



Available Online at www.hithaldia.in/locate/ECCN
All Rights Reserved

ORIGINAL CONTRIBUTION

Design and Implementation of an IoT-Based Biometric Access Control and Attendance System with Cloud Synchronization

¹Rajesh Karmakar, ²Saumil Maulik, ³Rakesh Ghosh, ⁴Kishor Basak, ⁵Akinchan Das

^{1,2,3,4}UG student, Dept. of Electronics and Communication Engineering, Haldia Institute of Technology, Haldia, Purba Medinipur, West Bengal

⁵Dept. of Electronics and Communication Engineering, Haldia Institute of Technology, Haldia, Purba Medinipur, West Bengal

ABSTRACT

The increasing need for secure access management and automated attendance monitoring has created demand for reliable authentication systems that overcome the limitations of conventional methods. Physical keys, ID cards, passwords, and manual attendance records are prone to loss, misuse, identity fraud, and human error. This study presents an affordable IoT-based biometric access control system using an ESP32 microcontroller and optical fingerprint sensor. The system integrates fingerprint authentication, electronic door-lock control, real-time attendance management, local data storage, cloud synchronization, and web-based monitoring. An RTC records the exact time of each access event. SQLite storage maintains attendance data during temporary Wi-Fi loss and synchronizes it with Google Sheets when connectivity is restored. An ESP32-hosted web interface enables users to view attendance and manage administrative functions. The system provides a scalable solution for secure and automated access and attendance management in educational institutions, offices, and restricted-access environments.

KEYWORDS: IoT, ESP32, Biometric Authentication, Cloud Synchronization, Real Time Clock (RTC).

1. INTRODUCTION

In educational institutions, laboratories, offices, and other restricted spaces, secure access control and reliable attendance management are crucial. Traditional methods such as physical keys, ID cards, passwords, and attendance registers may suffer from identity sharing, credential loss or duplication, impersonation, and recording errors. This creates a need for automated systems that reduce human effort while providing reliable identification. Biometric authentication offers a promising solution by identifying individuals through physiological characteristics. Among various biometric techniques, fingerprint recognition is particularly suitable for access-control applications because of its distinctiveness and compatibility with compact embedded systems. However, authentication alone does not address attendance management and administrative monitoring. Many existing systems either operate as standalone devices or depend on continuous network connectivity for attendance management. Temporary Internet unavailability presents another challenge, as

network-dependent systems may be unable to immediately transfer access and attendance records. Therefore, an effective system should perform essential operations locally while synchronizing data with a remote platform when connectivity is restored. This study addresses these issues through the development of an integrated biometric access-control and attendance-management system. The proposed approach combines biometric identification, automated access control, attendance recording, local data retention, and cloud synchronization in a low-cost platform suitable for small- and medium-scale environments. The remainder of this paper presents the related work and research gap, followed by the proposed system architecture and implementation. The experimental evaluation examines authentication, access control, attendance recording, and offline data handling, followed by a discussion of limitations and future scope.

2. LITERATURE REVIEW

Mittal et al. [1] developed a fingerprint biometric-based access-control system for classroom entry and attendance management. The system identified authorized users through fingerprint authentication and automatically recorded attendance details.

Habib et al. [2] proposed a GSM-based biometric access-control system using fingerprint authentication. The system provided secure access and allowed remote monitoring through GSM technology.

Anitha et al. [3] developed a fingerprint-based door-lock system with a buzzer. The system automatically unlocked the door after successful fingerprint verification and generated an alert for unauthorized attempts.

Anirudh et al. [4] proposed a multilevel biometric authentication locking system using Arduino UNO. The system improved door security by replacing conventional keys with fingerprint-based authentication.

Sutikno et al. [5] developed a fingerprint-based smart door-lock system using Arduino and smartphone connectivity. Chowdhury et al. [6] similarly proposed an embedded fingerprint door-lock system with electronic locking and alert mechanisms, focusing on secure and convenient access control.

Permana et al. [7] developed an IoT-based smart door-lock system combining fingerprint and keypad authentication. The system used ESP32 and Firebase for secure access control and remote management.

Handini et al. [8] proposed a smart-door access system using fingerprint biometrics and PIN authentication. The IoT-based system provided an additional authentication layer and smartphone-based control.

Alsayaydeh et al. [9] developed an IoT-based biometric smart lock using fingerprint authentication and ESP32. The system supported real-time monitoring, mobile control, and security alerts.

Ziad et al. [10] developed an ESP32-based smart door-lock system integrating fingerprint recognition, RFID, and IoT technology. The

system provided multiple authentication methods and real-time door-access monitoring.

