Edge AI-Based Multimodal Biometric Smart Reader Using YOLOv8 for Integrated Academic Attendance Systems

Nurhadi[1*], Emil Naf'an[2], Desyanti[3], Mustazzihim Suhaidi[4]
[1]*Digital Business, Institut Teknologi dan Bisnis Riau Pesisir, Dumai, Indonesia*
[2]*Faculty of Computer Science, Universitas Putra Indonesia YPTK Padang, Padang, Indonesia*
[3,4]*Informatics Engineering, Institut Teknologi dan Bisnis Riau Pesisir, Dumai, Indonesia*
*corr-author: nurhadi@itbriaupesisir.ac.id

Abstract - Attendance systems in vocational education institutions face challenges related to accuracy, security, and susceptibility to manipulation due to the use of single-modality authentication methods. RFID-based systems are vulnerable to card sharing, fingerprint systems suffer from latency during peak usage, and face recognition systems are sensitive to illumination and pose variations. This study proposes an Edge AI-based multimodal biometric smart reader integrating RFID, fingerprint, and YOLOv8-based face recognition for an academic attendance system at SMK Negeri 1 Dumai. The system is implemented on NVIDIA Jetson Nano as an edge computing device and integrated with an academic information system through an IoT-based architecture for real-time attendance monitoring. A decision-level fusion approach using majority voting is applied, where authentication is accepted if at least two of three modalities match. The system is evaluated using accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), and response time. Experimental results show that the proposed multimodal system achieves an accuracy of 98.72%, outperforming RFID (89.34%), fingerprint (92.15%), and YOLOv8 face recognition (95.63%). The system also reduces FAR to 0.82% and FRR to 0.91%, with an average response time of 1.47 seconds, making it suitable for real-time deployment. Overall, the proposed Edge AI-based multimodal biometric system demonstrates high accuracy, improved security, and efficient real-time performance, providing a scalable solution for intelligent attendance systems in vocational education environments.

Keywords: Edge AI; YOLOv8; multimodal biometrics; smart attendance; face recognition.

I. INTRODUCTION

Attendance monitoring plays a crucial role in improving discipline, academic performance, and administrative efficiency in educational institutions, particularly in vocational schools where practical learning activities require strict time management. However, conventional attendance systems still face several challenges, including low accuracy, susceptibility to manipulation, and limited integration with academic information systems. Manual attendance recording is prone to human error, while RFID-based systems allow proxy attendance due to card delegation [1,2,3]. Fingerprint-based authentication improves reliability but introduces delays and hygiene concerns, especially during peak attendance periods [4,5,6]. Single-modality face recognition systems, although contactless, are often affected by illumination variation, pose changes, and occlusion, leading to false acceptance and rejection [7,8,9].

Recent advancements in artificial intelligence and computer vision have enabled the development of intelligent attendance systems using deep learning-based face recognition [10,11,12]. Object detection models such as YOLO have demonstrated high performance for real-time face detection tasks. The latest YOLOv8 architecture provides improved accuracy, reduced computational complexity, and faster inference speed, making it suitable for deployment in edge computing environments [2,13,14]. Edge AI enables on-device processing, reducing latency and dependency on cloud infrastructure while improving data privacy and system reliability. Despite these advantages, most existing attendance systems still rely on single biometric modalities, which limits authentication robustness [15,16,17].

Multimodal biometric authentication has emerged as a promising solution to improve identification accuracy and system security. By combining multiple biometric modalities such as RFID, fingerprint, and face recognition, multimodal systems can reduce False Acceptance Rate (FAR) and False Rejection Rate (FRR). Decision-level fusion techniques allow the system to validate identities based on multiple matching criteria, minimizing authentication errors [1,8,18]. However, previous studies mainly focus on either cloud-based systems or single biometric approaches, and limited research integrates multimodal biometrics with edge AI and academic information systems in vocational education environments [9,19,20].

Limited synchronization with academic databases causes reporting delays and data inconsistencies in attendance systems. This study proposes an Edge AI-based multimodal biometric smart reader integrating RFID, fingerprint, and YOLOv8 face recognition. Implemented on NVIDIA Jetson Nano with IoT-based academic system integration, the proposed system was evaluated at SMK Negeri 1 Dumai. The multimodal authentication mechanism uses decision-level fusion to enhance accuracy, reduce authentication errors, and prevent attendance manipulation [21,22,23].

The main contributions of this study focus on the development of an Edge AI-based multimodal biometric smart reader for academic attendance systems. The proposed system implements YOLOv8-based real-time face recognition deployed on embedded edge computing hardware to ensure fast and reliable identification. In addition, the system integrates RFID, fingerprint, and face recognition using a decision-level fusion authentication approach to enhance accuracy and reduce authentication errors. Furthermore, real-time integration with academic information systems is developed through an IoT-based architecture, enabling automatic synchronization of attendance data. The proposed system is deployed and evaluated in a real vocational school environment to assess its effectiveness under practical conditions. The experimental results demonstrate improved attendance accuracy while reducing False Acceptance Rate, False Rejection Rate, and response time [15,24,25]. The proposed approach provides a scalable, reliable, and secure smart attendance solution that improves attendance accuracy, enhances security, and supports integrated attendance monitoring in vocational education.

II. METHOD

This study adopts the Design Science Research (DSR) methodology to develop and evaluate an Edge AI-based multimodal biometric smart reader. The research includes problem identification, requirement analysis, system design, implementation, and evaluation, with validation conducted at SMK Negeri 1 Dumai.

A. System Architecture

The system proposed in this study implements a multimodal biometric authentication approach that integrates multiple identification sources, namely RFID, fingerprint, and image-based facial recognition [26, 27, 28]. The verification process enhances attendance accuracy and reliability through YOLOv8-based face detection and feature extraction. The overall workflow is shown in Fig. 1.

