International Journal of Electrical and Computer Engineering (IJECE)
Vol. 15, No. 6, December 2025, pp. 5616~5632
ISSN: 2088-8708, DOI: 10.11591/ijece.v15i6.pp5616-5632

Design and development of home-grown biometric fingerprint device and software for attendance and access control

Jumoke Soyemi[1], Ogunyinka Olawale Ige[2], Olugbenga Babajide Soyemi[3], Ajibodu Franklin Ademola[4], Adaramola Ojo Jayeoba[2], Afolayan Andrew Olumide[5], Habeeb O. Amode[1], Mukail Aremu Akinde[6]
[1]Department of Computer Science, School of Pure and Applied Sciences, Centre for Information and Communication Technology, Federal Polytechnic Ilaro, Ilaro, Nigeria
[2]Department of Computer Engineering, School of Engineering, Federal Polytechnic Ilaro, Ilaro, Nigeria
[3]Department of Civil Engineering, School of Engineering/Innovation Centre, Federal Polytechnic Ilaro, Ilaro, Nigeria
[4]Department of Electrical Engineering, School of Engineering, Federal Polytechnic Ilaro, Ilaro, Nigeria
[5]Department of Science Laboratory Technology (Physics Electronics), School of Pure and Applied Sciences, Federal Polytechnic Ilaro, Ilaro, Nigeria
[6]Department of Taxation, School of Management Studies, Federal Polytechnic Ilaro, Ilaro, Nigeria

Article Info

Article history:

Received Mar 13, 2025
Revised Aug 6, 2025
Accepted Sep 14, 2025

Keywords:

Access control
Attendance
Biometric device
Home-grown biometric device
Smart campus
Technology

ABSTRACT

This study details the design, development, and deployment of an Android-based Biometric Fingerprint system tailored for institutional access control, attendance tracking, exam monitoring, and staff management. Developed collaboratively by the Innovation Centre and departments across engineering and information and communication technology (ICT), the system integrates custom hardware and software. Hardware includes fingerprint sensors connected to an ATMEGA8 microcontroller and Android interfaces for portability. The software uses modular architecture, comprising a Kotlin-based mobile app with Jetpack Compose, a Laravel-powered web admin panel, and a secure backend API hosted on a virtual private server (VPS). Fingerprint data is safely stored using base64 encoding, enabling accurate user authentication and real-time tracking. A functional prototype was built, tested, and refined, with 95 units deployed in a pilot phase. The system supports multiple fingerprint profiles, secure data handling, and integration with existing institutional platforms. Emphasizing customization, modularity, and adherence to ICT policies, the research also serves as a training tool for staff and students, enhancing operational efficiency and supporting local technology development. Performance evaluation showed a FAR of 0.5%, FRR of 1.2%, and an average authentication time of 2.3 seconds. Post-deployment, student attendance increased by 15%, fee compliance by 10%, and 89% of users rated the system as easy to use. This work demonstrates effective hardware-software co-design for scalable biometric authentication in educational settings.

Corresponding Author:

Jumoke Soyemi
Department of Computer Science, School of Pure and Applied Sciences, Federal Polytechnic Ilaro
Ogun State, Nigeria
Email: jumoke.soyemi@federalpolyilaro.edu.ng

1. INTRODUCTION

The need for educational institutions to modernize their administrative processes is increasing in response to growing student populations, evolving academic demands, and the need for enhanced security. One of the most persistent among these challenges is the accurate and efficient, effective, and proper

accountability of students and staff attendance and controlling access to restricted areas [1]–[4], including examination halls, libraries, laboratories, and staff offices. In most institutions, attendance is still recorded traditionally using a paper-pen procedure or plastic ID cards, which are prone to manipulation, errors, impersonation, and administrative delays [5], [6]. Such limitations have the potential to negatively affect the monitoring of student performance, adherence to regulations, and accountability.

The main problem this research seeks to address is the inadequacy of existing attendance and access control systems in providing secure, real-time, and tamper-proof identification and monitoring of users in educational environments. As institutions grow in size and complexity, particularly in developing contexts such as Nigeria, the need for scalable, cost-effective, and context-aware solutions becomes critical. The research, therefore, seeks to answer the question: How can a locally developed biometric fingerprint system be designed and implemented to meet the specific attendance and access control needs of a large academic institution, while being affordable, scalable, and sustainable?

Biometric technologies, particularly fingerprint recognition, have emerged as a leading solution [7]–[9] in identity management across multiple sectors due to their affordability, high accuracy, and ease of deployment. Fingerprint authentication stands out [10]–[12] because it leverages unique physiological traits that are difficult to forge, thus offering a secure, non-invasive, and efficient method of verifying identity [13]–[17]. While many commercial biometric systems are available, they often fail to meet the unique demands of educational settings. These off-the-shelf solutions tend to be expensive, rigid in functionality, dependent on foreign vendors, and unable to accommodate local operational peculiarities such as irregular schedules, data privacy concerns, and offline data collection needs.

This paper presents a novel solution in the form of a home-grown, Android-based biometric fingerprint device and a custom-built software system designed specifically for attendance and access control within a higher education institution in Nigeria. The research is a multidisciplinary team project at the Federal Polytechnic Ilaro, which combines hardware and software innovations to deliver a mobile, user-friendly, and cost-effective biometric system. The formulation and implementation of the integrated biometric system have primary objectives of not only addressing the inadequacies of the traditional and commercial systems available but also the creation of local technical capacity and institutional self-sustaining technological advancements. The research uses the combination of hardware and software co-design methodology to meet its goals. On the hardware aspect, the system was designed on microcontrollers ATMEGA8, together with fingerprint sensors and an Android-based user interface to ensure functionality and portability. The software is structured in a modular manner and consists of a mobile application based on Jetpack Compose and Kotlin, a web administrative system created on Laravel, HTML5, CSS3, and JavaScript, and a backend API located on a virtual private server (VPS) that supports secure transfer of data.

One of the key technological aspects of the system is the support of a biometric authentication algorithm, which transforms fingerprint information into the base64 encoding form for secure and efficient comparison during identity verification [18]–[20]. The system architecture allows real-time attendance tracking, secure fingerprint storage, multiple user fingerprint profiles, and seamless integration with existing institutional data systems. In the design and deployment process, the research places a high priority on customization, modularity, and data sovereignty, whereby the system should fit the institutional policies of ICT and local conditions of operation.

This study has several novel contributions that make it stand out compared to the current commercial-based biometric attendance and access control in the context of educational institutions in developing countries. First, the research offers a homegrown, fully customizable biometric fingerprint system that is both software and hardware integrated. This is opposed to commercial systems, which usually come with more set features and vendor constraints. This system is made purposely for institutional use in environments that have their problems of logistics and infrastructure issues to overcome. The integration of fingerprint sensors into lightweight Android devices provides mobility and flexibility that was not possible in biometric installations that were set up in specific locations.

Second, the system facilitates the closure of technological innovation and local capacity building. The student and staff participation in design, assembly, and deployments made the chain value sustainable, whereas the end users also contributed to the development. The project facilitates skill transfer, ownership of technology, and cuts reliance on external technologies. Third, a new dual-mode (online/offline) biometric validation mechanism is one of the most important developments in settings where infrastructure is constrained. With periodic synchronization to the backend, the local device-level fingerprint matching algorithm works to ensure that the system still functions even on campuses that are remote or offline. Finally, the system enables multidimensional utilization other than attendance, which includes school fees payment validation, library access, hostel access, and administrative meeting attendance on the platform, which also substantiates the scalability and versatility of the platform. Overall, the research translates an important contribution to the ambit of educational technology by showing that locally developed solutions of biometric

technology can serve as an effective instrument in the development of institutional efficiency, accountability, and digital transformation.

To provide evidence of the feasibility and the effectiveness of this approach, the structure of this paper consists of six parts. The research problems, background, motivation, and contribution to the current knowledge are presented in the current section. The second part outlines the process of designing and developing the hardware of the biometric fingerprint device, its physical architecture, component choice, and prototyping. The third segment presents the software system architecture by emphasizing the development of mobile and web applications, system integration, and a fingerprint authentication algorithm. The fourth section displays the implementation outcomes, such as performance assessment and pilot deployment insights. The fifth section goes into detail in discussing the findings and the overall implications of the system later concerning education and technology. The conclusion is the final part of the study, which summarizes the contributions of this study and provides future research directions.

2. SYSTEM DESIGN AND IMPLEMENTATION

2.1. System design

The need to develop a mobile, reliable, and context-sensitive attendance and access control solution that can suit educational institutions informed the design phase of the biometric fingerprint system. A user-centered design approach based on understanding the reality of operating in the institution, including the large classes, minimal network infrastructure, and the requirement to do real-time data collection and reporting, was at the core of the design process in this case.

The conceptualized system was an android-based biometric device that would be integrated with a customer-built application software. Portability, fast fingerprint identity verification, data storage capacities, and wireless communication hardware were defining features of the design. The practical challenges that influenced these features included those relating to bottlenecks encountered on sign-ins into classes, the necessity to authenticate attendance via various access points, and the administrative overhead of manual reporting of attendance. The design also included a tougher physical casing that would allow handling of intense environments where handling rates and usage conditions were diverse.

