



Design and Development of a Secure Fingerprint-Based Verification System for Examination Attendance

S. Norwahidayah*, M. Luqman Haziq

University College TATI, Jalan Panchor, Telok Kalong, 24000 Kemaman, MALAYSIA

*Corresponding author email: norwahidayah@uctati.edu.my

KEYWORDS

Biometric
Attendance system
Student ID
PPDIOO
Fingerprint

ABSTRACT

Examination attendance management plays a critical role in ensuring academic integrity, yet conventional methods such as manual sign-in sheets, identity cards, and QR-based systems remain vulnerable to impersonation and fraudulent practices. Biometric authentication, particularly fingerprint verification, offers a reliable solution due to its uniqueness and permanence [8]. This paper presents the design and development of a secure fingerprint-based verification system for examination attendance. The proposed system focuses on a structured framework that integrates fingerprint enrollment, verification, and secure attendance recording to mitigate identity related misconduct during examinations. The system architecture is designed to include key components such as a fingerprint sensor, processing unit, secure database, and user management modules for administrators and invigilators. A detailed methodology is presented to describe the enrollment and verification workflows, authentication procedures, and security considerations, including template protection and access control mechanisms. Unlike existing studies that primarily emphasize implementation performance, this work concentrates on the conceptual design and system development aspects, highlighting security requirements specific to examination environments. The proposed framework aims to enhance the reliability, security, and integrity of examination attendance processes and serves as a foundation for future implementation, testing, and performance evaluation of biometric-based examination management systems.

Received 12 February 2026; Revised 19 Juen 2026; Accepted 30 June 2026; Published 01 October 2026

1.0 INTRODUCTION

The transition from conventional to automated attendance systems is driven by the growing need for accountability and security in educational institutions [9]. Manual attendance marking methods are prone to significant issues, including proxy attendance, where a student signs in on behalf of another and impersonation during examinations. These forms of academic misconduct not only compromise the integrity of the assessment process but also undermine the value of the education provided.

The articles reviewed highlight these deficiencies, pointing out that manual attendance is a time-consuming activity for both students and lecturers and that conventional approaches are

highly susceptible to fraud [1]. The advent of digital technologies has introduced various automated solutions, but many lack the security features required for a robust verification process, especially for sensitive events like final examinations [11].

Biometric systems, particularly those based on fingerprints, offer a promising solution by providing a non-repudiable and unique form of identification that is difficult to forge or manipulate [10]. The introduction established the foundation for this project by outlining the need for a secure and efficient exam attendance system. It has identified the key problems with current manual methods, including time wastage and vulnerability to academic fraud.

This section has also defined the specific objectives of the project, which aims to address these problems through the development of a fingerprint-based verification system. Finally, the scope of the project has been clearly delineated, specifying the functionalities that will be included in the prototype. The following chapters will detail the methodology, design and implementation of the proposed system to achieve these objectives.

2.0 PROBLEM STATEMENT

The existing methods of attendance management for examinations present several critical challenges that this project seeks to address. Many universities are transitioning from manual attendance to automated systems to improve efficiency and enhance security [13]. Fingerprint technology has emerged as a leading approach in this shift. For example, [1] demonstrated that fingerprint biometrics effectively prevent students from marking attendance on behalf of others.

However, their study was limited to general classroom attendance and did not account for the stricter requirements of formal examinations. Similarly, [2] confirmed that fingerprint-based systems can save time and reduce student delays, yet their work focuses mainly on daily check-ins rather than high-stakes exam verification. More recently, [3] proposed comprehensive security framework that combined biometrics, CCTV and script submission to safeguard examinations [14].

While highly secure, the approach is too complex and costly to be applied solely for attendance verification. In another direction, [4] explored IoT-based biometric systems for identity verification, highlighting their flexibility and ability to integrate with modern infrastructures. Nevertheless, their study focused on assessing service quality rather than addressing the urgent need to prevent impersonation and fraud in exam settings [15].

In short, while various biometric attendance systems have been proposed, most existing solutions were not designed to meet the high-security, fast and reliable verification requirements of exam attendance [16], [17]. This project aims to fill that gap by developing a dedicated fingerprint verification system that ensures secure and efficient exam hall check-ins.

3.0 OBJECTIVE

To address the weaknesses of existing manual attendance verification methods and to enhance the security, accuracy and efficiency of examination processes, this project is guided by the following objectives:

- i. To design a secure fingerprint verification system for accurate student examinations attendance.
- ii. To develop and implement enrolment modules to capture and store fingerprint template linked to student ID.
- iii. To implement verification system that can authenticate students accurately during exam sessions.

4.0 RELATED WORK

4.1 Overview of Biometric Attendance System

Biometrics refers to the automatic identification or verification of individuals based on unique physiological or behavioural characteristics such as fingerprints, face, iris or voice. Biometric systems are categorized into verification (one-to-one matching) and identification (one-to-many matching) [18]. Verification ensures that a user's identity matches a specific template stored in the system, while identification searches for a match within an entire database [3].

