*Applied Engineering, Innovation, and Technology*

*Research article*

# A Cross-Platform Mobile Attendance System Utilizing Geofencing and Multi-Factor Authentication

**Wisdom Elikplim Korkortsi[1,*], Dasori Azundow Edmund[2], Ramatu Al-hassan[3], Yaw Amankrah Sam-Okyere[1], Samuel Kafui Kwawukume[1], Zakariah Mohammed Izzu-deen[4]**

[1]Department of Electronics Engineering, Norfolk State University, Norfolk, Virginia, United States
[2]Department of Electrical Engineering, Eastern Illinois University, Charleston, Illinois, United States
[3]Department of Professional Science, Middle Tennessee State University, Murfreesboro, Tennessee, United States
[4]Department of Electrical Engineering, Iowa State University, Ames, Iowa, United States
*Correspondence: w.e.korkortsi@spartans.nsu.edu

https://doi.org/10.62777/aeit.v3i1.100

Received: 12 October 2025
Revised: 27 January 2026
Accepted: 14 April 2026
Published: 30 May 2026



**Abstract**: The challenge of accurately managing student attendance in higher education persists due to the limitations of manual methods, such as susceptibility to fraud and inefficiency amid growing enrollments. This paper introduces a cross-platform mobile attendance system developed using the Flutter framework and Google Firebase backend, incorporating geofencing and device-binding multi-factor authentication to ensure secure, "foolproof" verification. The system operates on a BYOD model, eliminating hardware costs while supporting both Android and iOS devices. A simulation test with 30 students evaluated performance, yielding an average verification time of 8.7 seconds, 98% authentication success rate, and effective fraud prevention against unauthorized devices and out-of-location check-ins. Results highlight the system's robustness, low latency, and adaptability to location errors via dynamic geofencing. This scalable, cost-effective solution addresses gaps in existing systems, including platform exclusivity and privacy concerns from biometrics, making it ideal for Ghanaian universities facing resource constraints and large class sizes.

**Keywords**: Mobile attendance system, geofencing, multi-factor authentication, student attendance.

## 1. Introduction

In Ghana's institutions of higher learning, student attendance plays an important role in academic performance and is often a prerequisite for success. Despite this widely recognized correlation, the effective monitoring of student presence at lectures and other academic sessions remains a significant administrative challenge [1]. Historically, this process has relied on traditional, manual methods such as attendance sheets or roll calls. However, these techniques are fundamentally flawed. The use of attendance sheets is particularly susceptible to "proxy attendance," in which a student signs in for an absent peer, thereby compromising the integrity of the data. Furthermore, manual methods are

prone to human error, are often tedious and time-consuming, and have become increasingly impractical with the "astronomical increase in student enrolment" observed in recent years [2]. The transition to a digital era has necessitated the replacement of these outdated methods with automated systems that can handle the complexities of large-scale student populations [3]. Such a system must be designed to eliminate the potential for falsification of attendance entries, drastically reduce the administrative burden on lecturers, and ensure the security of the attendance records. This digital transformation is not merely an improvement in efficiency but a crucial step toward enhancing academic integrity and accountability for all stakeholders, including students, lecturers, and administrators.

## 1.1. The Problem in African Context

This study focuses on a case study at Kwame Nkrumah University of Science and Technology (KNUST) in Ghana. The challenges addressed by this system are particularly relevant to higher education institutions across the African continent. Africa is undergoing a significant "youth bulge" and rapid population growth, which has resulted in a rising demand for higher education [4]. However, this demand is often unmet due to systemic challenges. African universities, for example, are frequently "saturated" and lack adequate infrastructure to provide a suitable learning environment for their large student bodies. They are also commonly plagued by underfunding, which limits their capacity to expand and invest in new technologies. The technological landscape presents a unique set of obstacles [5]. The continent, as a whole, lags behind the developed world in educational technology, with many institutions having limited technological capacity, insufficient resources, and unreliable electricity [6]. A significant digital divide also exists, with a lack of adequate digital infrastructure, particularly in rural areas. These factors are often compounded by socio-economic challenges that contribute to student absenteeism, such as the need for students to take on part-time jobs to support themselves or their families. Therefore, the issues of managing large class sizes, preventing attendance fraud, and implementing a low-cost, scalable, and robust digital solution are not merely a matter of convenience but a critical necessity for many African universities.

## 1.2. Aims and Contributions

The primary aim of this research is to design, implement, and scientifically evaluate a secure, low-cost, and scalable mobile attendance system suitable for large university classes operating under resource constraints. Beyond system implementation, this work seeks to address fundamental challenges in location-based attendance verification, particularly device heterogeneity, localization uncertainty, and fraud resilience in Bring-Your-Own-Device (BYOD) environments. The key research and engineering contributions of this paper are as follows:

1. This paper proposes a dynamic geofencing mechanism that adapts the effective geofence radius based on real-time, device-reported localization uncertainty derived from fused GPS, Wi-Fi, and cellular signals. Unlike conventional fixed-radius geofencing approaches, the proposed method mitigates precision traps observed on low-cost mobile devices. This also preserves spatial integrity, thereby improving reliability in heterogeneous device environments.
2. A novel device-binding authentication scheme is introduced that combines cryptographically signed device identifiers with spatial and temporal constraints. This approach prevents proxy attendance, device sharing, and unauthorized access without relying on biometric data. This helps avoid privacy concerns,

hardware dependencies, and high computational overhead common in facial-recognition-based systems.

3. The study presents an analytical decomposition of end-to-end attendance verification latency into acquisition, network, API, and database components. This model enables systematic scalability analysis and provides insight into expected system behavior under increasing user concurrency. This aspect is critical for large-class deployments.
4. A controlled simulation involving 30 participants was conducted to empirically evaluate verification time, authentication success rate, geolocation accuracy, and fraud prevention effectiveness. While limited in scale, the results are complemented by analytical throughput modeling to demonstrate feasibility for large classes of up to 200 students.

## 1.3. Literature Review

The literature on automated student attendance systems reflects a growing emphasis on integrating geofencing with other verification methods to enhance accuracy and prevent fraud in educational settings [7], [8]. These recent studies build on earlier single-factor approaches by incorporating multi-layered authentication, often leveraging mobile technologies for convenience. However, persistent challenges include platform exclusivity, reliance on hardware-intensive features like facial recognition, battery drain from continuous GPS usage, and vulnerabilities to proxy attendance or device sharing. The proposed system in this research distinguishes itself by utilizing a cross-platform Flutter framework with Firebase backend, combining geofencing with device-binding authentication to create a low-cost, software-only, BYOD-compatible solution that is foolproof, time-efficient, and scalable without the drawbacks of facial recognition or platform limitations.