To enhance functionality and future scalability, the system was also conceived to support facial recognition and iris scanning. While these features were not implemented in the current prototype, they were embedded in the design architecture to allow easy integration in future iterations. This foresight highlights the system's adaptability and potential for evolution, distinguishing it from rigid commercial biometric products.

2.2. Hardware development

Figure 1 is the block diagram of the biometric system. The hardware development process was executed in three distinct phases, each building on the successful completion of the previous. In the first phase, in Figure 2, the circuit design was prototyped using an open and tested to ensure correct interfacing between the core components, including the fingerprint sensor, microcontroller, display screen, and power supply unit. A key design consideration was the use of low-power, high-efficiency components that could support extended use in lecture halls and remote classrooms without frequent recharging.

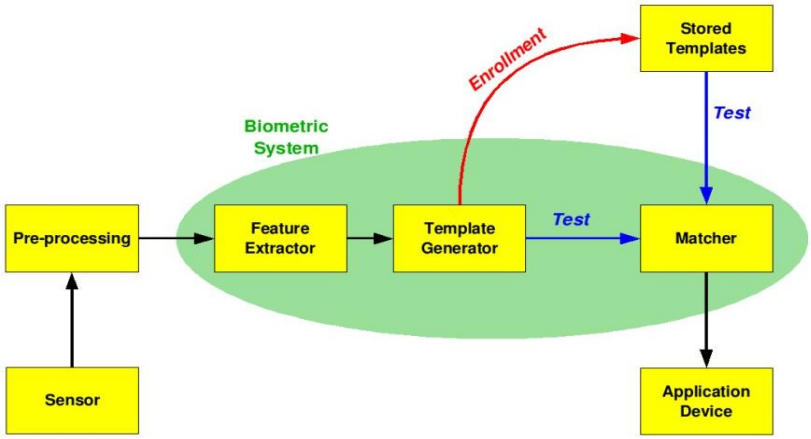


Figure 1. The basic block diagram of a biometric system

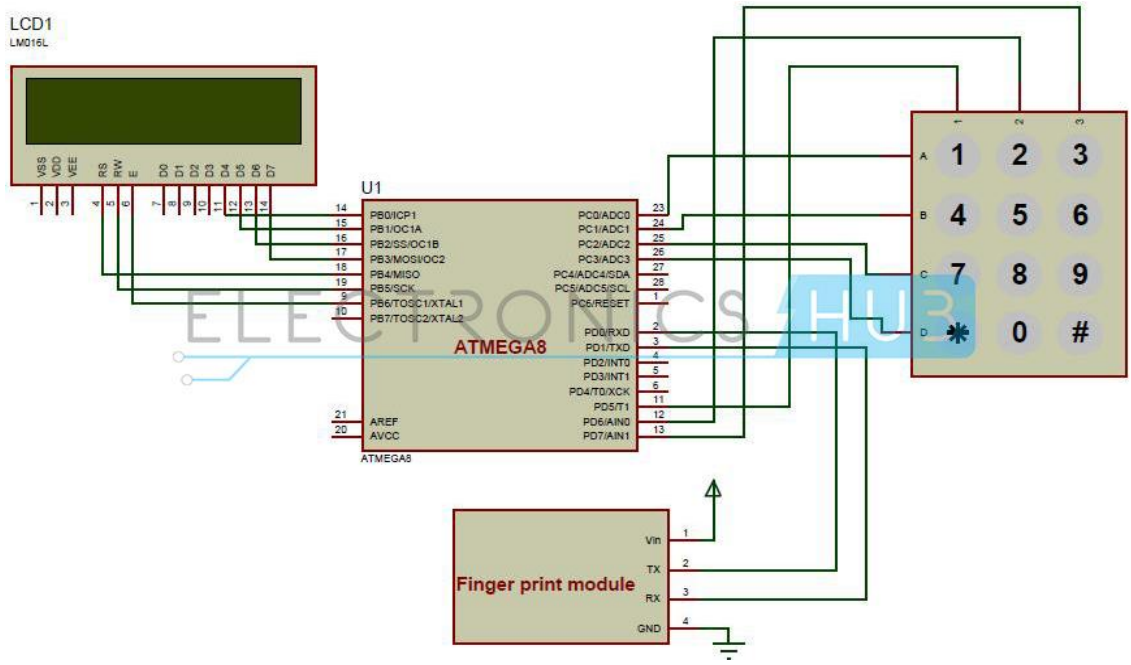


Figure 2. Circuit diagram of the biometric device [21], [22]

The second phase, Figure 3, included the purchase of all the important hardware components. These were capacitive HFP 360 fingerprint sensors, PCB terminal block - MKDS 1/ 2-3,5 HT BK (for the initial system design), ARM-based microcontrollers (for final hardware system design and implementation), 8-inch touch-screen LCD Gorilla Glass 1200×1920 TFT display, 10,000 mAh lithium-polymer battery, and communications modules (Wi-Fi and Bluetooth), direct conversion receiver, processor Atmega32, battery management system, Mini-circuits, TC4-14+, RF transformer 4:1, PCB for DE9941A SDR demonstrator and many connectors. The criteria used to choose the components were cost versus durability and performance trade-off. Indicatively, the selection of optical fingerprint sensors justified the fact that optical sensors were not only reliable but also not costly to make them viable in a large-scale setting within an academic setup.

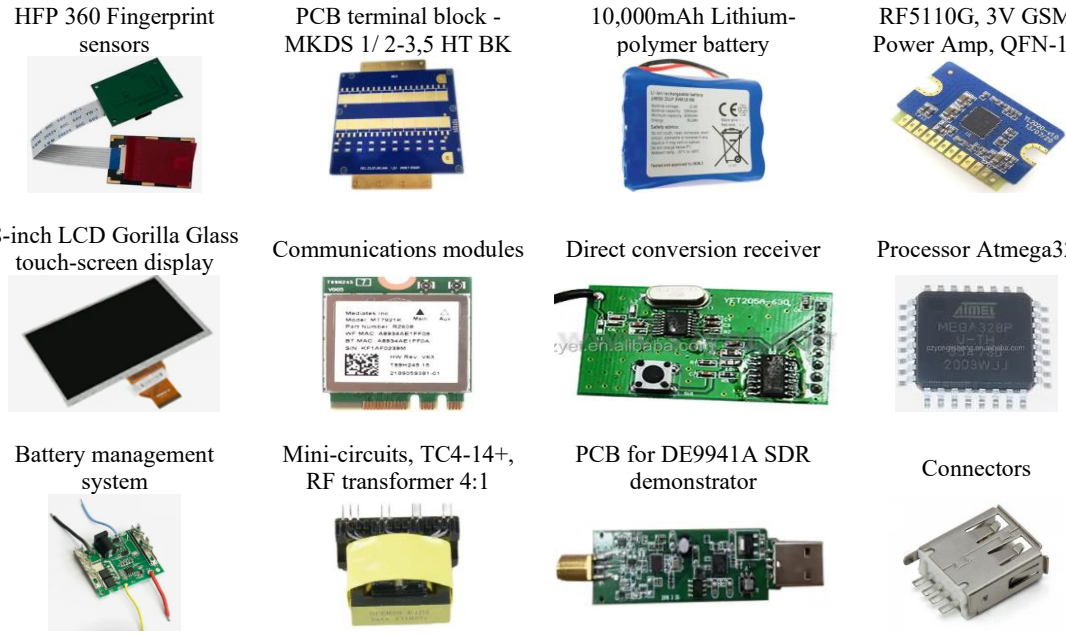


Figure 3. Important hardware components of the biometric attendance device

2.3. Simulation of a microcontroller-based biometric verification system

The simulation of a microcontroller-based biometric verification system consists of three main parts: the host controller, the fingerprint sensor, and the internet link, as displayed in Figure 4. The host controller can work in either enrollment mode or scan mode. When in enrollment mode, the host controller receives fingerprint data from the fingerprint sensor. This fingerprint data represents the Hexadecimal format. The host controller then matches this fingerprint data with a user ID and uploads it to the cloud via the internet link. When in scan mode, the host controller receives fingerprint data from the sensor and sends it to the internet link, which searches the database for the user ID linked with that hex code. If it exists in the database, it returns the user ID to the host controller, which displays it on the screen. If there is no user ID on the database linked to that name, it displays the error message "NOT FOUND."The fingerprint sensor is a subsystem that consists of a capacitive sensor, a microcontroller that translates the output of the capacitive sensor into digital signals and communicates with an external system via serial communication (USB), and a power supply to convert the battery's voltage to 3.3V for the capacitive sensor and the control circuitry. An internet connection is a subsystem that comprises a SIM module (of GSM or 2G, HSDPA or 3G or LTE or 4G). It also possesses a controller that runs the SIM module upon command permission from an outer host controller. It passes this information to the host controller through UART. Most SIM modules work on 1.8-3.3 V, hence the internet connection subsystem has its own regulator that steps the battery down to something that can be used. Three of these communication modules (HFP360) will convert USB signals to UART signals since the ATMega328 is not allowed to use USB. It has UART, I2C, and SPI. The fingerprint sensor is communicated using a USB-to-UART communication module.

