

Research Article

Privacy-preserving proximity-based attendance verification using passive mobile device signals

B. E. Otaru^{a,b}, M. B. Abdullahi^a & A. Saleh^b

^aDepartment of Computer Science, School of Information and Communication Technology, Federal University of Technology, Minna, Nigeria.

^bDepartment of Computer Science, Faculty of Science, Federal University of Education, Kontagora, Nigeria..

Abstract

The increasing adoption of smart technologies in educational institutions has accelerated the transition from manual attendance recording to automated attendance management systems. However, existing approaches such as biometric authentication, Radio Frequency Identification (RFID) cards, and mobile-based check-ins often present significant challenges related to privacy, infrastructure costs, and vulnerability to proxy attendance. This study proposes a privacy-preserving proximity-based attendance verification system that utilizes passive wireless signals emitted by mobile devices, specifically, Bluetooth Low Energy (BLE) advertisements and Wi-Fi probe requests, to infer physical presence without collecting personally identifiable information. The proposed framework integrates Received Signal Strength Indicator (RSSI)-based proximity estimation, temporal aggregation and signal filtering techniques filtering techniques to support reliable attendance verification in classroom environments. To address privacy concerns, the framework adopts privacy-by-design principles, including real-time processing, avoidance of persistent device identifiers, anonymised signal handling, and minimal data retention. The proposed architecture consists of signal acquisition, processing and inference, and attendance decision layers that collectively enable passive and non-intrusive attendance monitoring. A comparative analysis with existing attendance systems highlights the potential advantages of the frameworks in terms of privacy preservation, scalability, cost-effectiveness, and resistance to attendance fraud. Although the framework has not yet undergone full-scale experimental validation, it provides a foundation for future prototype development and empirical evaluation. The study contributes to ongoing research in privacy-aware Internet of Things (IoT) systems and smart educational technologies by presenting a design-oriented approach to attendance verification that balances operational efficiency with user privacy.

Keywords: Privacy-preserving systems, smart attendance, Bluetooth Low Energy (BLE), Wi-Fi probe requests, proximity detection.

1. Introduction

Attendance monitoring remains a critical administrative function in educational institutions, forming the basis for academic assessment, institutional accountability, and student participation tracking. Accurate attendance records are essential for evaluating student engagement, enforcing academic policies, and ensuring compliance with institutional standards. Traditionally, attendance has been recorded using manual methods such as roll calls and paper-based registers. Although simple and inexpensive, these approaches are inefficient, time-consuming, and highly prone to human error and deliberate manipulation, including impersonation and proxy attendance.

As class sizes increase and educational systems become more digitized, traditional attendance recording methods

have become increasingly inadequate. This challenge has stimulated the development of various automated attendance systems aimed at improving efficiency, accuracy, and record management. Early solutions relied on technologies such as Radio Frequency Identification (RFID) and Quick Response (QR) codes. RFID-based systems automate attendance capture through tag detection, while QR-code systems allow students to register attendance using mobile devices. Although these approaches reduce administrative workload, several studies have reported significant limitations. RFID systems are vulnerable to proxy attendance because RFID cards can easily be exchanged among students, allowing absent students to be falsely marked as present. Similarly, QR-code systems depend heavily on active user participation and remain susceptible to code sharing, screenshot

*Corresponding authors: B. E. Otaru

Email address: oe.blessing@fuek.edu.ng (B. E. Otaru)

ORCID: <https://orcid.org/0009-0001-6288-0520>

Received: 20/05/2026; Accepted: 28/06/2026; Published: 31/07/2026



forwarding, and unauthorized attendance registration. Furthermore, both approaches require additional infrastructure, periodic maintenance, and effective monitoring to ensure reliability (Farag & Abouelela, 2022; Miao *et al.*, 2020).

To overcome these weaknesses, researchers have explored biometric-based attendance systems that utilize fingerprints, facial recognition, and iris patterns to establish user identity. While biometric systems generally provide stronger resistance to impersonation and attendance fraud, they introduce substantial privacy, ethical, and legal concerns. The collection, storage, and processing of sensitive biometric data expose institutions to risks associated with data breaches, unauthorized access, and misuse of personal information. In addition, biometric systems often require specialized hardware, regular calibration, and significant financial investment, making large-scale deployment difficult in resource-constrained educational environments. Environmental conditions such as poor lighting, camera positioning, fingerprint quality, and network connectivity may also reduce recognition accuracy and affect system performance (Badmus *et al.*, 2021; Oshin *et al.*, 2025; Musa *et al.*, 2023).