In educational environments, biometric systems improve attendance management by ensuring that only authorized students can register their presence. This reduces impersonation, minimizes administrative work and allows real-time monitoring through integrated databases and dashboards

4.2 Fingerprint Recognition Technology

Fingerprint technology relies on the distinct ridges and minutiae points found on human fingers [19]. The system captures these patterns using a fingerprint sensor and converts them into a digital template for storage in a database. During verification, the system compares the scanned fingerprint with existing templates using matching algorithms [2]. Fingerprint systems are considered cost-effective, easy to use and highly accurate. However, factors such as dirty fingers, poor sensor calibration or unstable internet connectivity may affect accuracy [1]. Compared to RFID or face recognition, fingerprint authentication offers better resistance to impersonation and spoofing, making it suitable for examination setting.

4.3 Implementing Student Attendance System Using Fingerprint

The development of a client-server fingerprint attendance system using the ZK-TECO fingerprint device integrated with a MySQL database [3]. The system automated attendance and reduced manual record-keeping, particularly in classroom environments. However, its limitation lies in the absence of exam-level security measures, such as anti-fraud verification or multiple authentication stages.

4.4 Fingerprint-Based Student Attendance for Olabisi Onabanjo University

The proposed idea of introduced a C# and SQL-based attendance management system that improved data security and reduced attendance time [4]. The system featured a simple GUI that allowed quick scanning and verification for multiple users. Despite its effectiveness in daily attendance, the system was not optimized for exam conditions where speed and strict validation are required.

4.5 IoT-Based Biometric Recognition System for Education

This study explored the integration of biometric systems with IoT-based cloud verification [5]. The system used a cloud server for real-time verification and performance monitoring through a Quality Assessment Model (QAM). The approach demonstrated high reliability but depended heavily on stable internet connectivity. For exam use, reliance on cloud services could cause latency during simultaneous verifications [20].

4.6 Security Framework for Examination Monitoring

A high-security framework that combined biometrics, CCTV, and secure scripting for offline exam monitoring proposed by [6]. The approach effectively improved examination integrity and identity validation. However, it was too complex and costly for typical university-level deployment. The framework is particularly effective in environments that require strict

invigilation because each security feature complements the others. Biometric verification confirms the student's identity at the entrance, while CCTV cameras provide real-time surveillance inside the hall. The added script-submission validation ensures that the correct answer booklet is returned by the student who sits the exam [21].

4.7 Previous Work

Table 1: Summary of related study

Author (Year)	Title	Method	Benefits	Limitations
[1]	Implementing Student Attendance System Using Fingerprint Biometrics for Kolej University Poly-Tech Mara (KUPTM)	Client-server fingerprint system using ZK-TECO device integrated with MySQL database.	Automated attendance, reduced manual record keeping, improved data storage and retrieval accuracy	Focused only on classroom attendance; lacks multilayer exam verification and anti-fraud security features.
[2]	A Fingerprint-Based Students Attendance Management System for Olabisi Onabanjo University	C# application with SQL Server back-end; fingerprint verification at entry terminals.	Improved attendance efficiency and enhanced security; reduced check-in time.	System not optimized for high-pressure examination scenarios; limited scalability beyond small classes
[3]	IoT-Based Biometric Recognition Systems in Education for Identity Verification Services: Quality Assessment Approach	IoT biometric framework using cloud server with quality-assessment model.	Reliable real-time verification and remote monitoring; measurable accuracy and speed indicators.	Dependent on stable internet; risk of latency or downtime during time-sensitive exam verification.
[4]	Framework for Design of Security Systems for Monitoring Examinees and Proctors During External Offline Examinations in Nigeria	Integrated biometrics + CCTV + secure script framework for exam surveillance.	Provided high-security multi-layer framework for offline examinations	Excessive complexity and cost, no real-time biometric feedback; impractical for routine campus use.
[5]	Fingerprint-Based Biometric Attendance System Using Arduino	Arduino Uno with R307 sensor and local storage; embedded verification.	Low-cost, portable prototype suitable for small-scale classroom deployment; minimal maintenance.	Limited speed and database capacity, unsuitable for large-scale or multi-terminal university deployment.

5.0 RESEARCH GAP

Although many biometric attendance systems have been proposed, most of existing studies focus primarily on general classroom attendance rather than examination environments. Classroom settings typically allow slower verification speeds, basic identity checks and minimal security requirements. However, examinations demand a significantly higher level of accuracy, faster processing time and robust anti-impersonation mechanisms. None of the reviewed systems, including those by [1] and [2], address the unique operational challenges of exam check-ins where hundreds of students may need to be verified within a short time window.

Furthermore, several existing approaches rely heavily on internet connectivity or cloud-based verification, as seen in the IoT-based framework by [3]. While cloud verification offers scalability, it introduces latency and reliability risks that are unacceptable in examination halls, especially in environments with unstable Wi-Fi or bandwidth limitations. This highlights a clear gap for an offline-capable fingerprint verification system that maintains high accuracy without depending on external networks.

In addition, some of the reviewed studies propose complex, multi-layered security systems such as the biometric-CCTV hybrid framework [4]. Although effective, these solutions are too expensive, infrastructure heavy and impractical for standard university examination settings that only require secure identity verification at the entry point. This demonstrates the need for a more cost-effective, lightweight and scalable solution that universities can realistically implement.