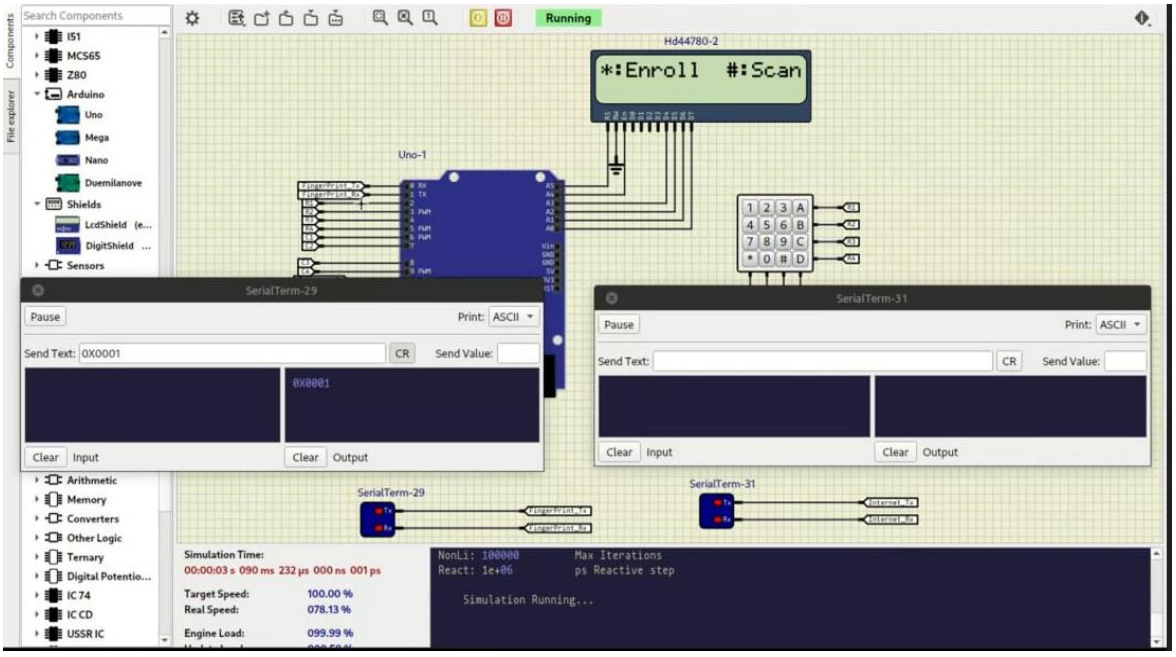


Figure 4. Schematic diagram of the simulation

The last stage of hardware development, depicted in Figures 5 and 6, was the assembly of all components into one device and the creation of a physical enclosure with AutoCAD in Figure 5. The enclosure (casing) developed was then 3D-printed with plastic for the prototype casing and was rubber-padded to allow it to survive impact. Ergonomics was also taken into consideration so that the device could be easily carried and used by faculty and administrative personnel when taking attendance. Upon the completion of the assembly, every unit went through a set of durability and environmental tests to ensure its strength and operational stability in different conditions.

Figure 5 is a 2D design of the device drawn using AutoCAD. The design features a fingerprint scanner, Android display, microcontroller, power button, USB port, card slot, and optional wireless communication interfaces. Figure 6 shows the assembled biometric attendance device with the external rubber-studded cover for the casing. This shields away from external damage, thus making it safe and secure.

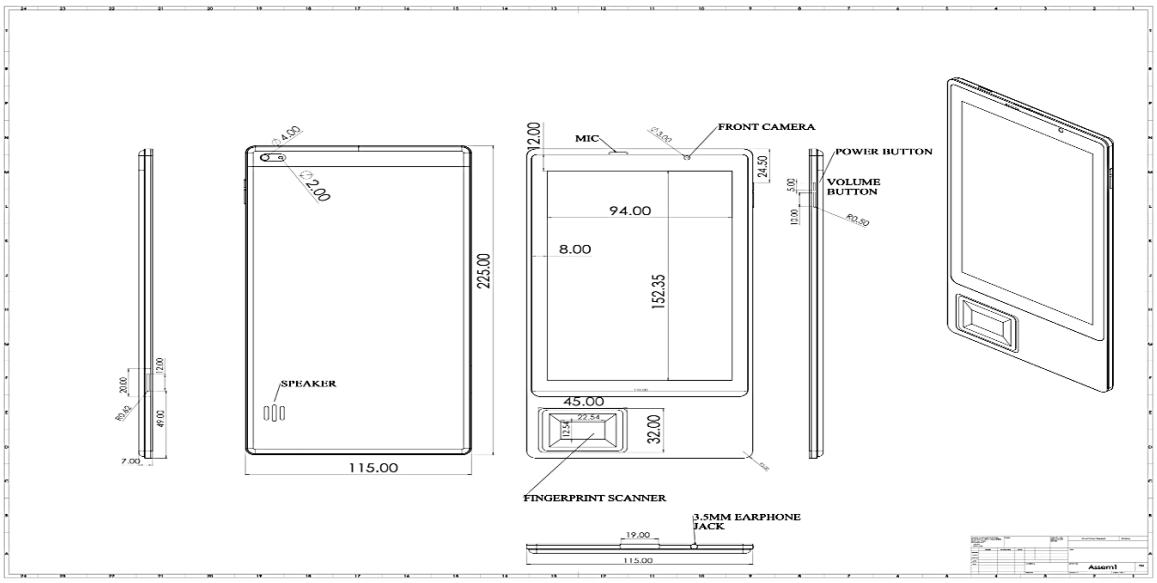


Figure 5. 2D design drawing of the biometric

Figure 6. Customized mobile biometric attendance device

2.4. Software development

The software aspect of the solution was designed as a two-platform implementation, including a mobile app and a web-based dashboard that are connected with each other via a safe RESTful API. Jetpack Compose and Kotlin were used to create a mobile application and take advantage of the Android strong development framework, whereas Laravel (PHP), HTML5, CSS3, and JavaScript were used to create a web portal allowing flexible administrative access and on-time reporting. The main purpose of the mobile application was to scan biometric data, match the fingerprint against the stored templates, and make an attendance entry. The data would be sent to the server in real-time or in batches, depending on the network availability. This online-offline model played a significant role when it came to the functionality within environments characterized by intermittent internet coverage. The application also accommodated registration of up to five samples of fingerprints per person, making it much more resistant to situations involving finger injury or failure of authentication.

Web-based administrative dashboard was provided with functionality to register students and staff, monitor attendance, create events, as well as generate statistics. Administrators could add bulk student records using CSV or APIs, control attendance by events, such as meetings or exams, and report to assist in decision making. The data exchanges were also encrypted and hosted on a VPS under Ubuntu 18.04 with Apache, which guarantees safe and scalable deployment. An OTP authentication system through SMTP was also set up to protect access to sensitive controls by the admins.

2.5. System implementation and testing

The last development phase was the integration of the hardware and the software into a functional, coherent system with the consequent intensive pilot testing. Their implementation started with a pilot of 2 units financed by the Federal Polytechnic, Ilaro Management, and after the successful launch with all

functions working as designed, an additional 95 units were produced with the support of the Tertiary Education Trust Fund (TETFund). The devices were deployed among the various departments that were chosen to be tested live in real operating environments. The testing was in the context of fingerprint matching speed, attendee log accuracy, user acceptance, and ease of use. The fingerprint authentication procedure had an average of fewer than 2 seconds per user, an accuracy value of more than 98 percent, with an effectiveness rate of 100 percent, confirmed by a controlled test of more than 500 people. Initial bugs involving clashing database entries and UI latency, among others, were determined using user feedback and fixed on an iterative basis.

Students and staff training was undertaken to facilitate appropriate use and develop a sense of ownership. The training sessions also involved local capacity building to allow departmental staff and students in Engineering and ICT to develop practical experiences using biometric devices, data management, and hardware assembly. The system was seen to be so effective when it comes to real-time attendance monitoring, especially during mass events like the Academic Board Meeting, where the system was used instead of manual signature registers. Lecturers described better attendance in classes, and administrators valued less time given to reconciliation of attendance and monitoring compliance. The mobile nature of the system also made it deployable in off-site lecture halls, which served to increase its flexibility in terms of operation.

3. SOFTWARE SYSTEM ARCHITECTURE AND IMPLEMENTATION

The software system was implemented in the form of a framework that was designed to tackle the problem of real-time tracking attendance, verification of identities, and controlling access to resources within a decentralized educational system. The biometric attendance system was designed as a 3-tier solution that consists of a mobile app, a web app, and an API that cooperate to provide the users with smooth data flow, secure validation of fingerprints, and effective reporting.

