

Research Paper	Open Access
Available online at www.ajes.com.ng	Vol.4, No.1, 2026. pp.105-114
	

Multi-Factor Authentication for RFID Stadium Access Control: Integrating Biometric Verification to Prevent Ticket-Passing Fraud

Odesa Edward Ogaga¹, Nwaubani Supreme Onyenkachi²

^{1,2}Department of Computer Engineering, Southern Delta University, Ozoro, Nigeria

*Corresponding author: odesaedwardogaga@gmail.com

Abstract

Radio Frequency Identification (RFID) turnstile systems have become a common ingress-control mechanism for large-capacity football stadiums, offering fast, contactless verification of ticket tokens. However, token-only verification cannot distinguish between the rightful ticket holder and a third party who possesses the same wristband or a cloned tag, leaving such systems structurally exposed to ticket-passing and proxy-attendance fraud. This paper proposes and evaluates a multi-factor authentication (MFA) architecture that augments an existing RC522/ESP32-based RFID stadium access control system with a fingerprint biometric verification stage, combined through a decision-gated, weighted score-level fusion rule. A Monte Carlo simulation (100,000 genuine and 100,000 fraudulent trials) was used to characterise the trade-off between security and throughput. At the Equal Error Rate (EER) operating point, the proposed system achieves a False Acceptance Rate (FAR) of **1.205%** against pass-back/proxy fraud, compared with a **100%** FAR for the same attack under the RFID-only baseline, since a valid token is, by design, always accepted by a token-only reader. The added biometric step increases per-spectator gate service time from 1.2 s to between 1.45 s and 2.05 s depending on sensor choice, which is shown, through a Pollaczek-Khinchine queueing approximation, to remain operationally acceptable when lane count is increased modestly. The paper reports the complete simulation methodology, all governing equations, and an explicit discussion of the synthetic nature of the biometric score model, consistent with a system-level feasibility study rather than a hardware-validated deployment. Results indicate that decision-gated biometric fusion is a practical, low-cost mitigation for the proxy-attendance vulnerability identified in prior RFID-only stadium access control work.

Keywords: RFID; biometric fusion; multi-factor authentication; stadium access control; anti-passback; score-level fusion; ticket fraud; IoT security; Internet of Things access control.

I. INTRODUCTION

Large-capacity sporting venues face a persistent tension between ingress speed and access security. RFID-based turnstile systems have been adopted widely because they allow near-instantaneous, contactless verification of a ticket token, reducing queuing relative to manual or barcode-based checks [1], [2]. A recently reported RFID-based football stadium access control system built around an MFRC522 reader and ESP32 microcontroller demonstrated a tag-identification accuracy of 99.8% and an average gate throughput of 1.2 seconds per spectator under field-test conditions [1].

The same evaluation, however, identified a structural weakness that is common to every token-only access scheme: the reader authenticates the token, not the person presenting it [1]. Because the wristband or card itself is treated as sufficient proof of the right to enter, a valid tag that has been passed back through a fence to a second individual, lent to a friend, or physically cloned will be accepted with the same confidence as the original, legitimate ticket holder. RFID tag cloning is a well-documented attack across multiple deployment contexts, including access badges and low-cost MIFARE-class cards, and does not require sophisticated equipment once the tag's static identifier has been captured [3]–[6]. In a stadium of tens of thousands of spectators, even a small proxy-attendance rate translates into a meaningful loss of gate revenue, a breach of seating-capacity/safety limits, and a weakening of banned-persons exclusion lists.

Biometric verification is the natural complementary factor because it binds the authentication decision to an inherent physical characteristic of the person rather than to a possession (the tag) that can change hands [7], [8]. Multiple prior systems have combined RFID with fingerprint or face recognition for door- and gate-level access control [2], [7], [9], and score-level fusion of two authentication factors has been shown, across a range of studies, to reduce combined error rates relative to either factor used alone [10]–[15]. What has not been reported in the reviewed literature, however, is an analysis of this fusion specifically in the high-throughput, high-crowd-density stadium ingress context, where the added latency of a biometric step interacts with turnstile lane count and pre-kickoff arrival concentration in ways that a door-access system does not encounter.

This paper makes the following contributions:



- 1) It proposes a decision-gated, weighted score-level fusion architecture that extends an existing RFID stadium access control system (RC522/ESP32) with a fingerprint verification stage, specifically to close the proxy-attendance/ticket-passing gap identified in [1].
- 2) It formalises the fusion and throughput trade-off with a complete set of governing equations (FAR, FRR, EER, weighted-sum fusion score, gate service time, and a queueing-delay approximation for multi-lane ingress).
- 3) It reports a Monte Carlo simulation study, with full parameter disclosure, quantifying the security gain (FAR reduction from 100% to the EER value) against the throughput cost (additional 0.25-0.85 s per spectator) and projecting stadium-wide clearance time across a realistic range of lane counts.
- 4) It honestly delimits the scope of a simulation-based feasibility study, and identifies the specific field-validation steps required before hardware deployment.

