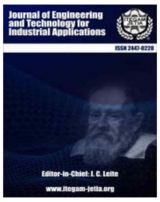
Journal of Engineering and Technology for Industrial Applications

ISSN ONLINE: 2447-0228

ITEGAM-JETIA

Manaus, v.11 n.51, p. 9-19. January/February., 2025.
DOI: https://doi.org/10.5935/jetia.v11i51.1305



RESEARCH ARTICLE OPEN ACCESS

# A FINGERPRINT-BASED ATTENDANCE SYSTEM FOR IMPROVED EFFICIENCY

**Olayiwola Charles Adesoba[1] and Israel Mojolaoluwa Joseph[2]**

[1,2] Federal University of Technology, Akure., Nigeria.

[1]https://orcid.org/0009-0007-1238-2287, [2]https://orcid.org/0009-0005-8802-8730

Email: ocadesoba@futa.edu.ng, josephisrael206@gmail.com

**ARTICLE INFO**

***Article History***
Received: October 24, 2024
Revised: November 01, 2024
Accepted: November 20, 2024
Published: January 30, 2025

***Keywords:***
Radio Frequency Identification (RFID),
Microcontroller,
Recognition,
Bluetooth Low Energy (BLE),
Attendance.

## ABSTRACT

This paper presents the design and implementation of a fingerprint-based attendance system to address challenges in lecture attendance monitoring in developing countries. Leveraging a handheld fingerprint sensor, the proposed system streamlines attendance recording, eliminating manual collection inefficiencies and enhancing record reliability. The system enables lecturers to create and manage attendance sessions effortlessly, while students register and verify attendance conveniently. Key features include automated attendance tracking, reduced administrative burden, and improved accuracy. The system's successful deployment demonstrates its potential to improve operational efficiency and educational outcomes in resource-constrained environments. Results show significant reductions in attendance management time (by 75%) and errors (by 90%), alongside increased student accountability. User feedback indicates high satisfaction rates (95%). The system's effectiveness, usability, and scalability are discussed, highlighting its potential for widespread adoption. This research contributes to the development of efficient and reliable attendance monitoring solutions, providing valuable insights for educational institutions seeking to adopt biometric technology.

## I. INTRODUCTION

Effective attendance tracking is vital for educators to monitor students' academic progress. Traditional attendance methods, however, can be cumbersome and time-consuming. Calling out each student's name in a large classroom can significantly slow down the process. Furthermore, managing attendance records for substantial student numbers can be overwhelming. Another issue arises when students sign on behalf of their absent peers on attendance sheets circulated in class, compromising the integrity of the attendance-tracking process.

To ensure students' academic success, prioritizing efficient attendance tracking is vital. It's encouraging to see numerous institutions adopting digital attendance systems. However, many institutions of higher learning worldwide still rely on outdated paper-based methods [1].

Therefore, it's important to encourage the adoption of modern technology and efficient attendance tracking systems to improve productivity and ensure the academic success of students. This study presents a biometric attendance system with a fingerprint feature which is portable and eliminates the weak point of using the existing method of marking attendance on paper or standing in long queues. Few of these other automated systems are attendance facial recognition systems, attendance RFID scanning systems, attendance iris scanning systems, and many others.

While facial recognition is a straightforward feature for automated attendance system, it is, however, often less effective as the standard facial recognition techniques embed inherent drawbacks that affect prima facie verification and enrollment features [2].

An example of such biometric recognition techniques is iris recognition whereby images of the iris patterns of either one or both of the eyes of a certain individual are taken and scanned employing some mathematical pattern recognition systems that are very stable and unique and can be obtained from a certain distance [3].

Corporate radio frequency identification (RFID) technologies include a system for noncontagious data transfer [4]. The system employs an RFID tag and RFID reader where the RFID TAG has a unique ID number for each tag. While this form of attendance system is efficient, it can also undermine the purpose of attendance by permitting proxy attendance. This research proposes the design of an access control system which incorporates an ESP32 microcontroller with integrated Wi-Fi and an R305 fingerprint module. The R305 finger print scanner is equipped with a good performance image sensor which captures the finger image and analyzes it in milliseconds with an inbuilt memory of one thousand fingerprints. Each and every person will have to be given an ID number that will be captured during the enrolment of fingerprints. The ESP8266 Wi-Fi module is used for setting up an access point through which the client can link to the device. The client application is developed utilizing Node.js, an open-source JavaScript platform, and MongoDB is employed for database management.

MongoDB which is a Document-oriented database is used to store unstructured data contrary to Structured query language (SQL) which is relational database. It is a document oriented database, which is characterized by high speed and volume efficiency. This type of database works by grouping data into collections and keeping them in documents [5].

The document-oriented database is one of the non-relational databases, which are built in solutions that address the modern day's problems of large amounts of new categories of data being generated that have a possibility of being changing rapidly as well. These databases offer efficient query mechanisms, flexible querying capabilities, and seamless integration with modern programming languages through a natural document-data-model-to-object mapping [6].

Under the working conditions, the device is capable of authenticating a person by fingerprint and uploading the attendance with the time stamp to the client machine. Biometric attendance systems offer improved security, accuracy, and efficiency over traditional methods, reducing human error and enhancing data integrity. These systems use pattern recognition to capture biometric data, extract features, and compare them to a database for unique identification.

Recent advancements have expanded beyond fingerprint recognition to include facial recognition, iris scanning, GPS tracking, and voice recognition. Finger imaging remains widely accepted for identification [7]. GPS tracking requires users to install an APK and input office coordinates for automatic data transmission [8].

While facial recognition shows promise, it has accuracy issues due to factors like aging and posture [9],[10]. Automated systems continue to evolve, incorporating methods like fingerprint matching and data transmission via Zigbee [11].

## II. MATERIALS AND METHODS

Fingerprint identification is one of the most well-known and common biometric identification systems. Because of their uniqueness and consistency over time, fingerprints have been used for identification for over a century, more recently becoming automated due to advancements in computing capabilities. The system will maintain a record of the fingerprints of various students in the database, and they will be matched and marked present when they place their finger on the fingerprint sensor. In designing the proposed system, both software and hardware implementations are required.

The design is divided into five sections: the power source section, control and LCD section, fingerprint section, indicator section, and IoT communication section. The block diagram in Figure 1 illustrates the methodology of the proposed system.

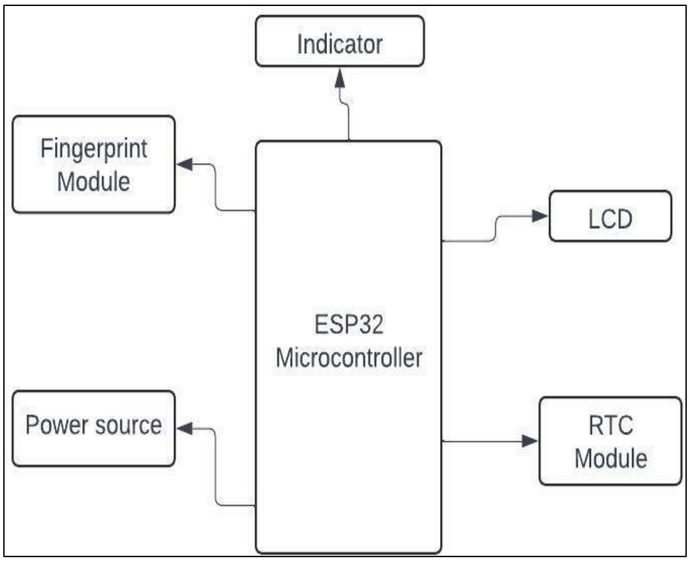


Figure 1: Block Diagram of the Proposed System.
Source: Authors, (2025).

