Asian Journal of Applied Science and Technology (AJAST)
Volume 9, Issue 3, Pages 147-161, July-September 2025

IoT-Enabled Fingerprint Biometric Attendance System for Secure and Real-Time Student Monitoring

Ramgopal A.[1*], Jai Jothi K.[2], Godson S.[3], Aarush Jeimen M.[4], Babisha R.[5] & Jino Shiny V.[6]

[1,2,3,4,5,6]*Department of Electronics and Communication Engineering, Stella Mary's College of Engineering, Tamil Nadu, India.*
Corresponding Author Email: ramgopal.a1611@gmail.com[*]

DOI: https://doi.org/10.38177/ajast.2025.9314

Article Received: 21 June 2025 *Article Accepted: 26 August 2025* *Article Published: 28 August 2025*

ABSTRACT

Biometric attendance systems offer a reliable and automated method for identifying individuals based on physiological or behavioural traits. Frequently utilized biometric modalities encompass fingerprints, facial recognition, iris scans, and vocal patterns. In academic settings, such systems improve the precision and efficiency of monitoring student attendance while reducing manual errors. This study presents a fingerprint-based IoT attendance system that automates attendance recording via biometric authentication. The system utilizes an optical sensor to capture a student's fingerprint and securely stores the attendance data in a cloud database through IoT connectivity. By eradicating manual procedures and averting proxy attendance, the system guarantees reliable and instantaneous record management. Additionally, the stored data can be accessed by faculty through a secure web portal, providing transparency and ease of use.

Keywords: AES-256; Data Encryption; Fingerprint Sensor; Real-Time Data Logging; Sensor Fusion; Encrypted IoT; Multimodal Biometric.

1. Introduction

Attendance tracking is a vital administrative function in both educational institutions and workplaces. It serves not only as a mechanism to monitor presence and participation but also as an essential tool for ensuring discipline, accountability, and resource optimization. Accurate attendance records are crucial for performance evaluation, salary calculations, compliance with institutional policies, and even legal requirements in some sectors [1]. Despite its importance, the methods traditionally employed to record attendance often fall short of modern efficiency and accuracy standards. Conventional methods such as manual roll calls, signature registers, and paper-based logbooks have been widely used for decades. However, these approaches are inherently time-consuming, especially in large classrooms or organizations with hundreds of employees [2]. Teachers and administrators often spend a significant portion of productive time manually verifying attendance, which reduces the time available for core academic or organizational tasks. Furthermore, manual systems are susceptible to errors and manipulations. Issues such as illegible handwriting, misrecorded entries, and intentional fraud, including proxy attendance, compromise the reliability of the data collected [3]. These shortcomings undermine the credibility of the system, create unnecessary administrative burdens, and reduce accountability.

The amalgamation of biometric technologies with the Internet of Things (IoT) has surfaced as a viable remedy to address these constraints. Biometric systems utilize distinct physiological or behavioral traits of individuals to offer a secure and tamper-proof identity verification method. Fingerprint recognition is one of the most widely adopted biometric modalities, alongside facial recognition, iris scanning, and voice recognition, due to its uniqueness, permanence, cost-effectiveness, and user acceptance [5]. In contrast to passwords or identification cards, which are susceptible to forgetfulness, theft, or sharing, a fingerprint is distinctive to each individual, rendering it a robust protection against fraudulent activities like impersonation or buddy punching. Recent advancements in fingerprint sensor technologies have improved the precision and rapidity of fingerprint-based systems. Sensors such as the GT521F52 have been engineered to facilitate secure, rapid fingerprint acquisition and template comparison [4], [5].These sensors are compact, energy-efficient, and cost-effective, making them highly suitable for embedded applications in resource-constrained environments such as schools and small enterprises. With features such as on-device storage, encryption support, and rapid matching algorithms, modern fingerprint sensors minimize latency while maintaining security.

The effectiveness of biometric authentication in attendance systems can be further enhanced by integrating it with IoT-based platforms. IoT technology enables devices to connect, communicate, and exchange data over the internet in real time. In the case of attendance management, the integration of fingerprint sensors with microcontrollers like the ESP32 allows seamless data capture and transmission [6]. The ESP32, with its built-in Wi-Fi and Bluetooth connectivity, provides a reliable gateway for transferring attendance data from the sensor module to cloud-based services. Cloud services such as Google Firebase play a significant role in this ecosystem. By transmitting authenticated attendance records to Firebase in real time, institutions gain centralized access to updated data [7]. This enables administrators, faculty, and management staff to monitor attendance remotely, generate reports instantly, and make data-driven decisions without manual intervention. Moreover, the system enhances accessibility, as records can be retrieved securely from any location using authorized portals [8]. Importantly, modern systems also support offline functionality. When network connectivity is unavailable, data can be cached locally in the microcontroller or an external memory unit and automatically synchronized with the cloud once the connection is restored. This ensures uninterrupted operation, even in regions with inconsistent internet access.