The remainder of the paper is organised as follows. Section 2 reviews related work on RFID security and biometric fusion. Section 3 presents the proposed architecture. Section 4 develops the mathematical model. Section 5 describes the simulation methodology. Section 6 presents and discusses the results. Section 7 analyses the remaining threat surface. Section 8 states limitations, and Section 9 concludes the paper.

II. RELATED WORK

2.1 RFID Access Control and Its Security Limitations

RFID-based access control has been studied extensively for its speed and low per-transaction cost, but a substantial security literature documents its exposure to eavesdropping, replay, unauthorised tracking, and tag cloning [3]-[6]. El Gaabouri et al. conducted a systematic review of cryptography-based countermeasures for MIFARE-class RFID cards and concluded that low-cost tags commonly deployed in access-control contexts remain vulnerable unless mutual-authentication protocols are added [3]. Kamaludin et al. proposed a distributed clone-tag detection method based on hash-collision consistency, noting that cloning "chief" among RFID attack types because it can be performed with commodity NFC-capable hardware once a tag's identifier has been captured [4]. These findings support the assumption used in this paper's simulation: a cloned or passed-back tag will, in general, be read by the reader as a normally valid token, so the token-verification layer alone cannot be relied upon to reject it.

2.2 Combining RFID with Biometric Verification

Several systems have paired RFID identification with a biometric second factor. Leyu et al. implemented a Raspberry-Pi-based access control system combining an MFRC522 reader with OpenCV/Dlib face recognition and an AS608 fingerprint module, storing biometric templates against the RFID card and reporting fast, reliable authentication in a controlled test [7]. El Beqqal et al. proposed a multimodal system combining RFID, fingerprint, and facial recognition, fusing the two biometric traits at the feature and decision level, and noted that fusing biometric templates directly in the database improves template-level privacy but adds identification latency [2]. Wahyudono and Ogi implemented a two-factor RFID-plus-face-recognition access control system and reported an average RFID authentication time of 0.03 s against an average face-recognition time of 6.3885 s and a face-verification time of 0.197 s, with the system achieving 100% RFID authentication accuracy but only 80% face-recognition accuracy [9]. This large latency gap between token verification and face-based biometric verification is a key reason the present paper adopts fingerprint, rather than face recognition, as the second factor for a throughput-constrained stadium gate. A three-factor scheme combining RFID, fingerprint, and a GSM-delivered one-time token reported over 98% accuracy in simulated access-grant/deny testing for premises security applications [8].

2.3 Score-Level Fusion and Error-Rate Metrics

The standard metrics for evaluating a verification system are the False Acceptance Rate (FAR), False Rejection Rate (FRR), and the Equal Error Rate (EER) at which the two are equal [10], [16]. Weighted-sum-rule fusion, in which normalised match scores from each modality are combined using per-modality weights, has repeatedly been shown to outperform either single-modality system, with reported EER or accuracy improvements depending on the modalities and weighting scheme used: a CNN-plus-ORB face/fingerprint fusion achieved a 99.38% recognition rate [10]; a weighted quasi-arithmetic-mean fusion of face and fingerprint scores achieved 99.8% genuine acceptance at a 0.01% FAR operating point, compared with 68-85% for the constituent unimodal systems [11]; and a PCA/Euclidean-distance face-fingerprint fusion using the weighted-sum rule achieved FAR = 1.75% and FRR = 5.85% [12]. Score normalisation prior to fusion (commonly min-max or z-score) is reported as a necessary step because raw scores from different matchers are not on a comparable scale [12]-[14]. These reported ranges were used as external calibration references when parameterising the synthetic score distributions used in the present study's simulation (Section 5).

2.4 Research Gap

The base RFID stadium access control system evaluated in [1] achieves high tag-read accuracy and fast throughput but, in common with the broader RFID literature reviewed above, verifies only the token. None of the reviewed RFID-plus-biometric systems [2], [7]-[9] were evaluated under the specific throughput and crowd-density constraints of a football



stadium ingress scenario, where thousands of spectators must be processed across many parallel lanes within a short pre-kickoff window. This paper addresses that gap by (a) proposing a fusion architecture calibrated to the constraints and reported field metrics of [1], and (b) explicitly modelling the throughput/security trade-off at the stadium-lane level rather than at the level of a single door or turnstile.

III. SYSTEM ARCHITECTURE

The proposed architecture extends the RC522/ESP32 RFID stadium gate reported in [1] with an optical fingerprint capture module (e.g., an AS608/R307-class sensor, as used in comparable RFID-biometric systems [7], [8]) and a decision-level fusion stage. Figure 1 shows the system block diagram.