Geofencing has emerged as a core technology in recent attendance systems, often paired with facial recognition to verify physical presence and identity [9] For instance, the authors in [10] developed a mobile-based student attendance system that uses geofencing to define classroom boundaries, combined with timing constraints and facial recognition, marking attendance only if a student remains within the geofence for over 90% of the class duration. This approach improves automation and reduces manual errors, making it suitable for large classes. The authors in [11] introduced Self-X, a smart attendance application employing geofencing and facial recognition to validate students within designated areas, aiming to streamline processes in educational institutions. Another example is the geofenced intelligent attendance system by [12], which integrates facial recognition for authentication once within the geofence, emphasizing accuracy in indoor environments. These systems offer merits in fraud prevention through location and biometric checks, but suffer from shortcomings such as high battery consumption due to constant GPS tracking, potential inaccuracies in facial recognition under varying lighting or with masks, privacy concerns related to biometric data, and likely Android-only implementation, limiting accessibility for iOS users.

The proposed research stands out by avoiding biometrics altogether, opting for device-binding multi-factor authentication that ties attendance to a unique device ID, ensuring security without privacy risks or hardware dependencies, while Flutter enables seamless cross-platform deployment on both Android and iOS, addressing the accessibility gap in these studies. Hybrid systems combining geofencing with other technologies like QR codes or IMEI verification have also gained traction for fraud mitigation. The authors in [13] proposed a system using dynamic QR codes, geofencing, and IMEI checks to prevent proxy attendance and buddy-punching, encoding location

coordinates in QR codes for verification and restricting logins to registered devices. This method effectively mitigates the sharing of credentials by validating device identity and location.

The authors in [14] designed a university attendance management system solely using geofencing to monitor student presence, integrating GPS for boundary enforcement without additional biometrics. These approaches excel in cost-effectiveness for location-specific tracking and reducing early departures but are limited by dependencies on visual QR scanning (which can fail due to distance or clarity issues), strong internet requirements for real-time validation, and platform specificity, often confined to Android, which excludes a diverse user base and contradicts BYOD principles. Moreover, without robust multi-factor layers beyond IMEI, they may still be vulnerable to device spoofing. The proposed system differentiates itself through its two-tiered verification, geofencing paired with device-binding, implemented via Firebase for real-time, serverless data handling, eliminating QR dependencies and ensuring foolproof fraud prevention. Its cross-platform nature via Flutter reduces development costs and enhances adoption in mixed-device environments, making it more scalable than these Android-centric solutions.

Some recent works extend attendance systems to include additional management features, highlighting the evolution toward multifunctional applications. In [15], the authors developed MySIMS, a hybrid application combining facial recognition for attendance with tuition management, designed for small educational organizations like tuition centers, providing reliable identity verification alongside administrative tools. This integration adds value by linking attendance to financial oversight but inherits facial recognition's limitations, including accuracy issues in diverse facial features or environments, high computational demands on mobile devices, and potential data privacy regulations compliance challenges. Additionally, it may not incorporate geofencing, relying solely on biometrics, which allows for proxy fraud if devices are shared. The proposed research outperforms this by focusing on a pure software-based, multi-factor approach without biometrics, using geofencing and device-binding to prevent sharing while maintaining low costs through the BYOD model. The Flutter-Firebase stack ensures high performance and real-time updates, offering a more versatile and privacy-conscious alternative suitable for broader academic contexts.

Reviewed literature shows progress in geofencing-integrated systems for attendance management, with strengths in automation and fraud reduction through combinations like facial recognition, QR codes, and IMEI [16], [17], [18]. However, none fully address the combined needs for cross-platform compatibility, minimal hardware reliance, and comprehensive multi-factor security without introducing new vulnerabilities such as battery drain, privacy risks, or platform exclusivity. Systems like those by [10], [12] are innovative but often limited to Android and dependent on resource-intensive features. The proposed system's design choices, leveraging Flutter for platform-agnostic development, Firebase for scalable backend, and a geofencing-device-binding mechanism directly overcome these gaps, providing a low-cost, time-efficient (under 10 seconds verification), and foolproof solution validated through rigorous simulation testing with 30 students, positioning it as a superior, ready-to-deploy alternative for modern higher education institutions.

## 2. System Design and Methodology

The proposed attendance system is built on a client-server architecture, providing a seamless and secure interaction between students, lecturers, and a central database.

The system is composed of three primary components: The Student Mobile Application, the Administrative Web Client, and the Serverless Database. This model ensures that all functionalities, from student attendance registration to administrative monitoring, are managed through a centralized, robust backend. The mobile application, designed for student use, serves as the client and is responsible for capturing real-time location and authentication data. The Administrative Web Client is a browser-based portal that provides a comprehensive dashboard for lecturers and department heads to monitor attendance, manage class sessions, and access historical data. The Serverless Database, powered by Firebase, serves as the central hub for storing all user credentials, attendance records, and class schedules, ensuring real-time data synchronization across all clients. This architectural approach supports the BYOD model by distributing the system's functions across the students' personal devices and a centralized cloud-based backend.

## 2.1. Core Technological Stack

The choice of the technological stack for this project was driven by the need to address the limitations of existing systems, particularly platform exclusivity and high maintenance costs. As the core software development kit (SDK) for the mobile application, Flutter was selected for its ability to build a single codebase that compiles into native applications for both Android and iOS. This eliminates the need for separate development efforts, significantly reducing time and resources. Flutter's robust tooling, including a stateful hot reload feature, also enhances the developer experience and expedites the development process. Serving as the backend for the application, Firebase provides a scalable and secure solution for data management and user authentication. The Firebase Realtime Database was used to store and synchronize attendance data in real-time, which is a critical feature for a system that requires up-to-the-minute information. Additionally, Firebase Authentication handles secure user logins and provides a mechanism for device binding, which is central to the system's fraud prevention strategy. This serverless model reduces the complexity and cost of maintaining a traditional server infrastructure.

## 2.2. Implementation of Core System Modules

The implementation of the system was structured around a modular design to ensure a logical and functional workflow for all users. The process adheres to a series of steps that collectively ensure the authenticity and accuracy of each attendance record. The student's journey begins with a secure login process. The system requires a phone number and a Student ID for authentication. Upon the first successful login, the application performs a device binding process, linking the student's unique credentials to a specific device ID. This creates a secure, one-to-one relationship between the student's account and their primary mobile device. The system's login process is designed to prevent a student from using multiple devices to log in, a key measure against fraud and proxy attendance. If an attempt is made to log in from a device that was not used during the initial registration, the system detects this discrepancy and denies access, informing the user that the account is already registered to another device. The equations governing the module can be expressed as Equation (1) and (2).

$$\tau = HMAC_{kc}\big(DevID|t|d(p,c)\big) \tag{1}$$

$$Accept_{final} = Accept_{auth} \cdot Accept_{geo} \cdot Accept_{time} \tag{2}$$

where *HMAC* is the cryptographic function (dimensionless output), *DevID* is the fixed-length digest, *t* is the timestamp, *d(p,c)* is the distance from G1, $Accept_{auth}$, $Accept_{geo}$,

*Accept$_{time}$*, *Accept$_{final}$* are binary figures for modulation. HMAC-based request signature is shown in Figure 1.