Despite these advancements, many existing attendance systems are not without limitations. Several reported systems lack features such as robust offline data handling, end-to-end encryption, and role-specific user portals. The absence of offline storage mechanisms leads to data loss or synchronization issues when connectivity fails, undermining the reliability of the system [2], [9]. Similarly, systems that fail to implement strong encryption remain vulnerable to cyber threats, including data breaches and identity theft [10]. Additionally, the absence of separate web portals for students and staff reduces usability, as the system cannot provide customized access privileges, dashboards, or role-specific reports tailored to the needs of different stakeholders. These limitations restrict the applicability of such systems in real-world institutional contexts, where data integrity, confidentiality, and user convenience are non-negotiable requirements. This paper delineates the design and implementation of a fingerprint-based IoT attendance system that addresses existing deficiencies by integrating numerous layers of security, usability, and resilience. One of the primary enhancements of the proposed system is the integration of AES (Advanced Encryption Standard) encryption to ensure the security of biometric templates and to enable secure communication between the fingerprint sensor, microcontroller, and cloud platform. AES is a symmetric encryption algorithm that is globally recognized and provides a harmonious combination of robust cryptographic security and computational efficiency, thereby protecting sensitive attendance records from unauthorized access [3], [11]. In addition to encryption, the system incorporates an offline data storage mechanism. Attendance data captured during network outages are securely stored on local memory, ensuring that no records are lost due to connectivity issues. Once the system detects an active internet connection, the locally cached data are automatically synchronized with the cloud. This feature enhances system reliability and makes it suitable for deployment in regions with limited or unstable network infrastructure. Another key contribution of the system is the development of separate web portals for students and staff. By designing role-specific interfaces, the system enhances usability and ensures that stakeholders have access only to relevant information. For instance, students can log in to view their attendance history, monitor percentage compliance with institutional policies, and receive notifications of shortages. On the other hand, staff members can access comprehensive records, generate customized reports, and monitor class or department-wide statistics in real time. This division of functionality improves overall system security while delivering a tailored user experience [12].

The proposed fingerprint-IoT attendance framework offers several advantages over existing models. First, by integrating fingerprint recognition with IoT-enabled real-time data transmission, it ensures high accuracy and eliminates fraudulent practices such as proxy attendance. Second, the use of AES encryption enhances security, addressing concerns about data breaches and identity theft. Third, the offline caching mechanism guarantees robustness in environments with unreliable network access. Finally, the modular architecture, combined with role-specific web portals, makes the system highly adaptable across diverse institutional settings—from schools and universities to corporate organizations and government offices. This paper provides a comprehensive discussion of the system architecture, implementation strategy, and benefits of the proposed attendance system. It emphasizes the enhancements in accuracy, security, accessibility, and scalability by juxtaposing its features with previous works. The amalgamation of biometric fingerprint recognition with IoT platforms, AES encryption, and cloud services establishes the system as a progressive solution adept at resolving persistent issues in attendance management.

1.1. Study Objectives

The proposed system aims to automate attendance tracking by eliminating manual intervention through fingerprint authentication, thereby ensuring accurate and efficient logging of records. To strengthen data security, all biometric and attendance information will be securely stored and transmitted using encrypted communication methods. Real-time cloud integration will be achieved through Google Firebase, enabling faculty to access attendance data instantly from any location. Furthermore, the system addresses a major limitation of earlier IoT-based solutions by supporting offline data handling, allowing attendance records to be temporarily stored locally during internet outages and automatically synchronized once connectivity is restored. To improve accessibility, a user-friendly web portal will be developed, enabling students and faculty to easily view, filter, and manage attendance records. Finally, the system enhances transparency and reliability by preventing proxy attendance and ensuring accurate reporting of both student and staff participation.

1.2. Role of IoT in Attendance

The Internet of Things (IoT) has emerged as a transformative technology, significantly altering various industries, including healthcare, agriculture, smart cities, and particularly education. The Internet of Things (IoT) facilitates automation, real-time monitoring, and data-driven decision-making through the integration of interconnected devices, sensors, and cloud services, which were previously unachievable. In the education sector, a significant and effective application of IoT is in attendance management systems, where automation can eradicate inefficiencies and guarantee fairness, accuracy, and reliability in monitoring student and staff participation.

Conventional attendance systems, including manual roll calls, RFID cards, and facial recognition, have been utilized in educational institutions and workplaces for an extended period. Although these methods have fulfilled their intended function, they possess significant deficiencies. Manual roll calls are labor-intensive and susceptible to human error. RFID systems, though faster, are vulnerable to misuse since students can hand over their ID cards to peers, leading to proxy attendance. Even advanced techniques like facial recognition face challenges such as changes in lighting conditions, low image quality, and susceptibility to spoofing using photographs or videos. Additionally, these conventional methods often suffer from limited scalability and restricted remote access, making them less suitable for large institutions or blended learning environments.

In contrast, IoT-enabled attendance systems overcome many of these limitations by integrating biometric authentication, cloud-based synchronization, and wireless communication protocols. Biometric techniques, including fingerprint recognition, iris scans, and palm vein authentication, offer superior security and precision due to their uniqueness to each individual and resistance to duplication. When integrated with IoT devices and cloud platforms, these biometric systems autonomously document attendance, synchronize it in real time, and enable authorized stakeholders to securely access the data from any location. This integration guarantees that attendance records are secure from tampering, transparent, and exceptionally reliable. A primary benefit of IoT-based systems is their real-time synchronization with cloud platforms like Google Firebase, Amazon Web Services (AWS), or Microsoft Azure. This not only offers immediate access to attendance data for faculty and administrators but also enables integration with other institutional management systems, including grading portals, student information systems (SIS), or performance dashboards.

Additionally, IoT systems can be engineered to facilitate offline data caching, which is especially advantageous in regions with unreliable or nonexistent internet connectivity. During outages, data is locally stored on the IoT device and is automatically synchronized with the cloud upon restoration of connectivity. This feature markedly enhances system reliability and service continuity, rectifying a major limitation of previous RFID or cloud-dependent systems. Furthermore, IoT-enabled attendance solutions promote remote accessibility and scalability, making them highly relevant in today’s hybrid and online learning environments. Teachers and administrators can monitor attendance patterns from their laptops or mobile devices, while students can verify their attendance records through secure web portals or mobile applications. This increases transparency and accountability, reducing disputes over attendance and ensuring that records remain accurate and verifiable at all times.

