Engineering and Technology Journal e-ISSN: 2456-3358
**Volume 11 Issue 06 June-2026, Page No.- 10702- 10715**
**DOI: 10.47191/etj/v11i06.46, I.F. – 8.595**


# Design, Development, and Quality Evaluation of A Tensorflow.Js-Based Multiple Face Recognition System For Campus Gate Enrollment Verification

**Kyle Andrei Domingo[1], John Guiller Hernando[2], Eliza B. Ayo[3]**
[1,2,3] School of Science and Technology, Centro Escolar University – Manila, Philippines

**ABSTRACT:** Manual student enrollment verification at institutional entry gates is susceptible to human error, identity misrepresentation, and administrative inefficiencies — particularly during high-volume entry periods. This study describes the design, development, and evaluation of the Multiple Face Recognition System (MFRS), a browser-based, gate-deployed biometric platform developed using TensorFlow.js and face-api.js for real-time student identity verification and enrollment status validation in higher education institutions. Grounded in the Technology Acceptance Model and the Systems Development Life Cycle, the MFRS was built using a descriptive-developmental research design and implemented with React.js, Node.js, Express, and PostgreSQL. Core system features include simultaneous detection and recognition of up to three faces per scanner request, Euclidean-distance facial matching against a centralized template database, active head-turn liveness validation, role-based access control for administrators and security personnel, and automated timestamped enrollment verification logging. The system was evaluated through technical quality assurance testing, expert assessment using ISO/IEC 25010 software quality criteria (n = 5 technical evaluators), and a student respondent acceptance survey (n = 50). Results indicated an overall technical evaluation mean of 3.99 (Excellent) and a student acceptance mean of 4.32 (Excellent), with Usability rated Outstanding (M = 4.50). Backend API performance averaged 6.37 milliseconds per response under controlled conditions. Overall recognition accuracy reached 77.05% under controlled conditions, while the active liveness validation success rate was 53.85%, indicating the need for further anti-spoofing development before full institutional deployment. The MFRS constitutes a functional prototype with a clearly defined improvement pathway for gate-based biometric enrollment verification in Philippine higher education.

**KEYWORDS:** Multiple Face Recognition, Tensorflow.Js, Enrollment Status Verification, Biometric Authentication, ISO/IEC 25010, Liveness Detection, Gate-Based Verification, Technology Acceptance Model, Educational Institutions.

## 1. INTRODUCTION

The rapid digitalization of higher education has intensified institutional demand for secure, accurate, and efficient systems to manage student identity verification and campus access control. At institutional entry gates, traditional verification processes — relying on physical identification cards, manual inspection, and security personnel judgment — remain commonplace despite well-documented limitations including human error, identity fraud, unauthorized campus access, and administrative inefficiencies (Mendoza & Cruz, 2022). These challenges are amplified in high-volume campus environments where confirming each student's enrollment status manually at multiple entry points is operationally impractical.

Advances in biometric authentication, and facial recognition in particular, offer a compelling pathway for addressing these limitations. Facial recognition technology operates contactlessly, integrates with standard webcam hardware, and supports rapid automated identification without requiring physical tokens (Jain & Ross, 2021; Li & Zhao, 2024). Deep learning architectures have substantially improved recognition precision through high-dimensional facial embeddings and sophisticated feature extraction pipelines, enabling reliable identification under variable lighting conditions and camera angles characteristic of gate entry environments (Kumar & Singh, 2023; Zhang & Li, 2023).

In the Philippine higher education context specifically, many institutions continue to depend on manual gate monitoring and physical ID-based identity checking, practices that may yield inconsistent verification outcomes during peak entry hours, incomplete records, and limited real-time visibility into enrollment-based campus access patterns. These systemic limitations represent a substantive research and practical gap warranting targeted technological intervention.

Responding to this gap, this study presents the Multiple Face Recognition System (MFRS), a gate-deployed biometric platform designed for enrollment status verification in educational institutions. The MFRS integrates real-time multiple face detection and recognition, enrollment status cross-referencing, active liveness validation, device management, role-based access control, and automated verification logging into a single cohesive web-based platform. The system was developed and evaluated against the ISO/IEC 25010 software quality framework to ensure systematic assessment across multiple quality dimensions beyond recognition accuracy alone.

**1.1 Research Problem**

research problem addressed in this study is the pervasive reliance on manual student enrollment verification processes at institutional entry gates in higher education, which are highly susceptible to human error, identity misrepresentation, and administrative inefficiencies, particularly during peak traffic periods. This operational impracticality leads to inconsistent access control, incomplete security records, and a distinct lack of real-time visibility into student enrollment status. While biometric alternatives like facial recognition exist, current localized academic implementations are limited to controlled environments and lack critical features necessary for gate deployment, such as simultaneous multiple face processing, cross-referencing with live enrollment databases, presentation attack (spoofing) safeguards, and validation against standardized software quality frameworks

**1.2 Gap in the Literature**

The substantive gap in the existing literature centers on the lack of a unified, gate-deployed biometric platform tailored for higher education that simultaneously handles multi-face processing, live database verification, and robust anti-spoofing. While prior research in the Philippine educational context has demonstrated the feasibility of camera-based facial recognition for classroom or laboratory attendance, those systems remain confined to controlled environments and are missing critical campus access features. Specifically, current literature lacks a singular solution that integrates real-time, simultaneous recognition of multiple faces (up to three) at high-traffic entry points, cross-references those faces with a centralized, real-time enrollment database, embeds active liveness validation to prevent presentation attacks (such as photo or screen-replay spoofing), and undergoes formal software quality assessment based on the ISO/IEC 25010 framework.

**1.3 Objectives of the Study**

The primary objective of this study was to design, develop, and evaluate the Multiple Face Recognition System (MFRS), a browser-based, gate-deployed biometric platform tailored for student enrollment status verification at institutional entry points in Philippine higher education. Specifically, the study sought to engineer a system capable of executing real-time, simultaneous detection and recognition of up to three faces per scanner request , matching facial data against stored templates using Euclidean distance , and cross-referencing those identities with a centralized database to validate live enrollment status. Additionally, the objective included implementing active head-turn liveness validation to mitigate spoofing attempts , establishing automated timestamped verification logging and role-based access control , and rigorously assessing the platform's technical quality and user acceptability using the ISO/IEC 25010 software quality framework alongside surveys administered to technical experts, students, and security personnel.

**1.4 Significance of the Study**

This study holds significance for contribution toward modernizing campus security and administrative efficiency within higher education, particularly in the Philippine context, by replacing error-prone manual gate verification with a secure, automated biometric platform. For **educational institutions and security personnel**, the study provides a scalable, web-deployed blueprint that streamlines peak-hour traffic management, prevents identity fraud, and ensures real-time visibility into enrollment-based campus access patterns. For **software developers and biometric researchers**, the study offers valuable technical baselines for executing browser-side, multiple face inference using TensorFlow.js in resource-constrained environments, while illustrating how to balance high security with functional design. Finally, the study contributes to **academic literature and regulatory compliance** by successfully bridging the gap between deep learning engineering and local data privacy mandates (such as the Data Privacy Act of 2012), establishing a formal ISO/IEC 25010-based quality evaluation framework that can guide future institutional implementations of sensitive biometric technologies.

