

NextGen GeoSecure: Intelligent Attendance Management with Multi-Level Authentication

Dr. Pallavi Chaudhari¹, Rhythm Dabur², Ananya Bhujade³, Abhishek Yadav⁴, Yasir Bhat⁵, Tanu Saini⁶

¹*Professor, Dept of CSE, Priyadarshini College of Engineering*

^{2,3,4,5,6}*U.G. Students, Dept of CSE Priyadarshini College of Engineering*

Abstract—Attendance management remains one of the most time-consuming and error-prone administrative tasks faced by educational institutions. Manual roll-call is slow and easily manipulated, while first-generation digital solutions such as static QR codes, RFID cards and single-factor GPS checks remain vulnerable to proxy attendance through screenshot sharing, code forwarding and location spoofing. This paper presents NextGen GeoSecure, an intelligent attendance management system that layers four independent verification checks — a dynamic, session-bound QR code, GPS-based geofencing that restricts check-ins to a 10-metre radius of the classroom, device-identity verification through App Set ID/Firebase Installation ID binding, and JSON Web Token (JWT) based authentication of every client-server exchange — so that a proxy attempt must defeat all four checks at once rather than just one. The system exposes two interfaces: an Android client that students use to scan the live QR code and submit their location, and a Spring Boot-backed faculty dashboard that instructors use to start or stop a session, monitor live check-ins, flag suspicious attempts and export attendance records. By combining lightweight, smartphone-native verification with per-session QR rotation and device binding, NextGen GeoSecure targets the device-versus-identity gap that persists across the existing QR-and-GPS literature while remaining deployable on ordinary smartphones without additional classroom hardware.

Index Terms—Attendance Management System, Dynamic QR Code, GPS Geofencing, Device Verification, JSON Web Token, Multi-Factor Authentication, Proxy Attendance Prevention.

I. INTRODUCTION

Attendance recording is a compulsory and recurring task in every academic institution, used to evaluate student participation and to maintain official records. Traditional paper-based roll-call is time-consuming,

prone to human error and, because attendance is often marked by a proxy on a classmate's behalf, unreliable as a measure of physical presence. Early automated alternatives such as RFID cards, fingerprint scanners and barcode readers reduced some of this manual burden but introduced their own constraints: dedicated hardware at every entry point, hygiene concerns around shared biometric sensors, and continued exposure to card or ID sharing.

The widespread availability of smartphones has since pushed attendance systems toward QR-code and GPS-based verification, since both capabilities already exist on a student's own device and require no additional institutional hardware. However, a QR code that stays valid for an entire session, or a location check used in isolation, can still be defeated: a code can be screenshotted and forwarded to an absent classmate, and a spoofed or borrowed device can be made to appear inside the permitted radius. A system that relies on a single verification factor therefore has a single point of failure.

NextGen GeoSecure addresses this by combining four independent checks in one workflow: a dynamic QR code that is regenerated and invalidated on a per-session basis, GPS-based geofencing that confirms the scanning device is within a 10-metre radius of the classroom, device-identity verification that ties attendance to a single pre-registered device per student, and JSON Web Token (JWT) authentication that secures every request between the client and the backend. A proxy attempt must now defeat all four checks simultaneously rather than exploiting whichever single factor a prior system relied on. Beyond proxy prevention, the system aims to reduce paperwork, cut faculty workload through automation, and give instructors a live, exportable record of attendance.

The remainder of this paper is organized as follows. Section II reviews related attendance systems from recent literature and the research gaps they leave open. Section III describes the proposed system's requirements, workflow and architecture. Section IV covers the implementation and technology stack. Section V presents a comparative analysis against existing approaches. Section VI discusses the expected behaviour and evaluation plan of the system, Section VII concludes the paper, and Section VIII outlines directions for future work.

II. RELATED WORK

Attendance automation research follows several different tracks depending on the technology a given group favours: biometric and computer-vision groups trust cameras and liveness checks, networking and embedded-systems groups favour short-range radio such as Bluetooth Low Energy (BLE), and application developers tend to pair GPS with a QR code because both are already present on a student's phone. Nine representative systems, spanning pure proposals to systems tested at institutional scale, were reviewed to motivate the design of NextGen GeoSecure.

