International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN (Online): 2347-5552, Volume-14, Issue-5, Sep-Oct 2026
DOI: https://doi.org/10.55524/ijircst.2026.14.5.6
Article ID IRP-1788, Pages 48-54
www.ijircst.org

A Multi-Factor Zero-Trust Framework for Anti-Proxy Attendance Verification in Educational Institutions

Akash Sahu[1], Kanchan[2], and *Yojna Arora[3]

[1, 3] Department of Computer Science & Engineering, Sharda University, Greater Noida, Uttar Pradesh, India
[2] Department of Computer Applications, Axis Institute of Higher Education, Kanpur, Uttar Pradesh, India

Correspondence should be addressed to *Yojna Arora; yojana183@gmail.com

Received: 2 Sep 2026; **Revised:** 17 Sep 2026; **Accepted:** 30 Sep 2026; **Published Online:** 12 Oct 2026

Copyright © 2026 *Yojna Arora et al. This is an open-access article distributed under the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ABSTRACT- Proxy attendance, whereby attendance is recorded for a student who is absent, continues to pose a problem in higher education institutions, since single-factor verification methods like static QR codes, RFID cards, and GPS-only location checks each have a well-documented, low-effort way of being circumvented. Although more recent multi-factor methods that combine QR codes, facial recognition, and GPS-based geofencing have improved on the single-factor approaches, they still depend on satellite-based location verification, which suffers from considerable degradation in accuracy in indoor, multi-storey classroom settings, and generally assess the various factors together using a strict conjunctive policy without taking into account the increased false-rejection rate that this causes for students who are truly present. The present paper puts forward a multi-factor, zero-trust attendance verification framework that replaces GPS-based geofencing with ad-hoc Bluetooth Low Energy (BLE) proximity detection broadcasts sent from the instructor's own smartphone, thus getting rid of both the indoor accuracy problems associated with GPS and the need for dedicated beacon hardware that is required by fixed-infrastructure BLE systems. The framework also combines a quickly rotating cryptographically-signed QR token with an on-device face-liveness check and includes persistent device-hardware binding, and introduces a weighted-confidence fusion policy which ensures strong protection against proxy attacks while at the same time explicitly reducing the compounded false-rejection rate that is inherent in using a strict multi-factor conjunction. The system's architecture, the design of the individual modules, and the verification process are described, together with a probabilistic analysis of the reliability trade-offs involved. Only the authentication and device-binding module have been implemented thus far, and an experimental evaluation of the entire system has yet to be carried out.

KEYWORDS- Anti-Spoofing, Bluetooth Low Energy, Dynamic QR Code Technology, Face liveness Detection, Geofencing, Zero-Trust Authentication.

I. INTRODUCTION

In higher education attendance recording is still a routine activity of operational importance since it is often used when making decisions about eligibility, scholarships, and academic performance. Taking attendance manually is slow and can be easily manipulated when a student who is present answers for a classmate who is absent, which is why institutions have turned to digital solutions such as RFID cards, static QR codes, and GPS-based check-ins, but each of these methods has a well-documented way to be circumvented: an RFID card can be given to another student, a static QR code can be photographed and then passed on so that it can be scanned remotely, and GPS coordinates can be falsified using widely available mock-location programs. In particular, GPS is less reliable indoors than is generally thought—an early but still referenced study of measurement found root-mean-square errors ranging from less than 5 metres in wooden buildings to less than 10 metres in brick or concrete ones, and embedded mobile-phone GPS performed even worse [2]; this is exactly the level of accuracy at which it becomes impossible to tell one classroom apart from an adjacent one.

Bluetooth Low Energy (BLE) proximity detection has been suggested as a practical alternative to GPS for use indoors, and various recent systems have shown that this is feasible, for example one fairly recent design in which the signal is broadcast from the instructor's own smartphone rather than from specialised beacon equipment [4]. That said, BLE does have its own drawbacks: it is known that signal strength readings can vary considerably depending on device orientation, obstruction, and channel conditions [3], and BLE-based attendance systems have in fact been found to be vulnerable to signal-imitation and relay attacks in practice, even in the case of a real university implementation [1]. For these reasons, BLE should be treated in the same way as QR and biometric checks – as just one of several imperfect signals – rather than as standalone evidence of presence.

