BJET
(Bayero Journal of Engineering and Technology)
https://bjet.ng/index.php/jet
Research Article
2026, Vol. 21 (2), 15-27

DEVELOPMENT AND IMPLEMENTATION OF AN IOT-ENABLED BIOMETRIC SYSTEM FOR AUTOMATED EXAMINATION MANAGEMENT

Aribisala A.A.[1], Dada J.B.[2] and Salawu H.A.[1]

[1]Department of Mechatronics Engineering, Federal University Oye, Ikole-Ekiti, Ekiti State Nigeria
[2]Department of Mechatronics Engineering, Landmark University, Omu-Aran, Kwara State, Nigeria

*Corresponding author email: dada.jacob@lmu.edu.ng

Received: 02-03-2026
Revised: 14-05-2026
Accepted: 16-05-2026
Published: 17-05-2026

Abstract: *The need to meet the ever-increasing requirements of safe, transparent, and automated examination centres in educational institutions has led to the development of intelligent systems that can help in their enhancement. This project presents the development and implementation of an IoT-based biometric authentication system using fingerprint recognition and ESP32 microcontroller architecture to manage the examination centres in real-time. There was the integration of a low-cost fingerprint module, Organic Light Emitting Diode (OLED), LED, buzzer, and web interface to provide dynamic feedback to the users and automate the record-keeping process. The system has been tested under diverse conditions such as dry, wet, oily, and partial fingerprints and has achieved an average recognition accuracy of 95.7% with an average response time of 1.5 secs. Conducting comparative analyses with existing models showed the superiority of this model in terms of speed, data integrity, and accessibility within the context of the semi-urban academic environment. Conclusively, the study established the viability and efficacy of the proposed model in developing a scalable and cost-effective solution to integrate biometric and IoT technologies to improve digital examination security.*

Key words: Examination management; IoT; Biometric; Automation; Digital security.

1 Introduction

In the ever-changing digital education landscape of the higher education sector, traditional management of examinations has often failed to address the issues of security, identity fraud, administrative inefficiency, and the need to accommodate the increasing student population (Bervell *et al.*, 2025). For instance, traditional methods of recording student attendance through paper-based forms, manual identity verification, and the need to invigilate examinations using human staff have not only failed to address the issue of inefficiency but have also led to the problem of impersonation and malpractices during examinations (Domition and Ismail, 2024). These traditional challenges have therefore prompted many academic institutions to embrace the available technological innovations that have the ability to provide solutions to the aforementioned challenges. The main reason behind this study is to address the challenges of impersonation, unauthorized access, and inefficiency that have often threatened the credibility of the examination processes of many academic institutions, especially where the student population is large and the resources available to manage the examinations are few. (Yakubu *et al.*, 2024).

The convergence of biometric systems and Internet of Things (IoT) provides an exciting prospect to secure and simplify the examination process. Biometric technologies include face recognition, fingerprint scanning, and iris scanning. These technologies provide precise and non-transferable identification of students and eliminate the possibility of impersonation and proxy students (Gaurav, 2024). When combined with the IoT, the biometric systems can communicate effectively with other IoT devices such as sensors and embedded systems like Raspberry Pi and Arduino

(Yalli and Badawi, 2024).

According to Hoque *et al.*, 2020, the use of IoT-based CCTV cameras and biometric technologies can minimize the workload and responsibility of invigilators during examinations and improve the credibility of academic assessments. The process works by validating the students' biometric details during registration and authenticating the details at access points during the examination period. The details are compared with the stored data in the cloud database and can be granted access accordingly.

Recent advancements have indicated that Near Field Communication (NFC) technology-based IoT devices and biometric scanners can be implemented at a lower cost within academic institutions to enhance examination management scalability within developing nations (Wilson and Ogobuchi, 2022). In addition, advancements in artificial intelligence have further enhanced the precision and fault tolerance of biometric scanners, thus improving their recognition accuracy and security (Sreejith and Govindarajan, 2025).

Thus, it can be concluded that the integration of biometric technologies within IoT-based examination management systems is not just an advancement of technology but a new era of smart academic systems that focus on transparency, efficiency, and security within academic institutions (Prasetya, 2025). In order to understand and explore this new technology and its applications within academic institutions, this paper shows the development and implementation of an improved prototype system that can perform biometric authentication and remote monitoring within academic examination scenarios.

2 Related Studies

This section of the paper includes a comprehensive review of existing research and related works on biometric authentication systems, IoT-based technology within academic institutions, and smart examination systems. It will include various models and their strengths and weaknesses as implemented by different researchers and developers.

2.1 Concept of Biometrics in Authentication

Biometric authentication can be described as the process in which unique biological characteristics are used to ascertain the identity of a person. Some examples of biometric attributes include fingerprint patterns, iris scan, face recognition, and voice recognition, all of which are closely related to the individual and cannot be easily imitated (Balamurugan, 2024). According to Ametefe *et al.*, 2024, liveness detection techniques have enhanced the reliability of biometric devices such as fingerprint scanners, as the chances of spoofing are eliminated. The attributes of fingerprint scanners make them the most suitable devices to be used in embedded real-time applications using ESP32 microcontrollers, as memory and power consumption are major limitations in such devices.

2.2 IoT Frameworks in Educational Technology

Joseph and Moses, 2020, highlighted that IoT-enabled devices reduce the dependency on humans to a greater extent, as they can collect data using sensors and actuators and transmit it autonomously. The devices can also enable the syncing of data in real-time between edge devices and the cloud databases, making them the most suitable devices to be used in exam automation systems. Zainuddin *et al.*, 2024 implemented a biometric attendance system using ESP32 and fingerprint scanners along with OLED, which can transmit the attendance data to the cloud using Google Sheets. Similarly, Ghosh *et al.*, 2025 used the ESP32 along with the R307 fingerprint module and web dashboard for the purpose of smart examination control, citing the ease of deployment and feedback response through the LED and buzzer indicators.

