International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
|70-0434 www.zesterapublications.com Original Research Paper

Smart Attendance System Using Dynamic QR Code

Received: 20-04-2026 | Accepted: 28-05-2026 | Published: 04-06-2026

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
|70-0434 www.zesterapublications.com Original Research Paper

Mr. Manas Sundar Kar
Student, Dept. of CSE,
GIFT Autonomous, Bhubaneswar

Mr. Bhim Tudu
Student, Dept. of CSE,
GIFT Autonomous, Bhubaneswar

Prof. Dr. Jagannath Ray
Project Guide, Dept. of CSE,
GIFT Autonomous, Bhubaneswar

Abstract

Traditional paper-based and biometric attendance systems suffer from inefficiencies such as proxy attendance, time c
onsumption, and data management difficulties. This paper presents a Smart Attendance System that leverages Dynamic QR Code generation with automatic token expiry and Google OAuth 2.0 single sign-on (SSO) authentication to mark student attendance in real time. The system is built on the MERN stack (MongoDB, Express.js, React.js, Node.js) and uses JSON Web Tokens (JWT) for session management. Faculty members generate time-limited QR codes for each class session; students scan these codes via their mobile browsers after authenticating through their institutional Google accounts. The system prevents proxy attendance through device-based and token-based validation. Attendance records are stored in a cloud-based database (MySQL/MongoDB) and made available to faculty as downloadable CSV/PDF reports. Evaluation results demonstrate an attendance marking accuracy of 98.6% and an average QR scan-to-record latency of under 1.2 seconds. The proposed system significantly reduces administrative overhead and eliminates manual errors.

Keywords—Smart Attendance; Dynamic QR Code; Google OAuth 2.0; MERN Stack; JWT Authentication; Real-time Web Application; Proxy Prevention.

I. INTRODUCTION

Manual attendance marking in educational institutions is a time-consuming and error-prone process. The traditional roll-call method consumes valuable class time and is susceptible to proxy attendance, where students mark attendance on behalf of absentees. Biometric systems, while more secure, require expensive hardware installations and physical contact, which raises hygiene and accessibility concerns.

The rapid proliferation of smartphones and ubiquitous internet connectivity provides an opportunity to design a software-only attendance solution that is both secure and efficient. QR (Quick Response) code technology, originally developed for inventory tracking, has emerged as a versatile tool for information transfer. When combined with modern web authentication protocols such as OAuth 2.0, QR codes can serve as a reliable medium for student identification and attendance verification.

This paper proposes a Smart Attendance System (SAS) that addresses the limitations of existing methods. The system uses dynamically regenerated QR codes that expire every 90 seconds, making them resistant to screenshot-based proxy attempts. Students authenticate using their institutional Google accounts via OAuth 2.0, eliminating the need for a separate registration process. The back-end REST API, built with Node.js and Express.js, processes attendance records in real time, while the React.js front-end provides an interactive dashboard for both faculty and students.

The remainder of this paper is organized as follows. Section II reviews related work. Section III describes the system architecture and design. Section IV discusses the implementation. Section V presents evaluation results. Section VI outlines open research issues, and Section VII concludes the paper.

Received: 20-04-2026 | Accepted: 28-05-2026 | Published: 04-06-2026

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
www.zesterapublications.com Original Research Paper
Zestera PUBLICATIONS
70-0434

II. RELATED WORK

Several approaches have been proposed to automate attendance management. Misbahuddin et al. [1] proposed a QR-code-based attendance system using static QR codes printed on student ID cards. While effective, static codes are vulnerable to sharing and photograph-based proxy attacks. The proposed system overcomes this by generating a fresh QR token for every class session with a configurable expiry window.

Biometric-based systems using fingerprints [2] and facial recognition [3] have demonstrated high accuracy. However, these approaches require dedicated hardware and raise privacy concerns under regulations such as GDPR. Cloud-based facial recognition solutions reduce hardware dependency but introduce network latency and storage costs. Our approach avoids biometric data entirely, relying instead on OAuth-based identity verification.

RFID-based systems [4] offer contactless operation but mandate that each student carry an RFID tag and that readers be installed in every classroom. Islam et al. [5] implemented a Bluetooth Low Energy (BLE) beacon system that detects student proximity; however, BLE signals can traverse walls, compromising location accuracy.

Mobile application-based systems using GPS geofencing [6] restrict attendance marking to a defined physical area. While promising, GPS accuracy degrades indoors, and students can spoof GPS coordinates using third-party applications. The QR scan approach inherently provides location verification because the QR code is displayed on a screen inside the classroom.

Recent work by Gupta et al. [7] explored a hybrid system combining NFC tags and one-time passwords (OTP). The system achieved 97% accuracy but required NFC-enabled devices, limiting accessibility. The proposed SAS operates on any smartphone with a camera and a modern web browser, ensuring maximum compatibility.

III. SYSTEM ARCHITECTURE

The Smart Attendance System follows a three-tier client-server architecture consisting of a presentation layer, an application logic layer, and a data persistence layer.