**1.5 Scope and Delimitations**

MRFS is focused on the design, development, and quality evaluation of the Multiple Face Recognition System (MFRS), a full-stack, web-based biometric platform engineered specifically for real-time student identity verification and enrollment status validation. The study was conducted at Centro Escolar University – Manila, with physical testing delimited to the North Quadrangle and South Gate entry points to simulate realistic, high-volume campus entry conditions. Technically, the platform is restricted to detecting and recognizing a maximum of three faces simultaneously per scanner request using TensorFlow.js and face-api.js (TinyFaceDetector), utilizing 128-dimensional descriptor vectors compared via a hardcoded Euclidean distance threshold of 0.55 and a distinctiveness gap of 0.08. The evaluation is strictly delimited to a specific sample size consisting of five technical evaluators who assessed the system against selected ISO/IEC 25010 product quality characteristics, 50 student respondents who served as scanned subjects and completed acceptance questionnaires based on the Technology Acceptance Model (TAM), and six security guards who operated the stations. Furthermore, the system's anti-spoofing capability is delimited to an active challenge-response mechanism requiring a specific head-turn action, rather than deploying depth-sensing hardware or passive texture analysis. Finally, the platform is functionally constrained to enrollment verification and automated access logging, purposely omitting integration into broader institutional ecosystems like Student Information Systems (SIS) or Learning Management Systems (LMS) , and its performance benchmarks reflect controlled local laboratory and multi-condition field test environments rather than scaled institutional network traffic.

### 1.5 Theoretical Framework

This study is grounded in two complementary theoretical foundations. The Technology Acceptance Model (TAM; Davis, 1989) posits that user adoption of technology is determined primarily by perceived usefulness and perceived ease of use. Within this study, TAM provided the conceptual basis for designing the student respondent acceptance evaluation and interpreting acceptance outcomes across usability, functional suitability, and perceived utility dimensions.

The Systems Development Life Cycle (SDLC) theory provided the structural framework for the systematic planning, design, development, testing, and iterative refinement of the MFRS. The Agile implementation of the SDLC employed in this study facilitated continuous feedback integration and incremental system improvement throughout the development process. Together, TAM and SDLC supported the study's dual focus on producing a technically sound system and validating its acceptance among intended users.

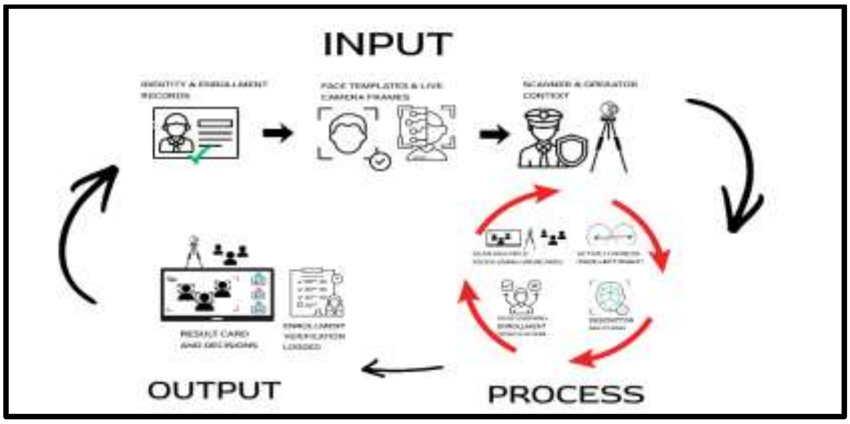


**Fig. 1. Conceptual Framework**

## LITERATURE REVIEW

This review synthesizes literature from 2020 onward across four thematic domains most pertinent to the MFRS: (a) biometric systems and facial recognition in educational settings, (b) deep learning approaches to facial recognition, (c) liveness detection and anti-spoofing, and (d) privacy, user acceptance, and software quality evaluation. Both international and Philippine-based literature are integrated within each theme.

### Biometric Systems and Facial Recognition in Educational Settings

The adoption of biometric technologies in educational institutions has expanded significantly as institutions seek to improve identity assurance, automate administrative processes, and strengthen access control (Necochea-Chamorro et al., 2024). Among biometric modalities, facial recognition has emerged as particularly attractive because it operates contactlessly, integrates with existing camera infrastructure, and minimizes disruption to daily workflows (Li & Zhao, 2024; Pattnaik & Mohanty, 2020). Raheem et al. (2021) reported that facial recognition combined with machine learning can substantially improve identity capture speed and convenience compared with conventional methods, directly supporting its applicability in gate-monitoring contexts.

In the Philippine educational context, several studies have demonstrated the feasibility of deploying facial recognition systems for attendance and identity monitoring. Balagtas et al. (2023) implemented an attendance monitoring system using Viola-Jones and Principal Component Analysis algorithms, demonstrating that facial recognition can function effectively in local institutional environments. However, their system focused exclusively on attendance recording and lacked enrollment status verification, device registration, or anti-spoofing safeguards. Similarly, Valenzuela et al. (2025) developed a facial recognition attendance monitoring system for laboratory settings, confirming the practical utility of camera-based identification in controlled academic environments but without gate-based deployment or enrollment status cross-referencing. Domingo and Ladia (2024) extended facial recognition application to employee attendance management, demonstrating integration with web-based reporting platforms while remaining outside the student identity verification domain. These local studies collectively affirm the readiness of Philippine educational institutions for biometric deployment while revealing a consistent gap: the absence of systems that simultaneously address enrollment status verification, multiple face recognition, anti-spoofing, and formal quality evaluation at campus entry points.

Mondal and Mondal (2024) provided broader empirical context, showing through a systematic review that attendance collection in educational settings remains heavily dependent on manual and semi-digital methods, even when automated approaches demonstrably improve consistency and reduce administrative burden. This finding substantiates the institutional need that the MFRS was designed to address.

### Deep Learning and Facial Recognition Pipeline Design

The performance of modern facial recognition systems is substantially attributable to deep learning architectures that generate high-dimensional face embeddings enabling finegrained identity discrimination (Kumar & Singh, 2023). Boe et al. (2024) demonstrated that recognition accuracy in institutional settings is directly influenced by image capture quality, facial alignment, and the calibration of recognition thresholds -- considerations that directly informed the MFRS design, particularly in its use of the TinyFaceDetector model, 128-dimensional descriptor vectors, and a Euclidean distance threshold of 0.55 with a distinctiveness gap of 0.08. Zhang and Li (2023) further established that efficient facial recognition deployment is achievable in resource-constrained educational environments through browser-based frameworks such as TensorFlow.js, validating the architectural choice of client-side inference in the MFRS.

