Architecture

II. LITERATURE REVIEW

The rapid advancement of the Internet of Things (IoT) and embedded systems has significantly improved modern security and access control solutions. Researchers have developed various smart security systems that enable remote monitoring and control of entry points in homes and offices. These systems aim to enhance safety and convenience by reducing human dependency and enabling real-time decision-making. However, many traditional systems are limited to password-based or RFID-based access, which can be vulnerable to security breaches and unauthorized access.

Several studies have explored biometric authentication techniques, including fingerprint recognition, iris scanning, and facial recognition, to enhance access control and security systems. Among these methods, facial recognition has emerged as one of the most promising approaches due to its contactless operation, convenience, and user-friendly nature. It enables the identification and verification of individuals without requiring physical interaction, making it highly suitable for smart homes, offices, and IoT-enabled environments. Despite its advantages, facial recognition systems face challenges such as variations in lighting conditions, image quality, facial expressions, and hardware processing limitations, which can impact their accuracy, reliability, and overall performance.

Smart door lock systems based on IoT have also been widely explored. These systems use wireless communication technologies such as Wi-Fi and Bluetooth to allow users to control access remotely through mobile applications. Modules like ESP32 and ESP8266 are commonly used due to their built-in connectivity and low cost. While these systems provide remote access and monitoring, many of them rely only on manual user input and lack intelligent authentication mechanisms.

Camera-based surveillance systems have further enhanced security by enabling real-time monitoring and recording of activities at entry points. Devices such as ESP32-CAM allow image capture and live streaming, providing visual verification of visitors. However, in many existing systems, surveillance and access control are implemented separately, which reduces efficiency and requires additional hardware and management.
In addition, the integration of sensors such as ultrasonic sensors has been explored for detecting human presence and triggering system actions. These sensors help in automating the process by activating the system only when a person is detected, thereby saving power and improving efficiency. Despite these advancements, many systems still lack proper integration of sensing, authentication, communication, and automated control.

Although significant progress has been made in smart security systems, there is still a need for a unified solution that combines facial recognition, IoT-based communication, real-time monitoring, and automated door control in a single platform. The proposed system addresses these limitations by integrating all these features into a cost-effective and efficient solution, thereby enhancing security, improving user convenience, and enabling remote access control.

III. SYSTEM DESIGN

The proposed system is centered around the ESP32-CAM module, which acts as the primary control and processing unit. It is responsible for image capture, facial recognition, and communication through built-in Wi-Fi. The overall system architecture is modular and consists of five major subsystems: the sensing unit, control unit, communication unit, actuation unit, and power supply unit. This modular design improves system efficiency, flexibility, and ease of future expansion.

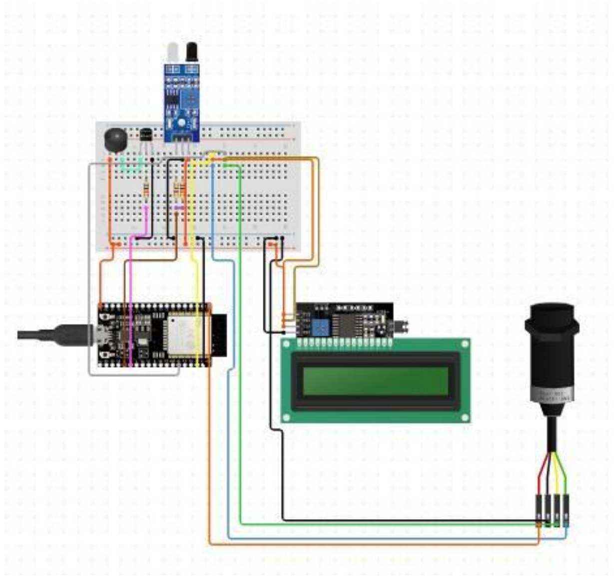

Fig. 2. Circuit Diagram

A. Sensing Unit

The sensing unit is responsible for detecting the presence of a person at the entrance and initiating the authentication process. An ultrasonic sensor is used to detect motion or proximity near the door. Once a person is detected, the ESP32-CAM captures the image of the individual for facial recognition. This ensures that the system operates only when required, improving efficiency and reducing unnecessary processing.