The paper presents a multi-factor, zero-trust system for verifying attendance which incorporates a QR token that rotates quickly and is cryptographically signed, a Bluetooth Low Energy (BLE) proximity detection signal sent ad hoc from the instructor's device, a face-liveness check carried out on the device itself, and a permanent binding to the device's hardware, with the various factors combined using an explicit two-stage acceptance rule rather than requiring that every factor be satisfied simultaneously. Figure 2 gives an overview of the system's architecture. Section II places this design in context by comparing it with other patented and previously published systems. Section III presents the threat model which motivated this design. Section IV

outlines verification factors for the proposed system. Section V describes the system architecture and the module design. Section VI examines the trade-off between the compounded probability of false rejection and the level of security. Section VII concludes with a report on the current state of implementation and future research directions.

II. RELATED WORK

Existing proxy-resistant attendance research falls into only a few classes, summarised in Table 1. QR-based systems are the most common in the literature, ranging from simple static codes to cryptographically signed time-bounded variants explicitly designed to prevent the forwarding of screenshots; others more recently utilize device-bound one-time passwords or cryptographic signing schemes to improve static tokens' tamper-resistance [24], [25]. BLE-based systems offer another category, motivated by total inadequacy of GPS indoors; class-scale deployments using students' and instructors' own equipment, in place of dedicated infrastructure, have demonstrated room-level discernment at low deployment cost [21], and importantly for this design proposal, a 2026 system explicitly uses the instructor's own mobile device as the BLE broadcaster to avoid having to install fixed beacon hardware in every room [4], which is architecturally very similar to the proximity layer proposed here.

Table 1: Comparison of Existing Verification Approaches

Approach	Location Signal	Identity Check
BLE-Based Attendance [8]	BLE proximity	None (by design)
Dynamic QR Code [9]	None	Face recognition
GPS-Based Attendance [13]	GPS	Dynamic code
Static QR code[24],[25]	None	None (forwardable)
RFID card[26]	None (fixed reader)	None (transferable)
Proposed System	BLE (ad-hoc)	QR + face liveness

Face-recognition-based solutions constitute the third category of considered solutions; more recent works emphasize the importance of implementing liveness detection mechanisms since standard face comparison algorithms can be circumvented by simply presenting a printed picture or a video, as is standard practice in lightweight and portable face-liveness attendance systems designed precisely for such low-cost deployment [22]. Multiple solutions make use of a combination of the described methods. For instance, Narayanan [5] proposes to combine BLE proximity and facial recognition by requiring that the student's BLE be within an approximate range of 5 metres from the instructor by the time a face is matched; there is no rotating QR token, nor an explicit device-hardware binding, two features which are included in the framework proposed in this paper. Similarly, Kumbhar [6] suggests a two-factor BLE-and-biometrics verification system for academic integrity. Nwabuwe, Sanghera, Alade, and Olajide [7] design a QR code-based system with dynamic codes and geofencing enhanced with IMEI (device) identification to prevent attendance fraud, thus being conceptually close to the current work, apart from using GPS location instead of BLE proximity.

Finally, two patent applications describe systems very similar to the current one. An Indian patent application published in early 2026 [8] describes a system, which uses BLE proximity detection, signed QR codes, and dynamic device/WiFi binding with optional anomaly detection, yet no biometric verification is employed, as explicitly noted by the authors. A Chinese patent application published in 2019 [9] employs a dynamic QR code requiring one-factor authentication from a messaging app and facial recognition, yet proximity checks are absent; instead, the suggested system uses a rotating QR code that only changes every minute. One Indian patent application [13] uses GPS coordinates instead of short-range proximity discovery; QR codes are used as time-sliced tokens, not rotating ones.

The literature review shows that while individual verification methods described in this paper have been extensively studied and combined with other security measures, no prior work explicitly mentions using phone-to-phone BLE proximity, rotating QR tokens, on-device liveness detection, and binding of hardware devices together in a single system. As such, while phone-to-phone proximity has been loosely mentioned in patents as a replacement for GPS, it was never explicitly combined with dynamic QR code verification or on-device liveness checks (either explicitly stated in the papers or used as a part of mentioned dynamic QR code generation). Moreover, while some works mention QR code rotation or time-slicing, it is usually done at much lower frequencies (per minute, rather than per second) or is absent altogether. A survey of the broader multi-factor attendance and continuous-authentication literature [10] suggests that architectures which combine several verification factors consistently improve spoof resistance but are rarely evaluated for the usability cost of doing so: authors repeatedly note increased friction and a higher chance that a legitimate user fails at least one step, particularly during face capture or location sensing. This is consistent with established results in the broader multimodal-biometrics literature (naively requiring every factor to pass compounds false rejection, and weighted or score-level fusion policies can substantially mitigate this without discarding the security benefit of multiple independent signals [11], [23]). It is also consistent with classroom-scale BLE evaluations (reporting acceptable room-level accuracy only when signal readings are treated probabilistically (through repeated sampling, filtering, or hysteresis) rather than as a single hard threshold [12]). The present work adopts this position directly: rather than treating the combination of QR, BLE, and face-liveness checks as a strict conjunctive gate, it proposes a weighted-confidence fusion policy and identifies the absence of adversarial, real-classroom evaluation of any such combined stack as the primary open gap this work addresses.