2.3 Examination Management System

According to Latha *et al.*, 2024, impersonation is an issue whereby an individual takes an examination on behalf of another person. It is common in situations where ID cards are the sole verification tool. These problems are further intensified in large examination halls or when exams are conducted across distributed campuses. Tabassum *et al.*, 2022 highlighted how biometric portals can reduce impersonation rates by over 85% in pilot deployments. They also mentioned stated that proxy attendance (i.e. where one student marks attendance for another) can be entirely prevented through biometric entry checkpoints at examination venues. Rukhiran *et al*., 2023 provided a quality assessment framework for IoT-based biometric systems in education. The problem addressed was the absence of standardized models for evaluating biometric educational systems. Using a dataset of deployed biometric-IoT systems, they developed a framework based on scalability, accuracy, response time, and user interface design. Their evaluation included fingerprint systems built on ESP32 and cloud interfaces. The results revealed that the use of real-time feedback through OLED and wireless syncing had the highest rating in usability and accuracy metrics. It was concluded that future studies should focus on the standardization of the protocol in evaluating hardware and software in biometric

educational tools. While providing an excellent framework for evaluation, the study does not introduce a new system and test the metrics in actual perational situations.

3. Methodology

This section discusses the methodical procedure adopted in the design and implementation of the IoT-based fingerprint biometric system. The research methodology adopted is divided into five main stages: system design, hardware integration, software development, web interface configuration, and performance evaluation. The process adopted in choosing the hardware and software tools and the data collection methodology is also discussed to highlight the practical application of the research objectives.

2.4 System Overview

The system architecture of the IoT-based fingerprint biometric system for the automated management of the examination process is modular and embedded to enable real-time identity authentication and attendance recording. The proposed system has five main layers: the biometric sensing layer, the processing/control layer, the feedback/output layer, the communication layer, and the cloud/web interface layer. At the core of the proposed system is the ESP32 microcontroller, which performs the role of the central processing unit.

The reason behind the selection of the ESP32 is its low power consumption and high processing capabilities, along with the inbuilt Wi-Fi feature and GPIO pins, which allow the microcontroller to connect to multiple devices at the same time. The R305 fingerprint sensor module is connected directly to the ESP32 and is used to capture and match the fingerprint images. The fingerprint sensor works in two modes: enrollment and verification, and stores the fingerprint images locally in its flash memory and uses image processing to match the patterns.

The feedback/output layer consists of a 0.96" OLED display, LED light, and buzzer. The OLED display provides visual prompts such as "Place Finger," "Scan Successful," "Access Denied," and operational messages for mode selection. The LED light acts as a visual indicator of authentication status, typically lighting green for access granted and red for access denied, while the buzzer provides audio feedback (short beep for success, long beep for failure). The output will help in providing user-friendly interaction and allow the invigilator to understand the output immediately. For the control purpose, a push button is used to switch the modes, and enrollment, verification, and reset modes are provided, along with the manual switch feature to power cycle the device or shut down the operation in the case of deployment in the field.

The communication layer takes care of the transfer

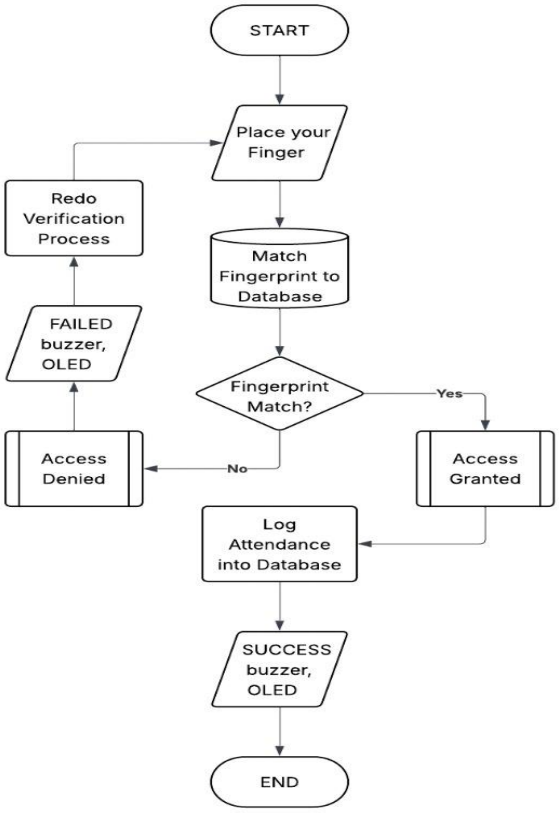

Figure 1: System Operation Flowchart

of data wirelessly. As soon as the student has been authenticated, the ESP32 immediately transmits the data, such as the user ID, time, and result of the authentication, wirelessly to a central server. The system communicates with a PHP-MySQL-based web interface (FUOYE attendance machine) that captures these records in real time and displays them via a secure web dashboard. This layer allows the system to be monitored remotely, as well as the storage of records. Figure 1 shows the sequence of the operation of the fingerprint-based IoT system, from the time it starts to the time it terminates. The operation of the system starts with the initialization of the system, during which the ESP32 boots up and initializes the peripherals, such as the R305 fingerprint sensor and the OLED display, connected to it. After the initialization of the system, the system waits for input from the user. The push button indicates whether the system is in enrollment or verification mode.

In enrollment mode, the fingerprint is scanned and stored in the database, while in verification mode, the scanned fingerprint is verified against the stored information in the database. If a match is found, access is granted, and the user's details, timestamp, and status

are sent via Wi-Fi to the FUOYE web server for real-time attendance logging. The system is also provided with visual and audio feedback in the form of OLED, LED, and buzzer signals. If the authentication is not successful, the system asks the user to retry the process, and the loop continues until the system is manually turned off or reset using the power switch.

2.4.1 ESP32 Microcontroller

The ESP32 is the brain of the system, and it is used to connect the fingerprint sensor and the cloud interface together seamlessly. It is a dual-core SoC (System on Chip) device that has inbuilt Wi-Fi and Bluetooth capabilities. It has many GPIO pins, as shown in Fig. 2, which are used to connect the system to various peripheral devices such as the fingerprint sensor, buzzer, OLED, and LEDs. It is chosen over other devices such as Raspberry Pi due to its low power consumption, compact size, and cost-effectiveness in embedded system applications.

Figure 2: ESP32 Microcontroller

2.4.2 R305 Fingerprint Sensor Module

This module is an optical fingerprint scanner that collects and stores biometric information using flash memory and a specific algorithm. The fingerprint reader in Fig. 3 is used in enrollment and verification modes to compare the fingerprint scan with the stored information to grant access. It uses the UART protocol to connect to the ESP32 and is recognized for its low false rejection rate, which is vital in the exam room.