The control and display section are formed by ESP32 System on Chip (SOCs) microcontroller and an alphanumeric LCD display. The biometric scanner section is an optical fingerprint scanning module R305, and DS3231 RTC Module is the IoT communication section, and buzzer 5v and LED 5mm for indicator section. Thepower source is a 3.7v 18650 lithium battery with 5 V power bank charger regulator.

### II. 1. COMPONENTS UTILIZED

The following components were used for the overall setup of the hardware device. Here is a brief description of what each component does in the complete hardware.

a) ESP32-WROOM-32 Microcontroller

This specific module is quite interesting due to its flexibility and efficiency which is the reason as to why it fits perfectly into fingerprint biometric attendance system. To its high performance AS GTX8266, Espressif Systems, almost tops the chart among the WE MOVED Boards with superior dual-core, 32 bits, LX6 microprocessor at clock speeds of about 240 MHz: a very reasonable overclock for intricate processes. The module has built in wireless communication modules that includes Wi-Fi and Bluetooth which is essential for this device. Only the microcontroller has SRAM of 520 kb and 448 kb of ROM making it bulky in processing and storage memory. The consumption of low powers, thanks to TSMC's 40nm technology has been optimized making the chip useful in the case of portable devices and battery powered devices. The peripherals that ESP32-WROOM-32 can interface with includes, but are not limited to, capacitive touch interfaces, SD cards and Ethernet, which greatly expands the applications. Moreover, the module has several I/Os, ADCs, DACs, PWM outputs giving the ability to connect different types of sensors and actuators. Built in security features such as secure boot and flash encryption provide basic protection against data loss. In one word, the creation of smart and efficient attitude control system based on fingerprint biometric attendance system can be easily achieved in the framework of the ESP32-WROOM-32 (Figure 2).

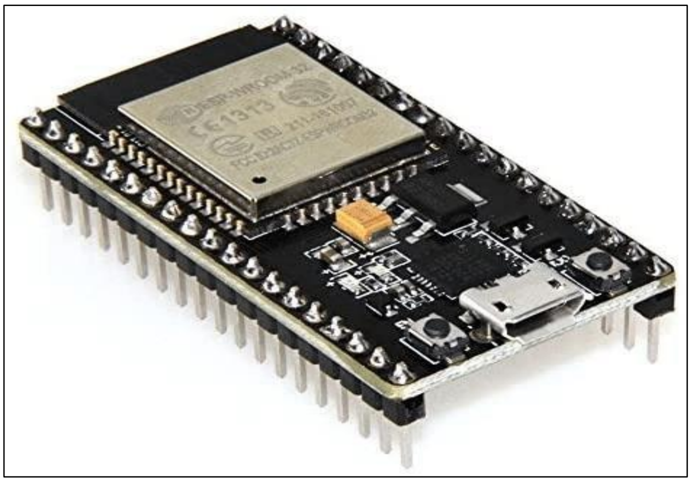


Figure 2: ESP32 Microcontroller.
Source: Authors, (2025).

b) 16x2 LCD Display with 12C

This display module shows real-time information such as attendance status, error messages, and prompts, enhancing user interaction and system feedback. The I2C interface simplifies wiring byreducing the number of pins required for connection, making it easier to integrate with microcontrollers like the ESP32. Additionally, the I2C interface allows for efficient communication between the LCD and the microcontroller (Figure 3).

In a fingerprint attendance system, this display can show messages like “Sending FP data,” “Access Denied,” or “Error in image,” providing immediate feedback to users. It can also display the current date and time, sourced from the RTC module, ensuring users are aware of the system’sstatus at all times. This enhances the overall user experience and makes the system more intuitiveand user-friendly.

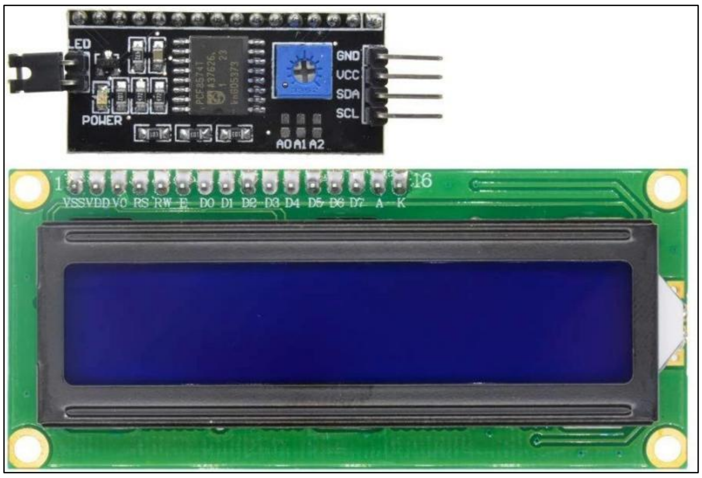


Figure 3: 12864 LCD 16x2 and I2C Adapter.
Source: Authors, (2025).

c) DS3231 RTC Module

The DS3231 RTC (Real-Time Clock) module is a highly accurate timekeeping device, ideal for use in a fingerprint attendance biometric system. Unlike the DS1307, the DS3231 has an integrated temperature-compensated crystal oscillator, which ensures precise timekeeping even in varying environmental conditions. This makes it particularly reliable for applications where accurate time and date stamps are crucial. It relies on a backup battery to maintain accurate timekeeping even when the main power is off. If you remove this battery, the module will lose its timekeeping dataand reset. This means that when the power is restored, the DS3231 will no longer have the correcttime and date information. In a fingerprint attendance system, the DS3231 ensures that each fingerprint scan is accurately timestamped. This module communicates with microcontrollers like the ESP32 via the I2C protocol, using just two pins (SDA and SCL). When a user scans their fingerprint, the system logsthe exact time and date of the scan, which is then stored in a database (Figure 4).

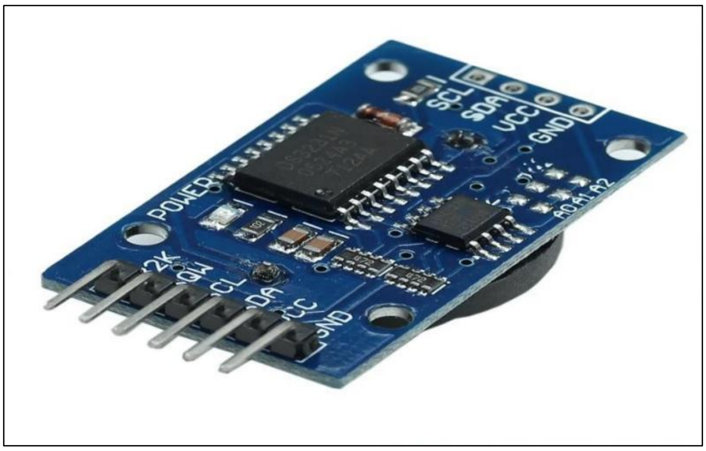


Figure 4: DS3231 RTC Module.
Source: Authors, (2025).

d) JM101B Fingerprint Module

The JM101B fingerprint module is an integrated optical fingerprint processing module, ideal for use in a fingerprint attendance biometric device. This module combines the optical path and fingerprint processing components into a compact unit, making it suitable for space-constrained applications. It features low power consumption, a simple interface, and high reliability, which are crucial for continuous operation in attendance systems. The JM101B module (Figure 5) communicates with microcontrollers like the ESP32 via UART, making it easy to integrate into your project. It has a high recognition speed and good adaptability to both wet and dry fingers, ensuring accurate and quick fingerprint identification. When a user scans their fingerprint, the module captures the fingerprint image, processes it, and compares it with stored templates to verify the identity of the user.