Gupta et al. [1] surveyed more than fifteen geolocation-based attendance designs and proposed an architecture combining GPS geofencing, JWT authentication and blockchain-secured logs, but the design was never implemented or measured. Kumar et al. [2] added a liveness-detection layer on top of face recognition to defeat photo and screen-replay spoofing, reporting 97.4% accuracy on a six-person test group, though camera placement itself was never verified. Vu-Quoc et al. [3] combined continuous facial recognition with BLE presence signals to confirm that a student remained in the room for an entire session, but accuracy fell sharply beyond three to four metres from the camera.

Pathan et al. [4] proposed a two-portal QR-and-GPS system closest in spirit to the present work, in which a session-bound QR code is cross-checked against the scanning device's live GPS coordinates; however, the system confirms only where a device is, not who is holding it, since an unlocked phone can be handed to a classmate inside the same geofence. Fitriyani et al. [5] and Taju et al. [6] each deployed GPS-only or QR-

plus-GPS systems with real pilots, but neither layered a device-identity or biometric factor on top, leaving the same code-and-device-sharing loophole open. Patil et al. [7] combined OTP, fingerprint and GPS geofencing in one design and a separate CCTV-based face-recognition pipeline in another, without evaluating either. Kumari and Kumar [8] and Tejas et al. [9] both reported high claimed accuracy (99.2% and 99.9% respectively) for QR-plus-Haversine-distance systems at a larger scale, but neither paper describes its measurement methodology, and neither test against GPS spoofing.

Across all nine systems, three gaps recur. First, most systems rely on only one or two verification factors, creating a single point of failure if that factor is bypassed. Second, GPS spoofing is almost never tested even though every GPS-dependent paper in this set is, in principle, vulnerable to a fake-location application. Third, and most consistently, a QR-plus-GPS check confirms that a device was in the right place at the right time, not that the enrolled student was the one holding it — none of the reviewed systems combine QR validity, location and device identity in a single mandatory pipeline. NextGen GeoSecure is designed specifically to close this device-versus-identity gap by adding device-identity binding and token-based authentication on top of the QR-and-geofencing pattern already shown to be lightweight and hardware-free.

III. PROPOSED SYSTEM

A. Problem Statement

Existing QR-based attendance systems remain prone to proxy attendance because they lack geofencing and proper device-level authentication: a student can share a QR code, a screenshot, or an attendance link with a classmate who is not physically present in the classroom. Traditional manual marking is, independently, time-consuming, difficult to audit and error-prone. A secure and automated system is therefore needed that checks the actual location of the student, the identity of the device being used, and the validity of the current attendance session before an attendance record is accepted.

B. Objectives

- Provide proxy-proof attendance marking through layered verification.

- Reduce manual paperwork and faculty administrative workload.
- Automate attendance recording and reporting end to end.
- Save classroom time compared with manual roll-call.
- Keep attendance data secure through authenticated, encrypted communication.
- Provide instructors with real-time dashboards and exportable attendance reports.

C. Requirements Analysis

The functional requirements of NextGen GeoSecure are summarised in Table I. The system operates through a dual view: an Android application for students and a web-based faculty dashboard for instructors.

TABLE I. FUNCTIONAL REQUIREMENTS

Category	Details
Platform	Android app + web faculty dashboard
Student data	Name, roll no., device ID
Session data	Course, location, date, start/end time
Verification factors	QR, GPS, device ID, JWT

D. Multi-Level Verification Workflow

Attendance is accepted only after the scanned request passes every stage of a sequential verification pipeline. The logic below summarises the check performed at each stage.

```
IF Validate_QR(Scanned_QR) == FALSE THEN
  Display ("Invalid QR Code. Attendance Denied.");
  EXIT
```

```
IF Validate_Location(Student_GPS,
  Classroom_GPS) > 10m THEN Display("Outside
  Geofence. Attendance Denied."); EXIT
```

```
IF Validate_Device(App_Set_ID) !=
  Registered_Device THEN Display("Unrecognized
  Device. Attendance Denied."); EXIT
```

```
IF Validate_JWT(Token) == FALSE THEN Display
  ("Session Expired. Attendance Denied."); EXIT
```

```
Record_Attendance(Student_ID, Session_ID)
Display ("Attendance Successfully Recorded.")
```

Each stage is independently sufficient to block a specific attack: QR validation rejects an expired or

replayed code, geofencing rejects a device outside the classroom, device-identity verification rejects a shared or unregistered handset even inside the geofence, and JWT validation rejects a tampered or replayed network request.

