e-ISSN: 2582-5208

International Research Journal Of Modernization In Engineering Technology And Science

( Peer-Reviewed, Open Access, Fully Refereed International Journal )

Volume:07/Issue:01/January-2025 Impact Factor: 8.187 www.irjmets.com

# ATTENDRO: A PORTABLE, SESSION-CONTROLLED BIOMETRIC ATTENDANCE SYSTEM WITH CENTRALIZED FINGERPRINT DATABASE FOR EDUCATIONAL INSTITUTIONS

**Atharv S. Ghandat[*1], Sanika P. Desai[*2], Tanisha H. Chavan[*3], Kunal S. Mahalunge[*4]**

[*1,2,3,4]Department of Artificial Intelligence and Machine Learning, K.E. Society's Rajarambapu Institute of Technology Polytechnic, Lohegaon, Pune, Maharashtra, India

## ABSTRACT

The major problem in academic administration is the ineffective manual tracking of attendance and the use of proxy signatures. The paper is a design and validation of a portable, IoT-based biometric system called Attendro that implements session-controlled authentication. The device is based on the ESP32 dual-core microcontroller and the R307 optical fingerprint reader and communicates with a Supabase cloud backend through secure HTTPS/TLS protocols. In contrast with non-portable biometric readers, Attendro proposes unique "session windows" managed by faculty members, implying that data on attendance are legally attached to a particular time and place. N=50 experimental validation experiments showed a False Acceptance Rate (FAR) of less than 0.001, 1.37 seconds of average end-to-end latency, and more than 12 hours of steady battery use. These results affirm that the alternative to the conventional fixed infrastructure is portable, serverless biometric architectures, which are both cost-effective and secure.

**Keywords:** Fingerprint Authentication, ESP32, Cloud Computing, IoT, Attendance Management, Session Control, Biometric Systems, Supabase.

## I. INTRODUCTION

The monitoring of academic attendance is one of the very crucial administrative practices, which has a direct correlation with the performance of students and the responsibility of the institutions. The conventional manual recording methods, extending to paper registers and roll calls, are inherently inefficient in terms of systemic aspects, stealing beneficial lecture hours and vulnerable to loci malpractice like proxy attendance [1]. Due to emerging requirements of automated, secure, and data-driven identification systems, the move to Smart Campus environments in educational institutions has been difficult to keep up with [3].

The initial interventions based on technology were Radio Frequency Identification (RFID) systems, in which students verified presences actively using passive transponders [2]. Although these systems minimized the administrative overheads, they did not solve the main problem of identity verification, whereby cards can be traded, rendering the attendance record obsolete [5]. Student data privacy has also elicited ethical concern that has also demanded strong and safe paradigms of design in tracking technology [4].

The solution to all these verification hurdles is biometric authentication, which has come out to be the final solution to the issue. Institutions can ensure non-repudiation in the attendance information by checking individual physiological attributes, including fingerprints or iris markings [6]. Rukhiran et al. [1] show that biometric systems with an IoT can substantially improve identity verification services in learning institutions. Fingerprint technology

e-ISSN: 2582-5208

International Research Journal Of Modernization In Engineering Technology And Science

( Peer-Reviewed, Open Access, Fully Refereed International Journal )

Volume:07/Issue:01/January-2025 Impact Factor: 8.187 www.irjmets.com

is better than complex iris recognition setups to provide the best balance between accuracy, processing time, and cost-effectiveness in high-throughput settings [10].

This essay introduces the reflective project, Attendro, which is a biometric attendance system with IOT capabilities and runs on ESP32 architecture. In response to the shortcomings of traditional installations based on fixed hardware, Attendro seeks to use the wireless connectivity [7], [8] to offer a session-based, location-unaware attendance system, which is seamlessly integrated with cloud infrastructure.

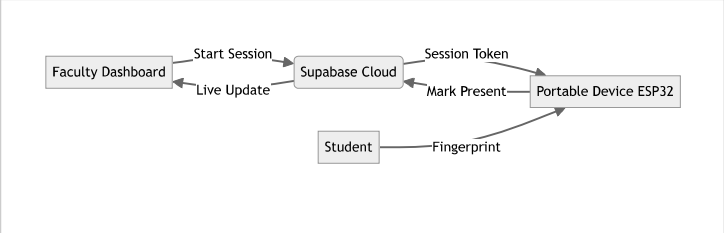


**Figure 1: System Component Interaction Diagram**

## II. LITERATURE SURVEY

The development of the attendance management system also indicates the general tendency to automation and the Internet of Things (IoT) in education infrastructure. This segment evaluates the available methodologies, including token-based systems and high-end biometric systems.