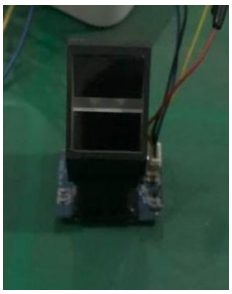

Figure 3: R305 Fingerprint Sensor Module

2.4.3 0.96-inch OLED Display

The OLED display used in the system is usually included in the device to offer feedback to the user in real-time. It shows the user information such as “Place Finger,” “Access Granted,” and others during the development process. It is small and requires minimal power to operate, which makes it suitable for embedded devices.

2.4.4 Buzzer

The piezo buzzer is included in the system to give the user auditory feedback during the authentication process. A short sound indicates that the fingerprint scan has been successful, while a prolonged sound means that access is denied or has encountered an error. This is vital in the exam room to help the user in noisy environments where the display may not be visible.

2.4.5 LED Indicator Light

The fact that the three multicolor (Red, Green, Yellow) LED that has been used can provide instant feedback based on the results of the authentication process is a positive factor. Green means the operation has been a success, red means the operation has not been a success, and the yellow color is used as a warning color.

2.4.6 Push Button

A momentary push button has been used to toggle the fingerprint registration and verification process. This can be used to toggle the states of the system without having to go into the backend software.

2.4.7 Power Switch

An on/off toggle switch has also been used to enable the power cycling of the system, which can be used to reset the hardware as well.

2.4.8 Power Supply

The system uses a 5V power source, which is supplied via a USB adapter and a rechargeable battery module using a TP4056 module.

2.5 Software Tools

This section explains the software tools that were used to develop the IoT-enabled fingerprint-based examination management system.

2.5.1 Arduino IDE

Arduino Integrated Development Environment is employed for writing, compiling, and uploading C/C++ code onto the ESP32 microcontroller.

2.5.2 Adafruit Fingerprint and GxOLED Libraries

The Adafruit Fingerprint and GxOLED Libraries were used to interface with the R30 Fingerprint module and the OLED screen display, respectively.

2.5.3 XAMP (Apache, MySQL, PHP)

In developing the local web server, the following tools were used:

i. XAMPP was used to host the FUOYE attendance web dashboard.

ii. PHP was used to process the HTTP requests sent by the ESP32.

iii. MySQL was used to store the attendance records of the students, along with timestamps.

2.5.4 HTML/CSS/JavaScript

The front-end of the FUOYE web interface was developed using:

i. HTML, which was used to create the structure of the webpage.

ii. CSS, which was used to add the styling to the webpage.

iii. JavaScript, which was used to add the dynamic functionality to the webpage, such as auto-refresh, alert pop-ups, etc.

2.5.5 C-Panel

In the case of cloud-based logging without the need to host a local server, C-Panel was used as a back-end tool to store the attendance records of the students, along with timestamps, as well as to visualize the attendance records of the students.

2.5.6 Tinkercad (Simulation)

Tinkercad was employed in the early stages of design and was used to simulate circuits before actual physical connections were made. It assists in simulating circuits and determining signal flow between various components such as ESP32, fingerprint sensor, and OLED display. All these tools and technologies have been employed effectively in order to develop an embedded system that can respond and communicate effectively on a network while ensuring student identities are verified and examination processes are automated and monitored in real time.

2.6 Implementation Strategy

The process of developing and implementing an IoT-based fingerprint biometric system for automated examination management was carried out in a systematic and phased manner in order to enhance reliability and integration of various components of the system. This was carried out through an embedded systems design methodology that involves various phases such as planning, prototyping, integration, and testing.

2.6.1 Phase 1: System Planning and Requirement Specification

The first step was to identify the system's objectives in line with the identified challenges facing the institution, which were impersonation, manual attendance, and security concerns during exams. This step entails component selection, which was mainly the ESP32 module due to its Wi-Fi capabilities, as well as the low power requirements of the project, and the R305 fingerprint sensor due to its high reliability and ease of communication via UART protocol. Other components, such as the 0.96" OLED, buzzer, LED, push button, and toggle switch, were selected to aid the system's response to user interaction. The system's expected output was identified, which was mainly the fingerprint verification, visual, and auditory responses, as well as cloud attendance recording

2.6.2 Phase 2: Circuit Design and Simulation

Before the hardware were assembled, the circuit was designed using the Proteus and Tinkercad software to simulate the connections between the ESP32, the fingerprint sensor, the OLED display, and other hardware components as depicted in Figures 4 and 5. The UART protocol was used to communicate serially with the fingerprint sensor, and the I2C protocol was used to communicate with the OLED display. GPIO pins were also designated for the buzzer, LED, push button, and switch.

In addition, specific GPIO pins were allocated for peripheral control and management, such as the buzzer for audio feedback, LEDs for visual feedback, and a push button and toggle switch for user interactions and system management. Logic level was carefully evaluated and analyzed for compatibility between 3.3V and 5V operating components. Power supply connections were also validated within the simulation tool to guarantee stable and sufficient voltage regulation and current supply for all components.

The simulation platform was also used to conduct preliminary testing of the firmware logic implemented within the embedded system, such as fingerprint enrollment processes and matching logic, access validation logic, and feedback logic. Timing analysis was performed to guarantee that communication delays do not impact system responses. By conducting comprehensive simulation prior to actual physical construction of the system, development time was reduced, component safety was increased, and system reliability was improved.