In summary, by leveraging IoT in attendance management systems, educational institutions gain access to a highly secure, automated, and resilient solution that addresses the shortcomings of traditional methods. With biometric authentication for accuracy, cloud integration for real-time access, offline caching for reliability, and wireless communication for scalability, IoT-based attendance tracking provides a future-ready framework. Such systems not only streamline administrative tasks but also align with the broader goal of smart campus initiatives, where technology drives efficiency, transparency, and enhanced learning experiences.

1.3. Drawbacks in Previous Works & How Our Study Solves Them

Many previous fingerprint-based IoT attendance systems encountered significant challenges that limited their effectiveness and widespread adoption. One of the most common issues was the heavy dependence on constant internet connectivity for real-time data synchronization. In such systems, if the network went down or connectivity was unstable, attendance data was often lost or left incomplete. This made them unreliable, particularly in rural or semi-urban areas where internet coverage fluctuates. Another critical drawback was related to data security. A number of earlier solutions did not implement strong encryption techniques, leaving biometric and attendance records vulnerable to unauthorized access, tampering, or even potential identity theft. Considering that biometric data is highly sensitive and unique to each individual, the absence of adequate security safeguards posed a serious risk to user privacy and system trustworthiness.

Transparency and accessibility were also major limitations in older models. Most systems did not provide easy ways for students or staff to check their attendance records, leading to reduced user engagement and a lack of trust in the system. When records were only available to administrators, disputes over attendance became more difficult to resolve, and users often felt excluded from the process. Alongside these issues, hardware constraints further hindered performance. Many fingerprint sensors lacked onboard storage, meaning that if connectivity failed or the system was interrupted, no backup of the records was available. Similarly, the absence of power backup mechanisms led to frequent operational failures, leaving attendance sessions incomplete and creating a poor overall user experience. These factors collectively reduced the reliability and practicality of earlier IoT-based attendance systems in real-world educational environments.

Our proposed project is designed to overcome these drawbacks by incorporating several critical improvements. To address connectivity issues, the system implements offline data storage directly on the fingerprint sensor and microcontroller. This ensures that attendance data is captured and stored locally even when the internet is unavailable. Once connectivity is restored, the system automatically synchronizes the locally stored records with the cloud, guaranteeing accuracy and completeness without manual intervention. This offline-first approach significantly improves system resilience and reliability in areas with unstable networks. In terms of security, all sensitive data is protected using AES encryption during both transmission and storage. This ensures that biometric information and attendance logs remain confidential and resistant to tampering, thereby safeguarding user privacy and building confidence in the system. Accessibility has also been enhanced by integrating user-friendly web portals tailored for both students and staff. Through these portals, individuals can conveniently view, filter, and manage their attendance records from any location, fostering greater transparency and user engagement. To improve usability, the system provides immediate feedback via an LCD display, allowing users to confirm that their attendance has been successfully recorded.

Finally, the inclusion of a reliable power backup system ensures uninterrupted operation even during electricity outages, preventing data loss and improving user trust. With these advancements, the proposed IoT-based fingerprint attendance system delivers a secure, transparent, and resilient solution that addresses the shortcomings of earlier approaches while offering a more reliable and user-centered experience.

2. System Architecture

The Fingerprint-Based IoT Attendance System is designed to automate and secure the process of attendance tracking with minimal manual intervention. Its core functionality revolves around biometric authentication, where the GT521F52 Optical Fingerprint Sensor captures a student's fingerprint and generates a unique digital template. This template is compared with pre-registered entries stored in the sensor's EEPROM. Upon a successful match, the ESP32 microcontroller records the student's ID along with the current date and time, and the attendance data is transmitted to a cloud database via Wi-Fi using Google Firebase. A significant advancement in this system is its ability to function efficiently even during network failures. Unlike previous models that lost data when connectivity was interrupted, the proposed system temporarily stores the attendance data locally—either in the ESP32's memory or in the sensor's EEPROM. Upon restoration of the internet connection, the system automatically synchronizes the locally stored data with the cloud, guaranteeing that no attendance information is lost. The system features a robust backend and a user-friendly interface. An OLED or 16x2 LCD display offers immediate feedback by verifying successful attendance or notifying the user of errors, thus enhancing the overall user experience and minimizing confusion during the attendance procedure. To further enhance accessibility, a web-based dashboard was developed using HTML, CSS, JavaScript, and Firebase. Students can log in securely to view their personal attendance records, while faculty members have the ability to filter and analyze attendance by academic year, specific dates, or student batches. A dedicated staff attendance module also allows teachers to view their own entry and exit times, promoting transparency and better time management. One of the most important aspects of our design is safety. In order to ensure the safety of attendance records and biometric data, they are encrypted using the Advanced Encryption Standard (AES) before being transmitted and stored. Attendance records are only accessible to authorized personnel, which protects sensitive data from being accessed or used inappropriately by unauthorized individuals.

