

# A Hybrid Attendance Framework Using Proximity Sensing and Temporal Verification

SHIVAM

BE CSE AIML CHANDIGARH UNIVERSITY GHARUAN, PUNJAB

\*\*\*

**Abstract** - Hybrid E-attendance system is a Framework designed to monitor students' attendance in institutions using proximity and AADHAAR enabled biometric attendance system (AEBAS) Along with temporal facial Authentication, Till date The institutions use traditional method for attendance monitoring and management, which often fail to ensure actual presence of student and are vulnerable to proxy attendance. The proposed system leverages AEBAS for user Authentication using fingerprint or iris recognition, that generates a dynamic QR code or Network credentials outside the class, with this user connects to a certain WIFI or Bluetooth network, the connectivity time is measured and user is marked present only if satisfies The 80 percent rule, to further mitigate vulnerabilities, periodical facial verifications are conducted, this approach ensures secure entry, identity validation throughout the class and ensures continuous presence tracking. The system demonstrates improved reliability and robustness compared to single-factor traditional attendance systems and conventional biometric systems.

**Key Words:** E-attendance, AEBAS, Proximity Sensing, Face Recognition, Temporal Verification, Biometric Authentication, Proxy Detection

## 1. INTRODUCTION

Attendance systems play a crucial role in institutions as they reflect student's presence and participation in academic sessions, and their discipline and consistency towards studies. Accurate attendance records are essential for institutional compliance and academic evaluation. Traditional methods used in marking attendance such as manual registration by verification, are time-consuming and are prone to human error. Although automated systems such as AEBAS and RFID-based attendance systems are being used, they still fail to ensure continuous presence of student throughout the class duration.

The major limitation of these existing attendance systems lies in their **single-point verification mechanism**. Most systems validate attendance once only at the beginning of the session, introducing several loopholes in these systems:

- Proxy attendance, where one student marks attendance for another.
- Early exit, where students leave after initial verification.
- Lack of continuous monitoring throughout the class.

Biometric systems, including fingerprint and iris recognition like AEBAS ensure secure authentication, and are suitable for initial identity verification but are limited to entry-level authentication. As they do not incorporate temporal validation or continuous presence tracking (proximity), which are essential for correct evaluation of attendance.

This hybrid E-attendance system inculcates idea of proximity-based attendance using WIFI and Bluetooth technologies. These systems determine whether a student is physically present in a session by monitoring his device connectivity and evaluate his attendance status by calculating attendance percentage. Let:

- $T$  = Total duration of class
- $C$  = Connectivity time of the student device

The attendance percentage can be calculated as:

$$A = \frac{C}{T} \times 100$$

Attendance is evaluated based on a predefined threshold condition:

- If  $A \geq 80\%$  → Student is marked **Present**
- If  $A < 80\%$  → Student is marked **Absent**

While proximity sensing allows us to continuously monitor students, it alone is not sufficient due to possible misuse, such as sharing device or leaving the device within the proximity range. Therefore, a **multi-factor approach** is required to enhance system reliability and security.

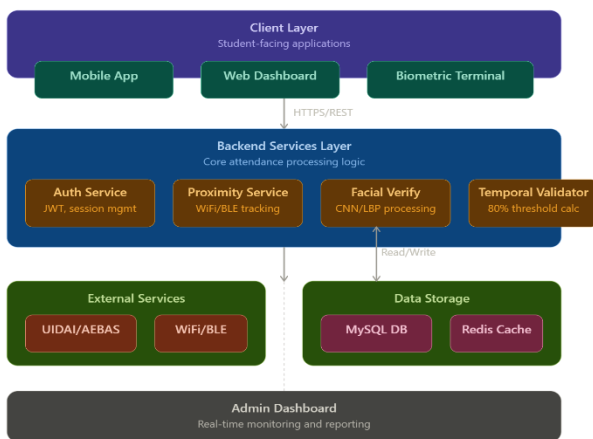
To overcome these limitations, this paper proposes a framework integrating biometric authentication, proximity sensing, temporal validation, and facial verification. The system operates in multiple stages:

