Journal Homepage: www.ijarpr.com ISSN: 3049-0103 (Online)

International Journal of Advance Research Publication and Reviews

Vol 03, Issue 10, pp 547-565, October, 2026

# A Secure Fingerprint-Based Examination Attendance Management System for Tertiary Institutions: Design, Implementation, and Technical Evaluation

***Temitayo Oyebamiji Morakinyo[1], Akeem Rotimi Gbopa[1], Sikiru Olanrewaju Kilani[2] and Abiodun Sunday Olowookere[2]***

[1]Department of Computer Engineering Technology, Oyo State College of Agriculture and Technology, Igboora, Oyo State, Nigeria

[2]Department of Computer Science, Oyo State College of Agriculture and Technology, Igboora, Oyo State, Nigeria

**Email:** tmorak36@gmail.com

**ABSTRACT**

Examination impersonation, proxy attendance, inefficient manual verification, and weak attendance traceability remain operational challenges for tertiary institutions. Although fingerprint biometrics can strengthen identity verification, a successful biometric comparison alone does not establish eligibility for a particular examination or guarantee the integrity of the resulting attendance record.

This study presents the design, implementation, and technical evaluation of a secure fingerprint-based examination attendance management system developed for Oyo State College of Agriculture and Technology, Igboora, Nigeria.

The system integrates student biodata management, academic catalogue administration, examination and session management, examination registration, administrator-controlled biometric enrollment, fingerprint verification, eligibility validation, attendance reporting, and audit logging. The application was implemented using Python, FastAPI, SQLAlchemy, MySQL, Bootstrap, JavaScript, and a .NET native bridge connected to a DigitalPersona U.are.U 4500 fingerprint reader. Windows Data Protection API (DPAPI) was used to protect local development enrollment artifacts. The database stores enrollment metadata and an opaque protected-artifact reference rather than raw fingerprint images or unprotected biometric templates.

Attendance creation is governed by a sequence of academic, authorization, biometric, and transaction-integrity checks. The implementation passed 41 automated tests, Python compilation checks, and Alembic schema validation, with no new schema upgrade operations detected. Real fingerprint-reader access, capture, enrollment-template creation, and successful and unsuccessful 1:1 verification outcomes were also demonstrated.

The findings establish the technical feasibility of integrating fingerprint verification with examination eligibility controls and transaction-safe attendance recording in a controlled, single-workstation environment.

**Keywords:** biometric authentication; fingerprint verification; examination attendance; examination impersonation; biometric template protection; transaction integrity; digital identity; tertiary education.

## 1. Introduction

Reliable identity verification is essential in environments where access, participation, or a recorded transaction must be linked to a specific individual. In tertiary education, examination attendance is not simply a record of physical presence. It is an administrative control that must establish the identity of a candidate, verify eligibility for a particular examination, record attendance accurately, and preserve evidence for subsequent review.

Traditional examination attendance procedures frequently rely on paper registers, signatures, identity cards, or manually maintained clearance lists. Although these approaches are familiar and relatively inexpensive, they may create administrative overhead, make record retrieval difficult, and provide limited protection against proxy attendance. Their effectiveness also depends on the consistency of manual checks and the integrity of the resulting records.

Biometric recognition offers an additional mechanism for verifying identity through measurable physiological or behavioural characteristics. Fingerprints are particularly relevant to workstation-based verification because dedicated readers can capture fingerprint samples and compare them with previously enrolled references. Nevertheless, biometric systems introduce security and privacy concerns because compromised biometric information cannot be replaced as easily as a conventional password. Research on biometric template attacks and protection mechanisms continues to identify risks associated with template compromise, reconstruction, and misuse (Abdullahi et al., 2024).

The deployment of fingerprint verification in an examination environment must therefore address more than the matching operation. A candidate may present a valid fingerprint but lack registration for the examination, attempt to attend a closed session, have an inactive institutional record, or already possess an attendance record for the same session. A reliable system must coordinate identity verification with academic eligibility rules, authorization controls, and database integrity constraints.

International guidance also makes biometric information protection and performance evaluation central considerations. ISO/IEC 24745:2022 addresses confidentiality, integrity, renewability or revocability, secure binding between biometric and identity references, and privacy-compliant processing. ISO/IEC 19795-1:2021 establishes principles for measuring and reporting biometric performance.

Against this background, this study presents a fingerprint-based examination attendance management system developed for Oyo State College of Agriculture and Technology (OYSCATECH), Igboora, Nigeria. The system combines institutional academic records with real fingerprint acquisition, one-to-one (1:1) verification, examination eligibility checks, attendance transaction controls, and audit logging.

The implementation also distinguishes between demonstrated technical functionality and performance claims that require a dedicated empirical study. Rather than reporting unsupported biometric accuracy percentages, the study documents software testing, integration evidence, and the boundaries of the current evaluation.

### *1.1 Problem Statement*

Examination attendance management in tertiary institutions can be affected by challenges associated with student identification, attendance verification, record keeping, and examination eligibility control. Reliance on manual attendance procedures may create opportunities for impersonation and proxy attendance, while the manual verification of student identities and examination eligibility can cause delays during examination administration. In addition, attendance records may be incomplete, duplicated, illegible, or difficult to retrieve, thereby reducing the accuracy, reliability, and efficiency of the attendance management process. Limited integration between examination registration and attendance recording may also make it difficult to confirm whether a student is duly registered and eligible to participate in a particular examination. Furthermore, inadequate real-time visibility into attendance status, inconsistent report generation, and insufficient audit trails can complicate the monitoring of examination participation and the investigation of disputed attendance records.

Although biometric technologies, particularly fingerprint verification, offer opportunities to strengthen student identification and reduce dependence on manual identity checks, biometric verification alone does not adequately address all the challenges associated with examination attendance management. An effective solution must also incorporate examination eligibility validation, duplicate attendance prevention, role-based access control, reliable record management, and comprehensive audit trails. In addition, the collection, storage, processing, and eventual deletion of biometric data must be managed securely to protect students' privacy and prevent unauthorized access or misuse. Therefore, the problem addressed by this study is the need for a secure, reliable, and integrated fingerprint-based examination attendance management system that verifies student identities, confirms examination eligibility, maintains accurate attendance records, supports efficient report generation, and provides appropriate security and accountability mechanisms throughout the attendance management process.

### *1.2 Aim and objectives*

The aim of this study is to design, implement, and technically evaluate a secure fingerprint-based examination attendance management system for tertiary institutions, using OYSCATECH as the implementation context.

The specific objectives are to:

1. Design a fingerprint-based examination attendance workflow that integrates student identity and examination eligibility.
2. Implement secure management of biometric enrollment references, attendance records, and audit metadata.
3. Develop an administrative interface for managing students, examinations, sessions, enrollment, verification, and reporting.
4. Evaluate the implementation through automated testing, hardware integration checks, workflow verification, and an assessment of security and operational limitations.

### *1.3 Research questions*

The study addresses the following questions:

- RQ1: How can fingerprint verification be integrated with examination registration and eligibility rules to control attendance recording?
- RQ2: How can biometric enrollment references be handled without storing raw fingerprint images or unprotected templates in the relational database?
- RQ3: What technical evidence demonstrates the feasibility of the implemented system, and what additional evaluation is required before institutional deployment?

### *1.4 Research contributions*

The study makes four practical contributions.

First, it implements an integrated examination attendance workflow in which biometric verification is separated from academic eligibility validation.

Second, it demonstrates the integration of a physical DigitalPersona fingerprint reader with a web-based administrative application through a native .NET bridge.

Third, it implements a data-minimizing enrollment architecture in which MySQL stores enrollment metadata and an opaque reference to a locally protected artifact rather than raw fingerprint images or unprotected templates.

Fourth, it documents the results and limitations of software and hardware integration testing without treating those tests as a substitute for formal biometric performance evaluation.

## 2. Related Work and Theoretical Background

### *2.1 Biometric recognition and fingerprint verification*

Biometric recognition uses measurable characteristics to establish or verify an individual's identity. Fingerprint verification typically involves acquiring a live sample, extracting or generating a representation suitable for comparison, evaluating the sample against a reference, and producing a decision according to the recognition system's matching process.

