iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VIII **Month of publication:** August 2026

DOI: https://doi.org/10.22214/ijraset.2026.84589

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VIII Aug 2026- Available at www.ijraset.com

SmartAICampus: An Anti-Proxy Attendance System using Rotating QR, Bluetooth Proximity and Device-Lock

Perseus Bhavnagri
Student, Wilson College (Autonomous), Mumbai, University of Mumbai

Abstract: ***Institutional attendance underpins academic eligibility and statutory reporting, yet it remains easy to falsify. Manual roll-call, static QR codes and simple check-in apps are all defeated by proxy ("buddy") attendance, and increasingly by remote relay, in which an absent student is marked present over a video call. This paper presents SmartAICampus, a multi-tenant campus operations platform whose core contribution is an anti-proxy attendance mechanism that composes three independent locks: a rotating time-based one-time password (TOTP) QR code, short-range Bluetooth Low Energy (BLE) proximity between the student and the teacher's device, and a device-lock that binds each student to a single enrolled phone. The system follows a thin-client, fat-backend design on Firebase, with sensitive logic in Cloud Functions, role-based access enforced through custom claims, and per-institute data isolation. The work is assessed through Design Science Research: a matrix of 22 functional test cases, a catalogue of 12 proxy-attack simulations, and a micro-benchmark of the cryptographic scan path. Eleven of twelve attacks are blocked, the verification path costs under 0.1 ms per scan, and an automated suite of 146 tests passes. The findings support the claim that layering cheap, independent signals defeats proxy attendance that any single signal permits — while honestly bounding one residual attack and projecting, rather than load-testing, scale to institute size.***
Keywords: Proxy attendance; anti-proxy; rotating QR; TOTP; Bluetooth Low Energy proximity; device binding; multi-tenant SaaS; Firebase Cloud Functions; role-based access control; Design Science Research.

I. INTRODUCTION

Attendance is a statutory and academic obligation in Indian higher education. Universities commonly require students to attend at least 75% of lectures in each subject to sit examinations, and institutions must report attendance for audits, scholarships and regulatory compliance. Because so much depends on the record, there is a strong incentive to falsify it — and the tools used to capture attendance have not kept pace with the ways students defeat them.

1) Proxy attendance: The central threat is proxy, or "buddy," attendance: a present student marks an absent friend. Manual roll-call falls to a friend answering in a student's place; a fixed or printed QR code is easily snapped and sent to someone off-site; and a basic check-in app can be opened from any location. The problem has sharpened with remote relay, where an absent student joins a video call and a friend in the room points the camera at the code, so the mark is captured from outside the room entirely. Single-signal systems cannot separate these cases, because each rests on one piece of evidence that is easy to copy or move.

2) A layered, on-device approach: SmartAICampus requires three independent signals at the moment of marking, each cheap to produce but hard to forge together: a rotating time-based one-time password (TOTP) inside a QR code that changes every few seconds; short-range Bluetooth Low Energy (BLE) proximity confirming the student's phone is physically near the teacher's device; and a device-lock binding each account to one enrolled handset. Sensitive checks run in the backend (Firebase Cloud Functions), not on the phone, so rules can be corrected or tightened by a server deployment without waiting for an app-store release.

3) Problem statement and need for the study: Existing methods optimise for convenience and record a single, copyable signal; they therefore admit proxy attendance, and now remote relay, at scale. There is a need for an attendance mechanism that resists these attacks while remaining practical on ordinary student phones and workable for institutions of several thousand students.

4) Need for the Study: This study is undertaken to —

- characterise how existing methods (manual, static QR, single-app, biometric/RFID, GPS/geofence) fail against proxy and remote-relay attacks;
- design a mechanism that composes rotating QR, BLE proximity and device-lock so that defeating it requires defeating all three at once;

- evaluate that mechanism against a catalogue of proxy attacks plus functional and performance tests, using the built system's own evidence;
- report honestly on its boundaries — the attacks it does not stop, and the scale it projects to but has not yet load-tested.

II. LITERATURE REVIEW

Research on automated attendance has largely pursued a single distinguishing signal, and each family of work trades one weakness for another.