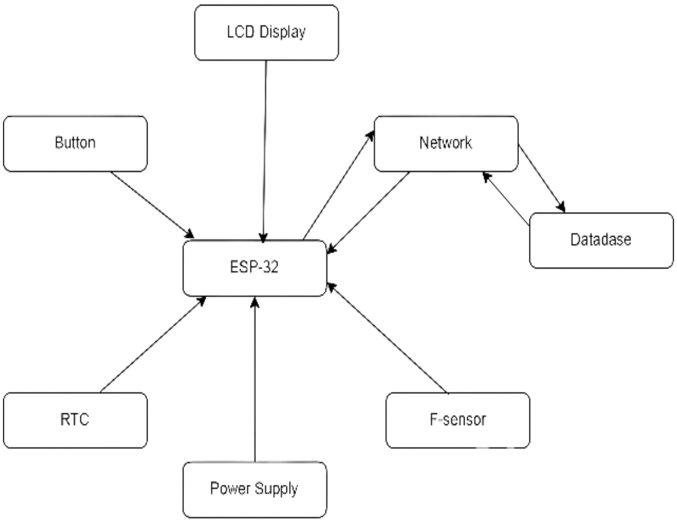


Figure 1. Component Flowchart

2.1. Components Used

The development of our fingerprint attendance system that is based on the Internet of Things required a combination of hardware and software components that collaborated with one another to ensure that the system functions without any interruptions. These are the primary elements that were utilized in our project:

2.1.1. Hardware Components

The hardware components of the proposed IoT-based Fingerprint Attendance System are carefully integrated to ensure accurate fingerprint authentication, efficient data processing, and real-time attendance monitoring. The primary component is the GT521F52 Optical Fingerprint Sensor, which captures and authenticates student fingerprints using an advanced optical sensing mechanism. It scans the unique ridge patterns of a fingerprint and compares them with stored templates, ensuring high accuracy and fast recognition speed. With the capability to store up to 200 templates internally, the sensor provides seamless and secure authentication, making it suitable for educational environments where large groups of students must be processed quickly. The ESP32 microcontroller, which serves as the central processing unit and is responsible for coordinating all of the system's operations, is located at the very center of the overall system.

By utilizing the Wi-Fi module that is built into the device, it is able to receive data from the fingerprint sensor, process that data, and then communicate with the cloud. Because of its low power consumption, high computational efficiency, and ability to handle tasks in real time, the ESP32 is an extremely efficient controller that can be used for continuous operation. In order to ensure that attendance records are instantly updated and that authorized users are able to access them remotely, the integrated Wi-Fi functionality plays a crucial role in enabling wireless data transfer to the cloud database. For the purpose of user interaction, the system incorporates an LCD display (16x2 or OLED), which provides real-time feedback such as student names, fingerprint authentication results, and attendance status. This enables both students and faculty to verify that the attendance marking was successful immediately.

The system is equipped with additional push buttons for navigation and fingerprint registration, and LED indicators display the operational status of the system, including whether or not scans were successful, whether errors occurred, or whether processing is still ongoing. To ensure uninterrupted functionality, the system is powered by a stable 5V/3.3V adapter with battery backup support, which prevents data loss and guarantees reliable performance even during power fluctuations.

2.1.2. Software Components

When it comes to the functionality of the system, the software components are the most important because they make it possible for the hardware and the cloud to communicate without any interruptions. The Arduino Integrated Development Environment (IDE) is the primary development environment that is utilized for the purpose of programming the ESP32 microcontroller. In addition to supporting libraries that are required for integrating the fingerprint sensor and managing wireless data transmission, it makes the process of code compilation and deployment more straightforward or simplified. By ensuring that the ESP32 and other system components are able to coordinate with one another in a seamless manner, the Arduino IDE makes it possible to process fingerprint authentication and attendance in an effective manner. For cloud-based data management, the system integrates Google Firebase as a secure, real-time database. Firebase stores attendance records instantly whenever a student’s fingerprint is authenticated. This enables teachers, administrators, and other authorized personnel to access, monitor, and manage attendance data from anywhere using connected devices. The integration of Firebase ensures data security, real-time synchronization, and scalability, making the system highly reliable for large-scale deployment.

In summary, the combination of advanced hardware components for accurate fingerprint sensing and robust software components for efficient data handling provides a fast, secure, and user-friendly attendance management solution. The system's real-time connectivity, interactive display, and reliable power management make it a modern, scalable, and efficient platform suitable for educational institutions and organizations.

░3. System Implementation

The fingerprint scanner is a crucial component of the IoT-based attendance system, serving as the primary element for secure and accurate student authentication. Its main function is to capture the unique fingerprint pattern of each user and convert it into a digital template that can be compared with stored records in the system database. Since no two fingerprints are alike, this method ensures that the process of attendance tracking is both reliable and tamper-proof. Unlike traditional methods such as manual roll calls, RFID cards, or password-based systems, fingerprint-based authentication cannot be easily duplicated or forged, making it one of the most effective biometric approaches for identity verification.

The sensor operates on advanced fingerprint recognition technologies, either optical or capacitive. Optical sensors capture fingerprint images using light reflection and detection, while capacitive sensors rely on electrical signals to map the ridges and valleys of a fingerprint. Both methods are widely regarded for their high precision, quick recognition speed, and adaptability in real-world environments. After a fingerprint has been placed on the scanner, it is immediately processed and converted into a digital code, which is commonly referred to as a fingerprint template. In order to confirm the student's identity, this template is subsequently compared with entries that have been previously saved in the database. When a successful match is made, the system immediately updates the cloud database with the student's attendance information and records it in real time. This allows for centralized storage and monitoring of the information.

