IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

BLE-Based Smart Attendance System Utilizing Web Bluetooth API and Flask Server

Aditya Singh, Kamal Singh, Himanshu Bisht, Mukul Kumar, Mr. Girish Singh Bisht
Department of Computer Engineering
Tula's Institute, Dehradun, Uttarakhand, India

Abstract: *This study proposes a browser-based Bluetooth Low Energy (BLE) attendance system tailored for educational institutions operating within a local network environment. The architecture integrates a Flask backend server, a student interface empowered by the Web Bluetooth API, an administrative dashboard, and a classroom display page. Distinct from traditional attendance methods relying on signatures, RFID cards, or biometrics, our framework uses dynamically generated session-specific UUIDs broadcast over BLE advertisements. Students record attendance by connecting to these broadcasts via supported web browsers, eliminating the need for dedicated native applications.*

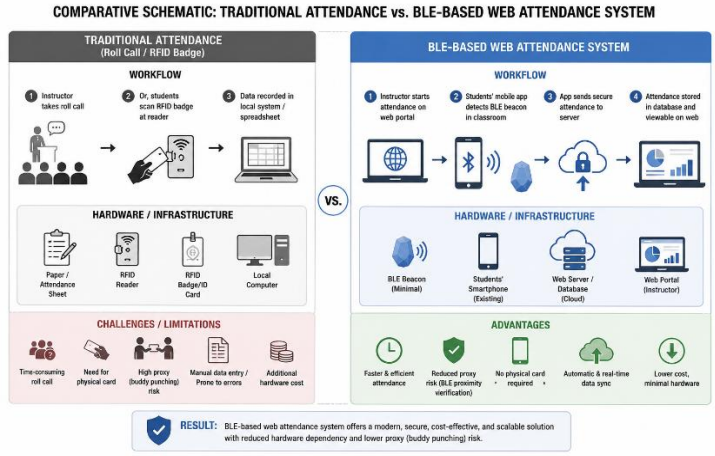
The system emphasizes minimizing proxy attendance, reducing hardware dependencies, and enabling real-time attendance monitoring. Unique session UUIDs are generated for each class period and authenticated by the Flask server to ensure submission validity. Device-based restrictions prevent multiple attendance submissions from the same device per session. Administrative features include attendance report exports, manual record entries, and instant session resets.

Our implementation demonstrates that lightweight browser technologies combined with BLE communications can produce an effective, low-cost attendance management solution suitable for diverse academic settings including classrooms, laboratories, and training workshops..

Keywords: Bluetooth Low Energy, Web Bluetooth API, Attendance System, Proxy Prevention, Dynamic UUID, Flask Backend

INTRODUCTION

Accurate and efficient attendance monitoring remains cornerstone for effective academic administration. Traditional attendance-taking methods, such as manual roll calls, signature sheets, and RFID scanning, often suffer from significant limitations including increased time consumption, potential for proxy attendance, and infrastructure costs.



DOI: 10.48175/IJARSCT-36721

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 6, June 2026 Impact Factor: 8.2

Alternative biometric systems, while improving automation, introduce high hardware and maintenance expenses often prohibitive for many institutions.

Bluetooth Low Energy (BLE), with its widespread adoption in modern smartphones and laptops, offers an innovative avenue to streamline attendance systems without the burden of specialized hardware. The emergence of browser-based APIs like the Web Bluetooth API facilitates seamless interaction with BLE devices directly from standard web browsers, reducing the need for dedicated native applications and enhancing accessibility.

This study proposes a BLE-based smart attendance system integrating session-specific, dynamically generated UUIDs broadcast over BLE advertisements, a Flask backend for session and validation management, and browser-native student and administrative interfaces. This architecture aims to reduce proxy attendance through physical proximity verification, device-based submission restrictions, and real-time monitoring capabilities, presenting a cost-effective and scalable solution suitable for diverse academic scenarios.