Lastly, prototype-level solutions such as the Arduino-based system [5] highlight the limitations of low-cost biometric devices, including slow processing times and low template capacity. This underscores another gap for a system that balances affordability with performance, utilizing hardware like the Raspberry Pi that can support faster matching while still being cost-efficient [22]. Therefore, there is a clear research gap for a dedicated, offline, secure, exam-focused fingerprint verification system precisely what the proposed project aims to develop.

6.0 METHODOLOGY

The PDIOO model is selected because it provides a structured and iterative development framework that is suitable for projects involving both hardware and software integration [23]. In the context of examination attendance systems, where real-time verification, reliability and accuracy are critical, the PDIOO model allows systematic refinement at each development stage to ensure the system meets operational requirements [24].

6.1 PPDIIO Model

The PPDIIO model is used as the system development methodology for this project. It consists of six main phases: Prepare, Plan, Design, Implement, Operate and Optimize [25]. Each phase addresses a specific aspect of system development, starting from problem understanding and requirement analysis to system deployment and performance improvement [26]. This model is particularly suitable for biometric verification systems as it supports iterative testing and optimization, which are necessary to ensure fast and accurate fingerprint matching in time-critical environments such as examination halls.

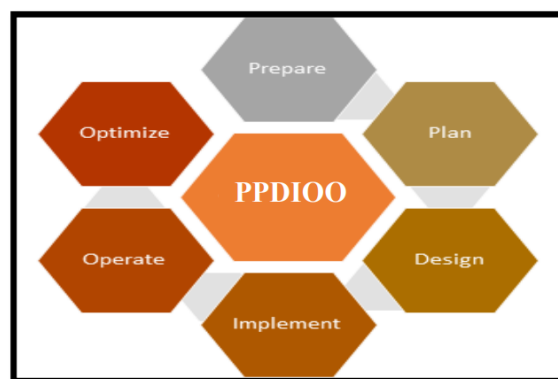


Figure 1: PPDIIO Model

The Prepare phase focuses on understanding the project background, identifying the core problem and reviewing existing studies related to biometric attendance and examination verification systems [27]. In this phase, weaknesses of manual examination attendance methods

and limitations of existing fingerprint-based systems are analyzed through literature review. The findings from this phase help define the initial system requirements, particularly the need for a fast, secure and offline capable fingerprint verification system suitable for examination environments. These findings directly influence the planning and design decisions in the subsequent phases.

The Plan phase involves defining both functional and non-functional requirements of the system, as well as selecting appropriate hardware and software components [28]. In this phase, Raspberry Pi 5 is chosen as the main processing unit due to its higher processing power, larger memory capacity and ability to support real-time database and web-based dashboard operations compared to microcontrollers such as Arduino. A fingerprint sensor is selected for biometric data capture, while a local MySQL database is used to store fingerprint templates and attendance records to ensure offline operation during examination sessions. The system workflow, database structure and user roles are also planned in this phase to ensure smooth integration between hardware, backend processing and the admin dashboard.

The Design phase focuses on defining the overall system architecture, data flow and verification process [29]. This includes designing the interaction between the fingerprint sensor, Raspberry Pi, database and web-based admin dashboard. The verification workflow is designed to support fast fingerprint matching to accommodate high-volume student check-ins during examination sessions. Once a fingerprint is captured, the system processes the data locally and updates the attendance record in real time, allowing administrators to monitor attendance status instantly through the dashboard.

The Implement phase involves the integration of hardware and software components based on the designed architecture [30]. The fingerprint sensor is interfaced with the Raspberry Pi to capture and process biometric data, while the database and dashboard are implemented to store and display attendance records. System functionality is validated through successful fingerprint enrolment, accurate identity verification and real-time attendance updates on the admin dashboard. Basic performance indicators such as response time during verification and successful matching rate are observed to ensure the system operates effectively in examination conditions.

The Operate phase focuses on testing the system under simulated examination conditions. Multiple fingerprint verification attempts are conducted to evaluate system stability and responsiveness during peak usage [27]. Administrators use the dashboard to monitor attendance status in real time, ensuring that the system functions as intended in an exam hall environment.

The Optimize phase involves refining the system based on observations made during operation [28]. Minor improvements such as optimizing verification speed, improving system responsiveness and enhancing user interface clarity are considered to ensure reliable performance. This phase ensures that the system is stable and suitable for demonstration as a functional examination attendance prototype.

6.2 Flowchart

The overall system flowchart describes the complete process of exam attendance verification using fingerprint authentication. When a student arrives, the system prompts them to scan their fingerprint. The fingerprint image is captured by the sensor and sent to the Raspberry Pi for processing. The system then compares the scanned template with the stored template in the database.

If a match is found, the system records the student's attendance, provides successful feedback through the LCD display and buzzer will allow the student to enter the exam hall. If the fingerprint does not match any record, the system displays an error message and denies entry. This ensures that only registered students are allowed to sit the examination.