Biometric systems tie attendance to a physical trait rather than a token. Josphineleela and Ramakrishnan [11] built a fingerprint-based classroom system using a fingerprint-reconstruction technique, Bhatti et al. [5] developed a camera-based facial-recognition attendance system, and Patel et al. [19] applied deep-learning face recognition to existing classroom CCTV feeds. Biometrics identify a person directly, but they demand dedicated sensors or good cameras, raise privacy and consent concerns over storing templates — often for minors — and slow a large class in which students enrol and match one at a time.

Token- and card-based systems identify the student through something they carry. Rjeib et al. [22] and Arulogun et al. [1] used RFID cards to log attendance automatically, Irawan et al. [10] extended the idea with an IoT-connected reader that streams records to the cloud, and Ayu and Ahmad [3] used a Near-Field-Communication tap on the student's own phone. Such systems are fast and inexpensive, but they authenticate the card or tag, not the student — a token handed to a friend marks its owner present, which is precisely the proxy problem.

QR-code systems are the closest to the present work. Masalha and Hirzallah [15] proposed a system in which the class scans a displayed code. Because a static code is merely data that can be photographed and forwarded, later designs bind the code to context: Taju et al. [24] bound each scan to the student's GPS geolocation; Imanullah and Reswan [9] randomised the displayed code on every scan so a captured image is worthless to anyone else; and Nwabuwe et al. [18] combined a dynamic code with a geofence and the phone's IMEI device identifier. These measures raise the bar, yet a code displayed to a live video call can still be relayed to someone outside the room.

Proximity- and location-based signals try to prove physical presence. Kriz et al. [13] and Zhuang et al. [26] characterised indoor positioning with Bluetooth Low Energy beacons, and Puckdeevongs et al. [21] allowed a mark only when the student's phone was located inside the classroom by BLE indoor positioning — a short-range signal a video relay cannot carry. Location schemes based on GPS are weaker: Tippenhauer et al. [25] demonstrated that GPS can be spoofed, which undermines the geofenced check-in of Fernandez et al. [7]; to compensate, Ayop et al. [2] combined a QR scan with GPS and Soewito and Simanjuntak [23] fused GPS with an on-device biometric check, while Khan et al. [12] inferred presence from institutional Wi-Fi signal strength. Proximity is a valuable ingredient, but a lone check can be relayed and GPS can be faked outright.

A few studies look beyond a single signal. Labayen et al. [14] combined multimodal biometrics to authenticate students and detect impersonation during remote assessment, and Nguyen et al. [17] proposed a three-layer Internet-of-Things and cloud framework for contactless attendance at scale. These works confirm the direction of travel — combine signals and move the decision to the server — but stop short of compelling a proxy to defeat liveness, proximity and identity at the same instant of marking.

Because the platform serves many institutions from one codebase, it also inherits the concerns of multi-tenant software. Bezemer and Zaidman [4] discussed how multi-tenancy affects maintainability and isolation, motivating the strict per-tenant data separation adopted here.

III. GAP ANALYSIS

Across these strands each system leans on one signal — a fingerprint, a card, a code, or a location — so an attacker who defeats that single signal defeats attendance. None combines independent, mutually reinforcing signals such that a proxy would have to satisfy all of them at the same instant, and none specifically addresses remote-relay attendance, where marking happens over a video call from outside the classroom. The gap this work targets is a mechanism that (a) makes the code un-replayable by rotating it every few seconds, (b) requires short-range BLE proximity to the teacher's device so a relayed or off-campus scan fails, and (c) binds each student to one enrolled phone so a single present device cannot mark many absentees — all within a multi-tenant architecture that keeps each institution's data isolated.

IV. OBJECTIVES, VARIABLES AND HYPOTHESIS

A. Objectives

This study aims to —

- design an attendance mechanism that composes three independent signals — a rotating TOTP QR code, BLE proximity, and a device-lock — so that proxy and remote-relay marking are prevented;
- implement it as a thin-client, fat-backend system on Firebase, with per-institute data isolation and role-based access control;
- evaluate its resistance against a catalogue of proxy attacks and its correctness against a matrix of functional test cases;
- measure the overhead the verification path adds to the marking process;
- assess, and honestly bound, the mechanism's limitations and its scalability toward institute size.