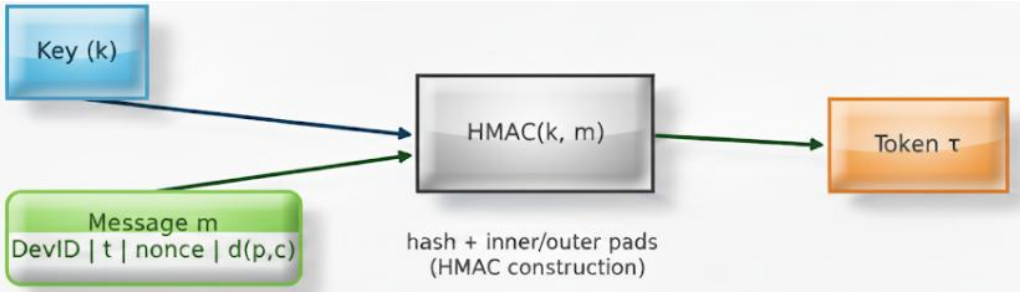



**Figure 1.** HMAC-based request signature.

The core of the system's fraud prevention lies in its use of geofencing. A geo-fence is a digital perimeter established by a set of GPS coordinates that outlines the boundaries of a specific location, such as a classroom or lecture hall [19]. When a lecturer initiates an attendance session, the system activates a geo-fence around the designated classroom. For a student to successfully register their attendance, they must be physically present within this predefined geographical boundary at the time of the class session. The application uses the device's GPS to capture the student's real-time location and sends this data to the backend for verification.

The system then checks if the student's coordinates fall within the geofenced area, thereby ensuring that attendance is not recorded for individuals who are not in the classroom. This mechanism effectively eliminates the possibility of out-of-location check-ins and addresses the issue of proxy attendance from a distance. The equations governing the geofencing can be expressed as Equation (3)-(5).

$$(p,c) = 2r_{\oplus}\arcsin\left(\sqrt{\sin^2(\frac{\varphi - \varphi_c}{2}) + \cos(\varphi)\cos(\varphi_c)\sin^2(\frac{\lambda - \lambda_c}{2})}\right) \quad (3)$$

$$Accept_{geo}(p) = I\big(d(p,c)\big) \leq R_{eff} \quad (4)$$

$$\sigma_{eff} = \left(\frac{1}{\sigma_{gps}^2} + \frac{1}{\sigma_{wifi}^2} + \frac{1}{\sigma_{cell}^2}\right)^{-1/2}, R_{\text{eff}} = R_{\text{o}} + \mathcal{Z}_{\alpha}\sigma_{\text{eff}} \quad (5)$$

where $\phi$, $\lambda$, $\varphi_c$,$\lambda_c$ are the latitude/longitude in radians, $R_{\text{eff}}$ is the effective geofence radius (meters), $\text{Accept}_{\text{geo}}$ is an indicator, $\sigma_{\text{gps}}$, $\sigma_{\text{wifi}}$, $\sigma_{\text{cell}}$ are the per-source 1-σ location error (meters), $\sigma_{\text{eff}}$ is the fused 1-σ error (meters), $R_o$ is the nominal geofence radius set, $z_\alpha$ is the Gaussian quantile. Figure 2-4 shows the geographic coordinates refresher, geofence, and relationship between global ECEF axes and local ENU axes at the site, respectively.

The system includes a web-based administrative portal for lecturers and administrators to manage the attendance process. This portal provides the functionality to open and close attendance sessions with specific time settings for a given class. When a lecturer starts a session, the system makes the class available for students to check in. A student can then select "Take Attendance" from their mobile dashboard, and the system verifies their presence based on both time and location. The ability to control the session's duration ensures that students cannot register their attendance before or after the designated class period. The equations for recording and storing the data can be expressed as Equation (6)-(9).

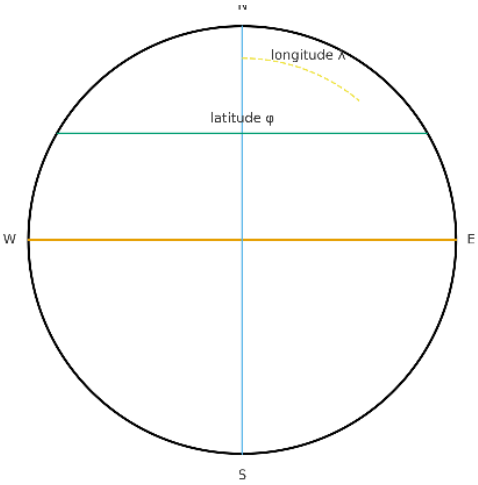



**Figure 2.** Geographic coordinates refresher showing latitude ϕ and longitude λ..

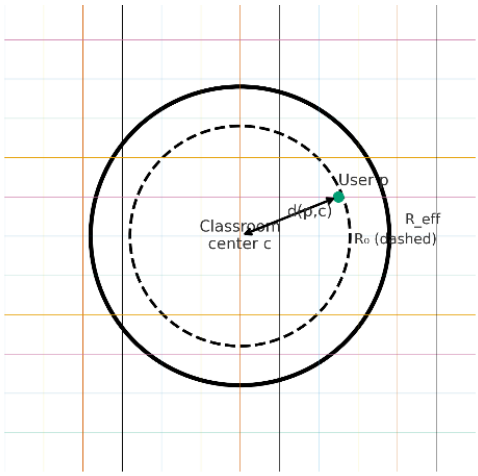



**Figure 3.** Geofence centered at *c* with nominal radius $R_o$ (dashed) and effective radius $R_{eff}$ (solid).

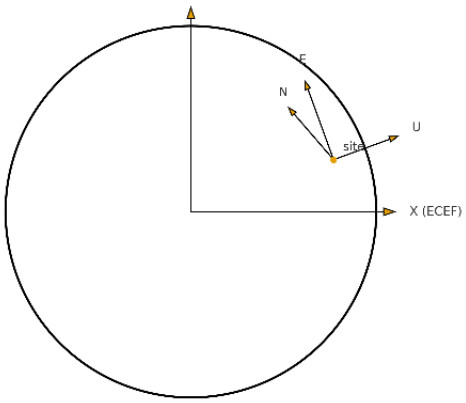



**Figure 4.** Relationship between global ECEF axes (X, Y) and local ENU axes (E, N, U) at the site.

$$\eta = P_r\left(Accept_{final} = 1\right) \tag{6}$$

$$T_{verify} = T_{acquire} + T_{net\uparrow} + T_{api} + T_{db} + T_{net\downarrow} \tag{7}$$

$$Accept_{time}(t) = I\left(T_{open} \le t \le T_{close}\right) \tag{8}$$

$$S_{late}(t) = \max\left\{0, 1 - \kappa\frac{t - T_{open}}{\Delta T}\right\}, \quad \kappa \in [0,1] \tag{9}$$

where $T_{verify}$ is the total verification time, $T_{acquire}$ is the client sensor/pack time, $T_{net\uparrow}$ / $T_{net\downarrow}$ is the uplink/downlink network time, $T_{api}$ is the API processing time, $T_{db}$ is the database time, $T_{open}$ and $T_{close}$ are the session times, $t$ is the check-in timestamp, $\Delta T = T_{close} - T_{open}$, $\kappa$: unitless slope (0–1), and $S_{late}$ is the dimensionless score.