E. System Architecture

The instructor's device generates a session-bound dynamic QR code, which is displayed to the class. Each student scans the code from the Android application, which silently reads the device's App Set ID/Firebase Installation ID, requests the device's current GPS coordinates through the Fused Location Provider, and packages all three (QR payload, coordinates, device ID) into a JWT-authenticated request to the Spring Boot backend. The backend runs the four-stage verification pipeline described above; on success the attendance record is written to the MySQL database and the faculty dashboard updates in real time, while on failure the attempt is logged as a rejected or suspicious entry without being counted as attendance.

IV. IMPLEMENTATION

A. Technology Stack

The Android client is built with Java and the Android SDK with an XML-based UI. The backend is implemented in Spring Boot, secured with Spring Security and JWT, and persists data to MySQL through Hibernate/JPA. Table II lists each component and its role.

TABLE II. TECHNOLOGY STACK

Component	Technology
Android app	Java + Android SDK
UI design	XML
Backend	Spring Boot (Java)
Security	Spring Security + JWT
Database	MySQL
ORM	Hibernate (JPA)
QR generation	ZXing
QR scanning	ML Kit / ZXing
Location	Fused Location Provider + Geofencing API
Device check	App Set ID / Firebase Installation ID

B. Working Flow

The end-to-end sequence is: Teacher Login → Generate QR → Student Scan → GPS Verification → Device Verification → JWT Validation → Attendance Stored → Dashboard Updated. Once the instructor logs in and starts a session, a fresh QR code is generated and displayed; every subsequent scan is checked in sequence against location, device identity and token validity before the faculty dashboard is refreshed with the new entry.

C. Faculty Dashboard

The faculty dashboard gives instructors direct control over each session and visibility into its results.

Core functions include:

- Start Attendance / Stop Attendance controls to open and close a session's QR code.
- A live count of students who have successfully checked in.
- Attendance reports per session, per course and per date range.
- Flagging of suspicious attempts (failed geofence, device mismatch or expired token).
- Export of attendance records to Excel or PDF for institutional records.

D. Security Considerations

Per-session QR invalidation prevents a screenshot from being reused in a later class. A fixed 10-metre geofence radius restricts valid check-ins to the physical classroom. Device-identity binding ties each student's attendance to one pre-registered device, so a code or an unlocked phone handed to a classmate inside the geofence is still rejected at the device-verification stage. All client-server communication is authenticated with short-lived JWTs, reducing exposure to token replay and request tampering.

V. COMPARATIVE ANALYSIS

Table III positions NextGen GeoSecure against manual attendance and the QR/GPS-based systems reviewed in Section II. Where those systems verify at most two independent factors — typically QR validity and GPS location — NextGen GeoSecure adds device-identity binding and JWT-based request authentication, directly targeting the device-versus-identity gap identified across the literature.

TABLE III. FEATURE COMPARISON

Feature	Manual	QR+GPS [4],[6],[8],[9]	GeoSecure
Manual entry needed	Yes	No	No
Session-bound QR	—	Partial	Yes
GPS geofencing	No	Yes	Yes (10m)
Device-ID check	No	No	Yes
Token-based security	No	Rarely	Yes (JWT)
Security level	Low	Medium	High

VI. RESULTS AND DISCUSSION

As a four-layer pipeline, NextGen GeoSecure is designed so that each verification stage independently neutralises a distinct spoofing vector observed in the reviewed literature: session-bound QR rotation defeats screenshot and link sharing across classes, the 10-metre geofence defeats remote or off-campus marking, device-identity binding defeats a borrowed or shared phone being used inside the geofence, and JWT validation defeats replayed or tampered network requests. Because a proxy attempt must simultaneously satisfy all four checks, the design narrows the single point of failure that recurs across the QR-only and QR-plus-GPS systems discussed in Section II.

Several of the systems reviewed in Section II report high headline accuracy figures without describing their measurement protocol or sample size [8], [9], while others report no quantitative evaluation at all [1], [6], [7]. To avoid repeating that gap, formal institutional-scale evaluation of NextGen GeoSecure — including scan accuracy, false-acceptance rate, verification latency under concurrent classroom load, and structured student and faculty usability feedback — is treated as a distinct, ongoing activity rather than an assumed outcome of the architecture, and is carried forward as a near-term extension of this work.