To further strengthen security, the biometric data captured by the scanner undergoes encryption before being transmitted or stored. This prevents unauthorized access or tampering and ensures that sensitive information remains protected at all times. Unlike traditional attendance systems where proxy attendance is common, fingerprint-based systems provide a foolproof solution since biometric traits cannot be shared or replicated. This enhances trust among students, faculty, and administrators, while also promoting transparency in attendance tracking. One of the standout features of the GT521F52 fingerprint sensor, often used in modern IoT-based attendance systems, is its built-in EEPROM storage. This internal memory allows the device to temporarily save attendance data even in the absence of an active internet connection. During periods of network outage, the system continues to function offline without interrupting the attendance process. Once connectivity is restored, all locally stored data is automatically synchronized with the cloud. This offline-first capability significantly improves system reliability and eliminates the risk of data loss, a common limitation in many earlier attendance management systems. Despite its robust functionality, the fingerprint scanner is not without challenges. In some cases, users may experience slower recognition due to worn-out or unclear fingerprint patterns, particularly for students whose daily activities may cause abrasions on the skin. Environmental conditions such as dust, moisture, or dirt on the scanner surface can also impact performance. However, these issues can be effectively managed through regular maintenance of the hardware, software-level optimizations, and calibration of the sensor. Modern scanners are designed with adaptive algorithms that improve recognition accuracy over time, minimizing false rejections and enhancing the overall user experience.

In addition to accuracy and reliability, user interaction is also streamlined through immediate feedback mechanisms. When a fingerprint is scanned, the system provides instant confirmation through an LCD or OLED display, notifying the student whether their attendance has been successfully recorded or if an error has occurred. This direct feedback reduces confusion, eliminates the need for manual verification, and improves efficiency in environments with large groups of students.

Overall, the fingerprint scanner plays a pivotal role in transforming attendance systems from outdated, error-prone methods into highly secure, automated, and resilient solutions. By combining unique biometric identification, built-in data storage, real-time cloud integration, and robust error-handling mechanisms, it ensures that attendance tracking is seamless, transparent, and reliable. While occasional challenges such as slower recognition or maintenance requirements may arise, these can be easily managed through system-level enhancements, making the fingerprint scanner an indispensable part of a modern IoT-based attendance management framework.

3.1. Working

The IoT-based fingerprint attendance system automates the process of attendance tracking through biometric authentication and real-time data handling. The workflow begins with the fingerprint sensor capturing the unique fingerprint pattern of each user and generating a digital template. This template is then compared with pre-registered records to verify identity. Once authenticated, the system records the attendance, stores it securely in the cloud using Firebase, and provides immediate on-screen feedback to the user. By integrating biometric recognition with IoT and cloud technology, the system ensures accuracy, transparency, and efficiency while eliminating errors common in traditional methods. The IoT-based fingerprint attendance system operates through a structured sequence that ensures accuracy, security, and efficiency. The process begins with fingerprint scanning, where a student places their finger on the fingerprint sensor. The sensor captures the fingerprint image, analyzes the ridge and valley patterns, and converts them into a unique digital template. This template is then used for authentication and verification by comparing it with pre-stored records in the system’s database. If a match is found, the student’s identity is confirmed, and the system proceeds to the next stage. Once authentication is successful, the attendance is automatically marked without any manual intervention.

At this point, the ESP32 microcontroller, which functions as the central processing unit, handles the data processing, ensuring smooth communication between the fingerprint sensor, storage modules, and cloud database. The verified attendance record is transmitted through the built-in Wi-Fi module and updated in a cloud platform such as Google Firebase. This integration with cloud storage allows teachers and administrators to access real-time attendance data from any device, ensuring convenience, transparency, and timely monitoring. To enhance usability, a display module such as an OLED or LCD provides instant on-screen feedback to the student. The display confirms whether the attendance has been marked successfully and may also show additional details like the student's name and ID for further confirmation. This immediate feedback reduces errors and builds trust in the system. By combining biometric authentication, cloud synchronization, and real-time reporting, the system provides a secure and user-friendly solution to attendance management. It eliminates common issues like proxy attendance, reduces the workload of faculty, and ensures that records remain accurate, transparent, and readily available. Overall, this approach modernizes the attendance process and makes it more reliable for educational institutions.

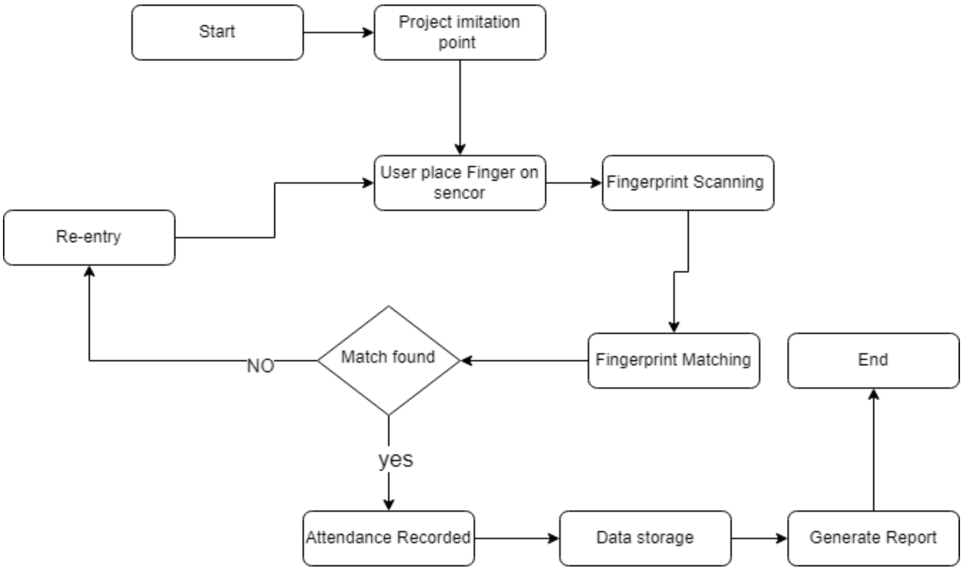
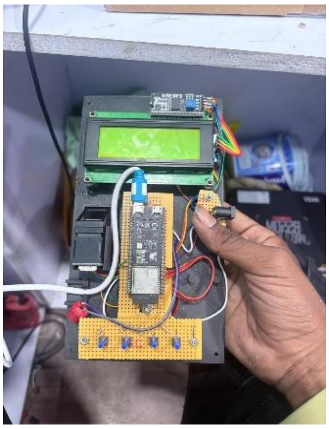