While the reviewed studies demonstrate progress in biometric attendance, IoT-based access control, and smart door-lock systems, most focus on individual functions or partial combinations of these features. Limited attention has been given to integrating biometric authentication, automated attendance, local data storage, cloud synchronization, and web-based administration in a single low-cost platform. The proposed system addresses this gap by combining these functions with offline attendance storage and subsequent cloud synchronization.

3. PROPOSED SYSTEM

3.1. System Architecture

The proposed system integrates biometric authentication, access control, attendance recording, local storage, and cloud monitoring using an ESP32 as the central controller. As shown in Fig. 1, the overall system consists of the fingerprint sensor, RTC module, OLED display, relay module, electronic door lock, Wi-Fi connection, SQLite database, and cloud-based Google Sheets. It interfaces with the fingerprint sensor, RTC, OLED display, relay, electronic door lock, and Wi-Fi network. The ESP32 coordinates the authentication, attendance recording, and access-control operations. The system also manages data storage and synchronization with the cloud when network connectivity is available. After successful authentication, the ESP32 identifies the user, records the access time, and controls the door lock.

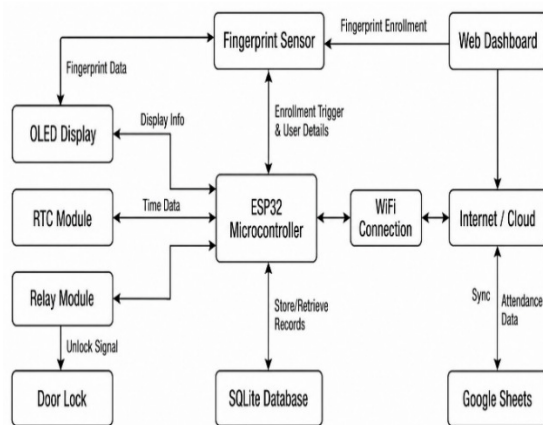


Figure 1: Block diagram of the proposed biometric access-control and attendance system.

3.2. Hardware Components

Table 1 summarizes the principal hardware components used in the system.

Table 1. Hardware Components

Components	
Microcontroller	Voltage Regulator
OLED Display Module	Optical Fingerprint Module
Buzzer	LED
Electronic Door Lock	Resistor
Power Supply	Capacitor
SMPS	Diode
RTC Module	Vero Board
Relay	PBT Connector
Optocoupler	Bug Strip
BJT	

3.3. Biometric Authentication and Access Control

The R307 sensor captures the user's fingerprint and compares it with registered templates. When a valid match is obtained, the corresponding user ID is sent to the ESP32. The controller then activates the relay to unlock the electronic door and allows the authenticated user to enter. An unsuccessful match results in access denial.

3.4. Attendance Recording and Data Storage

After successful authentication, the ESP32 obtains the current date and time from the RTC and generates an attendance record containing the user ID, date, time, and status. The record is stored in the local SQLite database. This local

storage allows attendance information to be retained during temporary Wi-Fi failures.

3.5. Cloud Synchronization and Web Administration

When Wi-Fi is available, attendance records are synchronized from the local database to Google Sheets for remote monitoring. If connectivity is unavailable, the records remain stored locally and are synchronized after the connection is restored. A web-based interface allows administrators to view attendance records and manage system functions.

4. METHODOLOGY

The operational logic of the proposed biometric access-control and attendance system follows a continuous authenticate–record–authorize–synchronize cycle, illustrated in the steps below.

1. Initialization: On power-up, the ESP32 initializes the fingerprint sensor, RTC module, OLED display, relay, Wi-Fi communication, and required database functions.

2. Fingerprint Authentication: The R307 fingerprint sensor continuously waits for a fingerprint. The captured fingerprint is compared with the registered templates, and a valid match returns the corresponding user ID to the ESP32.

3. User Identification and Access Control: After successful authentication, the ESP32 identifies the registered user and activates the relay to control the electronic door lock. If no valid fingerprint is detected, access is denied and the door remains locked.

4. Attendance Recording: For a successful authentication, the ESP32 obtains the current date and time from the RTC and generates an attendance record containing the user ID, date, time, and attendance status. The record is stored in the local SQLite database.

5. Cloud Synchronization: The system checks the availability of Wi-Fi connectivity. When the network is available, the stored attendance information is synchronized with Google Sheets. During network failure, the records remain stored locally and are synchronized after connectivity is restored.

6. Web-Based Monitoring: The web-based administrative interface allows authorized administrators to view attendance records and manage relevant system functions. This provides remote access to attendance information while maintaining local data storage for network-independent operation.