Figure 5: JM101B Fingerprint Module
Source: Authors, (2025).

e) 18650 Lithium Battery

The 18650-lithium battery is a popular rechargeable lithium-ion cell, named after its dimensions:18mm in diameter and 65mm in length. 18650 batteries can provide a reliable and portable powersource (Figure 6).

Figure 6: 18650 Lithium Battery.
Source: Authors, (2025).

f) Power Bank 18650 Charger

The power bank module can convert the 3.7V output to a stable 5V, suitable for powering components like the ESP32 microcontroller, fingerprint sensor, etc. (Figure 7).

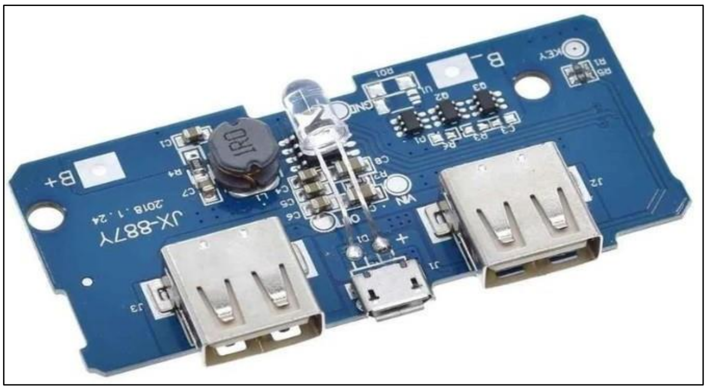


Figure 7: Power Bank 18650 Charger
Source: Authors, (2025).

## II. 2. HARDWARE DESIGN

A modular design approach was used. Connectors were employed to interface different components wherever possible, facilitating better assembly and easier repair in the future. The microcontroller used in this design is the ESP32-Wroom-32. A fingerprint module is connected to the Universal Asynchronous Receiver-Transmitter (UART) interface, linking the transmitter and receiver pins of the module to those of the microcontroller. A bi-color LED indicates the status of fingerprint authentication. The graphic LCD's data connectors, control signal connectors, and power signal connectors are interfaced with the microcontroller circuit. The backlight of the graphic LCD is controlled through a microcontroller port, allowing it to be adjusted as needed. A USB type-A female connector is connected to the ESP32 using a USB module. The system uses an RTC DS1307 to keep track of time, interfaced with the ESP32-WROOM-32 via the I2C protocol. A 3V CR2032 CMOS battery serves as a backup. Figure 8 shows the circuit schematic of the device.

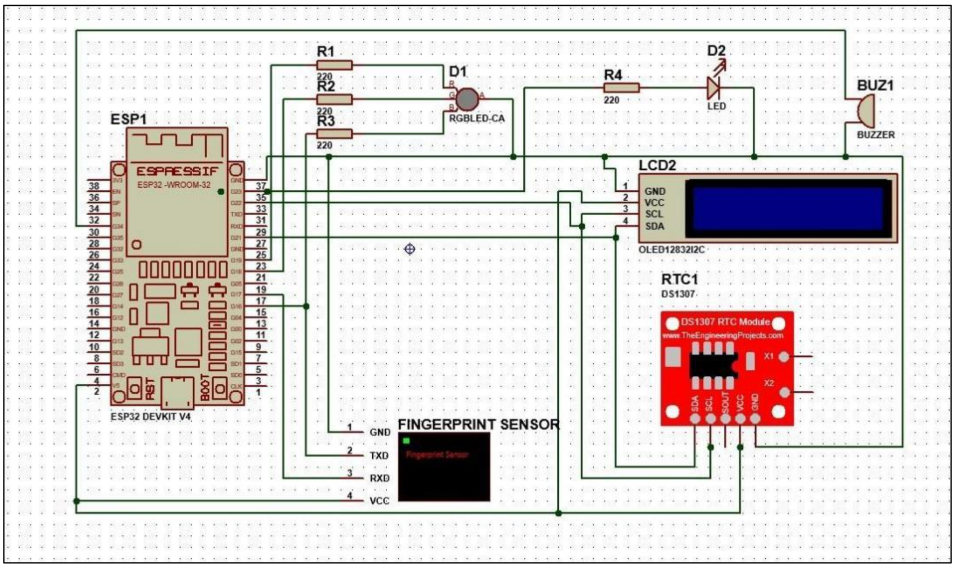


Figure 8: Circuit Schematic of the Device
Source: Authors, (2025).

The study employed the Bluetooth Low Energy (BLE) protocol for data transmission of fingerprints due to its advantages in low power consumption and efficient data transfer. BLE is widely used in applications requiring minimal energy usage, making it an ideal choice for devices that need to operate for extended periods on small batteries. This characteristic is crucial in environments such as wearable technology, IoT devices and health monitoring systems where battery life is a critical concern. One of the key advantages of BLE over other wireless communication protocols such as Wi-Fi, Zigbee or classic Bluetooth is its power efficiency. BLE operates by transmitting small data packets at intervals, sometimes as low as once per second, which significantly reduces the power required for communication [12]. BLE also supports a large number of devices connected simultaneously, often referred to as a mesh network, which is particularly advantageous in IoT environments where multiple sensors and actuators need to communicate with a central hub or among themselves [13]. These characteristics make it an ideal choice for this research.

The system utilizes the R307 optical fingerprint verification module which features a high-powered DSP chip for image rendering, calculation, feature-finding and searching. This module offers high sensitivity and accuracy with a resolution of 500 DPI. The R307 module is interfaced with a microcontroller via TTL serial communication, enabling data packet transmission for image capture, print detection, hashing, and searching. The Adafruit Fingerprint Sensor Library is employed to interact with the fingerprint module, providing functions for fingerprint enrollment and verification. Further details on the pinout connection are provided in Table 1.

Table 1: Pinout Connection to Fingerprint Module.

| FINGERPRINT SENSOR | ESP32 |
|---|---|
| VCC | 5V (RED WIRE) |
| TX | GPIO 17 (YELLOW WIRE) |
| RX | GPIO 16 (WHITE WIRE) |
| GND | GND |

Source: Authors, (2025).

The R307 fingerprint module was connected to the ESP32 microcontroller by establishing the following connections: the VCC pin of the R307 was connected to the 5V pin on the ESP32, providing the necessary power for operation. The TX (transmit) pin of the R307 was connected to GPIO 17 on the ESP32, enabling data transmission from the fingerprint module to the microcontroller. The RX (receive) pin of the R307 was connected to GPIO 16 on the ESP32, allowing the microcontroller to receive data from the fingerprint module. Finally, the GND pin of the R307 was connected to the GND pin on the ESP32, completing the electrical circuit and ensuring a common ground between the two devices.