Figure 2. User Interface Flowchart

4. Result and Discussion

The IoT-based fingerprint attendance system is built using a combination of hardware and software components that work seamlessly together to deliver accurate and efficient attendance management.



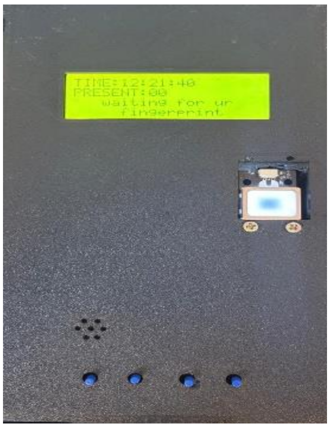
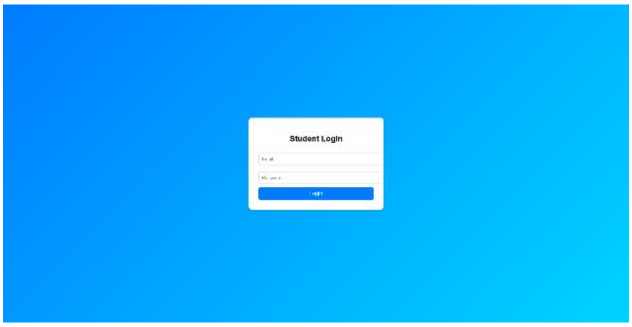


Figure 3. Components Image **Figure 4.** Device Image

The hardware setup serves as the backbone of the system, as it is directly responsible for capturing attendance data from students in real time. Components such as the fingerprint sensor, ESP32 microcontroller, display modules, and power backup ensure that the process of authentication, data processing, and cloud synchronization happens smoothly and reliably. The fingerprint sensor is used to capture each student's biometric input, which is then processed by the microcontroller and stored securely in the cloud database. The display module provides instant confirmation so that students and faculty members know immediately whether the attendance has been recorded successfully. These hardware elements ensure speed, accuracy, and system resilience, even in cases of unstable internet connectivity, by temporarily storing data locally and syncing it once connectivity is restored. On the software side, the system provides an intuitive and user-friendly interface for both students and faculty. A dedicated student portal has been designed where learners can log in securely using their unique ID and password credentials. After successful authentication, they are directed to a personalized dashboard that allows them to view only their individual attendance records. This personalized access prevents unauthorized viewing of others' data, thereby ensuring both transparency and privacy.

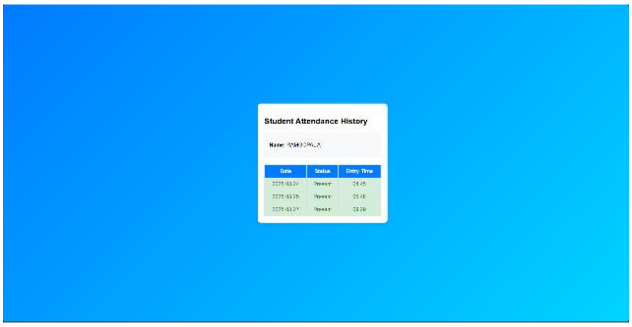

Student Login

Email

Password

Figure 5. Student Login

For faculty, the portal offers extended functionality to filter, analyze, and generate attendance reports based on specific dates, student groups, or academic sessions. This dual integration of hardware and software not only automates the attendance process but also enhances accessibility and transparency for all stakeholders. Overall, the system reduces manual workload, prevents proxy attendance, and ensures that records are consistently accurate, reliable, and easily available for both students and faculty.


Student Attendance History

Name: [illegible]

Date	Status	Entry Time
2025-03-24	Present	09:45
2025-03-26	Present	09:48
2025-03-27	Present	09:39

Figure 6. Student Attendance

The staff portal is designed to provide faculty members with an efficient and structured way to access and manage student attendance data. After logging in securely through their unique credentials, staff members are directed to a dashboard where they can select specific criteria to filter and analyze attendance records. One of the key features is the ability to choose between different academic years, such as the second, third, or fourth year, allowing faculty to focus on the attendance of a particular batch of students. Once an academic year is selected, the portal displays the relevant student records in a clear and organized format, complete with options to sort by date, course, or student roll number. This functionality simplifies the process of tracking attendance trends across different classes and ensures that faculty can quickly identify irregularities, such as frequent absences or low attendance percentages. By integrating these selection criteria, the staff portal eliminates the need for manual compilation of records and provides instant access to accurate data. In addition, the portal supports real-time synchronization with the cloud database, ensuring that staff always works with the latest attendance information. This improves efficiency, enhances transparency, and helps faculty in academic planning, reporting, and student engagement.