5. IMPLEMENTATION

The system was designed using the Vero board containing the ESP32, R307 fingerprint sensor, OLED display, DS3231 RTC, relay, optocoupler, BC547 transistor, buzzer, LED, and other components. The overall operating sequence of the proposed attendance and access-control system is illustrated in Fig. 2. The electronic door lock was connected to the relay, while the fingerprint sensor was connected to the ESP32. The latter was programmed to read fingerprints, unlock the door, record attendance with the RTC timestamp, and notify the user through the buzzer and OLED display. The SQLite database was used to store attendance records, which were further synchronized with Google Sheets via Wi-Fi. The system was configured to retain attendance records locally during temporary network failures. The authentication process was tested using registered and unregistered fingerprints to verify access control. The response of the electronic lock, attendance logging, and user feedback were also evaluated before final deployment.

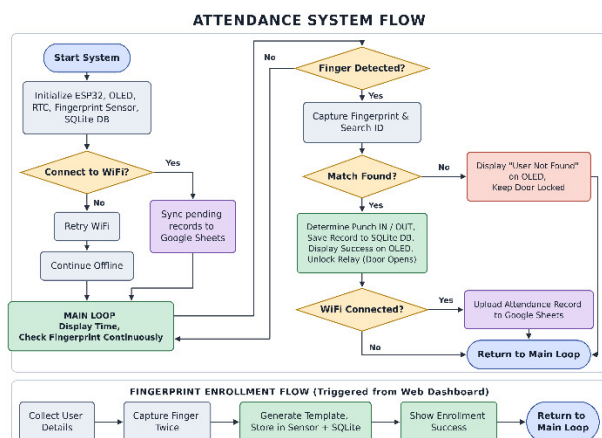


Figure 2: Flow Chart

6. RESULTS AND DISCUSSION

The developed system was successfully implemented and tested for biometric authentication, access control, attendance recording, local data storage, and cloud synchronization. The R307 fingerprint sensor successfully identified registered users, after which the ESP32 activated the relay-controlled electronic door lock. The OLED display provided immediate feedback for successful and unsuccessful authentication. The developed prototype is shown in Fig. 3, while the internal hardware assembly is shown in Fig. 4.



Figure 3: Biometric Access and Attendance control unit

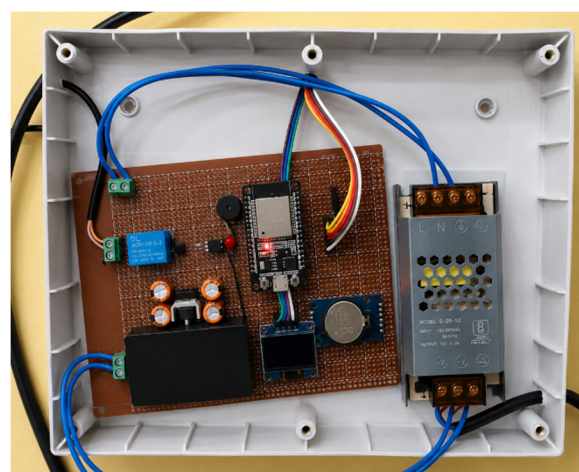


Figure 4: Internal Hardware Configuration of the Biometric Attendance System

For each successful authentication, the system recorded the user details with the date and time obtained from the DS3231 RTC. Attendance records were stored in the local SQLite database and synchronized with Google Sheets when Wi-Fi was available. During network interruption, the records remained stored locally and were synchronized after connectivity was restored. The web dashboard provided user enrollment, attendance monitoring, system configuration, and database-management functions. The web-based administrative dashboard is shown *Fig. 5*, and the synchronized attendance record is presented in *Fig. 6*.

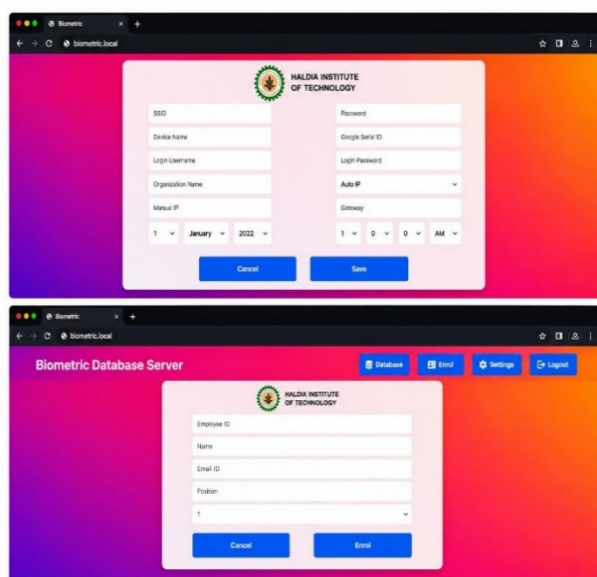


Figure 5: Website Dashboard

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Date	Time	Employee_ID	Employee_Name	Employee_Email	Position	Punch In	Punch Out					
2													
3													
4													
5													
6													
7													
8													
9													
10													
11													
12													
13													
14													
15													
16													
17													
18													
19													
20													