B. Variables

As this is a system evaluation, the variables are properties of the mechanism, not of a sampled population:

TABLE I
STUDY VARIABLES

Dependent (observed) variables	Independent variable
(i) Attack outcome — blocked or admitted	The marking configuration: whether an attempt must satisfy all three signals together (the composed system) or any single signal alone (the single-signal baselines drawn from the literature).
(ii) Functional correctness — pass or fail against each test case	
(iii) Verification latency — the time to validate a scan	
(iv) Tenant isolation — whether one institution's data can be reached from another	

C. Hypotheses

The evaluation is organised around three claims, each judged against a pre-stated acceptance criterion (not a statistical p-value, since the system is deterministic):

H1. Requiring three independent signals at marking time prevents the proxy and remote-relay attendance that any single signal permits.

H2. The added verification imposes negligible overhead on the marking process.

H3. The architecture enforces per-institute isolation and can scale toward institute size (~10,000 students) on commodity infrastructure.

V. METHODOLOGY

A. Research Design

This work follows Design Science Research [8], [20], in which knowledge is produced by building and rigorously evaluating an artefact — here, the anti-proxy attendance mechanism. The study is applied and evaluative: it does not test statistical hypotheses about a population. The evidence is technical and self-generated — it comes from exercising the built system, not from an external dataset. The artefact was implemented as a cross-platform Flutter application backed by Firebase Cloud Functions (region asia-south1), Firestore, Authentication, Cloud Messaging and App Check, with all sensitive checks on the server. Its marking mechanism combines a rotating time-based one-time password [16], short-range Bluetooth Low Energy proximity [6], and a device-lock that binds each account to one enrolled handset.

B. Data Collection

Evidence was collected by running the system under three regimes: (i) functional testing, in which each required behaviour was exercised by an automated test case; (ii) adversarial testing, in which a catalogue of proxy and remote-relay attacks was simulated against the marking flow; and (iii) performance measurement, in which the cryptographic verification path was micro-benchmarked. For each trial the recorded outcome was, respectively, pass/fail, blocked/admitted, and elapsed time. A defect log was also drawn from the project's version history to gauge how maintainable the thin-client design proved in practice.

C. Sample Size

Because the artefact is deterministic, a marking attempt either satisfies the required signals or it does not; there is no sampling variability, so a statistical sample-size calculation (for example, Cochran's formula) does not apply. In its place the evaluation uses a fixed corpus: 22 functional test cases, 12 attack scenarios, an automated regression suite of 146 tests (84 backend and 62 client), and a micro-benchmark averaged over repeated iterations of the verification helpers. Each case is a definitive trial rather than a draw from a population.

VI. DATA ANALYSIS AND FINDINGS

A. Description of the data set.

The evaluation data are the outcomes produced by the built system itself, not an external corpus: the pass/fail results of 22 functional test cases, the blocked/admitted results of 12 proxy-attack simulations, the pass count of a 146-test automated suite, and timing samples from a micro-benchmark of the verification path. All values reported below are measured on the running system.

1) Numerical Summary

TABLE II
NUMERICAL SUMMARY OF RESULTS

Measure	**Result**
Functional test cases (TC-01 – TC-22)	22 defined; all pass
Automated regression suite	146 tests pass (84 backend, 62 client)
Static analysis	flutter analyze: 0 issues; ESLint and tsc: clean
Proxy-attack scenarios (AT-01 – AT-12)	12 simulated; 11 blocked, 1 not prevented
Verification-path latency	< 0.1 ms per scan
Defects logged (version history)	9; 6 resolved by a backend deploy alone

2) Attacks by Defence Layer

TABLE III
ATTACKS BLOCKED, BY DEFENCE LAYER

Defence layer	Attacks blocked
Rotating TOTP QR code	1
BLE proximity	3
Device-lock	2
Server-side gates	2
Security rules	3
Not prevented (AT-12: handover of the enrolled phone)	0

Eleven of the twelve attacks are blocked. The single exception, AT-12, is a student physically handing over their enrolled, unlocked phone; no on-device signal can distinguish this from genuine presence.

3) Verification Performance (Apple M1 Pro, Node 24)

TABLE IV
VERIFICATION PERFORMANCE (APPLE M1 PRO, NODE 24)

Operation	Time
QR-code verification (typical)	23.2 µs
QR-code verification (worst case)	34.6 µs
BLE token verification	27.9 – 41.3 µs
QR token batch generation	88.9 µs
Whole cryptographic path	< 0.1 ms per scan

Hypothesis 1: Requiring three independent signals prevents proxy and remote-relay attendance that any single signal permits.