Based on the flow in Fig. 1, the process begins with reading an RFID card as the initial identification, followed by fingerprint scanning and capturing the user's facial image. The facial image is then processed using the YOLOv8 method for face detection, followed by feature extraction and data matching [15,29,30]. Next, the system performs multimodal decision fusion to determine the validity of attendance based on a minimum of two biometric matches. If the criteria are met, the attendance data is declared valid and sent to the Academic Information System. If it does not meet the threshold, the system will display a rejection status or ask the user to repeat the authentication process [31].

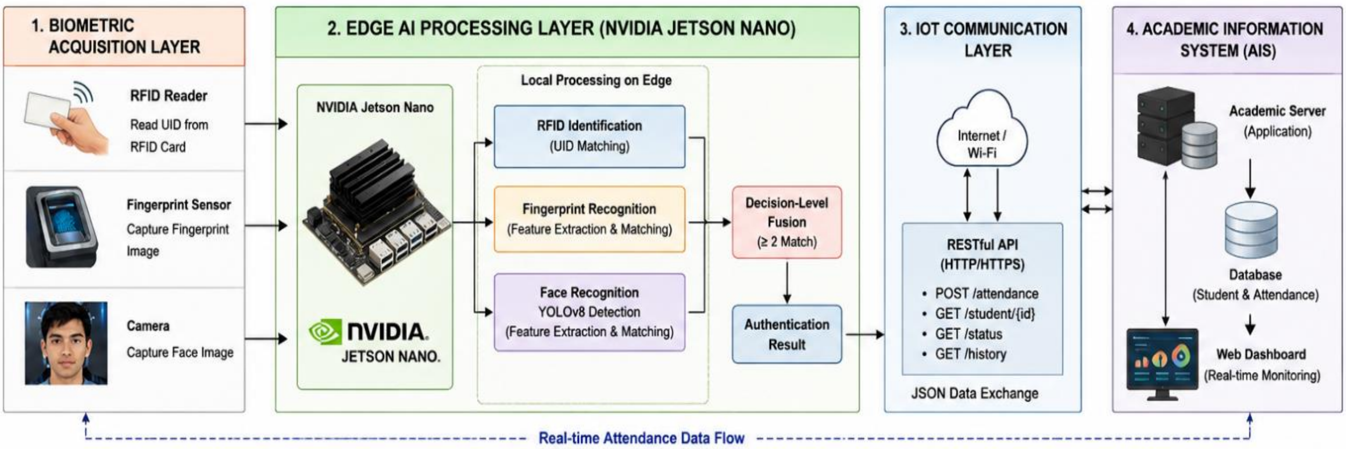

Fig. 1 Flowchart of the proposed Edge AI-based multimodal biometric authentication system

B. Multimodal Biometric Authentication Model

The proposed system implements a multimodal biometric authentication approach by combining three identification modalities: Radio Frequency Identification, fingerprint recognition, and facial recognition using the YOLOv8 model. The integration of these three modalities aims to improve authentication accuracy and minimize false acceptance and false rejection errors [15,24]. At the decision-making stage, a decision-level fusion strategy using the majority voting method is used. An authentication process is declared valid if at least two of the three modalities match the registered user's identity. This approach provides greater system resilience against failure of any one modality. The proposed multimodal biometric architecture operates using a parallel authentication mechanism rather than a sequential approach. Each biometric modality including RFID, fingerprint, and YOLOv8-based face recognition independently performs feature extraction and identity verification simultaneously. The modality outputs are fused through decision-level majority voting, enhancing authentication robustness, fault tolerance, and reliability. Mathematically, the decision function is expressed as in (1).

$$M = \{\mathrm{RFID}, \mathrm{FP}, \mathrm{Face}\} \tag{1}$$

where M is the set of authentication modalities used, namely $RFID$, $fingerprint\,(FP)$, and $Facial\ recognition$. The authentication decision is determined based on the number of matches for each modality, which is formulated as in (2).

$$\sum_{i=1}^{3} \mathrm{Match}_i \geq 2 \tag{2}$$

with $Match_i \in \{0,1\}$ where a value of 1 indicates that the nth modality successfully matches the user's identity, and a value of 0 indicates a mismatch. Thus, authentication is considered valid if at least two of the three modalities produce a match. To improve authentication accuracy and security, this study proposes a multimodal biometric system integrating RFID, fingerprint, and deep learning-based face recognition. The extracted features are fused at the decision level, as shown in Fig. 2.

Based on Fig. 2, each modality produces identification output independently after the feature extraction process, where face detection is performed using YOLOv8, while RFID and fingerprint use their respective reader sensors. Next, all identification results are combined in the decision-level fusion stage and evaluated using the majority voting method to determine the final authentication status [22,32,33].

C. YOLOv8-Based Face Recognition

The face recognition module uses YOLOv8 to provide accurate and low-latency detection on NVIDIA Jetson Nano. Real-time facial images are captured and processed for face detection and localization. Following detection, the system performs feature extraction to transform the visual data into high-dimensional facial embeddings [34]. The extracted facial features are matched with enrolled templates using cosine similarity or Euclidean distance. Identity verification is performed based on a predefined similarity threshold, providing reliable input for the multimodal decision-level fusion. The similarity is computed as in (3).

$$\mathrm{Sim}(x, y) = \frac{\sum_{i=1}^{n} xi \cdot yi}{\sqrt{\sum_{i=1}^{n} x_i^2}\ \sqrt{\sum_{i=1}^{n} y_i^2}} \tag{3}$$

where $x \cdot y$ denotes the dot product operation between the facial feature vectors, while $\| x \| \times \| y \|$ represents the multiplication of the Euclidean magnitudes (norms) of both vectors used for cosine similarity normalization. The arithmetic operator "×" in the denominator is explicitly added to ensure mathematical correctness and clarity of the implemented similarity computation.