Figure 6: Attendance sheet

Overall, the results demonstrate that the proposed system provides an integrated and practical solution for automated access control and attendance management while reducing manual record-keeping. The system showed reliable operation during normal use, although fingerprint condition, Wi-Fi stability, and power availability may affect performance.

7. CONCLUSION

The proposed system provides accurate and automated attendance and entry/exit monitoring using fingerprint authentication, ESP32, RTC-based time stamping, automatic door control, and local SQLite storage. Integration with Google Sheets and a web interface enables convenient record management and monitoring, while local storage ensures reliable operation during temporary network interruptions. Overall, the system offers a cost-effective and reliable solution for biometric access and attendance management, with potential for enhanced security, monitoring, and scalability.

ACKNOWLEDGMENT

The authors gratefully acknowledge the guidance of Dr. Ritwik Haldar, Department of Electronics & Communication Engineering, Haldia Institute of Technology, throughout this work, and the Department for providing the laboratory facilities used to build and test the prototype.

REFERENCES

- [1] Mittal, Y., Varshney, A., Aggarwal, P., Matani, K., & Mittal, V. K. (2015). Fingerprint biometric based access control and classroom attendance management system. *2015 Annual IEEE India Conference (INDICON)*, 1–6. doi: <https://doi.org/10.1109/INDICON.2015.7443699>
- [2] Habib, H., Zungeru, A. M., Susan, A. A., Kelechi, I. G., & Oluwatosin, O. B. (2014). Design of a GSM-based biometric access control system. *Control Theory and Informatics*, 4(8).
- [3] Anitha, S., Hima Bindu, Ch., & Sriram Pavan, J. (2020). Biometric based door lock system with buzzer. *Mathematical Statistician and Engineering Applications*, 69(1), 373–379. doi: <https://doi.org/10.17762/msea.v69i1.1655>
- [4] Anirudh, R., Chandru, V., & Harish, V. (2021). Multilevel security biometric authentication locking system using Arduino UNO. *Advances in Parallel Computing*, 40. doi: <https://doi.org/10.3233/APC210121>
- [5] Sutikno, T., Ubaidillah, M. A. F., Arsadiando, W., & Purnama, H. S. (2024). Fingerprint based smart door lock system using Arduino and smartphone application. *Computer Science and Information Technologies*, 5(1), 91–98. doi: <https://doi.org/10.11591/csit.v5i1.p91-98>
- [6] Chowdhury, A. M. M. (2023). Fingerprint based door lock system. *International Journal of Innovative Engineering*, 1(1), 8–15. doi: <https://doi.org/10.60044/ijie.v1i1.7>
- [7] Permana, K. A. K., Piarsa, I. N., & Wiranatha, A. A. K. A. C. (2024). IoT-based smart door lock system with fingerprint and keypad access. *Journal of Information Systems and Informatics*, 6(3). doi: <https://doi.org/10.51519/journalisi.v6i3.844>
- [8] Handini, W. T., Endri, J., & Salamah, I. (2025). Implementation of fingerprint biometrics on smart door entrance access integrated with Internet of Things-based PINs. *Indonesian Journal of Artificial Intelligence and Data Mining*, 8(1), 102–109. doi: <https://doi.org/10.24014/ijaidm.v8i1.31738>
- [9] Alsayaydeh, J. A. J., Yusof, M. F., Mamchenko, S., Hamzah, R. A., & Herawan, S. G. (2025). Design and evaluation of a biometric IoT-based smart lock system with real-time monitoring and alert mechanisms. *International Journal of Advanced Computer Science and Applications*, 16(7). doi: <https://doi.org/10.14569/IJACSA.2025.0160737>
- [10] Ziad, A., Darnila, E., & Kurniawati. (2024). Development and implementation of an ESP32 microcontroller and monitoring system for smart door lock using RFID sensor for E-KTP ID and fingerprint based on the Internet of Things. *Proceedings of Malikussaleh International Conference on Multidisciplinary Studies (MICO MS)*, 4. doi: <https://doi.org/10.29103/micoms.v4i.908>