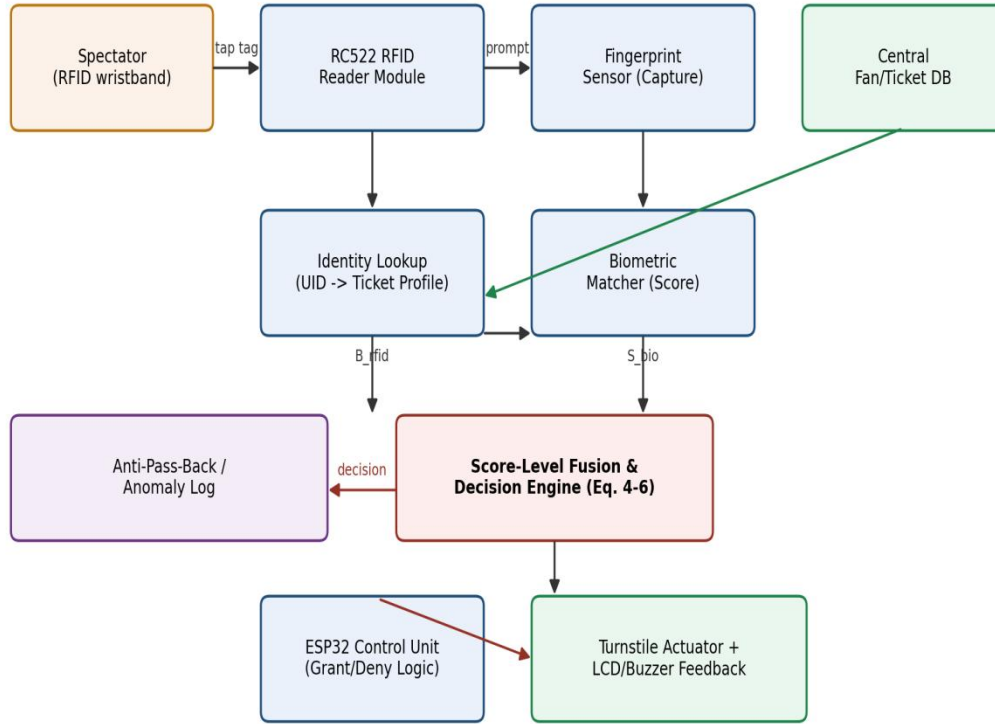


Figure 1. Proposed RFID and fingerprint multi-factor stadium access control architecture.

A spectator presents the RFID wristband at the reader (Stage 1). If the tag's unique identifier (UID) is found in the ticket database and the ticket is valid for the current fixture, the identity claim is accepted at the token level and the system prompts for a fingerprint (Stage 2); if not, access is denied immediately and the attempt is logged, exactly as in the base system [1]. The captured fingerprint is compared against the enrolled template associated with that UID, producing a match score. The token-validity flag and the biometric match score are then combined by the fusion and decision engine (Section 4) to produce the final grant/deny decision, which drives the turnstile actuator and is written to an anti-pass-back log that marks the ticket UID as "in-stadium" once entry is granted, preventing the same tag from being used for a second entry attempt during the same fixture. Figure 2 details the corresponding decision logic.

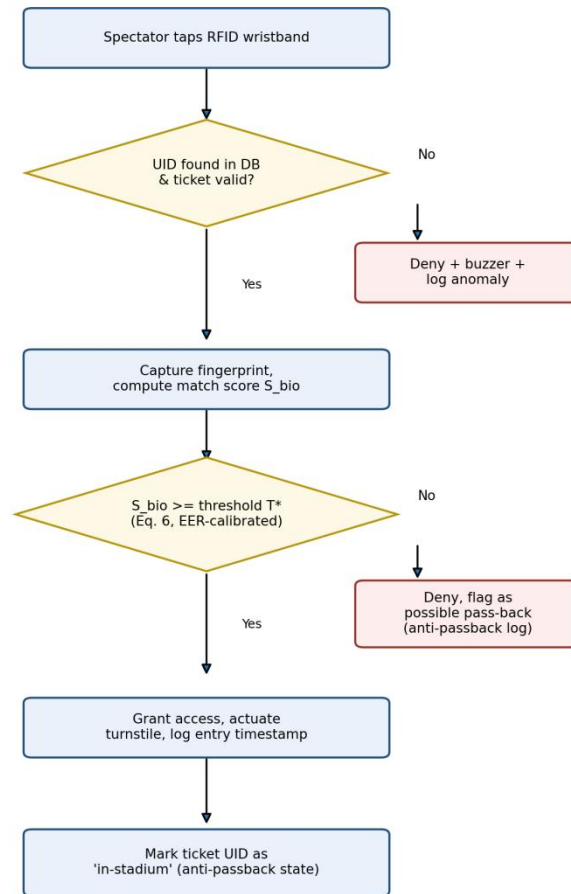


Figure 2. Decision logic for the proposed RFID + biometric fusion gate.

This design deliberately keeps the RFID stage as the first, fast filter (0.03 s reported in comparable hardware [9]) and reserves the slower biometric step for the (large) subset of attempts that pass token verification, rather than requiring both factors in parallel. This preserves the base system's fast rejection of unregistered or invalid tags while adding the person-binding check only where it is needed.