The system features a 16x2 LCD display module, which provides a user interface for feedback and information display, including prompts, status messages and attendance status. The LCD display utilizes an i2c interface, reducing the required pins to four and enabling easier integration. Additionally, the display includes a built-in potentiometer for adjusting contrast between the background and characters. The LiquidCrystal_I2C library (version 1.1.2) in Arduino IDE was employed to interface with the display, offering functions for initialization, cursor positioning and text printing. The pinout connection details are provided in Table 2.

Table 2: Pinout Connection to I2C LCD.

| LCD WITH I2C | ESP32 |
|---|---|
| VCC | 5V |
| GND | GND |
| SDA | GPIO 21 |
| SCL | GPIO 22 |

Source: Authors, (2025).

To establish communication between the i2c interface and the ESP32 microcontroller, the VCC pin of the i2c interface was connected to the 5V pin on the ESP32, providing the necessary power for the fingerprint module to operate. The SDA pin was connected to GPIO 21 on the ESP32, enabling data transmission from the fingerprint module to the microcontroller. The SCL pin was connected to GPIO 22 on the ESP32, allowing data reception from the microcontroller to the fingerprint module. Finally, the GND pin of the i2c interface was connected to the GND pin on the ESP32, completing the electrical circuit and ensuring a common ground between the two devices. These connections enable the ESP32 microcontroller to communicate with the fingerprint module via the i2c interface, allowing for data exchange and fingerprint recognition. The use of GPIO 21 and GPIO 22 on the ESP32 ensures reliable data transfer while the common ground connection prevents data corruption and ensures a stable power supply.

The DS3232 RTC module was employed to obtain current time, date and day for the fingerprint reader. This module maintains accurate time even during power outages, ensuring proper time stamping of attendance records. The RTClib library (version 2.1.4) in Arduino IDE was used to interface with the DS3232, providing functions to read and set the time and date. The pinout connection details are provided in Table 3.

Table 3: Pinout connection to RTC Module.

| LED WITH 220 Ω RESISTOR | ESP32 |
|---|---|
| RED | GPIO 19 |
| BLUE | GPIO 23 |
| GREEN | GPIO 18 |
| BLUE | GPIO 16 |

Source: Authors, (2025).

To interface the DS3232 Real Time Clock (RTC) module with the ESP32 microcontroller, the VCC pin of the RTC module was connected to the 5V pin on the ESP32, providing the necessary power for the module to operate. The SDA pin was connected to GPIO 21 on the ESP32, enabling data transmission from the RTC module to the microcontroller. The SCL pin was connected to GPIO 22 on the ESP32, allowing data reception from the microcontroller to the RTC module. Finally, the GND pin of the RTC module was connected to the GND pin on the ESP32, completing the electrical circuit and ensuring a common ground between the two devices. These connections enable the ESP32 microcontroller to communicate with the DS3232 RTC module, allowing for accurate time and date retrieval. The use of GPIO 21 and GPIO 22 on the ESP32 ensures reliable data transfer while the common ground connection prevents data corruption and ensures a stable power supply. The device employs two LEDs for status indication: a power LED and a status LED. The power LED indicates the power status while the status LED displays the fingerprint status. A RGB LED and a blue LED with a 220Ω resistor are used to provide visual indicators. The pinout connection details are provided Table 4.

Table 4: Pinout Connection to LEDs.

| D3231 RTC | ESP32 |
|---|---|
| VCC | 5V |
| GND | GND |
| SDA | GPIO 21 |
| SCL | GPIO 22 |

Source: Authors, (2025).

The RGB LED and additional blue LED were connected to the ESP32 microcontroller. The red LED (RGB) was connected to GPIO 19, enabling the microcontroller to control the red color. The green LED (RGB) was connected to GPIO 18, allowing the microcontroller to control the green color. The blue LED (RGB) was connected to GPIO 23, enabling the microcontroller to control the blue color. Additionally, a separate blue LED was connected to GPIO 16, providing an extra indicator. These connections enable the ESP32 microcontroller to control the RGB LED and additional blue LED, allowing for visual indicators of various statuses and notifications. The use of GPIO pins ensures reliable communication between the microcontroller and LEDs.

The device incorporates several user interface and feedback mechanisms to enhance user experience and provide effective communication. A push button is used for resetting the system, allowing for quick reinitialization in case of errors or malfunctions. This ensures that the system can be easily restored to its default state. A buzzer provides audible feedback when a student places their finger on the fingerprint sensor, indicating successful or failed scans and enhancing user interaction. Additionally, a power ON button enables easy switching of the system on and off, providing users with control over the system's operation. These mechanisms work together to create an intuitive and user-friendly experience, ensuring effective interaction and clear feedback on the system's status.

## II. 3. SOFTWARE DESIGN

The Waterfall model was employed as the software development lifecycle to enhance the automated attendance system with a fingerprint-based approach in this study. The model's structured and sequential process ensured that each phase of development was completed before progressing to the next, thereby maintaining clarity and order throughout the study's duration. The linear approach of the Waterfall model facilitated a logical and methodical development process, which was particularly suited for this research's requirements. The features of the mobile application and programming languages implemented are discussed below:

a) Frontend Development

The frontend of the attendance system was developed using React Native, an open-source User Interface (UI) software framework created by Meta Platforms, Inc. [14]. React Native enables the development of native mobile applications for iOS and Android using JavaScript and React. Specifically, it was utilized to create the mobile application for this study. For biometric authentication, the react-native-biometrics package was employed, providing a simple bridge to native iOS and Android keystore management. This allows for the creation of public-private key pairs stored in native keystores and protected by biometric authentication. Furthermore, React Native's robust ecosystem offers various libraries and packages, such as react-native-ble-plx, which enables communication with devices and sends fingerprint data to the database. By leveraging React Native and its associated packages, the frontend development was streamlined and a seamless user experience was achieved.

b) Backend Development

Node.js was utilized as the backend technology to develop a server for handling authentication requests, interacting with MongoDB for data storage and retrieval, and managing application logic. Node.js is a cross-platform, open-source JavaScript runtime environment that leverages the V8 JavaScript engine, which powers Google Chrome, to achieve exceptional performance. The non-blocking, event-driven architecture of Node.js enabled the handling of thousands of concurrent connections without creating new threads for each request. This allowed for efficient use of system resources and improved responsiveness. The standard library's asynchronous I/O primitives prevented JavaScript code from being blocked, ensuring that I/O operations such as database access and network reads did not waste CPU cycles. By employing Node.js, this study effectively harnessed its benefits to develop a scalable and efficient backend system.

c) Database Selection and Design

MongoDB, a NoSQL database was selected for its flexibility in storing and retrieving large volumes of data, a critical requirement for managing attendance records in the system. Unlike traditional relational databases, MongoDB offers a document-oriented format for storing unstructured data, allowing for greater adaptability to the project's evolving needs. Each attendance record is stored as a document containing fields such as user ID, timestamp and metadata, facilitating easy querying and analysis. Moreover, MongoDB's scalability ensures that the system can efficiently handle an increasing number of records as the user base grows, without compromising performance.