3.1. System architecture overview

The overall system architecture was designed with modularity, scalability, and security as core principles. As shown in Figure 7. The architecture consists of a mobile-based biometric capture application, a web-based administrative portal, and a centralized backend API hosted on a VPS. The Android-based mobile application handles biometric enrolment, validation, and attendance marking. It communicates with the backend via encrypted requests, either in real-time or deferred when offline.

The API server is installed in a secure Ubuntu 18.04 with an Apache framework and performs the task of communication between the biometric equipment and the administrative dashboard. It keeps biometric templates, user profiles, and attendance records in a well-organized database and makes endpoints available to access data, manage events, and report. This tiered system means that there is still a functioning continuity of devices regardless of whether the connection is working, as they may store data locally and resync it later.

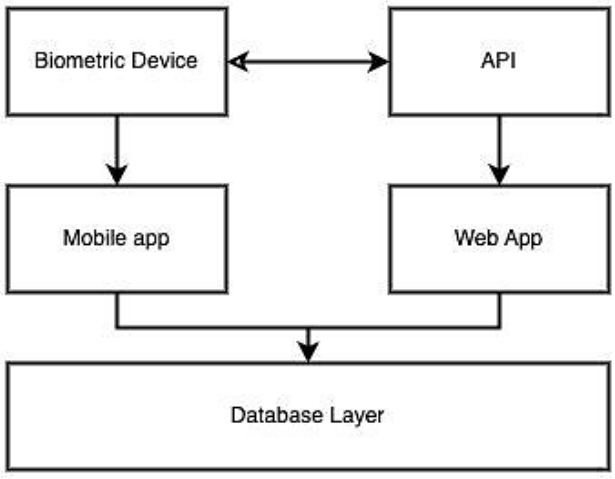


Figure 7. Systems architecture of the biometric system

3.2. Mobile application functionality

The mobile application is written in Jetpack Compose, together with Kotlin, due to its modern, declarative UI patterns and support of Android hardware. The application interface was made user-friendly and simple to navigate, particularly with academic employees who are not very conversant with high-tech. Fingerprint enrolment and validation are also another major attribute of the mobile app, and it supports enrolment up to five fingerprints per individual. Such redundancy will maintain functionality, whereby an injury or poor-quality fingerprints would have otherwise inhibited verification.

Attendance validation occurs through the biometric scanner integrated into the custom Android device. Once a user places a finger on the sensor, the captured biometric data is converted into a Base64 string and securely transmitted to the API for comparison. Upon a successful match, attendance is automatically marked as "present," and a confirmation is displayed. In the case of a failed match, the user is prompted to retry using another registered finger, thereby reducing false rejections. Additional functionalities in the mobile app include real-time dashboard updates, offline mode for remote locations, and seamless synchronization of attendance data. Figures 8 to 10 show some of the various activities that can be performed within the mobile application.

Figure 8(a) is the landing page of the Biometric fingerprint attendance application launched on the mobile device. When launched, the application loads directly to the dashboard as shown in Figure 8(b), showing five modules: Student registration, staff registration, student attendance, staff attendance, and examination attendance. Each module is activated based on the operation to perform at any point in time.

(a) (b)

Figure 8. Various activities that can be performed within the mobile application: (a) biometric device landing page and (b) biometric device dashboard

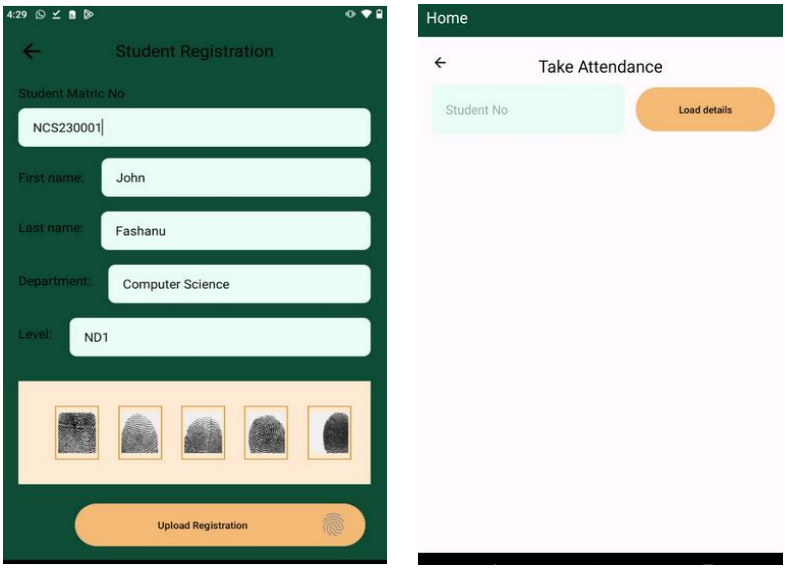
Figure 9(a) shows the student biometric capturing/registration page, allowing five fingers to be captured per student. When a student's matriculation number is entered, the system retrieves data only for eligible students; defaulters are automatically flagged. Biometric data is then captured for eligible students. Figure 9(b) is the student attendance page, where attendance is done by simply inputting the matric number, granting access to services such as class attendance, examinations, the library, the laboratory, hostel facilities, and gate access.

Figure 10(a) shows how staff biometrics are captured just like those of the students. The staff number is entered and fetches the information from the database for biometric registration. The staff can then carry out sign-in and sign-out each day as shown in Figure 10(b). Figure 10(c) is a typical staff sign-in and sign-out at a section of the campus different from other parts of the campus.

3.3. Web-based administrative portal

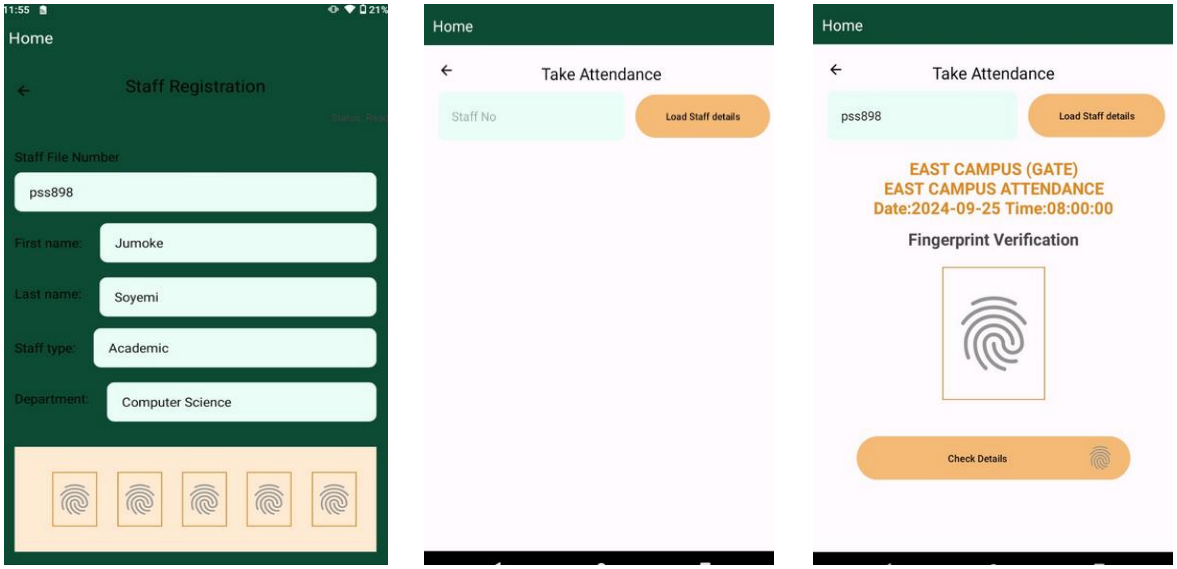
The web application was developed using Laravel (PHP framework) alongside standard web technologies (HTML5, CSS3, and JavaScript) to provide administrative control over the biometric system. The portal is accessible only to authorized personnel and includes multiple features such as student/staff

registration, attendance analytics, and system configuration. Admins can bulk upload users via CSV or automatically sync with existing student information systems through the student API.