D. IoT-Based System Integration

The proposed architecture integrates the Academic Information System (AIS) via IoT-based communication using RESTful APIs and JSON to enable efficient data exchange. This integration facilitates real-time attendance synchronization, enabling a seamless flow of data from edge devices to a centralized database [35,36,37]. To maintain system integrity, the framework incorporates a secure communication protocol for all data exchanges between the Jetson Nano and the server [26,38]. A web-based dashboard enables real-time attendance monitoring and automatic record logging for administrative auditing.

E. *Dataset* and Experimental Setup

The proposed system is evaluated using a dataset consisting of 80 subjects (60 students and 20 staff) through 200 authentication attempts under varying lighting conditions, facial poses, and time of day. Experiments are designed to evaluate the system's accuracy and response time in a realistic academic environment as shown in Table I.

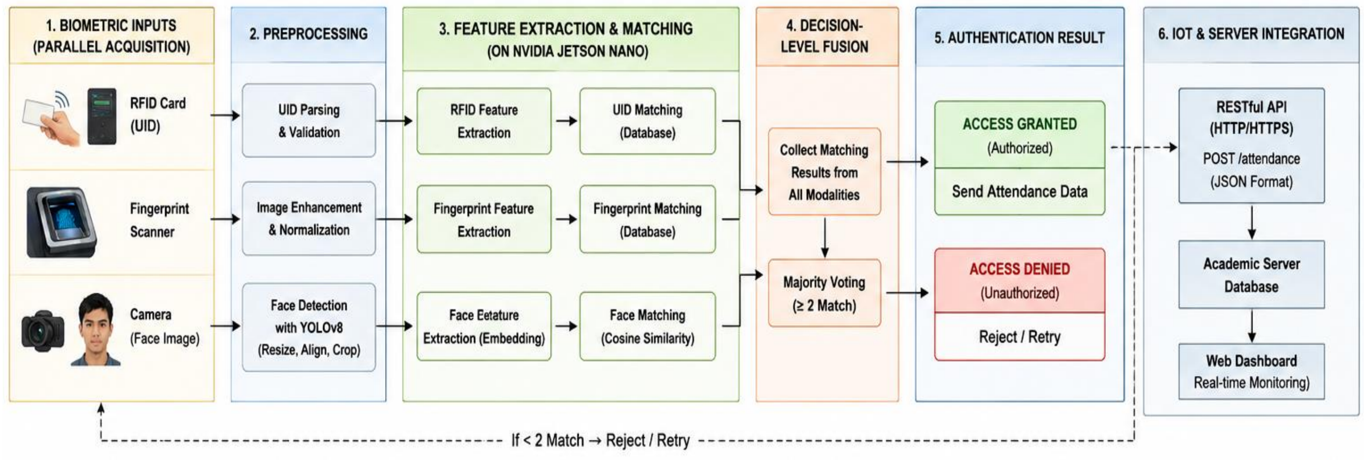

Fig. 2 System architecture of the proposed multimodal biometric authentication system

TABLE I
DATASET COMPOSITION AND EXPERIMENTAL SCENARIOS

No	Experimental Scenario	Authentication Instances	Category	Description
1	Controlled Lighting Condition	60	Controlled	Face acquisition under stable indoor illumination
2	Low Lighting Condition	30	Uncontrolled	Reduced illumination affecting facial visibility
3	Pose Variation	40	Uncontrolled	Different head orientations and viewing angles
4	Morning Attendance	35	Controlled	Authentication performed before 12:00 PM
5	Afternoon Attendance	35	Controlled	Authentication performed after 12:00 PM
6	Partial Facial Occlusion	20	Uncontrolled	Presence of glasses, masks, or partial face obstruction
	Total Authentication Instances	200		

The experimental dataset consists of 200 authentication instances collected under both controlled and uncontrolled operational scenarios to simulate realistic academic attendance conditions. Controlled scenarios include stable indoor lighting and scheduled attendance sessions, while uncontrolled scenarios involve illumination variation, pose changes, and partial facial occlusion. The dataset was designed to evaluate system robustness under diverse conditions. Performance was assessed using Accuracy, FAR, FRR, and the corresponding TP, TN, FP, and FN values derived from the authentication results.

F. Performance Evaluation Metrics

System performance was evaluated using four metrics to measure biometric authentication accuracy and computational efficiency.

1) Identification Accuracy: Accuracy is the fundamental metric used to determine the overall correctness of the system in identifying authorized and unauthorized individuals [4,39,40]. It is calculated as the ratio of correct predictions to the total number of authentication attempts with (4). This equation represents the system's overall effectiveness in classifying data. A high accuracy value indicates the model's ability to accurately distinguish between authorized and unauthorized users in the school environment.

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \quad (4)$$

2) False Acceptance Rate (FAR): In a security context, FAR represents the probability that the system incorrectly authorizes an unregistered or unauthorized user [15,25,27]. A lower FAR is critical for ensuring system integrity against spoofing or intrusion as in (5). False Acceptance Rate (FAR) measures the probability of incorrectly granting access to unauthorized users. Lower FAR values indicate higher system security.

$$FAR = \frac{FP}{FP+TN} \quad (5)$$

3) False Rejection Rate (FRR): FRR quantifies the likelihood that the system fails to recognize a legitimate user [15,25]. Monitoring the FRR is essential to ensure user convenience and operational efficiency within the school environment as in (6). The FRR measures the system's failure rate in recognizing legitimate registered users. A low FRR is crucial in student attendance systems to ensure smooth operations and avoid long queues due to repeated identity rejections.

$$FRR = \frac{FN}{FN+TP} \quad (6)$$

4) System Response Time: Beyond biometric precision, the temporal efficiency of the system is evaluated to ensure real-time performance on edge devices [21,41,42]. The total response time (T) is defined as the duration between the initial sensor input ($t\_\{input\}$) and the final decision output ($t\_\{output\}$), encompassing detection, extraction, and fusion processes with (7). This metric evaluates the system's real-time computing performance. Response time (T) encompasses the total processing time from data acquisition by sensors to sending decision results to the Academic Information System (AIS). This is highly dependent on the optimization of the YOLOv8 algorithm on the Jetson Nano edge device.

$$\mathrm{T} = \mathrm{t_{output}} - \mathrm{t_{input}} \quad (7)$$

G. Evaluation

The evaluation of the proposed system is executed through a systematic three-stage experimental framework to validate its robustness and accuracy. The procedure is structured as follows:

1) Unimodal Performance Assessment: RFID, fingerprint, and YOLOv8-based face recognition were independently evaluated to establish baseline performance in terms of Accuracy, FAR, and FRR [19,25,43].

