

Smart Classroom Automation, Student Monitoring, and Secure Identity Management Using IoT and AI

Mr. Harish Kumar C R¹

*Assistant Professor,
Department of Electronics and
Communication Engineering,
Adichunchanagiri Institute of
Technology, Chikkamagaluru,
Karnataka, India*

Dr. Mahesh D S²

*Assistant Professor,
Department of Electronics and
Communication Engineering,
Adichunchanagiri Institute of
Technology, Chikkamagaluru,
Karnataka, India*

Preethi R Rathod³

*Student,
Department of Electronics and
Communication Engineering,
Adichunchanagiri Institute of
Technology, Chikkamagaluru,
Karnataka, India*

Spandana K G⁴

*Student,
Department of Electronics and
Communication Engineering,
Adichunchanagiri Institute of
Technology, Chikkamagaluru,
Karnataka, India*

Thrisha J B⁵

*Student,
Department of Electronics and
Communication Engineering,
Adichunchanagiri Institute of
Technology, Chikkamagaluru,
Karnataka, India*

Sudarshan D⁶

*Student,
Department of Electronics and
Communication Engineering,
Adichunchanagiri Institute of
Technology, Chikkamagaluru,
Karnataka, India*

Abstract—This paper presents a design framework for an integrated smart classroom that combines occupancy-based energy control, RFID door access, teacher-authorized fingerprint attendance, AI-assisted examination surveillance, secure student record retrieval, and GPS-based safety monitoring. An ESP32 handles local sensors and relay commands; a separate vision processor analyzes camera frames; and an authenticated backend provides role-limited dashboards for administrators, teachers, and parents. The proposed implementation enforces a configurable 5–10 min attendance window, duplicate rejection, time-stamped event logs, and geofence alerts based on fresh location fixes. A pin-level low-voltage circuit diagram and module workflow are provided, together with an end-to-end test protocol. The project quotation and associated technical report define proposed behavior but do not contain measured hardware trials. Consequently, this paper reports the implementation architecture and evaluation criteria rather than unverified performance figures.

Index Terms—Artificial intelligence, attendance, ESP32, fingerprint authentication, GPS, Internet of Things (IoT), RFID, smart classroom.

Date of Submission: 08-10-2026

Date of acceptance: 18-10-2026

I. INTRODUCTION

Classroom monitoring often depends on independent systems for attendance, lighting, access control, examination supervision, and student information. Manual registers increase administrative workload; unattended appliances waste energy; and separate platforms make it difficult to reconstruct a time-ordered classroom event. The project considered here integrates these functions through an IoT and web-based platform with local autonomy and centralized oversight [1], [2], [6], [7].

The design targets seven linked modules: (1) PIR-based light and fan operation; (2) RFID-controlled entry; (3) teacher-enabled fingerprint attendance; (4) camera-based suspicious-behavior flagging; (5) scanned student records with restricted access; (6) GPS tracking and geofencing; and (7) an administrator, teacher, and parent dashboard. The system is an engineering design, not a claim of completed deployment. Security and human review are treated as first-class requirements.

II. RELATED WORK

Zhao et al. explored an IoT classroom attendance architecture using RFID and facial recognition and identified environmental and interaction constraints [1]. Badmus et al. studied the use of fingerprint and RFID methods in a time-based attendance context [2]. Farag likewise investigated RFID-based school attendance and monitoring [5]. These studies support combining explicit authorization with event timestamps while avoiding assumptions that an RFID token alone establishes physical identity.

Kaddoura and Gumaï investigated deep-learning-based exam cheating detection [3]. Because a model-generated flag is not proof of misconduct, the present architecture treats candidate events as evidence requiring teacher review. Nguyen et al. examined ethical principles for educational AI [4]; those concerns motivate restricted footage access, retention limits, audit trails, and an appeal path for false alerts. This paper focuses on system integration rather than introducing a new recognition algorithm.

III. SYSTEM ARCHITECTURE

Fig. 1 shows three cooperating layers. The ESP32 samples the PIR motion sensor, scans the MFRC522 RFID reader, accepts messages from the fingerprint sensor over UART, reads GNSS sentences, and drives opto-isolated or properly interfaced relay inputs. Time-critical occupancy control continues locally when connectivity is temporarily lost. A camera is attached to a separate edge computer or approved video-processing host, avoiding unrealistic real-time video inference on the basic ESP32 controller. A backend API validates device messages, enforces roles, stores events and produces reports.