- **Stage1: Authentication** Students authenticate using AEBAS (fingerprint/iris) outside the classroom
- **Stage2: Access Generation** A dynamic QR code or secure network credential is generated
- **Stage3: Proximity Monitoring** Students connect to a designated WIFI/Bluetooth network and connectivity is tracked
- **Stage4: Temporal Validation** Attendance is calculated based on connectivity duration ( $C/T$ )

- Stage5: Identity Reinforcement** Periodic facial verification ensures the same individual remains present

This layered approach ensures:

Secure identity verification at entry like AEBAS systems and then Continuous presence tracking by proximity with designated network allowing Detection of proxy attendance and early exits from the sessions giving us Improved accuracy in comparison to traditional attendance systems and methods, allowing secure automated monitoring



reducing manual work.

**FIGURE -1:** System Architecture Diagram

The combination of these components results in a robust, scalable, and efficient attendance management system suitable for modern educational environments. Compared to single-factor traditional systems, the proposed framework provides enhanced accuracy and reliability by combining identity authentication with real-time presence validation with proximity and facial authentication.

This paper discusses the system design, implementation details, and performance evaluation of the proposed hybrid-attendance system.

## 2. LITERATURE REVIEW

Multiple researchers have proposed various methods for the automation of attendance systems including advanced technologies such as biometric based systems, RFID, IoT, and many web based systems. The evolution of traditional attendance management systems reflects a digital transformation of educational institutions, shifting from manual or labour-intensive processes to automated, cyber-physical frameworks.

Traditional attendance management systems primarily included manual paper-based registers, which has long been the standard in educational environments. However, as noted in early studies by Hussain et al. [1], these methods are highly unreliable due to high latency in entry of data and is exposed to human error or proxy attendance where a

student marks attendance for an another absent student. This is a loophole that manual verification cannot deal with, so they developed an RFID-based attendance system that automatically records student entry by scanning RFID cards. Although effective in reducing manual effort, it requires specific hardware and infrastructure setup, increasing implementation costs. Also a research by Farag [2] highlighted a critical flaw: RFID tags verify only the presence of the token, not the individual. This allows for proxy attendance where a single student carries multiple RFID tags, marking large scale false attendance, making it unreliable in case of large academic institutions.

In context of Indian institutions, the Aadhaar Enabled Biometric Attendance System (AEBAS) is one of the most efficient way for secure identity verification, Eze et al. [3] proposed a biometric finger print based attendance system that ensures identity verification and eliminates proxy attendance. This approach enhances accuracy but may face challenges in scalability and hygiene when dealing with large student populations. This biometric based framework significantly mitigates identity fraud by using the centralized unique identification authority of India UIDAI database directly for real-time authentication. Despite its robustness in real-time identity verification, AEBAS primarily functions as a entry-only "checkpoint" technology. As argued in recent literature by Oluwole et al. [4], biometric check-ins by AEBAS are typically performed only at the point of entry. This creates a "temporal void"—a window of time where a student who have successfully authenticated their identity at entry may exit the session before hand. Without a secondary layer of of verification or continuous monitoring, AEBAS cannot distinguish between a student who attended the full duration and one who left immediately or prematurely after the initial scan.

Similarly, Rani et al. [5] and Nair et al. [6], implemented a face recognition-based attendance system using computer vision and machine learning algorithms to identify students through camera or live real time images. The primary algorithm that can be used in face recognition are Convolutional Neural Networks (CNN) and Local Binary Patterns (LBP) as they leverage computer vision to deal with early-exit problems by real-time monitoring of students. The system they produced showed high accuracy under certain conditions but was very sensitive to factors like variations in illumination levels, facial orientation, and different camera quality and angles, leading to false rejection rates FRR degrading user's experience. Despite these minor flaws, it represents a promising step toward AI-driven automated

attendance systems. With a major challenge of large scale implementation due to continuous processing of high resolution video in multiple classrooms across the institute.

Recent researches has explored various digital methods and proposed hybrid attendance systems that combine multiple verification techniques to improve reliability and efficiency. These systems integrate biometric authentication with additional mechanisms such as QR codes, mobile-based access, and temporal validation and facial authentications to address the limitations of individual approaches, Nair et al. [7]. Like Singh et al. [8] proposed an IoT-enabled attendance monitoring system using ESP32 microcontrollers and radio frequency identification RFID modules, connected to a cloud database. Their system offered real-time updates, allowing administrators to monitor students attendance easily via web applications and dashboards. This approach improved scalability and accessibility but required stable internet connectivity.