III. THREAT MODEL

Before describing the framework proposed to address them, it is worth explicitly stating the adversarial behaviours

which motivate our framework. In particular, we consider those attacks that make an unauthenticated attendance 'appear as' authenticated to the system. The identified threats are summarized in Table 2, according to the threat model under which they operate.

Table 2: Threat Model Summary

Threat	Description	Mitigated By
Screenshot/forward	Static QR photographed and scanned remotely	2-second QR rotation
Device sharing	One student's account used from a friend's phone	Persistent device-hardware binding
Photo/video spoof	Printed photo or replayed video shown to camera	On-device liveness check
GPS spoofing	Fake-GPS apps report a false location	BLE proximity used instead of GPS
Signal relay	BLE signal captured and retransmitted from elsewhere	Signal-strength thresholding + audit logging

The threat model extends beyond impersonation or spoofing of signals used for BLE-based attendance systems (Section I), as BLE proximity checks are also vulnerable to relay attacks, in which a BLE signal is extracted from one location and re-transmitted from another, simulating presence at both locations simultaneously [16]. Dedicated spoof-detection measures, such as those implemented in BlueShield [17], have been proposed for proximity checks, operating at the level of links to detect anomalies indicative of relay attacks. This highlights the motivation for our approach, described in Section V-D, to require BLE proximity as a mandatory check while treating facial liveness as an optional signal in support of location, rather than relying on the mere presence of a BLE signal to authenticate location.

IV. PROPOSED SYSTEM

A. Design Rationale

The framework (see below figure 1) is designed according to the zero-trust architecture, emphasizing multi-signal verification instead of a one-point verification [18]. Under the framework, a student is marked present only if three mandatory checks pass — (i) a valid time-constrained cryptographic token, (ii) confirmation that the request is coming from the student's registered device, and (iii) short-range Bluetooth proximity to the instructor's device — and (iv) an optional supporting check, a liveness-checked facial match, that raises the confidence of an attempt but is not required on its own. This mandatory-plus-supporting-pair design, rather than requiring all four to pass, is what allowed the framework to be resistant to attacks while avoiding the compounded false-rejection rate discussed in Section VI-A; the exact acceptance rule is defined formally in Section V-D. The framework utilizes three fundamentally different classes of security proof, namely cryptography, computer vision, and radio proximity, thus making attacks on all three simultaneously significantly harder than attacking any one category.