(a) (b)

Figure 9. Various activities that can be performed within the mobile application: (a) biometric student registration and (b) biometric student attendance

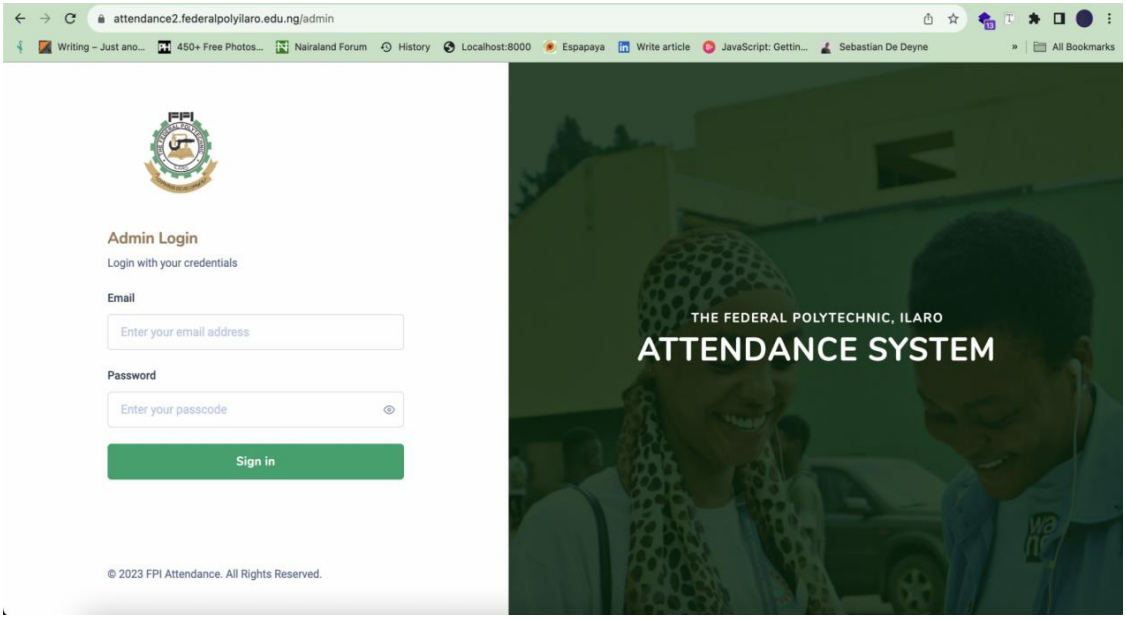


(a) (b) (c)

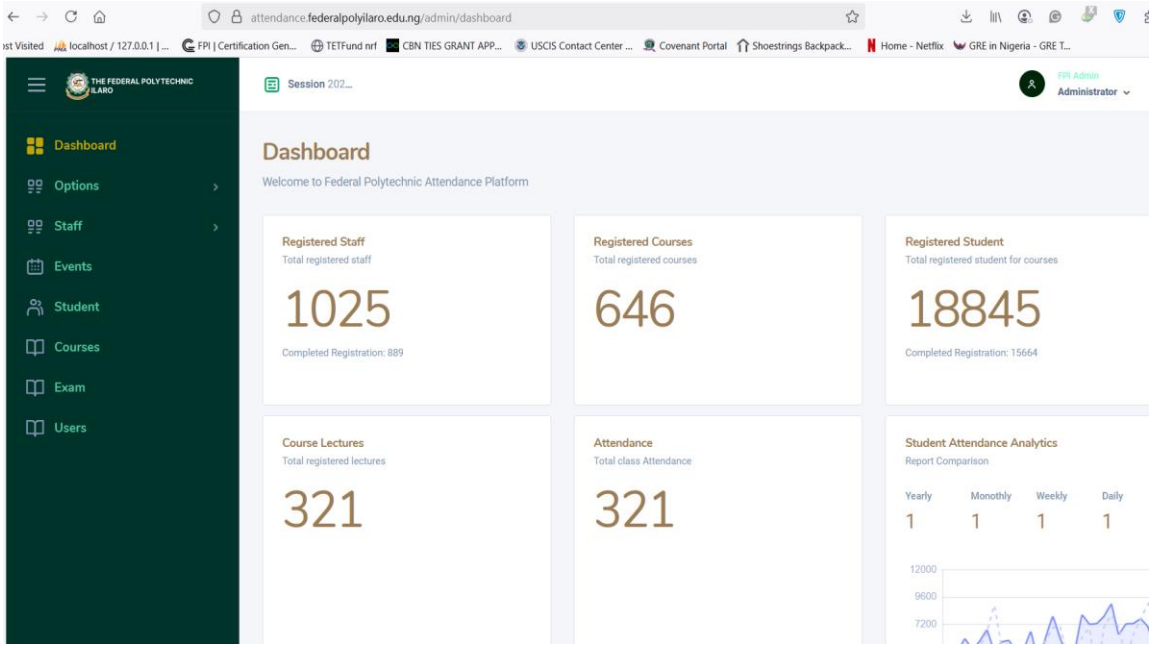
Figure 10. Various activities that can be performed within the mobile application: (a) biometric registration, (b) biometric attendance, and (c) biometric attendance sign-in-out

Figures 11 to 13 illustrate some of the components of the administrative dashboard. These include the login interface, the registration pages for students and staff, among others. The application also supports custom reporting features. Attendance data can be exported for audits, compliance checks, and academic performance correlation. The system flags irregular attendance patterns automatically, providing early warning signals for intervention. Feedback from administrators indicated that the dashboard significantly reduced the time spent manually compiling attendance records, especially during mass events like matriculation or exams.

Figure 11 is the Admin/Dashboard page. To gain access to the admin dashboard, the admin will navigate to the administrator's login page shown in Figure 11(a) and provide valid login credentials. The admin dashboard, as shown in Figure 11(b), gives statistics on the registered number of Students and Lecturers, and it also includes the number of courses and attendance. These figures change in real time.



(a)



(b)

Figure 11. Administrative dashboard (a) Admin login page and (b) Admin dashboard page

Figure 12(a) shows a list of all staff and also indicates staff who already have their biometrics captured and registered. Administrators can register staff manually to capture new members of staff or perform bulk uploads using CSV files in case of multiple members of staff. The same goes for Figure 12(b). However, students' data can be fetched directly from their school portal by connecting to an API.

Figure 13 shows a particular lecturer page with Figure 13(a) displaying the dashboard that 2 courses and 2 classes were registered by the Lecturer with 1,413 students altogether. Figure 13(b) displays the

2 courses that can be expanded further to display the details of lectures taken, and the students' attendance in percentage as seen in Figure 13(c). Only one class was recorded at this time.

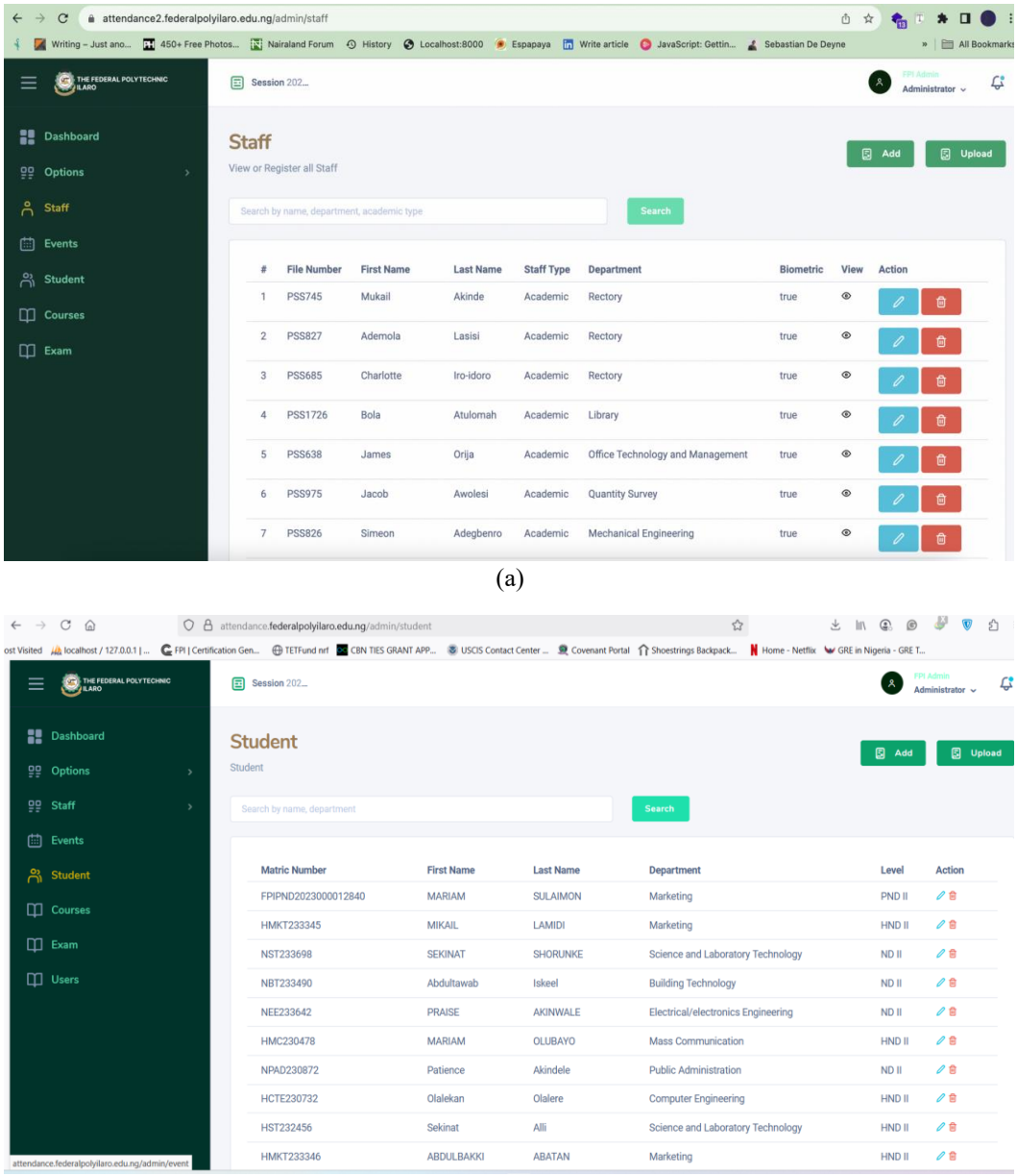
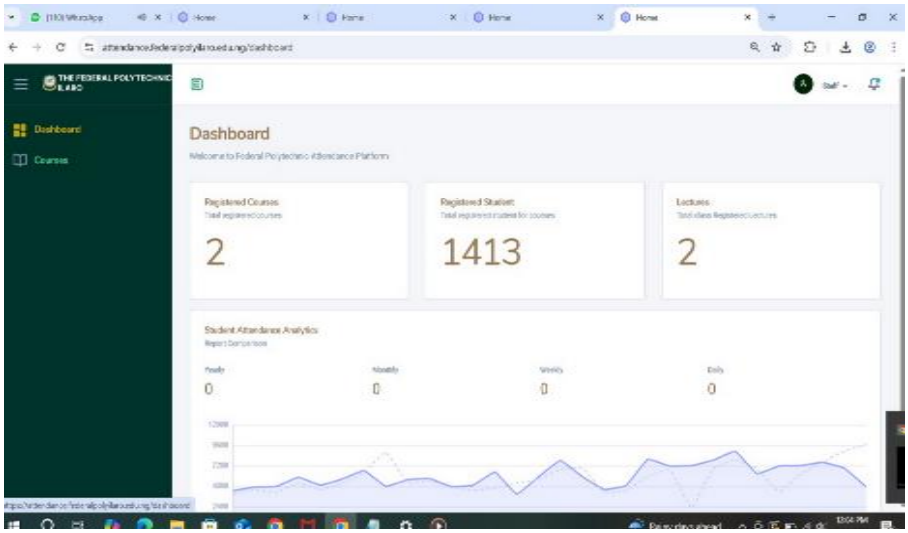