## III. SYSTEM MODELING DIAGRAMS

## III. 1. FLOWCHART DIAGRAM

The flowchart depicted in Figure 9 illustrates the sequential steps involved in the fingerprint attendance system. The process initiates with *Enrollment*, where a new user registers their biometric fingerprint data. During enrollment, the user places their finger on the fingerprint sensor, capturing a fingerprint image. This image is then securely stored in the database. Once enrolled, the user marks their attendance by placing their finger on the sensor. The system compares the captured fingerprint with the stored template. If the fingerprints match, the user's identity is verified and their attendance is recorded in the database along with the time and date. In cases of non-matching fingerprints, the system displays an error message or prompts the user to try again.

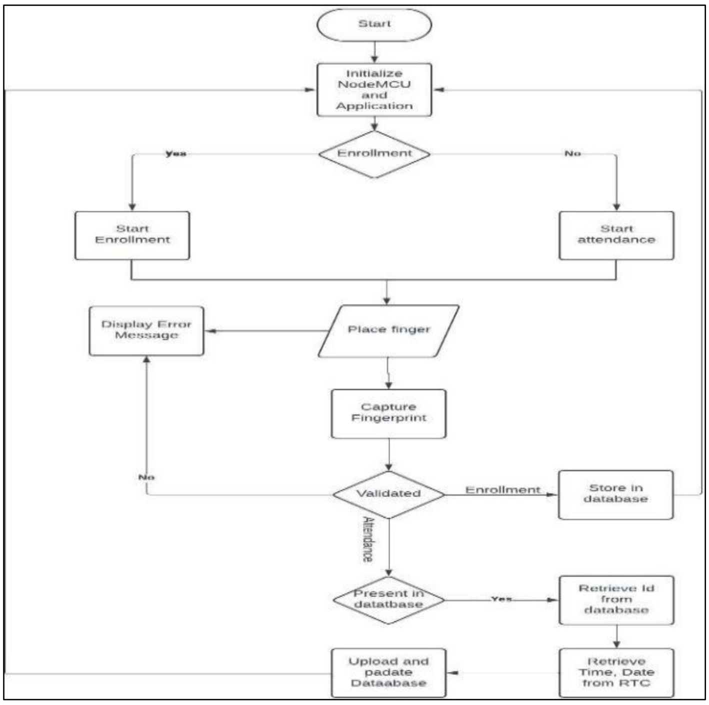


Figure 9: Flowchart of the entire system.
Source: Authors, (2025).

### III. 2. DATAFLOW DIAGRAM

The Data Flow Diagram (DFD) provides a visual representation of the fingerprint attendance system's data flow, illustrating the interaction between various components. Figure 10 details this diagram. The DFD utilizes standardized symbols to represent four primary elements: inputs, which are external data sources including student information and attendance records; processes, which are actions performed on the data such as fingerprint capture, identity verification and attendance recording; data stores, which are locations where data is stored including databases and files; and outputs, which are the final results produced by the system including attendance reports and notifications. Arrows in the DFD indicate the direction of data flow between these components, facilitating a comprehensive understanding of data collection, processing, and distribution within the system (Figure 10).

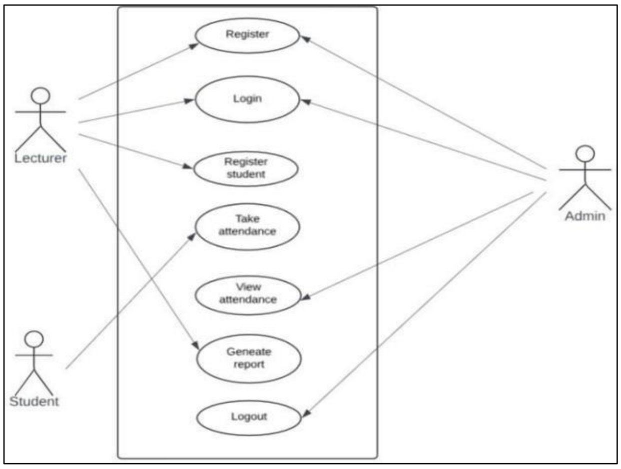


Figure 10: Dataflow for the Database.
Source: Authors, (2025).

### III. 3. USE CASE DIAGRAM

The use case diagram provides a visual illustration of user interactions within the fingerprint biometric attendance system. Ovals represent distinct system actions, such as "Register Student," "Verify Attendance," and "Take Attendance," while lines link these actions to their corresponding system users, also known as actors (students, administrators and lecturers). This visualization clearly maps user roles and system interactions, offering an instant understanding of the system's functionality and user engagement (FIgure 11).

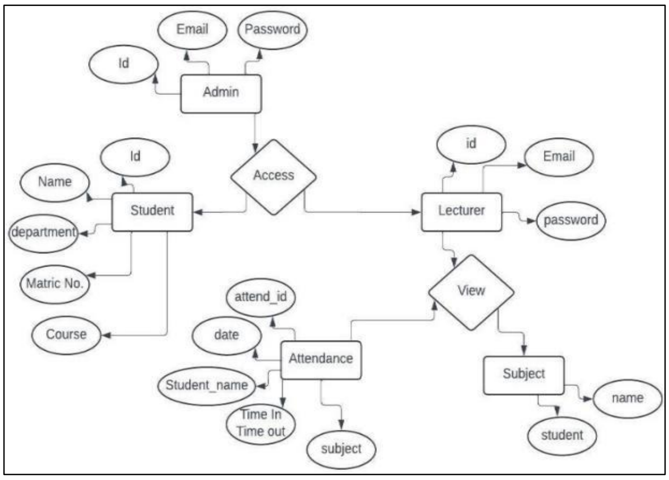


Figure 11: Use Case of the Mobile Application.
Source: Authors, (2025).

## IV. RESULTS AND DISCUSSIONS

### IV. 1. IMPLEMENTATION OF THE NEW SYSTEM

The deployment of the fingerprint-based attendance system encompasses multiple phases, integrating hardware components, software applications, and data flow to ensure seamless functionality. The system architecture consists of a fingerprint scanning device linked to an application responsible for recording and managing attendance data. This application features a user-friendly interface, enabling lecturers to effortlessly view and manage attendance records.

a) Hardware Setup

The experimental setup consisted of the installation and configuration of the JMI01B fingerprint sensor connected to the ESP32 microcontroller. Supporting components integrated into the system included an RTC module, 16x2 LCD display, and RGB LEDs. Power supply management was achieved using two 3.7V LiPo batteries connected in series with an 18650-power bank module. The experimental setup is as shown in Figure 12.

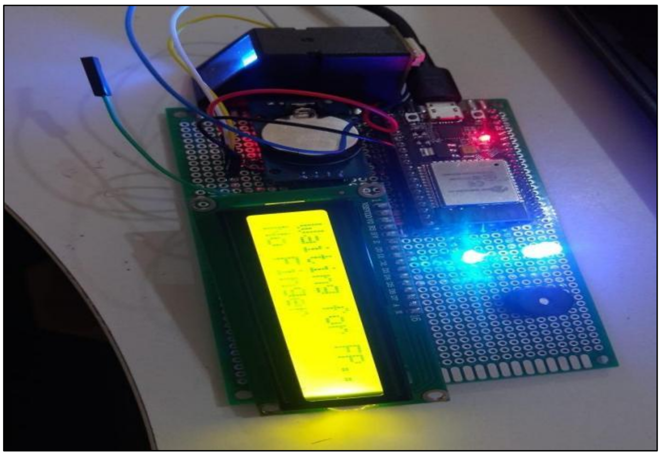


Figure 12: Device Setup.
Source: Authors, (2025).

b) System Architecture and Deployment

The proposed attendance management system's architecture comprises a backend server and a mobile application. The backend server leverages MongoDB for data storage and Node.js with Express.js for API endpoint configuration, handling fingerprint data registration, student attendance tracking and attendance retrieval. The backend server is deployed on Render's cloud server. The mobile application, built using React Native, facilitates student registration and attendance management through real-time data transmission with the fingerprint device via BLE communication, implemented using the React Native BLE PLX library. The application's user interface prioritizes intuitiveness, ensuring easy access to attendance lists for lecturers.

c) System Integration and Validation

The developed system underwent rigorous testing to validate hardware-software communication and backend-frontend synchronization. Hardware-software communication was verified by confirming the successful transmission of fingerprint data from the device (Figure 13) to the ESP32 microcontroller and subsequently to the mobile application via BLE. Data flow validation ensured reliable transmission to the backend server. Backend-frontend synchronization was achieved through thorough testing of application-backend API interactions, ensuring data consistency. Student records and attendance logs were synchronized in real-time, enabling lecturers to access accurate and up-to-date information.