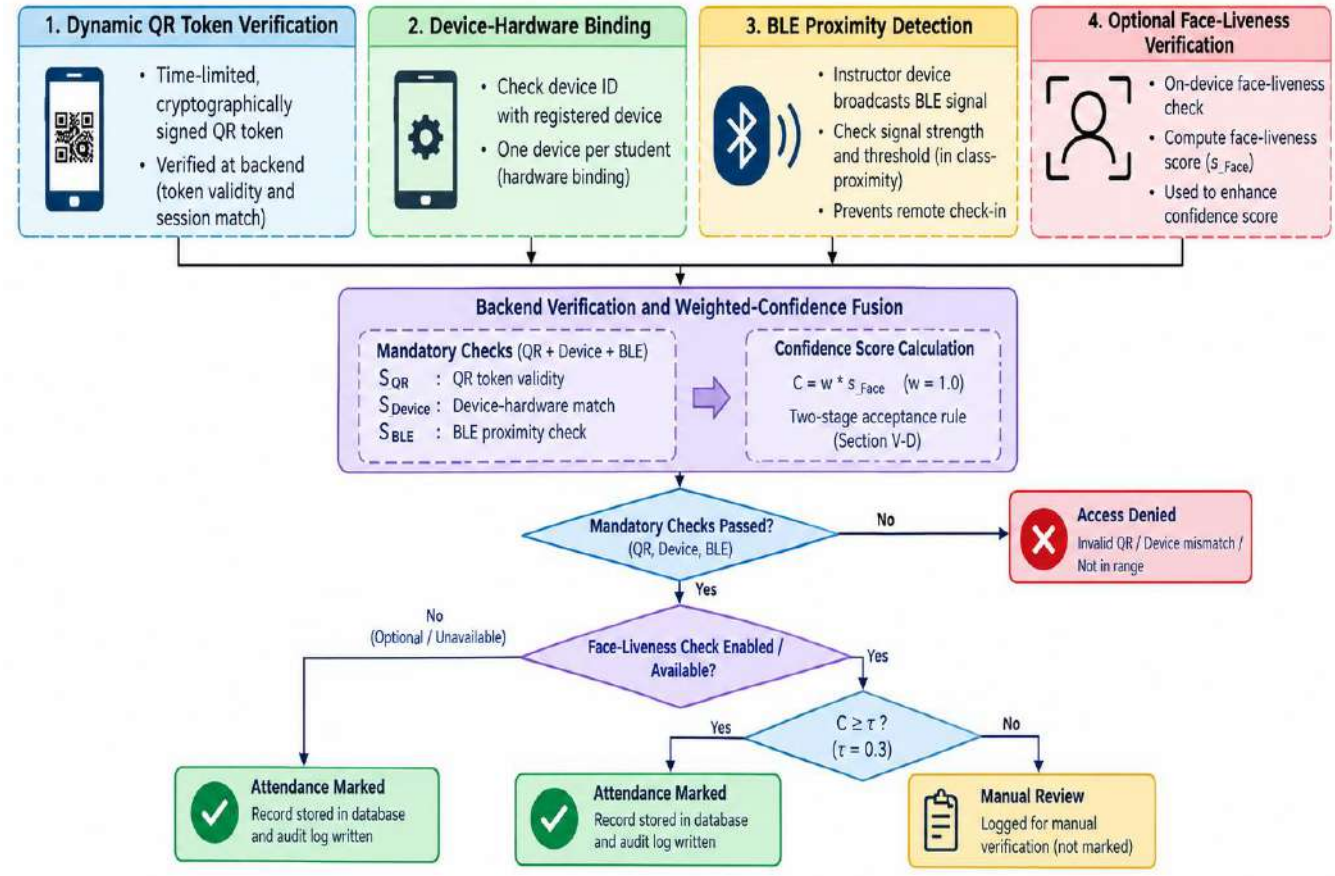

Figure 1: Proposed Multi-Factor Zero-Trust Attendance Verification Framework

In the above Figure 1 suggested a multi-factor zero-trust attendance verification architecture. The system uses dynamic QR token verification, device-hardware binding, and BLE proximity sensing. Face-liveness verification provides an optional supporting signal. The weighted-confidence fusion policy guides the backend to identify the correctness of the verification results and mark the attendance, refer to manual review, or reject it.

B. Verification Factors

Dynamic QR Token: a token of the form Token = HMAC-SHA256(ClassroomID, ServerTimestamp, SecretKey) is generated server side and renewed at a short interval (like every 2 seconds) on the server, and is only valid against the server's clock, not the device's clock where it is displayed.

BLE Proximity: the instructor's own phone acts as an ad-hoc BLE peripheral during the duration of the class, saving cost and complexity of deploying a beacon in every classroom; this is a required check, and the student app only accepts a scan when the RSSI (averaged across packets to reduce variance due to single-sample noise) exceeds a minimum threshold.

Face Liveness Check: a simple on-device liveness check (like blink or smile detection) combined with facial-embedding comparison to a previously registered (and consented to) reference embedding would ensure that a live matching face is present at the time of scanning.

Device-Hardware Binding: a student's account is only registered to a single device hardware ID; if the student logs in from another device, instead of automatically binding the request to the new device, an explicit re-binding is required. This has also been observed in related authentication literature [19], [20], where hardware, sensor-based and clock-based device fingerprinting have been used to reliably bind a request to a particular device, as opposed to merely an account.

V. SYSTEM ARCHITECTURE AND MODULE DESIGN

A. High-Level Architecture

The system consists of two client apps: a web-based instructor dashboard and a mobile student app, which communicates with a Spring Boot backend via REST + WebSocket APIs, as seen in Figure 2. The backend leverages a separate Python-based microservice for facial-embedding verification over an internal REST call, and utilizes an in-memory data store (Redis) to temporarily store QR token validations, thus keeping the highest-volume read/write path off of the main relational database.