Identity verification in higher education has increasingly been examined as a systems-level challenge. Nguyen and Roberts (2022) reviewed current practices and emerging technologies, noting that reliable enrollment verification requires both accurate recognition and integration with institutional record systems -- a dual requirement that the MFRS directly addresses through its two-stage verification pipeline combining facial matching with enrollment database cross-referencing. Rahman et al. (2021) similarly argued that integrating facial recognition into institutional workflows can reduce identity errors, automate verification logging, and streamline security operations.

**Liveness Detection and Anti-Spoofing**

Facial recognition accuracy alone does not guarantee secure authentication; presentation attack resistance is an equally critical requirement in security-sensitive deployments. Xing et al. (2025) provided a comprehensive review of face anti-spoofing approaches based on deep learning, establishing that passive texture analysis and active challenge-response mechanisms represent the principal methodological families for distinguishing live faces from fabricated representations. Antil et al. (2025) similarly argued that presentation attack detection has become indispensable in institutional biometric systems because matching accuracy provides no defense against photograph-based or screen-replay spoofing attempts. These findings directly motivated the inclusion of active liveness validation in the MFRS, which requires a head-turn action before accepting a scan result, providing a behavioral challenge that static or replayed presentations cannot satisfy.

**Privacy, User Acceptance, and Governance**

The governance and acceptance dimensions of facial recognition deployment are essential co-determinants of institutional viability. The National Academies of Sciences, Engineering, and Medicine (2024) emphasized that mature facial recognition systems require clear auditability mechanisms, proportionate data use, and policy frameworks governing their institutional application -- considerations reflected in the MFRS through its verification logging, role-based access control, and data minimization design. Chen and Wang (2023) highlighted cross-jurisdictional tensions between operational efficiency and privacy protection, reinforcing the importance of embedding governance considerations directly into system design rather than treating them as post-deployment concerns.

In the Philippine regulatory context, the National Privacy Commission (NPC, 2023) issued guidance classifying facial recognition templates as sensitive personal information under the Data Privacy Act of 2012 (Republic Act 10173), requiring institutions to establish lawful processing bases, implement technical security measures, and disclose biometric data practices to data subjects. The NPC (2025) subsequently affirmed that proportionality and data minimization principles must govern the scope of biometric collection, reinforcing the MFRS's delimitation to enrollment verification purposes only.

Regarding user acceptance, Choung et al. (2024) found that adoption of AI-powered facial recognition in institutional contexts depends significantly on trust, perceived security benefit, and privacy risk perception. Wang et al. (2024) similarly reported that student acceptance of facial recognition is shaped by trust and perceived privacy risk. These findings guided the design of the student respondent evaluation instrument and the interpretation of acceptance results in this study.

**Software Quality Evaluation**

The ISO/IEC 25010:2023 standard specifies eight product quality characteristics -- functional suitability, performance efficiency, compatibility, usability, reliability, security, maintainability, and portability -- that together provide a systematic multi-dimensional framework for evaluating software systems (ISO, 2023). Rojas (2025) identified sustained research attention to ISO/IEC 25010 across software domains, affirming its continuing relevance as a structured quality assessment instrument. For the MFRS, ISO/IEC 25010 provided the structural basis for the technical evaluation instruments administered to expert evaluators, ensuring that system quality was assessed comprehensively rather than on recognition accuracy alone.

**Research Gap and Study Contribution**

Across the reviewed literature and related systems, a substantive research gap is evident: no existing system reviewed integrates simultaneous multiple face recognition at campus entry gates, real-time enrollment status cross-referencing, active liveness validation, and formal ISO/IEC 25010 quality evaluation within a single platform designed specifically for Philippine higher education. The MFRS addresses this gap by unifying these capabilities within a role-based, web-deployed, and formally evaluated biometric verification platform. This gap justifies the study's developmental focus and positions the MFRS as a meaningful and original contribution to biometric systems development in the local higher education context.

## 3. METHODOLOGY

### 3.1 Research Design

This study employed a descriptive-developmental research design. The developmental component entailed the systematic design, construction, and iterative refinement of the MFRS through five structured phases. The descriptive component provided the analytical framework for evaluating and characterizing the system's technical performance, functional completeness, and user acceptance across ISO/IEC 25010 quality dimensions.

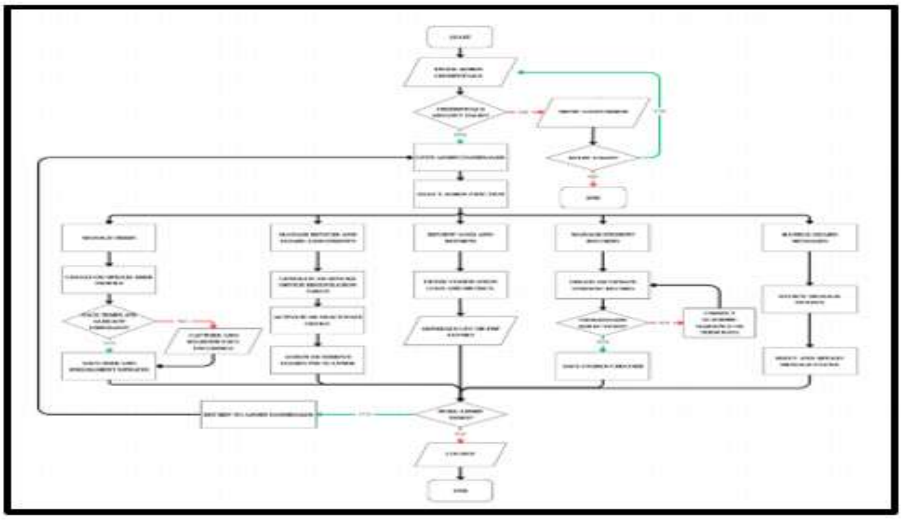

**Fig. 2. System Flowchart**

### 3.2 Research Locale

System development and evaluation were conducted at Centro Escolar University -- Manila, specifically at the North Quadrangle and South Gate entry points, which served as the primary testing environment for assessing system performance under realistic campus entry conditions.

### 3.3 System Architecture and Technology Stack

The MFRS is implemented as a full-stack web application organized into four functional layers: (a) a hardware layer comprising webcam-equipped scanner workstations and display units at designated entry gates; (b) a processing layer that executes face detection, facial landmark extraction, face descriptor generation, active liveness validation, and Euclidean distance matching; (c) a data layer storing student profiles, facial encoding templates, scanner device records, guard assignments, verification outcomes, and enrollment verification logs; and (d) an application layer providing web-based dashboards for administrators and scanner interfaces for security personnel.