More recently, Internet of Things (IoT)-based attendance systems have emerged to support real-time monitoring and centralized management of attendance records. Although IoT solutions improve scalability and automation, many implementations depend on persistent identifiers such as MAC addresses, device IDs, or user accounts for attendance verification. Such dependence raises concerns regarding user tracking, behavioural profiling, and long-term privacy violations. Similarly, wireless sensing approaches based on Bluetooth Low Energy (BLE) and Wi-Fi technologies have demonstrated potential for passive attendance monitoring; however, many existing implementations still rely on identifiable device information, thereby creating opportunities for re-identification and surveillance. Furthermore, wireless signal fluctuations caused by environmental interference, device heterogeneity, and mobility can negatively affect detection reliability. These limitations highlight the need for attendance systems that can provide accurate presence verification while preserving user privacy and minimizing dependence on persistent identity information.

To address these limitations, biometric-based attendance systems were introduced. These systems utilize unique physiological characteristics such as fingerprints, facial features, or iris patterns to verify identity. In Nigerian educational contexts, biometric systems have been widely studied and implemented. For example, fingerprint-based attendance systems have been shown to improve accuracy and reduce impersonation in university environments (Badmus *et al.*, 2021). Similarly, facial recognition systems have been explored in Nigerian tertiary institutions to automate attendance processes and improve administrative

efficiency (Oshin *et al.*, 2025; Musa *et al.*, 2023). Despite their effectiveness, biometric systems introduce significant privacy concerns due to the collection and storage of sensitive personal data. Additionally, they require expensive hardware and maintenance, making them less suitable for resource-constrained institutions.

The emergence of the Internet of Things (IoT) has further transformed attendance systems by enabling interconnected sensing, communication, and data processing capabilities. IoT-based systems integrate sensors, wireless communication technologies, and cloud platforms to support real-time attendance tracking and centralized monitoring (Nguyen *et al.*, 2022). In Nigeria, IoT-enabled attendance systems have been proposed to improve scalability and monitoring efficiency in academic institutions (Olasupo, A.O., *et al.*, 2022). However, many IoT-based systems rely on persistent identifiers such as MAC addresses or user accounts, which can expose individuals to tracking and profiling. This contradicts modern data protection principles that emphasize data minimization and user anonymity.

More recently, wireless communication technologies such as Bluetooth Low Energy (BLE) and Wi-Fi have been explored for attendance detection. These technologies leverage signals emitted by mobile devices to enable passive and non-intrusive monitoring. BLE-based systems, in particular, offer low power consumption and support proximity detection, making them suitable for smart attendance applications (Vishwakarma *et al.*, 2025; Hayat *et al.*, 2025). Wi-Fi-based systems utilize probe requests emitted by smartphones to infer user presence, enabling implicit authentication without direct interaction (Panca *et al.*, 2020). Despite their advantages, many of these systems still rely on device identifiers, which introduces privacy risks.

Privacy concerns have become increasingly important in modern digital systems. Recent research has explored privacy-preserving approaches to reduce the risks associated with user identification and long-term tracking. For example, Wi-Fi probe request-based investigation as a means of detecting user presence without directly associating wireless signals with individual identities (Simončič *et al.*, 2023). While these approaches represent important progress toward privacy-aware sensing, several challenges remain. Many existing solutions still rely on device-level identifiers that may permit re-identification under certain conditions, while others provide limited mechanisms for preventing long-term tracking and behavioural profiling. In addition, environmental factors such as signal interference, device heterogeneity, and mobility can affect the reliability of wireless sensing systems. Consequently, there remains a need for attendance verification frameworks that simultaneously prioritize privacy preservation, passive operation, scalability, and reliable presence inference in dynamic education environments.

To address the identified limitations of existing

attendance systems, this study proposes a privacy-preserving attendance verification framework based on passive BLE and Wifi sensing. Unlike conventional systems that depend on identity verification, biometric templates, or persistent device identifiers, the proposed framework focuses on presence inference through proximity estimation. The framework is designed to support attendance verification while minimising privacy risks and deployment costs. This paper presents the architecture, design principles, signal processing mechanisms, and expected operational benefits of the proposed framework.