While such systems demonstrate improved robustness and reliability compared to single-factor or traditional methods, many still lack a unified framework that ensures secure entry, continuous monitoring, and multi-stage identity verification simultaneously. Most existing frameworks prioritize either security (Biometrics), duration (Proximity), or real-time recognition or validations, but rarely include all the factors at once. There is a clear research gap for a hybrid E attendance system that utilizes AEBAS for identity verification, triggers a proximity-based temporal monitor using a 80% connectivity threshold rule, and reinforces the entire session with intermediate facial authentications. This paper addresses this gap by proposing a layered hybrid framework that ensures that authenticated student remains connected to the session for the entire duration.

### 3. PROPOSED METHODOLOGY

The proposed hybrid attendance system is designed as a multi-layered cyber-physical framework that integrates biometric identity authentication AEBAS, network-based proximity sensing, temporal validation for connectivity analysis, and periodic facial verification in between the sessions into a cohesive pipeline. The architecture of this system is depicted in Table. 1. Each stage in this pipeline addresses a specific vulnerability present in existing conventional attendance systems, and together they form a robust and reliable mechanism capable of resisting proxy attendance, early or intermediary exit fraud, and device-sharing exploitations.

### A. System Architecture Overview

TABLE -1: System components and technology mapping

Module	Function	Technology / Standard
Biometric Terminal	Fingerprint and iris capture for identity verification	AEBAS / UIDAI API
Credential Generator	Issues session-specific dynamic QR or token	JWT, QR Code Gen
Proximity Module	Tracks device connectivity in classroom zone	Wi-Fi RSSI / BLE Beacon
Temporal Validator	Computes $A = (C/T) \times 100$ and applies threshold	Backend timer logic
Facial Verifier	Periodic identity re-confirmation via camera	CNN / LBP (OpenCV)
Attendance DB	Stores complete session logs and records	Cloud RDBMS (MySQL)
Admin Dashboard	Real-time monitoring and export interface	Web App (REST API)

The framework consists of five sequential stages that are logically ordered to ensure that each verification layer reinforces the previous one. The five stages are: (1) biometric authentication via the AEBAS, (2) dynamic credential generation for session access, (3) continuous proximity sensing through wireless network connectivity like WIFI/BT, (4) temporal validation using the connectivity-duration ratio, and (5) periodical facial verification for continuous identity verification throughout the class session.

This system architecture follows a client-server model in which a central main attendance server manages authentication tokens, session credentials, connectivity logs, and attendance records of the student. Student-side interactions are done through a dedicated mobile application installed on the student's device. The server communicates

with the UIDAI (Unique Identification Authority of India) database for real-time biometric validation of identity and maintains an independent cloud-hosted attendance database accessible to educational institutions administrators through a web-based dashboard.

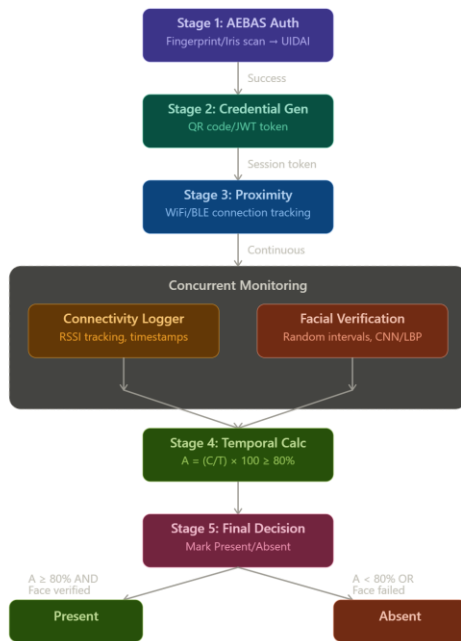


FIGURE -2: System Flow Diagram

### B. Stage 1-Biometric Authentication Using AEBAS

Upon arriving outside the classroom, the attendance process initiates at a designated biometric terminal positioned on the entrance of the classroom. The terminal is integrated with the AEBAS system, which supports two types of biometric inputs: fingerprint scanning and iris recognition. These two modes are selected for their universality, reliability, and resistance to malfunctions under standard operational conditions.