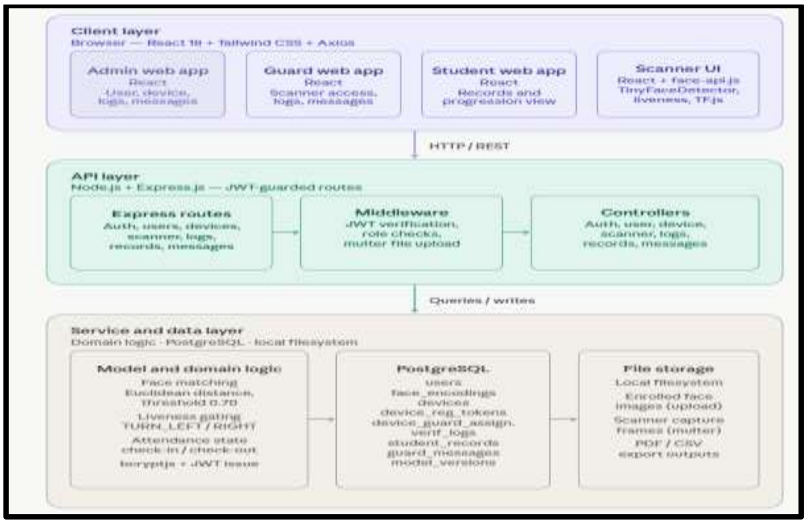


**Fig. 3. System Architecture and Technology Stack**

Client-side facial recognition was implemented using TensorFlow.js and face-api.js, with the TinyFaceDetector model performing face detection at approximately 250-millisecond intervals. Facial recognition employed 128-dimensional descriptor vectors compared via Euclidean distance with a matching threshold of 0.55 and a distinctiveness gap of 0.08 to ensure identity disambiguation. The backend REST API was developed using Node.js and Express, with PostgreSQL as the relational database. Authentication employed JSON Web Tokens (JWT) with role-based access control differentiating Administrator and Guard user roles. Table 1 presents the complete technology stack by system layer.

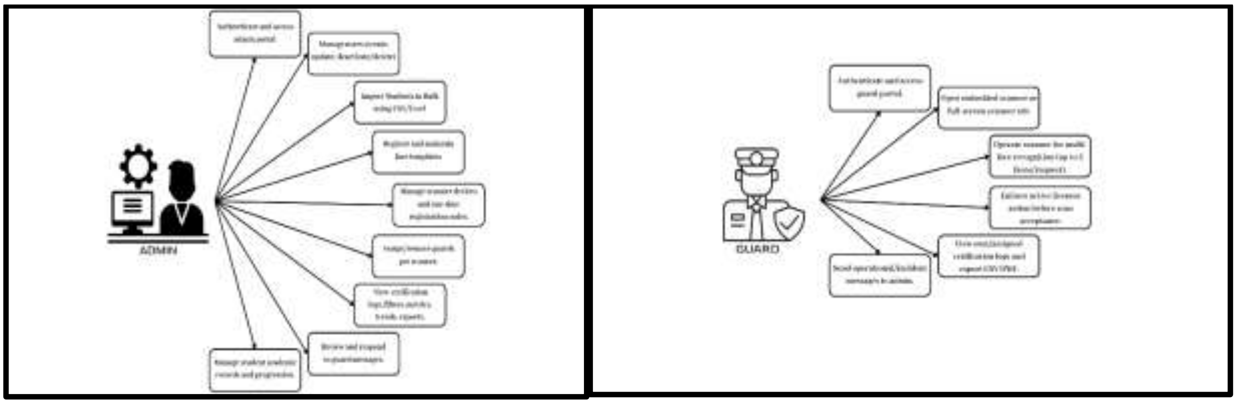


**Fig. 4. Use Cases**

**Table 1: Technology Stack by System Layer**

| Layer | Technologies |
|---|---|
| Frontend | React 18, React Router v6, Axios, face-api.js (TinyFaceDetector), Recharts, Lucide React |
| Backend | Node.js, Express, pg (PostgreSQL client), jsonwebtoken, bcryptjs, multer |
| Database | PostgreSQL 13+ |
| File Handling & Reports | xlsx, json2csv, pdfkit, jspdf, jspdf-autotable |

**Note.** The frontend face-api.js library executes all facial detection and descriptor extraction client-side within the browser, offloading inference load from the backend server.

### 3.4 System Parameters and Implementation Constraints

Several critical operational parameters were established through empirical calibration during development and are implemented as hardcoded system constraints. These parameters governed the face recognition pipeline behavior, scanner performance, and device communication. Table 2 presents the complete set of system-level constraints with values and implementation justifications.

**Table 2: System-Level Operational Parameters and Justifications**

| Parameter | Value | Justification |
|---|---|---|
| Maximum simultaneous faces per scan | 3 | Limits detection scope to prevent false matches in group scenarios |
| Face matching threshold (Euclidean distance) | 0.55 | Boundary between recognized and unrecognized descriptor states |
| Distinctiveness gap | 0.08 | Minimum distance difference between top two candidates to confirm identity |
| Face detection interval | 250 ms | Near-real-time responsiveness within recommended hardware capacity |
| Registration token expiry | 10 min | Limits scanner registration exposure window |
| Device heartbeat interval | 30 s | Maintains live monitoring of scanner device status |

### 3.5 Hardware Requirements

The scanner station is the most hardware-sensitive component, as it executes continuous browser-based inference at 250-millisecond intervals via face-api.js. Minimum requirements for the scanner station include an Intel Core i5 (8th generation) or equivalent processor, 8 GB RAM, a GPU with WebGL support, a 720p/30 fps camera, and ambient lighting of at least 200 lux on the subject's face. Recommended specifications include an Intel Core i5/i7 or Ryzen 5/7 processor, 16 GB RAM, a dedicated GPU, a 1080p/30 fps autofocus camera, and 300-500 lux lighting. The server requires a minimum of 4 CPU cores, 8 GB RAM, and 100 GB SSD storage; recommended specifications are 6-8 cores, 16 GB RAM, and 250+ GB SSD with a wired gigabit network interface.

### 3.6 Development Approach

System development followed an Agile SDLC methodology implemented through five sequential phases: (1) Requirements Analysis and System Design -- identification of manual verification limitations, definition of system requirements and security considerations, and design of the complete system architecture; (2) System Development -- construction of the face detection pipeline, descriptor generation, active liveness validation, facial matching, enrollment status verification, verification logging, device management, guard assignment, and web-based administrative dashboard; (3) Testing and Evaluation -- performance measurement under controlled and varied operational conditions; (4) Refinement and Optimization -- iterative improvement based on testing results and user feedback; and (5) Final Evaluation and Documentation -- assessment against defined performance objectives and preparation of study documentation.