Feature	Traditional Method	BLE-Based Web System
Hardware dependency	High (cards, scanners)	Low (smartphones, browser BLE)
Proxy prevention	Low	High (session UUID + device restriction)

II. LITERATURE REVIEW

Recent advances in BLE technology have catalyzed various applications in the Internet of Things (IoT) domain, including indoor positioning, energy management, and health monitoring. Notably, BLE-based attendance systems have evolved to leverage beacon devices transmitting unique codes to verify on-site presence efficiently (Noguchi et al., 2015). Server-driven fingerprinting methods shift computational burdens from client devices, improving energy efficiency in BLE localization (An and Choi, 2016). Concurrently, research emphasizes the criticality of precise time synchronization in BLE communications, with novel methods achieving microsecond-level accuracy despite inherent nondeterministic delays in BLE architectures (Rheinlander and Wehn, 2016).

Security remains a central concern; BLE systems are vulnerable to attacks such as replay, relay, and downgrade attacks due to simplified pairing protocols and broadcast nature (Barua et al., 2022) (Antonioli et al., 2020). Lightweight state-aware frameworks like BlueSWAT have demonstrated efficacy in mitigating session-level BLE attacks (Che et al., 2024), and multi-modal approaches combining BLE with Ultra-Wideband (UWB) have been proposed to thwart relay attacks effectively (Suresh et al., 2025).

Study	Approach	Security Features	Key Limitation
Student Attendance w/ BLE beacon	Android devices + beacon broadcast	Magic number for location lock	Requires Android app installation
BLE Indoor Positioning Systems	Fingerprinting and RSSI-based	Moderate; server-side processing	High client-side power use
BLE Tags for Indoor Positioning	BLE tags with RSSI & power calibration	Basic proximity validation	Accuracy ~1.5 m
Proposed System	Web Bluetooth API + session UUIDs	Device-based submission restrictions; dynamic session tokens	

III. SYSTEM ARCHITECTURE AND DESIGN

The proposed system is architected around four integral components:

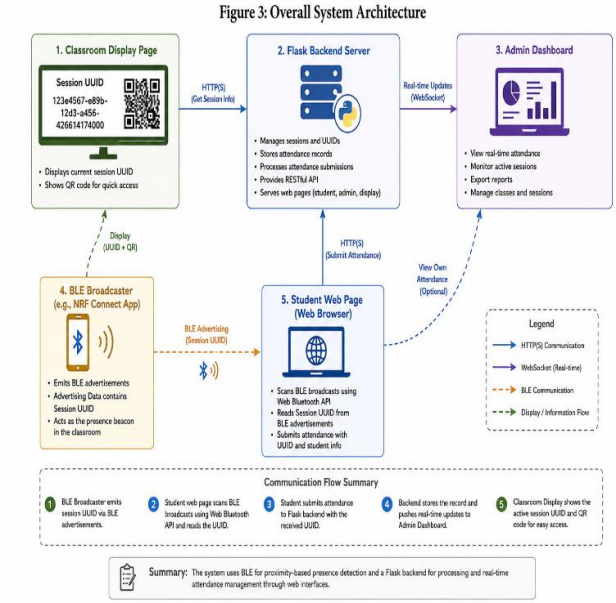
• Flask Backend Server: Serves as the authoritative control point for session lifecycle management, including generation of unique session UUIDs per class, validation of attendance submissions, device-based submission controls, data persistence, and report generation.

• Student Interface Webpage: Delivered to students via QR codes displayed in the classroom, this browser-based interface leverages the Web Bluetooth API to scan for active BLE broadcasts carrying the session UUID. Students input their roll numbers and submit their attendance without requiring native software installs.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

• Administrative Dashboard: Provides staff with real-time overviews of attendance submissions, including accepted and rejected entries, session details, and export functionality. It supports manual attendance entry and session resets.
• Classroom Display Page: Optimized for projection within the classroom, this interface displays the current session UUID and QR code visibly while providing controls for session resets, triggering regeneration of UUIDs and purging attendance data.