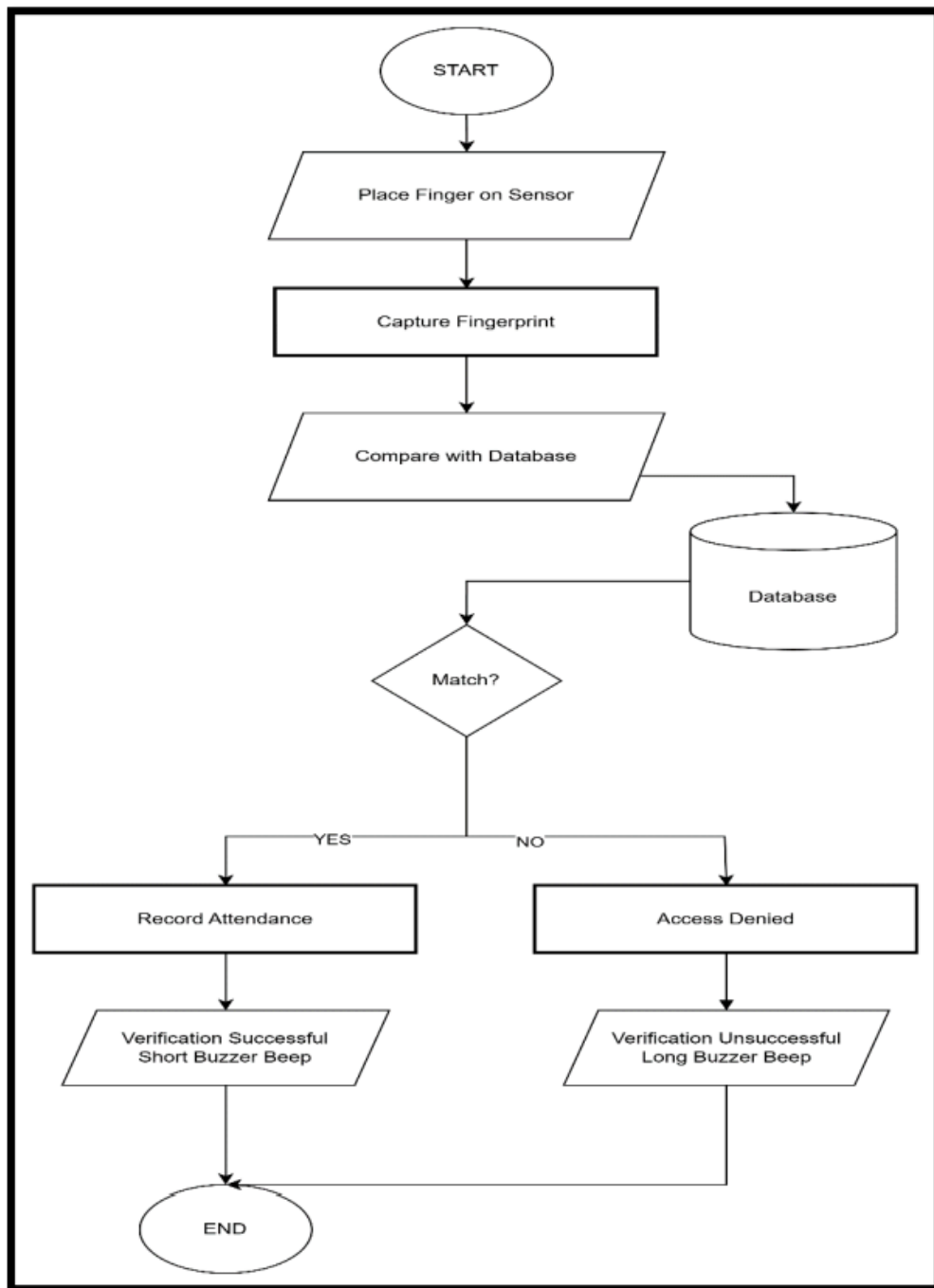


Figure 2: Flowchart

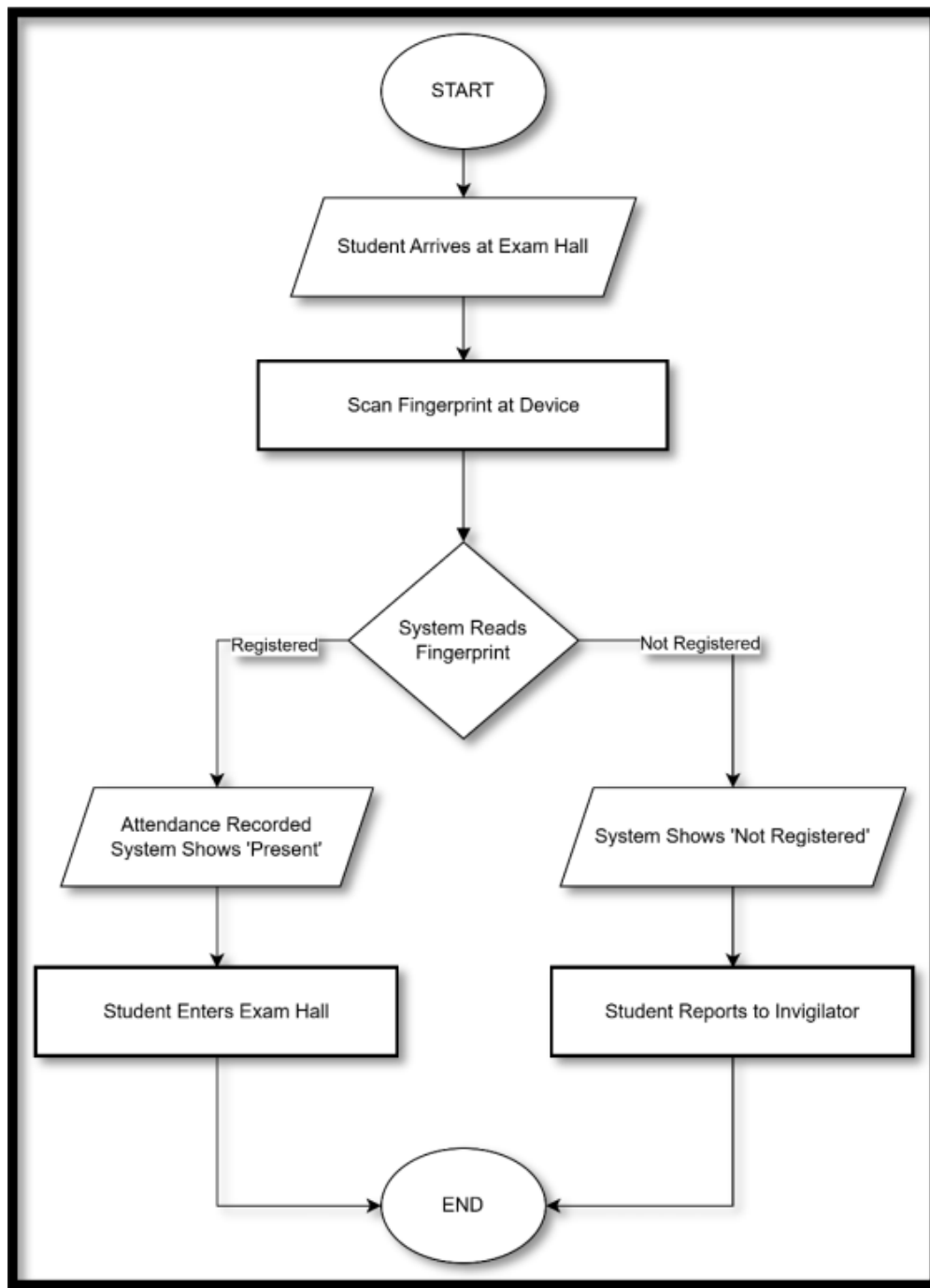


Figure 3: User Flow System (student)

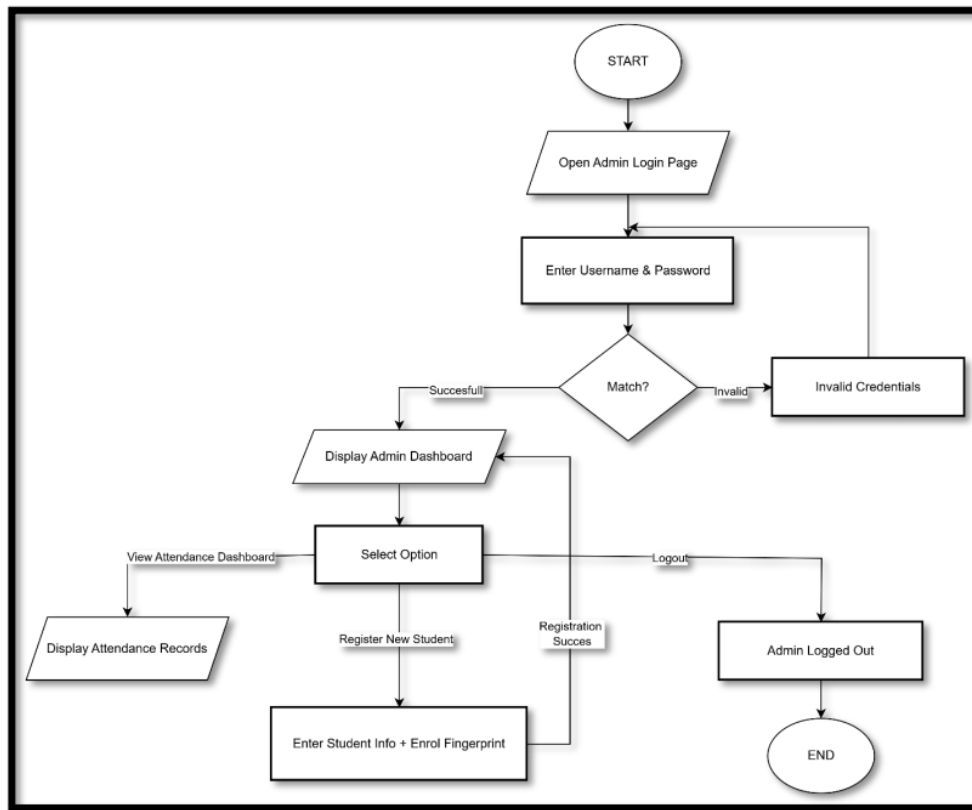


Figure 4: Admin Flow System

6.3 Entity Relationship Diagram (ERD)

The Entity Relationship Diagram (ERD) illustrates the database structure used in the Exam Attendance Fingerprint System. It shows the main entities, including Students, Exam_Students, Attendance and Admin_Users, along with their attributes and relationships. The ERD defines how student information, exam lists and attendance records are connected. Composite primary keys are used in the Exam_Students and Attendance tables to ensure each student_exam record is unique. This ERD supports efficient data management, fingerprint verification and accurate attendance tracking within the system.