A distinction must be made between identification and verification. Identification generally searches across a population of enrolled references to determine whose biometric sample has been presented. Verification instead evaluates whether a sample corresponds to a particular claimed identity. The present system follows a 1:1 verification model: a student supplies a matriculation number, the application resolves the corresponding record, and the live sample is compared with that student's active enrollment reference.

This approach limits the comparison scope and allows academic eligibility checks to be linked to an explicit student record. However, the security of the process depends on the reliability of identity resolution, reference binding, access controls, and the matching mechanism.

### *2.2 Fingerprint attendance systems*

Fingerprint attendance systems have been investigated as alternatives to manual attendance recording in educational and organisational environments. Their practical attraction lies in the possibility of reducing dependence on signatures and identity cards while supporting electronic record retrieval and reporting.

Nevertheless, an attendance application designed for general timekeeping does not necessarily address the requirements of examination administration. Examination attendance must be associated with a specific examination and session, and the candidate must be registered and eligible for that event.

The present study consequently treats fingerprint verification as one component of a wider administrative workflow. The implementation integrates student biodata, examination records, session registration, biometric enrollment, eligibility checks, attendance creation, and reporting. This integration is the principal operational distinction of the proposed artifact.

### *2.3 Biometric template protection and privacy*

Biometric references require protection because disclosure may create long-term privacy and security consequences. Abdullahi et al. (2024) review

attacks against biometric templates and contemporary protection mechanisms, highlighting the importance of considering threats throughout the biometric processing lifecycle. Research on privacy-preserving authentication also examines approaches intended to reduce exposure of sensitive biometric information during storage and comparison.

ISO/IEC 24745:2022 provides an international framework for biometric information protection, including secure binding between biometric references and identity references. It also addresses confidentiality, integrity, revocability, and privacy-compliant processing.

The implementation described here uses Windows DPAPI to protect local development enrollment artifacts. This is a practical local protection mechanism, but it should not be equated with a cancelable biometric transformation, a cryptographic biometric template-protection algorithm, or a complete enterprise key-management architecture.

The distinction matters because encryption and template protection address related but different concerns. Encryption can restrict access to stored data under an appropriate security configuration, whereas cancelable biometric methods aim to produce protected representations that can be revoked and reissued under defined conditions.

### *2.4 Biometric performance evaluation*

A biometric system should not be evaluated solely by whether a fingerprint can be captured or whether a sample produces a successful match. Formal evaluation requires an appropriate protocol, defined test populations, repeated attempts, documented operating conditions, and relevant error measures.

ISO/IEC 19795-1:2021 establishes principles for biometric performance testing and reporting, including error rates, throughput, data recording, and test-protocol design.

Part 1: Principles and framework

Relevant measures may include:

- False match rate (FMR): the proportion of non-mated comparison attempts incorrectly accepted as matches.
- False non-match rate (FNMR): the proportion of mated comparison attempts incorrectly rejected as non-matches.
- Failure to acquire: the proportion of attempts in which a usable biometric sample is not acquired.
- Failure to enroll: the proportion of enrollment attempts that do not result in a usable reference.
- Verification latency: the time required to complete a defined verification transaction.
- Operational throughput: the number of successful or attempted verifications processed per unit of time under stated conditions.

These measures are not interchangeable. For example, the number of automated software tests passed cannot be used to calculate FMR or FNMR. Similarly, a successful hardware demonstration establishes that the reader integration works under the demonstrated conditions, not that the system has achieved a particular recognition accuracy.

### *2.5 Presentation attacks and sensor security*

Fingerprint systems may be exposed to presentation attacks involving artificial or altered biometric presentations. ISO/IEC 30107-3:2023 defines principles and methods for assessing presentation-attack detection mechanisms and reporting their results.

Part 3: Testing and reporting

The current implementation demonstrates physical-reader integration and fingerprint comparison, but presentation-attack detection was not independently evaluated. Accordingly, resistance to spoofing or other presentation attacks is not claimed as an established result.

### *2.6 Privacy and data protection in Nigeria*

Biometric data processed for uniquely identifying individuals requires careful consideration under applicable data protection requirements. The Nigeria Data Protection Act 2023 establishes the national legal framework for personal-data processing and associated rights and responsibilities.

For an institutional examination system, privacy considerations extend beyond database encryption. They include the purpose and lawful basis for processing, transparency to students, restrictions on access, retention and deletion, handling of biometric enrollment withdrawal, incident response, and

procedures for addressing access or correction requests.

The system's data-minimisation approach is a useful technical control, but it does not by itself establish legal compliance. Institutional deployment requires a documented privacy assessment and approval under the institution's applicable governance procedures.

### *2.7 Design science and information-system development*

Design science research is appropriate when a study produces and evaluates an information-system artifact intended to address a practical problem. The research process should connect the identified problem, objectives, design decisions, implementation, demonstration, evaluation, and communication of findings.

This study follows an artifact-oriented approach. It identifies weaknesses in examination attendance management, defines functional and security requirements, implements the application and biometric integration, demonstrates the resulting workflows, and evaluates the artifact using software tests and observed hardware integration behaviour.

### *2.8 Research gap*

The reviewed literature and standards establish the importance of biometric verification, reference protection, performance testing, and presentation-attack assessment. However, the implementation problem addressed in this study is more specific than fingerprint matching alone.

The research focuses on the integration of the following controls within one examination attendance workflow:

- Student identity resolution and active-record validation.
- Examination and session registration.
- Administrator-controlled biometric enrollment.
- Protected local enrollment artifacts.
- Live 1:1 fingerprint verification.
- Eligibility validation before attendance creation.
- Duplicate prevention through database integrity constraints.
- Operator attribution and audit logging.
- Attendance reporting and documented recovery limitations.

The study addresses this implementation gap through a working institutional artifact. Its contribution is an integrated, security-conscious implementation and technical evaluation, rather than a claim to have developed a new fingerprint recognition algorithm.

## 3. Materials and Methods

### *3.1 Study area and implementation context*

The study was conducted in the context of Oyo State College of Agriculture and Technology, Igboora, Oyo State, Nigeria. The institution provides the operational context for student biodata, departments, programmes, courses, examinations, examination sessions, attendance records, and examination administration.

The implemented artifact is designed for local operation on a designated Windows workstation connected to a DigitalPersona U.are.U 4500 fingerprint reader. The backend communicates with a MySQL database and invokes the native biometric bridge for reader operations.

The study describes a system implementation and technical evaluation. It does not claim that a representative population of students was recruited for a formal biometric accuracy trial.

### *3.2 Research design*

An applied design-science and software-engineering approach was adopted. The development process comprised:

1. Identification of examination attendance problems.
2. Specification of functional and non-functional requirements.
3. Design of the application architecture and data model.
4. Implementation of academic administration and attendance workflows.
5. Integration of the physical fingerprint reader.
6. Implementation of local enrollment-artifact protection.
7. Software testing, schema validation, and hardware integration checks.
8. Documentation of findings, limitations, and deployment requirements.

The evaluation was limited to evidence available from the implemented system. No unobserved biometric accuracy figures or population-level performance estimates were introduced.

### *3.3 Existing-system analysis*

The existing process was modelled as manual or paper-based examination attendance. In such a process, staff check names or identification details, mark attendance, and subsequently compile records for reporting.

The principal weaknesses considered in the system design were the risk of proxy attendance, slow verification, duplication, incomplete records, weak traceability, and the separation of attendance marking from formal examination registration.

The implemented system addresses these issues by integrating student records, session registration, biometric verification, eligibility validation, and electronic attendance recording.

### *3.4 Functional requirements*

The system was designed to support the following functions:

1. Authenticate authorised operators.
2. Manage departments, programmes, courses, and students.
3. Create examinations and examination sessions.
4. Register students for relevant examination sessions.
5. Restrict biometric enrollment to authorised administrative personnel.
6. Capture fingerprints using the connected DigitalPersona reader.
7. Compare a live sample with the claimed student's active enrollment reference.
8. Validate examination eligibility before attendance creation.
9. Prevent duplicate attendance for the same student and examination session.
10. Record operator identity and transaction timestamps.
11. Support enrollment revocation at the application-metadata level.

12. Generate, filter, print, and export attendance reports.

13. Record audit metadata while excluding unnecessary sensitive values.

### *3.5 Non-functional and security requirements*

The non-functional requirements included maintainability, data minimisation, database integrity, role-based access, safe API responses, rate limiting, operational error handling, and documented recovery procedures.