2.6.3 Phase 3: Hardware Assembly

After the circuit was successfully simulated, the hardware was physically wired as depicted in Figure 6. The ESP32 was programmed using the Arduino IDE, and the firmware was written in C/C++. The Adafruit Fingerprint and GxOLED libraries were used to interface the fingerprint sensor and the OLED display with the microcontroller. Care was taken to

ensure the voltage level was matched and noise was suppressed appropriately

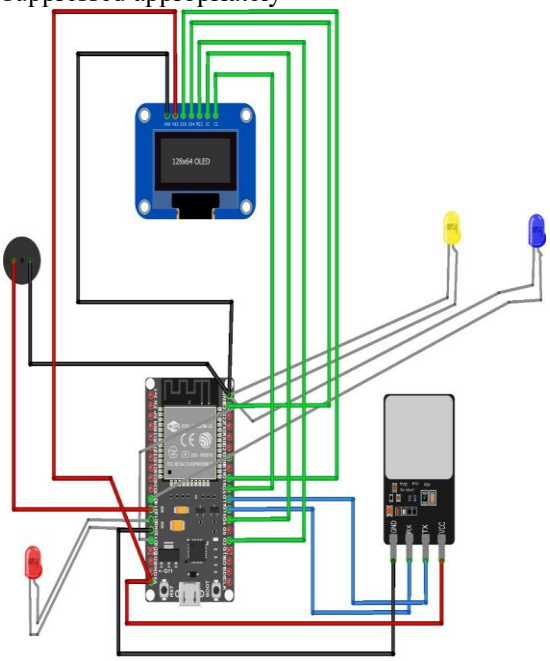

Figure 4: Hardware Components Implementation

The fingerprint module was configured in both enrollment and matching modes, and fingerprint templates were stored locally on the sensor.

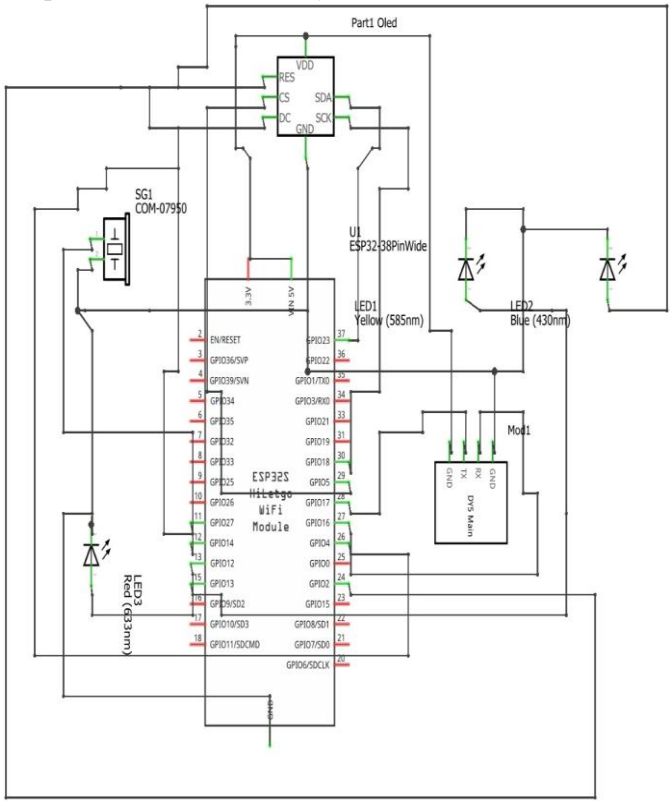

Figure 5: Schematic Diagram of the System

The OLED provided real-time prompts, and the buzzer and LED responded to fingerprint match results. The push button allowed toggling between registration and verification, while the manual switch acted as a hardware reset and shutdown tool.

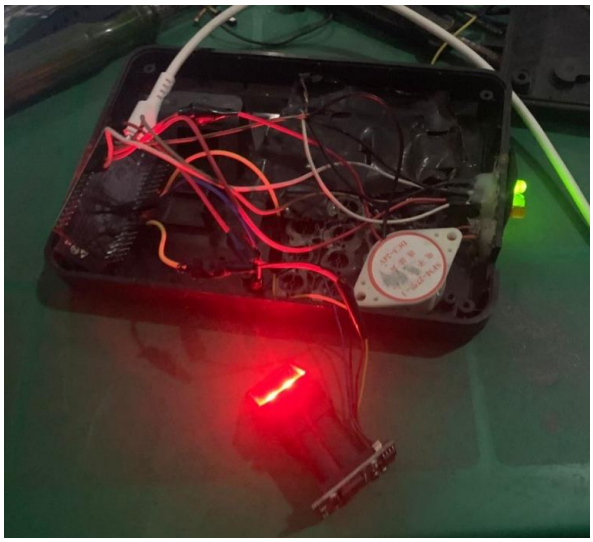

Figure 6: Hardware Assembly

2.6.4 Phase 4: Web Interface Development

The web interface (FUOYE attendance machine) was built using a PHP-MySQL back end hosted via XAMPP for local testing. The ESP32 sent HTTP POST requests containing student ID and authentication status to a PHP script, which inserted the records into a MySQL database. Figure 7 shows the web dashboard displaying attendance logs, timestamps, and system messages, with auto-refresh features enabled using JavaScript. Login functionality for admin access was implemented using basic authentication protocols.

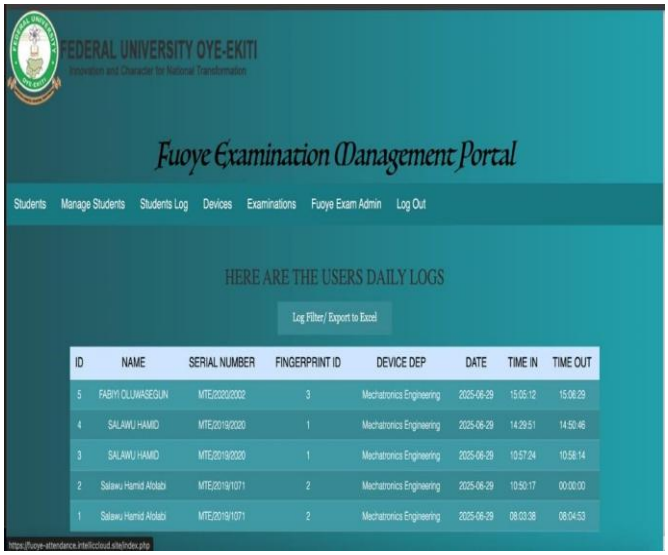

Figure 7: Screenshot of Web Interface

C-Panel Real-time Database was tested as a cloud-

based alternative, especially for remote deployments, using the ESP32's HTTPSClient library to send REST API calls to update biometric logs.