2. Review of related works

The evolution of automated attendance systems has been extensively explored in the literature, with research focusing on improving efficiency, accuracy, security, and usability. Existing systems can be broadly classified into biometric systems, RFID-based systems, IoT-based frameworks, wireless signal-based systems, and privacy-preserving approaches.

2.1. Classification of attendance systems

2.1.1. Biometric-based Attendance Systems

Biometric authentication systems are widely used due to their ability to uniquely identify individuals based on physiological traits such as fingerprints, facial features, or iris patterns. These systems offer high accuracy and significantly reduce impersonation risks. In Nigeria, several studies have demonstrated the effectiveness of biometric systems in academic environments. For example, fingerprint-based attendance systems have been successfully implemented to improve attendance accuracy and reduce manual errors in universities (Badmus *et al.*, 2021). Similarly, facial recognition-based attendance systems have been deployed in Nigerian tertiary institutions to automate attendance tracking and improve administrative efficiency (Oshin *et al.*, 2025; Musa *et al.*, 2023).

Despite their advantages, biometric systems present serious limitations. They require the collection and storage of sensitive personal data, raising privacy, ethical, and legal concerns. Furthermore, biometric systems are often expensive to deploy and maintain, requiring specialized hardware and consistent calibration, which limits their scalability in resource-constrained environments.

2.1.2. RFID-Based Attendance Systems

RFID technology has been widely used in automated attendance systems due to its simplicity and reliability. RFID-based systems typically involve tags assigned to students and readers installed at entry points. Research has demonstrated the effectiveness of RFID in improving attendance recording accuracy (Miao *et al.*, 2020). In addition, low-cost RFID monitoring systems have been developed to enhance accessibility and reduce operational

costs (Farag & Abouelela, 2022).

In Nigeria, IoT-enabled RFID systems have been proposed to improve attendance monitoring in academic institutions (Oyediji *et al.*, 2025). However, RFID systems remain vulnerable to proxy attendance, as tags can be shared among users. They also require dedicated infrastructure, which increases deployment complexity and cost.

2.1.3. IoT-Based Attendance Systems

IoT technologies have enabled the development of intelligent attendance systems that integrate sensors, communication networks, and cloud computing platforms. These systems support real-time monitoring and centralized data processing, making them suitable for large-scale deployments. Nguyen *et al.* (2022) proposed a comprehensive IoT-based attendance framework that improves automation and scalability.

In Nigeria, IoT-based biometric attendance systems have been developed to enhance monitoring efficiency in universities (Olasupo, *et al.*, 2022). However, many IoT systems rely on persistent identifiers or biometric templates, which introduce privacy risks and potential misuse of personal data.

2.1.4. Wireless Signal-Based Attendance Systems

Wireless communication technologies, particularly Bluetooth Low Energy (BLE) and Wi-Fi, have emerged as promising alternatives for automated attendance detection in educational environments. BLE-based systems offer low power consumption and support proximity detection through signal strength analysis, making them suitable for passive attendance monitoring (Vishwakarma *et al.*, 2025). Frictionless attendance systems based on BLE have been proposed to reduce manual intervention and improve user convenience (Hayat *et al.*, 2025). Similarly, Wi-Fi-based attendance solutions have demonstrated the feasibility of leveraging probe requests and wireless sensing for presence detection and classroom monitoring (Panca *et al.*, 2020; Simončič *et al.*, 2023). Recent studies further indicate that wireless sensing approaches can provide scalable and cost-effective alternatives to conventional attendance systems while reducing operational overhead (Nguyen *et al.*, 2022).

Wi-Fi-based systems utilize probe requests emitted by mobile devices to infer user presence within a monitored area. Such systems enable implicit authentication and attendance verification without requiring active student participation (Panca *et al.*, 2020; Simončič *et al.*, 2023). However, many implementations rely on persistent device identifiers or MAC address tracking, which may introduce privacy concerns and increase the risk of user re-identification (European Parliament and Council of the European Union, 2016; ENISA, 2022).