### A. Token-Based and RFID Systems

The first automation was mainly based on Radio Frequency Identification (RFID). Koppikar et al. [2] have suggested an RFID smart attendance monitoring system based on the IoT to simplify data entry into the system. In the same vein, Wakchoure et al. [5] exhibited a multi-approach RFID system that had the capabilities of registering entry and exit times. As efficient at cutting down on the amount of labor as they are, these systems are susceptible to the problem of buddy punching, wherein a student swipes another student into work. The coping mechanism of proving physical presence has led to the adoption of biometric substitutes [2], [5].

### B. Biometric Identification Technologies

Biometrics are used to identify the system of people using inherent physical or behavioral traits [10]. Maltoni and Cappelli [10] set the basic validity of fingerprint recognition in regard to large-scale recognition. The comparative study examinations by Kadry and Smaili [9] on iris recognition show high accuracy rates, although the cost of its usage in the classroom is prohibitive, and the hardware is too complex. Conversely, fingerprint sensors take the place of fingerprint scanners in the education sector because of their affordability and simple installation [1]. This method was again confirmed by Adedoyin et al. through the development of a biometric management system that combined the internet of things (IoT) technology to eliminate the data latency problems that were experienced with the use of standalone scanning devices [6].

e-ISSN: 2582-5208

International Research Journal Of Modernization In Engineering Technology And Science

( Peer-Reviewed, Open Access, Fully Refereed International Journal )

Volume:07/Issue:01/January-2025 Impact Factor: 8.187 www.irjmets.com

### C. Portable and IoT-Enabled Architectures

The contemporary implementations are focused more on movement and real-time connectivity of data. Kumar and Singh [7] used the NodeMCU platform to develop a Wi-Fi-enabled biometric system, which demonstrated that data on attendance could be forcefully sent to a central server. Developing on this, Sharma and Bhatt [8] emphasized portability, which they developed, and they came up with a battery-operated unit that does not require the use of fixed wiring within classrooms. The present study builds on the previous work by incorporating the ESP32 microcontroller [11], [3], which provides better processing capabilities and dual-core performance than previous versions of the NodeMCU, which thus allows more robust encryption and template matching.

## III. METHODOLOGY

The Attendro system has three related parts, including a portable hardware module, a web dashboard for the faculty, and a cloud backend to handle data persistence and business operations. Their combined activity of coordination realizes the session-controlled attendance paradigm, which is the core of this work.

### A. Hardware Architecture

The microcontroller used as the central processing unit of the portable device is the ESP32 microcontroller. The ESP32 has a dual-core Xtensa(r) 32-bit LX6 microprocessor, with the required computational capability between cryptography and network stack operation, as described in the technical reference manual [11]. In the case of biometric acquisition, the system incorporates the DY50/R307 optical fingerprint sensor [12]. The module carries out onboard image processing and pattern matches, outsources the performance of key calculations to the main controller, and provides a quick check outcome (less than 1.0 second latency) [12].

e-ISSN: 2582-5208

International Research Journal Of Modernization In Engineering Technology And Science

( Peer-Reviewed, Open Access, Fully Refereed International Journal )