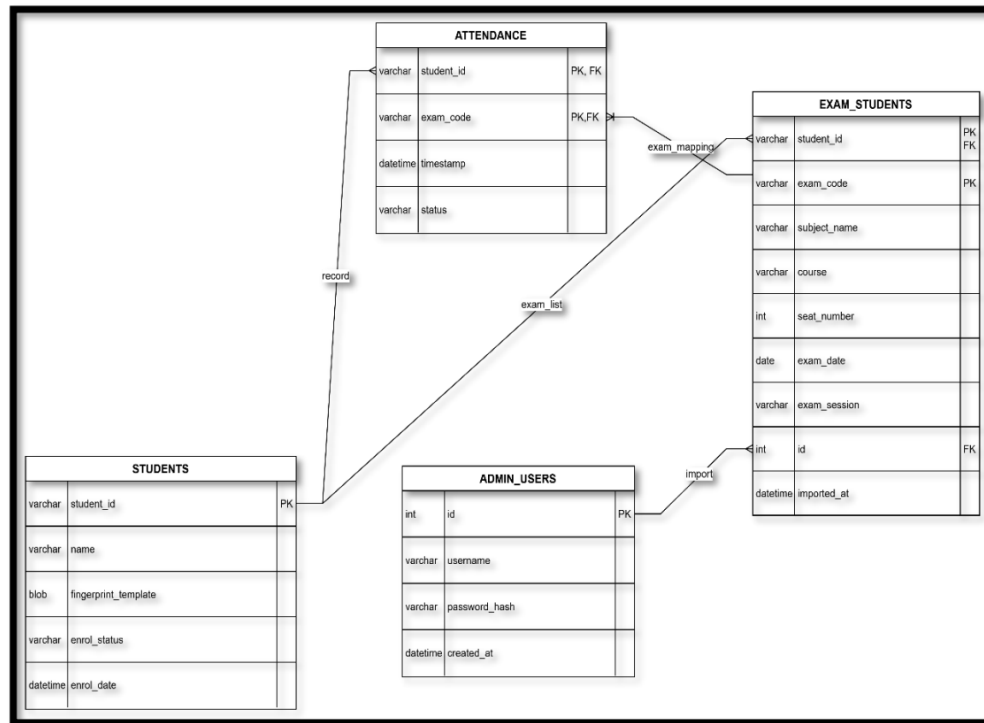


Figure 5: ERD of the Exam Attendance Fingerprint System

6.4 Block Diagram

Figure 6 illustrates the block diagram of the proposed fingerprint-based examination attendance system. The diagram provides an overview of the system architecture and explains how biometric data flows through the system during enrolment and authentication processes. During the enrolment phase, the student's fingerprint is captured using the fingerprint sensor. The captured biometric image undergoes feature extraction, where unique fingerprint characteristics are processed and converted into a digital template. This template is then securely stored in the database and linked to the corresponding student identification record.

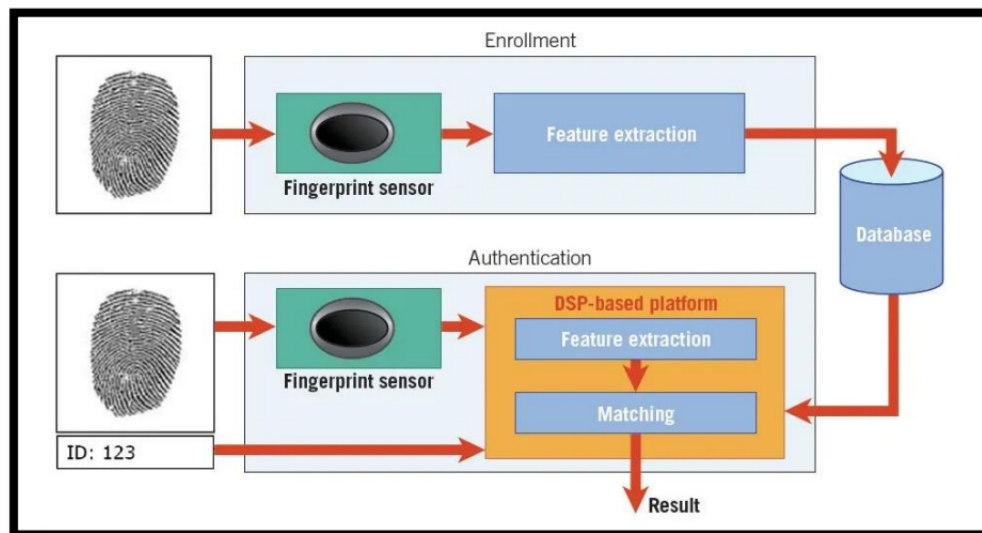


Figure 6: Block Diagram of the Fingerprint-Based Exam Attendance System

7.0 SECURITY CONSIDERATION

Security is a critical requirement for examination attendance systems due to the high risk of impersonation, unauthorized access, and data manipulation. The proposed fingerprint-based verification system is designed with security as a core consideration to protect both user identity and attendance records.