The biometric sample captured at the terminal outside the classroom is transmitted in an encrypted form to the UIDAI for one-to-one verification against the student's Aadhaar-linked profile. This verification step is essential to confirm the student's identity with a high level of certainty, as Aadhaar-based biometric records are managed centrally and are secure from local tampering. Upon successful verification, the AEBAS terminal generates a confirmation signal to the central attendance server, triggering the next phase that is generating credentials. If verification fails due to unregistered or mismatch in biometric data, or a sensor error, access is denied and the student is directed to a human supervisor for manual resolution in case of any discrepancy.

The use of AEBAS at initial stage ensures that the identity of the individual who is initiating the attendance process is established properly, before any proximity sensing or facial checks are performed. This eliminates the most fundamental loopholes of proxy attendance, where one student attempts to mark attendance on behalf of another absent student.

### C. Stage 2 -Dynamic Credential Generation

Following by successful biometric authentication, the attendance server generates a specific credential for the authenticated student. This credential can be issued in one out of two forms depending on the available infrastructure in the educational institutions: a dynamic QR code rendered on the student's mobile application or a one-time network access token delivered through a secure notification on the device. The QR code or token is specifically valid only for the duration of the current session and is bound to the student's unique identifier and the session timestamp making it non-transferable and non-reusable.

The dynamic nature of the credential is an important design choice as it addresses a critical weakness in static credential methods, where a student could share login details or the fixed QR code to another student for proxy marking false presence. Since the credential expires at the end of the designated session and is regenerated fresh at start of each class, it cannot be pre-captured and distributed in advance.

The credential generation module is implemented on the main server using token-based authentication protocols and are generated through Technologies like JWT, QR code generator. The mobile application on the student's device communicates with the server over a secured HTTPS connection, and the credential is displayed exclusively within the authenticated application for the session, preventing screen-capture exploitation.

### D. Stage 3- Proximity Sensing via Network

With the session credentials in hand, the student connects to the network through their registered device specific network either can be a Wi-Fi access point or a Bluetooth beacon designated for that session only. The connection event is logged in by the proximity sensing module on the server, which records the connection timestamps for the student's session entry time.

The proximity module on the server continuously checks the network for device connectivity at regular intervals throughout the class duration. Both Wi-Fi and Bluetooth are complementary channels for proximity. Wi-Fi connectivity is assessed using the Received Signal Strength Indicator (RSSI), which provides us a method to quantitatively measure the

signal strength and allows the system to distinguish between a device that is genuinely present within the classroom range (typically 10–15 meters for an indoor Wi-Fi access point) and one that is barely connected with the network from an closer location. Bluetooth proximity sensing serves as a secondary layer for confirmation, particularly useful in environments with overlapping Wi-Fi coverage zones.

The network infrastructure required for this stage consists of either a dedicated wireless router or Bluetooth gateway or both per classroom, configured in such a way so that the network is isolated from adjacent classrooms, A middleware service running on the attendance server receives periodic connectivity data from each students registered device and maintains a real-time presence log recording of connection and disconnection events with millisecond-level timestamps.

#### E. Stage 4- Temporal Validation and the 80% Threshold Rule

At the end of the session, the attendance server processes the connectivity logs for each student to calculate an attendance percentage using the following formula:

- $T$  = Total duration of class
- $C$  = Connectivity time of the student device

The attendance percentage can be calculated as:

$$A = \frac{C}{T} \times 100$$

Here, Both C and T are measured in seconds to ensure precision.

The computed attendance percentage A is then evaluated against a predefined threshold condition aligned accordingly with standard requirements in education institutions, keeping in mind a 20% buffer for washroom breaks and connectivity issues during the session:

- If  $A \geq 80\%$  → Student is marked **Present**
- If  $A < 80\%$  → Student is marked **Absent**

This threshold-based rule ensures that students who are present in the class for the majority of the duration are marked as present, while accommodating brief, unavoidable disconnections in connectivity such as those caused by momentary interference in network. Simultaneously, it penalizes students by marking them absent, for leaving the session early or before its conclusion, thus addressing the early-exit problem that is common in traditional or single-point check-in systems.