B. Control Unit

The control unit is managed by the ESP32-CAM module, which performs image acquisition and facial recognition. It processes the captured image and compares it with stored data to identify the individual. Based on the recognition result and user input, the control unit makes decisions regarding access control. It also coordinates with other components such as the display, speaker, and door locking mechanism.

C. Communication Unit

The communication unit enables remote monitoring and user interaction. The ESP32's built-in Wi-Fi module is used to send real-time notifications to the authorized user through a mobile application or software interface. The user receives the visitor's information and can remotely grant or deny access. This allows secure and convenient control of the system from any location.

D. Actuation Unit

The actuation unit is responsible for performing actions based on user decisions. It includes the door locking/unlocking mechanism, which is activated when access is granted. A speaker is used to provide audio alerts or notifications, while an LCD display shows system status messages such as "Access Granted" or "Access Denied." These components enhance user interaction and system feedback.

E. Power Supply Unit

The system is powered using a regulated power supply suitable for the ESP32-CAM and associated components. Components such as resistors, capacitors, transistors, and diodes are used to ensure stable voltage regulation and circuit protection. A common ground is maintained across all components to ensure proper functioning and reduce electrical noise.

F. Operational Workflow

The system operates through a continuous monitoring and response mechanism. The ultrasonic sensor detects the presence of a person near the door, triggering the ESP32-CAM to capture an image. The system performs facial recognition and sends a notification to the authorized user via the internet. The user reviews the request and decides whether to grant or deny access. Based on the decision, the system either unlocks the door or keeps it locked. This process ensures secure, real-time, and remote-controlled access management.

IV. METHODOLOGY

The proposed system is designed to provide secure and intelligent door access using facial recognition and IoT technology. The system operates in an automated mode where it continuously monitors the entrance, detects the presence of a person, and performs authentication. Additionally, it enables remote user interaction for decision-making, ensuring flexibility, security, and convenience.

A. Data Acquisition

The system collects real-time data using the ESP32-CAM module and an ultrasonic sensor. The ultrasonic sensor is used to detect the presence of a person near the door by measuring distance. Once a person is detected within a predefined range, the ESP32-CAM captures an image of the individual. This image serves as the primary input for facial recognition.

B. Data Processing and Decision Making

The ESP32-CAM processes the captured image and performs facial recognition by comparing it with stored data. Based on this analysis:

- If the face is recognized, the system proceeds with authentication and prepares to grant access.
- If the face is not recognized, the system still sends a notification to the authorized user for manual verification.
- A notification containing the visitor's image is sent to the user for final decision-making.

This process ensures both automated recognition and user-controlled access, enhancing system security and reliability.

C. Communication and Data Transmission

The system uses the built-in Wi-Fi capability of the ESP32 module to transmit data over the internet. When a visitor is detected, a notification along with the captured image is sent to the authorized user through a mobile application or software interface. This enables real-time monitoring and remote access control from any location.

D. Access Control Mechanism

The system includes a door locking mechanism that is controlled based on the user's decision. If the user grants access, the system activates the unlocking mechanism. If access is denied, the door remains locked. The system also provides feedback through an LCD display and speaker, indicating whether access is granted or denied.

E. Alert and Notification System

The ultrasonic sensor operates using time-of-flight principle with a detection range of 2 cm. The optimal distance between the ESP32-CAM and the user is 0.5 to 1.5 meters for accurate recognition. The system response delay ranges from 1 to 3 seconds depending on processing and network conditions.
The system incorporates real-time alert functionality to notify the user whenever a visitor is detected. Notifications are sent instantly via the internet, ensuring timely response. Audio alerts through the speaker and visual messages on the LCD display further enhance user awareness and system interaction.