Volume:07/Issue:01/January-2025 Impact Factor: 8.187 www.irjmets.com

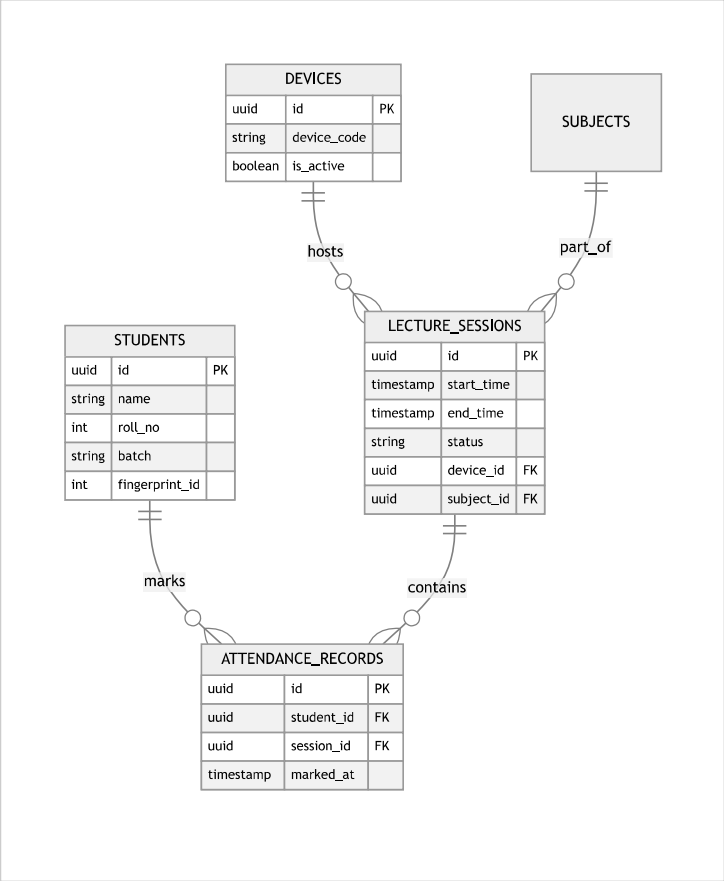


**Figure 2: Entity-Relationship Diagram of Attendro Database Schema**

### B. Session Control Mechanism

The ability of Attendro to operate on a session basis is what makes it unique as compared to the traditional biometric systems. Attendance marking is not always ready to work, but it is valid only in case a lecture session is actually started by a faculty member with the usage of the web dashboard. The architecture means that a fingerprint scan should be used with a meaning only in the context it was meant.

### C. Cloud Backend Implementation

The system uses Supabase [13] as a Backend-as-a-Service (BaaS) with its managed PostgreSQL database and serverless Edge Functions to package the business logic. The architecture makes sure that there is real-time data synchronization between the edge devices and the central repository. The database schema is structured on the principles of the Third Normal Form (3NF), and the normalized structure consists of entities that ensure the management of the devices, students, lecture sessions, and attendance logs.

e-ISSN: 2582-5208

International Research Journal Of Modernization In Engineering Technology And Science

( Peer-Reviewed, Open Access, Fully Refereed International Journal )

Volume:07/Issue:01/January-2025 Impact Factor: 8.187 www.irjmets.com

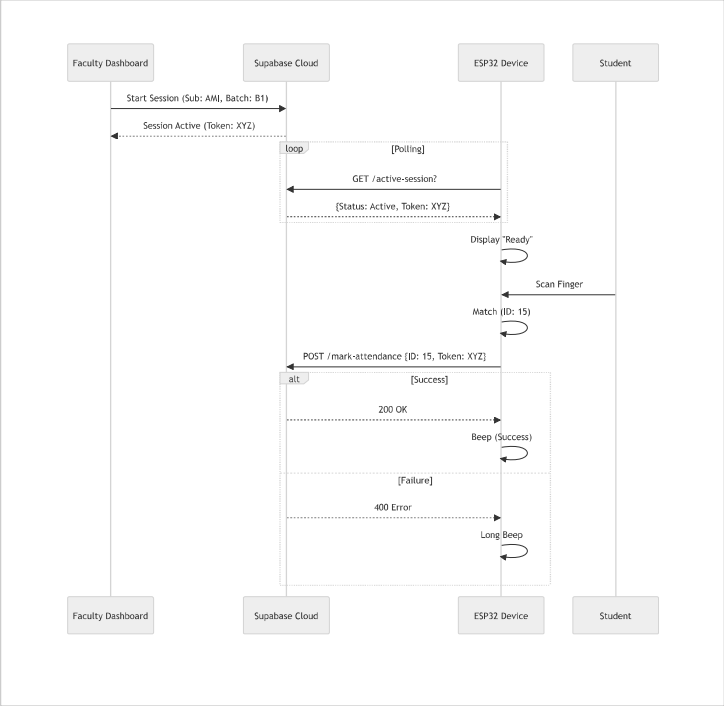


**Figure 3: Sequence Diagram for Attendance Marking Process**

## IV. SYSTEM DESIGN

### A. Database Architecture and Schema

Attendro backend is based on Supabase using a core of PostgreSQL to ensure strict relational integrity. The schema is normalized (3NF) by reducing redundancy. Specific Row Level Security (RLS) policies are strictly implemented such that device writes would be cryptographically separate and faculty reads would be cryptographically separate [13]. Table 1 describes the core entity functional responsibilities.