2.1.5. Proximity-Based IoT Systems

However, many proximity-based attendance systems continue to depend on persistent device identifiers or centralized user profiling mechanisms, raising concerns regarding privacy, data minimization, and long-term user tracking (Cavoukian, 2011; European Parliament & Council of the European Union, 2016; ENISA, 2022).

2.1.6. Privacy-Preserving Attendance Systems

Privacy-preserving approaches aim to minimize or eliminate the exposure of sensitive user data. Simončič et al. (2023) proposed a non-intrusive presence monitoring system using Wi-Fi probe requests while reducing direct identification. These systems represent an important step toward privacy-aware sensing but still face challenges in ensuring complete anonymity and maintaining robustness in dynamic environments.

Table 1: Comparative Analysis Table

Feature	RFID	Biometrics	QR Code	Conventional BLE	Proposed Framework
Privacy Protection	Low	Very Low	Medium	Medium	High
User Interaction	Required	Required	Required	Minimal	None
Proxy Resistance	Low	High	Low	Medium	High
Cost	Medium	High	Low	Low	Low
Scalability	Medium	Medium	High	High	High

This layered design is consistent with IoT-based attendance frameworks proposed in prior studies, which emphasize modularity and scalability for real-time monitoring (Nguyen *et al.*, 2022). In contrast to conventional IoT systems that rely on identity mapping, the proposed architecture eliminates persistent user identification to ensure privacy preservation.

2.2. Signal Acquisition Model

The Signal Acquisition Layer is responsible for collecting wireless signals transmitted by nearby mobile devices. In the proposed framework, Bluetooth Low Energy (BLE) advertising packets and Wi-Fi probe requests are captured using passive packet-sniffing mechanisms deployed on low-cost sensing nodes. Each sensing node continuously scans the surrounding environment and records detected signal events within a predefined sampling interval of two seconds. Captured information includes signals timestamps, signal type (BLE or Wi-Fi), and Received Signal Strength Indicator (RSSI) values. To preserve user privacy, device identifiers such as MAC addresses are neither stored nor linked to user identities.

The framework considers two primary wireless signals sources:

- BLE advertising packets
- Wi-Fi probe requests

These signals are periodically broadcast by modern smartphones during normal device operation and therefore do not require active user participation. The captured signals are forwarded to the Processing and Inference Layer for filtering, temporal aggregation, and proximity estimation (Vishwakarma *et al.*, 2025).

2.2.1. Pre-processing and Noise Filtering

Raw wireless signals are inherently noisy due to environmental interference, multipath propagation, and device heterogeneity. To address this, the system applies:

- Signal filtering to remove weak or spurious signals
- Deduplication of repeated probe requests
- Temporal smoothing using sliding time windows

These pre-processing steps are intended to improve signal reliability and by reducing noise and duplicate observations before proximity estimation. Similar signal refinement techniques have been used in BLE-based attendance systems to enhance accuracy in real-world environments (Hayat *et al.*, 2025).

2.3. Proximity Inference Using RSSI

The system estimates physical proximity using the Received Signal Strength Indicator (RSSI). RSSI values provide an indirect measure of distance between the device and sensor node. The relationship between signal strength and distance is modelled as:

2.3.1. RSSI-Based Distance Estimation

The relationship between RSSI and distance is approximated using the log-distance path loss model in Eq.1

$$RSSI = RSSI_0 - 10_n \log_n(d) \quad (1)$$

Where:

$RSSI$ = received signal strength (dBm)

$RSSI_0$ = reference RSSI at 1meter

n = path loss exponent

d = distance (meters)

For attendance inference, devices with RSSI values greater than or equal to -75dBm are considered to be within classroom proximity.

To improve robustness, the system aggregates multiple RSSI readings over a defined time window rather than relying on instantaneous values. This approach reduces fluctuations caused by environmental noise and device

variability.

Proximity-based inference models have been widely adopted in IoT attendance systems due to their simplicity and effectiveness (Hayati & Nugraha, 2023). However, the proposed system extends this approach by integrating privacy-preserving constraints.

2.4. RSSI-Based Distance Estimation

The relationship between signal strength and estimated distance is represented by the logarithmic path-loss model in Eq. 2.

$$RSSI(d) = RSSI_0 - 10n \log_{10}(d) \quad (2)$$

Where:

$RSSI(d)$ = Received Signal Strength Indicator at distance d

$RSSI_0$ = Signal strength measured at a reference distance of one meter

n = Environmental path-loss exponent

d = Estimated distance between the transmitting device and sensor node.