VII. CONCLUSION

NextGen GeoSecure is a smart attendance management system that combines a dynamic, session-bound QR code, GPS-based geofencing,

device-identity verification and JWT authentication so that only a genuinely present, registered student can mark attendance. By requiring all four checks to pass together, the system is designed to overcome both the proxy-attendance weaknesses of QR-only and GPS-only systems and the administrative overhead of manual roll-call, while offering instructors a real-time, exportable dashboard. The result is intended to be an efficient, scalable and paperless attendance workflow suitable for deployment across a college campus using only the smartphones that students and faculty already carry.

VIII. FUTURE WORK

- Bluetooth-based secondary proximity verification as an additional layer.
- AI-powered anomaly and fraud-pattern detection across historical attendance logs.
- Automated notifications to parents/guardians for repeated absences.
- Cloud-based analytics for attendance trends across courses and semesters.
- Multi-campus support for institutions with more than one location.

REFERENCES

- [1] S. K. Gupta, N. Yadav, A. Pandey, R. Sharma, and A. Chauhan, "Geolocation-based attendance tracking system: A comprehensive review," in *Proc. 2025 3rd Int. Conf. Communication, Security, and Artificial Intelligence (ICCSAI)*, 2025, pp. 932–935, doi: 10.1109/ICCSAI64074.2025.11064660.
- [2] N. Kumar, S. Sharma, A. Sharma, M. Singh, P. K. Verma, and H. Arora, "Real-time deep learning based anti-proxy presence monitoring," in *Proc. Int. Conf. Electronics, AI and Computing (EAIC)*, 2025.
- [3] A. Vu-Quoc, B. Nguyen-Phuc, L. Van-Thien, C. Dang-Le-Bao, T. Nguyen-Khanh, and Q. Le-Trung, "Research and development of attendance system for smart classroom using Bluetooth Low Energy and facial recognition technologies," in *Proc. 2024 RIVF Int. Conf. Computing and Communication Technologies (RIVF)*, 2024, pp. 266–270, doi: 10.1109/RIVF64335.2024.11009036.
- [4] S. Pathan, L. Bommireddipalli, B. Deka, S. Anandham, A. T. Bhattu, and S. Boorla, "A location and QR code-based solution for efficient attendance management," in *Proc. 2025 Int. Conf. Machine Learning and Autonomous Systems (ICMLAS)*, 2025, pp. 859–866, doi: 10.1109/ICMLAS64557.2025.10968718.
- [5] K. Fitriyani, K. Manaf, H. Purwanto, H. H. Solihin, E. Andiansyah, and D. Pitoyo, "Development of a web-based employee attendance application with gamification and GPS technology to improve attendance discipline," in *Proc. 2025 19th Int. Conf. Telecommunication Systems, Services, and Applications (TSSA)*, 2025, doi: 10.1109/TSSA68467.2025.11303815.
- [6] S. W. Taju, Y. P. Mamahit, and J. A. Pongantung, "Implementing QR code and geolocation technologies for the student attendance system," *COGITO Smart J.*, Universitas Klabat, vol. 10, no. 1, 2024.
- [7] P. Patil, S. Ringe, P. Gaikwad, P. Mahajan, and S. Mogare, "An Android application for attendance using geofencing," *Int. J. Adv. Res. Comput. Commun. Eng. (IJARCCE)*, vol. 13, no. 5, 2024.
- [8] S. Kumari and P. Kumar, "QR-attendance system with geo-location," *Int. J. Adv. Res., Ideas Innovations Technol. (IJARIIT)*, vol. 10, no. 6, 2024.
- [9] B. R. Tejas, S. M. Chithra, K. H. Prathibha, A. P. Kashyap, H. M. Rudresh, and K. J. Rajashekar, "GeoAttend: A dynamic QR code-based attendance system with real-time geofencing, live analytics dashboard, and automated exam eligibility verification," *Int. J. Adv. Sci. Innov.*, vol. 8, no. 1, 2026.
- [10] "AttendEase: An online-onsite router-based mobile application for tracking faculty and student attendance," *IEEE Xplore Conference Publication*, document ID 11137193.