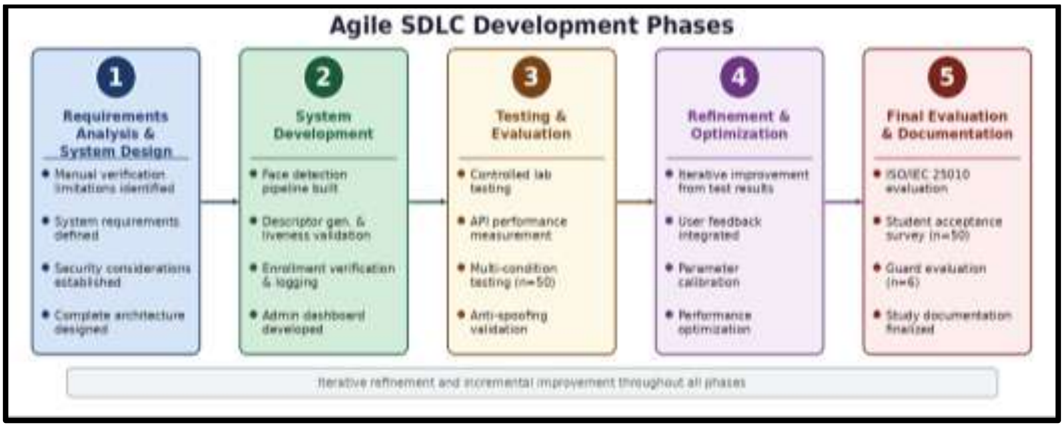


**Fig. 6. Agile SDLC Development Phases implemented in the construction of the MFRS.**

### 3.7 Participants and Respondents

Three groups participated in the evaluation: (a) five technical evaluators composed of IT experts and system specialists who assessed the system against ISO/IEC 25010 criteria; (b) 50 student respondents who participated as scanned subjects during system testing and subsequently completed acceptance questionnaires; and (c) six security personnel (guards) who operated scanner stations during testing and provided operational feedback through a structured evaluation survey.

### 3.8 Data Collection Procedures

System performance data were collected through a structured four-phase testing protocol. Phase 1 (Controlled Laboratory Testing) established baseline performance through predefined test scenarios simulating single-student verification, multiple face scenarios with up to three faces, high-traffic conditions, lighting variation, and spoofing attempts using printed photographs and digital screen replays. Phase 2 (Automated Data Collection) captured real-time verification logs recording timestamps, face detection confidence scores, recognition match scores, facial landmark results, lighting condition indicators, enrollment verification status, liveness validation outcomes, spoofing detection results, and processing times for each verification attempt. Phase 3 (Multi-Condition Testing) validated system consistency across the same 50 respondents under diverse conditions including lighting variation, facial angle variation, multiple face recognition, high-traffic simulation, and anti-spoofing testing. Phase 4 (Data Compilation and Validation) involved export of system logs in CSV and JSON formats, computation of performance metrics, and cross-verification of system logs and recorded outputs.

User acceptance and ISO/IEC 25010-based evaluations were collected using structured questionnaires administered to technical evaluators, student respondents, and security personnel using a five-point Likert scale (1 = Strongly Disagree/Poor; 5 = Strongly Agree/Outstanding). The verbal interpretation scale applied was: 4.50-5.00 = Outstanding; 3.50-4.49 = Excellent; 2.50-3.49 = Very Good; 1.50-2.49 = Good; 1.00-1.49 = Poor.

### 3.9 Statistical Treatment

Weighted mean scores were used to compute evaluation ratings across ISO/IEC 25010 dimensions and user acceptance criteria. Frequency and percentage statistics were used to summarize respondent demographic profiles. The False Acceptance Rate (FAR) and False Rejection Rate (FRR) were computed as the proportion of erroneous acceptance and rejection decisions relative to total identification attempts, respectively, expressed as percentages.

## 4. RESULTS

The results are organized into four sections corresponding to the major study objectives: (1) identification of manual verification gaps and system development outcomes, (2) technical quality assurance testing, (3) ISO/IEC 25010-based technical evaluation, and (4) student respondent and security personnel acceptance evaluation.

### 4.1 Manual Verification Gaps and System Development

Analysis of the current manual enrollment verification process identified the following principal limitations: time-consuming identity checking, susceptibility to human error, risk of identity misrepresentation, absence of real-time enrollment status confirmation, inconsistent record-keeping, and inefficiency during peak entry periods. The MFRS was developed to address each of these limitations through automated facial recognition, enrollment status cross-referencing, liveness validation, and automated logging. Table 3 presents the alignment between identified problems, implemented system features, and implementation status.

**Table 3: System Development Feature Alignment with Identified Problem Areas**

| Problem Area / Objective | Implemented System Feature | Status |
|---|---|---|
| Manual process gap analysis | Requirements analysis and system design | Addressed |
| Multiple face recognition capability | Browser-based scanner using TensorFlow.js and face-api.js | Implemented |
| Student identity verification | Face detection, descriptor extraction, and Euclidean distance matching | Implemented |
| Enrollment status confirmation | Cross-referencing recognized identity with stored enrollment records | Implemented |
| Multiple face processing | Up to three simultaneous detected faces per scanner request | Implemented |
| Spoofing prevention | Active liveness validation via head-turn action challenge | Implemented |
| Verification logging | Timestamped enrollment verification logs with device and result context | Implemented |
| Role-based user access | Administrator and Guard role modules with RBAC | Implemented |
| Report generation | Filterable logs and exportable verification reports | Implemented |
| Quality evaluation | Quality assurance testing and ISO/IEC 25010-based evaluation | Implemented |

### 4.2 Technical Quality Assurance Testing

Quality assurance testing was conducted using terminal-based and automated testing tools under controlled local conditions. Testing covered functionality, API performance, facial recognition deployment readiness, multiple face recognition capability, enrollment status verification, liveness validation, recognition accuracy, and code quality.

**Functionality Testing**

Endpoint access control was verified using PowerShell Invoke-WebRequest, and the frontend build was assessed through the React test runner. Protected API endpoints correctly returned HTTP 401 Unauthorized on unauthenticated requests, invalid device identifiers returned HTTP 404 Not Found, and the frontend test runner exited successfully with code 0. These results confirm correct authentication enforcement and appropriate handling of invalid resource requests. Automated unit test coverage for individual modules remained incomplete and is identified as a priority for future development.

**System Performance Testing**

Backend API response time was measured across 30 consecutive requests using PowerShell Measure-Command. Table 4 presents the performance results.

**Table 4: Backend API Response Time Across 30 Consecutive Requests (Local Conditions)**

| Metric | Value (ms) |
|---|---|
| Mean | 6.37 |

| Metric | Value (ms) |
|---|---|
| Median (p50) | 4.93 |
| 95th Percentile (p95) | 7.44 |
| Minimum | 3.47 |
| Maximum | 36.32 |

**Note.** Results reflect local benchmark conditions. Performance under actual institutional network traffic and concurrent multi-device load requires additional validation.

**Multiple Face Recognition Testing** The system was tested for its capacity to process multiple simultaneously detected faces within a single scanner request. All five test scenarios passed, as summarized in Table 5.