The framework utilizes RSSI measurements as indicators of relative proximity rather than precise distance estimation. Multiple RSSI measurements are aggregated over time to reduce fluctuations caused by environmental interference.

2.5. Temporal Aggregation Mechanism

To avoid incorrect attendance decisions caused by transient signals, the system applies temporal aggregation. A device is considered “present” only if:

- (i) It is consistently detected across multiple scans
- (ii) RSSI values must remain greater than or equal to -75dBm throughout the observation period.
- (iii) Detection must persist for at least 60 seconds within the observation window

This approach is inspired by frictionless BLE attendance systems, which emphasize continuous detection for reliability (Vishwakarma et al., 2025).

2.6. Privacy-Preserving Design Framework

A key innovation of this framework is its adherence to privacy-by-design principles. Unlike traditional IoT attendance systems that rely on MAC addresses or device identifiers, the proposed framework minimises the collection and retention of personally identifiable information. Device identifiers are discarded immediately after signal processing, and attendance decisions are based on aggregated proximity observations rather than individual identities. This approach aligns with the principles of data minimizations, purpose limitation, and privacy design advocated by the General Data Protection Regulations (GDPR) (European Parliament & Council of the European Union, 2016). This proposed system will ensure that:

- (i) No persistent identifiers are stored
- (ii) Device data is processed in real time
- (iii) Only aggregated attendance results are retained
- (iv) Identity linkage is completely removed

This design aligns with privacy-preserving sensing approaches such as Wi-Fi probe-based monitoring systems that aim to minimize user identification risks (Simončič et

al., 2023).

Additionally, the system avoids long-term data retention, thereby preventing re-identification or tracking across sessions. This is particularly important in educational environments where student privacy must be protected.

The proposed framework is therefore designed to support privacy-preserving attendance verification while remaining consistent with GDPR principles of privacy by design and data minimisation (European Parliament & Council of the European Union, 2016).

The final attendance decision is made based on a rule-based inference model:

A student device is marked as present:

IF $RSSI \geq -75\text{dBm}$

AND Detection count ≥ 5 scans

AND Observation Duration ≥ 60 seconds

THEN Present

ELSE Absent

This rule-based approach ensures transparency and interpretability, which is important in educational systems where auditability is required.

2.7. Attendance Decision Criteria

To reduce transient detections and improve reliability, attendance verification is based on three conditions:

- (i) RSSI value must be greater than or equal to the predefined threshold (-75 dBm).
- (ii) The device must be detected at least five times within the observation period.
- (iii) Detection must persist continuously within a 60-second observation window.

These parameters may be adjusted during future prototype implementation and calibration activities.

2.8. Privacy Threat Model

The framework considers the following privacy threats:

- (i) Device Tracking Attackers may attempt to monitor user movements through persistent device identifiers.
- (ii) User Profiling Attendance records may be linked to individual behavioural patterns.
- (iii) Unauthorized Data Retention Long-term storage of wireless identifiers may enable future re-identification.
- (iv) Attendance Manipulation Individuals may attempt to falsely register attendance without physical presence.

To mitigate these threats, the framework incorporates privacy-by-design principles including:

- No storage of MAC addresses.
- No persistent device identifier retention.
- Real-time signal processing.
- Storage of only aggregated attendance outcomes.
- Elimination of identity linkage mechanisms.

2.9. System Deployment Model

The system is designed for deployment using low-cost hardware such as:

- (i) Raspberry Pi sensor nodes

- (ii) Wi-Fi sniffing modules
- (iii) Central processing server

This makes the system suitable for resource-constrained environments, particularly in developing countries where cost-effective solutions are essential (Nguyen *et al.*, 2022). The modular architecture may facilitate future deployment across multiple classrooms. However, scalability evaluation is outside the scope of the present study and remains an area for future work

3. Summary of Methodology Contribution

The proposed framework integrates passive wireless sensing, RSSI-based proximity estimation, temporal aggregation, and privacy-preserving processing into a unified attendance verification architecture.

Unlike existing systems that rely on identity tracking or active user participation, this approach will ensure frictionless, anonymous, and scalable attendance verification.