**Table 1: Database Schema Specification**

| Entity Table | Primary Attributes | Functional Description |
|---|---|---|
| `devices` | UUID, MAC_Addr, Status | Hardware registry for authorized ESP32 nodes. |
| `students` | Roll_No, Finger_ID, Batch | Maps biometric IDs to academic profiles. |
| `sessions` | Session_ID, Subject, Time | Defines active attendance windows. |
| `logs` | Log_ID, Timestamp, Hash | Immutable record of verified presence. |

### B. Hardware Interfacing

Modularity and power efficiency are taken into account in the hardware design. The ESP32 will be the central controller, connecting the sensor with the biometric sensor and the display with OLED with a UART and I2C connection, respectively [11]. The physical connection topology as shown in figure 4 includes the direct interrupt lines to wake up the processor in deep sleep.

e-ISSN: 2582-5208

International Research Journal Of Modernization In Engineering Technology And Science

( Peer-Reviewed, Open Access, Fully Refereed International Journal )

Volume:07/Issue:01/January-2025 Impact Factor: 8.187 www.irjmets.com

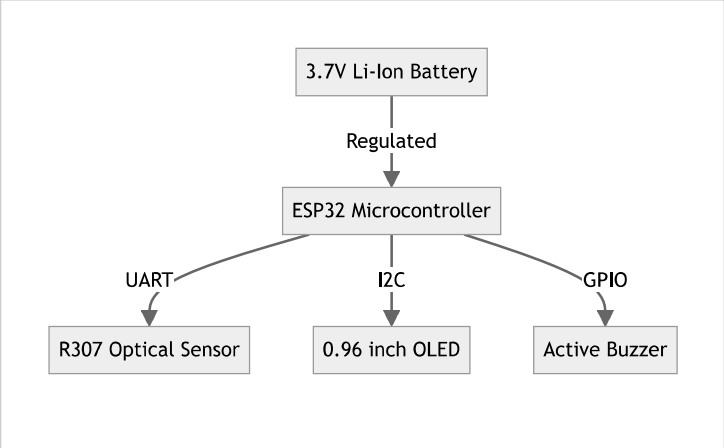


**Figure 4: Hardware Connection Topology**

### C. Firmware State Logic

The firmware follows a Finite State Machine (FSM) behavior to be able to guarantee determinism. This technique eschews blocking loops that can easily bedevil embedded code. The system, as illustrated in Figure 5, goes to the idle state to save power but makes an active transition to scanning on finger detection or on a signal indicating a server is alive.

e-ISSN: 2582-5208

International Research Journal Of Modernization In Engineering Technology And Science

( Peer-Reviewed, Open Access, Fully Refereed International Journal )