**Table 5: Multiple Face Recognition Test Results**

| Scenario | Expected Result | Actual Result | Status |
|---|---|---|---|
| One face detected | System detects and verifies one student | Single student detected and verified | Pass |
| Two faces detected | System detects and verifies up to two students | Both students detected and processed | Pass |
| Three faces detected | System detects and verifies up to three students | All three students processed simultaneously | Pass |
| More than three faces | System limits processing to maximum of three | Three faces processed; additional faces ignored | Pass |
| Registered and unknown faces in same frame | Registered students identified; unknown faces flagged | Enrolled students identified with status; unregistered faces marked Unknown | Pass |

**Enrollment Status Verification Testing**
The system correctly handled all five enrollment status test scenarios, as presented in Table 6. Verification outcomes -- Enrolled, Not Enrolled, Pending Enrollment, and Unknown -- were accurately returned in all cases, confirming that the two-stage verification pipeline (facial recognition followed by enrollment record cross-referencing) operates as designed.

**Table 6: Enrollment Status Verification Test Results**

| Test Case | Expected Result | Actual Result | Status |
|---|---|---|---|
| Registered and enrolled student | Enrolled status displayed | Enrolled status returned with student information | Pass |
| Registered but not enrolled student | Not Enrolled status displayed | Not Enrolled status returned; verification denied | Pass |
| Student with pending enrollment | Pending Enrollment status displayed | Pending Enrollment status returned | Pass |
| Unknown face (no matching record) | Unknown status displayed | Unknown status returned; no template match found | Pass |
| Recognized face with inactive enrollment | Not Enrolled status displayed | Not Enrolled returned for recognized student with inactive record | Pass |

**Liveness Validation and Anti-Spoofing Testing**

Active liveness validation was tested using live subjects, printed photographs, digital screen replays, and ID card images. Table 7 presents the test outcomes.

**Table 7: Liveness Validation and Anti-Spoofing Test Results**

| Scenario | Expected Result | Actual Result | Status |
|---|---|---|---|
| Live student performing head-turn | Accepted after successful liveness action | Scan accepted after head-turn action completed | Pass |
| Printed photograph | Rejected -- no detectable head movement | Rejected; no liveness action detected | Pass |
| Face displayed on mobile screen | Rejected -- no detectable head movement | Rejected; no liveness action detected | Pass |
| Student ID card photograph | Rejected -- no detectable head movement | Rejected; no liveness action detected | Pass |

**Note.** Although all controlled test scenarios passed, the overall liveness validation success rate under multi-condition testing was 53.85%, indicating meaningful performance degradation under real-world variability. This limitation is discussed in the Discussion section.

**Recognition Accuracy, FAR, and FRR**

Overall facial recognition accuracy under multi-condition testing reached 77.05%. The False Acceptance Rate (FAR) -- representing incorrect acceptance of unregistered or unauthorized individuals -- was 0%, indicating that no unauthorized subjects were incorrectly verified. The False Rejection Rate (FRR) -- representing incorrect rejection of registered and enrolled students -- was 22.95%, reflecting the proportion of legitimate recognition attempts that failed, primarily under adverse lighting or non-frontal angles. These results indicate adequate recognition performance under controlled conditions while highlighting the need for environmental optimization in real institutional deployments.

**Code Quality and Maintainability Testing**

Backend syntax validation and the frontend production build both passed successfully. However, review of the codebase identified
non-blocking ESLint warnings and numerous debug-level log statements in the backend. These findings indicate that while the system is operationally functional, the codebase requires cleanup, structured logging practices, and production-grade hardening prior to institutional deployment.

**4.3 Technical Evaluation Based on ISO/IEC 25010**

The five technical evaluators assessed the MFRS across seven selected ISO/IEC 25010 quality characteristics using a structured five-point Likert scale instrument. Table 8 presents the summary of technical evaluation results.

**Table 8: Summary of Technical Evaluation Results Based on ISO/IEC 25010 (n = 5)**

| ISO/IEC 25010 Quality Characteristic | Mean | Verbal Interpretation |
|---|---|---|
| Functional Suitability | 4.20 | Excellent |
| Performance Efficiency | 3.76 | Excellent |
| Usability | 4.08 | Excellent |
| Reliability | 4.00 | Excellent |
| Security | 4.20 | Excellent |
| Maintainability | 3.76 | Excellent |
| Compatibility | 3.96 | Excellent |
| Overall Mean | 3.99 | Excellent |

The overall technical evaluation mean of 3.99 was verbally interpreted as Excellent. Functional Suitability (M = 4.20) and Security (M = 4.20) received the highest ratings, indicating evaluator confidence in the system's core functions and access control mechanisms. Performance Efficiency (M = 3.76) and Maintainability (M = 3.76) received the lowest ratings within the Excellent range, reflecting evaluator recognition of optimization opportunities in runtime performance and code documentation. Compatibility (M = 3.96) and Reliability (M = 4.00) indicated satisfactory system behavior within intended deployment environments, while Usability (M = 4.08) confirmed that the interface was accessible for both administrator and guard users.

### 4.4 Student Respondent Acceptance Evaluation

Student respondents (n = 50) evaluated the MFRS based on their experience as scanned subjects during verification testing. Table 9 presents the summary of student acceptance evaluation results.

**Table 9: Summary of Student Respondent Acceptance Evaluation Results (n = 50)**

| Evaluation Dimension | Mean | Verbal Interpretation |
|---|---|---|
| Functional Suitability | 4.40 | Excellent |
| Performance Efficiency | 4.27 | Excellent |
| Usability | 4.50 | Outstanding |
| Reliability | 4.22 | Excellent |
| Security | 4.22 | Excellent |
| Overall Mean | 4.32 | Excellent |

Usability received an Outstanding rating (M = 4.50), the highest of all student acceptance dimensions, with all five usability sub-items -- ease of scanning process, clarity of verification feedback, interface readability, minimal required user action, and overall convenience -- rated at 4.50. Functional Suitability obtained the second-highest rating (M = 4.40), indicating that respondents perceived the system as effective in recognizing student identity and confirming enrollment status. Performance Efficiency (M = 4.27) reflected positive perceptions of scanning speed and real-time responsiveness, while Reliability (M = 4.22) and Security (M = 4.22) indicated general confidence in system consistency and data protection.

### 4.5 Security Personnel (Guard) Evaluation Results

Six security personnel who operated scanner stations during testing evaluated the MFRS across seven dimensions. Table 10 presents the summary of guard evaluation results.