4. Expected Performance and Discussion

This study presents a proposed framework and system architecture rather than a fully implemented attendance system. Consequently, quantitative performance metrics such as detection accuracy, precision, recall, false positive rates, and false negative rates are not reported. The discussion presented in this section focuses on the expected operational characteristics of the framework based on established principles from BLE-based, Wi-Fi-based, and IoT attendance systems reported in the literature.

4.1. Attendance Verification Reliability

The proposed framework is designed to support reliable attendance verification through the integration of RSSI-based proximity estimation and temporal aggregation mechanisms. Rather than relying on a single wireless signal observation, the framework evaluates multiple signal detections over a predefined observation period. This approach is intended to reduce the impact of transient wireless signals, environmental interference, and temporary device movement that may otherwise lead to inaccurate attendance decisions.

The use of a minimum detection count threshold and an RSSI threshold of -75 dBm provides an additional layer of validation by ensuring that attendance decisions are based on sustained proximity evidence. Similar approaches have been employed in BLE- and Wi-Fi-based presence detection systems to improve the reliability of proximity inference (Brena *et al.*, 2017; Simončič *et al.*, 2023). Although the framework has not yet undergone empirical testing, the combined use of proximity estimation and temporal filtering is expected to provide a more robust basis for attendance inference than single-event detection methods (Nguyen *et al.*, 2022).

4.2. Privacy Preservation Analysis

Privacy preservation represents a central design objective of the proposed framework. Unlike conventional attendance systems that depend on biometric identifiers, RFID tags, or persistent device identifiers, the framework minimizes the collection and storage of personally identifiable information. Device identifiers are discarded

immediately after signal processing, and attendance decisions are generated from aggregated proximity observations rather than individual identities. This approach aligns with the principles of data minimization, purpose limitation, and privacy by design advocated by the General Data Protection Regulation (GDPR) (European Parliament & Council of the European Union, 2016). Similar privacy-preserving principles have been recommended for IoT and wireless sensing systems to mitigate risks associated with tracking, profiling, and unauthorized disclosure of personal information (Cavoukian, 2011; ENISA, 2022). By eliminating identity linkage mechanisms and restricting data retention to attendance outcomes, the framework is expected to reduce privacy risks commonly associated with conventional attendance monitoring systems.

4.3. Resistance to Attendance Fraud

Attendance fraud remains a significant challenge in educational institutions, particularly in systems that rely on manual registration, RFID cards, or QR-code scanning. Such systems may be vulnerable to proxy attendance through card sharing, credential sharing, or code forwarding (Farag & Aboulela, 2022; Miao *et al.*, 2020). The proposed framework addresses this challenge by inferring attendance from sustained physical proximity rather than explicit user actions. Attendance decisions are based on repeated signal detections within a predefined observation period, making it more difficult for absent individuals to be falsely registered as present. Furthermore, the requirement for continuous proximity within the classroom environment is intended to reduce opportunities for attendance manipulation. While the effectiveness of these mechanisms requires future empirical validation, the framework provides a conceptual basis for mitigating common forms of attendance fraud.

4.3. Deployment Feasibility and Cost Implications

The proposed framework is designed with practical deployment considerations in mind. The architecture relies on low-cost sensing nodes capable of capturing BLE advertisements and Wi-Fi probe requests, thereby reducing infrastructure costs compared with many biometric attendance systems. Because the framework utilizes wireless signals that are already transmitted by modern smartphones during normal operation, no specialized user equipment is required. Similar low-cost IoT architectures have been reported as feasible solutions for educational environments seeking to automate attendance management while minimizing deployment expenses (Nguyen *et al.*, 2022; Badmus & Adeyemi, 2021). The modular architecture also supports incremental deployment, allowing institutions to implement the framework in selected classrooms before expanding to larger environments. These characteristics suggest that the framework may be particularly suitable for educational institutions operating under resource constraints.