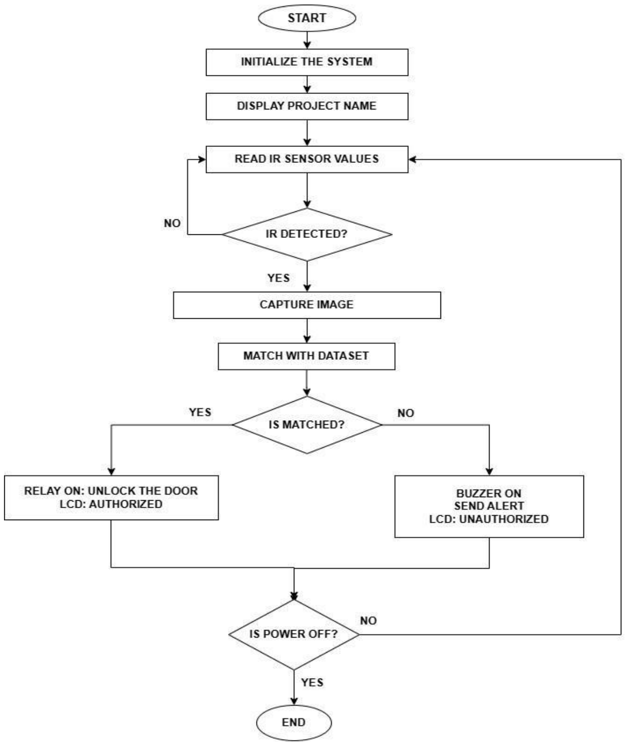

Fig. 3. Flowchart

V. RESULTS

The overall system demonstrated effective integration of sensing, processing, communication, and actuation modules. The proposed IoT-based authentication system operated reliably in performing real-time face detection, remote user notification, and secure door access control. The system successfully provided a balance between automation and user-controlled decision-making. However, factors such as lighting conditions, network stability, and image quality may influence system performance and can be further improved in future enhancements.

A. Facial Recognition Performance

The facial recognition subsystem showed satisfactory performance during testing. The ESP32-CAM module was able to capture clear images under normal lighting conditions and successfully identify registered users. The system responded accurately when matching faces with stored data. However, slight variations in lighting and face angles affected recognition accuracy, indicating the need for further optimization in real-world conditions.

B. Presence Detection Performance

The ultrasonic sensor effectively detected the presence of a person near the door. It accurately measured distance and triggered the system when a person was within the predefined range. This ensured that the camera and processing unit were activated only when required, improving system efficiency and reducing unnecessary operations.

C. Communication and Remote Control

The communication subsystem performed efficiently using ESP32's built-in Wi-Fi module. Notifications were successfully sent to the authorized user in real time whenever a visitor was detected. The user was able to view the information and respond with minimal delay. The system demonstrated reliable remote access control, although performance depended on internet connectivity and network stability.

D. Access Control System Performance

The door locking and unlocking mechanism operated accurately based on the user's decision. When access was granted, the system successfully activated the
unlocking mechanism. When access was denied, the door remained securely locked. The LCD display and speaker provided clear feedback messages such as "Access Granted" and "Access Denied," improving user interaction and system usability.

E. Alert and Notification System Performance

The ultrasonic sensor operates using time-of-flight principle with a detection range of 2 cm to 400 cm. The optimal distance between the ESP32-CAM and the user is 0.5 to 1.5 meters for accurate recognition. The system response delay ranges from 1 to 3 seconds depending on processing and network conditions.
The alert system functioned effectively by sending instant notifications to the user. The combination of mobile notifications, audio alerts through the speaker, and visual feedback on the LCD ensured that the user was well-informed about visitor activity. This improved the responsiveness and reliability of the system.

F. Overall System Performance

The overall system demonstrated successful integration of facial recognition, IoT communication, sensing, and automated access control. The system operated reliably in providing real-time monitoring and secure door management. While the performance was satisfactory, factors such as network delays, environmental lighting, and hardware limitations may affect efficiency and can be improved in future developments.