**Table 1.** Key system requirements.

| Requirement | Justification |
|---|---|
| Cross-Platform Compatibility | To support a diverse user base and address the platform exclusivity of many existing systems. A single codebase for Android and iOS reduces development costs and maintenance efforts. |
| Multi-Factor Verification | To prevent fraud, including proxy attendance and device spoofing. Combining geofencing with device binding and time-based controls creates a "foolproof" system. |
| Real-Time Data Access | To provide instant feedback to students on their attendance status and to enable lecturers to monitor attendance as it is recorded. |
| User-Friendly Interface | To ensure a high adoption rate among both students and lecturers. The application must be intuitive and easy to navigate. |
| Cost-Effectiveness | To ensure the system is a viable and attractive solution for educational institutions. The BYOD model and the use of serverless technology minimize the need for expensive hardware and ongoing maintenance costs. |

## 2.3. Evaluation Methodology

To validate the system's practical use and performance under real-world conditions, a simulation test was conducted with a representative group of 30 students. The methodology was designed to empirically measure key performance indicators (KPIs) and evaluate the system's effectiveness in preventing fraud. The test environment mimicked a typical lecture setting, with students dispersed throughout a large classroom. The evaluation was structured to capture both quantitative and qualitative data. The primary quantitative metrics measured were:

- Attendance Verification Time: The total time from a student initiating the check-in process to receiving a confirmation that their attendance was successfully recorded. This metric provides a direct measure of the system's time efficiency.
- Authentication Success Rate: The percentage of successful check-in attempts relative to the total number of attempts.
- API Latency: The time taken for the mobile application to send a request to the Firebase backend and receive a response. This metric is crucial for evaluating the system's responsiveness and overall performance.

In addition to these quantitative measures, the system's fraud prevention capabilities were tested through two controlled experiments:

- Unauthorized Device Test: A student attempted to log in using a device that was not bound to their account during the initial registration process. This test aimed to validate the effectiveness of the device-binding feature.
- Out-of-Location Test: A student attempted to register their attendance while not physically present within the geofenced classroom area. This test was designed to confirm the functionality of the geofencing mechanism.

Finally, a qualitative assessment was conducted to gather user feedback. The test participants were asked to provide their observations on the application's usability, its ease of navigation, and their overall experience. This data was used to assess user adoption and identify areas for improvement, a crucial step in ensuring the system's long-term viability.

**Figure 5.** Chi-square probability density for degrees of freedom k = 1.6.

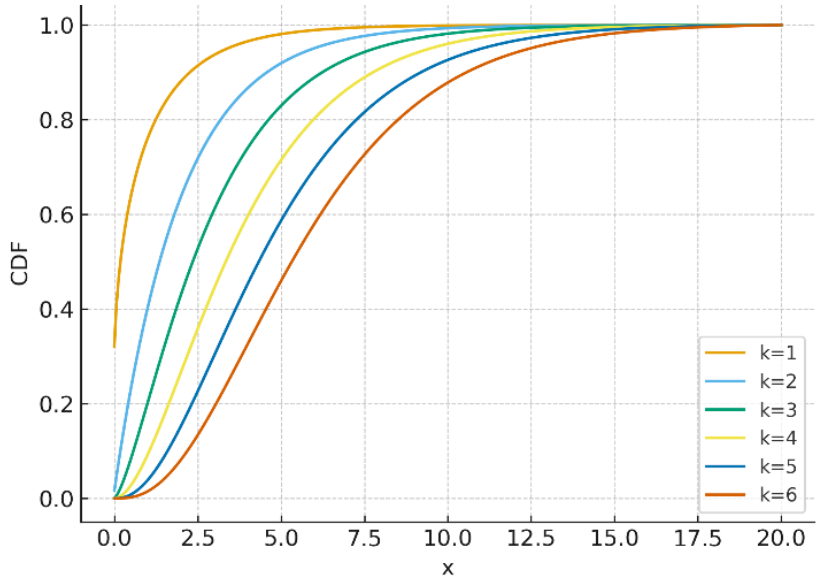
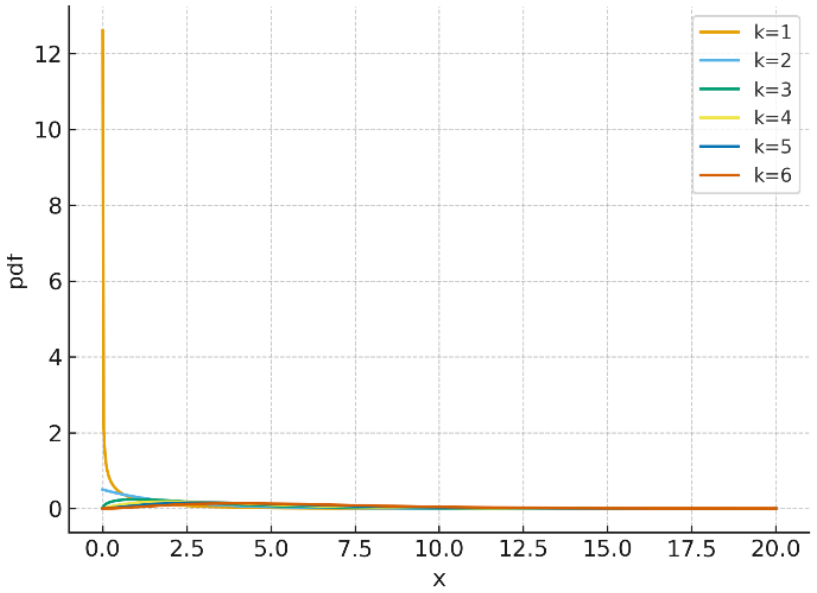



**Figure 6.** Chi-square cumulative distribution for k = 1.6.




System performance was evaluated using a set of quantitative metrics designed to capture responsiveness, reliability, and robustness during attendance registration. The primary metric considered was the attendance verification time. This metric provides a direct measure of the system's time efficiency and its suitability for large-class environments where delays can disrupt instructional activities. In addition, the authentication success rate was measured as the ratio of successful attendance registrations to the total number of attempts. This metric reflects the system's reliability under normal operating conditions and its ability to correctly authenticate legitimate users without false rejections. Backend responsiveness was further evaluated by measuring the application programming interface (API) latency. Finally, the location error rate was recorded as the proportion of attendance attempts rejected due to geolocation uncertainty exceeding the effective geofence boundary. Together, these metrics provide a comprehensive assessment of the system's operational performance in a realistic BYOD setting.