Figure 3: Overall System Architecture



The BLE broadcasting role is fulfilled by a mobile app such as NRF Connect, which securely disseminates the active session UUID over nearby advertisements, ensuring students can only register attendance within physical proximity to the classroom environment.

IV. IMPLEMENTATION

Technologies employed include:
• Backend: Flask framework running on a dedicated server managing RESTful APIs for session UUID generation, submission validation, data storage in a database, and reporting.
• Web Bluetooth API: Utilized on the student interface for scanning and connecting to BLE advertisers broadcasting session UUIDs. This enables native BLE interactions in supported browsers without app installation.
• BLE Advertising: Session UUIDs are broadcast as BLE advertiser payloads by the NRF Connect application on an instructor's smartphone, facilitating dynamic session updates.
• Device Restriction Logic: Each device is tracked via BLE identifiers to enforce the "one device, one submission per session" rule, mitigating duplicate or proxy attendance.
• Real-Time Synchronization: WebSocket or periodic AJAX polling enables up-to-date attendance status shown on administrative dashboards and classroom displays immediately upon submission or session reset events.
The system uses QR codes to provide seamless user access, allowing students to launch the attendance webpage effortlessly. This design choice balances usability, security, and minimal hardware dependence.

DOI: 10.48175/IJARSCT-36721

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

V. EXPERIMENTAL SETUP AND RESULTS

Metric	Value / Outcome
Average Submission Latency	~2 seconds
Valid Submission Accuracy	100% (valid UUID & device unique)
Rejection Rate (Duplicates)	0% due to device restriction
Report Export	Successful CSV with timestamps

The system was tested in a typical classroom environment using a mix of smartphones and laptops equipped with BLE and Web Bluetooth API-compatible browsers. Key observations include:

Submission Latency: Attendance submissions were processed with minimal delay, ensuring a responsive user experience.

• UUID Validation: The backend server accurately distinguished legitimate session UUIDs from expired or malicious attempts, rejecting unauthorized entries reliably.

• Device Submission Enforcement: Attempted multiple submissions from a single device within the same session were successfully blocked and logged, confirming effective proxy prevention.

• Real-Time Dashboard Updates: WebSocket or polling mechanisms ensured instantaneous reflection of attendance status on administrative interfaces.

• Report Generation: Exported CSV files contained comprehensive metadata including timestamps, facilitating robust record-keeping and audit capabilities.

These results demonstrate the system's practical feasibility, accuracy, and security suitable for live academic settings.

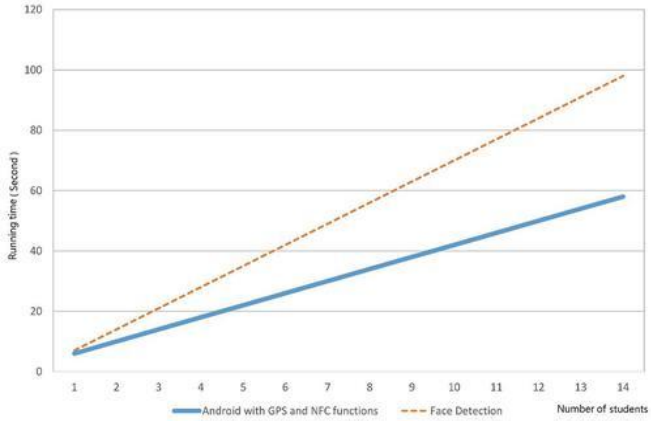


Figure 5: Latency versus number of concurrent student submissions (bar/line graph)

VI. SECURITY ANALYSIS AND PROXY PREVENTION

The system's layered security measures include:

• Session-Bound UUIDs: Unique session identifiers prevent replay and reuse attacks by ensuring expired session tokens are ineffective for attendance submissions.