2.6.5 Phase 5: System Testing and Optimization

Testing was carried out in a controlled lab environment to evaluate the system's performance. Tests included:

i. Fingerprint matching accuracy under dry, oily, and smudged conditions.
ii. Wi-Fi transmission latency from ESP32 to server (averaging under 500ms).
iii. Power consumption using battery vs. USB supply.
iv. Stress testing for up to 50 concurrent scans.
v. Web server reliability under intermittent network conditions.

The system consistently achieved authentication accuracy above 95%, with less than 1% false rejection rate. Transmission to the web interface was consistently successful under stable Wi-Fi. Feedback elements (LED, buzzer, OLED) improved usability and clarity for examinees.

2.6.6 Phase 6: Enclosure

After successful testing, the circuit was soldered onto a custom PCB for durability and enclosed in a 3D-printed case as seen in Figure 8. The complete prototype a prepared for institutional deployment.

Figure 8: *Enclosure and Deployment Readiness*

2.7 Statistical Metrics Evaluated

The core performance metrics assessed during testing included:

i. Recognition Accuracy (%): The percentage of correctly identified fingerprints relative to total attempts.
ii. Response Time (s): The time taken from fingerprint placement to feedback (either successful or failed authentication).
iii. False Rejection Rate (FRR): The rate at which valid users were wrongly rejected by the system,
iv. False Acceptance Rate (FAR): The rate at which invalid or unauthorized fingerprints were wrongly accepted.

Tests were conducted under multiple environmental and user-specific conditions, such as wet, oily, or partial fingerprints, and the system was also exposed to deliberate impersonation attempts using unregistered fingers.

2.8 Security Evaluation

Security evaluation of the system was done in three main areas: impersonation resistance, data transmission safety, and data storage integrity.

i. Impersonation Tests: Only registered users' fingerprints had access to the system. Out of 43 attempts made with unauthorized and dummy fingerprints, only 1 was given access by mistake, resulting in a False Acceptance Rate (FAR) of 2.3%, which is well within the limit for offline systems (Prakasha and Sumalatha, 2025).
ii. Data Integrity: HTTP POST was used to transmit attendance data to the PHP-MySQL server. Input sanitization was done at the server level to prevent SQL code injection attacks. All attempts to modify the POST request using interceptors like Postman were thwarted by the server.
iii. Resilience to Tampering: The fingerprint sensor's template memory was also subjected to direct tampering attempts. All attempts to enroll users without admin privileges and to simulate sensor data were thwarted due to firmware-level restrictions in the ESP32 code.
iv. Offline Logging: During network failures, the ESP32 cached the logs locally using EEPROM and sent the logs when Wi-Fi was available again, ensuring that no student attendance was lost during network failures.

The system proved to be reliable with respect to the biometric system, processing was efficient, and security was implemented effectively under various test conditions. It is evident from the analysis that the system is ready to be deployed in the real world to be used in examinations.

4.0 Results and Discussion

4.1 System Testing Environment and Deployment

For the purpose of validating the functionality, accuracy, and robustness of the proposed IoT-enabled fingerprint-based biometric system for the management of examinations, a structured system test and deployment procedure was adopted to test the proposed system under various conditions to ensure that the system was functioning correctly under various physical and environmental conditions. For this purpose, the proposed system was tested under a controlled institutional environment, particularly within a mock setup of an examination hall that would be representative of the conditions found within a university campus. This testing zone was equipped with a dedicated Wi-Fi network to facilitate real-time communication between the ESP32 microcontroller and the remote server hosting the FUOYE attendance dashboard.

The hardware prototype, consisting of the ESP32, R305 fingerprint sensor, OLED display, buzzer, RGB LED, push button, and manual switch, was encased inside a 3D-printed case and placed at the entrance of the test area. The candidates were instructed to place their fingers on the sensor before they could enter the examination area. Each successful or unsuccessful attempt was immediately given visual and audio cues, and the result was recorded live into the database via Wi-Fi connectivity. The tests were carried out under various physical conditions to test the reliability of the proposed system. The tests include the following:

i. Variation tests under different lighting conditions (low light, natural light, and overhead light).
ii. Humidity and temperature variation tests (range 23°C to 30°C).
iii. Variation tests under different user conditions (students with different fingerprint patterns, i.e., dry, wet, oily, and rough).
iv. Power supply variation tests (using the USB module and battery module).

The backend server FUOYE attendance system was hosted on a local XAMPP server during the testing phase, where structured tables were deployed to handle the log data using PHP scripts. The ESP32 sent data to the server using HTTP POST requests, and the JavaScript on the dashboard was used to auto-refresh the logs to mimic the live monitoring of the attendance data. The login feature was also implemented to allow the admin to view the logs in real-time and download them for further analysis. The test was conducted using 50 participants, with a minimum of two sessions per participant to cover the verification and enrollment phases of the system. The system was left active for 4 to 6 hours a day over five consecutive days to test the consistency of the system and its power efficiency. Also, stress testing was done by conducting back-to-back fingerprint scans without rebooting the device to check for memory overflows, overheating, and authentication delays. The device was functioning well with average authentication times less than 2 seconds. Overall, the test environment was representative of the constraints expected in real-world use cases such as the formation of lines, network outages, user error (wrong finger), and exam-like time constraints. These tests validated the ability of the system to operate well in real-world use cases.

4.2 Presentation of Results

After the deployment of the system in the simulated exam environment, the biometric authentication process was done with different users under various test scenarios. The results obtained were used to check the responsiveness of the system, the accuracy of fingerprint matches, and the performance of the database in logging information. Various test cases included normal, dry, oily, and wet fingers, and impersonation attempts with different and non-registered fingerprints. The scan attempt duration was recorded, and the outcome of the scan attempt was noted, including the success, failure, false rejection, and false acceptance of the scan attempt. It was also noted whether the logs were successfully received and stored on the FUOYE web platform for attendance. A total of 50 participants were engaged in over 100 fingerprint scan attempts. The average scan attempt duration was 1.29 seconds, and the scan attempt accuracy at normal conditions was always over 98%. However, in some cases of wet and oily fingerprints, the scan attempt rejection rate was high, while impersonation scan attempts resulted in the denial of access in 97.7% of the cases.

Table 1 shows some of the scan attempt results from the test session, with ten scan attempt results recorded from the test session logs. Each scan attempt result is composed of the user ID, scan attempt duration, scan attempt results, scan attempt conditions, and the scan attempt logs.