The temporal validation module also maintains even tiniest logs of all connectivity gaps exceeding a configurable tolerance threshold (defaulting to 5 minutes). These gap

records are stored in the attendance DB and are accessible to instructors who may wish to review cases with borderline attendance or investigate patterns of intentional and accidental disconnections and reconnections.

#### F. Stage 5- Periodic Facial Verification

While proximity sensing ensures that a student's registered device one that is connected to the network remains within the classroom, it does not prevent a student from leaving their device behind or passing it to another student. To address this loophole, the framework includes periodic facial verification mechanism that operates at random intervals during the session.

The facial verification subsystem is embedded within the student's mobile application and is triggered by push notifications sent from the attendance server at random intervals. Upon receiving the notification, the student's device activates the front-facing camera and captures a real-time facial image. This image is processed using one of two most reliable machine learning algorithms selected at the time of system configuration:

- **Convolutional Neural Networks (CNN):**

This deep learning approach extracts high-dimensional feature representations from facial images using multiple convolutional and pooling layers. CNN-based verification offers high accuracy even in multiple variations such as illumination, partial clarity, and facial expression but requires comparatively more computational resources on the server.

- **Local Binary Patterns (LBP):**

A computationally lightweight descriptor of texture that encodes the local structure of facial regions into binary patterns. LBP works well for a real-time facial verification in restricted resources and incorporates acceptable accuracy under controlled conditions.

This captured image is transmitted directly to the server, where it is compared with the student's enrolled facial profile image stored in database at the time of initial registration. The comparison gives a similarity score, which is evaluated with a predefined acceptance threshold. If the similarity score meets the expectation of threshold, the verification is considered to be successful and the session proceeds normally. If the score falls below the threshold then it can be a potential identity substitution—the system flags the event, logs the discrepancy, and may optionally send an alert to the course instructor of the concerned student.

The randomization of verification interval is a planned security design decision, as a fixed-interval schedule can be easily detected and exploited by students by briefly returning to their device at these scheduled intervals to pass facial verification. By randomizing the verification intervals within a configurable range (once every 15–30 minutes), the system ensures that the student is present throughout the session.

### G. Attendance Decision Logic and Final Marking

The final attendance for each student is computed by the logical attendance decision module at the end of each session. This module aggregates the outputs of all stages collectively and applies a conjunctive rule: a student is marked Present only if the temporal validation threshold ( $A \geq 80\%$ ) is satisfied AND no unresolved facial verification or biometric failure was recorded during the session. A facial verification failure is considered unresolved if the student did not successfully re-verify within a grace period following the failed check.

The decision logic also includes an override mechanism only accessible to authorized instructors to configure final marking, In cases where the system marks a student absent by mistake—due to technical faults such as unstable network connectivity, device malfunctions, poor lighting or camera conditions—the instructor can manually override attendance with a documented reason. All manual overrides are stored separately and included in the institutional records.

Once the decision is finalized, the attendance record is stored in the cloud database with a complete standardized format including the AEBAS authentication timestamp, session connectivity log summary, facial verification results, the computed attendance percentage, and the final attendance status. This record is visible on the administrative dashboard and can be exported for integration with the educational institution's existing Learning Management System (LMS) making it more feasible and efficient in real-time.

### H. Security Analysis and Vulnerability Mitigation

A critical advantage of the proposed Hybrid system lies in its multi-staged layered security model. Table II presents a structured analysis mapping each identified attack vector to the corresponding mitigation stages implemented within the system.