A. Presentation Layer

The front-end is developed using React.js 18 with functional components and React Hooks. The teacher dashboard provides controls for session creation, QR code generation, and attendance report export. The student interface is a responsive, mobile-first web page that activates the device camera to scan QR codes. Tailwind CSS is used for responsive styling, ensuring compatibility across devices ranging from 320px mobile screens to wide-screen desktops.

B. Application Logic Layer

The back-end REST API is built with Node.js 18 and Express.js 4. The API exposes authenticated endpoints for session management, QR token generation, attendance marking, and report generation. Authentication middleware validates JWT tokens on every protected route. Google OAuth 2.0 is integrated using the Passport.js library, enabling students to sign in with their institutional Google accounts without a separate username/password registration.

C. Data Persistence Layer

Attendance records, session metadata, and user profiles are stored in a relational MySQL database managed through phpMyAdmin. The schema consists of five core tables: teachers, students, subjects, sessions, qr_tokens, and attendance_records. Foreign key constraints enforce referential integrity across tables. Database queries are parameterized to prevent SQL injection attacks.

D. Dynamic QR Code Generation

When a faculty member initiates a session, the server generates a UUID v4 token and encodes it as a QR code using the qrcode npm package. The token, along with its expiry timestamp (current time + 90 seconds), is stored in the qr_tokens table. The QR code image is returned to the faculty dashboard as a Base64-encoded PNG. A server-side cron job invalidates expired tokens and triggers automatic regeneration, ensuring the displayed QR code is always valid. This 90-second

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
www.zesterapublications.com Original Research Paper
70-0434

refresh cycle makes screenshot-based proxy attendance practically infeasible.

IV. IMPLEMENTATION

A. Authentication Flow

Student authentication is handled via Google OAuth 2.0. On visiting the attendance URL embedded in the QR code, the student is redirected to Google's authorization server. After granting consent, an authorization code is returned to the callback endpoint, which exchanges it for an access token and retrieves the student's Google profile (name, email, and Google ID). The email domain is validated against a whitelist of institutional domains to prevent external accounts. A JWT containing the student's ID and session information is issued and stored as an HTTP-only cookie for subsequent requests.

B. Attendance Marking Process

Upon successful authentication, the system validates the scanned QR token against the qr_tokens table. Validation checks include: (i) token existence, (ii) expiry status, (iii) session activity status, and (iv) prior attendance record for the same student-session pair (enforced by a UNIQUE constraint on (student_id, session_id)). If all checks pass, an attendance record is inserted with the marked_at timestamp, IP address, and device user-agent string. A real-time WebSocket event (Socket.io) notifies the faculty dashboard of the new attendance entry without requiring a page refresh.

C. Report Generation

Faculty members can export attendance data in two formats: CSV (using the csv-writer library) and PDF (using PDFKit). Reports include session metadata (date, subject, faculty name), individual student records, and summary statistics (total present, total absent, attendance percentage). The export endpoint streams the file directly to the browser, avoiding temporary file storage on the server.

D. Security Measures

Beyond token expiry, several additional security measures are implemented. Rate limiting (express-rate-limit) restricts QR scan attempts to 10 per minute per IP address. CORS policy restricts API access to the

V. RESULTS AND EVALUATION

The system was evaluated over an 8-week pilot period involving 12 faculty members and 340 students across 6 departments. A total of 287 class sessions were conducted using the Smart Attendance System.

A. Performance Metrics

The average time from QR scan initiation to attendance confirmation was measured at 1.18 seconds on a 4G network and 0.82 seconds on the institutional Wi-Fi network. The system handled a peak concurrent load of 180 simultaneous scan requests (observed at the start of large lecture sessions) without degradation, achieving a 99.3% success rate for attendance marking. The remaining 0.7% of failures were attributed to transient network connectivity issues on student devices.

Metric	Value
Total Sessions	287
Students Enrolled	340
Avg. Latency (Wi-Fi)	0.82 s
Avg. Latency (4G)	1.18 s
Marking Accuracy	98.6%
Peak Concurrent Users	180
Success Rate	99.3%
Proxy Attempts Blocked	14

TABLE I: System Performance Evaluation Results

B. Proxy Prevention Effectiveness

During the pilot, 14 attempted proxy attacks were recorded — all involving students sharing screenshots of QR codes via messaging applications. In every case, the shared QR code had expired by the time the absent student attempted to use it, and the system correctly rejected the token. The 90-second refresh interval was found to be short enough to deter sharing while remaining long enough for all students in a classroom to scan comfortably.

C. User Satisfaction Survey

Received: 20-04-2026 | Accepted: 28-05-2026 | Published: 04-06-2026

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
|70-0434 www.zesterapublications.com Original Research Paper

institutional domain. All database queries use prepared statements. Sensitive environment variables (database credentials, OAuth client secrets, JWT secret) are stored in .env files and excluded from version control via .gitignore. HTTPS is enforced in production using Let's Encrypt TLS certificates.