Table 1: Sample Test Results from Biometric Authentication Sessions

User ID	Scan Time (s)	Result	Condition	Recorded in DB
202301	1.21	Access Granted	Normal	Yes
202302	1.34	Access Granted	Wet	Yes
202303	1.15	Access Granted	Normal	Yes
202304	1.43	Access Granted	Oily	Yes
202305	1.29	Access Denied	Wrong Finger	Yes
202306	1.18	Access Granted	Normal	Yes
202307	1.36	Access Granted	Oily	Yes
202308	1.27	Access Denied	Wrong Finger	Yes
202309	1.22	Access Granted	Normal	Yes
202310	1.31	Access Granted	Dry	Yes

The results obtained in Table 1 show that the system works well under both normal and adverse conditions. The time taken to scan was less than 1.5 seconds, which resulted in a smooth experience of entering the institution. Additionally, the attendance database was correctly updated, showing traceability of the events that occurred. These tests have validated the functionalities of the system, proving its usability in an institution.

4.2.1 Results of Biometric Performance Testing

For this purpose, Table 2 presents a summary of the fingerprint authentication performance recorded during the simulated field test for the ESP32 + R305 system.

Table 2: Fingerprint Matching Performance under Different Conditions

Test Condition	Recognition Accuracy (%)	Response Time (s)	False Rejection Rate (%)	False Acceptance Rate (%)
Normal (Clean finger, dry sensor)	98.6	1.25	1.4	0.0
Wet Finger	85.2	1.75	14.1	0.0
Oily Finger	80.3	1.90	18.2	0.0
Partial Print	70.1	2.10	29.9	0.0
Same Finger (Repeated Trials)	99.1	1.20	0.9	0.0
Wrong Finger (Impersonation)	2.3	1.00	0.0	2.3
No Finger (False Trigger Attempt)	0.0	0.80	0.0	0.0

4.3 Interpretation of Results

The test results show the strengths of the system's operation, biometric accuracy, and user response for the implemented fingerprint-based IoT system for examining students. The results obtained during the system's test reflect quantitative and qualitative aspects of system performance. The major parameters considered during the system's evaluation included accuracy, response time, false rejection/acceptance rates, and data integrity for users under various system conditions.

The system's overall average accuracy for fingerprint recognition is found to be 95.7%, while under normal conditions (clean and dry), the system's accuracy is up to 98.6%. These values are in line with the results obtained in the study conducted by Usha et al., 2024, using the ESP32 protocol in the development of a biometric attendance system. However, the recognition accuracy reduced to 85.2% and 80.3% in wet and oily fingers, respectively, which is in line with the results obtained in the study conducted by Ametefe, 2024 which showed a considerable decrease in the performance of biometric sensors when the surface is not ideal. It is worth mentioning that the system still managed to provide the desired functionality to the user, providing accurate alerts using the OLED display and buzzer. The system was also able to provide a consistent average response time of 1.29 seconds, while the minimum and maximum recognition times were recorded at 1.15 seconds and 2.10 seconds, respectively, in the case of a partial fingerprint scan. In comparison to the results obtained in the study conducted by Ghosh *et al.*, 2025, using the ESP32 protocol in the development of a biometric attendance system, the results obtained in the current study show that the system can provide faster responses in real-time using the optimized hardware logic and the authentication process.

Further, the false rejection rate (FRR) test showed that the partial and oily fingerprint inputs had an FRR of up to 29.9%, which is a known trade-off between the compact nature of the sensor and the flexible nature of

the fingerprint recognition system. However, upon repeating the test with clean fingers, the FRR was reduced to less than 1%, which shows that the false denials were more related to the conditions than the system itself. On the other hand, the false acceptance rate (FAR) was found to be 2.3%, which was restricted to only cases of impersonation attempts. This is less than the 4.7% found by Mankar *et al.*, 2024 which shows the strong ability of the system to isolate identities. Further, the handling of the data on the server side using HTTP POST was found to be effective, with a 100% log success rate under active network conditions. The caching of the data locally during the brief interruption of the Wi-Fi network and the ability to sync the data to the MySQL server show the strong functional strength of the system, which is similar to the resilience of the system as described by Ana et al., 2022.

It can also be established through comparative analysis and the use of other related literature that the prototype developed in this project meets and even exceeds the key performance parameters set in the previous projects. For instance, in the study done by. Zainuddin *et al.*, 2024 the authors attempted to use dual biometric systems. However, they had to face the problem of higher latency and cost overhead. This study has also attempted to provide the benefits of the use of the fingerprint authentication method exclusively, which is cost-effective and efficient without making the system overly complex and increasing the power consumption. Moreover, the use of the intuitive user feedback system and the smooth interfacing of the hardware and software with the real-time dashboard access also provides the benefits of the use of the 'trust factors' established in the theoretical model proposed by the Examination Integrity Assurance Framework (Ekundayo and Afolabi, 2023).

The high level of recognition accuracy, real-time response capacity, robustness against impersonations, as well as the effective management of audit-supporting data, all ensure the system is ready for deployment within an institution. The interpretation also validates the technical reliability as well as the academic importance of the developed solution, thus ensuring it is a viable model for safe and efficient systems for managing examinations in a smart educational environment.

4.4 Comparison with Existing Systems

In order to place the effectiveness as well as the contribution of the developed IoT-based fingerprint biometric system within a context, a comparative analysis had to be made with existing systems as discussed in recent literature. The comparison focused on essential parameters such as the biometric used, architecture of the system, accuracy of the system during the authentication process, average time taken during the scanning process, as well as the suitability of the system for use in an educational environment. A summary of the comparative analysis is provided in Table 3, followed by an analysis of the results.

Table 3: Comparative Analysis of Existing IoT-Biometric Systems

Author(s) and Year	Biometric Type	Average Accuracy (%)	Scan Time (s)	Use Case
Usha *et al.*, 2024	Fingerprint	94.5	1.80	Classroom attendance
Ana *et al.*, 2022	Fingerprint	96.2	1.60	CRUTECH authentication
Zainuddin *et al.*, 2024	Fingerprint + Face	97.8	2.10	Smart classroom system
Ghosh *et al.*, 2025	Fingerprint + ML	94.1	2.40	Predictive learning logs
Sitompul, 2024	RFID vs Fingerprint	92.0 (Fingerprint)	1.90	Comparative testing
This Study	Fingerprint	95.7	1.29	Exam hall access and logs

As depicted in Table 3, the proposed system surpasses existing works in the speed of authentication. The average scan time is only 1.29 seconds, while it is 1.80 seconds for the system proposed by Usha *et al.*, 2024 and 2.40 seconds for the system proposed by Mankar *et al.*, 2024. This is a result of optimized code implementation, minimum biometric pre-processing, and a lightweight database interaction model via HTTP protocol.