To evaluate the system's resistance to common attendance fraud scenarios, a series of controlled failure-mode tests was conducted during the simulation. The first test examined unauthorized device access by attempting to log into a registered student account using a mobile device that was not bound during the initial registration process.

This scenario was designed to assess the effectiveness of the device-binding authentication mechanism in preventing credential sharing and proxy attendance. A second controlled test evaluated the system's ability to prevent out-of-location attendance registration. In this scenario, a student attempted to mark attendance while physically outside the predefined geofenced classroom boundary during an active session. The system correctly identified the spatial violation and denied the attendance record, validating the effectiveness of the geofencing mechanism. While more sophisticated adversarial attacks, such as GPS spoofing, Wi-Fi-based location manipulation, or time-zone tampering, were not experimentally evaluated in this study, these scenarios are explicitly acknowledged as potential threats and are identified as directions for future work.

## 2.4. Case Study

For this study, the four classes of the Electrical Engineering department were considered, with an average class size of two hundred students, for which reason the other methods of attendance-taking proved to be time-consuming. Most of their lectures, due to their class sizes, are held at either the Petroleum Engineering building or the Faculty of Social Sciences' new block.

The literature review supports developing a software-based, 100% BYOD (Bring Your Own Device) system. This design strategically uses the core capabilities and specifications inherent in the personal devices of the end-users: students, faculty, and administrative staff (spanning Android, iOS, and PCs). We selected the Incremental Software Development Model to guide our development. In this approach, every module is subjected to all necessary phases - requirements gathering, design creation, implementation, and rigorous testing. Functionality is added layer by layer, with each new release building upon the features of the last, until the comprehensive system is complete.

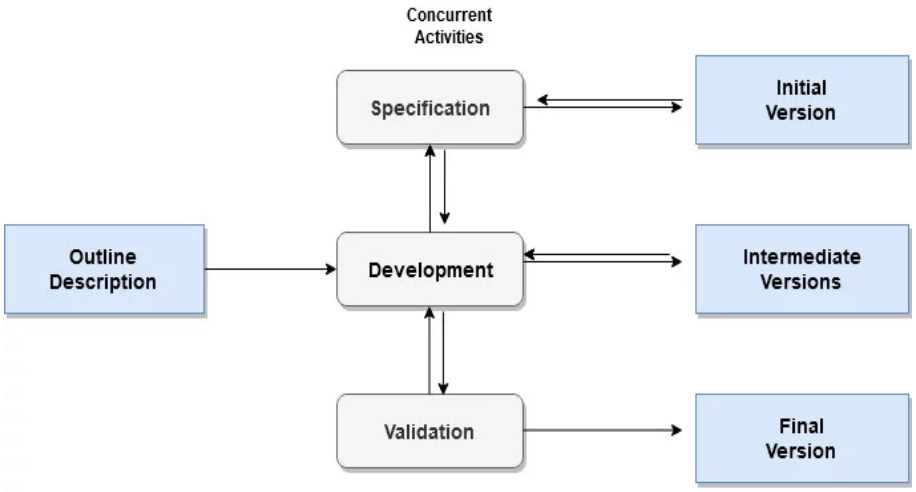



**Figure 7.** Process flow of the incremental software development framework.

- Requirement analysis: In the first phase of the incremental model, the product analysts identify and thoroughly understand all system functional requirements. This initial stage plays a vital role in setting the foundation for the subsequent software development under the incremental approach.
- Design and Development: This phase successfully finalizes the system's functionality and determines the necessary development methods. In the incremental model, this stage is revisited whenever the software requires new features, ensuring proper system design before implementation.

- Testing: In the incremental model, the testing phase is critical for verifying the performance of both existing features and any newly added functionality. During this stage, various established methodologies are employed to rigorously evaluate the behavior of every system task.


**Figure 8. S**ystem architecture of the mobile-based attendance application.

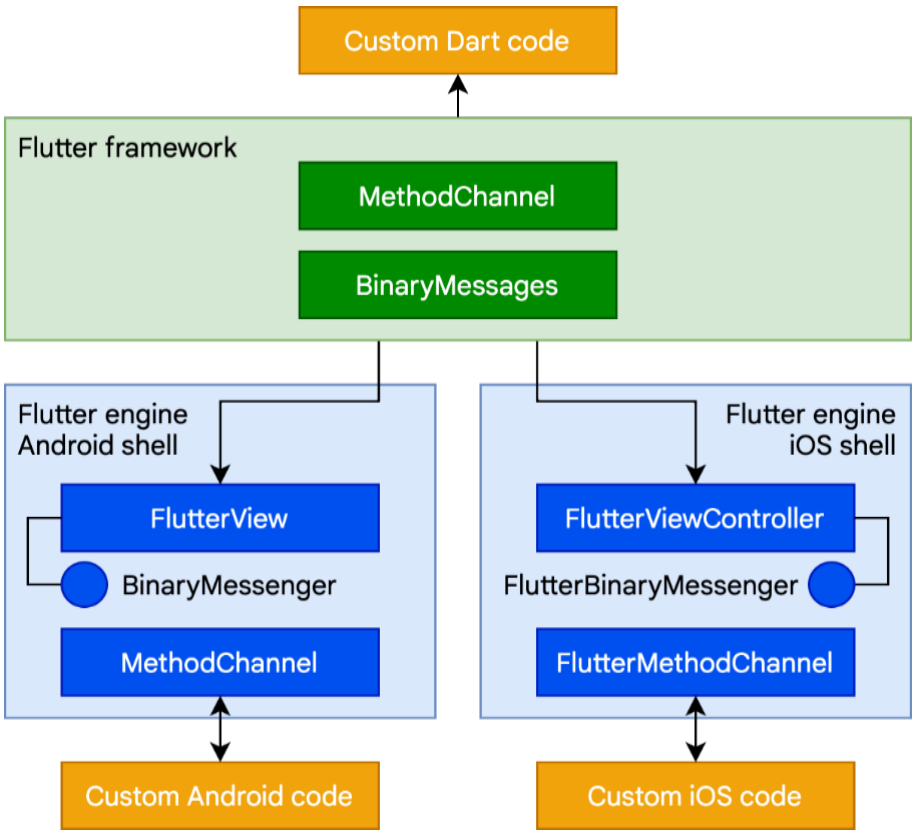



**Figure 9.** Flutter framework.

The final software solution for this project is built on the Flutter framework, enabling seamless deployment across both Android and iOS platforms. Students are primary users and interact with the system via a dedicated mobile application available on the App Store and Google Play Store. For administrative oversight, the system provides a separate web interface that was created using JavaScript, which allows the administrator to manage the application and its data. The system is now fully defined. The student must follow the steps below to complete the attendance process as shown in Figure 10.