2) Multimodal Integration and Fusion Testing: The second stage evaluates the performance of the integrated system utilizing the Decision Level Fusion strategy. This test assesses the effectiveness of the majority voting logic in synthesizing outputs from multiple sensors [6,9,37]. The evaluation assesses how multimodal fusion improves authentication reliability under environmental and physiological variations.

3) Comparative Empirical Analysis: The final stage involves a comprehensive comparative analysis between the unimodal results and the multimodal outcomes [21].

III. RESULT AND DISCUSSION

This section presents the performance evaluation of the proposed Edge AI-based multimodal biometric smart reader. The proposed method is compared with RFID, fingerprint, and YOLOv8-based face recognition using Accuracy, FAR, FRR, and response time to demonstrate its effectiveness in academic environments.

A. System Implementation

The proposed Edge AI-based multimodal biometric smart reader was successfully implemented at SMK Negeri 1 Dumai. The system integrates RFID, fingerprint, and YOLOv8-based face recognition on the NVIDIA Jetson Nano, where authentication is performed through decision-level fusion and synchronized with the academic information system via IoT. A web-based dashboard enables real-time attendance monitoring, while local edge processing ensures low latency, data privacy, and operational efficiency. The system implementation is illustrated through the Graphical User Interface shown in Fig. 3. As shown in Fig. 3, the system automatically authenticates users, records attendance, and synchronizes the data with the centralized database in real time.

B. Performance Evaluation Results

1) Accuracy Comparison: Table II compares the accuracy of each authentication modality and the proposed multimodal approach. As shown in Table II, the proposed multimodal approach outperforms single-modality methods in accuracy, improving authentication reliability and robustness.

2) FAR and FRR Analysis: Table III compares the False Acceptance Rate (FAR) and False Rejection Rate (FRR) of all authentication methods. As shown in Table III, the proposed multimodal approach achieves the lowest FAR and FRR, indicating superior security and reliability over single-modality methods.

Fig. 3 Graphical user interface of the proposed smart attendance system

TABLE II
ACCURACY COMPARISON

No	Method	Accuracy (%)
1	RFID	89.34
2	Fingerprint	92.15
3	Face Recognition (YOLOv8)	95.63
4	Multimodal	98.72

TABLE III
FAR AND FRR COMPARISON

No	Method	FAR (%)	FRR (%)
1	RFID	5.20	4.10
2	Fingerprint	3.10	2.80
3	Face Recognition (YOLOv8)	2.40	2.20
4	Multimodal	0.82	0.91

3) Response Time Analysis: Table IV compares the response time of all authentication methods, including the proposed multimodal approach. Table IV shows that RFID provides the fastest response time, whereas the proposed multimodal approach incurs slightly higher latency due to multimodal fusion. However, its average response time of 1.47 s remains suitable for real-time attendance applications (Fig. 4). As shown in Fig. 4, the proposed multimodal approach improves accuracy while reducing FAR and FRR, with response time remaining within real-time requirements.

C. System Integration Result

The proposed system integrates with the Academic Information System (AIS) for real-time attendance recording and monitoring. Authentication data are automatically synchronized with the academic database, and the integration performance is presented in Table V.

TABLE IV
RESPONSE TIME COMPARISON

No	Method	Response Time (s)	Description
1	RFID	0.70	Fastest single-modality authentication due to simple tag reading process
2	Fingerprint	1.00	Moderate processing time due to feature extraction and matching process
3	Face Recognition (YOLOv8)	1.20	Higher processing time caused by deep learning inference on image frames
4	Multimodal	1.47	Combined processing of RFID, fingerprint, and face recognition with fusion mechanism

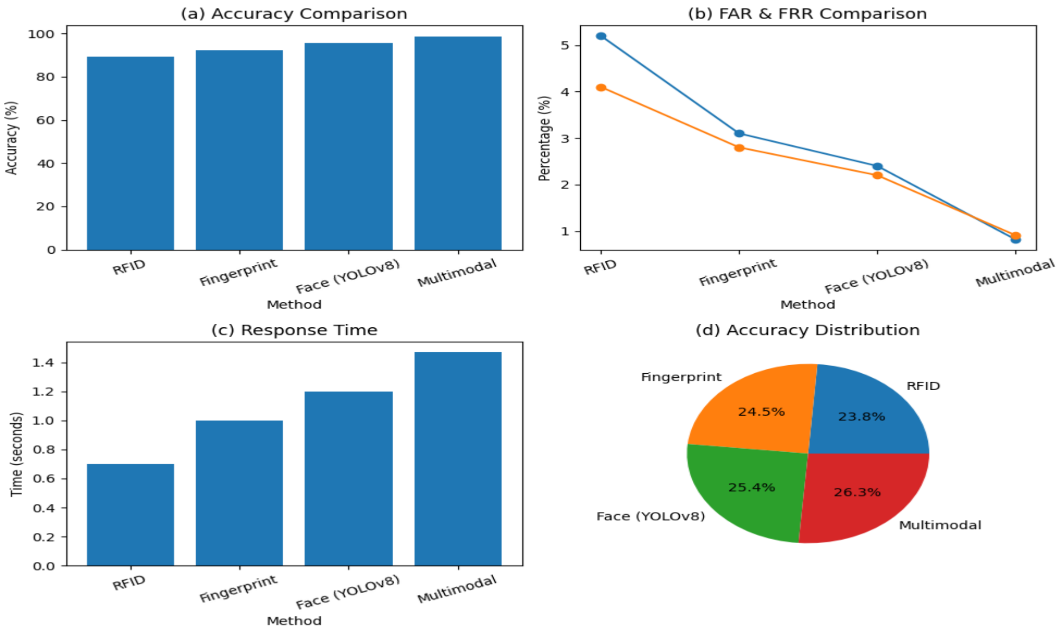

Fig. 4 Performance comparison of biometric authentication methods: (a) Accuracy, (b) FAR and FRR, (c) Response time, and (d) Accuracy distribution