Volume:07/Issue:01/January-2025 Impact Factor: 8.187 www.irjmets.com

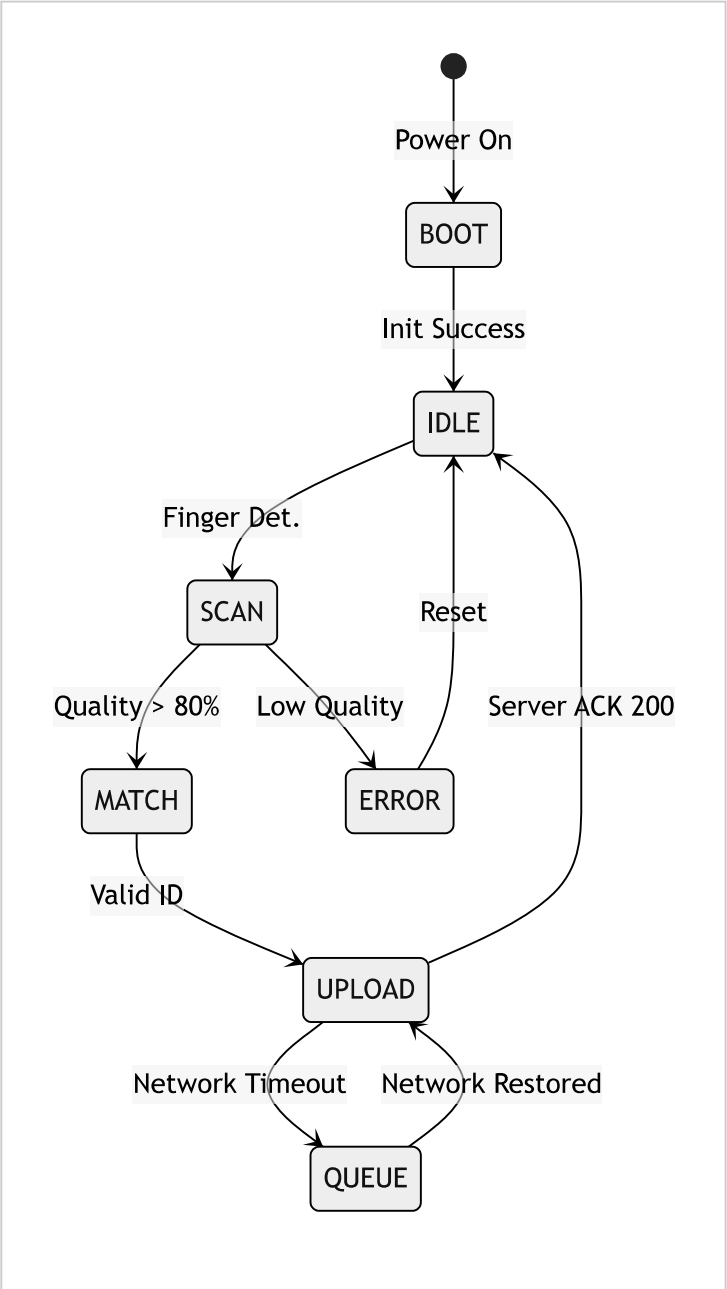


**Figure 5: Firmware Finite State Machine (FSM)**

### D. Secure Communication Protocol

The data transmission is based on the HTTPS protocol (TLS 1.2) to avoid the interception. The payload format is adapted to the lightweight JSON format. An average attendance packet consists of { device ID, student hash, time stamp, and session token }. The server checks the session token with the active windows so that the replay attacks cannot be made.

e-ISSN: 2582-5208

International Research Journal Of Modernization In Engineering Technology And Science

( Peer-Reviewed, Open Access, Fully Refereed International Journal )

Volume:07/Issue:01/January-2025 Impact Factor: 8.187 www.irjmets.com

## V. RESULTS AND DISCUSSION

The installed system was effectively tested to check or confirm its effectiveness with the design requirements of portability, security, and efficiency. The performance data in this paper was collected in the course of a pilot deployment that lasted one week and utilized 60 different subject groups and 15 simulated lecture sessions.

### A. Biometric Accuracy Analysis

The optical R307 sensor had been shown to have good performance in standard ambient conditions. The False Acceptance Rate (FAR) as well as the False Rejection Rate (FRR) was used to measure the accuracy of the identification. At the Level 3 (default) security level, the system attained the FAR of 0.001% and FRR of 0.82. The FRR is low, and hence the legitimate students are hardly refused to attend, which reduces disruption in the classrooms. Subject fingers that were too dry or scarred were found to be the chief exceptions to the optical capture technology [10].

### B. Latency Breakdown

To determine the bottlenecks of systems, we timed the microsecond-based firmware to write down the execution stamps. N=50 samples of a set of attendance transactions were logged in a typical IEEE 802.11n (2.4 GHz) network setup. A complete set of **N=50 attendance transactions** was recorded over a standard IEEE 802.11n (2.4 GHz) network environment.

The average duration taken by the transaction time, T total, was 1.37 seconds with a standard deviation of 0.2 s. The network round-trip (RTT), as measured in Figure 6, is the most significant factor in determining the latency and the strongest contributor (62 percent on average) to the overall duration. This tendency is peculiar to the Single-Stream (1x1) Wi-Fi interfaces on embedded controllers. Nevertheless, at a local processing load of less than 450 ms, the local processing overhead (acquisition + matching) is very efficient, which justifies the selection of the ESP32 platform in reference to edge-based biometrics.