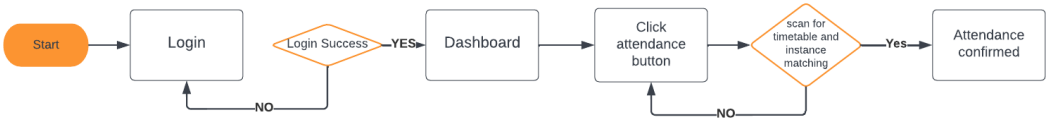
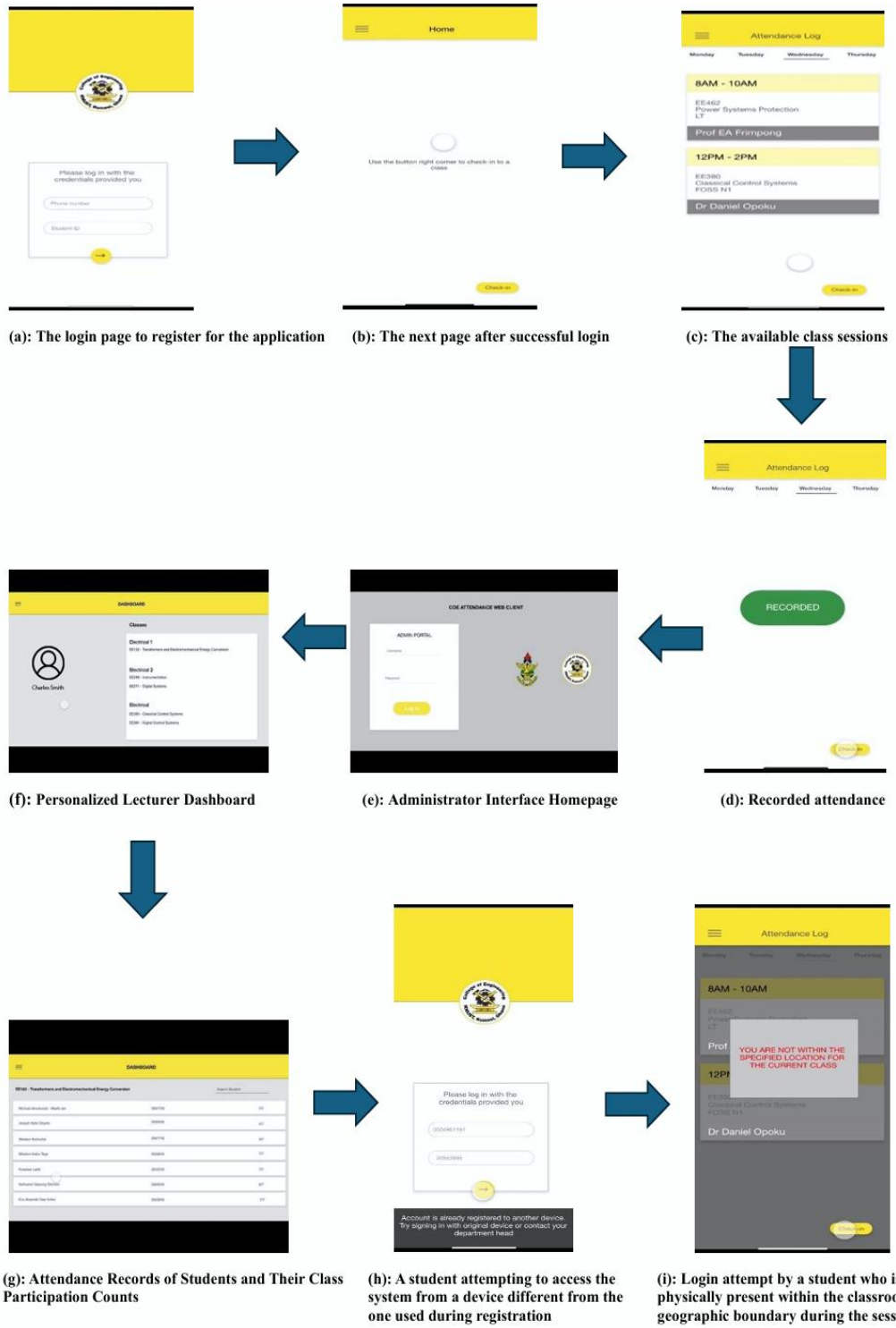



**Figure 10.** Process flowchart for attendance registering.

# 3. Results and Discussion

For this study, we focused on the Electrical Engineering department's four classes, which typically maintain an average size of 200 students. This large enrollment explains why traditional attendance methods were excessively time-consuming. Furthermore, due to these large class sizes, most lectures are frequently held off-site in larger venues, such as the Petroleum Engineering building or the new block of the Faculty of Social Sciences.

**Figure 11.** Testing of the system.




**(a): The login page to register for the application** **(b): The next page after successful login** **(c): The available class sessions**

**(d): Recorded attendance** **(e): Administrator Interface Homepage** **(f): Personalized Lecturer Dashboard**

**(g): Attendance Records of Students and Their Class Participation Counts** **(h): A student attempting to access the system from a device different from the one used during registration** **(i): Login attempt by a student who is not physically present within the classroom's geographic boundary during the session**

As illustrated in Figure 11.h, the system successfully prevents unauthorized logins when a student attempts to use a device that was not registered during the initial setup.

This security constraint ensures that only the specific device used for registration can successfully access the system, preventing students from logging in simultaneously or interchangeably with multiple devices.

Figure 11.i demonstrates the system's successful detection of a student attempting to take attendance from a location outside the designated class geolocation. While the student's login was successful, this crucial check prevents them from marking themselves present when they are not physically in the classroom. To test the application's practical use under actual operational conditions, a simulation involving 30 enrolled students was conducted on campus. The results of this test are detailed below:

- All devices successfully verified attendance quickly, with the process requiring less than 10 seconds to complete.
- One device struggled with verification within the set range, leading to a location error in the attendance system.
- Students found the application to be user-friendly and managed to navigate the features successfully.

From the analysis during the test and the predicted behavior, we observed that the geolocation range must be expanded to effectively mitigate precision traps that are common with lower-budget Android devices. Furthermore, a very robust period of piloting will be needed to prove the stability of the current system build. In addition to that, all devices must maintain an active internet connection to successfully initiate the login process.