VI. OPEN RESEARCH ISSUES

Despite the promising results, several open research challenges remain in the domain of QR-based attendance systems.

A. Offline Attendance Marking

The current system requires continuous internet connectivity for both QR generation and scanning. In institutions with unreliable network infrastructure, offline-capable attendance marking is a critical requirement. Progressive Web App (PWA) techniques and service workers could enable local caching of tokens with deferred synchronization, but ensuring the integrity and freshness of offline tokens presents a significant cryptographic challenge.

B. Multi-Factor Biometric Verification

While OAuth identity verification prevents unauthorized account usage, it does not physically confirm that the authenticated student is present in the classroom. Integrating lightweight, on-device biometric verification (such as facial liveness detection using the MediaPipe or TensorFlow.js frameworks) as a second factor could further strengthen proxy prevention without requiring server-side biometric data storage.

C. Scalability for Large Institutions

The current deployment handles up to 180 concurrent users. Universities with thousands of simultaneous sessions (e.g., during common lecture slots) would require horizontal scaling with load balancers, distributed session management (Redis), and database read replicas. Investigating the performance characteristics of the system under institutional-scale loads is an important direction for future work.

A post-pilot survey conducted among 180 students and 12 faculty members revealed that 91% of students found the system easier to use than manual roll-call, and 88% of faculty reported a reduction in class time spent on attendance. 95% of faculty indicated they would prefer to continue using the system in subsequent semesters.

D. Accessibility and Device Equity

The system assumes that all students possess a smartphone with a functioning camera. Students with disabilities or those without compatible devices are currently excluded. Future work should explore accessibility alternatives such as SMS-based one-time passwords (OTP) or NFC tap-based fallback mechanisms.

E. Data Privacy and Regulatory Compliance

The collection of IP addresses, device information, and Google profile data raises privacy concerns under regulations such as GDPR (European Union) and PDPB (India). A comprehensive data minimization strategy — retaining only the data strictly necessary for attendance verification — and a transparent user consent framework are essential for institutional adoption at scale.

F. AI-Driven Attendance Analytics

The system currently provides raw attendance counts and percentages. Integrating machine learning models to predict at-risk students based on attendance patterns, identify correlation between attendance and academic performance, and generate automated alerts for parents or advisors represents a high-value research and development opportunity.

VII. CONCLUSION

This paper presented a Smart Attendance System that uses Dynamic QR Code generation and Google OAuth 2.0 authentication to eliminate proxy attendance and reduce administrative overhead in educational institutions. The system, built on the MERN technology stack with a MySQL relational database, was validated through an 8-week pilot involving 340 students and 12 faculty members across 287 sessions. The results demonstrate an attendance marking accuracy of 98.6%, an average scan-to-record latency of under 1.2 seconds, and a 100% success rate in blocking the 14 recorded proxy attempts. User satisfaction surveys indicate strong faculty and student acceptance of the system.

Future work will focus on offline-capable operation, multi-factor biometric integration, AI-driven attendance analytics, and compliance with data privacy regulations. The proposed system demonstrates that a purely software-based, smartphone-native attendance solution can match or exceed the security of hardware-dependent alternatives while remaining more accessible and cost-effective.

References

[1] S. Misbahuddin, J. A. Ahamed, R. Mahammad and P. Habeeb, "QR code based dynamic attendance recording system," International Conference on Circuit, Power and Computing Technologies, 2015, pp. 1-5.

[2] A. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition," IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 2004, pp. 4-20.

[3] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2001, pp. 511-518.

[4] K. Mun Wai, H. Meng Huat, G. W. Chang and L. H. Kuan, "RFID attendance management system," Journal of Information Technology and Multimedia, 9(1), 2011, pp. 43-52.

[5] M. S. Islam, M. A. Ameen and M. A. Islam, "Design and implementation of a smart attendance system using Bluetooth low energy," International Journal of Computer Applications, 180(19), 2018, pp. 1-6.

[6] A. Kumar and A. Pande, "GPS-based student attendance system using Android and cloud computing," International Journal of Computer Applications, 180(27), 2018, pp. 12-17.

[7] R. Gupta, S. Yadav and A. Sharma, "A hybrid attendance management system using NFC and OTP," International Journal of Advanced Research in Computer Science, 9(2), 2018, pp. 394-398.

[8] M. K. Kakhani, S. Kakhani and S. R. Biradar, "Research issues in big data analytics," International Journal of Application or Innovation in Engineering & Management, 2(8), 2015, pp. 228-232.

[9] A. Gandomi and M. Haider, "Beyond the hype: Big data concepts, methods, and analytics," International Journal of Information Management, 35(2), 2015, pp. 137-144.

[10] N. Mishra, C. Lin and H. Chang, "A cognitive adopted framework for IoT big data management and knowledge discovery," International Journal of Distributed Sensor Networks, 2015, pp. 1-13.