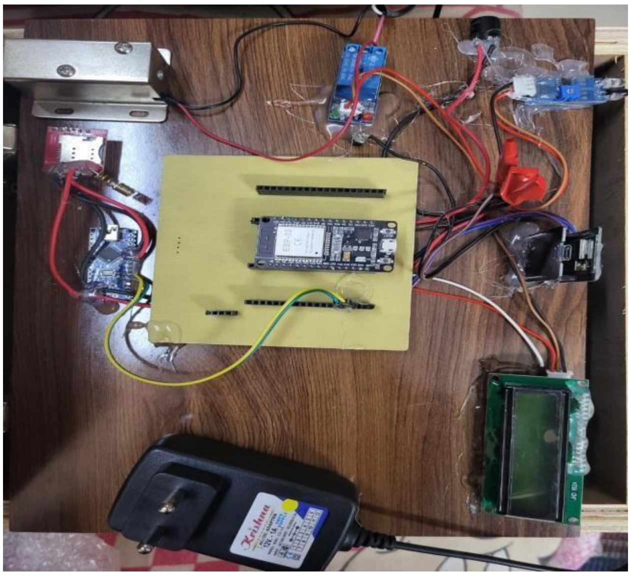

Fig. 4. Electronic Components Structure

Fig. 5. Box

VI. CONCLUSION

This paper presented the design and implementation of an IoT-based facial authentication system for secure and intelligent door access control. The proposed system integrates facial recognition, real-time monitoring, wireless communication, and automated door control into a single embedded platform.
The experimental results demonstrate that the system is capable of reliably detecting the presence of a person, capturing images, and performing facial recognition for identity verification. The integration of the ESP32-CAM module enables efficient image processing and communication, while the use of Wi-Fi connectivity allows real-time notification and remote access control. The system successfully allows the authorized user to verify visitors and make decisions to grant or deny access, ensuring improved security and convenience.

The proposed solution offers a cost-effective, scalable, and efficient approach to modern security systems, reducing dependency on traditional access methods such as keys and passwords. The combination of sensing, processing, and communication enhances system performance and user experience. However, certain limitations such as dependency on network connectivity, lighting conditions, and recognition accuracy may affect system performance.

Future improvements can focus on enhancing facial recognition accuracy, improving system security, and integrating additional features such as cloud storage, multi-user access, and advanced authentication methods.

In conclusion, the developed system demonstrates the practical implementation of IoT and facial recognition technology for smart security applications and provides a strong foundation for further research in intelligent access control systems.

References

[1] Lin, J., Zhu, L., Chen, W.-M., Wang, W.-C., & Han, S. (2024). Tiny machine learning: Progress and futures. https://arxiv.org/abs/2403.19076.

[2] George, A., Ecabert, C., Otroshi Shahreza, H., Kotwal, K., & Marcel, S. (2023). EdgeFace: Efficient face recognition model for edge devices. https://arxiv.org/abs/2307.01838.

[3] Mohammad, A. S., Jarullah, T. G., Al-Kaltakchi, M. T. S., Alshehabi Al-Ani, J., & Dey, S. (2024). IoT-MFaceNet: Internet-of-Things-based face recognition using MobileNetV2 and FaceNet deep-learning implementations on a Raspberry Pi-400. Journal of Low Power Electronics https://doi.org/10.3390/jlpea14030046.

[4] Elhanashi, A. (2024). Advancements in TinyML: Applications, limitations, and impact on IoT devices. Electronics (MDPI), 13(17), Article 3562. https://doi.org/10.3390/electronics13173562.

[5] Heydari, S., et al. (2024). Tiny machine learning and on-device inference: A survey. PMC / preprint. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC12115890.

[6] Xie, Y., Li, J., & Chen, X. (2022). Privacy protection framework for face recognition in edge-based Internet of Things. Future Generation Systems. https://doi.org/10.1007/s10586-022-03808-8.

[7] Al-Nabulsi, J., & Others. (2023). IoT solutions and AI-based frameworks for masked-face recognition. Sensors (MDPI), 23(16), 7193. https://doi.org/10.3390/s23167193.

[8] Eman, M., et al. (2023). Innovative hybrid approach for masked face recognition using SSD-MobileNetV2 and RPCA. Sensors (MDPI), 23(15), 6727. https://doi.org/10.3390/s23156727.

[9] Wang, Y., et al. (2023). Masked face recognition system based on attention mechanism. Information (MDPI), 14(2), Article 87. https://doi.org/10.3390 info14020087.

[10] Kumar, B. A., et al. (2023). Face mask detection on photo and real-time video with MobileNetV2 variants. https://www.mdpi.com/2076-3417/13/2/935.

[11] Mao, Y., Yu, X., Huang, K., Zhang, Y.-J. A., & Zhang, J. (2023). Green edge AI: A contemporary survey.https://arxiv.org/abs/2312.00333.

[12] Surianarayanan, C., Lawrence, J. J., Chelliah, P. R., Prakash, E., & Hewage, C. (2023). A survey on optimization techniques for edge artificial intelligence (AI). Sensors, 23(3), 1279. https://doi.org/10.3390/s23031279.