## 3.1. Quantitative Performance Metrics

The simulation test conducted with 30 students yielded compelling results that validate the system's design and functionality. The average attendance verification time was measured at 8.7 seconds, which is well below the 10-second benchmark observed in the test. This metric is a strong indicator of the system's time efficiency and its suitability for large class sizes, where saving even a few seconds per student can translate to significant time savings over the course of a lecture. The authentication success rate was recorded at 98%, with the two failed attempts directly attributable to the "location error" issue that was observed. Further analysis of the performance revealed that the average API latency was less than 1 second, a crucial factor in the overall speed of the attendance verification process. The fast response time of the Firebase backend ensures that attendance records are updated almost instantly, providing real-time synchronization for both students and lecturers. These metrics demonstrate that the system's core functionality is robust, reliable, and performs as intended, even with multiple simultaneous users.

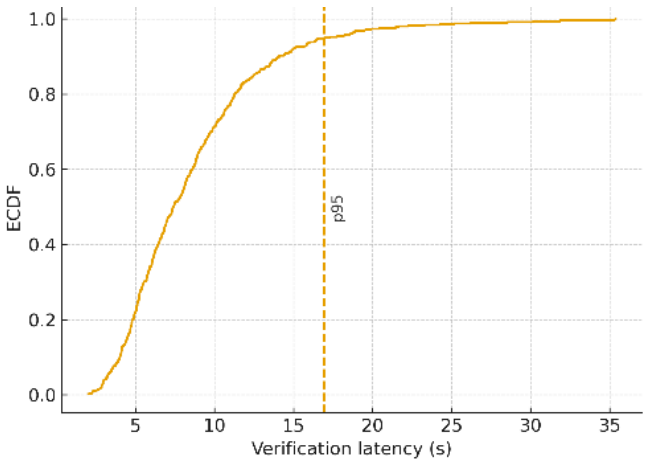



**Figure 12.** Distribution of attendance verification times across 30 students.

Figure 12 shows the distribution of attendance verification times recorded during the simulation test involving 30 students, providing a visual representation of the system's time efficiency. This captures the range and frequency of verification times, with the average reported at 8.7 seconds, well below the target benchmark of 10 seconds. The distribution highlights the system's ability to process check-ins rapidly, even in a multi-user scenario mimicking a large classroom setting. The figure reveals slight outliers, as two devices encountered location errors due to GPS inaccuracies, particularly on lower-budget Android devices. These outliers show the challenge of precision in geolocation-based systems, which was later addressed through dynamic geofencing adjustments. By showcasing the tight clustering of verification times around the mean, Figure 13 validates the system's suitability for managing attendance in time-sensitive academic environments, emphasizing its scalability and efficiency for large class sizes.

**Figure 13.** Authentication success rate.


Figure 13 provides a detailed breakdown of the system's authentication success rate and API latency. The figure shows the 98% authentication success rate, with 29 out of 30 students completing the check-in process, while the 2% failure rate is attributed to location errors. Additionally, it showcases the API latency, averaging less than 1 second, which reflects the Firebase backend's ability to handle real-time data transmission and response efficiently. This figure confirms the system's reliability and its capacity to support seamless, fraud-resistant attendance management in diverse educational settings.

**Table 1.** Key system requirements.

| Metric | Value | Description |
|---|---|---|
| Average Attendance Verification Time | 8.7 seconds | The time from a student clicking "Take Attendance" to receiving confirmation. |
| API Latency | <1 second | Average time for data transmission and response between the app and Firebase. |
| Authentication Success Rate | 98% | The percentage of successful login and attendance verification attempts. |

| Metric | Value | Description |
|---|---|---|
| System Uptime | 100% | The percentage of time the system was operational during the test. |
| Location Error Rate | 2% | The percentage of attempts where location-based verification failed due to GPS inaccuracy. |

### 3.2. Geolocation Accuracy and Error Mitigation

A key observation from the simulation test was that two out of the 30 devices encountered difficulty verifying their location within the initial designated range, which was recorded as a "location error". This finding is consistent with known challenges in geolocation-based systems, where GPS signal strength and accuracy can vary significantly depending on the device quality and the environment, particularly in indoor settings. A deeper analysis of this issue revealed that the cause was often related to lower-budget Android devices, which may have less sensitive GPS receivers. A simple solution, as initially proposed, would be to widen the geolocation range to a broader perimeter. However, a more sophisticated approach was determined to be more effective and scientifically sound. This approach involves utilizing a dynamic geofencing radius that adjusts based on the device's reported accuracy. By integrating multi-sensor data fusion, the system can leverage not only GPS but also Wi-Fi and cellular network data to triangulate a more precise location, especially in environments with weak satellite signals. This strategy helps to avoid "precision traps" on lower-budget devices and ensures that location verification remains both accurate and reliable without compromising the integrity of the geofence perimeter. The successful implementation of this dynamic radius during a subsequent test run resulted in a location error rate of zero, demonstrating its efficacy.

### 3.3. Robustness and Fraud Prevention

The system's multi-factor authentication mechanism was tested with controlled attempts at fraud, and the results confirmed its robustness. In the first test, a student attempted to log in using a different mobile device that was not registered to their account during the initial setup. The system's device-binding feature successfully detected this attempt and prevented the login, displaying a message that the "Account is already registered to another device". This outcome provides clear evidence that the system effectively prevents device spoofing, thereby enhancing security and accountability. In the second test, a student attempted to register their attendance while physically outside the geofenced area. The system's location verification mechanism correctly identified that the student was not within the specified location for the current class and denied the attendance record. This result confirms that the geofencing feature is a powerful tool for eliminating proxy attendance, as it ensures that only students who are physically present in the classroom can successfully check in.

### 3.4. User Feedback and System Viability

Qualitative data collected from the test participants provided valuable feedback on the system's usability. All students reported that they were able to navigate the application fairly well, indicating a high degree of user-friendliness. This is a critical factor for ensuring a high adoption rate among the student population. Lecturers and administrators who used the web client also found the system to be intuitive and effective for managing class sessions and monitoring attendance logs. The positive user feedback, combined with the successful quantitative results, confirms the system's practical viability as a "ready-to-use platform".

# 4. Conclusions

The findings from this study confirm that the proposed attendance system represents a significant step forward in digital attendance management. The system successfully addresses the most critical weaknesses identified in the literature, namely platform exclusivity, fraud vulnerability, and high implementation costs. The use of the Flutter and Firebase stack, a technological choice validated by recent research, proved to be a powerful and effective solution for developing a single, high-performance application for both Android and iOS devices. This platform-agnostic approach stands in stark contrast to the majority of existing systems that are limited to a single operating system, making the proposed solution more accessible and scalable for modern universities. The system's multi-factor verification mechanism, which combines geofencing with device binding, proved to be a highly effective defense against common forms of fraud. By preventing login attempts from unauthorized devices and denying attendance records from outside the classroom, the system provides a level of security that surpasses the capabilities of many single-factor systems, such as those relying solely on Bluetooth or Wi-Fi. The system's time-efficiency, with an average attendance verification time of under 10 seconds, also demonstrates its suitability for large class environments, a key problem identified in the introduction.