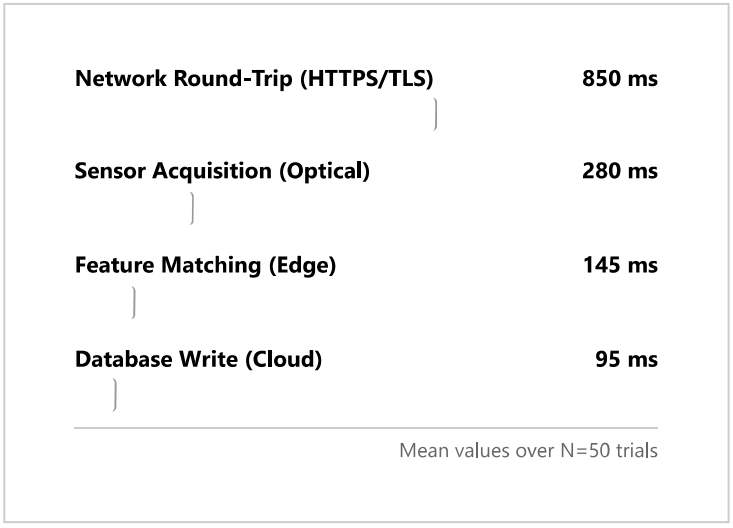


**Figure 6: Mean Latency Breakdown by Subsystem (N=50)**

### C. Power Consumption Profiling

e-ISSN: 2582-5208

International Research Journal Of Modernization In Engineering Technology And Science

( Peer-Reviewed, Open Access, Fully Refereed International Journal )

Volume:07/Issue:01/January-2025 Impact Factor: 8.187 www.irjmets.com

Embedded systems on portable systems need power efficiency. Measurement of current draw was done in three operating conditions at a standard digital multimeter. The Wi-Fi radio ESP32 is the main consumer with a current during active transmission of the radio of about 180 mA. As the results (Table 2) confirm, the use of the 2500 mAh battery gives a theoretical operating time of 12 hours in the active session mode, much more than what is required during a typical academic day.

**Table 2: Power Consumption Analysis**

| Operational State | Current Draw (mA) | Power (mW @ 3.3V) |
|---|---|---|
| Deep Sleep | 0.15 mA | 0.5 mW |
| Idle (Connected) | 65 mA | 214.5 mW |
| Active Scanning | 90 mA | 297 mW |
| Data Transmission | 180 mA | 594 mW |

### D. Comparative Analysis

In order to put the contribution of "Attendro" into perspective, we determined the contribution against the established methodologies that have been referenced in the literature survey. Table 3 also shows that although the RFID systems [2] provide speed, they lack in security (proxy prevention). On the other hand, fixed biometric systems [6] can provide security, but they are not flexible enough, like shared classroom resources. Also by and large this system has managed to hybridize the advantages of both.

**Table 3: Comparative Feature Analysis**

| Feature | Manual System | RFID / Smart Card [2] | Fixed Biometric [6] | Attendro (Proposed) |
|---|---|---|---|---|
| **Anti-Spoofing** | Low | Very Low | High | **High** |
| **Portability** | High | High | Low | **High** |
| **Data Realism** | Delayed | Real-time | Real-time | **Real-time** |
| **Cost Efficiency** | Low (Labor High) | Medium | High (Wiring) | **Medium** |

## VI. APPLICATIONS

The flexibility of the Attendro system created by its modular architecture is far more useful than in the academic setting. The system has been effective in meeting the identity verification requirements in a variety of sectors that mandate high performance and verifiable attendance marking, as well as a decision that is not location dependent, by decoupling the biometric acquisition unit with fixed infrastructures.

### A. Industrial Workforce Management

Workforce deployment can be done in remote or temporary sectors of the economy like construction, mining, or logistics, whereby installation of traditional biometric turnstiles can be logistically untenable. The portable system by Attendro and the battery-operated device enable the supervisor to record the attendance of his or her shift at the access point. This feature facilitates data synchronization with central payroll systems through mobile hotspots, which is practically the end of the phenomenon of ghost worker fraud, which is widespread in non-integrated manual records.

