A Secure Hybrid Attendance System with Face Recognition QR Validation, and Session-Level Restrictions

Abstract

This paper presents a secure hybrid attendance system designed to prevent proxy attendance, multi-device misuse, and fake scans in academic environments. Unlike existing methods such as manual roll call, QR-only systems, or simple face recognition, our system integrates multiple layers of verification. It combines QR validation with face recognition, enforces a one-device-per-student rule, applies session-level face lock, and introduces an IT-controlled logout policy. Additionally, it incorporates time-bound QR codes (8-second expiry) and liveness detection (blink verification) to prevent spoofing. The results show that the proposed system provides fraud-resistant, low-cost, and scalable attendance management.

Introduction / Problem Statement

Attendance is an essential process in educational institutions. Traditional approaches such as manual roll call are slow and error-prone, while biometric systems require specialized hardware and may still allow proxying. QR-only attendance systems can be shared easily, and basic face recognition can be spoofed with photos or videos. The key problems are proxy attendance, multi-device misuse, and fake scans. Institutions need a system that is secure, reliable, and scalable.

Related Work

Manual roll call is outdated and unreliable. Biometric systems such as fingerprint and RFID improve accuracy but require costly infrastructure. QR-only systems are lightweight but vulnerable to code sharing. Face recognition systems remove QR dependency but can be fooled with photos and videos. Existing methods fail to combine multi-factor validation with device and session restrictions. This gap motivates the development of our hybrid approach.

Proposed Method

The proposed system introduces the following key contributions:

1. Hybrid Validation: Face recognition + QR scan together.
2. One-Device Restriction: Each student can log in on only one device.
3. IT-Controlled Logout: Logout requires IT Department approval to prevent misuse.
4. Session Face Lock: A student’s face can only be used once per session.
5. Time-Bound QR: Each lecture QR is valid only for 8 seconds.
6. Liveness Detection: Students must blink during scanning to prevent photo/video spoofing.
7. Proof of Attendance: Stores captured photo + hash + metadata for verification.

Implementation

- Frontend: React Native mobile application.
- Backend: Node.js with Express framework.
- Database: MySQL (fields include status, method, photo, hash, timestamp).
- Face Recognition: Implemented via Expo Camera / VisionCamera (upgrade planned with ML Kit).
- QR Codes: Secure lecture-generated QR codes with 8-second expiry.
- Security Rules: One-device login, IT-controlled logout, and session lock.

Results & Observations

The system was tested against common attendance fraud scenarios:
- Multi-device misuse: ■ Blocked.
- Logout/login misuse: ■ Blocked (IT approval required).
- Proxy via friend scanning: ■ Blocked (session lock + device rule).
- Fake QR codes: ■ Blocked (only lecture QR + 8-second expiry).
- Photo/video spoof: ■ Blocked (blink-based liveness detection).

The system ensures traceability by storing both the student’s photo and a secure hash in the database.

Comparison Table

System Type	Vulnerability	Security Level
QR-only	Shareable, can be faked	Low
Face-only	Can be spoofed by photo/video	Medium
Proposed Hybrid	QR+Face+Liveness+Restrictions	High

Conclusion

This research introduces a novel hybrid attendance solution that is secure, scalable, and cost-effective. By combining QR validation, face recognition, device restrictions, session locks, time-bound QR expiry, and blink-based liveness detection, the system effectively eliminates proxy attendance and misuse. It ensures reliability without requiring specialized hardware, making it suitable for widespread adoption in academic institutions.

Future Work

Future improvements include:
- Advanced face detection with ML Kit for faster and more accurate scans.
- Enhanced liveness checks such as head-turn or smile detection.
- AI-based face embeddings for stronger identity matching.
- Cloud-based deployment for cross-institution scalability.
- Integration with academic ERP systems for end-to-end automation.