The security design also aimed to prevent biometric information from being unnecessarily exposed in browser responses, attendance records, or audit logs. These are implementation objectives; their effectiveness must be interpreted in light of the testing scope and deployment configuration.

### *3.6 System architecture*

The application comprises five principal logical components:

1. Presentation layer: HTML, Bootstrap, CSS, and JavaScript interfaces for administrative operations and attendance workflows.

2. Application and authorization layer: a Python/FastAPI backend responsible for request processing, authentication, authorization, validation, and business rules.

3. Academic and attendance data layer: MySQL persistence through SQLAlchemy, with schema evolution managed using Alembic.

4. Native biometric integration layer: a .NET bridge that communicates with the DigitalPersona SDK and physical reader.

5. Local enrollment-artifact protection layer: Windows DPAPI protection for the development artifacts used by the biometric integration.

The browser communicates with the backend rather than directly manipulating the biometric reference store. The backend coordinates academic checks and native reader operations before requesting attendance creation.

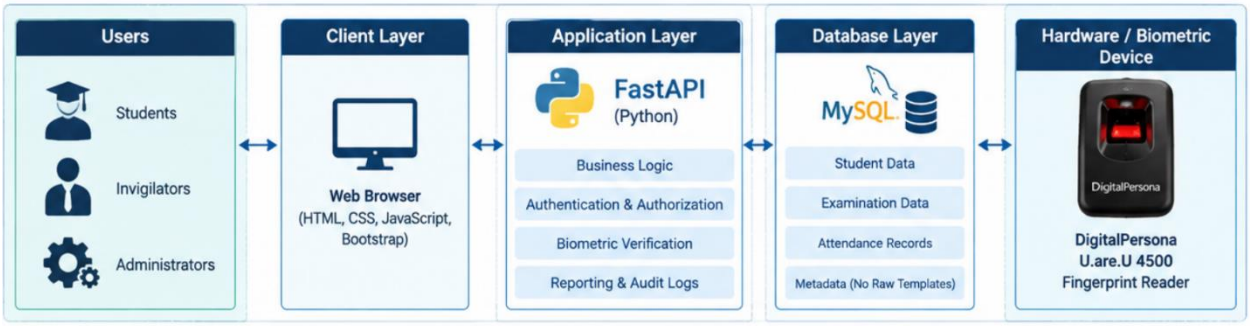



**Figure 3.1:** System Architecture of the Biometric Examination Attendance System

Figure 3.1. Proposed system architecture showing the presentation layer, FastAPI backend, authorization and eligibility controls, MySQL database, .NET biometric bridge, DigitalPersona reader, and protected local enrollment artifacts.

### *3.7 Database design*

The data model includes entities for operators, departments, programmes, courses, students, examinations, examination sessions, examination registrations, biometric enrollment metadata, attendance records, and audit events. Where applicable, revocation information is associated with the enrollment lifecycle.

The model separates examination registration from biometric enrollment. Registration establishes whether a student is eligible for a particular examination session, whereas enrollment establishes the reference required for biometric verification.

A database uniqueness constraint prevents duplicate attendance records for the same student and examination session. This constraint provides a persistence-level safeguard in addition to application-level validation.

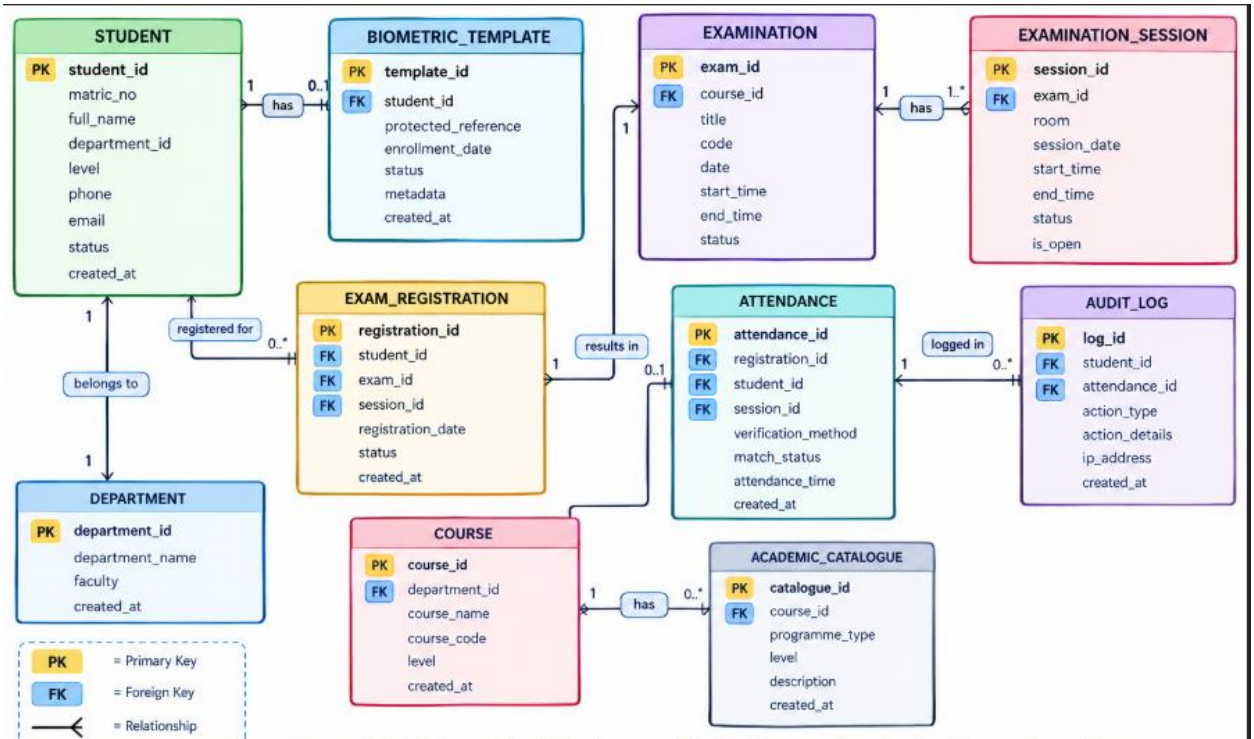



**Figure 3.2:** Entity-relationship diagram of the implemented academic, biometric metadata, attendance, and audit entities.

Figure 3.2. Entity-relationship diagram of the academic catalogue, student, examination, registration, biometric enrollment, attendance, operator, and audit entities.

### *3.8 Security and privacy design*

The security design incorporates administrator-controlled enrollment, role-protected operations, operator attribution, failed-attempt tracking, rate limiting, safe API responses, and restrictions on the disclosure of biometric data.

The system stores enrollment metadata and an opaque reference to a protected local artifact rather than raw fingerprint images or unprotected templates in MySQL. DPAPI is used to protect the relevant local development artifacts.

The protection boundary must be stated precisely. DPAPI protection is dependent on the Windows security context and deployment configuration. The current implementation does not establish a portable recovery mechanism, institution-wide key-management process, cancelable biometric scheme, or independent assurance against privileged endpoint compromise.

Accordingly, the design should be regarded as a controlled local implementation rather than a complete enterprise biometric protection architecture.

### *3.9 Examination verification and attendance workflow*

The verification workflow is designed to prevent a biometric match from automatically creating an attendance record without the necessary academic and operational checks.

The principal sequence is as follows:

1. The operator initiates verification using a student's matriculation number.
2. The system resolves the student record and checks the student's active status.
3. The application confirms that the examination session exists and is open.
4. The system verifies that the student is registered for the relevant examination session.

5. The system confirms that an active biometric enrollment reference is available.
6. The live fingerprint is acquired through the connected reader.
7. The native integration performs 1:1 comparison against the student's enrollment reference.
8. The application evaluates the verification result and relevant failure conditions.
9. Attendance is created only when all required conditions are satisfied.
10. The transaction records the appropriate attendance and audit metadata.

Failure conditions include missing or revoked enrollment, reader unavailability, acquisition timeout, unsuccessful comparison, ineligible registration, and duplicate attendance.