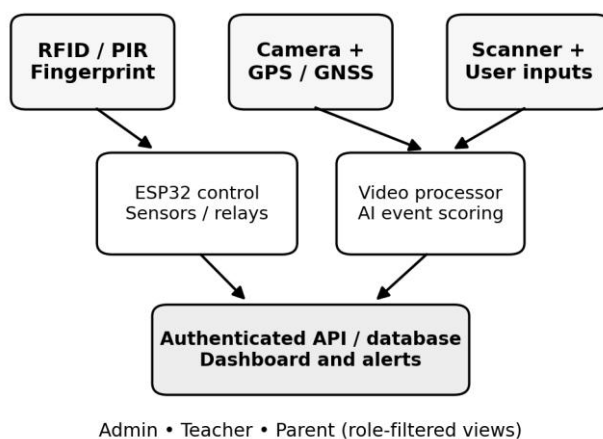


Fig. 1. Proposed integrated architecture and protected dashboard.

Teachers open attendance sessions for a configurable duration between five and ten minutes. Accepted check-ins are keyed by enrolled identity and session identifier so repeated scans do not create additional attendance. Parents receive only information associated with their children; administrative functions require elevated authorization. Scanned identity and academic documents are stored with explicit access controls, rather than exposed as public device database nodes.

Event and access-control model consists of minimal event record contains event_id, event_type, device_id, server_timestamp, actor_id where applicable, session_id, and a status code. Device-originated claims should be authenticated before the server commits them. Event identifiers provide idempotency when a temporary network outage causes retransmission; server-generated timestamps reduce reliance on unsynchronized board clocks. Attendance records form a unique combination of student_id and attendance_session_id, while access logs are retained separately from attendance to avoid inferring presence from a borrowed card.

Permissions are evaluated by the API on every read and write, even when the interface hides a feature. A teacher may inspect classes assigned to that role, a guardian may view only linked students, and a device account may append constrained telemetry but cannot retrieve identity documents. Sensitive uploaded files require encryption, recorded consent where applicable, short retention policies, and administrator-visible audit logs. This boundary is essential because a dashboard login alone is insufficient to prevent direct API access.

IV. HARDWARE DESIGN AND CIRCUIT

A. Embedded Interfaces

The reference controller is an ESP32 DevKit with a PIR HC-SR501-class sensor, MFRC522 RFID reader, UART fingerprint module (AS608/R307 class), GNSS receiver (NEO-6M class), and three control channels for room lights, fan and locking mechanism. The specific device variants and supply characteristics must be checked against actual module data sheets before assembly.

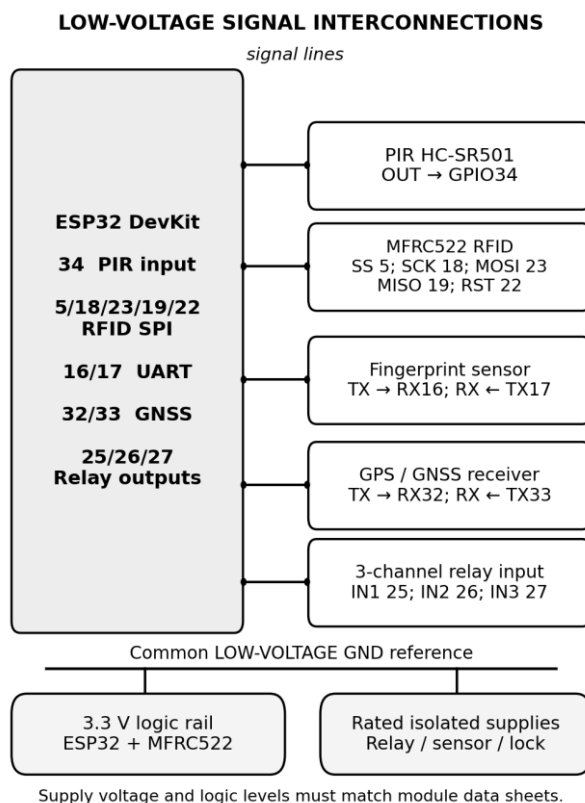


Fig. 2. Pin-level low-voltage signal connection diagram (proposed).

RFID is a 3.3 V SPI interface; its chip-select, clock, input, output and reset correspond to GPIO5, 18, 23, 19 and 22, respectively. PIR OUT connects to input-only GPIO34. Fingerprint TX/RX are crossed with GPIO16/17; GPS TX/RX connect to GPIO32/33. GPIO25, 26 and 27 command the light, fan and door relay channels, respectively. Ground references are shared only where required by the low-voltage interface and permitted by isolation design.