Figure 12. Administrative dashboard (a) registered staff page and (b) registered students page

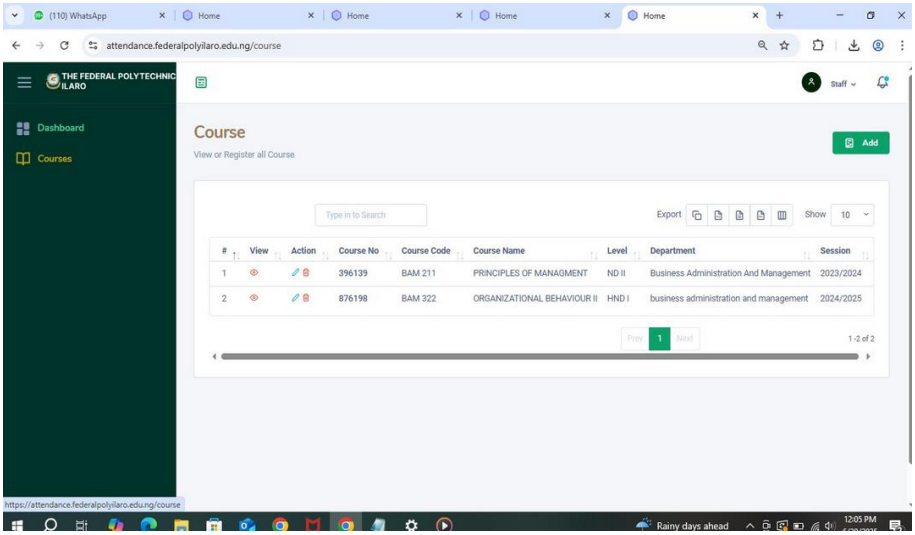
3.4. Biometric authentication algorithm

The fingerprint authentication process follows a two-stage algorithm: registration and verification. During registration, fingerprint inputs are captured, converted to base64 format, and sent to the server for secure storage alongside associated user data. During verification, the system compares the input against stored templates to determine a match. This logic is implemented both on the device and in the backend API to ensure quick local matching and remote verification when needed.

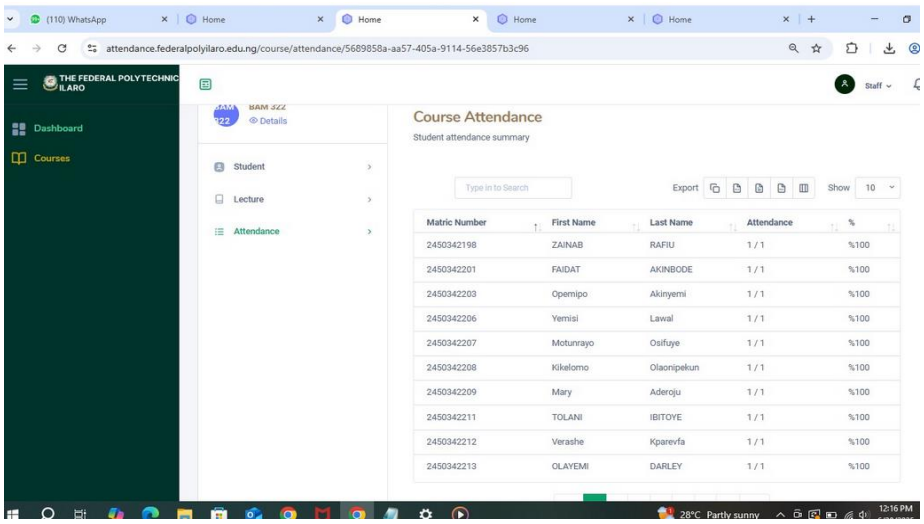
This dual-mode logic enables the system to remain functional even during server outages or in areas without internet connectivity. Local matches allow for uninterrupted attendance logging, while periodic syncing ensures consistency in central records. This architecture is particularly useful in large institutions like the Federal Polytechnic Ilaro, where multiple departments and remote lecture centers exist.



(a)



(b)



(c)

Figure 13. Administrative dashboard (a) lecturer's dashboard, (b) lecturer's registered courses, and (c) lecturer's student attendance

4. SYSTEM PERFORMANCE METRICS AND COMPARISON

4.1. System performance metrics

The system's biometric recognition accuracy and responsiveness were evaluated during a six-month pilot phase. Key performance indicators (KPIs) such as false acceptance rate (FAR), false rejection rate (FRR), and average authentication time were recorded and compared to those of commonly used commercial systems, as seen in Table 1.

The system's FAR and FRR are within acceptable ranges for biometric applications, indicating high accuracy. The slightly higher FRR relative to commercial systems is offset by the system's cost-effectiveness and full local control. Authentication speed was fast enough to prevent bottlenecks during peak attendance times. Also, the attendance compliance improved notably after system implementation. Departmental attendance rates were monitored over an academic semester, showing an average increase of 15% in student attendance and a 10% rise in fee payment compliance linked to biometric deployment. The results can be seen in Table 2.

Table 1. System performance metrics comparison

Metric	Our System	Typical Commercial Systems [24,25,26]
False acceptance rate (FAR)	0.5%	0.2% - 0.6%
False rejection rate (FRR)	1.2%	0.8% - 1.5%
Average authentication time	2.3 seconds	2 - 3 seconds
System uptime	99.7%	98.5% - 99.9%

Table 2. Comparison of attendance and fee compliance pre- and post-implementation

Metric	Pre-Implementation	Post-Implementation
Average class attendance (%)	68	83
Fee payment compliance (%)	72	82

These outcomes suggest that integrating biometric attendance with fee compliance mechanisms effectively incentivizes student participation and institutional revenue assurance. A survey of 1,500 users (students and staff) conducted three months after deployment revealed that 89% found the system easy to use, 93% trusted the biometric verification process, and 85% preferred mobile fingerprint devices over the previous manual attendance systems, highlighting strong user acceptance and notable operational improvements.

4.2. Comparison with prior work

Unlike commercial biometric systems referenced in prior studies [23]–[25], which typically rely on fixed hardware and cloud-based storage, our system offers on-premises data sovereignty and mobile hardware flexibility. The modular, open-source software architecture facilitates customization and continuous local development, features lacking in many proprietary solutions. While biometric accuracy is comparable to global standards, our system excels in scalability and cost-efficiency, which is key for educational institutions in developing countries. The link between biometric verification and fee enforcement is novel integration, seldom reported in existing literature, providing an innovative approach to improving institutional governance and student compliance. Moreover, the system's success in building local capacity through student involvement in hardware and software development sets a precedent for sustainable technological adoption in similar contexts.

5. DISCUSSION OF FINDINGS AND FUTURE IMPLICATIONS

Deployments of the home-grown biometric fingerprint attendance system have produced a huge outcome which underscores its reliability, flexibility, and situational aptitude. The system developed was deployed in the various units of the Federal Polytechnic, Ilaro, where it is used by over 10,000+ of the 19,000+ students and hundreds of staff. This has been used in attendance of classes/exams, authentication of tuition fees, accessing gates, and participation in meetings. This widespread use reflects the utility of the system and its ability to deal with objects of real-world institutional needs.

