



KEMENTERIAN PENDIDIKAN TINGGI

PITRAM 2026

Pertandingan Inovasi Antara Asasi Malaysia

Extended Abstract Book



11 dan 12 APRIL 2026

Dewan Berlian

Universiti Teknologi MARA

Cawangan Selangor

Kampus Puncak Alam



UNIVERSITI
TEKNOLOGI
MARA

Pusat
Asasi



KEMENTERIAN PENDIDIKAN TINGGI



MAJLIS DEKAN/PENGARAH ASASI
UNIVERSITI AWAM MALAYSIA

Biometric and Smart Identification Reader (B.A.S.I.R.): Combating Proxy Attendance via Multiprocessing Dual-Factor Authentication

Muhammad Azman Sutandaiman @ Zaihami¹, Muhammad Akid Zikri Ahmad Zaki¹,
Muhammad Danish Maswira¹, Adam Darwish Daswira¹, Darwish Isyraf Mohamad
Helmy¹, Nuramin Fitri Bin Aminuddin^{1,2,3}

¹Centre for Foundation Studies (CFS), International Islamic University Malaysia (IIUM),
Malaysia

²Institute of Electrical and Electronics Engineers (IEEE), Malaysia

³Board of Engineers Malaysia (BEM), Malaysia

*azman.sutandaiman@live.iium.edu.my

ABSTRACT

The increasing reliance on single-factor attendance systems, such as Quick Response (QR) codes and Radio Frequency Identification (RFID), has enabled widespread proxy attendance in higher education institutions. This issue is supported by a survey of 250 respondents conducted at the Centre for Foundation Studies (CFS), International Islamic University Malaysia (IIUM) and Universiti Tun Hussein Onn Malaysia (UTHM), where 94% of respondents reported witnessing QR code sharing and 84% of lecturers suspected proxy attendance without verifiable proof. This work aims to develop an attendance system that eliminates proxy manipulation while maintaining real-time performance in high-volume academic environments. The proposed solution, Biometric And Smart Identification Reader (B.A.S.I.R.), integrates RFID-based identification with facial verification and liveness detection. The system utilizes DeepFace (Facenet512) for 1:1 facial matching and MediaPipe for Eye Aspect Ratio (EAR)-based blink detection to ensure user authenticity. To address latency issues commonly associated with biometric systems, multiprocessing is implemented to distribute computational tasks across multiple Central Processing Unit (CPU) cores, enabling continuous operation at 30 frames per second (fps). Experimental evaluation through a fraud simulation test demonstrates that B.A.S.I.R. reduces proxy success rates to 8.2%, compared to 89.5% for QR codes and 36.4% for standalone RFID systems. Authentication latency is reduced from over 5.0 seconds to 1.4 seconds per user, supporting high-throughput operation without queueing delays. In conclusion, B.A.S.I.R. achieves a 91.8% integrity rate while maintaining real-time performance and demonstrates strong commercial potential for secure attendance management.

Keywords: Dual-Factor Authentication, Facial Recognition, Multiprocessing, Proxy Attendance

1. INTRODUCTION

Attendance tracking is an essential component of academic administration, particularly in large classroom settings where manual verification is often impractical (Patel, 2025). As a result, institutions commonly adopt digital systems such as QR codes and RFID due to their efficiency and ease of implementation (Patel, 2025). However, these systems rely on single-factor authentication (Qureshi et al., 2025), where only the presence of a token is verified rather than the identity of the individual. This limitation allows proxy attendance to occur, where attendance is recorded by someone other than the actual student. A survey of 250 respondents conducted at the Centre for Foundation Studies (CFS), International Islamic University Malaysia (IIUM) and Universiti Tun Hussein Onn Malaysia (UTHM) indicates that this practice is widely observed among students, as shown in Figure 1. In addition, lecturers reported difficulty in verifying suspected cases due to the limitations of existing systems. These findings suggest that current approaches do not adequately support attendance integrity.

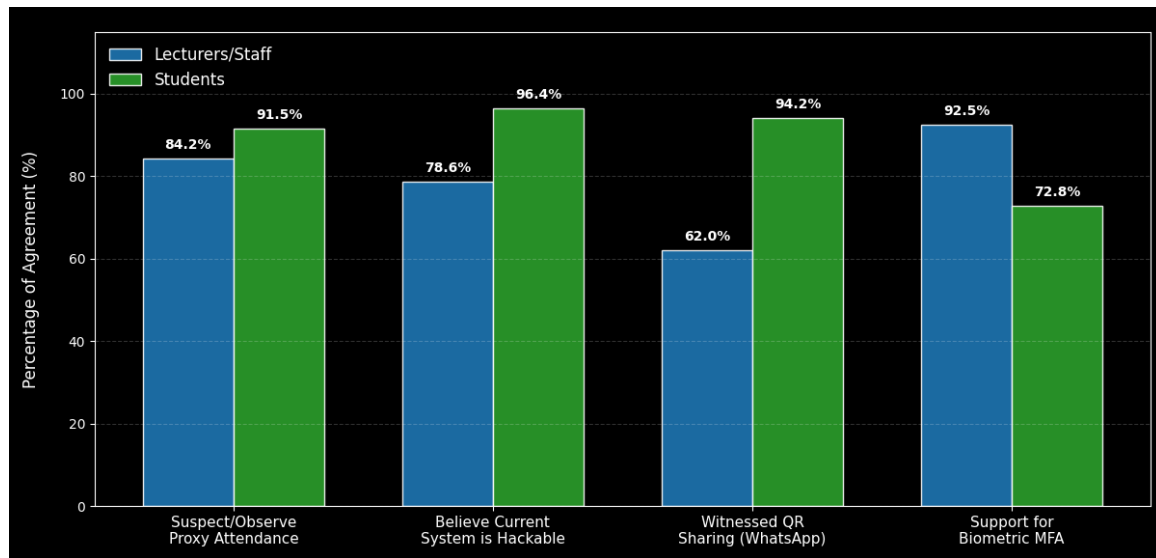


Figure 1. Data Source of B.A.S.I.R: Sample: n=250 respondents (CFS IIUM Gambang and UTHM Parit Raja).