4.4. Comparative Analysis with Existing Systems

A comparison of the proposed framework with existing attendance monitoring approaches reveals several potential advantages. RFID systems provide automated attendance recording but remain susceptible to proxy attendance through

tag sharing (Farag & Abouelela, 2022). Biometric systems offer stronger identity verification but introduce concerns related to privacy, data protection, and deployment costs (Musa *et al.*, 2023; Oshin *et al.*, 2025). QR-code systems are inexpensive and easy to implement but require active user participation and may be vulnerable to code sharing. Conventional BLE-based attendance systems improve automation but often depend on persistent device identifiers that may expose users to tracking risks (Simončič *et al.*, 2023). In contrast, the proposed framework emphasizes privacy preservation through the elimination of persistent identifiers while maintaining passive attendance verification capabilities.

4.5. Limitations of the Proposed Framework

Despite its potential benefits, the proposed framework has several limitations. Wireless signal measurements are inherently susceptible to environmental interference, physical obstructions, and variations in device hardware characteristics (Brena *et al.*, 2017). Signal fluctuations may affect the consistency of RSSI measurements and influence proximity estimation reliability. In addition, some mobile devices employ MAC address randomization and other privacy-enhancing mechanisms that may affect signal observation patterns (Simončič *et al.*, 2023). The framework also assumes that students carry BLE- or Wi-Fi-enabled devices and keep the relevant wireless interfaces active during attendance periods. Most importantly, the study focuses on framework design and has not yet undergone full-scale implementation or experimental validation. Consequently, performance characteristics such as detection accuracy, precision, recall, scalability, and privacy effectiveness remain subjects for future investigation.

5. Conclusion

This study presented a privacy-preserving proximity-based attendance verification framework that leverages passive BLE advertisements and Wi-Fi probe requests to infer physical presence in educational environments. Unlike traditional attendance systems that rely on biometric data, RFID tags, or persistent identifiers, the proposed framework adopts a privacy-by-design approach that eliminates identity-based tracking while supporting attendance verification through proximity estimation. The framework integrates RSSI-based inference, temporal aggregation, and anonymized signal processing to provide a foundation for non-intrusive attendance monitoring.

Although the framework has not yet undergone full-scale experimental validation, it establishes a conceptual and architectural basis for future implementation. Future work will involve prototype development, field deployment, performance evaluation, and optimization under real classroom conditions.

Abbreviations

RFID	Radio Frequency Identification
BLE	Bluetooth Low Energy
RSSI	Received Signal Strength Indicator
QR Code	Quick Response code

IoT	Internet of Things
MAC	Media Access Control

Author Contributions

Blessing Egbekhangbo Otaru: Conceptualization, Methodology, Investigation, Data Curation, Writing – original draft, Visualization, Funding Acquisition, Project Administration.

Muhammad Bashir Abdullahi: Validation, formal Analysis, Writing – Review & Editing, Supervision.

Abdulkareem Saleh: Resources, Writing – Review & Editing, Funding Acquisition.

Conflicts of Interest

The author(s) declare that they have no known competing financial interests, professional affiliations or personal relationships that could have appeared to influence the work reported in this paper.

Funding

None

References

- Badmus, E. O., & Odekunle, O. P., & Oyewobi, D. O. (2021). Smart fingerprint biometric and RFID time-based attendance management system. *European Journal of Electrical Engineering and Computer Science*, 5(4), 34–39. <https://doi.org/10.24018/ejeece.2021.5.4.339>.
- Brena, R. F., García-Vázquez, J. P., Galván-Tejada, C. E., Muñoz-Rodríguez, D., Vargas-Rosales, C., & Fangmeyer, J. (2017). Evolution of indoor positioning technologies: A survey. *Journal of Sensors*, 2017, 1–21.
- Cavoukian, A. (2011). Privacy by design: *The 7 foundational principles*. Information and Privacy Commissioner of Ontario.
- European Union Agency for Cybersecurity. (2023). *Engineering personal data sharing: Data protection and privacy considerations*. ENISA.
- European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*, 59(L119), 1–88.
- Farag, W. A., & Abouelela, M. E. (2022). Low-cost active monitoring of attendance using passive RFID technology. *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika*, 8(4), 552–564. <https://doi.org/10.26555/jiteki.v8i4.25168>
- Hayat, M. A. M., Rasyidi, M. F., Faisal, M., & Bakti, R. Y. (2025). A Bluetooth-based attendance system for educational administration at SMA Muhammadiyah:

- Cross-platform development and usability validation. *Jurnal Teknik Informatika (JUTIF)*, 6(5), 3602–3618. <https://doi.org/10.52436/1.jutif.2025.6.5.4873>
- Hayati, N., & Nugraha, A. E. (2023). Design and implementation proximity-based IoT for smart attendance system. *Buletin Pos dan Telekomunikasi*, 21(2), 16–31. <https://doi.org/10.17933/bpostel.v21i2.380>
- Imam, R. T., Ajayi, A. S., Ikuenayo, V. B., Adeleke, O. J., Ibe, B.O., Obeten, O. M., Afolabi, O. S., Ojajuni, B. A., Iyere, E. E. & Ogungbade, A. D. (2025). Design and implementation of a biometric and RFID-based attendance system using Arduino: A tapestry of automation and security. *World Academics Journal of Engineering Sciences*, 12(3), 98–109. <https://doi.org/10.26438/wajes/v12i3.98109>
- Kitchenham, B., Charters, S., & Budgen, D. (2020). Guidelines for empirical software engineering studies and evaluation metrics. *Empirical Software Engineering*, 25(4), 2853–2875.
- Miao, Q., Xiao, F., Huang, H., Sun, L. & Wang, R. (2020). Smart attendance system based on frequency distribution algorithm with passive RFID tags. *Tsinghua Science and Technology*, 25(2), 217–226. <https://doi.org/10.26599/TST.2018.9010141>
- Musa, Z. A., Yakubu, I. Z., Abubakar, F. A., Matinja, Z. I., Jibrin, A. A., & Muhamma, M. M., (2023). Smart attendance system using face recognition for tertiary institutions in Nigeria. *International Journal of Engineering Research & Technology (IJERT)*, 12(5), 224–229.
- Nguyen, V. D., Khoa, H. V., Kieu, T. N., & Huh, E.-N. (2022). Internet of Things-based intelligent attendance system: Framework, practice implementation, and application. *Electronics*, 11(19), 3151. <https://doi.org/10.3390/electronics11193151>
- Olasupo, A. O., Ademiluyi, O. S., Usman, M. A., Abdullahi, K. A., Olubanwo, O. O., Ayo, F. E., Ojumadu, U. H., Salami, E. O., & Ibiro, T.E. (2022). A fingerprint based students attendance management system, for Olabisi Onabanjo University. *FUDMA Journal of Sciences*, 6(1), 254–265.
- Onyishi, D. U., & Igbino, C. K., (2021). Design and implementation of a biometric students' time and attendance logging system. *Nigerian Journal of Technology*, 40(3), 484–490.
- Oshin, O., Amenaghawon, J., Moninuola, F., & Idowu-Bismark, O. (2025). Class attendance system using facial recognition. *Information Sciences Letters*, 30(2), 1589–1595. <https://doi.org/10.18280/isi.300617>.
- Oyediji, F. T., Adegbite, E. A., & Ayomikun, E. A., (2025). Development on an IoT-based automated attendance system using smart card technology. *Engineering and Technology Journal*, 10(11), 7891–7904. <https://doi.org/10.47191/etj/v10i11.20>.
- Panca, A., Rahardja, U., Aini, Q., & Santoso N.P.L. (2020). Utilising Wi-Fi probe requests for smart attendance monitoring in educational environments. *Journal of Physics: Conference Series*, 1477(5), 052040. <https://doi.org/10.1088/1742-6596/1477/5/052040>.
- Panca, B. S., Paulus, Y., & Karnalim, O. (2020). An automated attendance system in academia with implicit authentication via mobile devices and Wi-Fi connection. *International Journal of Online and Biomedical Engineering*, 16(7), 86–94. <https://doi.org/10.3991/ijoe.v16i07.13869>
- Simončič, A., Mohorčič, M., Michael, M., & Hrovat, A. (2023). Non-intrusive privacy-preserving approach for presence monitoring based on Wi-Fi probe requests. *Sensors*, 23(5), 2588. <https://doi.org/10.3390/s23052588>
- Vishwakarma, H. K., Jane, K., Shaikh, A., Bawanthare, P. D., Moon, A., & Gudadhe, M. M. (2025). Frictionless attendance system using BLE. *International Journal of Recent Advances in Engineering & Technology*, 14(3s), 166–170. <https://doi.org/10.65521/intjournalrecadvengtech.v14i3s.1687>