TABLE -2: Mitigation stage to Attack vector Mapping

Attack / Vulnerability	Mitigation Stage	Mechanism
Proxy at entry	Stage 1- AEBAS Authentication	Biometric uniqueness
Shared device / credential	Stage 2 -Credential Generator	Session-bound token
Early exit after entry	Stage 4 - Temporal Validation	C/T threshold $\geq 80\%$
Device left behind	Stage 5 -Facial Verification.	Random periodic checks
Identity substitution mid-session	Stage 5 -Facial Verification.	CNN / LBP matching
Network spoofing	Stage 3- Proximity	RSSI + BLE dual check

As observed in above Table, no single attack vector is able to destabilize the system because each stage independently verifies a different part of student presence monitoring. A student seeking to fraudulently mark proxy would need to simultaneously defeat biometric identity system, forge session-specific credentials, maintain a device within the classroom proximity zone for at least 80% of the class duration, and pass random facial verification checks a combination that presents a high safety barrier under realistic operational conditions.

### I. Scalability and Deployment Considerations

The proposed hybrid framework is designed while keeping educational institution’s scalability in mind. The server-side components are stored in a Database and can be deployed on cloud infrastructure, enabling system to accommodate large student populations across multiple simultaneous ongoing sessions. The AEBAS terminals represent a fixed hardware investment per building entry point instead of per classroom which reduces the implementation cost. Wireless access points are a common component of modern institutional networks these days, and the proximity sensing software

layer can be deployed as a lightweight service on existing hardware used for network management.

For educational institutions where all students use registered devices, the mobile app serves as the primary interface. For students with device connectivity issues and other technical problems, secondary mechanisms such as instructor-verified manual override and secondary biometric terminals at classroom entry points are being implemented within the system to ensure that unintentional problems do not unfairly penalize students.

This system has a modular design that allows partial deployment, where an institution may implement only selected stages of their choice — for example, Stages 1 to 4 leaving facial verification — as a starting choice, with the option to implement additional stages later as infrastructure increases. This modular system reduces the restriction to entry for institutions with comparatively lesser initial budgets while following a clear upgrade plan toward the full multi-factor framework

#### 4. RESULTS AND DISCUSSIONS

To evaluate the performance of the proposed hybrid framework, a prototype system was tested under artificial classroom conditions. The system was implemented consisting proposed layer using a combination of AEBAS, WIFI-based proximity sensing, temporal validation logic, and periodic facial verifications. A group of students was observed over multiple sessions of fixed duration to check system accuracy, reliability, and resistance to loopholes.

For evaluation, class duration ( $T$ ) of 50 minutes was considered. The connectivity time ( $C$ ) for each student device was recorded using WIFI monitoring, and attendance percentage ( $A$ ) was calculated using the proposed formula.

$$A = \frac{C}{T} \times 100$$

Attendance was marked based on the predefined threshold condition of 80%.

##### Analysis of Results

The results demonstrate that the system effectively enforces both **temporal and identity-based validation**. In a sample of 5 students, S1, S2, and S5 were correctly marked present as they satisfied both the connectivity threshold ( $A \geq 80\%$ ) and facial verification requirements. Student S3, despite passing facial verification, was marked absent due to insufficient connectivity time, demonstrating the effectiveness of the temporal threshold in detecting early exits and S4 was physically present or connected to network but marked absent due to failed facial validation, showing importance of identity check and indicating that the system successfully prevents proxy attendance even when the device remains within the proximity range.

#### Comparison with Existing Systems

TABLE -3: Proposed vs existing systems comparison

Attack Vector	Manual System	RFID Only	Biometric Only	Proposed System
Identity fraud at entry	High	High	Very Low	Very Low
Early exit after check-in	High	High	High	Very Low
Device sharing	N/A	High	N/A	Very Low
Device left behind	N/A	N/A	N/A	Very Low
Mid-session substitution	High	N/A	High	Very Low
Credential replay	N/A	Medium	N/A	Negligible

This comparison clearly shows that the proposed system efficiently outperforms traditional and single-factor systems that were being used by integrating **identity, proximity, and temporal validation** into a unified hybrid system.

##### System Performance

The proposed system was evaluated based on the following parameters:

- **Accuracy:** High accuracy in attendance marking due to combined multiple verification methods
- **Security:** Strong resistance to proxy attendance through biometric and facial validation methods.
- **Reliability:** Continuous monitoring ensures detection of early exits of student.
- **Scalability:** Can be deployed using existing WIFI infrastructure with minimal additional cost for hardware.