TABLE V
SYSTEM INTEGRATION PERFORMANCE OVERVIEW

No	Feature	Status	Description
1	Real-time Attendance Update	Active	Attendance is updated instantly after successful authentication
2	Centralized Database Storage	Active	All attendance data stored in a unified academic database
3	Web-based Monitoring Dashboard	Active	Provides real-time visualization of attendance records
4	Automated Reporting	Active	Generates attendance reports automatically based on system logs
5	Multi-device Accessibility	Active	System can be accessed via desktop and mobile devices

Table V confirms the successful integration of the proposed system with the Academic Information System (AIS). The data synchronization performance is further evaluated in Table VI using latency, transmission success rate, system availability, and database write accuracy.

Table VI shows reliable data synchronization, characterized by low latency, high transmission success, accurate database writing, and 99.2% system availability. The normalized performance comparison is presented in Fig. 5.

As shown in Fig. 5, the proposed multimodal system achieves higher accuracy with lower FAR and FRR than single-modality methods while maintaining acceptable response time. The relationship among Accuracy, FAR, and response time is further analyzed in Fig. 6.

Fig. 6 indicates a strong negative correlation between Accuracy and FAR. Z-score normalization was applied to standardize the performance metrics, and the results are presented in Fig. 7.

As shown in Fig. 7, the proposed multimodal system consistently achieves higher Z-score values than single-modality methods, indicating superior standardized performance.

TABLE VI
DATA SYNCHRONIZATION PERFORMANCE

No	Parameter	Value	Unit	Description
1	Average Sync Latency	320	milliseconds (ms)	Time required to synchronize attendance data between the Edge AI device and the academic server
2	Data Transmission Success	99.6	%	Successful data transfer rate
3	System Uptime	99.2	%	Availability of system during operation
4	Database Write Success Rate	99.8	%	Accuracy of data recording process