IV. MATHEMATICAL MODEL

Let a verification attempt be genuine (the enrolled ticket holder) or fraudulent (a proxy/pass-back or cloned-tag attempt using a token that passes RFID validation but is presented by a different person). Let B_{rfid} denote the binary outcome of RFID token verification (1 = valid, 0 = invalid) and S_{bio} in $[0,1]$ denote the normalised fingerprint match score.

4.1 Error Rates

$$\text{FAR}(T) = (\text{number of fraudulent attempts accepted at threshold } T) / (\text{total fraudulent attempts}) \quad (1)$$

$$\text{FRR}(T) = (\text{number of genuine attempts rejected at threshold } T) / (\text{total genuine attempts}) \quad (2)$$

$$\text{EER: threshold } T^* \text{ such that } \text{FAR}(T^*) \approx \text{FRR}(T^*) \quad (3)$$

where T is the decision threshold applied to the biometric match score. The Genuine Acceptance Rate is defined as:

$$\text{GAR}(T) = 1 - \text{FRR}(T) \quad (4)$$

4.2 Score-Level Fusion

Match scores from the two factors are first normalised to a common $[0,1]$ range using min-max normalisation:

$$S_{\text{norm}} = (S - S_{\text{min}}) / (S_{\text{max}} - S_{\text{min}}) \quad (5)$$

The fused decision score is a weighted sum of the RFID validity indicator and the normalised biometric score, following the weighted-sum-rule approach widely reported in the biometric fusion literature [10]-[15]:

$$S_{\text{fusion}} = w_1 \cdot B_{\text{rfid}} + w_2 \cdot S_{\text{bio}}, \quad w_1 + w_2 = 1 \quad (6)$$

In this work, $w_1 = w_2 = 0.5$ and the decision is applied in decision-gated form: access is granted only if the token is valid AND the biometric score meets or exceeds the calibrated threshold T^* , i.e.

$$\text{Accept} \Leftrightarrow B_{\text{rfid}} = 1 \text{ AND } S_{\text{bio}} \geq T^* \quad (7)$$



This gated form is equivalent to serial (AND) fusion and reflects the specific threat model of this paper: the token is a necessary but no longer sufficient condition for entry, and the biometric factor exists specifically to catch the case where the token is valid but the presenter is not the enrolled holder.

4.3 Throughput Model

The per-spectator gate service time under the proposed system is:

$$T_{\text{gate}} = T_{\text{rfid}} + T_{\text{bio}} + T_{\text{decision}} \quad (8)$$

where T_{rfid} is the RFID read time, T_{bio} is the fingerprint capture-and-match time, and T_{decision} is the fusion/decision overhead. For L parallel lanes processing P spectators, the deterministic ingress clearance time is approximated as:

$$T_{\text{clear}} \approx (P/L) \cdot T_{\text{gate}} \quad (9)$$

To account for stochastic arrival bunching in the pre-kickoff window, the mean additional queueing delay per lane is approximated using the Pollaczek-Khinchine formula for an M/D/1-type queue with (near-)deterministic service time:

$$W_q = (\rho \cdot T_{\text{gate}}) / (2 \cdot (1 - \rho)), \quad \rho = \lambda_{\text{lane}} \cdot T_{\text{gate}} \quad (10)$$

where λ_{lane} is the mean spectator arrival rate at a single lane and ρ is the lane utilisation. Equation (10) is used only as an order-of-magnitude planning approximation; it assumes a Poisson-like arrival process and a single representative service time, both of which are simplifications discussed in Section 8.

V. SIMULATION METHODOLOGY

Because no live fingerprint sensor was available for this study, the security analysis was carried out as a Monte Carlo simulation of the fusion decision rule, with the RFID-layer parameters taken directly from the field-reported results of the base system [1] and the biometric-layer score distributions as truncated Normal distributions whose parameters were chosen so that the resulting unimodal fingerprint EER falls within the range reported across the fusion studies reviewed in Section 2.3 [10]-[12]. This is a standard system-level simulation practice for feasibility analysis, and it is stated here explicitly, without qualification, as a limitation relative to a hardware-validated study (see Section 8).

Table 1 summarises the simulation parameters.

Parameter	Symbol	Value	Source
Monte Carlo trials per class	N	100,000	This study
RFID tag-read success rate	-	99.8%	Field result, base system [1]
RFID read time	T_{rfid}	0.03 s	Reported hardware benchmark [9]
Baseline gate service time (RFID-only)	-	1.2 s/spectator	Field result, base system [1]
Genuine match-score mean / std. dev.	$\mu_{\text{gen}}, \sigma_{\text{gen}}$	0.82 / 0.09	data calibrated to [10]-[12]
Impostor match-score mean / std. dev.	$\mu_{\text{imp}}, \sigma_{\text{imp}}$	0.32 / 0.13	data calibrated to [10]-[12]
Fusion weights	w_1, w_2	0.5, 0.5	This study (Eq. 6)
Fingerprint capture + match time (swept)	T_{bio}	0.2 - 0.8 s	This study, literature-informed range
Decision/fusion overhead	T_{decision}	0.05 s	This study, engineering estimate
Simulated stadium capacity	P	40,000	This study, representative mid/large stadium