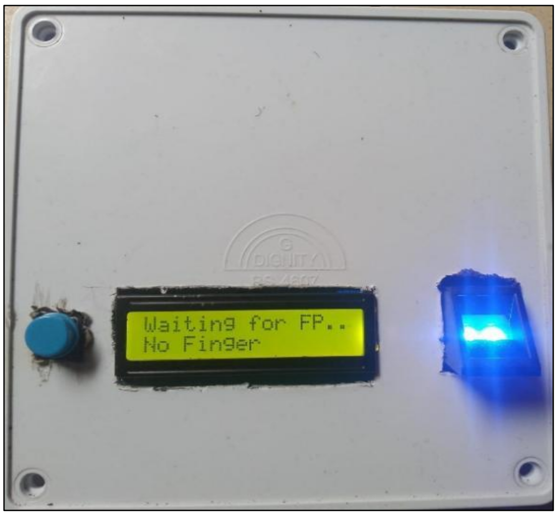


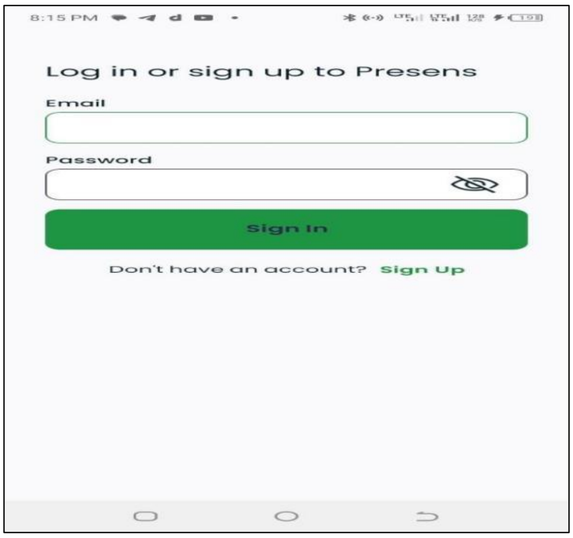
Figure 13: The Device.
Source: Authors, (2025).

## IV. 2. USER INTERFACE ANALYSIS AND VISUALIZATION

This section presents a comprehensive examination of the developed attendance management system's software application screens, supplemented by visual representations (screenshots) to illustrate the interface. The objective of this analysis is to verify that each screen meets functional requirements while providing a seamless user experience.

a) Login Screen

As shown in Figure 14, the login screen presents a minimalistic design, requiring email and password input. Successful login redirects users to the homepage, while incorrect credentials trigger an error message. This design ensures secure authentication and intuitive navigation.



8:15 PM

Log in or sign up to Presens

Email

Password

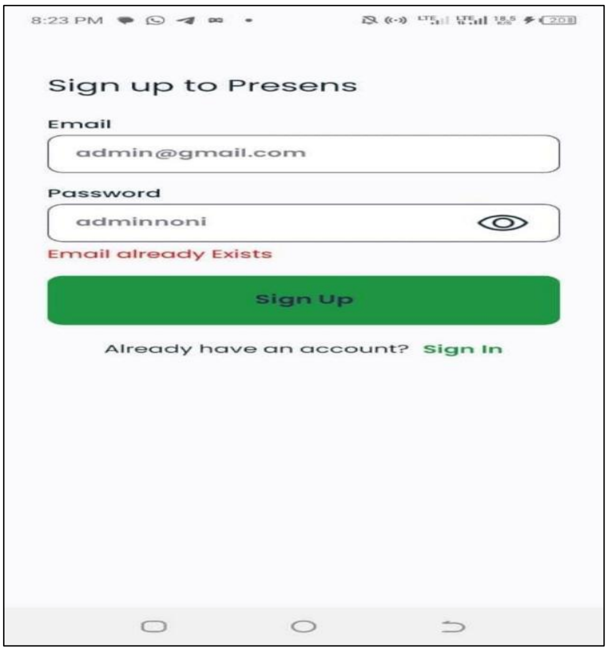
Sign In

Don't have an account? Sign Up

Figure 14: Login Screen
Source: Authors, (2025).

b) Signup Screen

The sign-up screen as shown in Figure 15 facilitates user registration, requiring email and password input. Upon successful registration, users are redirected to the homepage.



8:23 PM

Sign up to Presens

Email
admin@gmail.com

Password
adminnoni

Email already Exists

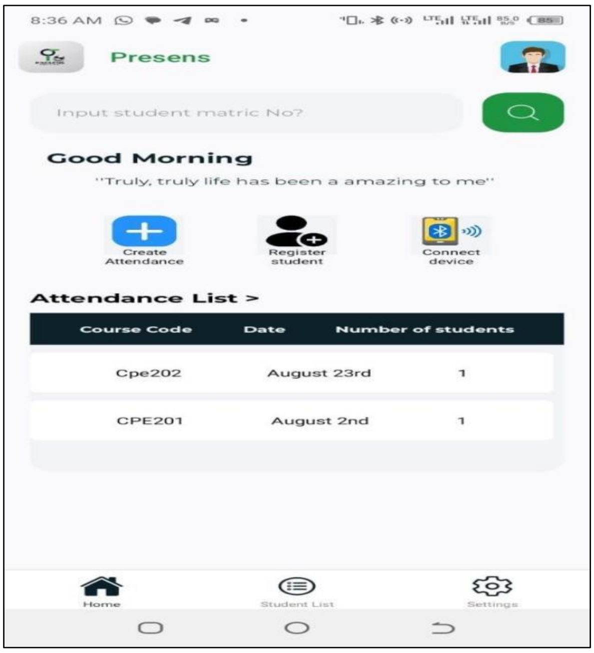
Sign Up

Already have an account? Sign In

Figure 15: Signup Screen.
Source: Authors, (2025).

c) Homepage

The homepage displays the time, network connectivity status and a greeting message. The main features of the app are accessible through icons: "Create Attendance" for marking attendance, "Register Student" for adding new students to the database and "Connect Device" for pairing biometric fingerprint readers. Additionally, there are tabs for "Attendance List," "Student List," and "Settings" (Figure 16).



8:36 AM

Presens

Input student matric No?