B. Driver and Power Safety

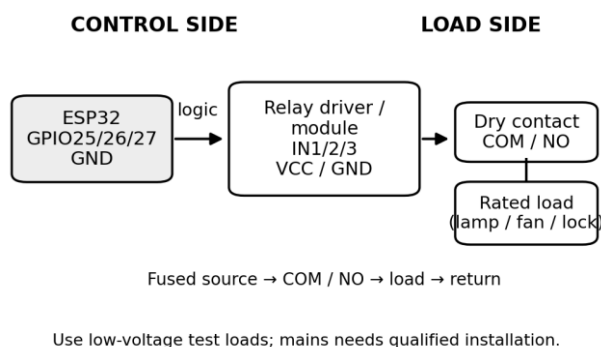


Fig. 3. Proposed isolated relay and separate load-power interface.

The contacts switch a separately fused, rated source for each load. The relay module must meet ESP32 logic-level and coil-current specifications; neither a motor nor an electric strike should be powered directly from a GPIO. Door release must provide code-compliant emergency egress. Fig. 3 is a safe functional wiring abstraction and not a certification-ready mains installation drawing.

C. Interface Validation and Fault Isolation

First validate each UART and SPI peripheral with other loads disconnected. Supply the RFID reader from a regulated 3.3 V rail and check card detection at more than one orientation. Set UART rates to the actual fingerprint and GNSS module configurations; use a logic-level translator when peripheral voltage limits differ. Relay input polarity depends on the selected module and must be determined before enabling an external supply. Check startup transients so lamps and the door strike do not activate during ESP32 boot.

The sensing/controller ground is a low-voltage reference, not a license to join mains wiring or defeat optocoupler isolation. Relays must be rated for motor inrush where fans are switched. Fuse, enclosure, surge protection, and thermal management should be specified after finalizing the load ratings. Where safety policy requires fail-safe or fail-secure door behavior, its choice must be reviewed independently of firmware and paired with mechanical emergency release.

V. SYSTEM WORKFLOW AND IMPLEMENTATION

At start-up, firmware configures safe relay states and initializes sensor buses. Each polling cycle updates room occupancy, checks known RFID credentials, and evaluates an attendance session. Presence requests appliance activation; prolonged inactivity returns the outputs to their configured idle states. Authorized entry issues a limited door release and logs an access event, while rejected cards generate an auditable denial. Teacher authentication enables the fingerprint acceptance interval; only an enrolled template not already used in that session creates a present record.

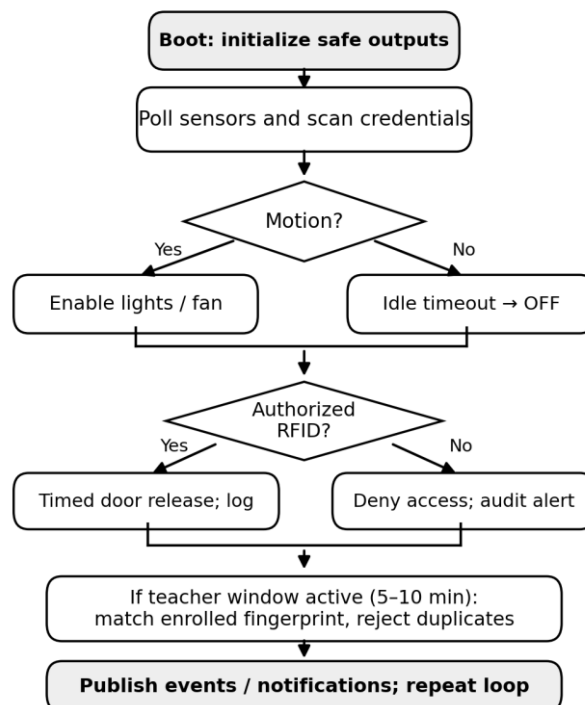


Fig. 4. Embedded access, occupancy and attendance workflow.

In parallel, the camera host samples exam video, detects candidate head turns or unusual movements and submits short reviewable events. Teacher assessment, rather than automatic punishment, determines the final interpretation. The GPS feed provides position, fix-age and quality indicators; boundary crossings are accepted only for fresh valid fixes and may be debounced to avoid edge jitter. The record service supports controlled scanning, indexing and retrieval of marksheets and identification documents.