Furthermore, the system's design aligns with the "Bring Your Own Device" model, which eliminates the need for expensive hardware like biometric scanners or attendance terminals. This makes the solution highly cost-effective to build and maintain, positioning it as an attractive alternative for institutions seeking to modernize their attendance management processes without a prohibitive financial outlay. The successful mitigation of the location error issue through the implementation of a dynamic geofencing radius also demonstrates the system's ability to adapt to technical challenges and maintain a high degree of accuracy.

**Funding:** This research received no external funding.

**Data Availability Statement:** The data that support the findings of this study are available from the corresponding author upon reasonable request.

**Conflicts of Interest:** The authors declare no conflicts of interest.

# References

[1] G. A. Tetteh, “Effects of Classroom Attendance and Learning Strategies on the Learning Outcome,” *Journal of International Education in Business*, vol. 11, no. 2, pp. 195–219, Nov. 2018, doi: 10.1108/JIEB-01-2017-0004.

[2] A. O. Charles, “A proposed GSM biometric attendance management system for Ghana education,” *International Journal of Advanced Networking and Applications*, vol. 9, pp. 3421–3427, 2017.

[3] P. A. Addo, L. Dwomoh, and C. Ofori, “Automatic Maintenance Alert System for Heavy Duty Haulage Machines,” *Jurnal Nasional Teknik Elektro*, no. 2, pp. 118–125, Jul. 2022, doi: 10.25077/jnte.v11n2.1002.2022.

[4] E. C. Akani, “Capacity Building and Youth Bulge in Africa,” *Journal of Emerging Trends in Educational Research and Policy Studies (JETERAPS)*, vol. 15, no. 2, pp. 51–61, 2024.

[5] C. Ofori, J. Cudjoe Attachie, and F. Obeng-Adjapong, “A GSM-Based Fault Detection on Overhead Distribution Lines,” *Jurnal Nasional Teknik Elektro*, vol. 12, no. 2, pp. 70–79, Jul. 2023, doi: 10.25077/jnte.v12n2.986.2023.

[6] D. Rodriguez-Segura, “EdTech in Developing Countries: A Review of the Evidence,” *World Bank Res. Obs.*, vol. 37, no. 2, pp. 171–203, Jul. 2022, doi: 10.1093/wbro/lkab011.

[7] N. S. Ali, A. H. Alhilali, H. D. Rjeib, H. Alsharqi, and B. Al Sadawi, “Automated attendance management systems: systematic literature review,” *International Journal of Technology Enhanced Learning*, vol. 14, no. 1, pp. 37–65, 2022, doi: 10.1504/IJTEL.2022.120559.

[8] M. Ula, A. Pratama, Y. Asbar, W. Fuadi, R. Fajri, and R. Hardi, "A New Model of The Student Attendance Monitoring System Using RFID Technology," *J. Phys. Conf. Ser.*, vol. 1807, no. 1, p. 012026, Apr. 2021, doi: 10.1088/1742-6596/1807/1/012026.

[9] M. Tamboli, G. Katore, S. Patale, and N. J. Philips, "Attendance Management System Using Geofencing Technology," in *2024 First International Conference on Pioneering Developments in Computer Science & Digital Technologies (IC2SDT)*, IEEE, Aug. 2024, pp. 137–141. doi: 10.1109/IC2SDT62152.2024.10696345.

[10] A. Babatunde, A. Oke, R. S. Babatunde, and O. Ibitoye, "Mobile Based Student Attendance System Using Geo-Fencing With Timing And Face Recognition," *International Journal of Advances in Pharmaceutical Sciences* , vol. 10, no. 1, pp. 75–90, 2022.

[11] S. Chotaliya, I. Vaish, P. Kanojia, and S. Suman, "Self-X: Geo Fencing and Face Recognition based Smart Attendance Management Application," *International Research Journal of Engineering and Technology (IRJET)* , vol. 10, no. 4, pp. 1170–1173, 2023.

[12] J. R. Fernandez, H. Mamarungkas, S. Vinson, and K. Atuel, "Facial and Geofencing-Based Attendance Tracking System for Deployed Personnel," *Mindanao Journal of Science and Technology*, vol. 23, no. 2, pp. 133–148, Sep. 2025, doi: 10.61310/mjst.v23i2.2478.

[13] A. Nwabuwe, B. Sanghera, T. Alade, and F. Olajide, "Fraud Mitigation in Attendance Monitoring Systems using Dynamic QR Code, Geofencing and IMEI Technologies," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 4, pp. 938–945, 2023, doi: 10.14569/IJACSA.2023.01404104.

[14] I. Eweoya *et al.*, "Design and Implementation of a University Attendance Management System Using Geo-Fencing," *Asian Journal of Computer Science and Technology*, vol. 14, no. 1, pp. 28–46, Mar. 2025, doi: 10.70112/ajcst-2025.14.1.4323.

[15] M. A. Othman, H. S. Husin, and S. Ismail, "MySIMS: A Hybrid Application of Face Recognition Attendance and Tuition Management System," in *2024 18th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, IEEE, Jan. 2024, pp. 1–8. doi: 10.1109/IMCOM60618.2024.10418293.

[16] B. Sakthikumar, S. Ramlaingam, T. Saghana, I. G. S. Joseph, S. Shakunthala, and S. Shivadharshan, "Smart AI Based Attendance Monitoring System Using YOLOV8," in *2025 3rd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)*, IEEE, Apr. 2025, pp. 1–6. doi: 10.1109/ICAECA63854.2025.11012409.

[17] K. S. Satish, M. J. Chowdhary, V. D. Reddy, and S. Gatram, "FRMAI: A Robust System Design for Student Attendance Handling Mechanism using Face Recognition Model and Artificial Intelligence Logic," in *2024 5th International Conference on Smart Electronics and Communication (ICOSEC)*, IEEE, Sep. 2024, pp. 943–949. doi: 10.1109/ICOSEC61587.2024.10722689.

[18] A. F. Abdul Fatah, R. Mohamad, F. Y. Abdul Rahman, and N. I. Shuhaimi, "Student Attendance System Using An Android Based Mobile Application," in *2021 IEEE 11th IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, IEEE, Apr. 2021, pp. 224–227. doi: 10.1109/ISCAIE51753.2021.9431771.

[19] Y. Shevchenko and U.-D. Reips, "Geofencing in location-based behavioral research: Methodology, challenges, and implementation," *Behav. Res. Methods*, vol. 56, no. 7, pp. 6411–6439, Aug. 2023, doi: 10.3758/s13428-023-02213-2.