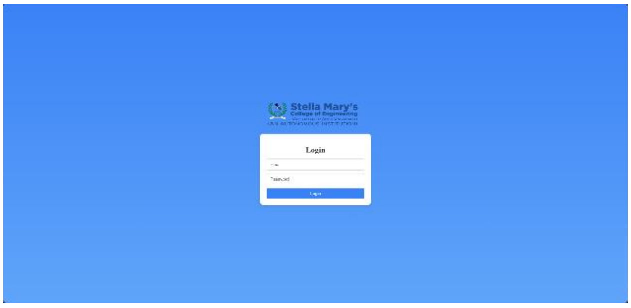


Figure 7. Staff Login

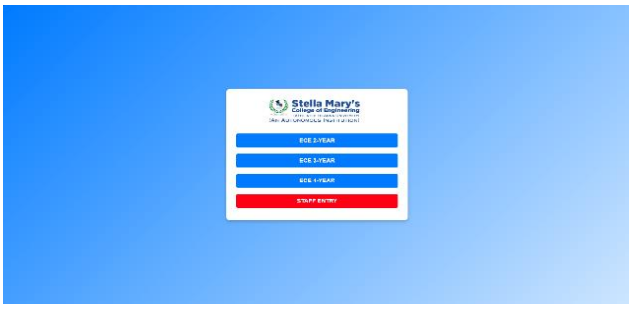
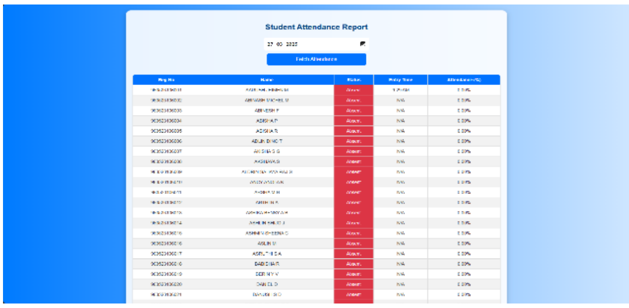


Figure 8. View student attendance

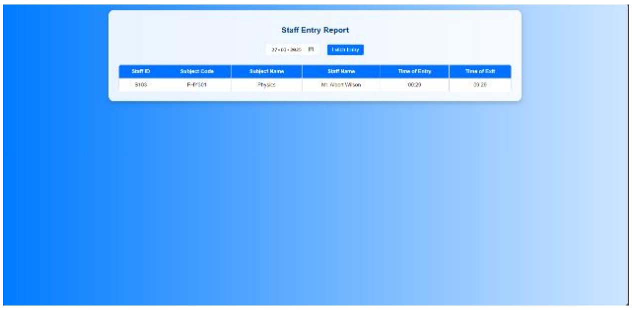


Student Attendance Report

27-03-2025

Reg No	Name	Status	Entry Time	Attendance (%)
[illegible]	[illegible]	Absent	[illegible]	[illegible]
[illegible]	ABINASH MICHEL M	Absent	N/A	0.00%
[illegible]	ABINESH P	Absent	N/A	0.00%
[illegible]	ABISHA P	Absent	N/A	0.00%
[illegible]	[illegible]	Absent	N/A	0.00%
[illegible]	ADLIN DINO T	Absent	N/A	0.00%
[illegible]	[illegible]	Absent	N/A	0.00%
[illegible]	[illegible]	Absent	N/A	0.00%
[illegible]	[illegible]	Absent	N/A	0.00%
[illegible]	[illegible]	Absent	N/A	0.00%
[illegible]	[illegible]	Absent	N/A	0.00%
[illegible]	[illegible]	Absent	N/A	0.00%
[illegible]	[illegible]	Absent	N/A	0.00%
[illegible]	[illegible]	Absent	N/A	0.00%
[illegible]	[illegible]	Absent	N/A	0.00%
[illegible]	ASLIN M	Absent	N/A	0.00%
[illegible]	ASRUTHI S A	Absent	N/A	0.00%
[illegible]	BABISHA R	Absent	N/A	0.00%
[illegible]	[illegible]	Absent	N/A	0.00%
[illegible]	DANIEL D	Absent	N/A	0.00%
[illegible]	[illegible]	Absent	N/A	0.00%

Figure 9. All Student's Attendance



Staff Entry Report

27-03-2025

Staff ID	Subject Code	Subject Name	Staff Name	Time of Entry	Time of Exit
S103	PHY301	Physics	Mr. Albert Wilson	09:20	09:26

Figure 10. Staff Attendance

A filtering option enables staff to fetch attendance data for a specific date, making it easier to track attendance patterns over time. Additionally, a staff attendance module allows staff members to monitor their own attendance records. Within the staff attendance section, further categorization is available to view attendance based on different academic years (2nd-year staff, 3rd-year staff, and 4th-year staff). Upon selecting a specific category, staff can view entry & exit times, helping in tracking their working hours effectively. This structured system enhances accessibility, simplifies attendance management, and ensures that both students & staff have transparent and organized records of their attendance data.