A practical sequence is to enroll credentials, validate each sensor independently, connect the controller to an authenticated API, exercise relay channels with low-voltage test loads, configure roles, enable the camera service, and then validate GPS and notification integration. Server timestamps, reconnection events and dashboard read permissions should be logged throughout.

Event-Processing and notification logic consists of local firmware is best implemented as nonblocking periodic tasks or a single time-bounded state machine. Each PIR sample updates `last_motion_ms`. A relay state transition is emitted only when occupancy changes or the inactivity timeout expires, which avoids redundant network writes. RFID scans are compared with a revocable enrollment list; any temporary cached authorization must have a short lifetime. The attendance record is accepted only when the server or verified session command indicates an active teacher window.

Notifications are queued after the authoritative event is stored. Teachers can receive attendance summaries by email and guardians can receive approved mobile alerts; transmission failure should generate a retry record rather than duplicate attendance. GPS geofencing requires at least a valid coordinate and fix age. The school boundary may be represented by a radius or polygon, with hysteresis to reduce oscillation near the boundary. For examination monitoring, frames should be analyzed under a declared policy and candidate alerts sent for manual adjudication rather than automatic disciplinary action.

VI. EVALUATION METHODOLOGY

The supplied design report defines a twenty-scenario verification matrix but does not provide completed measurements, experimental photographs or repeatable accuracy statistics. Therefore the evaluation below specifies what must be measured before any quantitative results are claimed. Bench tests should capture board model, firmware revision, sensor supply, room conditions, enrolled card/fingerprint identifiers, network state, and time-stamped logs.

For energy automation, record device power under a baseline manual-control period and a comparable occupancy-control period. Savings must be derived from metered energy, $E = \text{integral of } P(t) \text{ over time}$; relay state alone is an insufficient measurement. For attendance, evaluate genuine enrollment matches, failed impostor attempts, duplicate rejection and expiration enforcement. For vision, measure precision, recall and F1 against a consented labeled dataset with human adjudication. For GPS, log location age, crossing delay and false geofence alarms over repeated trajectories.

Table I summarizes acceptance scenarios. Each row is a target test, not an observed success. Device restart, network loss, stale GNSS fixes, unauthorized document requests and emergency egress should be evaluated as negative or fault-injection cases.

1. Reproducible Metrics

Attendance acceptance rate is the ratio of correctly accepted authorized attempts to all authorized attempts. Rejection rate for unauthorized attempts, false attendance acceptance rate, and duplicate suppression must be reported separately because a high acceptance rate can coexist with a security defect. Let TP, FP, and FN denote correctly flagged, incorrectly flagged, and missed suspicious-event clips; AI precision = $TP/(TP+FP)$, recall = $TP/(TP+FN)$, and $F1 = 2TP/(2TP+FP+FN)$. A student-level claim requires per-subject train/test separation to prevent optimistic leakage.

The event-delay metric should be calculated from source activation to a synchronized server acknowledgment, with medians and upper-percentile delays over multiple trials. Power is measured with a suitable calibrated meter and compared under comparable occupancy patterns; an ON/OFF log cannot replace physical energy readings. To assess geofencing, perform repeated controlled inside-to-outside and outside-to-inside traversals and record valid-fix age, alert latency and spurious transitions. No metric should be filled in using assumed rather than logged readings.

Trials should be repeated for multiple users and different environments: an empty room, a classroom with stationary occupants, a crowded entry, normal examination behavior, and artificially simulated device faults. Class enrollment files must be separated from camera-test labels to preserve evaluation independence. The protocol must record the number of trials and confidence intervals or variability, not a single best-case demonstration. A successful test requires matching records in device logs, the backend audit trail, and the authorized dashboard; mismatches should be investigated as possible message loss or inconsistent identity mapping.

A controlled comparison is recommended for each module. For lighting, compare equivalent hours and occupancy patterns under manual and automated control. For RFID, test enrolled, revoked, unreadable and duplicated credentials. For fingerprint attendance, test repeated scans, closed-window scans and teacher-session restart. For exam AI, preserve only consented evaluation clips and make a clear separation between detecting an unusual movement and identifying academic dishonesty. For GPS, test a geofence on open ground with clear satellite reception before attempting operation near buildings or indoors.

Table I summarizes acceptance scenarios. Each row is a target test, not an observed success. Device restart, network loss, stale GNSS fixes, unauthorized document requests and emergency egress should be evaluated as negative or fault-injection cases.