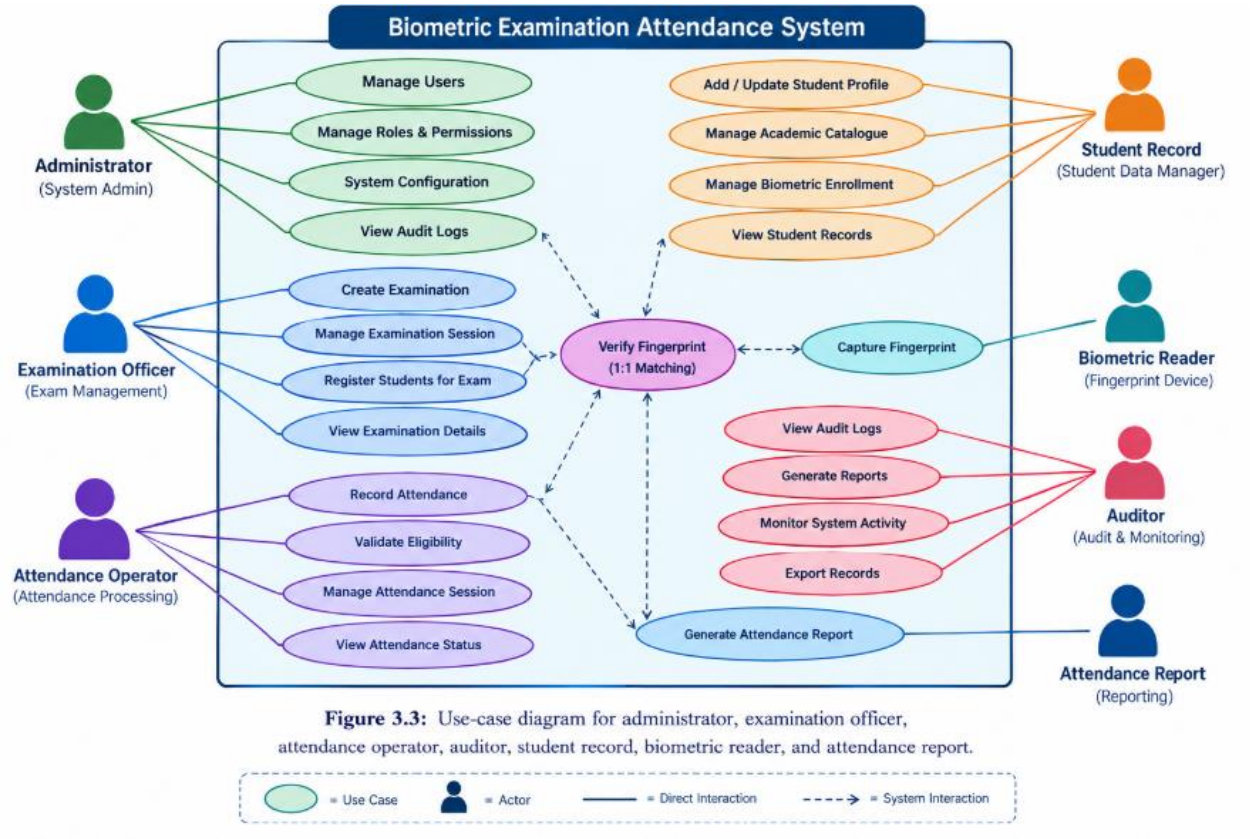



**Figure 3.3:** Use-case diagram for administrator, examination officer, attendance operator, auditor, student record, biometric reader, and attendance report.

Figure 3.3. Examination attendance verification workflow showing student lookup, session validation, registration checks, fingerprint acquisition, 1:1 comparison, eligibility decision, and transaction-safe attendance recording.

### *3.10 Data collection and analysis*

The evaluation evidence was obtained from automated software tests, compilation checks, database schema validation, and observed hardware integration operations. These sources were used to determine whether the implemented components and workflows operated as expected within the tested environment.

The available evidence included:

- The automated test suite, comprising 41 tests.
- Python compilation checks.

- Alembic schema validation, which detected no new upgrade operations.
- Demonstrations of reader opening and fingerprint capture.
- Demonstrations of enrollment-template creation.
- Observed successful and unsuccessful 1:1 verification outcomes.

The analysis was descriptive and implementation-focused. Test outcomes were used to establish functional feasibility and identify evaluation limitations. No false-match rate, false-non-match rate, population accuracy, or throughput estimate was calculated because the necessary controlled biometric dataset and measurement protocol were not available.

For a subsequent empirical evaluation, the recommended protocol is to document genuine and impostor attempts, reader and software versions, matching thresholds where exposed, acquisition failures, elapsed verification time, and the operational conditions under which each attempt occurs. Results should be reported using appropriate biometric performance measures and a reproducible test protocol.

## 4. System Implementation and Results

### *4.1 Development technologies*

The system was implemented using the technologies presented in Table 1.

**Table 1. Implemented technologies and their functions**

| Component | Technology | Function |
|---|---|---|
| Backend | Python and FastAPI | Request processing, validation, and application logic |
| Database | MySQL | Academic, enrollment metadata, attendance, and audit persistence |
| ORM and schema management | SQLAlchemy and Alembic | Database operations and schema versioning |
| Data validation | Pydantic | Request and response validation |
| Frontend | HTML, Bootstrap, CSS, JavaScript | Administrative interface and user interaction |
| Biometric integration | .NET native bridge and DigitalPersona SDK | Reader access, capture, and fingerprint comparison |
| Fingerprint reader | DigitalPersona U.are.U 4500 | Physical fingerprint acquisition |
| Local artifact protection | Windows DPAPI | Protection of local development enrollment artifacts |
| Deployment context | Windows workstation | Controlled single-machine operation |

The implemented backend uses Python and FastAPI, the biometric integration uses a .NET bridge, and the verified physical reader is the DigitalPersona U.are.U 4500. The distinction is documented to maintain consistency between the original proposal and the implemented artifact.

### *4.2 Landing page and institutional identity*

The landing page presents the OYSCATECH institutional identity, the purpose of the system, and the route to authorised operator access.

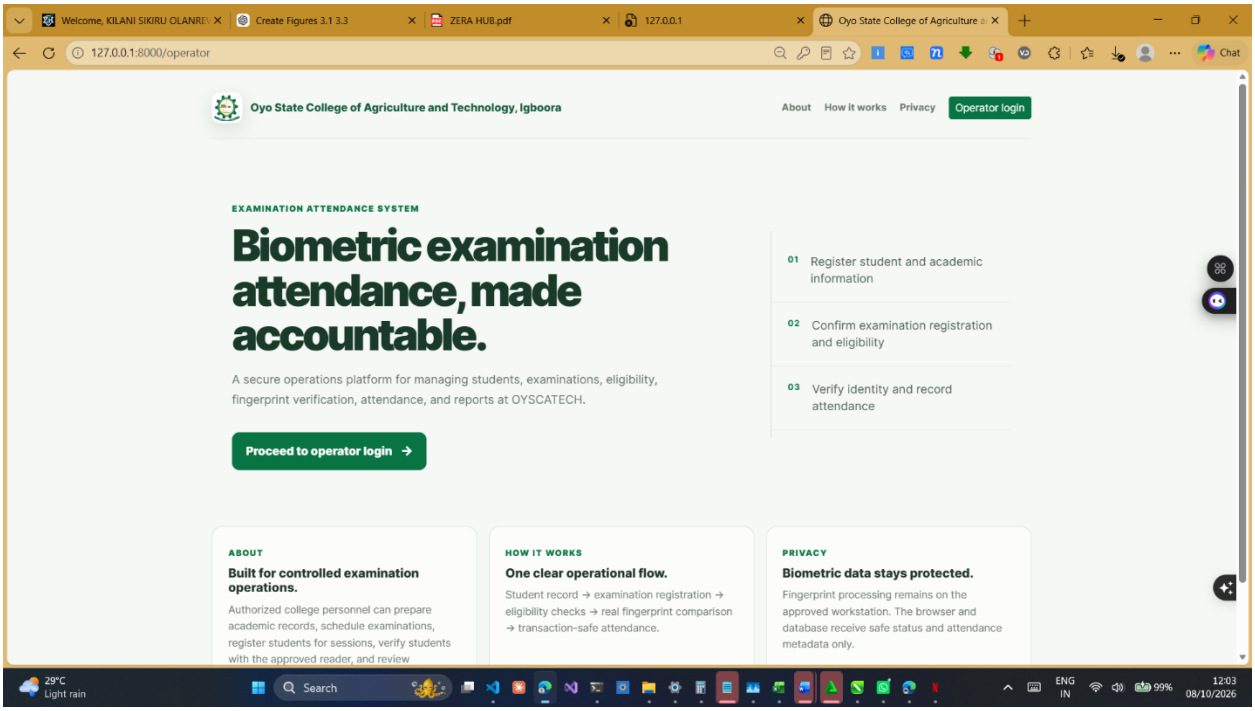



*Figure 4.1. Screenshot of the OYSCATECH biometric examination attendance system landing page.*

### *4.3 Operator authentication*

The authentication module provides access to authorised operators before protected administrative functions become available. Authentication establishes the operator's application identity, while authorization determines which operations the operator may perform.