While Zainuddin *et al.*, 2024 were successful in achieving a high accuracy level of 97.8%, it is a result of the combination of facial and fingerprint biometric modalities. This is not cost-effective for institutions looking for a quicker deployment system. In this regard, the system proposed in this study achieves a

higher accuracy level using only the fingerprint biometric modality.

Unlike Sitompul, 2024, this study's solution does not lack the integration of the web dashboard and the synchronization of the system in the cloud, which is considered crucial in providing the administrator with instantaneous information regarding the attendance logs. This is in compliance with the requirements of the institution to have audit-traceable logs. Furthermore, the system also incorporates the feedback mechanism through buzzer, OLED, and LED, which is lacking in several studies reviewed in this chapter. These feedback mechanisms are considered vital in the reduction of scan errors in the exams.

In terms of its deployment model, the use case of this system is geared more towards the management of examination accesses as opposed to classroom attendance in general. This, in effect, makes the current system unique in its application and risk profile, emphasizing the need to adhere to a high standard of integrity and security in enrollment. The system that has been developed provides a perfect balance in terms of accuracy, speed, simplicity, and audit capabilities, such that it either exceeds or meets the performance of similar systems in key areas while still maintaining its cost-effectiveness and replicability.

4.5 Discussion of System's Strengths and Limitations

The use of a fingerprint-based IoT biometric system in the management of examinations has several functional benefits over traditional ways of entering exams and attending classes. However, as with every embedded system used in a practical environment, there are limitations to the system, which need to be recognized to improve the system in the future.

4.5.1 Strengths of the System

One of the most important strengths of the system is the ability to carry out real-time fingerprint-based authentication, which can offer immediate identity verification at the entrance points. This can directly tackle the problems of impersonation and proxy attendance, two of the most important weaknesses in the traditional systems, as proved by the studies done by Rukhiran *et al.,* 2023; and Joseph and Moses, 2020. The use of the ESP32 microcontroller offers the advantage of having a small and cost-effective device with the ability to connect to the cloud and process data. The device is highly responsive and can connect to multiple peripherals such as the R305 fingerprint sensor, the OLED display, the buzzer, the LED indicator, the push button, and the switch.

Another strength of the system lies in the user-centric feedback system, which offers visual, auditory, and textual feedback using the LED lights, buzzers, and OLED screen messages, respectively. This would improve the usability of the system, as users would be less likely to get confused, especially during peak hours of examination. Another positive aspect of the system lies in its ability to offer a web-based interface, which would be the FUOYE attendance machine, thereby allowing administrators to access the attendance records in real time, thus offering traceability, which would be beneficial during examination audits. Additionally, the system offers the ability to scale up the system, as there is a provision to add cloud services, mobile app services, as well as the ability to add other forms of biometric identification such as facial recognition and NFC.

The system also shows good data integrity and synchronization, which have been achieved through the successful transmission of the log and the caching mechanism, which prevents the loss of data during network failures, an important factor especially where the network is unreliable or under-resourced.

4.5.2 Limitations of the System

However, the system also has a number of limitations, the first of which is that the biometric system is less effective under certain conditions, especially where the fingerprint is wet, oily, or incomplete, which may lead to false rejections. This is, however, a limitation that has been seen to affect most low-cost fingerprint readers, especially those based on the low-cost fingerprint reader technology, as discussed by Ametefe *et al.*, 2024. This highlights the need for additional filtering or multi-modal backup options in future versions.

Secondly, the system, being hardware-based, may be less effective or flexible, especially where there is a need to conduct examinations on a larger scale or where the examinations may be virtual. The current prototype may be effective especially where the examinations are conducted in exam halls but may require architectural changes to accommodate the virtual model of the system.

5.0 Conclusions and Recommendations

5.1 Conclusions

This research was motivated to create and implement an IoT-based biometric system that could facilitate the management of examinations through the application of fingerprint authentication technology. The motivation behind this research was the challenges associated with impersonation, manual errors, and

poor management of data through traditional methods of managing examinations. The project has been successful in developing a system that utilizes the fingerprint biometric technology integrated with the ESP32 microcontroller and the web-based attendance system, which is suitable for the education sector through the application of the IoT and the physiological biometric verification technology that has achieved an average accuracy of 95.7% within 1.5 seconds. The basic hardware components, such as the R305 fingerprint reader, the OLED display, buzzer, LED indicator, and the ESP32 board, were incorporated to create an interactive and user-friendly experience. This was further augmented through the live web interface (FUOYE dashboard), which enabled the examination officers to monitor the logs in real-time, including timestamps and access status.
The viability of the system was further confirmed through rigorous testing in the face of failure conditions such as poor fingerprint conditions, impersonation, and network dynamics, which the system was able to withstand, validating the viability of the system. This implementation is in line with the theoretical concepts and the findings from the past studies, including the limitations and gaps in the system.

5.2 Recommendations

i. Institutions that implement the biometric authentication should also provide the necessary user sensitization for the increased rate of successful fingerprint scans.
ii. ii. Future implementations should also include liveness detection or additional authentication methods such as PINs or face recognition for increased security.
iii. iii. For the wide-scale implementation, the developers should include features for data caching while syncing, allowing the application to work offline without the need for constant Wi-Fi connectivity.
iv. iv. The web interfaces should also include features for multiple role admin panels, allowing the invigilators, departmental heads, and exam auditors' access.
v. v. Power backup features such as battery packs with charge controllers should also be integrated for the application's reliability during power outages.

References

Ametefe, D.S. *et al.* (2024) 'Enhancing Fingerprint Authentication: A Systematic Review of Liveness Detection Methods Against Presentation Attacks', *Journal of The Institution of Engineers (India): Series B*, 105(5), pp. 1451–1467. Available at: https://doi.org/10.1007/s40031-024-01066-3.