TABLE I
PLANNED VERIFICATION TESTS (NO MEASURED RESULTS PROVIDED)

Subsystem	Verification condition
Energy	PIR event $\rightarrow$ commanded ON; timeout $\rightarrow$ OFF
Access	Known RFID accepted; unknown tag denied
Attendance	Teacher window 15 min; duplicate rejected
Exam AI	Flag review + precision / recall reporting
GPS safety	Fresh fixes + repeatable boundary alerts

Record access	Teacher authorized; unrelated user denied
Resilience	Offline occupancy operation; safe power recovery

VII. RESULTS AND DISCUSSION

The architectural outcome is an implementable separation of low-power classroom control, compute-intensive vision, and sensitive cloud records. The controller can maintain room automation without waiting for video inference or dashboard refresh. Fingerprint check-ins can be tied to teacher-authorized sessions; server-side role checks can restrict student data. These are design properties, not experimentally confirmed operating results.

Quantitative claims about reduced energy use, biometric success rate, false AI alerts, GPS accuracy, message delivery, or system latency remain pending instrumented prototype testing. Engineering limitations include PIR blind spots, lost or shared RFID tags, enrollment errors, occluded cameras, GPS indoor weakness, and unstable networking. Using local timeouts, device authentication, stale-fix filtering, configurable review thresholds and audited access mitigates—but does not remove—these risks.

1. Integration Trade-offs

A shared dashboard improves traceability but also concentrates sensitive information. Therefore device-event ingestion and human record access should use distinct authorizations and retention periods. A single PIR sensor is inexpensive yet may fail to detect stationary occupants, so occupancy timeout selection trades energy savings against nuisance shutoff. Likewise, shorter geofence hysteresis improves detection speed at the cost of more boundary jitter, while stricter AI thresholds reduce false alarms but may miss true events.

Field deployment must also address consent and legal requirements when working with minors, biometrics and examination footage. Biometrics should be handled as protected templates rather than raw publicly readable images; GNSS tracking requires clear scope and authorization. Before installation, qualified personnel should assess electrical isolation, egress behavior and physical failure modes. These requirements explain why architecture-level feasibility cannot be treated as equivalent to successful deployment.

VIII. CONCLUSION AND FUTURE SCOPE

A consolidated smart classroom system has been specified using an ESP32-based access and occupancy controller, a separate AI video host, a GPS safety subsystem and a role-protected dashboard. The accompanying flowchart and pin-level circuit provide a reproducible starting point for a prototype. Future work should include physical integration, security and egress inspection, controlled user trials, comparative power metering, AI model calibration, privacy review, and publication of measured validation data. No numerical prototype performance is asserted before those trials are completed.

REFERENCES

- [1] M. Zhao, G. Zhao, and M. Qu, "College Smart Classroom Attendance Management System Based on Internet of Things," *Computational Intelligence and Neuroscience*, vol. 2022, Art. no. 4953721, 2022, doi: 10.1155/2022/4953721.
- [2] E. O. Badmus, O. P. Odekunle, and D. O. Oyewobi, "Smart Fingerprint Biometric and RFID Time-Based Attendance Management System," *European Journal of Electrical Engineering and Computer Science*, vol. 5, no. 4, 2021, doi: 10.24018/ejece.2021.5.4.339.
- [3] S. Kaddoura and A. Gumaï, "Towards effective and efficient online exam systems using deep learning-based cheating detection approach," *Intelligent Systems with Applications*, vol. 16, Art. no. 200153, 2022, doi: 10.1016/j.iswa.2022.200153.
- [4] A. Nguyen, H. N. Ngo, Y. Hong, B. Dang, and B.-P. T. Nguyen, "Ethical principles for artificial intelligence in education," *Education and Information Technologies*, vol. 28, pp. 4221–4241, 2023, doi: 10.1007/s10639-022-11316-w.
- [5] W. A. Farag, "An RFID-based smart school attendance and monitoring system," *BOHR Journal of Computational Intelligence and Communication Network*, vol. 1, no. 1, pp. 26–34, 2023, doi: 10.54646/bjcicn.2023.05.
- [6] Spherenex Innovation Labs, "Smart Classroom Automation, Student Monitoring, and Secure Identity Management System Using IoT and AI," project quotation KS5394, 28 Mar. 2026, pp. 1–9 (supplied as "KS5526 (2).pdf").
- [7] "Smart Classroom Automation, Student Monitoring, and Secure Identity Management Using IoT and AI," accompanying final project report, supplied manuscript, 2026.