Password hashes and other sensitive authentication values are not intended to be exposed in browser responses or routine API output.

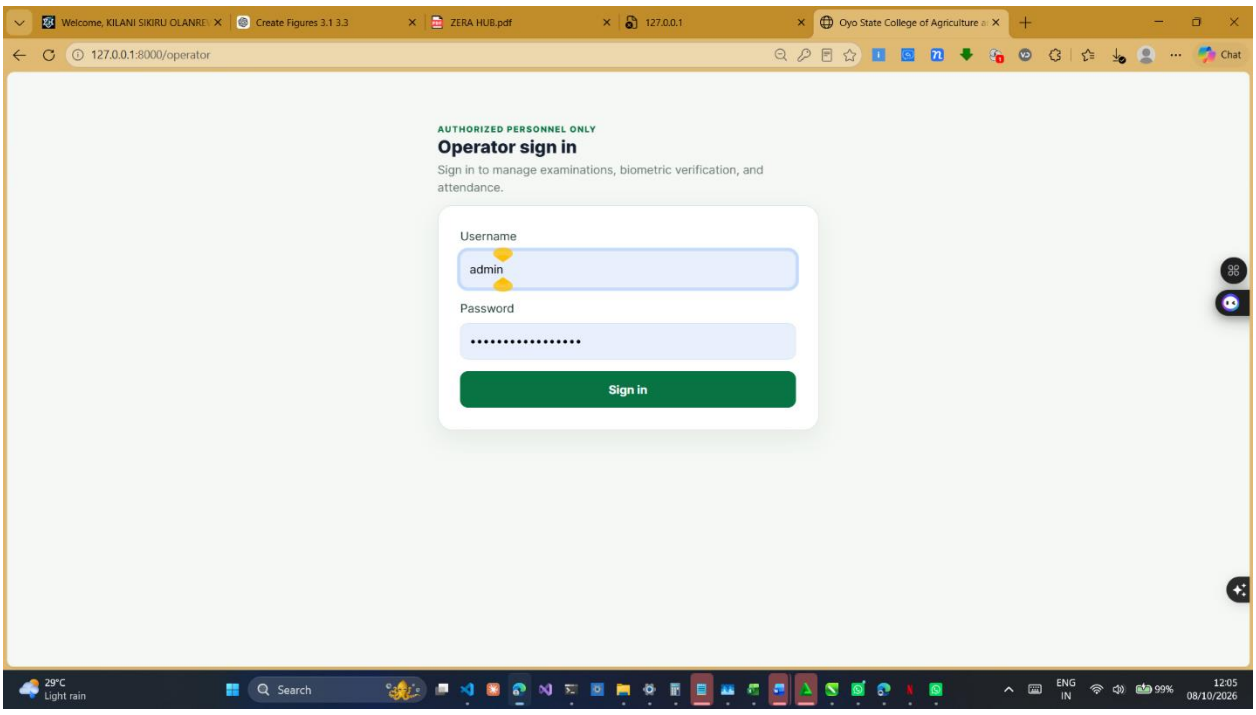



*Figure 4.2. Screenshot of the operator login page.*

### *4.4 Operator dashboard*

The dashboard provides navigation to the major application functions, including student management, academic catalogues, examinations, biometric enrollment, attendance verification, reporting, and audit records.

This structure separates the principal administrative tasks and provides a consistent entry point for authorised users.

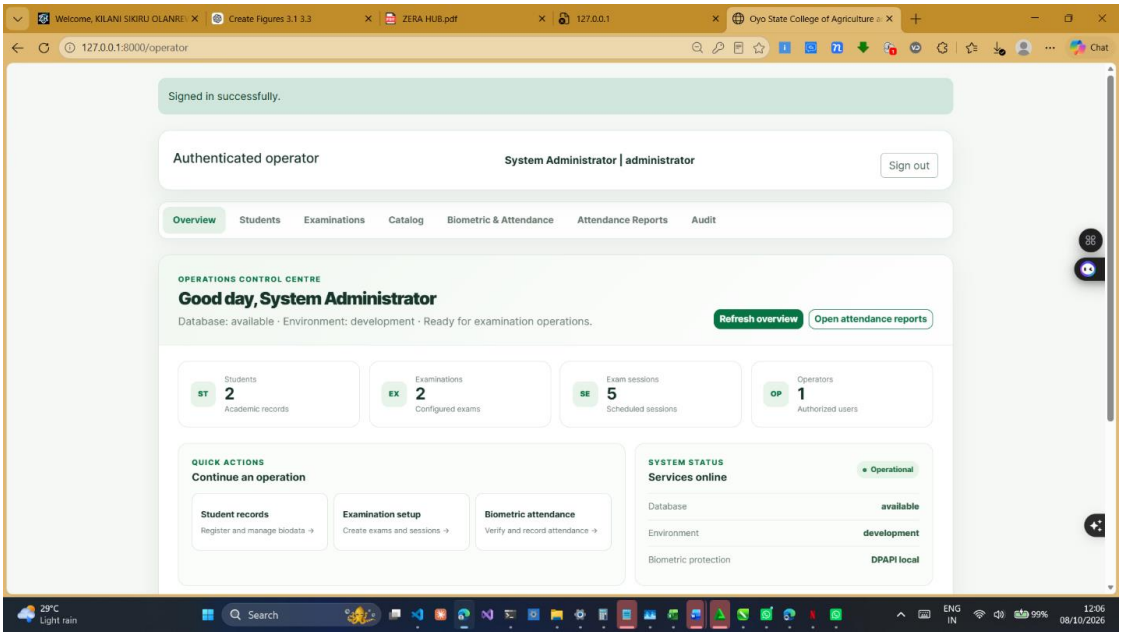



*Figure 4.3. Screenshot of the authenticated operator dashboard.*

### *4.5 Student biodata registration*

The student module supports the management of institutional biodata and academic information. The available fields include matriculation number, student name, programme or course of study, level, semester, and related academic attributes.

Department and programme records are established in the academic catalogue and referenced during student registration. This approach supports consistency between student records and the academic structures used in examination administration.

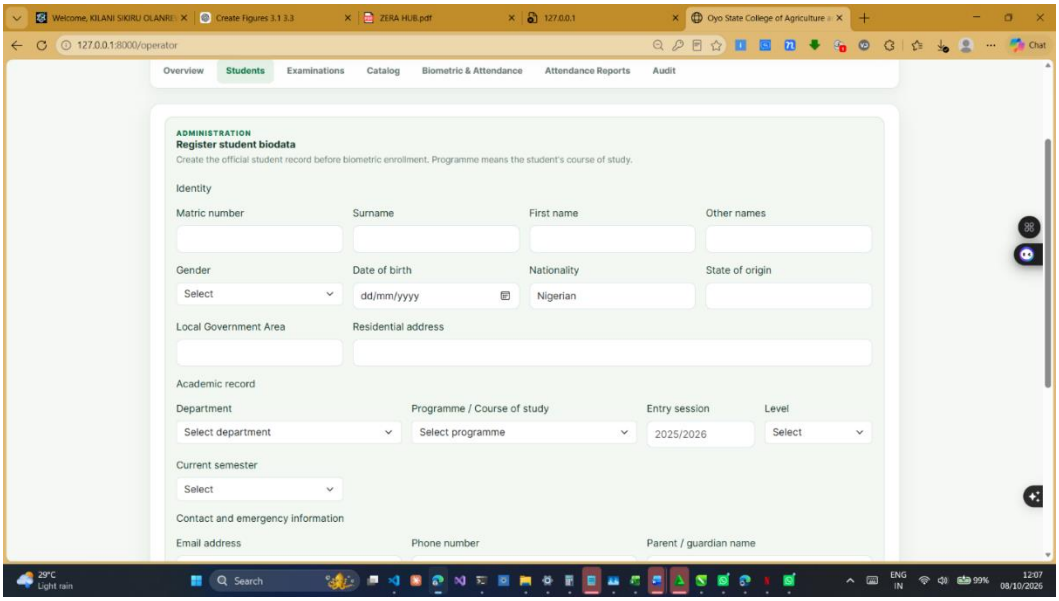



*Figure 4.4. Screenshot of the student biodata registration form.*

### *4.6 Examination and session management*

The examination management module enables authorised users to create examination records and sessions, maintain their status and relevant timing information, and associate them with the applicable academic records.