Good Morning

"Truly, truly life has been a amazing to me"

Create Attendance · Register student · Connect device

Attendance List >

| Course Code | Date | Number of students |
|---|---|---|
| Cpe202 | August 23rd | 1 |
| CPE201 | August 2nd | 1 |

Home · Student List · Settings

Figure 16: Homepage Screen
Source: Authors, (2025).

d) Student Registration Screen

The student registration page is where the registration of students is done. When the student registration menu is clicked on, on the homepage, it takes the user to the student registration page thatwill display the registration form (Figure 17a and Figure 17b).

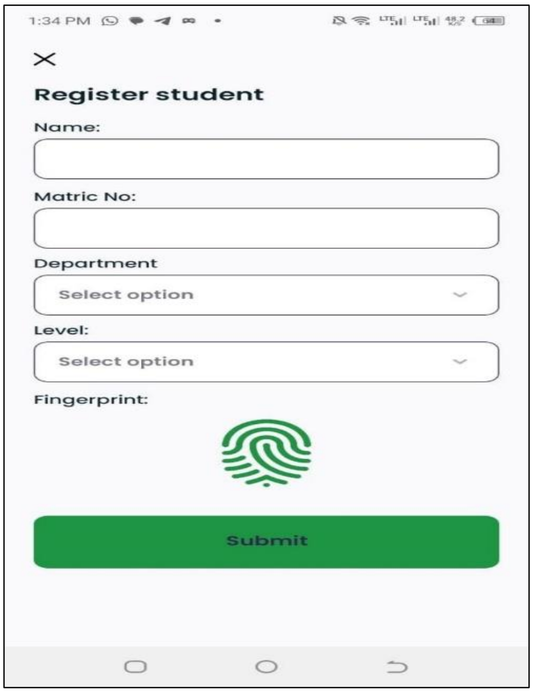
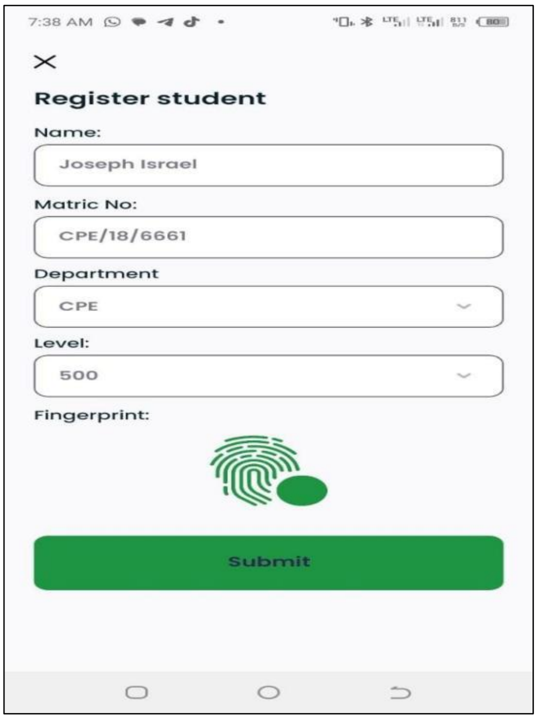


Figure 17a: Student Registration Screen.
Source: Authors, (2025).



Name: Joseph Israel

Matric No: CPE/18/6661

Department: CPE

Level: 500

Figure 17b: Student Input Screen.
Source: Authors, (2025).

e) Attendance Creation Screen

This is the screen where the creation of new attendance is done. It displays the creation form of the attendance in Figure 18.

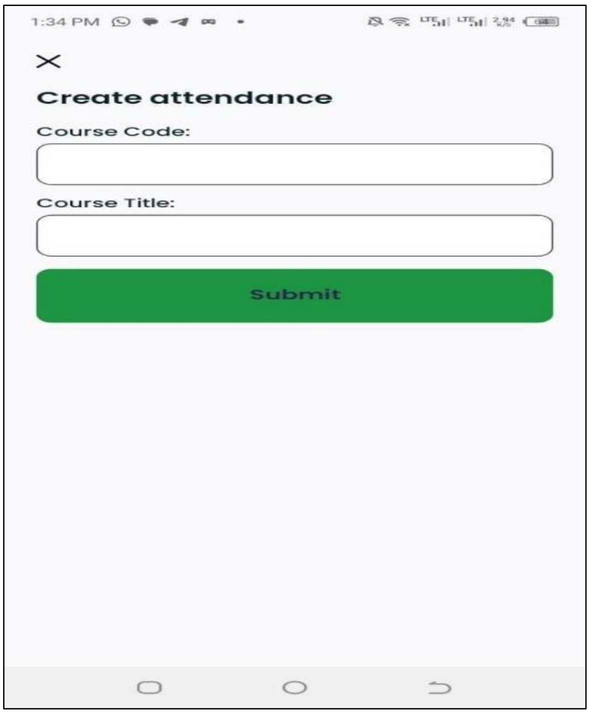


Figure 18: Attendance Creation Screen
Source: Authors, (2025).

f) Attendance List Screen

This displays the attendance list; it also has an icon that leads to a modal for taking fingerprint of student on each particular attendance created in Figure 19.

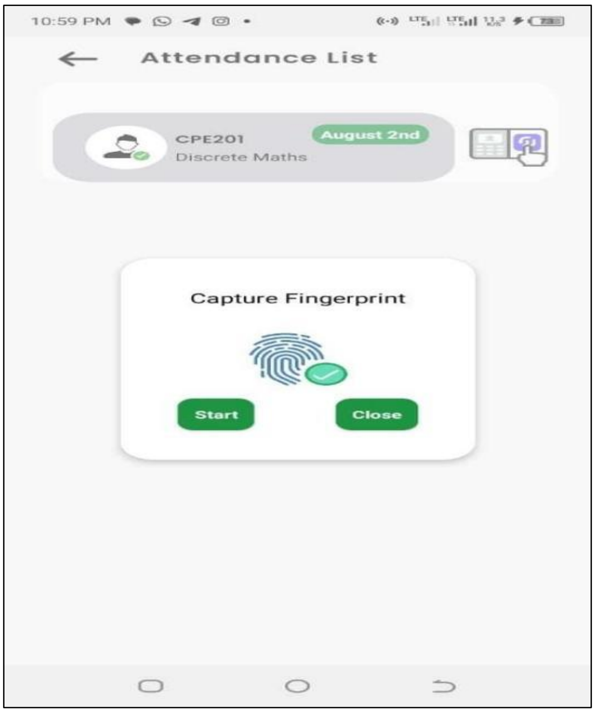
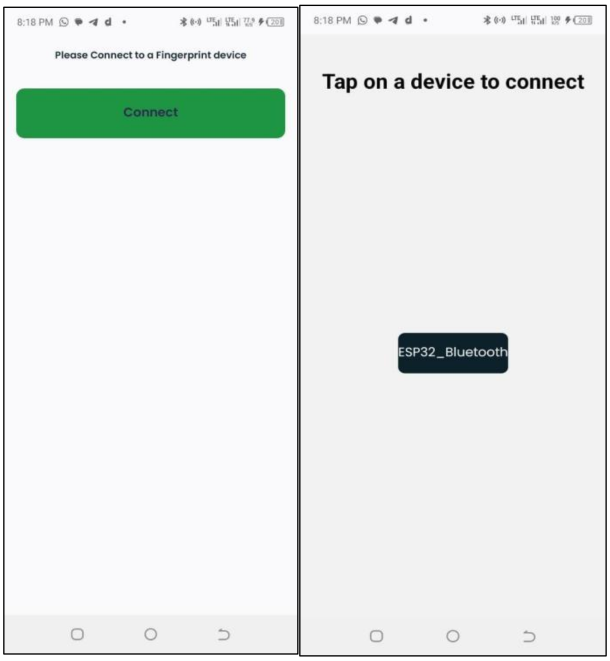


Figure 19: Attendance List Screen.
Source: Authors, (2025).

g) Connect Device Screen

The Connect Device screen serves as an onboarding interface for pairing Bluetooth devices, displaying a modal with available devices for connection in Figure 20.