**Table 10: Summary of Security Personnel Evaluation Results (n = 6)**

| Evaluation Dimension | Mean | Verbal Interpretation |
|---|---|---|
| Usability | 4.34 | Excellent |
| Security | 4.06 | Excellent |
| Reliability | 4.20 | Excellent |
| Functional Suitability | 3.97 | Excellent |
| Performance Efficiency | 4.33 | Excellent |
| Compatibility | 4.33 | Excellent |
| Overall Satisfaction | 4.17 | Excellent |
| Overall Mean | 4.17 | Excellent |

Guards rated the MFRS positively across all seven dimensions, with an overall mean of 4.17 (Excellent). Usability (M = 4.34), Performance Efficiency (M = 4.33), and Compatibility (M = 4.33) received the highest ratings, reflecting guard confidence in system operability and institutional fit. Overall Satisfaction received a mean of 4.17 (Excellent), with the item 'I am satisfied with the facial recognition system overall' rated at 4.50 (Outstanding). Qualitative feedback identified four recurring operational challenges: (1) scanning delays during peak entry periods; (2) recognition difficulties under direct sunlight or inadequate outdoor lighting; (3) the absence of an offline or fallback mechanism; and (4) requests for higher-resolution camera equipment.

**5. DISCUSSION**

The findings of this study collectively demonstrate that the MFRS constitutes a viable and functionally sound prototype for gate-based enrollment status verification in Philippine higher education institutions. The system successfully integrates multiple face recognition, enrollment cross-referencing, liveness validation, and comprehensive administrative logging within a single browser-deployable platform -- a combination not identified in any comparable system reviewed in the literature. The overall technical evaluation mean of 3.99 and student acceptance mean of 4.32, both rated Excellent, support the rejection of the null hypothesis and confirm that the system met the minimum evaluative threshold across ISO/IEC 25010 quality dimensions.

The outstanding Usability rating (M = 4.50) among student respondents is particularly noteworthy. Consistent with TAM’s emphasis on perceived ease of use as a determinant of technology acceptance (Davis, 1989), students found the scanning process straightforward, the verification feedback clear, and the overall experience convenient. This result aligns with Valenzuela et al. (2025), who similarly reported strong usability ratings for a Philippine facial recognition attendance system, suggesting that well-designed scanner interfaces can achieve high acceptance regardless of the underlying recognition complexity.

The strong Security ratings from both technical evaluators (M = 4.20) and student respondents (M = 4.22) reflect the effectiveness of the MFRS’s multi-layered security architecture, which combines JWT-based authentication, role-based access control, device authorization tokens, and active liveness validation. These findings are consistent with the governance-oriented design principles recommended by NASEM (2024) and Chen and Wang (2023), and with the NPC (2023, 2025) guidelines governing biometric data processing in the Philippine context.

The performance efficiency dimension revealed a meaningful discrepancy between controlled and real-world conditions. Although the backend API achieved a mean response time of 6.37 milliseconds under local benchmark conditions -- well within the requirements for real-time verification -- technical evaluators rated Performance Efficiency at 3.76 (Excellent, lower bound), and both student and guard respondents noted scanning delays during peak entry simulations. This pattern is consistent with Boe et al.’s (2024) finding that image capture quality and threshold calibration directly affect recognition pipeline throughput in institutional settings, and suggests that the browser-based inference architecture may face throughput constraints under concurrent multi-user load. Hardware GPU acceleration at scanner stations and staggered detection intervals are identified as prioritized mitigation strategies.

The liveness validation success rate of 53.85% represents the most critical limitation identified in this study. While the active head-turn challenge successfully rejected all spoofing attempts in controlled testing (Table 7), its performance under real-world variability -- encompassing variable head positions, lighting conditions, and subject compliance -- was substantially lower. This finding aligns with Xing et al. (2025) and Antil et al. (2025), who argued that challenge-response liveness mechanisms provide meaningful but insufficient protection against adversarial presentation attacks, and that reliable anti-spoofing requires supplementary depth-sensing or dedicated liveness detection algorithms. The current liveness implementation should therefore be characterized as a baseline deterrent rather than a comprehensive anti-spoofing solution.

The overall recognition accuracy of 77.05% under multi-condition testing, combined with an FRR of 22.95% and an FAR of 0%, indicates that the system is appropriately calibrated to prioritize security (no false acceptances) at the cost of some recognition completeness (non-trivial false rejections). This tradeoff is appropriate for an enrollment verification context, where admitting unauthorized individuals presents a greater institutional risk than requiring legitimate students to be rescanned under corrected conditions. Nevertheless, an FRR of 22.95% suggests that environmental factors -- particularly lighting, camera angle, and subject distance -- materially affect recognition reliability. The recommended 300-500 lux lighting range and camera mounting constraints (0.7-1.8 m subject distance) established during development are supported by these findings and should be treated as mandatory implementation requirements.

The student privacy concerns surfaced in the acceptance evaluation -- despite technically sound data protection -- are consistent with Choung et al.’s (2024) finding that user acceptance of AI-based facial recognition depends as much on perceived transparency and governance as on technical performance. This finding underscores the importance of visible data retention disclosures, explicit consent workflows during biometric registration, and periodic privacy notifications, as recommended by NPC (2023, 2025). Embedding these transparency mechanisms into the system interface rather than relying on institutional policy documents alone is a recognized design imperative for future MFRS versions.

Taken together, these findings position the MFRS as a functional prototype validated under controlled conditions, with a clearly delineated improvement pathway before full institutional deployment. Its architecture is technically sound, its user acceptance is positive, and its security posture is appropriate for educational use. The critical priorities for future development are liveness validation robustness, peak-hour performance optimization, offline resilience, and privacy transparency -- all of which are tractable engineering challenges rather than fundamental architectural limitations.

**Link to Software Demonstration:**
https://tinyurl.com/bdhnpkpz

## 6. CONCLUSION

This study designed, developed, and evaluated the Multiple Face Recognition System (MFRS), a gate-deployed biometric platform for student enrollment status verification at institutional entry points in Philippine higher education. The system successfully integrates real-time multiple face recognition, Euclidean-distance facial matching, active liveness validation, two-stage enrollment verification, role-based access control, and automated verification logging within a single web-based platform deployable on standard institutional hardware.

Evaluation results demonstrated that the system achieved an overall technical evaluation mean of 3.99 (Excellent) across seven ISO/IEC 25010 quality dimensions as assessed by five technical evaluators, and an overall student acceptance mean of 4.32 (Excellent) among 50 student respondents. Security personnel evaluation yielded an overall mean of 4.17 (Excellent). These results support the rejection of the null hypothesis and confirm that the MFRS meets the established evaluative threshold for institutional acceptability.

Functional Suitability and Security were the highest-rated technical dimensions, reflecting the system's design emphasis on correct core functionality and multi-layered access control. The Outstanding Usability rating (M = 4.50) from student respondents indicates that the scanning and verification workflow is sufficiently intuitive and convenient for day-to-day institutional use.

The study also transparently acknowledged two significant limitations that preclude immediate full-scale deployment: the liveness validation success rate of 53.85% under real-world conditions, which indicates that the current head-turn challenge mechanism requires strengthening before it can serve as a reliable anti-spoofing barrier; and the overall recognition accuracy of 77.05%, which -- while appropriate for a controlled prototype -- must be improved through hardware optimization and algorithm refinement before the system can reliably function as the primary gate verification mechanism at scale.