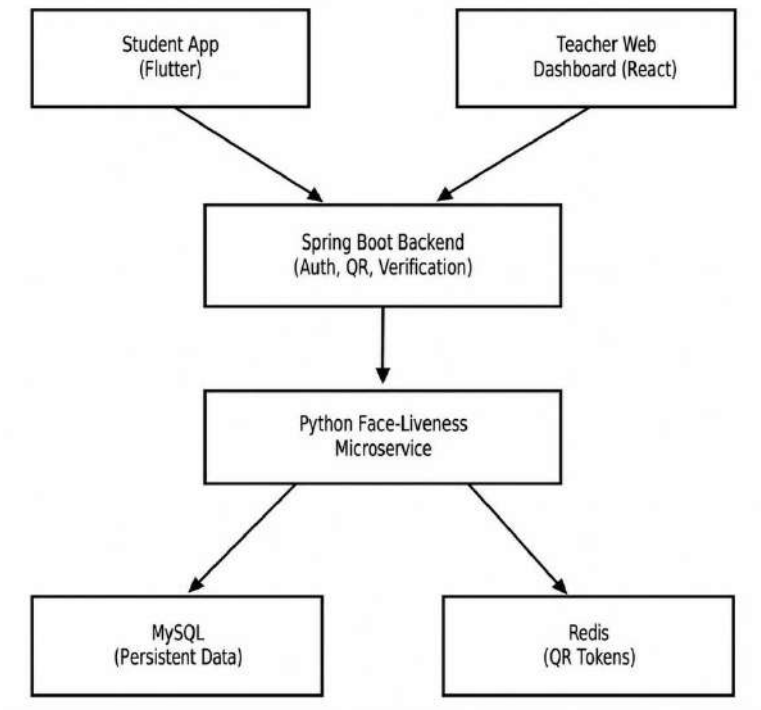

Figure 2: High-Level System Architecture

B. Core Modules

Table 3: Core System Modules

Module	Responsibility
Auth & Device Binding	Credential verification, JWT issuance, one-device-per-account enforcement
Session / Dynamic QR	Timetable-driven session initiation; token generation and rotation via Redis
BLE Proximity	Instructor-device broadcasting; student-side RSSI sampling and thresholding
Face-Liveness Service	Independent microservice for embedding registration and liveness verification
Verification Pipeline	Aggregates factor outcomes; applies the weighted-confidence acceptance policy
Correction Request	Student dispute flow, reviewed against the stored audit trail

C. Verification Sequence

On receiving a scan, the backend performs the steps shown in Figure 3.

It verifies that the presented QR token is valid in the in-memory store, that the hardware identifier of the presenting device matches that of the account's registered device, and that the reported BLE signal strength is within the mandatory proximity floor.

If all three checks pass, it optionally computes a face-liveness confidence score, and compares it against the acceptance threshold τ defined in Section V-D. An attendance record is written and an audit-log entry, containing all signal values for potential dispute resolution.