One of the major findings is the system's ability to function without dependence on third-party infrastructure, a contrast to many commercial biometric solutions that rely heavily on proprietary cloud storage or centralized vendor support. This addresses a key limitation in prior systems, such as those described in [23]–[25], where institutions expressed concerns over data security, high acquisition and licensing costs, and the inability to customize for specific local workflows. In contrast to these commercial

systems, our implementation supports full data sovereignty and on-premises control of biometric records, aligning with institutional governance policies and enhancing trust in the system. Moreover, the modular design of our solution allowed for iterative updates during the pilot phase, including performance optimization, durability improvements to the hardware, and expanded biometric capture (supporting five fingers per user).

Another outcome was the observed increase in attendance compliance across departments. Since the biometric system was integrated with student fee validation, students were compelled to regularize their payments and maintain consistent class attendance. This behavioral impact echoes findings in earlier studies [26], [27] that biometric enforcement mechanisms reduce absenteeism, but our approach goes further by linking compliance directly with access control at campus gates, a feature rarely reported in literature but highly effective in our context. Furthermore, our use of Android-based devices with fingerprint sensors, rather than fixed wall-mounted biometric devices, addressed the mobility limitations observed in earlier systems. This innovation is particularly significant in a large and growing institution like Federal Polytechnic, Ilaro, where lectures and exams are held across scattered buildings and locations. The portable design ensured minimal congestion, improved real-time data synchronizing, and allowed for flexible deployment during fieldwork or examination periods, capabilities not typically supported by proprietary biometric systems.

Comparatively, our system also expands on the open-source biometric pipeline by integrating Kotlin and Jetpack Compose for mobile development, a web interface built with Laravel, and an API hosted on a virtual server. This aligns with modern development trends while maintaining affordability and scalability. User feedback further supported these technical findings, with both staff and students expressing satisfaction with the system's ease of use, speed, and accuracy. Importantly, the training component embedded within the project, where students were involved in hardware assembly and software testing, demonstrated the feasibility of capacity transfer and skills development, adding educational value alongside technological innovation.

The results of this study demonstrate that a locally developed, fully integrated biometric system can perform as reliably as commercial alternatives while offering greater customization, lower costs, and added socio-technical benefits. These findings not only validate the design decisions made during the system's development but also advance the field by providing a replicable model for indigenous biometric solutions tailored to educational institutions.

This paper has a number of impressive future implications, making its applicability more than just pertinent in this case study. First, it demonstrates a scalable model that can be scalable and replicable in other tertiary institutions in Nigeria and other comparable situations in other countries of the world, especially in settings where financial resources as well as increased security requirements render commercial-based biometrics systems unviable. This project also preconditions the subsequent integration of multi-modal biometric authentication into the system, which encompasses facial and iris recognition, thus increasing the system's robustness on the basis of multi-factor authorship authentication methodologies.

The system is useful in the wider context of digital transformation of education, as it allows data-driven administration of attendance, academic results, and ways of distributing resources. Not only does this enhance efficiency in the administration, but it also assists in evidence-based decision-making in institutional planning. In addition, the technological framework presented by the biometric platform gives a basis to build the infrastructure of a smart campus, including automated gate control, classroom occupancy analytics, and custom student services. Finally, the effective use of such a system can impacts the policy and policy formulation of an institutional setting by encouraging the utilization of safe, responsible, and domestically advanced digital solutions in institutional administration.

6. CONCLUSION

This paper has revealed that a locally implemented biometric fingerprint attendance and access control system is viable and efficient when the system is designed to meet the actual needs of educational establishments. Solving the old problem of impersonation, manual errors, and inefficiencies in access controls, the system offers an affordable, home-grown alternative to expensive commercial solutions. Designed and built by the Federal Polytechnic Ilaro through interdisciplinary collaboration, it shows a deep awareness of local issues facing it: insufficient infrastructure, large student population, and lack of consistent network access. One of the innovations is seen in the focus on data sovereignty, offline capabilities, and total institutional control of the system. The system does not depend on cloud infrastructure that is managed by the vendor, so the safety of the data is guaranteed, and the system does not contradict internal ICT policies. They have a facility to support five fingerprint captures per user, ensuring the authentication reliability, especially when there is an injury or degradation of a fingerprint. Its dual-mode (online/offline) specification will make it run at all times, even in low connectivity settings.

The pilot deployment performance shows high accuracy (98%+), fast response time, and uptime, promoting over 10,000 students and employees. The integration of attendance monitoring with the ability to access other important services like the examinations, classrooms, and hostel entry directly compelled student compliance and fee regularization. These outcomes point to the system's value not only in technical performance but also in improving institutional governance. Moreover, involving students and staff in development and deployment promoted local capacity building, sustainability, and institutional ownership. This participatory model enhances long-term maintenance and offers a replicable approach for other institutions facing similar challenges. The research validates the potential of indigenous biometric technologies in enhancing accountability, operational efficiency, and digital transformation in education. Future improvements could include integrating facial or iris recognition and AI analytics, as well as scaling the system nationally. This work contributes meaningfully to the growing body of research on context-sensitive educational technology.

ACKNOWLEDGMENTS

This work acknowledges the impact and support of the Management, Engr. Oseni, Abiodun, Adebayo, A.B, Chairmen of ASUP, SANNIP, and NASU of the Institution, Dean, Student Affairs, Members of staff, and students of the Federal Polytechnic during this research.

FUNDING INFORMATION

The research was supported by the Management of the Federal Polytechnic Ilaro, who provided the initial capital to build a prototype and funded the software development and an additional 20 devices. Further funding was accessed from the Tertiary Education Trust Fund [TetFund] through the fabrication funding intervention to build an additional 75 pieces.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Jumoke Soyemi		✓	✓	✓	✓	✓			✓	✓	✓		✓	
Ogunyinka Olawale Ige		✓		✓	✓	✓				✓	✓	✓	✓	
Olugbenga Babajide Soyemi		✓		✓	✓	✓				✓	✓		✓	
Ajibodu Franklin Ademola		✓		✓	✓	✓				✓	✓		✓	
Adaramola Ojo Jayeoba		✓		✓	✓	✓	✓			✓	✓		✓	
Afolayan Andrew Olumide		✓		✓	✓	✓				✓	✓		✓	✓
Habeeb O. Amode		✓	✓	✓	✓	✓				✓	✓		✓	
Mukail Aremu Akinde	✓									✓			✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors declare that there is no conflict of interest.

REFERENCES

[1] O. MuhtahirO., A. Adeyinka O., and A. Kayode S., "Fingerprint biometric authentication for enhancing staff attendance system," *International Journal of Applied Information Systems*, vol. 5, no. 3, pp. 19–24, 2013, doi: 10.5120/ijais12-450867.

[2] M. El Beqqal, M. A. Kasmi, and M. Azizi, "Access control system in campus combining RFID and biometric based smart card technologies," in *Advances in Intelligent Systems and Computing*, 2017, pp. 559–569, doi: 10.1007/978-3-319-46568-5_56.

[3] V. Garg, A. Singhal, and P. Tiwari, "A study on transformation in technology-based biometrics attendance system: human resource management practice," in *Proceedings of the 8th International Conference Confluence 2018 on Cloud Computing, Data*