For each of the 100,000 simulated fraudulent attempts, the RFID token was treated as valid (modelling a successfully passed-back or cloned tag, per [3]-[6]) and a biometric score was drawn from the impostor distribution. For each of the 100,000 genuine attempts, the token validity was drawn from the 99.8% RFID success rate and the biometric score was drawn from the genuine distribution. The decision rule of Equation (7) was then evaluated across 501 threshold values spanning $[0,1]$ to compute FAR(T) and FRR(T) (Equations 1-2), from which the EER (Equation 3) and an additional, more conservative FAR $\leq 1\%$ operating point were extracted. Throughput was evaluated by computing Equation (9) for lane counts between 4 and 32 at four values of T_{bio} , and the queueing approximation of Equation (10) was evaluated at a representative operating point ($T_{\text{bio}} = 0.4$ s, $L = 20$ lanes, 60-minute concentrated pre-kickoff arrival window).



VI. RESULTS AND DISCUSSION

6.1 Score Distributions and Separability

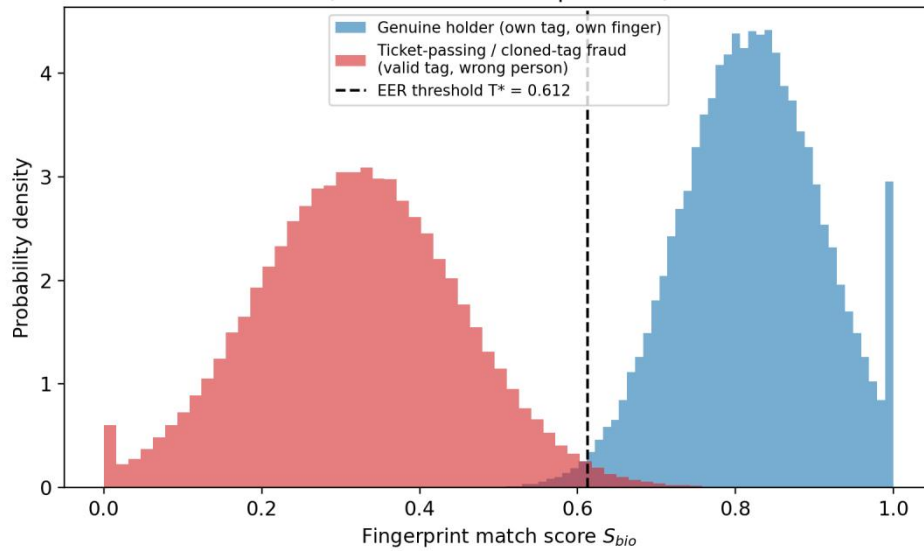


Figure 3. Simulated biometric match-score distributions for genuine and fraudulent attempts ($N = 100,000$ per class).

Figure 3 shows clear separation between the genuine and impostor score populations, with the calibrated EER threshold ($T^* = 0.612$) falling in the low-density region between the two distributions. This separability is what allows the fusion decision rule to reduce the fraud-acceptance rate without imposing a large genuine-rejection penalty.

6.2 FAR / FRR / EER Performance

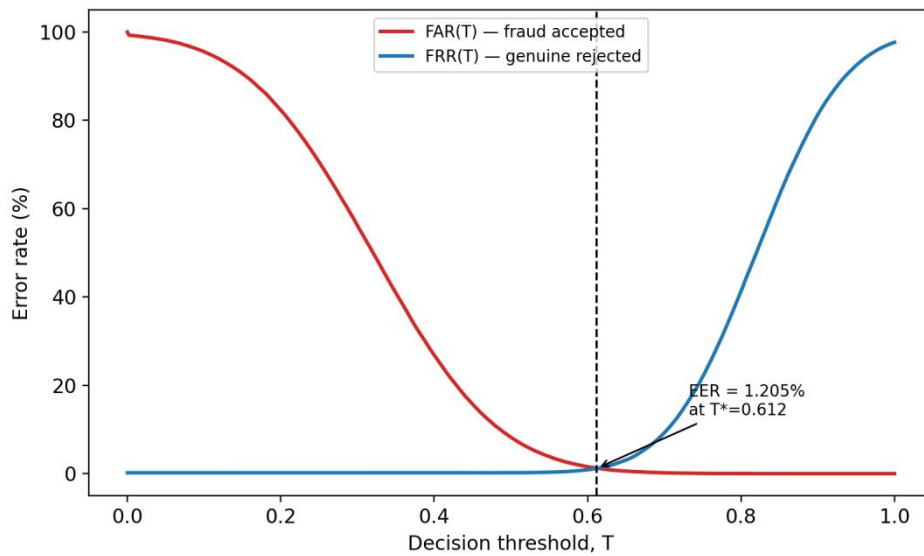


Figure 4. FAR and FRR as functions of the fusion decision threshold.