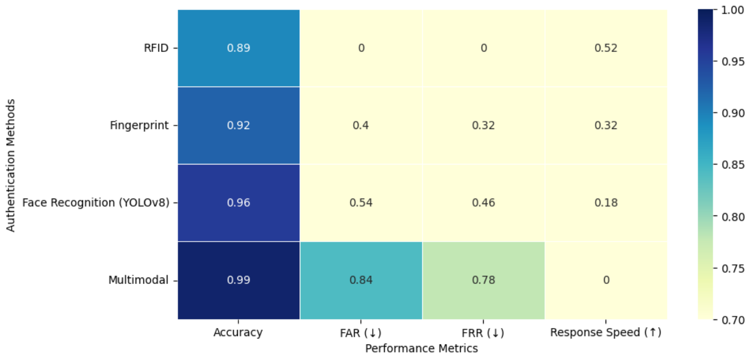

Fig. 5 Performance comparison of biometric authentication methods

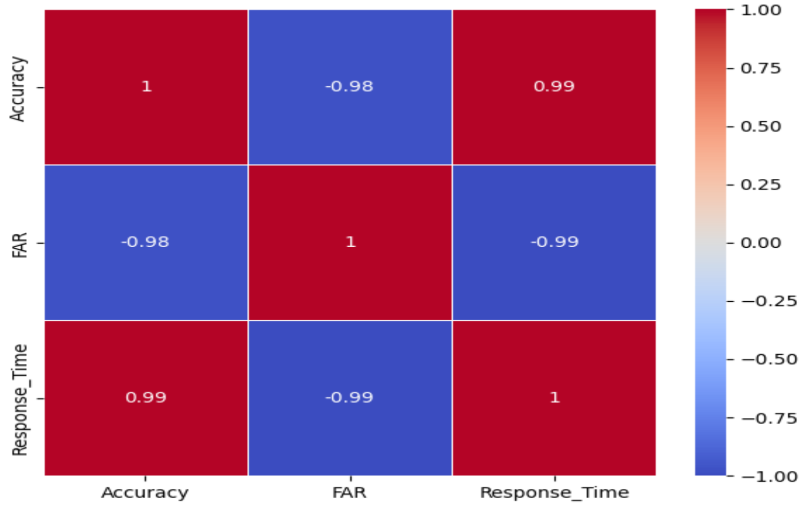

Fig. 6 Correlation matrix of biometric authentication performance metrics

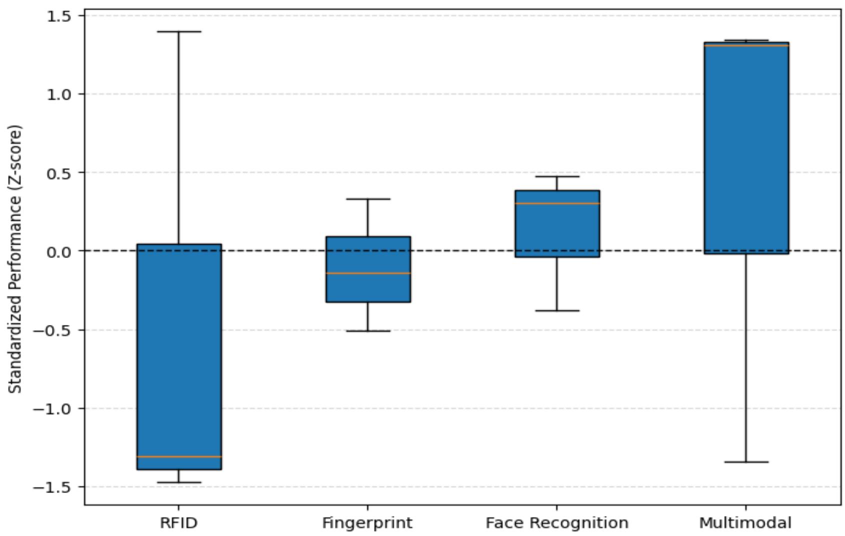

Fig. 7 Z-score normalized comparison of biometric authentication methods

D. Experimental Results

The proposed Edge AI-based multimodal biometric smart reader significantly outperforms single-modality methods by achieving 98.72% accuracy, 0.82% FAR, and 0.91% FRR, while maintaining a real-time response of 1.47 s. Statistical analysis (one-way ANOVA, $p < 0.05$) confirms the significance of these improvements, and Z-score normalization further demonstrates consistently superior performance. These results indicate that integrating RFID, fingerprint, YOLOv8-based face recognition, and Edge AI provides a reliable, secure, and efficient attendance system for smart educational environments.

Although the proposed multimodal system introduces a higher response time compared to single-modality authentication, the observed latency remains acceptable for real-time academic attendance applications. The increased response time primarily originates from the computational overhead associated with deep learning inference using YOLOv8, multimodal feature extraction, and decision-level fusion processing on the NVIDIA Jetson Nano platform. Face recognition contributes the highest computational load due to image preprocessing, facial embedding generation, and similarity matching operations.

Nevertheless, the deployment of Edge AI significantly reduces overall latency compared to conventional cloud-based architectures because all inference operations are executed locally on the embedded device without requiring continuous internet-based processing. Furthermore, the multimodal fusion mechanism substantially improves authentication reliability, resulting in significantly lower FAR and FRR values. Therefore, the additional processing time represents a practical trade-off between computational complexity and biometric security enhancement. Compared to previous studies utilizing single biometric modalities, the proposed system demonstrates superior authentication robustness while maintaining acceptable operational responsiveness for vocational education environments. These findings confirm that the integration of multimodal biometrics with Edge AI architecture provides an effective balance between security, accuracy, and real-time performance.

IV. CONCLUSION

This study successfully proposes and implements an Edge AI-based multimodal biometric smart reader using YOLOv8 for an integrated academic attendance system at SMK Negeri 1 Dumai. The system combines RFID, fingerprint, and face recognition through a decision-level fusion mechanism to enhance authentication reliability and prevent attendance manipulation. The integration of YOLOv8 on embedded edge computing (Jetson Nano) enables real-time face detection and recognition with low latency and high efficiency. Experimental results demonstrate that the proposed multimodal approach achieves a high accuracy of 98.72%, significantly outperforming single-modality methods. In addition, the system effectively reduces False Acceptance Rate (FAR) to 0.82% and False Rejection Rate (FRR) to 0.91%, while maintaining an average response time of 1.47 seconds, making it suitable for real-time deployment in educational environments. Future work will focus on expanding the system with cloud-based analytics, mobile application integration, and larger-scale deployment to further improve system performance and usability. Future research will focus on optimizing computational efficiency through lightweight YOLO architectures, TensorRT acceleration, and edge-cloud collaborative inference to further reduce system latency. In addition, future studies may explore adaptive multimodal fusion strategies, liveness detection mechanisms, and large-scale deployment across multiple educational institutions to improve scalability, robustness, and security against spoofing attacks.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to Vocational High School 1 Dumai for the opportunity, facilities, and support provided to conduct this research. The authors also acknowledge the support of the Research Grant from the Ministry of Higher Education, Science, and Technology - Under the Research Scheme: Applied Research Model Outputs in 2025.

REFERENCES

[1] N. A S, “IoT Based Smart Attendance Management System,” *Interantional J. Sci. Res. Eng. Manag.*, vol. 08, no. 03, pp. 1–11, 2024, doi: 10.55041/ijsrem29283.

[2] K. P. Hasaraddi, G. Thambkar, A. P. Bidargaddi, A. P. Patil, and G. Betageri, “YOLOv8-Enhanced Facial Recognition for One-Shot Learning Attendance System,” *2024 5th Int. Conf. Emerg. Technol. INCET 2024*, vol 1, no. 2, pp. 1–7, 2024, doi: 10.1109/INCET61516.2024.10593178.

[3] A. Aljohnai, R. E. Al-Mamlook, and N. Alharbe, “Ai-Based Attendance Management System Using Image Processing Techniques During Covid-19 Pandemic,” *ICIC Express Lett.*, vol. 16, no. 12, pp. 1287–1299, 2022, doi: 10.24507/icicel.16.12.1287.

[4] A. S. Lateef and M. Y. Kamil, “Face Recognition-Based Automatic Attendance System in a Smart Classroom,” *Iraqi J. Electr. Electron. Eng.*, vol. 20, no. 1, pp. 37–47, 2024, doi: 10.37917/ijeee.20.1.4.

[5] O. Faruque, F. H. Siddiqui, and S. B. Noor, “Face Recognition-Based Mass Attendance Using YOLOv5 and ArcFace,” *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST*, vol. 490 LNICST, no. 1, pp. 496–510, 2023, doi: 10.1007/978-3-031-34619-4_39.

[6] K. Alkanan, Y. Zhong, X. Luo, and R. Dong, “Advanced multimodal biometric authentication for IoT-enabled smart home security: Integrating deep learning-based face recognition with behavioral patterns,” *Kuwait J. Sci.*, vol. 53, no. 2, p. 100548, 2026, doi: 10.1016/j.kjs.2026.100548.

[7] M. Fikry, M. Ula, M. Yani, and A. Anugrah Pohan, “Performance Analysis of Smart Technology with Face Detection using YOLOv3 and InsightFace for Student Attendance Monitoring,” *Orig. Res. Pap. Int. J. Intell. Syst. Appl. Eng. IJISAE*, vol. 2024, no. 4, pp. 3490–3499, 2024, [Online]. Available: www.ijisae.org, doi: https://ijisae.org/index.php/IJISAE/article/view/6865.