Examination registration is maintained separately from biometric enrollment. Consequently, possession of an enrolled fingerprint reference does not automatically confer eligibility to attend every examination.

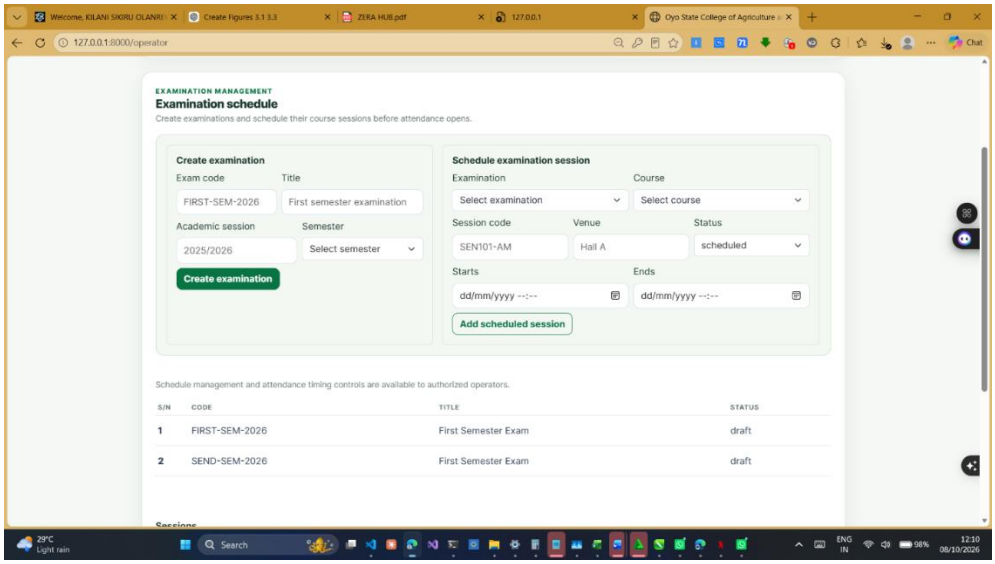



*Figure 4.5. Screenshot of the examination and examination-session management interface.*

### *4.7 Administrator-controlled biometric enrollment*

Biometric enrollment is restricted to the authorised administrative workflow. The process includes student lookup, identity confirmation, reauthentication, an approval reference, and administrator authorization.

Multiple real fingerprint captures are acquired from the same finger to support the enrollment process. The resulting enrollment artifact is created in memory and protected using DPAPI before the system retains the relevant reference and metadata.

The relational database does not store raw fingerprint images or unprotected fingerprint templates. However, the security of the local artifact remains dependent on the operating-system protection context, endpoint security, and the implementation's recovery arrangements.

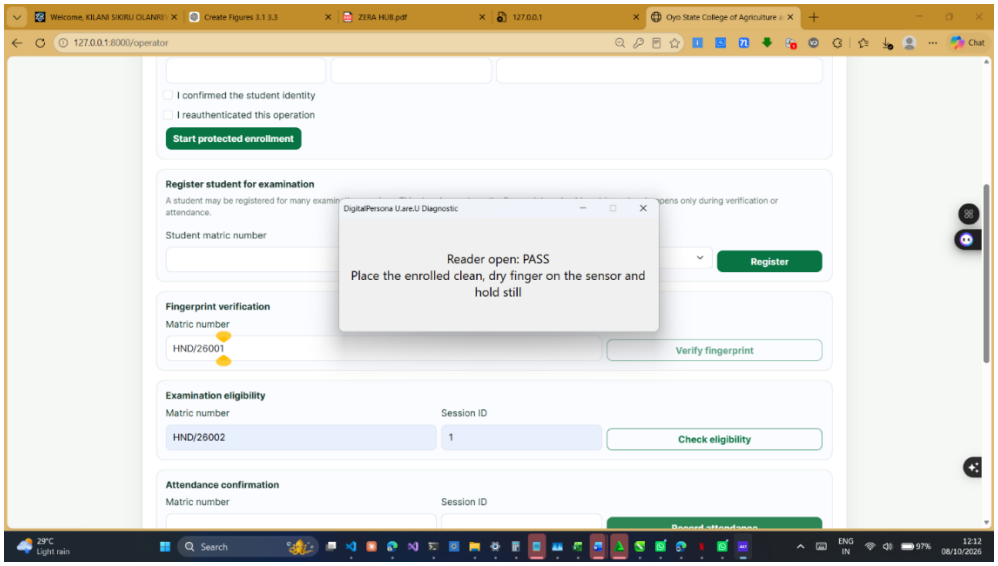



*Figure 4.6. Screenshot of the administrator-controlled biometric enrollment interface.*

### *4.8 Fingerprint verification and eligibility validation*

Verification begins with a matriculation number. The system resolves the student record, validates the relevant academic and enrollment conditions, acquires a live fingerprint, and performs 1:1 comparison against the student's active reference.

The application supports successful and unsuccessful comparison outcomes and handles operational failures such as missing enrollment, revoked enrollment, reader unavailability, and acquisition timeout.

The application-level result is not based solely on the fingerprint comparison. Examination eligibility and attendance rules are also evaluated before the attendance transaction can be completed.

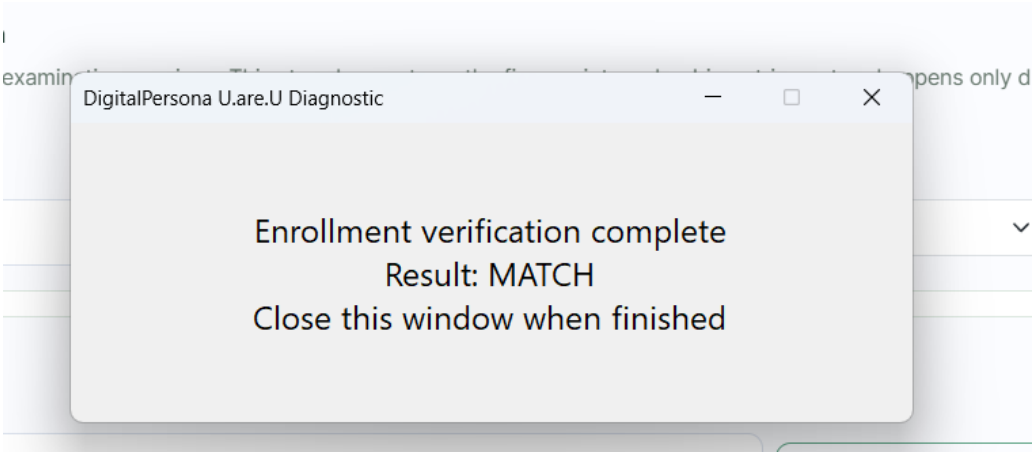



*Figure 4.7. Screenshot of the biometric verification interface showing a representative safe verification result.*

### *4.9 Attendance recording*

Attendance is recorded only after the required verification and eligibility conditions have been satisfied. The resulting record contains relevant academic and operational metadata, including the student, examination or session, attendance status, operator, verification outcome, and recording time.

The attendance record does not contain a raw fingerprint image or an unprotected biometric template. Database-level duplicate protection supplements the application workflow by preventing more than one attendance record for the same student and examination session.

### *4.10 Attendance reporting*

The attendance reporting module provides a structured view of recorded attendance. The report fields include serial number, matriculation number, student name, programme, department, level, examination, course, session, attendance status, verification outcome, and recorded time.

The interface supports filtering and pagination. Reports can be printed, saved through the browser's PDF workflow, and exported as CSV for administrative use.