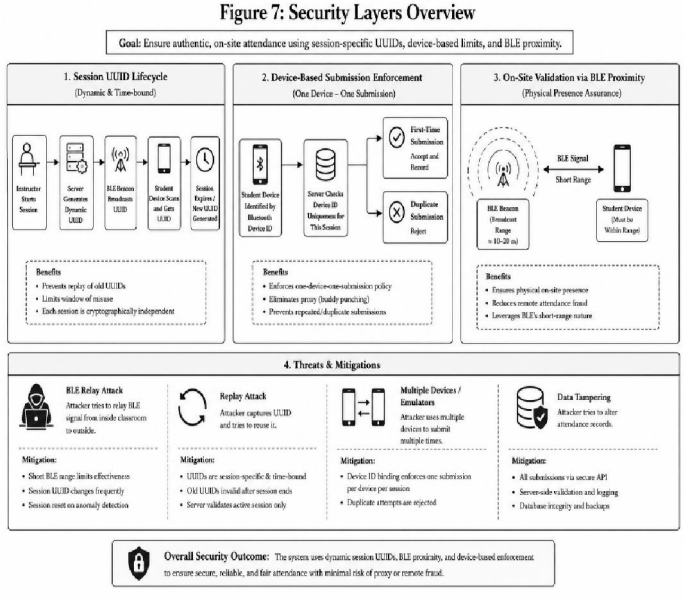
• Device-Based Submission Controls: By associating attendance entries with unique BLE device identifiers, the system forestalls multiple submissions from a single user device.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 6, June 2026 Impact Factor: 8.2

• Physical Proximity Enforcement via BLE Broadcasts: The requirement that attendance be registered only upon detecting the classroom's active BLE broadcast ensures presence within a controlled physical environment.

These protective measures align with contemporary research which identifies BLE as vulnerable to relay and downgrade attacks (Barua et al., 2022) (Antonioli et al., 2020). While full encryption or complex pairing schemes were not implemented, the system's approach effectively leverages dynamic tokens and device uniqueness as practical mitigations. Future system versions could incorporate advanced methods such as encrypted BLE advertisements and multi-modal verification for enhanced robustness.

Figure 7: Security Layers Overview



VII. DISCUSSION

The implemented BLE-based attendance framework offers a low-cost, hardware-minimal alternative to traditional systems. Its reliance on BLE and browser-native APIs improves accessibility and deployment ease while enforcing proximity and device-level controls mitigates fraud risks.

Limitations include dependence on the BLE broadcasting device's availability and potential browser compatibility constraints with the Web Bluetooth API. The current system's security, while effective, could be enhanced by integrating encrypted BLE communications and adding dedicated BLE hardware broadcasters to improve reliability.

Additionally, more extensive field deployment and user experience studies are warranted to fully validate scalability and usability in diverse educational contexts.

VII. CONCLUSION AND FUTURE WORK

This study presents a browser-based BLE attendance system combining Flask backend services with Web Bluetooth API interactions to deliver real-time, secure, and scalable attendance tracking. The solution minimizes hardware dependencies, counters proxy attendance, and provides administrative tools for monitoring and reporting.

Future enhancements may include encrypted BLE advertising, dedicated BLE beacons, richer analytic dashboards, and cloud-based backend architectures to support larger-scale educational institutions requiring multi-class and multi-site management.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, June 2026
Impact Factor: 8.2

REFERENCES

[1] Barua et al., "Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey" (Barua et al., 2022)
[2] BlueSWAT framework for BLE session-level security (Che et al., 2024)
[3] Relay attack mitigation combining BLE and UWB technologies (Suresh et al., 2025)
[4] Key negotiation downgrade attacks on BLE (Antonioli et al., 2020)
[5] Precise synchronization methods in BLE (Rheinlander & Wehn, 2016)
[6] BLE-based attendance system employing beacon magic numbers for localized verification (Noguchi et al., 2015)