[8] X. Zhang, Y. Ding, X. Huang, W. Li, L. Long, and S. Ding, “Smart Classrooms: How Sensors and AI Are Shaping Educational Paradigms,” *Sensors*, vol. 24, no. 17, 2024, doi: 10.3390/s24175487.

[9] S. Almuwayziri, A. Al-Nafjan, H. Aljumah, and M. Aldayel, “Deep Learning-Based Fingerprint–Vein Biometric Fusion: A Systematic Review with Empirical Evaluation,” *Appl. Sci.*, vol. 15, no. 15, pp. 1–22, 2025, doi: 10.3390/app15158502.

[10] N. Ammour, Y. Bazi, and N. Alajlan, “Multimodal Approach for Enhancing Biometric Authentication,” *J.*

Imaging, vol. 9, no. 9, 2023, doi: 10.3390/jimaging9090168.

[11] Y. Darmi, A. S. Utama, D. Abdullah, M. Marhalim, R. Rizky, and D. A. Lima, "A Multi-Modal IoT-Based Attendance System Using RFID and WhatsApp Notification for Smart Academic and Healthcare Environments," *J. Intell. Comput. Heal. Informatics*, vol. 6, no. 1, p. 36, 2025, doi: 10.26714/jichi.v6i1.17283.

[12] S. Rastogi, S. Kumar, and M. Ali, "Sequential Multimodal Biometric Authentication Fusion System," *Mathematics*, vol. 01, no. 2, pp. 1–24, 2026, doi: https://doi.org/10.3390/math14071178.

[13] S. Qiang, "Towards the Classroom of the Future: Improvement Strategies for Automatic Attendance Systems Using Facial Recognition Combining Behavioral Recognition," in *Proceedings of the 2024 International Conference on Artificial Intelligence and Communication (ICAIC 2024),* Atlantis Press International BV, 2024, vol. 1, no.1, pp. 627–637. doi: 10.2991/978-94-6463-512-6_66.

[14] E. Utami, E. Syahrudin, A. D. Hartanto, and S. Raharjo, "A Multispectral YOLOv8-Based System for Real- Time Object Detection and Distance Estimation in Blind Navigation," *JUITA J. Inform.*, vol. 14, no. 1, pp. 133–144, 2026.

[15] B. K. Putra, A. G. Putrada, and I. D. Oktaviani, "YOLOv8 and FaceNet Algorithm for Real-Time Face Recognition Attendance System," *Proc. 2025 IEEE Int. Symp. Futur. Telecommun. Technol. SOFTT 2025*, vol. 01, no. 01, pp. 401–406, 2025, doi: 10.1109/SOFTT67007.2025.11213461.

[16] M. B. Thakur, "A Systematic Review On Smart Attendance System Leveraging Deep Learning-Based Face Recognition Techniques," *IOSR J. Comput. Eng.*, vol. 27, no. 4, pp. 80–86, 2025, doi: 10.9790/0661-2704048086.

[17] M. V. S. Pavankumar and B. Balaji, "Face Authentication Using Yolov8 and Facenet," *Int. J. Sci. Res. Eng. Dev.*, vol. 8, no. 3, pp. 1527–1532, 2025.

[18] V. V Panchbhai, O. D. Waghmare, P. D. Tijare, M. H. Bhoyar, and V. Patle, "Smart Attendance System: An Internet of Things (IoT)-Enabled Concept," *Cureus J. Comput. Sci.*, vol. 03, no. 1, pp. 1–15, 2024, doi: 10.7759/s44389-024-00164-z.

[19] K. Jha, A. Jain, and S. Srivastava, "Feature-level fusion of face and speech based multimodal biometric attendance system with liveness detection," *AIP Adv.*, vol. 14, no. 11, 2024, doi: 10.1063/5.0234430.

[20] M. Idris, R. Wijaya, T. Agung, and B. Wirayuda, "Employee Attendance System Based on Face Recognition and Liveness Detection Using," *IND. J. Comput.*, vol. 10, no. 2, February, pp. 32–43, 2026, doi: 10.21108/indojc.v10i2.10294.

[21] Y. I. Hamodi Aljanabi, M. F. Mahdi, S. I. Hadi, S. K. Shnain, I. Abbas, and S. S. Maidin, "Energy-Aware Multimodal Biometric Authentication Systems for Mobile," *Int. J. Eng. Sci. Inf. Technol.*, vol. 5, no. 1, pp. 516–525, 2025, doi: 10.52088/ijesty.v5i1.1356.

[22] J. S. Mane, S. Bhosale, and S. Urooj, "A Deep Learning-Based Multimodal Biometric Authentication Framework Using Fingerprint and Iris with Score-Level Fusion," *Ing. des Syst. d'Information*, vol. 30, no. 12, pp. 3217–3224, 2025, doi: 10.18280/isi.301214.

[23] P. M. Than and H. Nguyen, "Efficient Multimodal Biometric Identification via Gabor-Enhanced Attention Networks," *J. Robot. Control*, vol. 6, no. 3, pp. 1175–1186, 2025, doi: 10.18196/jrc.v6i3.26490.

[24] O. Oloniyo, F. D. Samuel, and A. Fredrick, "Design of a Multimodal Attendance System Using RFID, Face Recognition, Fingerprint Biometric, and GSM Notification," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 8, pp. 1266–1275, 2025, doi: 10.38124/ijisrt/25aug720.

[25] U. Sumalatha, K. Prakasha, S. Prabhu, and V. C. Nayak, "Multimodal biometric authentication: a novel deep learning framework integrating ECG, fingerprint, and finger knuckle print for high-security applications," *Eng. Res. Express*, vol. 7, no. 1, 2025, doi: 10.1088/2631-8695/ad9aa0.