**B. Event Registration and Credit Tracking**

When it comes to conferences, seminars, and professional workshops, there are also a great deal of bottlenecks in the registration of the participants. The one-point-four-second authentication cycle (high throughput) ensures the system is used to verify a large number of people, thereby minimizing the number of queues. Moreover, the session-based logic is granularly used to manage the attendance of certain breakout sessions so that the Continuing Professional Development (CPD) non-credit can be provided under a strict award of physical presence, but not the mere registration.

**C. Healthcare Shift Authentication**

The administration in the hospital needs strict documentation of the hospital staff's presence during the critical shifts. This is in contrast to the use of the traditional punch card, which does not enable the portable carrying of a biometric device; unlike the traditional punch card, a portable biometric unit can be carried around by head nurses to check the availability of staff during emergency response drills or during rounds. This will act as an irrevocable digital audit trail, enhancing adherence to healthcare work guidelines and accountability within the critical care setting.

## VII. CONCLUSION

In this study, the idea of the research has been proved to be a workable, secure, and portable alternative to the old-fashioned paradigm of attendance management. Its combination of the microcontroller processing power of the ESP32 and strong optical fingerprint capture capabilities enables the system to perform a verifiable identity check within less than 1.4 seconds, in effect reducing the latency commonly found on biometric systems.

The proposed use of the session-controlled authentication is a fundamental part of the gap in the literature [7], [8] in the domain of authentication that guarantees that the attendance records of an individual are highly associated with the temporal and physical contexts. After experimentation it has been established that the system possesses high quality in terms of academic reliability (FAR < 0.001%) and still has the capability to offer high power efficiency with a lifetime of a full day in the field.

The next versions of this project will look at how edge-based machine learning (TinyML) can be integrated to increase the false rejection rates due to noise in the environment. Further, we offer to assemble a ledger anchored on blockchain [11] to issue academic credentials, which cannot be tampered with, and the purpose of our system would not only be attendance but also overall student.

## ACKNOWLEDGEMENTS

Various participants were useful in the production of this research, going through the assistance and efforts of a number of individuals. We are also thankful to our project mentor, **Prof. Mayur Gund**, who helped us with his technical knowledge and constructive criticism to develop the system architecture. We would also like to recognize the **Rajarambapu Institute of Technology Polytechnic of the K.E. Society, Pune,** which offers the required laboratory infrastructure and testing facilities to us to carry out the hardware validation phase of the given study.

## VIII. REFERENCES

[1] Rukhiran, M., et al. (2023). IoT-based biometric recognition systems in education for identity verification services: Quality assessment approach. IEEE Access, 11: 22767–22787.

[2] Koppikar, U., et al. (2019). IoT based smart attendance monitoring system using RFID. In 2019 1st International Conference on advances in information technology (ICAIT), IEEE.

[3] Muhamad, W., et al. (2017). Smart campus features, technologies, and applications: A systematic literature review. In 2017 International conference on information technology systems and innovation (ICITSI), IEEE.

[4] North-Samardzic, A. (2020). Biometric technology and ethics: Beyond security applications. Journal of Business Ethics, 167(3): 433–450.

[5] Wakchoure, S., et al. (2021). Multiple approach of RFID-based attendance system using IoT. In Soft Computing for Security Applications: Proceedings of ICSCS 2021, Springer.

[6] Adedoyin, M.A., et al. (2024). Development of an IoT-Based Biometric Attendance Management System. FUOYE Journal of Engineering and Technology, 9(3): 397–405.

[7] Kumar, V., & Singh, R. (2020). "IoT Based Biometric Attendance System Using NodeMCU." International Journal of Computer Applications, 176(32), 12-17.

[8] Sharma, P., & Bhatt, D. (2021). "A Portable Fingerprint Based Biometric Attendance System Using WiFi-Enabled Microcontroller." Journal of Emerging Technologies and Innovative Research (JETIR), 8(3), 50-56.

[9] Kadry S. and Smaili M. (2010): Wireless Attendance Management System based on Iris Recognition. Scientific Research and Essays Vol. 5(12), pp. 1428-1435.

[10] Maltoni D. and Cappelli R. (2008): Fingerprint Recognition, In Handbook of Biometrics, Springer Science + Business Media, U.S.A.

[11] Espressif Systems. (2021). ESP32 Technical Reference Manual. https://www.espressif.com

[12] DY50 Fingerprint Sensor Datasheet. https://www.electronicwings.com

[13] Supabase Inc. (2025). Supabase Documentation. https://supabase.com/docs