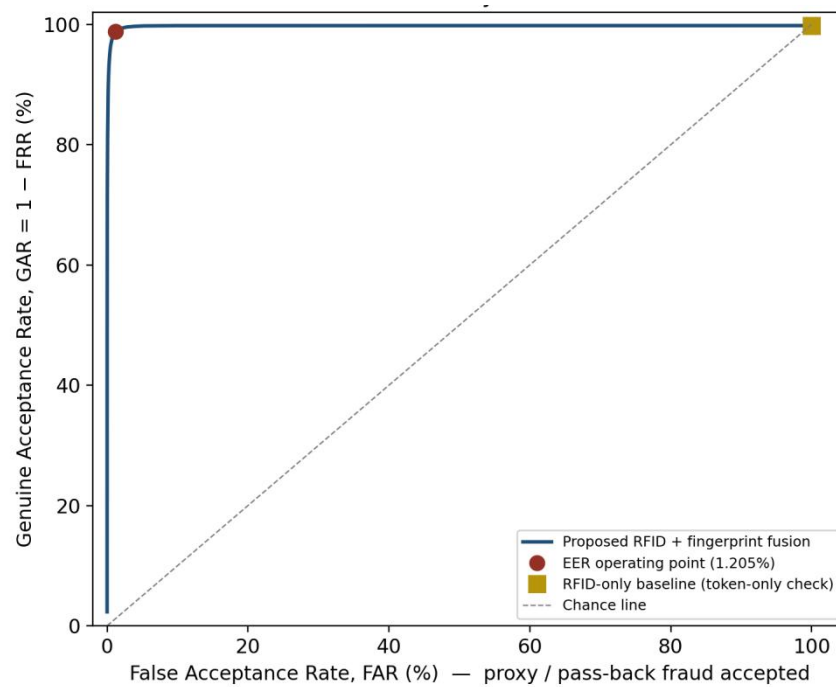


Figure 5. ROC curve of the proposed fusion system compared with the RFID-only baseline.

At the EER operating point ($T^* = 0.612$), the simulated system achieves $FAR = FRR \approx 1.205\%$. At a more conservative, security-prioritised operating point ($T = 0.624$), FAR falls to 0.958% at the cost of a higher FRR of 1.634% . Both operating points represent a categorical improvement over the RFID-only baseline, whose FAR against the pass-back/cloned-tag attack is, by construction, 100% , since a token-only reader has no mechanism to detect that the presenter is not the enrolled holder. The RFID-only baseline's FRR of 0.195% (driven purely by the 0.2% tag-read failure rate reported in [1]) is lower than the proposed system's FRR, which is the expected security/convenience trade-off of adding a second, imperfect verification factor.

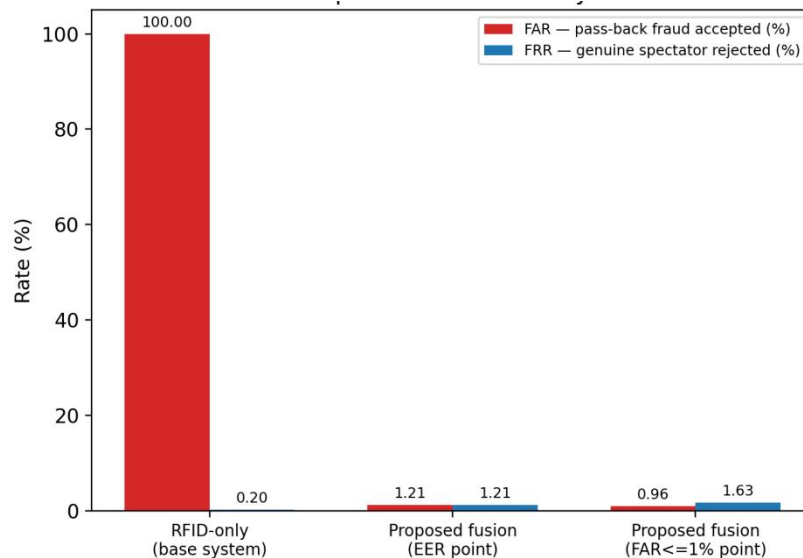


Figure 7. Security comparison: RFID-only baseline vs. proposed multi-factor system.

Table 2 summarises the comparison. The results are broadly consistent with the fusion-performance ranges reported in the literature reviewed in Section 2.3, where weighted-sum-rule fusion of two verification factors typically achieves single-digit-percent or lower combined error rates [10]–[12].