The principal contributions of this study are: (a) a functional, formally evaluated prototype demonstrating the feasibility of browser-based multiple face recognition for enrollment verification in Philippine higher education; (b) empirical performance baselines for system accuracy, FAR, FRR, and API response time under controlled conditions; (c) a structured ISO/IEC 25010 and user acceptance evaluation framework applicable to comparable biometric systems development; and (d) an identified research gap -- the absence of integrated multi-face recognition, enrollment cross-referencing, liveness validation, and quality evaluation in a single platform -- that the MFRS directly addresses.

Future research should prioritize longitudinal deployment studies across full academic semesters with larger and more diverse student populations, integration of dedicated liveness detection algorithms or depth-sensing hardware, peak-hour performance optimization through GPU acceleration and inference scheduling, and the development of offline fallback mechanisms to maintain verification continuity during network interruptions. API-based interoperability with existing Student Information Systems and Learning Management Systems represents a further extension pathway that would enhance the MFRS's institutional utility.

## REFERENCES


1. Antil, A., Sheikhfathollahi, M., Parkinson, S., Hill, R., & Khan, S. (2025). A comprehensive survey on the evolution of face anti-spoofing and presentation attack detection. Neurocomputing, 630, 128992. https://doi.org/10.1016/j.neucom.2025.128992
2. Balagtas, I., Padaon, J., & Punzalan, B. C. (2023). Attendance monitoring system using facial recognition applying Viola-Jones and Principal Component Analysis algorithm. Ani: Letran Calamba Research Report, 19(1).
3. Boe, C.-H., Ng, K.-W., Haw, S.-C., Naveen, P., & Anaam, E. A. (2024). An automated face detection and recognition for class attendance. International Journal on Informatics Visualization, 8(3), 1146-1153. https://doi.org/10.62527/joiv.8.3.2967
4. Chen, W., & Wang, M. (2023). Regulating the use of facial recognition technology across borders: A comparative case analysis of the European Union, the United States, and China. Telecommunications Policy, 47(2), 102482. https://doi.org/10.1016/j.telpol.2022.102482
5. Choung, H., David, P., & Ling, T.-W. (2024). Acceptance of AI-powered facial recognition technology in surveillance scenarios: Role of trust, security, and privacy perceptions. Technology in Society, 79, 102721. https://doi.org/10.1016/j.techsoc.2024.102721
6. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319-340. https://doi.org/10.2307/249008
7. Domingo, W. G., & Ladia, Z. J. M. (2024). QSUM-eASys: A face recognition and web-based attendance monitoring system for Quirino State University Maddela Campus. Isabela State University Linker: Journal of Engineering, Computing and Technology.
8. International Organization for Standardization. (2023). ISO/IEC 25010:2023 systems and software engineering -- Systems and software quality requirements and evaluation (SQuaRE) -- Product quality model. ISO.
9. Jain, A. K., & Ross, A. (2021). Bridging the gap: From biometrics to forensics. Proceedings of the IEEE, 109(5), 891-911. https://doi.org/10.1109/JPROC.2021.3049646
10. Kumar, A., & Singh, S. K. (2023). Deep learning-based facial recognition systems: A comprehensive review of recent advances. Pattern Recognition, 138, 109234. https://doi.org/10.1016/j.patcog.2023.109234

11. Li, H., & Zhao, X. (2024). Contactless biometric authentication systems: Recent developments and future directions. IEEE Access, 12, 15678-15692. https://doi.org/10.1109/ACCESS.2024.3356789
12. Mendoza, R. L., & Cruz, J. D. (2022). Digital transformation challenges in Philippine higher education institutions: An administrative perspective. International Journal of Educational Management, 36(4), 612-628. https://doi.org/10.1108/IJEM-08-2021-0321
13. Mondal, H., & Mondal, S. (2024). Methods of collecting and recording attendance of medical students in a classroom: A systematic review. Journal of Education and Health Promotion, 12, 427. https://doi.org/10.4103/jehp.jehp_737_23
14. National Academies of Sciences, Engineering, and Medicine. (2024). Facial recognition technology: Current capabilities, future prospects, and governance. The National Academies Press.
15. National Privacy Commission. (2023). Privacy Policy Office Advisory Opinion No. 2023-025. https://privacy.gov.ph/
16. National Privacy Commission. (2025). Advisory Opinion No. 2025-007 (Redacted). https://privacy.gov.ph/
17. Necochea-Chamorro, J. I., Sotelo Asalde, C. M., Loli Nunez, M. E., & del Rosario Vasquez Valencia, Y. (2024). Systematic literature review: Biometric technology applied to educational institutions. TEM Journal, 13(1), 570-580. https://doi.org/10.18421/TEM131-60
18. Nguyen, T. H., & Roberts, M. J. (2022). Identity verification in higher education: Current practices and emerging technologies. Journal of Educational Technology Systems, 50(3), 345-362. https://doi.org/10.1177/00472395211067543
19. Pattnaik, P., & Mohanty, K. K. (2020). AI-based techniques for real-time face recognition-based attendance system: A comparative study. In Proceedings of the 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA) (pp. 1034-1039). IEEE. https://doi.org/10.1109/ICECA49313.2020.9297643
20. Raheem, Y., Farooq, M. U., & Ahmad, R. (2021). Smart attendance system using facial recognition and machine learning. International Journal of Advanced Computer Science and Applications, 12(1), 217-223.
21. Rahman, M. A., Hossain, M. S., & Islam, M. R. (2021). Automated attendance management system using facial recognition: A comprehensive review. IEEE Access, 9, 108087-108109. https://doi.org/10.1109/ACCESS.2021.3100856
22. Rojas, H. (2025). Understanding performance efficiency in ISO/IEC 25010: A systematic literature review. International Journal on Informatics Visualization.
23. Valenzuela, J. T., Sandigan, C. R., Villar, C. R., Litang, L. R., Jae, H. K., & Nuesca, A. G. (2025). Development and evaluation of a facial recognition-based computer laboratory attendance monitoring system. Asia Pacific Journal of Academic Research in Social Sciences, 10(1).
24. Wang, M., Kang, Y., Deng, B., & Lan, X. (2024). Exploring college students' risk perception and acceptance intention of facial recognition technology in China. Telematics and Informatics, 95, 102193.
25. Xing, H., Tan, S. Y., Qamar, F., & Jiao, Y. (2025). Face anti-spoofing based on deep learning: A comprehensive survey. Applied Sciences, 15(12), 6891. https://doi.org/10.3390/app15126891
26. Zhang, Y., & Li, Q. (2023). Efficient facial recognition deployment in resource-constrained educational environments. Computers & Education: Artificial Intelligence, 4, 100126. https://doi.org/10.1016/j.caeai.2023.100126