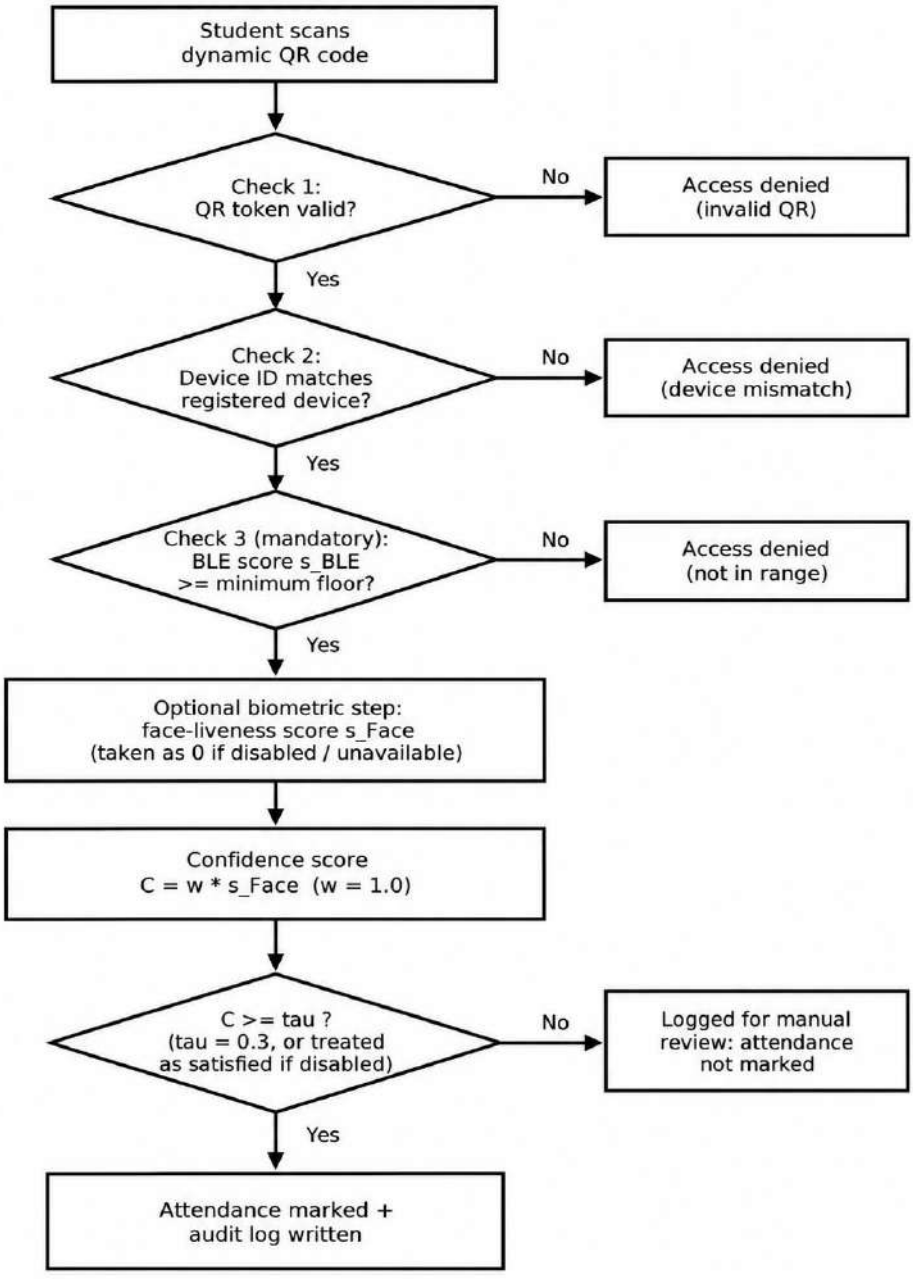

Figure 3: Attendance Verification Sequence

D. Weighted-Confidence Fusion Policy

Rather than requiring all four checks to pass, the framework makes use of an explicit two-stage acceptance rule. The QR-token-validity check, the device-hardware-binding check, and the BLE-proximity check are three mandatory gates, all of which must pass, or the attempt is rejected outright. A confidence score is computed from the face-liveness check as $C = w \cdot s_Face$, where s_Face is the normalized face-match score (in the range [0,1]) and $w = 1.0$ in the current design. Attendance is accepted if the three mandatory gates pass and $C \geq \tau$, where $\tau = 0.3$ is the configured acceptance threshold when face-liveness is used, or C is treated as satisfied by default when the face-liveness check is disabled or unavailable on a device, so that BLE-verified attempts are never blocked solely by the absence of a biometric check. Any attempt where the mandatory gates pass but the face-liveness score falls below τ is logged for manual review rather than being silently rejected, consistent with score-level fusion approaches shown to outperform naive conjunctive checks in the multimodal-biometrics literature [11], [23].

VI. DISCUSSION

A. The Compounded False-Rejection Problem

Requiring multiple independent factors reduces the probability that an erroneous proxy succeeds, but increases the probability that a genuinely present student is rejected, since each factor has its own real-world error rates. This trade-off is identical to established false-accept/false-reject analyses of ensembled biometric authenticators [14]. As an illustrative example only, and not as an experimental measurement of the implemented system, assuming the three factors were statistically independent and had reliabilities of approximately 0.99, 0.90, and 0.95, the joint probability of true acceptance would be about 0.846, or illustratively, a probability of false rejection of about 15.4% under a strict conjunctive (AND) policy across all three. The two-stage acceptance rule described in Section V-D is designed specifically to reduce this illustrative false-rejection rate in practice, though the extent of that reduction has not yet been measured empirically on a working prototype.

B. Evaluation Plan and Limitations

As future work, and in line with systematic reviews of continuous multimodal biometric authentication [15], we propose a basic empirical evaluation of a working prototype, covering: dynamic QR token validity, BLE proximity accuracy, face-liveness accuracy, device-hardware binding, resistance to proxy/relay attacks, factor-level and fused-level false-accept/false-reject rates (FAR/FRR), verification time, battery consumption, each across different classroom layouts and device models (rather than an aggregate accuracy). No results are available at the time of writing; the authentication and device-binding module is the only implemented part. BLE peripheral (broadcasting) conduct is also platform-specific, with iOS imposing stricter limitations on background operation than Android, and storing facial embeddings constitutes processing of biometric data requiring informed consent and a deletion policy in accordance with relevant data-protection legislation.