5. Conclusion

An IoT-based fingerprint attendance system transforms educational attendance management with modern technologies and user-friendly features. Biometric authentication ensures attendance records are accurate and secure. This eliminates proxy attendance and manual errors from roll calls and paper registers. After fingerprint authentication, the record is processed and stored in a cloud database for real-time monitoring and reliable record-keeping. This cloud storage integration lets administrators, faculty, and students access attendance data anytime, anywhere, improving convenience and transparency. The system also simplifies management with automated data synchronization, categorized staff records, and date-based attendance filtering. These features improve operational efficiency and reduce administrative workload. Beyond simplifying the routine process of attendance tracking, the system helps institutions reduce paperwork, save time, and transition toward a more technology-driven learning environment. Its robust design also incorporates offline reliability, ensuring that records are not lost during internet outages and are automatically updated once connectivity is restored. Looking ahead, the system provides a strong foundation for future enhancements, such as AI-based analytics to identify attendance trends and patterns, mobile application integration for easier accessibility, and the incorporation of additional authentication methods like RFID or NFC for added flexibility and scalability. By combining security, efficiency, and adaptability, the IoT-based fingerprint attendance system stands out as a robust and future-ready solution that not only addresses the shortcomings of traditional systems but also aligns with the growing demand for smart campus initiatives in modern educational institutions.

6. Future Recommendations

1) While the proposed Fingerprint-Based IoT Attendance System demonstrates significant improvements over traditional and existing IoT-based solutions, there remains considerable scope for further enhancement to make the system more advanced, scalable, and reliable.

2) One potential improvement is the integration of a dedicated mobile application for Android and iOS platforms, enabling students and faculty to conveniently access attendance records, receive real-time notifications, and manage their profiles on the go.

3) Another promising direction is the incorporation of artificial intelligence to analyze attendance patterns, detect irregularities, and generate predictive insights that can support better academic performance and classroom engagement.

4) To strengthen system security, multi-factor authentication can be implemented by combining fingerprint recognition with additional verification methods such as facial recognition, RFID, or one-time password (OTP) authentication, making the system more resistant to spoofing or unauthorized access.

5) Furthermore, adopting edge computing for data processing instead of relying solely on cloud servers would reduce latency, enhance offline reliability, and ensure faster response times, even in environments with poor internet connectivity.

6) Collectively, these enhancements would transform the system into a more robust, intelligent, and future-ready solution for educational institutions.

Declarations

Source of Funding

This study received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Competing Interests Statement

The authors declare that they have no competing interests related to this work.

Consent for publication

The authors declare that they consented to the publication of this study.

Authors' contributions

All the authors took part in literature review, analysis, and manuscript writing equally.

Availability of data and materials

Supplementary information is available from the authors upon reasonable request.

Institutional Review Board Statement

Not applicable for this study.

Informed Consent

Not applicable for this study.

References

[1] Rukhiran, M., et al. (2023). IoT-based biometric recognition systems in education for identity verification services: Quality assessment approach. IEEE Access, 11: 22767–22787. https://doi.org/10.1109/access.2023.3253024.

[2] Koppikar, U., et al. (2019). IoT based smart attendance monitoring system using RFID. In 2019 1st International Conference on advances in information technology (ICAIT), Pages 193–197, IEEE. https://doi.org/10.1109/icait47043.2019.8987263.

[3] Muhamad, W., et al. (2017). Smart campus features, technologies, and applications: A systematic literature review. In 2017 International conference on information technology systems and innovation (ICITSI), Pages 384–391, IEEE. https://doi.org/10.10.1109/icitsi.2017.8267975.

[4] North-Samardzic, A. (2020). Biometric technology and ethics: Beyond security applications. Journal of Business Ethics, 167(3): 433–450. https://doi.org/10.1007/s10551-019-04143-6.

[5] Wakchoure, S., et al. (2021). Multiple approach of RFID-based attendance system using IoT. In Soft Computing for Security Applications: Proceedings of ICSCS 2021, Pages 487–499, Singapore: Springer Singapore. https://doi.org/10.1007/978-981-16-5301-8_36.

[6] Adedoyin, M.A., et al. (2024). Development of an IoT-Based Biometric Attendance Management System. FUOYE Journal of Engineering and Technology, 9(3): 397–405. https://doi.org/10.1007/978-981-99-4433-0_32.

[7] Shinge, S., & Urmila, S. (2025). Empowering Education Industries with a Cloud Based IoT Framework. In 2025 4th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0, Pages 1–5, IEEE. https://doi.org/10.1109/otcon65728.2025.11070865.

[8] Suresh Kumar, K., Ananth Kumar, T., Radhamani, A.S., & Sundaresan, S. (2020). Blockchain technology: an insight into architecture, use cases, and its application with industrial IoT and big data. In Blockchain Technology, Pages 23–42, CRC Press. https://doi.org/10.1201/9781003004998.

[9] Moradi, M., et al. (2022). Security-Level Improvement of IoT-Based Systems Using Biometric Features. Wireless Communications and Mobile Computing, (1): 8051905. https://doi.org/10.1155/2022/8051905.

[10] Raj, E., et al. (2025). Hybrid Attendance System: Speech Recognition and IoT Hardware Integration. In 2025 6th International Conference on Inventive Research in Computing Applications (ICIRCA), Pages 504–508, IEEE. https://doi.org/10.1109/icirca65293.2025.11089680.

[11] Suresh Kumar, K., Radhamani, A.S., & Sundaresan, S. (2021). Proficient approaches for scalability and security in IoT through edge/fog/cloud computing: a survey. International Journal of Data Science, 6(1): 33–44. https://doi.org/10.1504/ijds.2021.117465.

[12] Kolonko, L., Maus, G., Velten, J., & Kummert, A. (2024). Early promotion of academic education through practical courses in the context of smart IoT systems. In 2024 IEEE 67th International Midwest Symposium on Circuits and Systems, Pages 1413–1417, IEEE. https://doi.org/10.1109/mwscas60917.2024.10658707.