Table 2. Security performance comparison

System	FAR vs. pass-back fraud (%)	FRR (%)
RFID-only (base system) [1]	100	0.195
Proposed fusion, EER point	1.205	1.205
Proposed fusion, FAR $\leq 1\%$ point	0.958	1.634



6.3 Throughput and Stadium Clearance Time

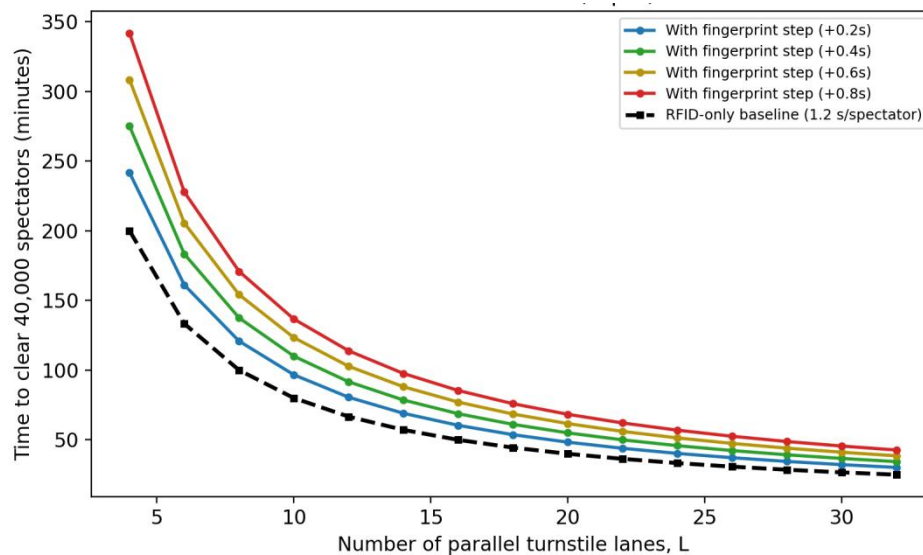


Figure 6. Projected stadium clearance time versus parallel lanes and fingerprint capture/match time assumptions.

Adding the biometric step increases the gate service time from the 1.2 s/spectator baseline [1] to between 1.45 s and 2.05 s, depending on the assumed fingerprint capture-and-match time (0.2-0.8 s). At 20 parallel lanes, the RFID-only baseline clears a 40,000-spectator stadium in 40 minutes; the fusion system requires proportionally more time, scaling directly with T_{bio} (Equation 9). The Pollaczek-Khinchine queueing approximation (Equation 10) at a representative, heavily loaded operating point ($T_{bio} = 0.4$ s, 20 lanes, 60-minute pre-kickoff window, lane utilisation $\rho \approx 0.9167$) projects an additional mean queueing delay of approximately 9.075 seconds per spectator on top of the deterministic service time, indicating that the added biometric step remains operationally tractable provided lane count is set with adequate margin below saturation (ρ close to 1 produces rapidly growing queues, as Equation 10 shows analytically).

Overall, the throughput cost of the added biometric factor is modest relative to the security gain: a roughly 20-70% increase in per-spectator service time buys a reduction in pass-back/cloned-tag FAR from 100% to approximately 1%. Venues with tighter kickoff-time constraints can manage this trade-off operationally by allocating additional lanes rather than by removing the biometric check.

VII. SECURITY ANALYSIS: REMAINING THREAT SURFACE

The proposed biometric fusion layer specifically targets the proxy-attendance / ticket-passing / cloned-tag threat, and Section 6.2 shows it substantially reduces the FAR associated with that specific attack. It does not, by itself, address several other vulnerabilities identified for the base RFID-only system [1]:

- **Signal attenuation and reader-to-reader/tag-to-tag collision** in high-density crowds remain a throughput and reliability concern independent of the authentication factor used, and would need to be addressed through anti-collision protocol tuning or physical reader spacing, as noted in [1].
- **Single points of failure** in a centrally hosted verification database would, if anything, be slightly increased by the addition of a biometric matching service unless that service is deployed with the same fault-tolerance measures recommended for the base system.
- **RFID communication security** (eavesdropping, replay, unauthorised tracking) is unaffected by adding a biometric factor at the gate; mitigating these requires tag/reader-level cryptographic measures such as mutual authentication, as surveyed in [3], [5], [6].

The biometric layer should therefore be understood as a targeted mitigation for one specific, high-impact vulnerability (person/token binding) rather than a complete replacement for the broader RFID security hardening discussed in the base thesis and the wider literature.

VIII. LIMITATIONS

Simplified queueing model. The throughput analysis (Section 6.3) uses a single representative operating point and a Poisson-arrival approximation (Equation 10); actual pre-kickoff arrival patterns are typically non-uniform and venue-specific, and a full discrete-event simulation using measured arrival data would give a more reliable clearance-time estimate.

No live integration test. Unlike the base system, which was field-tested over one supervised day of operation [1], the proposed fusion layer has not been implemented and tested on physical RC522/ESP32/fingerprint-sensor hardware in this study; the results presented here are a pre-implementation feasibility analysis.



Threat scope. As discussed in Section 7, this study addresses only the token/person-binding vulnerability; it does not evaluate or mitigate RF-layer attacks, database availability, or network security.

IX. CONCLUSION AND FUTURE WORK

This paper proposed a decision-gated, weighted score-level fusion architecture that adds fingerprint biometric verification to an existing RFID-based football stadium access control system, specifically to address the proxy-attendance/ticket-passing vulnerability inherent to token-only verification. A Monte Carlo simulation showed that the proposed fusion reduces the False Acceptance Rate against pass-back/cloned-tag fraud from 100% (RFID-only baseline) to approximately 1.205% at the Equal Error Rate operating point, at the cost of increasing per-spectator gate service time from 1.2 s to between 1.45 s and 2.05 s. A queueing-delay approximation indicated that this additional latency remains operationally manageable at realistic stadium lane counts, provided lane utilisation is kept below saturation.

