Identified Issues

Attendance Integrity

- Attendance is inferred from momentary Wi-Fi association rather than sustained presence, enabling short-duration presence gaming.
- There is no binding between a device and a physical individual, making proxy attendance trivial.
- Legitimate attendees may be marked absent due to Wi-Fi being disabled, cellular data usage, intermittent connectivity, power-saving modes, or device sleep states.
- No fallback or manual verification mechanism is defined.

Privacy and Security

- Data protection mechanisms are undocumented, including hashing salting, encryption key management, and cryptographic standards.
- There is no explicit user consent framework covering data scope, retention, or withdrawal.
- Role-based access control, access logging, and audit trails are unspecified, increasing insider-risk exposure.

Localization and Access Point Accuracy

- Claimed localization accuracy conflicts with real access point coverage, creating ambiguity at signal boundaries.
- Signal attenuation due to walls and obstructions is not modeled.
- Devices may remain associated with adjacent access points despite physical movement, leading to systematic room-level misattribution.

Schedule and Venue Dynamics

- No clear mechanism exists for handling venue changes, rescheduled classes, or emergency room reassignments.
- Temporal binding between course schedules and access points is unclear and appears manually managed.

Spatial Modeling Gaps

- There is no documented spatial database capturing access point coordinates, effective range, obstruction profiles, or adjacency relationships.
- Obstruction-aware propagation models are absent, despite known corridor and wall effects.
- Semester-specific course–time–AP mappings are not formally defined, despite being foundational.

Network Reliability

- The system relies on UDP-based SNMP traps without acknowledgment, making it vulnerable to packet loss during peak load.
- Throughput limits, ingestion capacity, and database saturation thresholds are undocumented and untested.

Transparency and Trust

- Students and faculty lack structured attendance reporting and discrepancy resolution workflows.

- Real-time attendance visibility risks enabling system gaming; mitigation strategies are not formalized.

Multi-Device Handling

- Users carrying multiple devices may be double-counted or inconsistently marked.
- Device clustering, identity resolution, and dynamic device registration are undefined.

Power Management Constraints

- Battery saver modes and Wi-Fi sleep policies can suppress background connectivity, increasing false negatives.
- No mitigation strategy or grace window is specified.

Infrastructure Documentation

- Network architecture, access point hardware details, SNMP configurations, and controller settings are undocumented.
- Absence of these details prevents reproducibility and troubleshooting.
- Need to obtain this information from the IT Department.

Accessibility and Equity

- The system assumes universal access to authenticated institutional Wi-Fi.
- Guest networks, incompatible devices, and authentication failures are not accommodated, excluding a subset of users.

Temporal Granularity

- Attendance is binary, with no entry/exit timestamps or duration tracking.
- Late arrivals, early departures, and partial attendance cannot be evaluated.

Irregular Academic Patterns

- Semester breaks, exams, events, holidays, and irregular schedules are not explicitly handled.
- Occupancy volatility is not modeled or adapted to.

Code and Reproducibility

- No source code, deployment artifacts, or demo environment is available.
- This prevents independent validation, auditing, or extension.

Monitoring and Operations

- Attendance is logged but not actively monitored.
- There is no real-time system health visibility, anomaly detection, or alerting.
- Attendance dispute resolution workflows are undefined.

Target User Ambiguity

- The system appears TA-centric, with unclear scalability or suitability for full student deployment.
- Multiple competing use cases are implied without a clearly defined primary objective.

Auditability and Compliance

- Data provenance is missing for attendance edits, overrides, and configuration changes.
- Compliance requirements (FERPA/GDPR-style access, correction, deletion, and audit logging) are not addressed.

Possible Solutions and Mitigations

Instructor-assisted multi-factor verification, enabling:

- Manual confirmation by the instructor for students present but incorrectly marked absent (e.g., device detected for only 30 minutes in a 90-minute class).
- Optional instructor-issued passcode announced in class to act as a second factor for attendance validation.
- Targeted roll call restricted to only those students not yet confirmed by the automated system.

Duration-based attendance validation, e.g., attendance marked only if cumulative non-overlapping presence ≥45 minutes for a 90-minute class.

Periodic presence re-verification instead of single-point Wi-Fi association.

Identity-level attendance tracking, aggregating all user devices under a single user identity.

Multi-device union logic, e.g., Phone (9:00–9:30) + Laptop (9:25–10:15) → 75 minutes total presence.

Digitized semester timetable database, binding courses to time slots and venues.

Course–Time–AP mapping table, for example:

```
Spring24 | CS101 | Mon 9–10 | Valid APs: [C21, C22] | Primary: C22 | Backup: C21
```

Access point spatial metadata store, including AP ID, building, floor, room association, effective radius, obstruction level (high/medium/low), and adjacent AP list.

RSSI-based eligibility thresholds and controlled handoff logic to reduce adjacent-room misattribution (e.g., preventing C21 association from marking presence in a C22 session).

Grace periods for intermittent connectivity, covering brief disconnects due to battery saver modes, Wi-Fi sleep, or transient network issues.

Delayed attendance visibility, showing final status only after session completion to reduce system gaming.

Optional per-course attendance dashboards for students and faculty with discrepancy reporting and justification logging.

Role-Based Access Control (RBAC), for example:

- Students: view own attendance
- Faculty: view, verify, and override class attendance with justification
- Administrators: manage mappings, schedules, and audits

Per-metric Access Control Lists (ACLs) controlling read/write/override permissions on attendance records.

Comprehensive audit logging, capturing original values, overrides, timestamps, and actor identity.

Entry and exit timestamp logging to support late arrival, early departure, and duration-based evaluation.

UDP loss mitigation, via acknowledgment-capable traps or redundant listeners to prevent missed attendance during peak load.

Database-level gap detection, flagging missing or inconsistent attendance events during expected high-activity periods.

Guest-network and non-Wi-Fi user handling, through controlled manual or alternative verification pathways.

Operational monitoring, including AP health, trap ingestion rate, processing latency, and anomaly alerts.