TABLE V
EVALUATION OF HYPOTHESIS H1

Hypothesis	Evaluation method	Observed result	Decision
H1	12 proxy / remote-relay attack simulations, against the criterion "no attack admits a proxy"	11 of 12 blocked; only AT-12 (handover of the enrolled phone) admits	Supported, with one bounded exception

Hypothesis 2: The added verification imposes negligible overhead on marking.

TABLE VI
EVALUATION OF HYPOTHESIS H2

Hypothesis	Evaluation method	Observed result	Decision
H2	Micro-benchmark of the verification path, against the criterion "overhead negligible within the marking window"	< 0.1 ms per scan — orders of magnitude below the rotation window	Supported in mechanism (live classroom timing not measured)

Hypothesis 3: The architecture enforces per-institute isolation and scales toward institute size.

TABLE VII
EVALUATION OF HYPOTHESIS H3

Hypothesis	Evaluation method	Observed result	Decision
H3	Analysis of tenant isolation plus a load projection from measured per-scan cost, against "isolation holds and scales to ~10,000"	Isolation enforced by security rules; capacity projected, not load-tested at 10,000	Supported in part (scale projected, not demonstrated)

VII. RESULT

1) H1 is supported. Layering three independent signals blocks every simulated proxy and remote-relay attack except AT-12, in which a student physically hands over their enrolled, unlocked phone — an act no on-device signal can distinguish from genuine presence, and one better addressed by invigilation policy than by the app.

2) H2 is supported in mechanism. The cryptographic verification adds well under a millisecond per scan, negligible against the seconds-long marking window; however, end-to-end timing in a live classroom, under real network and camera conditions, was not measured.

3) H3 is supported in part. Per-institute isolation is enforced architecturally by the security rules, and the measured per-scan cost implies ample headroom, but scale to roughly 10,000 students is projected from unit costs rather than demonstrated by a load test.

VIII. RECOMMENDATIONS BASED ON STUDY

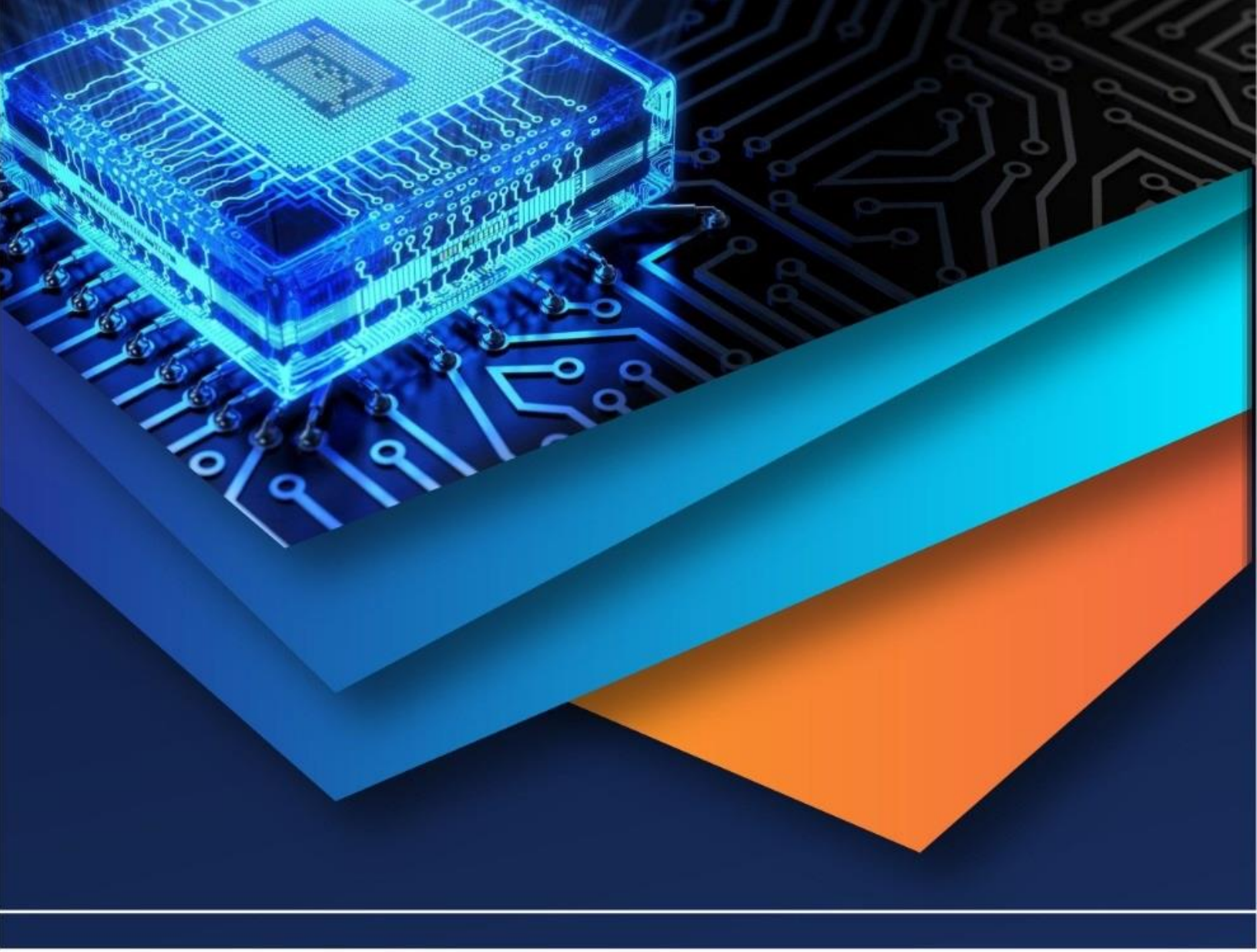
- run a load test at institute scale (~10,000 concurrent marks) to turn H3's projection into a measurement;
- conduct a full-semester field deployment to capture real classroom timing for H2 and gather usability feedback;
- add a fourth, harder-to-relay signal or an invigilation control to close the AT-12 handover gap;
- add an emulator-based security-rules regression suite and rate-limiting on the callable functions;
- widen the tested device matrix and commission an independent penetration test before large-scale rollout.