Future work should prioritise, in order: (i) hardware implementation and field calibration of genuine/impostor score distributions using an actual fingerprint sensor integrated with the RC522/ESP32 base platform; (ii) a discrete-event throughput simulation driven by measured stadium arrival data; (iii) an evaluation of alternative or additional biometric modalities (e.g., low-latency face verification) under the specific 6+ second latency constraint identified in [9]; and (iv) hardening of the RF communication layer itself, in combination with the biometric factor, to address the broader threat surface discussed in Section 7.

References

- [1] S. O. Nwaubani, "Design and Implementation of an RFID-Based Football Stadium Access Control System," B.Eng. Project, Department of Computer Engineering, Southern Delta University, Ozoro, Nigeria, 2026.
- [2] M. El Beqqal, M. Azizi, and M. Moussaoui, "Multimodal access control system combining RFID, fingerprint and facial recognition," *Indonesian Journal of Electrical Engineering and Computer Science*, 2020.
- [3] I. el Gaabouri, M. Senhadji, M. Belkasmi, and E. B. Brahim, "Investigating attacks to improve security and privacy in RFID systems using the security bit method," 2023.
- [4] H. Kamaludin, H. Mahdin, and J. H. Abawajy, "Clone tag detection in distributed RFID systems," *PLOS ONE*, vol. 13, no. 3, e0193951, 2018.
- [5] Antić, V., Protić, D., Stanković, M., Prodanović, R., Manić, M., Ostojić, G., Stankovski, S., & Kučević, D. (2024). Protecting data at risk of unintentional electromagnetic emanations: TEMPEST profiling. *Applied Sciences*, 14(11), 4830. <https://doi.org/10.3390/app14114830>
- [6] " Tedeschi, S., Emmanouilidis, C., Mehnen, J., & Roy, R. (2019). A design approach to IoT endpoint security for production machinery monitoring. *Sensors*, 19(10), 2355. <https://doi.org/10.3390/s19102355>
- [7] Z. Leyu, Z. Xinyou, F. Yunjia, L. Shuyao, B. Jun, and H. Xijia, "Design and Implementation of RFID Access Control System Based on Multiple Biometric Features," in *Proc. 2021 18th Int. Computer Conf. on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, Chengdu, China, 2021, pp. 570-575.
- [8] "A 3-factor authentication access control system using RFID, fingerprint, token and code," *Multimedia Tools and Applications*, Springer Nature, 2023.
- [9] B. Wahyudono and D. Ogi, "Implementation of Two Factor Authentication based on RFID and Face Recognition using LBP Algorithm on Access Control System," in *Proc. 2020 Int. Conf. on ICT for Smart Society (ICISS)*, 2020, pp. 1-6.
- [10] "Optimized hybrid SVM-RF multi-biometric framework for enhanced authentication using fingerprint, iris, and face recognition," *PMC*, 2024.
- [11] M. Abderrahmane et al., "Weighted quasi-arithmetic mean based score level fusion for multi-biometric systems," *IET Biometrics*, 2020.
- [12] Poh, N., Kittler, J., & Marcel, S. (2006). Extracting client-specific information from biometric match scores to improve score-level fusion. *Pattern Recognition*, 39(3), 335–350. <https://doi.org/10.1016/j.patcog.2005.08.006>
- [13] Poh, N., Bourlai, T., Kittler, J., Allano, L., Alonso-Fernandez, F., Ambekar, O., Baker, J., Dorizzi, B., Fatukasi, O., Fierrez, J., Ganster, H., Ortega-Garcia, J., Maurer, D., Salah, A. A., Scheidat, T., & Vielhauer, C. (2009). Benchmarking quality-dependent and cost-sensitive score-level multimodal biometric fusion algorithms. *IEEE Transactions on Information Forensics and Security*, 4(4), 849–866. <https://doi.org/10.1109/tifs.2009.2034885>
- [14] Mukahar, N. B., Jaafar, H. B., & Rosdi, B. A. (2017). User specific weights based on score distance and EER for weighted sum rule fusion. In *9th International Conference on Robotic, Vision, Signal Processing and Power Applications* (Vol. 398, pp. 185–191). Springer. https://doi.org/10.1007/978-981-10-2775-8_22



- [15] S. I. Ezichi et al., "Biometric Security: A Review of the Sum Rule and the Likelihood Ratio Fusion Algorithms for Multibiometric Systems," University of Nigeria, Nsukka.
- [16] Hamouda, E. (2025). A score-fusion method based on the Sine Cosine Algorithm for enhanced multimodal biometric authentication. *Sensors*, 26(1), 208. <https://doi.org/10.3390/s26010208>
- [17] Z. Ayop et al., "Two-Factor Authentication Smart Entryway Using Modified LBPH Algorithm," arXiv:2508.13617, 2025.