[26] P. P. Oroceo, J. I. Kim, E. M. F. Caliwag, S. H. Kim, and W. Lim, "Optimizing Face Recognition Inference with a Collaborative Edge–Cloud Network," *Sensors*, vol. 22, no. 21, 2022, doi: 10.3390/s22218371.

[27] R. Afiyanto, E. D. Astuti, A. A. Kamal, and N. P. L. Santoso, "Reliability Assessment of Attendance Systems Based on Face Recognition Under Varying Lighting Conditions," *Int. Trans. Artif. Intell.*, vol. 4, no. 1, pp. 25–37, 2025, doi: 10.33050/italic.v4i1.924.

[28] S. Ravipati, L. Modem, S. Yellinedi, T. R. Namburi, and S. S. Sk, "Enhanced Attendance Management of Face Recognition Using Machine Learning," *ITM Web Conf.*, vol. 74, no. 1, p. 01012, 2025, doi: 10.1051/itmconf/20257401012.

[29] M. I. Thanoon, "Artificial Intelligence-Based Smart Class Attendance System: an Iot Infrastructure," *Int. J. Qual. Res.*, vol. 18, no. 1, pp. 187–198, 2024, doi: 10.24874/IJQR18.01-12.

[30] R. A. Riskiansyah, Y. Setiawan, and F. Z. Rahmanti, "Real-Time Detection of Outdoor Parking Space Availability Using YOLOv8," *JUITA J. Inform.*, vol. 13, no. 3, pp. 339–347, 2025, doi: 10.30595/juita.v13i3.27278.

[31] A. R, L. S, and T. M, "Face Recognition Based Attendance System using OpenCV," *JETIR*, vol. 10, no. 4, pp. 766–773, 2025, doi: 10.4108/eai.28-4-2025.2357832.

[32] A. Sureshkumar, M. Sathyamoorthy, R. K. Dhanaraj, S. Aanjanadevi, and V. Palanisamy, "Secure facial biometric authentication in smart cities using multimodal methodology," *Sci. Rep.*, vol. 15, no. 1, pp. 1–25, 2025, doi: 10.1038/s41598-025-29048-5.

[33] J. Samatha and M. Gudavalli, “Smart attendance monitoring system using multimodal biometrics,” *Sigma J. Eng. Nat. Sci.*, vol. 43, no. 1, pp. 168–188, 2025, doi: 10.14744/sigma.2024.00030.

[34] T. V. Dang, “Smart Attendance System based on Improved Facial Recognition,” *J. Robot. Control*, vol. 4, no. 1, pp. 46–53, 2023, doi: 10.18196/jrc.v4i1.16808.

[35] R. Muzayanah, A. D. Lestari, and M. A. Muslim, “IoT-Integrated Smart Attendance and Attention Monitoring System For Primary and Secondary School Classroom Management,” *J. Electron. Technol. Explor.*, vol. 2, no. 1, pp. 21–25, 2024, doi: 10.52465/joetex.v2i1.381.

[36] A. A. Zainuddin, R. M. Nor, D. Handayani, M. I. Mohd. Tamrin, K. Subramaniam, and S. F. N. Sadikan, “Smart Attendance in Classroom (CObot): IoT and Facial Recognition for Educational and Entrepreneurial Impact,” *APTISI Trans. Technopreneursh.*, vol. 6, no. 3, pp. 608–622, 2024, doi: 10.34306/att.v6i3.497.

[37] W. Agustina, D.T. Nugrahadi, M.R. Faisal, T.H. Saragih, A. Farmadi, I. Budiman, J.M. Parenreng, M. Alkaff, “Multimodal Biometric Recognition Based on Fusion of Electrocardiogram and Fingerprint Using CNN, LSTM, CNN-LSTM, and DNN Models,” *J. Tek. Inform.*, vol. 6, no. 4, pp. 1911–1924, 2025, doi: 10.52436/1.jutif.2025.6.4.5098.

[38] M. F. Ahmed, M. F. Ahmed, K. Deekshitha, and B. Student, “Enhancing AI-Based Attendance Management Systems: Addressing Recognition Accuracy, Security, And Scalability,” *Int. J. Creat. Res. Thoughts*, vol. 13, no. 2, pp. 2320–2882, 2025, [Online]. Available: www.ijcrt.org, doi: 10.1729/Journal.39414.

[39] D. Ray, “A Face Recognition Based Attendance System with Geolocation and Real-Time Action Logging,” *Res. Sq.*, vol. 1, no. 3, pp. 1–18, 2025, [Online]. Available: https://www.researchsquare.com/article/rs-5931462/v1, doi: https://doi.org/10.21203/rs.3.rs-5931462/v1.

[40] R. Andrian and G. P. Kusuma, “Serial Multimodal Biometrics Authentication and Liveness Detection Using Speech Recognition with Normalized Longest Word Subsequence Method,” *Int. J. Informatics Vis.*, vol. 8, no. 3, pp. 1260–1270, 2024, doi: 10.62527/joiv.8.3.2247.

[41] H. Ma, D. Guo, J. Wang, P. Li, C. Xu, and Y. Wang, “Real-time face recognition algorithm based on lightweight neural network in the field of computer vision,” *Discov. Appl. Sci.*, vol. 8, no. 1, 2026, doi: 10.1007/s42452-025-08004-y.

[42] V. Darshan, D. S. Kenny, H. R. Shreyas, N. Vinay, and S. Revathi, “IoT Based Attendance Monitoring System Using Facial Recognition,” *2nd IEEE Int. Conf. Adv. Inf. Technol. ICAIT 2024 - Proc.*, vol. 1, no. 2, pp. 1–6, 2024, doi: 10.1109/ICAIT61638.2024.10690462.

[43] K. Ashwini, G. N. Keshava Murthy, S. Raviraja, and G. A. Srinidhi, “A Novel Multimodal Biometric Person Authentication System Based on ECG and Iris Data,” *Biomed Res. Int.*, vol. 1, no. 2, 2024, p. 8112209, 2024, doi: 10.1155/2024/8112209.