Science and Engineering, Confluence 2018, 2018, pp. 809–813, doi: 10.1109/CONFLUENCE.2018.8442957.
[4] S. C. Hoo and H. Ibrahim, "Biometric-based attendance tracking system for education sectors: A literature survey on hardware requirements," *Journal of Sensors*, vol. 2019, no. 1, 2019, doi: 10.1155/2019/7410478.
[5] B. A. Abdalkarim, "A mobile application for attendance tracking based on user authentication/Kullanıcı kimlik doğrulamaya dayalı katılım takibi için mobil uygulama," Sakarya Üniversitesi, 2023.
[6] S. Gupta, "QR code based attendance system," *International Journal for Research in Applied Science and Engineering Technology*, vol. 13, no. 4, pp. 2576–2582, 2025, doi: 10.22214/ijraset.2025.68710.
[7] M. Hernandez-de-Menendez, R. Morales-Menendez, C. A. Escobar, and J. Arinez, "Biometric applications in education," *International Journal on Interactive Design and Manufacturing*, vol. 15, pp. 365–380, 2021, doi: 10.1007/s12008-021-00760-6.
[8] M. A. Alsmirat, F. Al-Alem, M. Al-Ayyoub, Y. Jararweh, and B. Gupta, "Impact of digital fingerprint image quality on the fingerprint recognition accuracy," *Multimedia Tools and Applications*, vol. 78, no. 3, pp. 3649–3688, 2019, doi: 10.1007/s11042-017-5537-5.
[9] S. Von Paris and A. R. Jackson, "Bayesian evaluation of forensic fingerprint evidence with automatic biometric systems–implementation and statistical performance analysis." Staffordshire University, 2012.
[10] J. R. Vacca, *Biometric technologies and verification systems*. Elsevier, 2017.
[11] W. Yao, C. H. Chu, and Z. Li, "The adoption and implementation of RFID technologies in healthcare: A literature review," *Journal of Medical Systems*, vol. 36, no. 6, pp. 3507–3525, 2012, doi: 10.1007/s10916-011-9789-8.
[12] L. I. Millett and J. N. Pato, *Biometric recognition: challenges and opportunities*. 2010.
[13] U. Sumalatha, K. K. Prakasha, S. Prabhu, and V. C. Nayak, "A comprehensive review of unimodal and multimodal fingerprint biometric authentication systems: Fusion, attacks, and template protection," *IEEE Access*, vol. 12, pp. 64300–64334, 2024, doi: 10.1109/ACCESS.2024.3395417.
[14] A. N. Uwaechia and D. A. Ramli, "A comprehensive survey on ECG signals as new biometric modality for human authentication: Recent advances and future challenges," *IEEE Access*, vol. 9, pp. 97760–97802, 2021, doi: 10.1109/ACCESS.2021.3095248.
[15] A. J. Mohamed Abdul Cader, J. Banks, and V. Chandran, "Fingerprint systems: sensors, image acquisition, interoperability and challenges," *Sensors*, vol. 23, no. 14, p. 6591, 2023, doi: 10.3390/s23146591.
[16] F. Ghali, N. Ali, and A. Yousif, "Fingerprint recognition," in *IOP Conference Series: Materials Science and Engineering*, vol. 928, no. 3, Springer International Publishing, 2020, pp. 75–117.
[17] A. Mufron and Z. Wei, "Applying biometric technology in school attendance and security management," *Al-Hijr: Journal of Adulearn World*, vol. 3, no. 2, pp. 310–322, 2024, doi: 10.55849/alhijr.v3i2.667.
[18] O. C. Adesoba and I. M. Joseph, "AA fingerprint-based attendance system for improved efficiency," *Journal of Engineering and Technology for Industrial Applications*, vol. 11, no. 51, pp. 9–19, 2025, doi: 10.5935/jetia.v11i51.1305.
[19] L. V Sogoni, "Biometric technology adoption as a technique for tracking employee attendance at government-run schools in the Eastern Cape." 2023.
[20] A. Sunusi, "Developing an access control system for students' identification in higher institutions of learning using biometric technique," Kampala International University, School of Computing and Information Technology, 2019.
[21] S. C. Kim, S. C. Lim, J. Shin, and J. Choi, "Biometrics for electronic eyes: System authentication with embedded CMOS image sensor," *IEEE Transactions on Consumer Electronics*, vol. 62, no. 3, pp. 209–215, 2016, doi: 10.1109/TCE.2016.7613186.
[22] ElectronicsHub, "Biometric attendance system circuit." https://www.electronicshub.org/biometric-attendance-system-circuit (accessed Mar. 09, 2025).
[23] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, Jan. 2004, doi: 10.1109/TCSVT.2003.818349.
[24] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001, doi: 10.1147/sj.403.0614.
[25] A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of multibiometrics*. Springer, 2006.
[26] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of fingerprint recognition (2nd ed.)*. Springer, 2009.
[27] J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, *Biometric systems: technology, design and performance evaluation*. Springer, 2005.

BIOGRAPHIES OF AUTHORS

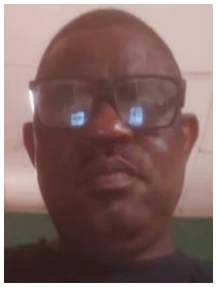
Jumoke Soyemi holds a B.Sc., M.Sc., and Ph.D. in computer science from Obafemi Awolowo University, the University of Ibadan, and Covenant University, respectively. She is the Director of the Centre for Information and Communication Technology and a lecturer in the Department of Computer Science at the Federal Polytechnic, Ilaro. Her research interests include artificial intelligence and bioinformatics. She has received several travel fellowships for international conferences and leads a TETFUND-NRF research project, alongside other grant awards. Dr. Soyemi was an institutional collaborator on a World Bank-funded Centre of Excellence project and is a member of the Covenant Bioinformatics Research Cluster (CuBRe). She is a Fellow of the Nigerian Computer Society and has authored numerous publications and books. She can be contacted at email: jumoke.soyemi@federalpolyilaro.edu.ng.

Ogunyinka Olawale Ige earned his HND, PGD, and M.Sc. in electrical/electronic and computer engineering from Yaba College of Technology, FUTA, and the University of East London in 2001, 2006, and 2012, respectively. He is currently pursuing a Ph.D. in computer science at Babcock University, Ogun State. A lecturer in the Department of Computer Engineering at the Federal Polytechnic, Ilaro since 2006, his research focuses on applying microcontrollers, sensors, and deep learning to automated irrigation and water conservation for food security. He has authored over 40 journal and conference papers and co-edited two textbooks. He can be contacted at email: olawaleige@federalpolyilaro.edu.ng.

Olugbenga Babajide Soyemi holds an HND and PGD in civil engineering from Yaba College of Technology and FUTA, respectively, and earned his MSc and Ph.D. in structural and civil engineering from the University of East London, UK. He has authored or co-authored several conference papers, journal articles, and textbooks. His research focuses on material engineering, steel fiber-reinforced concrete, plastocrete, alternative construction materials, and renewable energy. A COREN-registered engineer, he is a member of the Nigerian Institution of Civil Engineers and the Nigerian Institution of Facility Engineering and Management. He also serves with Rotary International. A former Head of Civil Engineering, he is currently the Director of the Innovation Centre at the Federal Polytechnic, Ilaro. He can be contacted at email: jidesoyemi@federalpolyilaro.edu.ng

Ajibodu Franklin Ademola received his B.Sc. in electrical/electronic engineering and M.Sc. degree in broadband telecommunication and networks at the Olabisi Onabanjo University Ogun State, Nigeria and Hertfordshire University United Kingdom in 2007 and 2015 respectively. He has been a lecturer at The Federal Polytechnic Ilaro, Ogun state Nigeria over 17 years. His research interest includes broadband and telecommunication; last-mile solutions and backhauls, embedded system, renewable energy, next generation PONs, MAC protocols, 5G RANs, optical/wireless convergence, and SDN cellular/satellite IP networks. He can be contacted at email: ajibodu@federalpolyilaro.edu.ng.

Adaramola Ojo Jayeoba earned his National Diploma (ND) in electrical and electronics engineering from The Federal Polytechnic Ilaro (1998) and a Higher National Diploma (HND) from Kwara State Polytechnic, Ilorin (2001). He obtained a Postgraduate Diploma in electronics and computer engineering from Lagos State University (2011) and an MSc in computer systems and network engineering from the University of Greenwich, UK (2016). He later earned an MSc (2018) and B.Eng. (2023) in computer engineering. Currently, he is HOD of Computer Engineering at The Federal Polytechnic Ilaro, specializing in electronics, computer, networking and wireless communication. He can be contacted at email address: ojo.adaramola@federalpolyilaro.edu.ng.



Afolayan Andrew Olumide is a Chief Lecturer in the Department of Science Laboratory Technology at the Federal Polytechnic, Ilaro, where he has served for over 25 years as both a Technologist, Instructor, and Lecturer in the Physics and Laboratory Units. He is a former Head of Department and teaches courses related to laboratory techniques. He holds an ND and HND in Science Laboratory Technology from Federal Polytechnic Ado-Ekiti, a PGD in computer science from FUTA, a B.Sc. in physics with electronics from Southwestern University, and an M.Sc. in physics. He is a member of NISLT, NIP, and a certified CISCO instructor. He also serves as an external examiner and item writer for academic bodies. She can be contacted at email: olumide.afolayan@federalpolyilaro.edu.ng.

Habeeb O. Amode received his National Diploma (ND) and Higher National Diploma (HND) in computer science from The Federal Polytechnic Ilaro, Nigeria. He is currently pursuing a Bachelor of Science (B.Sc.) degree in computer science at Ahmadu Bello University, Nigeria. He is a Software Engineer and specializes in building scalable and efficient software solutions. His research interests focus on software engineering, data engineering, and artificial intelligence. He has experience in developing web and mobile applications, optimizing system performance, and implementing DevOps practices. He can be contacted at email: amodehabeeb@gmail.com.

Mukail Aremu Akinde is a distinguished academic and administrator, currently serving as the Rector of the Federal Polytechnic, Ilaro, Ogun State, Nigeria. He holds an HND in accountancy from the Federal Polytechnic, Ilaro; a B.Sc. in accounting from Bells University; B.Sc. and M.Sc. in economics; and M.Sc. and Ph.D. in finance from Olabisi Onabanjo University, the University of Ibadan, the University of Lagos, and Covenant University, respectively. A Fellow of both the Institute of Chartered Accountants of Nigeria and the Chartered Institute of Taxation of Nigeria, he has authored over 80 journals and conference papers and 16 books. His research focuses on machine learning, accounting, finance, and investment analysis. He played a key role in mobilizing human and material resources for this project. He can be contacted at email: mukail.akinde@federalpolyilaro.edu.ng.