VII. CONCLUSION AND FUTURE WORK

This paper introduced a multifactor, zero-trust attendance verification framework which was a proposed design and not an evaluated system yet, using dynamic QR tokens, ad-hoc BLE proximity sensing using the instructor's own device, and on-device face-liveness verification; all without requiring dedicated per-classroom hardware. A survey of related patents/literature revealed that while each individual verification technique has been disclosed before, the combination of the three, plus an explicit weighted-confidence fusion policy to combine them, appears novel in the disclosed art. The authentication and device-binding module have been implemented; the session/QR, BLE-proximity, and face-liveness modules are currently being completed, after which empirical evaluation on the five criteria from Section V-B will be undertaken.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

ACKNOWLEDGMENT

The authors thank the Department of Computer Science and Engineering, School of Engineering and Technology (SSET), Sharda University, for its support during this project-based learning course.

REFERENCES

[1] Minkyung Kim, Jaehyun Lee, and Jeonggil Paek, "Neutralizing BLE Beacon-Based Electronic Attendance System Using Signal Imitation Attack," *IEEE Access*, vol. 6, pp. 77921–77930, 2018. Available from: https://doi.org/10.1109/access.2018.2884488

[2] Mikkel Kjærgaard, Henrik Blunck, Torben Godsk, Thomas Toftkjær, Dan Christensen, and Kaj Grønbæk, "Indoor Positioning Using GPS Revisited," in *Pervasive Computing*, pp. 38–56, 2010. Available from: https://doi.org/10.1007/978-3-642-12654-3_3

[3] Laura Flueratoru, Vasilii Shubina, Dragos Niculescu, and Elena-Simona Lohan, "On the High Fluctuations of Received Signal Strength Measurements With BLE Signals for Contact Tracing and Proximity Detection," *IEEE Sensors Journal*, vol. 22, pp. 5086–5100, 2022. Available from: https://doi.org/10.1109/jsen.2021.3095710

[4] Sana Shaikh, Sakshi Gupta, Akanksha Singh, Sanika Pal, and Kainat Sheikh, "Bluetooth-Based Smart Attendance System using BLE and Mobile Devices," *International Journal of Engineering Research & Technology (IJERT)*, vol. 15, no. 4, 2026. Available from: https://doi.org/10.5281/zenodo.19482324

[5] V. A. Narayanan, "Smart Attendance Marking System Using Bluetooth Low Energy and Facial Recognition Technology," *International Journal for Research in Applied Science and Engineering Technology*, 2022. Available from: https://doi.org/10.22214/ijraset.2022.40305

[6] K. Kumbhar, "Smart Attendance System: A Two-Factor BLE and Biometric Authentication Framework for Academic Integrity," *International Journal for Research in Applied Science and Engineering Technology*, 2026. Available from: https://doi.org/10.22214/ijraset.2026.83524

[7] Augustine Nwabuwe, Baljit Sanghera, Taiwo Alade, and Femi Olajide, "Fraud Mitigation in Attendance Monitoring Systems using Dynamic QR Code, Geofencing and IMEI Technologies," *International Journal of Advanced Computer Science and Applications*, 2023. Available from: https://doi.org/10.14569/ijacsa.2023.01404104

[8] "Automated student attendance monitoring and analytics system for college," Indian Patent Application No. IN202631017965A, Feb. 27, 2026. Available from: https://iprsearch.ipindia.gov.in/PublicSearch/PublicationSearch/Search

[9] "A facial recognition and two-dimensional code class anti-signature system based on WeChat public platform," Chinese Patent Application CN109300064A, published Feb. 1, 2019. Available from: https://patents.google.com/patent/CN109300064A/en

[10] Chalee Vorakulpipat, Siwaruk Pichetjamroen, and Ekkachan Rattanalerdnusorn, "Usable comprehensive-factor authentication for a secure time attendance system," *PeerJ Computer Science*, vol. 7, 2021. Available from: https://doi.org/10.7717/peerj-cs.678

[11] Wasiq Kabir, M. Omair Ahmad, and M. N. S. Swamy, "Normalization and Weighting Techniques Based on Genuine-Impostor Score Fusion in Multi-Biometric Systems," *IEEE Transactions on Information Forensics and Security*, vol. 13, pp. 1989–2000, 2018. Available from: https://doi.org/10.1109/tifs.2018.2807790

[12] Allan Mackey, Petros Spachos, Liang Song, and Konstantinos N. Plataniotis, "Improving BLE Beacon Proximity Estimation Accuracy Through Bayesian Filtering," *IEEE Internet of*

Things Journal, vol. 7, pp. 3160–3169, 2020. Available from: https://doi.org/10.1109/jiot.2020.2965583