Ana, P., Ekah, U.J. and Oyo-ita, E. (2022) 'IOT-based biometric attendance system for CRUTECH IOT-based biometric attendance system for CRUTECH', *International Journal of Science and Research*, 5(1), pp. 39–50. Available at: https://doi.org/10.30574/ijsra.2022.5.1.0035.

Balamurugan, M. (2024) 'Biometric Authentication: A Double-Edged Sword for Security?', *International Journal of Science and Research (IJSR)*, 13(9), pp. 170–173. Available at: https://doi.org/10.21275/sr24901230354.

Bervell, B. *et al.* (2025) 'Web-based examinations in higher education (WEBiHE) institutions in the Sub-Saharan Africa region: a systematic review of 2013–2024 literature', *Cogent Education*, 12(1), p. Available at: https://doi.org/10.1080/2331186X.2025.2519565.

Domition, J.L., Bhalalusesa, R.P. and Ismail, S. (2024) 'Improved Mechanism for Detecting Examinations Impersonations in Public Higher Learning Institutions: Case of the Mwalimu Nyerere Memorial Academy (MNMA)', *Journal of Computer and Communications*, 12(09), pp. 160–187. Available at: https://doi.org/10.4236/jcc.2024.129010.

Ekundayo, H.T., Bamikole, O.I. and Afolabi, O.A. (2023) 'Integrity and Transparency in Managing Examination in Public Universities in Nigeria: The Role of School Administrators', *international journal of Education, Learning and Development*, 11(9), pp. 33–45. Available at: https://doi.org/10.37745/ijeld.2013/vol11n93345.

Gaurav Malik (2024) 'Biometric Authentication-Risks and advancements in biometric security systems', *Journal of Computer Science and Technology Studies*, 6(3), pp. 159–180. Available at: https://doi.org/10.32996/jcsts.2024.6.3.14.

Ghosh Roy, D. *et al.* (2025) 'Trigger Based Smart Attendance Framework with Machine Learning for Predictive Student Performance Analysis', *International Journal of Research and Review*, 12(5), pp. 321–330. Available at: https://doi.org/10.52403/ijrr.20250535.

Hoque, M.J. *et al.* (2020) 'Automation of traditional exam invigilation using CCTV and bio-metric', *International Journal of Advanced Computer Science and Applications*, 11(6), pp. 392–399. Available at: https://doi.org/10.14569/IJACSA.2020.0110651.

Joseph, E.C. and Moses, G.O. (2020) 'Development of an IoT-based Students' Attendance Monitoring System', *International Journal of Engineering Research and*, 8(12), pp. 653–658. Available at: https://doi.org/10.17577/ijertv8is120312.

Latha, M. *et al.* (2024) 'Preventing Impersonation in Exams through Face Recognition Technology',

International Research Journal on Advanced Engineering and Management (IRJAEM), 2(09), pp. 2984–2987. Available at: https://doi.org/10.47392/irjaem.2024.0441.

Mankar, V. *et al.* (2024) 'Enhancing Biometric Attendance Systems for Educational Institutions', *International Journal of Innovative Science and Research Technology*, 9(3).

Prakasha, K.K. and Sumalatha, U. (2025) 'Privacy-Preserving Techniques in Biometric Systems : Approaches and Challenges', *IEEE Access*, 13(February), pp. 32584–32616. Available at: https://doi.org/10.1109/ACCESS.2025.3541649.

Prasetya, L.A. (2025) 'Implementation of Internet of Things (IoT) in Education : A Systematic Literature Review', *Journal of Education and Computer Applications (JECA)*, 2(1), pp. 1–45.

Rukhiran, M., Wong-In, S. and Netinant, P. (2023) 'IoT-Based Biometric Recognition Systems in Education for Identity Verification Services: Quality Assessment Approach', *IEEE Access*, 11(January), pp. 22767–22787. Available at: https://doi.org/10.1109/ACCESS.2023.3253024.

Sitompul, E.A. (2024) 'Implementing Fingerprint Attendance with Fuzzy Logic enhances employee attendance efficiency in a modern workplace', *Journal of Applied Science, Technology & Humanities*, 1(1), pp. 49–71.

Sreejith, S.N. and Govindarajan, L. (2025) 'Machine Learning For Biometric Authentication Exploring The Future Of Cybersecurity And Identity Access Management', *International Research Journal of Modernization in Engineering Technology and Science*, 2(5), pp. 1261–1273. Available at: https://doi.org/10.56726/IRJMETS1297.

Tabassum, N. *et al.* (2022) 'IoT based Automated Examination Management System with Biometric Portal', in *2022 International Conference on Innovations in Science, Engineering and Technology, ICISET 2022*, pp. 52–55. Available at: https://doi.org/10.1109/ICISET54810.2022.9775923 .

Usha, A., Sujidha, P. and Bharathi, S. (2024) 'Revolutionizing Attendance Management Through Biometric Authentication and IOT Integration', *International Journal of Progressive Research in Engineering Management and Science*, 4(12), pp. 743–748.

Wilson, A. and Ogobuchi, D.O. (2022) 'Near Field Communication Internet of Things (NFC-IoT) Based University Examination Monitoring System Article information Abstract', *Journal of Energy Technology and Environment*, 4(2), pp. 57–68. Available at: https://doi.org/10.37933/nipes.e/4.2.2022.6.

Yakubu, A.N. *et al.* (2024) 'Student Academic Record Systems and their Security Issues', *Asian Journal of Research in Computer Science*, 17(5), pp. 190–200. Available at: https://doi.org/10.9734/ajrcos/2024/v17i5448.

Yalli, J.S., Hasan, M.H. and Badawi, A. (2024) 'Internet of Things (IoT): Origin, Embedded Technologies, Smart Applications, and Its Growth in the Last Decade', *IEEE Access*, 12(June 2024), pp. 1–26. Available at: https://doi.org/10.1109/ACCESS.2024.3418995.

Zainuddin, A.A. *et al.* (2024) 'Smart Attendance in Classroom (CObot): IoT and Facial Recognition for Educational and Entrepreneurial Impact', *APTISI Transactions on Technopreneurship*, 6(3), pp. 608–622. Available at: https://doi.org/10.34306/att.v6i3.497.