##### Discussion

The experimental results confirm that the hybrid approach significantly improves reliability for attendance on E attendance systems by addressing key limitations of existing systems. The integration of AEBAS ensures secure initial authentication of student outside classroom, while WIFI-based proximity sensing enables continuous presence tracking inside classroom. Temporal validation enforces

minimum attendance duration, and periodic facial verification prevents device-based switching.

However, certain limitations were observed, such as dependency on stable network connectivity and sensitivity of facial recognition to various environmental conditions. These challenges can be addressed in future work by implementing offline synchronization mechanisms and more advanced AI-based facial recognition models.

## 5. CONCLUSION

This paper presented a hybrid e-attendance framework that integrates biometric authentication, proximity sensing, temporal validation, and periodic facial verification to address the limitations of traditional and single-factor attendance systems. The proposed system ensures secure identity verification using AEBAS, followed by continuous presence monitoring of student through WIFI and Bluetooth-based proximity sensing. The implementation of temporal analysis using the 80% threshold ensures majority presence of student in class, while periodic facial verification strengthens identity validation process.

The results demonstrate that the multi-layered hybrid approach significantly improves accuracy and reliability making it efficient in attendance marking by effectively tackling common issues such as proxy attendance, early exits, and device-based misuse. Unlike traditional systems that rely on single-point verification, the proposed framework provides continuous monitoring and multi-stage validation, making it more secure and robust for real-world implementation in educational institutions.

However, the system has certain limitations that can vary with the considerable factors including dependency on stable network connectivity and sensitivity of facial recognition to external environmental conditions. These challenges can be overcome in future work by incorporating more advanced AI-based recognition models, edge processing for faster verification, and other synchronising mechanisms to improve system resilience.

Overall, the proposed hybrid attendance system offers a scalable, efficient, and secure solution to traditional and modern attendance management methods and has strong potential for implementation in all kind of learning environments.

## REFERENCES

1. -S. T. Hussain, T. A. Taha, S. R. Ahmed, , "Automated RFID-Based Attendance and Access Control System" 2023 7th International Symposium on Innovative Approaches in Smart Technologies (ISAS), Istanbul, Turkiye,2023,pp.1-6,doi: 10.1109/ISAS60782.2023.10391615
2. W. A. Farag, "An RFID-based smart school attendance and monitoring system," BOHR J. Comput. Intell. Commun. Netw., vol. 1, no. 1, pp. 26-34, 2023, doi: 10.54646/bjicn.2023.05.
3. P. U. Eze, C. K. Joe-Uzuegbu, U. Laz, and F. K. Opara, "Biometric-based attendance system with remote real-time monitoring for tertiary institutions in developing countries," in Proc. IEEE NIGERCON, 2013, pp. 1-8.
4. A.S. Oluwole, O. P. Odekunle, and E. Olubakinde, "Smart fingerprint biometric and RFID time-based attendance management system," Eur. J. Electr. Eng. Comput. Sci., vol. 5, no. 4, pp. 34-39, Jul. 2021, doi: 10.24018/ejece.2021.5.4.339.
5. R. S. Rani, V. Manya, S. Parimi, and S. M. Nelavelli, "Optimizing attendance: Real-time mobile notifications through facial recognition with LBPH," in Proc. 2024 10th Int. Conf. Advanced Computing Commun. Syst. (ICACCS), Coimbatore, India, 2024, pp. 1-5.
6. A.Potdar, P. Barbhaya and S. Nagpure, "Face Recognition for Attendance System using CNN based Liveliness Detection," 2022 International Conference on Advances in Computing, Communication and Materials (ICACCM), Dehradun, India, 2022, pp. 1-6, doi: 10.1109/ICACCM56405.2022.10009024.
7. Varadannanavar, A. Nair, A. Kumar, P. K and A. R. Choudhury, "Automatic Attendance System Using Biometric Authentication and Varying QR Code," 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 2022,pp.24252429,doi:10.1109/ICAC3N56670.2022.10074099.
8. T. Singh, A. Chauhan, M. Dewan, and A. Agarwal, "IoT based digital attendance system using RFID and ESP32," Int. J. Mod. Trends Sci. Technol., vol. 8, no. 2, pp. 122-126, Feb. 2022.