One of the primary threats addressed by the system is exam impersonation, where an unauthorized individual attempts to register attendance on behalf of a legitimate student. This risk is mitigated through biometric fingerprint verification, which relies on the uniqueness of fingerprint patterns and cannot be easily replicated compared to conventional identification methods such as ID cards or passwords.

To protect biometric data, the system adopts a secure fingerprint template storage approach, where raw fingerprint images are not stored directly in the database. Instead, extracted features or templates are saved to reduce the risk of biometric data leakage. Access to the database is restricted through role-based authentication, ensuring that only authorized administrators can manage enrollment data.

Additionally, secure authentication procedures are implemented for system access by invigilators and administrators to prevent unauthorized system manipulation. Attendance records are automatically generated after successful verification, minimizing human intervention and reducing the possibility of record tampering. These security considerations collectively enhance the confidentiality, integrity, and reliability of the examination attendance process.

8.0 DISCUSSION

The proposed fingerprint-based verification system addresses several limitations identified in existing examination attendance methods. Traditional approaches, such as manual attendance sheets or card-based systems, are susceptible to impersonation, loss, and human error. By incorporating biometric verification, the proposed system improves the accuracy and trustworthiness of attendance recording in examination environments.

From a design perspective, the system emphasizes simplicity, scalability, and security, making it suitable for deployment in educational institutions with varying examination sizes. The modular architecture allows future integration with existing academic management systems, such as examination databases or learning management platforms.

However, certain limitations are acknowledged at the design stage. The effectiveness of fingerprint verification may be influenced by sensor quality, environmental conditions, and fingerprint readability issues. Additionally, user acceptance and privacy concerns related to biometric data collection must be carefully managed through institutional policies and proper data handling practices. Overall, the proposed design provides a structured and secure framework that supports examination integrity while offering flexibility for future enhancements and system expansion.

9.0 CONCLUSIONS AND FUTURE WORK

This paper has presented the design and development of a secure fingerprint-based verification system for examination attendance. The proposed framework focuses on system architecture, verification workflow, and security considerations tailored to examination environments. By leveraging biometric fingerprint authentication, the system aims to reduce impersonation risks, enhance attendance accuracy, and improve overall examination integrity.

Although this study is limited to conceptual design and methodology, it establishes a strong foundation for further system implementation and evaluation. Future work will involve the development of a functional prototype, performance testing in real examination settings, and evaluation of verification accuracy, response time, and system usability. Additional enhancements may include multi-biometric integration, encryption-based template protection, and cloud-based attendance management to further strengthen system security and scalability.

Author Contribution

S. Norwahidayah: Conceptualization, writing and editing. M. Luqman Haziq: Investigation, supervision, writing, methodology, investigation, visualisation.

Conflict of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The authors gratefully acknowledge the university for providing the academic environment, resources, and facilities that supported the completion of this research.

REFERENCES

- [1] Adoga, P. I. (2023). Framework for design of security systems for monitoring examinees and proctors during external offline examinations in Nigeria. *International Journal of Scientific and Research Publications*, 7(6), 167–186.
- [2] Lamin, N. Z., Jusoh, W. N. A. W., Zainudin, J., & Samad, H. (2021). Implementing student attendance system using fingerprint biometrics for Kolej Universiti PolyTech MARA. *IOP Conference Series: Materials Science and Engineering*, 1062(1), Article 012037. <https://doi.org/10.1088/1757-899X/1062/1/012037>
- [3] Olasupo, O. A., Adebayo, O. S., Umar, M. A., Akinwale, K.-K. A., Oladipo, O. O., Adeyemi, F. E., Usman, H. O., Sadiq, E. O., & Ibrahim, T. E. (2022). A fingerprint-based students' attendance management system for Olabisi Onabanjo University. *International Journal of Advanced Research in Computer Science*, 6(8), 2003–2005.
- [4] Direksilp C, Threepopnatkul, P. Performance improvement of PS From Expanded Polystyrene off-grade. *Energy Procedia*, 2014; 56(C), 135–141.
- [4] Badmus, E. O., Odekunle, O. P., & Oyewobi, D. O. (2021). Smart fingerprint biometric and RFID time-based attendance management system. *European Journal of Electrical Engineering and Computer Science*, 5(6), 15–21.
- [5] Aldabagh, M. (2025). A review of students attendance management systems: Methods and taxonomy. *Eurasian Journal of Science and Engineering*, 10(3), 136–145. <https://doi.org/10.23918/eajse.v10i3p13>
- [6] Sharma, A., & Gupta, A. (2024). Fingerprint-based biometric attendance system using Arduino (Bachelor's thesis, Electronics and Communication Engineering).
- [7] Tefera, A., & Negussie, N. (2024, June 1). Fingerprint attendance system using Raspberry Pi and MySQL database. <https://doi.org/10.13140/RG.2.2.23701.33764>
- [8] Chauhan, R., Negi, S., Kumar, A., & Devliyal, S. (2024). A Raspberry Pi-based smart attendance system. In *Proceedings of the 2024 International Conference on Automation and Computation (AUTOCOM)* (pp. 612–617). IEEE. <https://doi.org/10.1109/AUTOCOM60220.2024.10486161>
- [9] Badmus, E. O., Odekunle, O. P., & Oyewobi, D. O. (2021). Smart fingerprint biometric and RFID time-based attendance management system. *European Journal of Electrical Engineering and Computer Science*, 5(6), 15–21. <https://doi.org/10.24018/ejece.2021.5.6.339>
- [10] Newaskar, D., Paygude, V., Mahamulkarr, V., & Vyavhare, A. (2024). Fingerprint and face recognition based attendance system for examinations. *Journal of Telecommunication, Switching Systems and Networks*, 11(3), 26–33.
- [11] Kaur, T., Singh, A. P., Nagar, A., & Singh, S. K. (2024). Biometric fingerprint systems for secure and efficient attendance tracking in workplaces and universities. *International Journal of VLSI Circuit Design & Technology*, 2(2), 12–17.
- [12] Gudavalli, S. J. M. (2025). Smart attendance monitoring system using multimodal biometrics. *Sigma Journal of Engineering and Natural Sciences*, 43(1), 168–188.