IX. CONCLUSION

SmartAICampus shows that composing cheap, independent signals — a rotating QR code, BLE proximity and a device-lock — defeats the proxy and remote-relay attendance that any single signal permits, within a maintainable, multi-tenant Firebase architecture that keeps each institution's data isolated. Evaluated as Design Science Research on the built system, the mechanism blocks eleven of twelve simulated attacks at under 0.1 ms of verification cost per scan, while honestly bounding the one residual attack and projecting — rather than load-testing — scale to institute size. Beyond the artefact, the study contributes a reusable evaluation frame — a functional test matrix, an attack catalogue and a small set of performance metrics — that other anti-proxy attendance systems can adopt.

REFERENCES

[1] O. T. Arulogun, A. Olatunbosun, O. A. Fakolujo, and O. M. Olaniyi, "RFID-based students attendance management system," International Journal of Scientific & Engineering Research, vol. 4, no. 2, 2013.
[2] Z. Ayop, Y. L. Chan, S. Anawar, E. Hamid, and M. S. Azhar, "Location-aware event attendance system using QR code and GPS technology," International Journal of Advanced Computer Science and Applications, vol. 9, no. 9, 2018.
[3] M. A. Ayu and B. I. Ahmad, "TouchIn: An NFC supported attendance system in a university environment," International Journal of Information and Education Technology, vol. 4, no. 5, pp. 448–453, 2014.
[4] C.-P. Bezemer and A. Zaidman, "Multi-tenant SaaS applications: Maintenance dream or nightmare?" in Proc. Joint ERCIM Workshop on Software Evolution (EVOL) and Int. Workshop on Principles of Software Evolution (IWPSE), 2010, pp. 88–92.
[5] K. L. Bhatti, L. Mughal, F. Y. Khuhawar, and S. A. Memon, "Smart attendance management system using face recognition," EAI Endorsed Transactions on Creative Technologies, vol. 5, no. 17, art. 159713, 2018.
[6] Bluetooth SIG, "Bluetooth core specification, version 5.4," Bluetooth Special Interest Group, 2023.
[7] J. R. Fernandez, H. Mamarungkas, S. Vinson, and K. Atuel, "Facial and geofencing-based attendance tracking system for deployed personnel," Mindanao Journal of Science and Technology, vol. 23, no. 2, pp. 133–148, 2025.
[8] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," MIS Quarterly, vol. 28, no. 1, pp. 75–105, 2004.
[9] M. Imanullah and Y. Reswan, "Randomized QR-code scanning for a low-cost secured attendance system," International Journal of Electrical and Computer Engineering, vol. 12, no. 4, pp. 3762–3769, 2022.
[10] J. D. Irawan, E. Adriantantri, and A. Farid, "RFID and IoT for attendance monitoring system," MATEC Web of Conferences, vol. 164, art. 01020, 2018.
[11] R. Josphineleela and M. Ramakrishnan, "An efficient automatic attendance system using fingerprint reconstruction technique," International Journal of Computer Science and Information Security, vol. 10, no. 3, 2012.