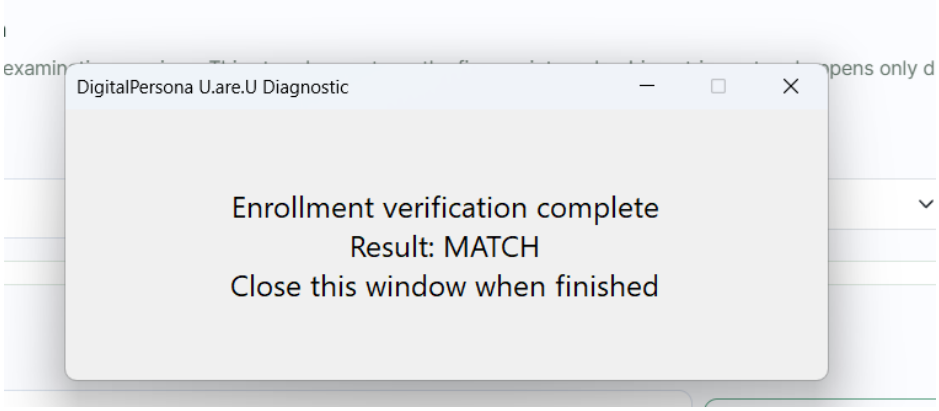



*Figure 4.8. Screenshot of the attendance reporting interface.*

### *4.11 Audit records*

The audit module provides metadata about relevant actions, entities, outcomes, operators, and timestamps. Its purpose is to support operational traceability and the investigation of disputed or unexpected events.

Audit records should exclude passwords, authentication tokens, DPAPI secrets, raw fingerprint images, unprotected templates, and unnecessary biometric comparison data. Their usefulness depends on the integrity of the audit trail and the authorization controls governing access to it.

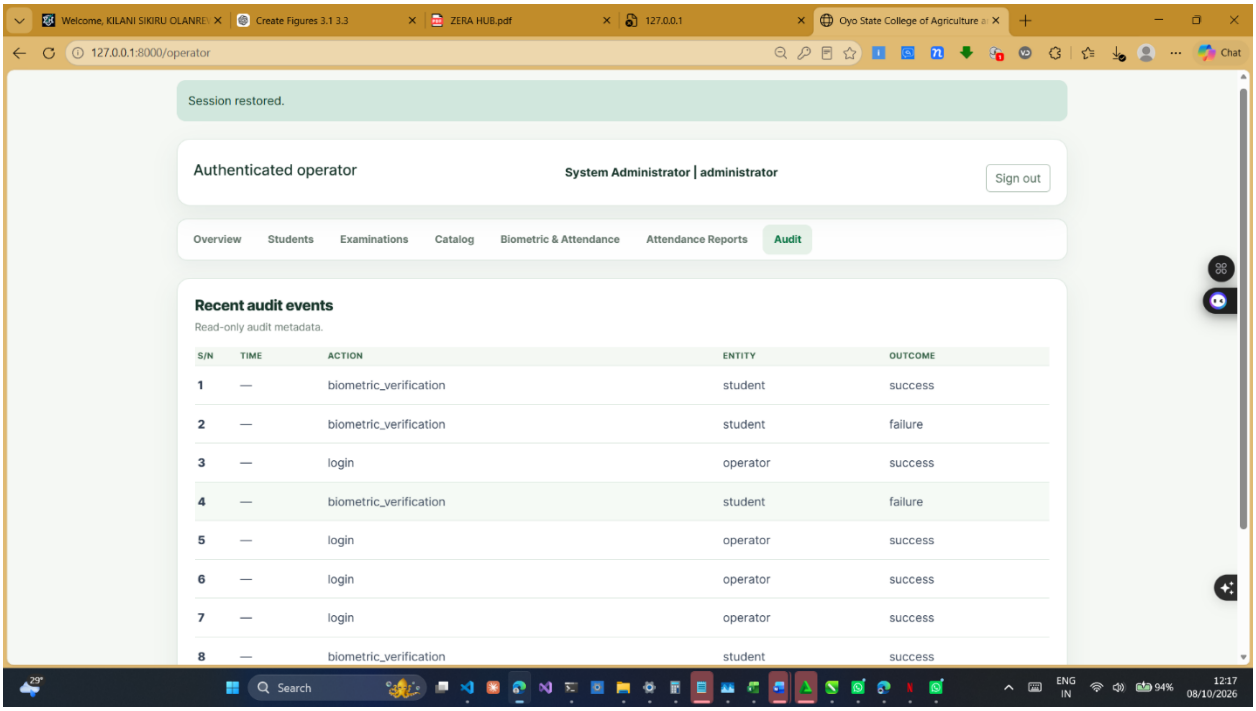



*Figure 4.9. Screenshot of the audit records interface.*

### *4.12 Software and integration test results*

The implementation was evaluated using the available automated software and hardware integration checks. The results are summarised in Table 2.

**Table 2. Summary of observed implementation checks**

| Evaluation item | Observed result | Interpretation |
|---|---|---|
| Automated test suite | 41 tests passed | The implemented test suite completed successfully |
| Python compilation | Checks completed | No compilation errors were reported by the checks performed |
| Alembic schema validation | No new upgrade operations detected | The current models and migration state showed no additional schema operations |
| Physical reader opening | Demonstrated | The application integration could access the reader under the demonstrated conditions |
| Fingerprint acquisition | Demonstrated | Real fingerprint capture was observed |
| Enrollment-template creation | Demonstrated | The enrollment workflow generated a reference for verification |

| Evaluation item | Observed result | Interpretation |
|---|---|---|
| 1:1 match outcome | Demonstrated | A successful comparison outcome was observed |
| 1:1 no-match outcome | Demonstrated | An unsuccessful comparison outcome was observed |
| Formal biometric error-rate evaluation | Not performed | FMR and FNMR remain unquantified |
| Presentation-attack evaluation | Not performed | Resistance to spoofing remains unestablished |
| Institutional-scale throughput study | Not performed | Population-level operational capacity remains unquantified |

The software test results support the conclusion that the tested application components operated as expected within the test environment. The hardware demonstrations provide evidence that the physical reader was integrated with the application and that the capture, enrollment, and comparison workflows were functional under the demonstrated conditions.

These findings must be interpreted within their scope. A passing software test suite does not establish that all possible security failures have been eliminated. Likewise, observing a match and a no-match outcome does not provide a statistically meaningful estimate of biometric recognition accuracy.

No numerical verification latency, false-match rate, false-non-match rate, failure-to-acquire rate, or presentation-attack detection rate is reported because these measures were not established through a dedicated empirical protocol.

### *4.13 Summary of implementation findings*

The implementation demonstrates the feasibility of combining institutional academic records, physical fingerprint acquisition, 1:1 verification, eligibility rules, attendance persistence, and administrative reporting in a single application.

The most important functional result is the separation of biometric identity verification from examination eligibility. A successful fingerprint comparison is necessary but not sufficient for attendance creation. This approach reduces the risk that a valid biometric reference alone will be treated as authorization to attend an examination.

The second important result is the separation of biometric enrollment metadata from raw fingerprint data. The database stores an opaque reference to a protected local artifact rather than an unprotected template. This improves data minimisation but does not eliminate the need for stronger lifecycle management and endpoint security before wider deployment.

## 5. Discussion

### *5.1 Integration of identity verification and academic eligibility*

The implemented system treats examination attendance as a controlled transaction rather than a simple biometric matching event. This is important because biometric verification establishes correspondence between a live sample and a claimed identity; it does not establish whether that identity is eligible for a particular examination.

By separating student identification, examination registration, session status, enrollment status, and attendance creation, the system provides a more complete operational model for examination administration. The same principle can be applied to other controlled institutional processes in which identity, authorization, and transaction validity must be established independently.

### *5.2 Contribution to biometric attendance system design*

The implementation extends the basic attendance-recording concept through its integration of academic data management, enrollment controls, biometric verification, database constraints, and auditability.

Its contribution is primarily architectural and implementation-oriented. It does not introduce a new fingerprint feature-extraction algorithm or claim superior matching performance relative to other biometric systems. Instead, it demonstrates how a commercially supported fingerprint reader can be integrated into a web-based examination workflow with explicit eligibility and transaction-integrity controls.

This distinction defines the appropriate interpretation of the research contribution: the work demonstrates a practical system architecture and its technical feasibility rather than a new biometric recognition technique.