Please Connect to a Fingerprint device

Tap on a device to connect

Figure 20: Onboarding to Connect.
Source: Authors, (2025).

## IV. 3. SYSTEM OVERVIEW AND DOCUMENTATION

This section provides an in-depth description of the developed attendance management system, outlining its functionality, user access levels, and navigation guidelines.

a) System Description

The proposed system facilitates automated attendance tracking for educational institutions. Lecturers create attendance records for classes, while students register their presence using the biometric fingerprint device. Post-lecture, lecturers can access their portal to view attendance records for the day, enabling accurate attendance scoring.

b) User Access Levels

The system accommodates two primary user categories: students and lecturers. Students are restricted to registering their attendance via fingerprint verification and mandatory system registration. Lecturers have elevated access, enabling them to manage attendance records, register students, and access their profile.

c) System Navigation

Upon launching the application, lecturers can log in or sign up, directing them to their home page. From this central hub, they can manage their profile, register students, create attendance records and access attendance reports. Students, on the other hand, utilize the biometric device to sign in during classes.

d) Student Enrollment and Attendance Tracking

At the semester's commencement, students must register on the system. Thereafter, they utilize their registered fingerprint to sign in on the biometric device during classes. This streamlined process ensures accurate attendance tracking and minimizes disruptions.

e) System Operation

The system operates seamlessly, allowing lecturers to create attendance records, monitor student attendance and generate reports. The biometric device ensures secure and efficient student registration, while the application's intuitive interface facilitates navigation and management.

## V. CONCLUSIONS

Traditional attendance tracking methods, using pen and paper registers are time-consuming, prone to errors and vulnerable to manipulation. Electronic biometric-based attendance management systems, specifically fingerprint recognition, offer a reliable and secure alternative. These systems utilize unique fingerprints to accurately identify and authenticate users, ensuring precise and secure attendance records. The fingerprint biometric attendance system consists of a scanner, database and software which captures and converts fingerprint images into digital templates, comparing them to stored templates to record attendance automatically. The implementation of fingerprint biometric attendance systems provides numerous benefits, including enhanced reliability, efficiency and security. It eliminates proxy attendance, reduces administrative burdens, saves time, prevents forged or duplicated records and minimizes human errors, thereby improving accuracy. Overall, fingerprint biometric attendance systems streamline attendance management, reducing errors and fraud. This modern solution addresses traditional method challenges, making it invaluable for organizations and institutions.

## VI. AUTHOR'S CONTRIBUTION

**Conceptualization:** Author One
**Methodology:** Author One and Author Two.
**Investigation:** Author One and Author Two.
**Discussion of results:** Author One and Author Two
**Writing – Original Draft:** Author One and Author Two.
**Writing – Review and Editing:** Author One and Author Two.
**Resources:** Author One and Author Two.
**Supervision:** Author One.
**Approval of the final text:** Author One and Author Two

## VII. ACKNOWLEDGMENTS

The authors would like to express their sincere gratitude to Almighty God for the successful completion of this research.

## VIII. REFERENCES

[1] H. Mondal & S. Mondal, "Methods of collecting and recording attendance of medical students in a classroom: A systematic review, *Journal of Education and Health Promotion*, vol. 12, no. 1, pp. 1-8, 2023, doi: 10.4103/jehp.jehp_737_23.

[2] N. A. Trivedi *et al.*, "Face Recognition Based Automated Attendance Management System", *International Journal of Scientific Research in Science and Technology*, vol. 9, no. 1, pp. 261-268, 2022, doi: 10.32628/ijsrst229147.

[3] A. B. Habibah, H. Rashid & S. M. Abubakar, "An Enhanced Iris Recognition and Authentication System using Energy Measure", *Science World Journal*, vol. 13, no. 1, pp. 11-17, 2018.

[4] U. Koppikar *et al.*, "IoT based Smart Attendance Monitoring System using RFID", *1st International Conference on Advances in Information Technology (ICAIT)*, pp. 193-197, 2019, doi: 10.1109/ICAIT47043.2019.8987434.

[5] C. Anjali, “A Review on Various Aspects of MongoDB Databases”, *International Journal of Engineering Research and Technology (IJERT),* vol. 8, no. 5, pp. 90-92, 2019.

[6] R. Deari, X. Zenuni, J. Ajdari, F. Ismaili & B. Raufi, “Analysis and Comparison of Document-Based Databases with Relational Databases: MongoDB vs MySQL, *International Conference on Information Technologies (InfoTech),* pp. 1-4, 2018, doi: 10.1109/infotech.2018.8510719.

[7] M. S. Rahman, K. M. Rumman, R. Ahmmed, M. A. Rahman & M. A. Sarker, “Fingerprint Based Biometric Attendance System”, *Section A -Research paper of European Chemical Bulletin,* vol. 12, no. S3, pp. 184-190, 2023, doi: 10.31838/ecb/2023.12.s3.026.

[8] L. Kamelia, E. A. D. Hamidi, W. Darmalaksana & A. Nugraha, “Real-Time Online Attendance System Based on Fingerprint and GPS in the Smartphone”, *2018 4th International Conference on Wireless and Telematics (ICWT),* pp. 1-4, 2018, doi: 10.1109/icwt.2018.8527837.

[9] J. F. Rusdi, F. R, Kodong, R. E. Indrajit, H. Sofyan, Abdurrohman & R. Marco, “Student Attendance using Face Recognition Technology”, *2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS),* pp. 1-4, 2020, doi:10.1109/icoris50180.2020.9320819.

[10] V. Wati, K. Kusrini, H. A. Fatta & N. Kapoor, “Security of Facial Biometric Authentication for Attendance System”, *Multimedia Tools and Applications,* vol. 80, no. 16, pp. 23625-23646, 2021, doi: 10.1007/s11042-020-10246-4.

[11] H. Tok, N. S. Batur, R. Tuzen, H. I. Yildirim & S. Demirci, “A Novel Zigbee Based Mobile Fingerprint Student Attendance System”, *2019 4th International Conference on Computer Science and Engineering (UBMK),* pp. 492-497, 2019, doi:10.1109/ubmk.2019.8907221.

[12] A. R. Chandan & V. D. Khairnar, “Bluetooth Low Energy (BLE) crackdown using IoT”, *2018 International Conference on Inventive Research in Computing Applications (ICIRCA),* pp. 1436-1441, 2018, doi: 10.1109/icirca.2018.8597189.

[13] C. Gomez, J. Oller & J. Paradells, “Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology”, *Sensors,* vol. 12, no. 9, pp. 11734-11753, 2012, doi: 10.3390/s120911734.

[14] O’Reilly, “Learning React Native”, [Online], Available at: https://www.oreilly.com/library/view/learning-react-native/9781491929049/ch01.html [Accessed 24 July 2024].