[13] "An intelligent attendance system with geolocation and anomaly detection," Indian Patent Application No. IN202521023180A, published Mar. 28, 2025. Available from: https://client2021.nsllegal.com/Public/JPatent/PJ_28Mar2025.pdf

[14] Neri Merhav, "False-Accept/False-Reject Trade-Offs for Ensembles of Biometric Authentication Systems," *IEEE Transactions on Information Theory*, vol. 65, pp. 4997–5006, 2019. Available from: https://doi.org/10.1109/tit.2019.2897065

[15] Randall Ryu, Sabrina Yeom, Soo-Hyung Kim, and Damon Herbert, "Continuous Multimodal Biometric Authentication Schemes: A Systematic Review," *IEEE Access*, vol. 9, pp. 34541–34557, 2021. Available from: https://doi.org/10.1109/access.2021.3061589

[16] P. Staat, K. Jansen, C. T. Zenger, H. Elders-Boll, and C. Paar, "Analog Physical-Layer Relay Attacks with Application to Bluetooth and Phase-Based Ranging," in *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2022. Available from: https://doi.org/10.1145/3507657.3528536

[17] J. Wu, Y. Nan, V. Kumar, M. Payer, and D. Xu, "BlueShield: Detecting Spoofing Attacks in Bluetooth Low Energy Networks," 2020, pp. 397–411.

[18] Q. Yao, Q. Wang, X. Zhang, and J. Fei, "Dynamic Access Control and Authorization System based on Zero-trust architecture," in *Proceedings of the 2020 1st International Conference on Control, Robotics and Intelligent System*, 2020. Available from: https://doi.org/10.1145/3437802.3437824

[19] Alaca and P. van Oorschot, "Device fingerprinting for augmenting web authentication: classification and analysis of methods," in *Proceedings of the 32nd Annual Conference on Computer Security Applications*, 2016. Available from: https://doi.org/10.1145/2991079.2991091

[20] H. Bojinov, Y. Michalevsky, G. Nakibly, and D. Boneh, "Mobile Device Identification via Sensor Fingerprinting," *arXiv*, abs/1408.1416, 2014. Available from: https://doi.org/10.48550/arxiv.1408.1416

[21] Puckdeevongs, N. Tripathi, A. Witayangkurn, and P. Saengudomlert, "Classroom Attendance Systems Based on Bluetooth Low Energy Indoor Positioning Technology for Smart Campus," *Information*, vol. 11, p. 329, 2020. Available from: https://doi.org/10.3390/info11060329

[22] N. Surantha and B. Sugijakko, "Lightweight face recognition-based portable attendance system with liveness detection," *Internet of Things*, vol. 25, Art. no. 101089, 2024. Available from: https://doi.org/10.1016/j.iot.2024.101089

[23] M. Singh, R. Singh, and A. Ross, "A Comprehensive Overview of Biometric Fusion," *arXiv*, abs/1902.02919, 2019. Available from: https://doi.org/10.1016/j.inffus.2018.12.003

[24] M. Isaac, "Design and Implementation of a Secure QR Code-Based Attendance Management System for Higher Education," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 2025. Available from: https://doi.org/10.32628/cseit25111699

[25] N. Azizah, A. Rahmadian, and W. Sirait, "Aplikasi Absensi Berbasis QR Code dan Time-Based One-Time Password Untuk Siswa SMA Adabiah Padang," *Explore*, vol. 15, no. 1, 2025. Available from: https://doi.org/10.35200/ex.v15i1.156

ABOUT THE AUTHORS

Akash Sahu is pursuing a B.Tech. in Computer Science and Engineering at Sharda University, Greater Noida, India. His research interests include Artificial Intelligence, Machine Learning, Computer Vision, and biometric image analysis. His research work focuses on fingerprint-based pattern analysis using AI and deep learning techniques. He has participated in academic and research-oriented technical projects. He is currently involved in research and project-based learning activities under the guidance of Dr. Yojna Arora.

Kanchan is pursuing a Bachelor of Computer Applications (BCA) at Axis Institute of Higher Education, Kanpur, India. Her academic interests include Computer Applications, Information Technology, and emerging technologies. She is interested in exploring innovative applications of technology and developing practical technical skills. She has participated in academic and technology-oriented learning activities. She is currently pursuing her undergraduate studies and aims to build a career in the field of Information Technology.

Dr. Yojna Arora is an Associate Professor in the Department of Computer Science & Engineering at Sharda University, Greater Noida, India. She has over 13 years of experience in higher education and research. Her research interests include Big Data Analytics, Large Language Models, Data Mining, and Network Security.