### *5.3 Biometric data protection*

The decision not to store raw fingerprint images or unprotected templates in MySQL reduces direct exposure of biometric data through ordinary database queries and database exports. Protecting local enrollment artifacts using DPAPI provides an additional security boundary in the controlled Windows environment.

However, protection of an artifact does not automatically establish that the entire biometric lifecycle is secure. The operating-system context, endpoint compromise, backup procedures, artifact recovery, enrollment revocation, and administrative access remain important considerations.

Recent surveys of biometric template attacks and privacy-preserving authentication identify continuing challenges in protecting references and limiting the consequences of compromise (Abdullahi et al., 2024). <Cite refs={["turn745225search0","turn745225search10"]}/>

Before institutional deployment, the current protection mechanism should be reviewed against a documented threat model. The institution should also establish a supported recovery procedure, tested backup and restoration arrangements, controlled revocation, access restrictions, and procedures for replacing compromised enrollment references where technically possible.

### *5.4 Interpretation of technical evaluation*

The 41 automated tests, compilation checks, schema validation, and observed reader operations provide evidence of implementation feasibility. They support a conclusion that the application was developed beyond the design stage and that its principal software and biometric integration components were exercised.

Nevertheless, implementation testing and biometric performance evaluation answer different questions. Software testing examines whether specified behaviours and constraints operate as expected. Biometric evaluation measures recognition errors and operational performance under a defined test protocol.

ISO/IEC 19795-1:2021 provides relevant principles for planning and reporting biometric performance evaluation.

The absence of a controlled biometric dataset means that the current study cannot establish FMR, FNMR, or population-level accuracy. A subsequent evaluation should include sufficient genuine and impostor comparison attempts, acquisition-failure records, timing measurements, and documented decision conditions. The test protocol should also explain how samples were collected, how independence between observations was maintained, and how uncertainty in estimated performance measures was handled.

### *5.5 Presentation-attack resistance*

A working fingerprint reader and successful comparison workflow do not demonstrate resistance to artificial fingerprints or other presentation attacks. Such resistance depends on the reader's capabilities, the SDK and application behaviour, the threat model, and the presence and effectiveness of presentation-attack detection controls.

ISO/IEC 30107-3:2023 provides a framework for assessing presentation-attack detection mechanisms and reporting the results of those evaluations.

Because presentation-attack testing was not performed in this study, the system should not be described as spoof-proof. The issue remains a deployment requirement for a supervised institutional pilot, especially if the examination environment is expected to face deliberate attempts to defeat the verification process.

### *5.6 Privacy, governance, and institutional deployment*

The system processes identifiable student records and biometric enrollment information. A technically functioning implementation is therefore only one part of institutional readiness.

Before deployment, the institution should establish the applicable lawful basis for processing, provide appropriate notices to students, define retention and deletion rules, document who may enroll or revoke biometric references, and specify how complaints and data-subject requests will be handled. The institution should also determine whether a formal data-protection impact assessment or other review is required.

DPAPI protection should not be represented as a substitute for institutional privacy governance. Similarly, the presence of audit records does not automatically demonstrate compliance unless audit integrity, access, retention, and review responsibilities are defined.

### *5.7 Operational suitability*

The current implementation is suitable as a technical feasibility demonstration in a controlled, single-workstation environment. Its local deployment model simplifies hardware access and avoids introducing untested distributed biometric workflows.

However, an institution-wide system may require concurrent workstation support, centralised configuration management, operational monitoring, resilient backups, disaster recovery, and carefully controlled communication between application nodes. These capabilities must be implemented and tested before extrapolating the current results to a multi-workstation environment.

## 6. Conclusion

This study designed, implemented, and technically evaluated a fingerprint-based examination attendance management system for tertiary institutions, using OYSCATECH as the implementation context. The system integrates student biodata, academic catalogues, examination sessions, student registration, administrator-controlled biometric enrollment, real DigitalPersona fingerprint capture, 1:1 comparison, eligibility validation, transaction-safe attendance recording, reporting, and audit logging.

The implementation passed 41 automated tests, Python compilation checks, and database schema validation. Real reader access, fingerprint capture, enrollment-template creation, and successful and unsuccessful comparison outcomes were also demonstrated. These findings provide evidence of technical feasibility within the controlled, single-workstation environment in which the system was tested.

A central contribution is the integration of biometric identity verification with academic eligibility and attendance transaction rules. The system does not treat a fingerprint match as sufficient authorization to record attendance. It also avoids storing raw fingerprint images or unprotected templates in MySQL, using DPAPI-protected local development artifacts and database-held enrollment metadata instead.

The findings should not be interpreted as proof of population-level biometric accuracy, presentation-attack resistance, or unrestricted production readiness. Before broader deployment, the system requires formal biometric performance evaluation, presentation-attack testing, recovery validation, privacy and security review, and supervised institutional pilot testing.

The study therefore establishes a practical foundation for secure electronic examination attendance management while identifying the empirical and governance requirements that must be addressed before the system can be considered ready for institution-wide operation.

**References**

Abdullahi, S. M., Sun, S., Wang, B., Wei, N., & Wang, H. (2024). Biometric template attacks and recent protection mechanisms: A survey. *Information Fusion, 103*, Article 102144. https://doi.org/10.1016/j.inffus.2023.102144

Arman, S. M., Yang, T., Shahed, S., Al Mazroa, A., Attiah, A., & Mohaisen, L. (2024). A comprehensive survey for privacy-preserving biometrics: Recent approaches, challenges, and future directions. *Computers, Materials & Continua*, *78*(2), 2087–2110. https://doi.org/10.32604/cmc.2024.047870

Federal Republic of Nigeria. (2023). *Nigeria Data Protection Act, 2023*. https://ndpc.gov.ng/wp-content/uploads/2024/03/Nigeria_Data_Protection_Act_2023.pdf

Hayat, A., Ali, S. S., Bhateja, A. K., & Werghi, N. (2024). FinTem: A secure and non-invertible technique for fingerprint template protection. *Computers & Security, 142*, Article 103876. https://doi.org/10.1016/j.cose.2024.103876

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75–105. https://doi.org/10.2307/25148625

International Organization for Standardization & International Electrotechnical Commission. (2021). *ISO/IEC 19795-1:2021: Information technology—Biometric performance testing and reporting—Part 1: Principles and framework*. https://www.iso.org/cms/live/live/en/sites/isoorg/contents/data/standard/07/35/73515.html

International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 24745:2022: Information security, cybersecurity and privacy protection—Biometric information protection*. https://www.iso.org/standard/75302.html

International Organization for Standardization & International Electrotechnical Commission. (2023). *ISO/IEC 30107-3:2023: Information technology—Biometric presentation attack detection—Part 3: Testing and reporting*. https://www.iso.org/standard/79520.html

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology,*

*14*(1), 4–20. https://doi.org/10.1109/TCSVT.2003.818349

Lahmidi, A., Moujahdi, C., Minaoui, K., Rziza, M., et al. (2022). On the methodology of fingerprint template protection schemes conception: Meditations on the reliability. *Journal on Information Security, 2022*, Article 3. https://doi.org/10.1186/s13635-022-00129-6

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems, 15*(4), 251–266. https://doi.org/10.1016/0167-9236(94)00041-2

Onyishi, D. U., & Igbinoba, C. K. (2021). Design and implementation of a biometric students' time and attendance logging system. *Nigerian Journal of Technology*, *40*(3), 484–490. https://doi.org/10.4314/njt.v40i3.14

Patel, V. M., Ratha, N. K., & Chellappa, R. (2015). Cancelable biometrics: A review. *IEEE Signal Processing Magazine*, *32*(5), 54–65. https://doi.org/10.1109/MSP.2015.2434151

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, *40*(3), 614–634. https://doi.org/10.1147/sj.403.0614

Sumalatha, U., Krishna Prakasha, K., Prabhu, S., & Nayak, V. C. (2024). A comprehensive review of unimodal and multimodal fingerprint biometric authentication systems: Fusion, attacks, and template protection. *IEEE Access*, *12*. https://doi.org/10.1109/ACCESS.2024.3395417

Wang, S., & Hu, J. (2016). A blind system identification approach to cancelable fingerprint templates. *Pattern Recognition*, *54*, 14–22. https://doi.org/10.1016/j.patcog.2016.01.001