- [13] Obiora, G. N., Aladejare, I. O., Igbinsosa, G. O., Fiemobebefa, C. B., & Bamido, O. A. (2025). Development of a fingerprint-based attendance monitoring system. *ABUAD Journal of Engineering Research and Development*, 8(1), 263–270.
- [14] Sarjiyus, O., El Yakub, M. B., & Ezra, B. (2023). Examination verification system using biometric authentication. *International Journal of Integrative Sciences*, 2(9), 1459–1478. <https://doi.org/10.55927/ijis.v2i9.6064>
- [15] Chandra Sekhar, P., Anagani, B., Reshmi, R., Aruna, & Sai Priya. (2023). Fingerprint based exam hall authentication. *IJRASET – Journal for Research in Applied Science and Engineering Technology*. <https://doi.org/10.22214/ijraset.2023.56392>
- [16] Ramgopal, A., et al. (2025). IoT-enabled fingerprint biometric attendance system for secure and real-time student monitoring. *Asian Journal of Applied Science and Technology*, 9(3), 147–161. <https://doi.org/10.38177/ajast.2025.9314>
- [17] Adesoba, O. C., & Joseph, I. M. (2025). A fingerprint-based attendance system for improved efficiency. *Journal of Engineering and Technology for Industrial Applications (ITEGAM-JETIA)*, 11(51), 9–19. <https://doi.org/10.5935/jetia.v11i51.1305>
- [18] Rahman, M. M. (2021). Study on introducing biometric fingerprint authentication in automated student attendance system. *New Visions in Science and Technology*, 4, 121–131. <https://doi.org/10.9734/bpi/nvst/v4/4580F>
- [19] Odulaja, G. O. (2025). Development of a fingerprint-biometric expert system for student class attendance monitoring. *Journal of Computing and Applications*, 2(2), 99–110.
- [20] Akanni, A. O., Oluwafemi, J., & Olufunke, S. M. (2024). Development and evaluation of a fingerprint-based biometric system for secured examination admittance in higher institutions. *FUOYE Journal of Engineering and Technology*.
- [21] Gabriel, E. M., Kelvin, A. B., & Kenneth, A. P. (2025). Implementation of biometric fingerprint attendance system using ESP8266 and fingerprint scanner. *Journal of Scientific and Engineering Research*, 11(9), 22–30.
- [22] Elebede, A. W., Omolara, O. O., Sodipo, Q. B., & Ayotunde, S.-L. T. (2024). Design and implementation of a fingerprint-based student attendance system. In *Proceedings of the IEEE 5th International Conf. on Electro-Computing Technologies for Humanity (NIGERCON)* (pp. 1–6). IEEE.
- [23] Bhat, S., R, N., & S, P. (2023). Design and implementation of a biometric and RFID attendance tracking system. *WAJES Journal*.
- [24] Ishaq, K., & Bibi, S. (2023). IoT based smart attendance system using RFID: A systematic literature review. *arXiv*.
- [25] Kaur, T., Singh, A. P., Nagar, A., & Singh, S. K. (2024). Biometric fingerprint systems for secure and efficient attendance tracking in workplaces and universities. *International Journal of VLSI Circuit Design & Technology*, 2(2), 12–17.
- [26] Newaskar, D., Paygude, V., Mahamulkarr, V., & Vyavhare, A. (2024). Fingerprint and face recognition based attendance system for exams. *Journal of Telecommunication, Switching Systems and Networks*, 11(3), 26–33.
- [27] Ayed, A. W. E., Omolara, O. O., & Sodipo, Q. B. (2024). Enhanced fingerprint-based automated attendance recording system. In *International Conference on Computing and Communication Technologies (conference proceedings)*.
- [28] International Journal of Research and Innovation in Social Science. (2025). Arduino-based fingerprint attendance system: Enhancing security and record integrity in educational institutions through biometric technology. *IJRISS*, 9(9), 5884–5901.