Biometric technologies provide a more reliable alternative by verifying physical identity (Rjab et al., 2026). However, their use in classroom environments is often limited by processing delays, which can affect system usability when handling large numbers of users. To address this challenge, this work proposes the B.A.S.I.R., a dual-factor authentication system that integrates RFID-based identification with facial verification and liveness detection. By incorporating multiprocessing techniques, the system is designed to maintain continuous real-time performance while performing computationally intensive tasks. The objective is to improve attendance integrity without compromising efficiency in high-volume settings.

2. METHODOLOGY

The B.A.S.I.R system is developed as a biometric-based attendance verification framework designed to enhance integrity in academic attendance tracking. The system integrates hardware and software components to perform multi-factor authentication using RFID, facial recognition, and liveness detection.

2.1 System Architecture

The system utilizes an ESP32 microcontroller integrated with an RC522 RFID reader and a webcam module. These hardware components are responsible for initial user identification and

real-time image capture. The embedded system is connected to a Python-based backend framework that processes biometric authentication using computer vision and deep learning techniques. OpenCV is used for video stream handling and image preprocessing.

2.2 Dual-Factor Authentication Process

The authentication mechanism follows a two-step verification approach:

- i. **RFID Identification**
Each user is assigned a unique RFID tag. When scanned using the RC522 reader, the system retrieves the user's identity from a centralized database. This step ensures fast and preliminary identification of the user.
- ii. **Facial Verification**
After RFID validation, the webcam captures the user's facial image. A 1:1 facial recognition process is performed using DeepFace with the Facenet512 model. The system compares the live facial embedding with the stored template to verify identity based on similarity scoring. Only users who successfully pass both RFID and facial verification are allowed to proceed to the next stage.

2.3 Liveness Detection

To prevent spoofing attacks such as photo or video replay, liveness detection is implemented using MediaPipe. The system applies EAR analysis to detect natural eye blinking patterns. A valid live user must demonstrate dynamic facial behaviour within a defined threshold, ensuring that only real-time human presence is authenticated.

2.4 Real-Time Processing and Optimization

To achieve smooth real-time performance, the system employs multiprocessing techniques in Python. Computationally intensive tasks such as face detection, embedding extraction, and liveness evaluation are distributed across multiple CPU cores. This parallel processing architecture allows the system to maintain approximately 30 fps, ensuring minimal delay during authentication. OpenCV manages continuous frame capture, while buffering

mechanisms are implemented to avoid frame drop and latency issues during peak processing load.

2.5 Backend Integration and Data Logging

Once authentication is successful, the ESP32 transmits verified user data, including RFID ID and timestamp, to a Python-based backend server via API communication. The system records attendance data into a centralized database in real time. Each record includes the user identity-based RFID, facial recognition result, liveness detection status and timestamp of attendance. This structured logging ensures transparency, traceability, and audit readiness.

3. RESULTS AND DISCUSSION

The findings and discussions are described in detail in this section.

3.1 System Vulnerability and Fraud Success Rates

To evaluate system security, a fraud simulation test was conducted across 400 attempts. The results indicate that traditional methods are highly susceptible to bypass, with Static QR Codes showing the highest fraud success rate at 89.5%. Manual signing and RFID-only systems followed with success rates of 48.2% and 36.4%, respectively. In contrast, the B.A.S.I.R. MFA system significantly reduced the fraud success rate to only 8.2%, demonstrating its effectiveness in preventing proxy logins.

3.2 Anti-Spoofing Effectiveness and Processing Optimization

The system proved highly resilient against static attacks, showing a 0.0% success rate for printed photos and 2.0% for digital photos. More sophisticated attacks, such as video playback and digital masks, yielded success rates of 8.0% and 10.0%, respectively. Efficiency was also benchmarked using serial versus multiprocessing optimization. By isolating heavy Facenet512 calculations to secondary CPU cores, the B.A.S.I.R. system reduced peak processing time from 2.8 seconds to 0.6 seconds per student. This optimization ensures the system remains scalable for high-traffic institutional use while maintaining rigorous biometric verification.

4. CONCLUSION

The B.A.S.I.R. system successfully integrates RFID, facial recognition, and liveness detection to provide a secure and reliable attendance verification solution. The multi-factor approach significantly reduces proxy attendance and spoofing risks while maintaining real-time performance through multiprocessing and optimized image processing. For future work, improvements such as cloud integration for large-scale deployment, and mobile support are recommended to enhance robustness and scalability.

ACKNOWLEDGEMENT

The authors express their sincere appreciation to the CFS, IIUM for providing funding and facilities for this research. Appreciation is also extended to UTHM for their collaboration and support during data collection.

REFERENCES

- Patel, P. (2025). Revolutionizing academic management: A digital approach to location-based QR attendance system and mobile application integration for lecture and laboratory oversight. *International Conference on Data Management, Analytics & Innovation*. Springer Nature Singapore.
- Qureshi, I., Kale, V., & Tharewal, S. (2025). Enhancing multifactor authentication with machine learning: A comprehensive framework for robust user verification. Atlantis Press. https://doi.org/10.2991/978-94-6463-738-0_52
- Rjab, I., & Sliman, L. (2026). Survey on biometric authentication for decentralized identity management: Trends, challenges, and future directions. *Future Internet*, 18(3), 122-126.