[12] S. M. Khan, M. T. Maliha, M. S. Haque, and A. Rahman, "WiFi received signal strength (RSS) based automated attendance system for educational institutions," in Proc. 11th Int. Conf. on Networking, Systems, and Security (NSysS), 2024.
[13] P. Kriz, F. Maly, and T. Kozel, "Improving indoor localization using Bluetooth Low Energy beacons," Mobile Information Systems, vol. 2016, art. 2083094, 2016.
[14] M. Labayen, R. Vea, J. Florez, N. Aginako, and B. Sierra, "Online student authentication and proctoring system based on multimodal biometrics technology," IEEE Access, vol. 9, pp. 72398–72411, 2021.
[15] F. Masalha and N. Hirzallah, "A students attendance system using QR code," International Journal of Advanced Computer Science and Applications, vol. 5, no. 3, pp. 75–79, 2014.
[16] D. M'Raihi, S. Machani, M. Pei, and J. Rydell, "TOTP: Time-based one-time password algorithm," Internet Engineering Task Force, RFC 6238, 2011.
[17] V. D. Nguyen, H. Van Khoa, T. N. Kieu, and E.-N. Huh, "Internet of Things-based intelligent attendance system: Framework, practice implementation, and application," Electronics, vol. 11, no. 19, art. 3151, 2022.
[18] A. Nwabuwe, B. Sanghera, T. Alade, and F. Olajide, "Fraud mitigation in attendance monitoring systems using dynamic QR code, geofencing and IMEI technologies," International Journal of Advanced Computer Science and Applications, vol. 14, no. 4, 2023.
[19] J. Patel, S. Gandhi, V. Katheriya, P. Pataliya, and A. Majumdar, "Enhancing classroom attendance systems with face recognition through CCTV using deep learning," Procedia Computer Science, vol. 258, pp. 3031–3041, 2025.
[20] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," Journal of Management Information Systems, vol. 24, no. 3, pp. 45–77, 2007.
[21] A. Puckdeevongs, N. K. Tripathi, A. Witayangkurn, and P. Saengudomlert, "Classroom attendance systems based on Bluetooth Low Energy indoor positioning technology for smart campus," Information, vol. 11, no. 6, art. 329, 2020.
[22] H. D. Rjeib, N. S. Ali, A. Al Farawn, B. Al-Sadawi, and H. Alsharqi, "Attendance and information system using RFID and web-based application for academic sector," International Journal of Advanced Computer Science and Applications, vol. 9, no. 1, pp. 266–274, 2018.
[23] B. Soewito and E. W. M. Simanjuntak, "Efficiency optimization of attendance system with GPS and biometric method using mobile devices," CommIT (Communication and Information Technology) Journal, vol. 8, no. 1, pp. 5–9, 2014.
[24] S. W. Taju, Y. P. Mamahit, and J. A. Pongantung, "Implementing QR code and geolocation technologies for the student attendance system," CogITo Smart Journal, vol. 10, no. 1, pp. 221–232, 2024.
[25] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Čapkun, "On the requirements for successful GPS spoofing attacks," in Proc. ACM Conf. on Computer and Communications Security (CCS), 2011, pp. 75–86.
[26] Y. Zhuang, J. Yang, Y. Li, L. Qi, and N. El-Sheimy, "Smartphone-based indoor localization with Bluetooth Low Energy beacons," Sensors, vol. 16, no. 5, art. 596, 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY