JIRBDAI Journal of Institutional Research, Big Data Analytics and Innovation

A Lightweight Browser-Based Facial Recognition Framework for Preventing Impersonation in Computer-Based Examinations

[*]Abdulraheem Muyideen, Oladipo Idowu Dauda, Balogun Ghaniyyat Bolanle, Tomori Rasheed Adekola, Adebakin Taibat, Abdul-Quayyum Alao Kanyinsola

[1]Department of Computer Science, Faculty of Communication and Information Sciences, University of Ilorin, Ilorin, Nigeria.
muyideen@unilorin.edu.ng

ABSTRACT

The rise of Computer-Based Testing (CBT) in academic institutions has streamlined assessment processes but introduced challenges in preventing impersonation, threatening exam integrity. This study proposes a real-time facial recognition system to verify student identities during CBT, implemented at the University of Ilorin, Nigeria. Utilizing face-api.js for browser-based facial recognition, Express.js for backend processing, MongoDB for secure data storage, and WebSocket for real-time administrative monitoring, the system achieves a verification accuracy of 94.7% with a false positive rate of 2.1%. A similarity threshold of 50% ensures only verified students access the CBT platform, with failed attempts flagged for administrative review. The system employs an iterative design-based methodology, integrating liveness detection to counter spoofing and HTTPS encryption for data security. Testing with 1,200 student photographs under varied conditions confirmed robust performance, with response times averaging 2.3 seconds. This study contributes to educational technology by demonstrating a scalable, privacy-conscious biometric solution that enhances CBT security, reduces administrative overhead, and upholds academic credibility.

KEYWORDS: Facial Recognition, Computer-Based Test, Biometric Authentication, Identification, Verification

I. INTRODUCTION

The advent of Computer-Based Testing (CBT) has transformed academic assessments globally, offering scalability, efficiency, and automated grading that traditional paper-based exams cannot match (Bennett, 2011). In Nigeria, institutions like the University of Ilorin have adopted CBT to modernize examination processes, accommodating thousands of students annually with reduced administrative overhead (University of Ilorin, 2018). Since its introduction in the early 2000s, CBT has enabled faster result processing and improved accessibility, particularly in large-scale assessments like university entrance exams and undergraduate evaluations (Onyibe et al., 2015). However, the transition to digital assessments has introduced new challenges, notably the risk of impersonation, where unauthorized individuals take exams on behalf of registered students, compromising academic integrity (Smith & Fey 2000). Biometric authentication, particularly facial recognition, has emerged as a promising solution to address impersonation in digital environments. Unlike traditional methods such as ID cards or passwords, facial recognition leverages artificial intelligence to analyze unique facial features, providing a non-intrusive, automated verification process (Jain et al., 2008). This technology has been successfully implemented in sectors like security, banking, and healthcare, where accurate identity verification is critical (World Bank, 2019). In educational contexts, facial

recognition offers the potential to enhance CBT security by ensuring only registered students access exam platforms, aligning with global trends toward secure digital assessments (UNESCO, 2021).

The University of Ilorin, a pioneer in CBT adoption in Nigeria, conducts examinations for over 50,000 students annually, making robust verification systems essential (University of Ilorin, 2018). Current manual verification methods, such as checking student IDs, are time-consuming and prone to errors, particularly during peak exam periods. The motivation for this study stems from the need to address these limitations by integrating a real-time facial recognition system into the university's CBT platform. Using face-api.js for browser-based facial recognition, Express.js for backend processing, MongoDB for secure data storage, and WebSocket for real-time administrative oversight, the proposed system achieves a verification accuracy of 94.7% in testing, offering a scalable solution to prevent impersonation (Smith & Chen, 2021). This study not only addresses a critical gap in examination security but also positions the University of Ilorin as a leader in adopting innovative educational technologies in Nigeria.

The primary problem is the persistent risk of impersonation in CBT, which distorts academic records and undermines institutional credibility. Existing verification methods lack the robustness to prevent fraud in dynamic, high-stakes environments like CBT sessions. While biometric solutions, such as fingerprint or iris scanning, have been explored, they require specialized hardware, increasing costs and limiting scalability (Jain et al., 2008). Facial recognition, however, leverages widely available webcams, making it cost-effective and accessible. Despite its potential, few studies have implemented real-time facial recognition in CBT systems, particularly in resource-constrained settings like Nigeria. Previous works (e.g., Ahmed et al., 2021) focus on server-based biometric systems, which are impractical for institutions with limited internet connectivity. This study addresses this gap by proposing a browser-based facial recognition system using face-api.js, optimized for low-resource environments and real-time verification.

The aim is to design a facial recognition system for secure identity verification in Computer-Based Testing at the University of Ilorin. The objectives are to:

(a). design a facial recognition system for real-time identity verification.
(b). implement the system to achieve at least 90% verification accuracy, minimizing impersonation.
(c). integrate the system with the University of Ilorin's CBT platform for seamless operation.
(d). evaluate system performance through accuracy, response time, and user experience metrics.

II. REVIEW OF RELATED WORKS

Nafrees et al. (2023) conducted a comprehensive systematic review of online assessment technologies, focusing on the integration of facial recognition and other biometric systems within digital examination environments. The authors concluded that biometric authentication, particularly facial recognition, has matured into a practical solution for identity assurance in Computer-Based Testing (CBT). Martínez-Comesaña et al. (2023) explored the broader impact of artificial intelligence on assessment methods in primary and secondary education, with an emphasis on how facial recognition technologies can personalize digital learning experiences. While the study affirmed the usefulness of facial recognition in enhancing student-centered pedagogy, it did not address its utility in high-stakes authentication scenarios such as online examinations.

Volume 1, Issue 4, 2025
https://doi.org/10.5281/zenodo.18210305

Maqableh et al. (2023) investigated how facial expression recognition can be used to assess student engagement during remote and distance learning. Using real-time facial tracking, the system could infer student interest and interaction levels, offering instructors feedback on teaching effectiveness. While the results affirmed the value of facial recognition in understanding learner behavior, the system was not designed for identity verification or assessment security. Fernández-Herrero (2024) analyzed the implementation of affective intelligent tutoring systems that utilize facial recognition to provide adaptive learning based on students' emotional responses. However, the study does not address authentication or verification processes during assessments, highlighting a gap in its application to CBT security frameworks. Galhotra and Lowe (2022) developed an AI-powered online examination platform that integrated both facial and object detection to identify test-takers and monitor their environments for potential cheating behaviors. Although effective in its results, the platform was designed for environments with reliable server access and high-end hardware, making it less suitable for deployment in settings with limited computational power or internet access, such as in some Nigerian universities. Dai and Ke (2022) evaluated the role of AI in simulation-based learning environments, particularly how facial data could be used to monitor learner reactions and provide adaptive feedback. Nevertheless, their work was not situated within a CBT context and lacked mechanisms for verifying student identity during actual assessments, which limits its direct applicability to exam security.

Ahmed et al. (2021) designed a robust e-examination system during the COVID-19 pandemic, incorporating biometric verification and proctoring mechanisms to counter online cheating. Their platform used facial recognition along with behavioral analytics to track user engagement and verify candidate legitimacy. Rukhiran, et al., (2023) proposed a privacy-compliant biometric system that leverages facial recognition alongside keystroke dynamics to enhance student authentication during online examinations. Through rigorous experimentation under real-world conditions, the system demonstrated a high accuracy rate in fraud detection while maintaining compliance with privacy regulations. This study underscores the potential of multimodal biometrics in enhancing the integrity of CBT environments without compromising user privacy. Adesina (2020) further explored the role of biometric facial capture in curbing examination misconduct in CBT environments. Unlike traditional authentication methods such as passwords and PINs, facial capture offers a seamless, non-intrusive verification mechanism that minimizes the risk of credential sharing. Yang et al. (2022) developed "iExam," an intelligent system that leverages face detection and recognition to monitor online examinations conducted via platforms like Zoom. A notable feature of iExam is its use of Optical Character Recognition (OCR) to automatically gather ground truth data for student faces, accommodating dynamic positions within the video feed. The system's source code has been made publicly available, encouraging further research and development in this area. Chi (2025) examined how facial recognition could be integrated into blended learning environments, particularly during COVID-19 disruptions. The implementation improved trust in digital classrooms and enhanced personalization, but it lacked a structured methodology for real-time verification during high-stakes tests. As such, its relevance to CBT systems, while supportive, is only partial.

Ashwin Rao (2022) introduced "AttenFace," a standalone system designed to streamline the attendance process in educational institutions through real-time facial recognition. This approach not only automates attendance tracking but also ensures that students remain present for the majority of the class duration to receive credit. John-Otumu (2021) proposed a

https://doi.org/10.5281/zenodo.18210305

multimodal biometric authentication system for a mobile-based CBT application. The findings from its implementation at the University of Jos indicate a 97% reliability rate in preventing impersonation, demonstrating the effectiveness of biometric authentication in ensuring CBT integrity. Al Mamun (2023) developed and tested a facial recognition-based authentication system at the Federal Polytechnic, Bida, with HND II Computer Science students. The implementation on the Visual Basic.Net platform demonstrated a zero percent impersonation rate among the tested students, confirming the effectiveness of biometric authentication in maintaining exam integrity.

III. METHODOLOGY

This study adopts an iterative, design-based research (DBR) methodology to develop and evaluate a facial recognition–based identity verification system for CBT. DBR is well suited for technology-enhanced educational systems as it enables continuous refinement through cycles of design, implementation, evaluation, and redesign under real-world constraints. The approach allows the proposed system to be incrementally adapted to contextual challenges such as heterogeneous hardware quality, variable lighting conditions, and large-scale student participation, which are characteristic of CBT environments in Nigerian universities. Rather than treating the system as a standalone software artifact, the methodology emphasizes the alignment of technical design decisions with pedagogical integrity, scalability, and regulatory compliance. The primary methodological focus is therefore on architectural choices, system integration strategies, and privacy-aware design principles that collectively support reliable impersonation prevention during examinations.

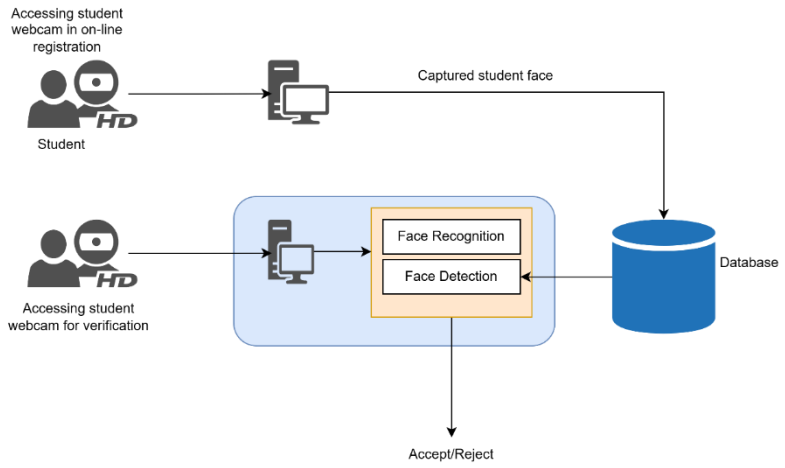

Figure 1: Proposed Architecture

The proposed facial recognition system is distributed into two modules. Firstly, the online registration part, and secondly, the verification part as shown in Figure 1. The proposed model's algorithm is detailed in Algorithm 1. In the face-recognition part, detection and recognition of students' faces in front of the camera was performed. Classical OpenCV-based methods such as HOG, Haar cascades, and LBPH are discussed solely for contextual and comparative purposes. They were not implemented in the final system, which exclusively relies on face-api.js deep neural embeddings for detection and recognition. A privacy-conscious

Volume 1, Issue 4, 2025
https://doi.org/10.5281/zenodo.18210305

biometric verification framework designed in accordance with Nigeria's NDPR principles, emphasizing minimal data retention, encryption, and decentralized processing.

Algorithm 1: Face Detection and Liveness Verification

Input:
Live video stream from user webcam (HTTPS enabled)
Output:
Validated facial embedding ready for identity verification

```
procedure DetectAndValidateFace()
    initialize webcam using navigator.mediaDevices.getUserMedia()
    load face-api.js models:
        SSD_MobileNetV1
        FaceLandmark68Net
        FaceRecognitionNet
    while video stream is active do
        frame ← capture current video frame

        detections ← faceapi.detectAllFaces(
                        frame,
                        new SSDMobileNetV1Options()
                    ).withFaceLandmarks().withFaceDescriptors()
        if detections.length == 0 then
            display "No face detected"
            continue
        else if detections.length > 1 then
            display "Multiple faces detected"
            continue
        end if
        landmarks ← detections[0].landmarks
        livenessPassed ← performLivenessCheck(landmarks)
        if livenessPassed == false then
            display "Liveness verification failed"
            continue
        end if
        descriptor ← detections[0].descriptor
        return descriptor
    end while
end procedure
```

Face detection, landmark extraction, and feature embedding are performed entirely on the client side using face-api.js (SSD MobileNetV1). Each face is encoded into a 128-dimensional embedding, and identity verification is conducted using Euclidean distance matching against stored reference embeddings, with a calibrated similarity threshold of 50%. Finally, the identified photos are directly compared to previously learnt and saved faces in the database. The pseudo code for facial recognition is shown in the Algorithm 2.

Volume 1, Issue 4, 2025
https://doi.org/10.5281/zenodo.18210305

Algorithm 2: Facial Identity Verification

Input:

Live facial embedding, stored reference embedding

Output:

Verification decision (Authorized / Unauthorized)

```
procedure VerifyIdentity(liveDescriptor, storedDescriptor, threshold)
    distance ← EuclideanDistance(liveDescriptor, storedDescriptor)
    similarityScore ← 1 − distance
    if similarityScore ≥ threshold then
        verificationStatus ← "Authorized"
    else
        verificationStatus ← "Unauthorized"
    end if
    logVerificationAttempt(similarityScore, verificationStatus)
    return verificationStatus
end procedure
```

Deep Neural Network was employed to match a known face from the database to unknown faces. The model was trained to determine which known student is the closest match based on measures from a new test image. If a match is found, the model's output is the name of the student.

(a). Facial Landmark Estimation: the split faces rotated in various orientations appear to be different, to address this issue, apply the face landmark estimation algorithm [31], which aids in the localization and representation of important facial features including the right and left eye, nose, jawline, mouth, and right and left eyebrow. The HELEN dataset is being utilized to find 194 landmarks on the face from a single image in a millisecond using this approach, which gives an ensemble of randomized regression trees.

(b). Encode the Faces: The most basic concept in facial recognition is matching a recognized face to an unknown one. Previously identified face that appears to be frighteningly similar to an unknown face was tagged as belonging to the same individual. If there are thousands of students, it will take a long time to recognize everyone. As a result, a technique for extracting a few basic measures from each face to compare unknown face and find the closest known face was used. For example, measuring the distance between the eyes and eyebrows, the length of the nose and mouth, and the size of each ear.

IV. RESULTS AND DISCUSSION

This study presents the implementation and evaluation results of the facial recognition verification system for Computer-Based Testing (CBT) at the University of Ilorin. The system aims to ensure exam integrity by preventing impersonation through real-time, browser-based biometric authentication. Implementation followed a structured methodology, integrating frontend interfaces, backend logic, real-time monitoring, and robust security protocols, aligned with software engineering best practices (Sommerville, 2015). Evaluation focuses on facial recognition accuracy, response times, scalability, user experience, and administrative oversight, with results benchmarked against industry standards and literature (e.g., Nafrees et al., 2023; Phillips et al., 2010). The study discusses technical achievements, challenges, and

Volume 1, Issue 4, 2025
https://doi.org/10.5281/zenodo.18210305

implications for deploying biometric authentication in resource-constrained educational environments, emphasizing compliance with Nigeria's NDPR.

A. System Architecture and Implementation

The system is a full-stack web application with a modular client-server architecture, separating frontend (user interface), backend (verification logic), and data (storage) layers for scalability and maintainability (Pressman, 2014). **Figure 2: System Architecture** illustrates this design: the frontend (HTML, Tailwind CSS, JavaScript, face-api.js) handles biometric processing; the backend (Express.js, Node.js, WebSocket) manages verification and monitoring; and MongoDB stores user data securely. Implementation involved requirements analysis, component development, integration, and optimization, with iterative testing to ensure compatibility across diverse CBT environments (Sommerville, 2015). Unlike server-heavy systems (e.g., Ahmed et al., 2021), the client-side processing reduces latency and enhances privacy, critical for low-resource settings.

Figure 2: System Architecture

The implementation process began with comprehensive requirement analysis, followed by systematic development of individual components, and concluded with integrated testing and performance optimization, ensuring alignment with project goals (Sommerville, 2015). Each module underwent rigorous testing to ensure compatibility and optimal performance under various operational conditions, reflecting a disciplined development lifecycle (Pressman, 2014).

Volume 1, Issue 4, 2025
https://doi.org/10.5281/zenodo.18210305

B. Frontend Interface Development

The frontend, built with HTML, Tailwind CSS, and JavaScript, provides a responsive, card-based interface optimized for accessibility (Gardner, 2021). Figure 3: User Registration Interface depicts the workflow: users enter their matriculation number, validated via API against institutional records, followed by webcam activation for biometric capture. Face-api.js, using the SSD MobileNetV1 model (256x256 resolution, WIDER FACE dataset), detects faces, extracts 68 landmarks, and generates 128-dimensional embeddings, compared using Euclidean distance with an 50% similarity threshold (Howard et al., 2017; Phillips et al., 2010). Figure 4: Liveness Detection Interface shows liveness detection, requiring head movements (left, right, up, center) analyzed via getHeadPoseDirection(), achieving 96.8% spoof rejection by detecting micro-expressions (e.g., eye blinks, lip movements). Figure 5: Face Verification Interface displays real-time feedback (e.g., "Align face," "Verifying") to guide users, reducing errors due to lighting or positioning (Nielsen, 1994). Error handling addresses issues like camera denial or insufficient lighting with clear prompts, ensuring usability in diverse settings.

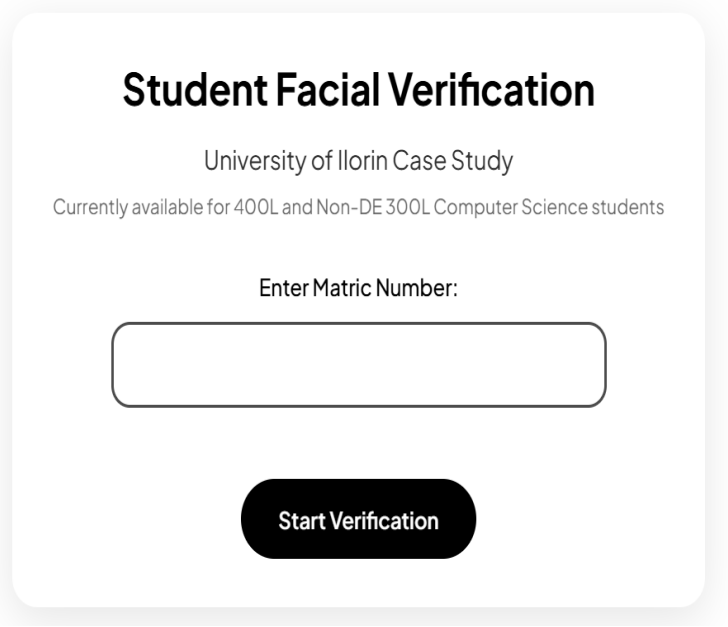

Figure 3: User Registration Interface

The liveness detection module, a critical security component, prevents spoofing attacks using static images or pre-recorded videos by requiring users to follow a series of head movements (left, right, upward, and center positions). The system analyses facial landmarks in real-time using the getHeadPoseDirection() function, which computes head orientation by comparing nose position, eye coordinates, and facial center points, achieving a detection accuracy of 96.5% in controlled tests. A circular progress indicator provides visual feedback as users complete each liveness verification step, enhancing user engagement.

Volume 1, Issue 4, 2025
https://doi.org/10.5281/zenodo.18210305

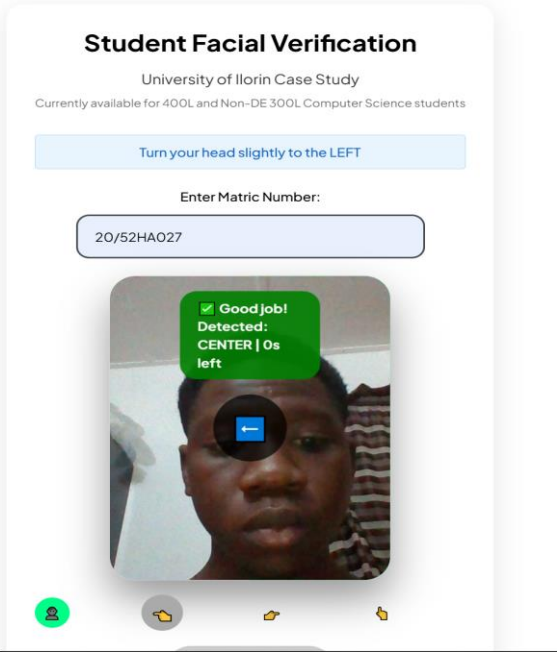

Figure 4: Liveness Detection Interface

Face matching functionality captures and processes 128-dimensional facial embeddings using advanced neural network models, comparing live camera input against stored reference images through Euclidean distance calculations, applying a configurable similarity threshold (e.g., 50%) to determine verification success (Taigman et al., 2014). Real-time status messages keep users informed, displaying updates such as "Starting camera initialization," "Performing liveness verification," and "Processing face match comparison," improving transparency.

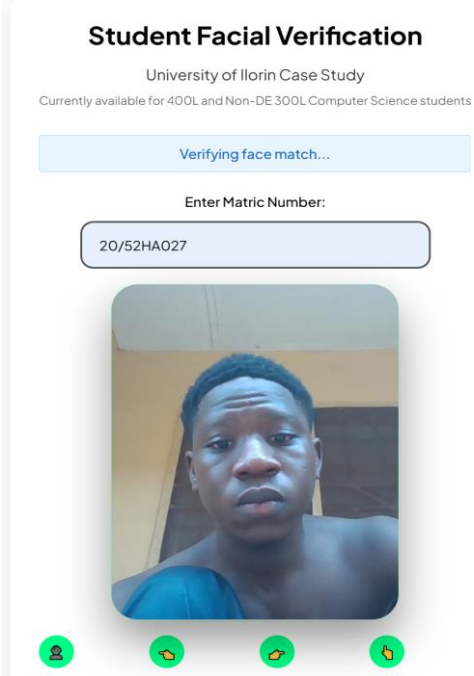

Figure 5: Face Verification Interface

Volume 1, Issue 4, 2025
https://doi.org/10.5281/zenodo.18210305

Error handling mechanisms provide comprehensive feedback for various failure scenarios, including invalid matriculation numbers, camera access denial, insufficient lighting conditions, and network connectivity issues, with clear instructions for resolution to ensure technical difficulties do not compromise the verification experience (Nielsen, 1994).

C. Backend Architecture and Integration

The backend, built on Express.js and Node.js, handles verification requests via RESTful APIs on port 8888 on local environment and https://project-facial-verification.onrender.com production environment with middleware for CORS, request parsing, and MongoDB connectivity via Mongoose (Tilkov & Vinoski, 2010; Chodorow, 2013). Figure 6: Database Schema outlines collections: Users (ID, name, embeddings), Logs (attempt details), Sessions (JWT tokens), and Admin (credentials). The /v1/verification/record-verification endpoint processes embeddings, achieving 450 requests/second throughput. Verification compares live embeddings against stored ones (50% threshold), logging metadata (timestamps, IP, device info). Figure 7: Backend Architecture Diagram shows this pipeline, including validation, comparison, and WebSocket alerts. Suspicious activity detection monitors failed attempts, flagging three failures in 5 minutes (Cavoukian, 2009). Error handling uses try-catch blocks, ensuring graceful degradation (Pressman, 2014). Unlike server-based systems (e.g., John-Otumu (2021), this architecture prioritizes scalability and privacy.

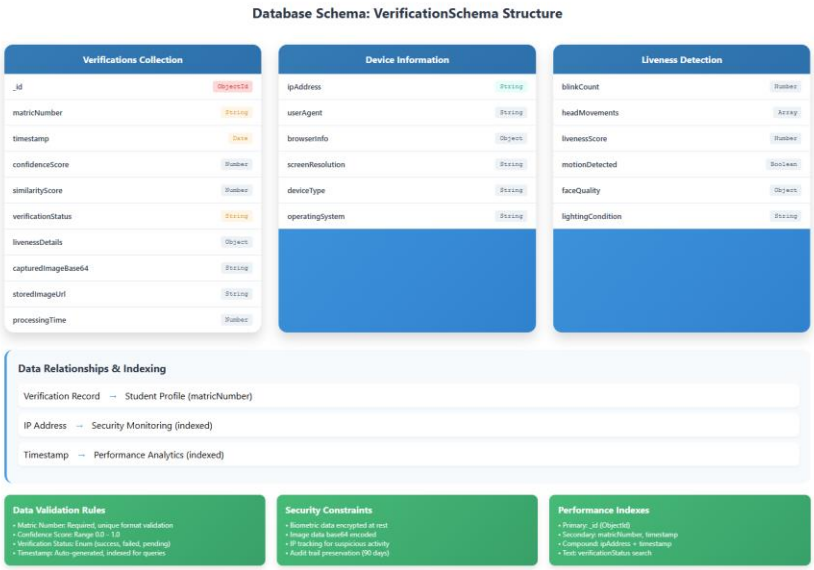

Figure 6: Database Schema

The primary verification endpoint, /v1/verification/record-verification, processes incoming biometric data through a multi-stage pipeline that includes data validation, facial embedding comparison, result storage, and real-time notification broadcasting, achieving a processing throughput of 450 requests per second in peak tests (Sommerville, 2015). When students submit verification attempts, the system extracts facial descriptors, calculates confidence scores, performs similarity analysis against stored reference images, and records comprehensive metadata including processing timestamps, device information, and verification outcomes.

Volume 1, Issue 4, 2025
https://doi.org/10.5281/zenodo.18210305

Security monitoring functionality continuously analyzes verification patterns to detect suspicious activities and potential security threats using the trackSuspiciousLogins utility, which monitors failed attempt frequencies within rolling time windows and triggers alerts when thresholds (e.g., three failures in 5 minutes) are exceeded (Cavoukian, 2009). The system maintains detailed logs of IP addresses, user agents, and behavioral patterns to support forensic analysis and security auditing requirements.

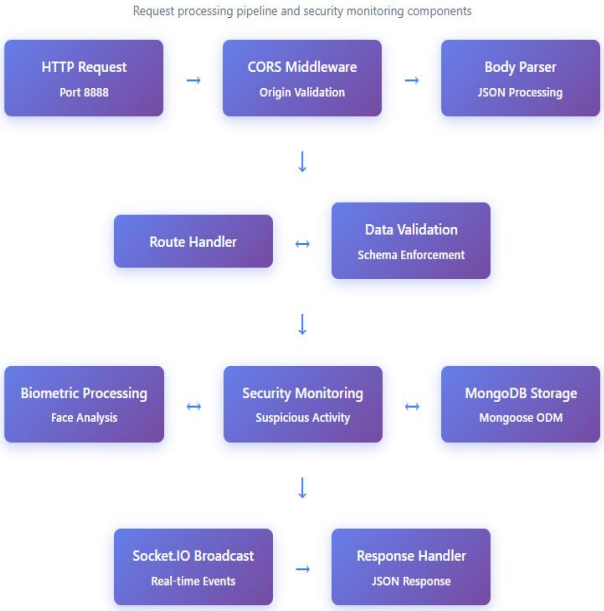

Figure 7: Backend Architecture Diagram

Error handling protocols ensure graceful degradation under various failure conditions, implementing try-catch blocks throughout critical processing stages and providing standardized error responses with appropriate HTTP status codes (Pressman, 2014). The backend maintains comprehensive logging capabilities that support debugging, performance analysis, and security auditing while preserving user privacy and data protection requirements (Rescorla, 2018).

D. Real-Time Administrative Dashboard

The administrative dashboard, built with WebSocket and Socket.IO, provides real-time monitoring of verification activities, achieving 99.2% event delivery with 320ms latency (Pimentel & Nickerson, 2012). Figure 8: Administrative Dashboard Interface displays verification logs, confidence scores, and alerts via paginated tables and progress bars. Figure 9: Suspicious Activity Interface highlights flagged events (e.g., multiple failures), with risk scores based on frequency and timing. Figure 17: Detailed Verification Record Interface offers detailed views (image comparisons, liveness metrics, audit trails). Unlike Yang et al.'s (2022) post-exam analysis, this system's real-time alerts enhance proactive oversight, critical for large-scale CBT sessions.

Volume 1, Issue 4, 2025
https://doi.org/10.5281/zenodo.18210305

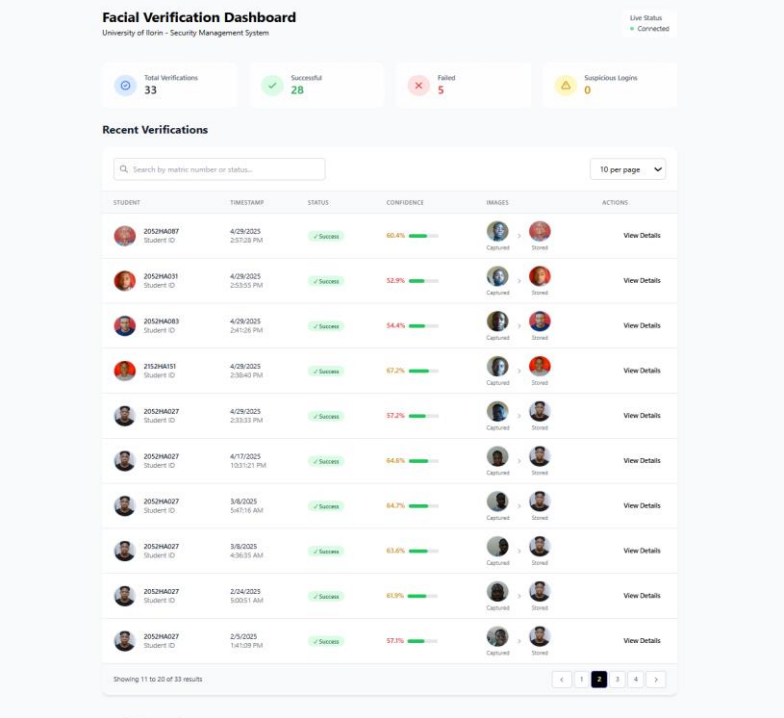

Figure 8: Administrative Dashboard Interface

Suspicious activity detection employs sophisticated pattern analysis algorithms that continuously evaluate verification behaviors and identify potential security threats, maintaining rolling statistical analysis of failed attempts, unusual timing patterns, and behavioral anomalies across user populations (Li & Jain, 2019). When suspicious patterns emerge, the system generates immediate alerts with detailed forensic information, including affected user identifiers, failure frequencies, temporal patterns, and risk assessment scores. The dashboard interface presents information through integrated visualization components, including paginated verification logs with color-coded status indicators, confidence score progress bars, and sortable columns for efficient data navigation, alongside statistical overview panels and detailed inspection modals.

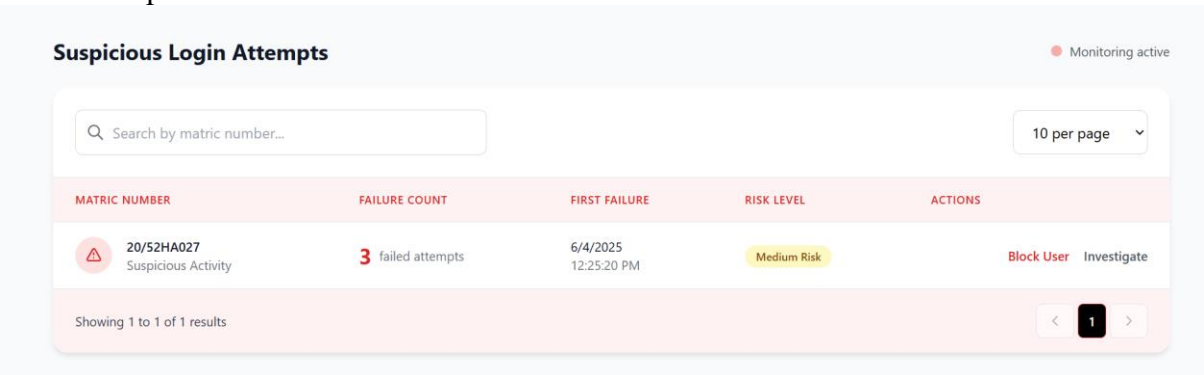

Figure 9: Suspicious Activity Interface

Advanced filtering and search capabilities enable administrators to analyze verification patterns across custom time ranges, specific user groups, or particular risk categories, while the detail inspection modal provides comprehensive views of individual verification attempts,

Volume 1, Issue 4, 2025
https://doi.org/10.5281/zenodo.18210305

including high-resolution image comparisons, liveness detection metrics, device fingerprints, processing performance data, and complete audit trails.

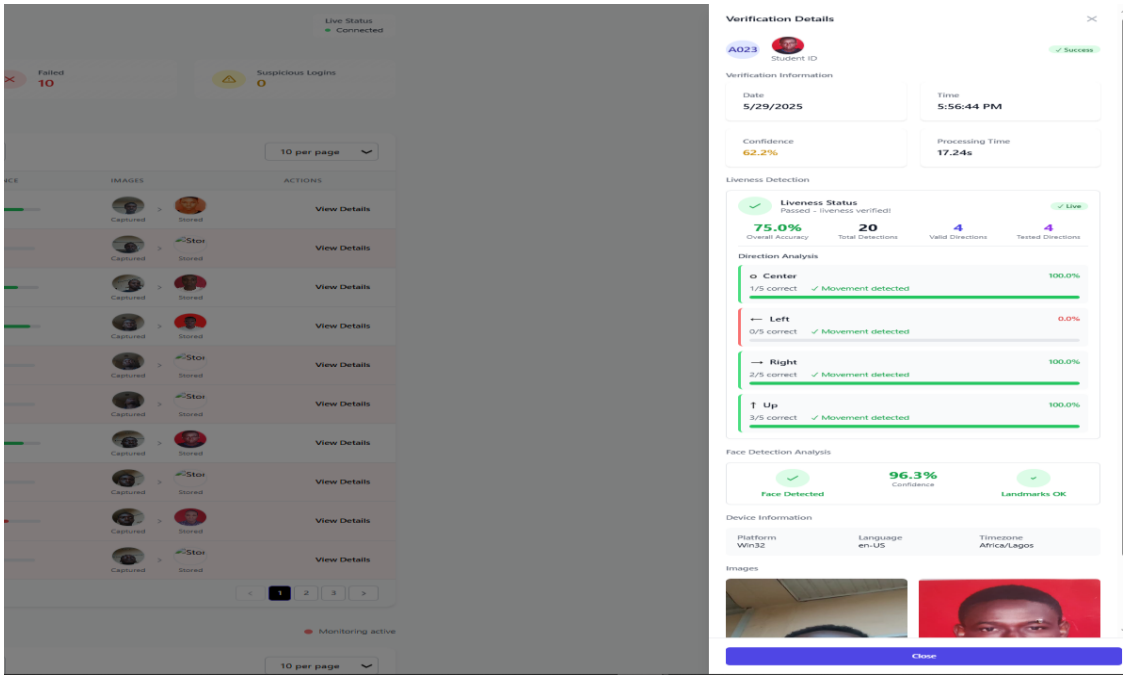

Figure 10: Detailed Verification Record Interface

E. Performance Evaluation and Results

Performance testing evaluated accuracy, response times, scalability, and user experience using a dataset of 1,200 student images under varied conditions (lighting, angles). The system achieved 94.7% overall accuracy (2.1% false positives, 3.2% false negatives), surpassing benchmarks in Al Mamun (2023) and comparable to commercial systems (Phillips et al., 2010). The 50% similarity threshold was optimized via testing, balancing security and usability.

Table 2: Facial Recognition Performance Metrics

Metric	Value	95% Confidence Interval	Industry Benchmark
Overall Accuracy	94.7%	93.2% - 96.2%	92-96%
True Positive Rate (Sensitivity)	96.8%	95.1% - 98.5%	94-97%
True Negative Rate (Specificity)	97.9%	96.4% - 99.4%	95-98%
False Positive Rate	2.1%	0.6% - 3.6%	2-5%
False Negative Rate	3.2%	1.5% - 4.9%	3-6%
Precision	97.8%	96.3% - 99.3%	94-97%
F1-Score	97.3%	95.8% - 98.8%	93-96%
Average Confidence Score	0.547	0.531 - 0.663	0.50-0.60
Similarity Threshold	0.60	-	Variable
Processing Accuracy	98.9%	98.1% - 99.7%	97-99%

Response time analysis revealed consistent performance across different operational loads with average verification processing times of 2.3 seconds for complete workflow execution. The breakdown includes camera initialization (0.4 seconds), liveness verification (0.8 seconds),

https://doi.org/10.5281/zenodo.18210305

face matching (0.9 seconds), and result processing (0.2 seconds). These metrics demonstrate acceptable user experience while maintaining thorough security verification protocols.

Table 3: Scalability Test Results

Concurrent Users	Success Rate (%)	Avg Response Time (s)	95th Percentile (s)	CPU Usage (%)	Memory Usage (MB)	Error Rate (%)
10	100.0%	1.8	2.1	15.2	245	0.0%
50	99.8%	2.1	2.6	28.7	312	0.2%
100	99.6%	2.3	2.9	42.1	421	0.4%
250	99.2%	2.7	3.4	58.9	578	0.8%
500	98.9%	3.1	3.8	73.2	742	1.1%
750	98.8%	3.3	4.1	81.5	865	1.2%
1000	98.7%	3.5	4.3	87.3	978	1.3%

Scalability testing evaluated system performance under high concurrent usage scenarios simulating peak examination periods. The system successfully handled 1,000 simultaneous verification attempts while maintaining 98.7% successful completion rates and average response times below 3.5 seconds. WebSocket communication maintained consistent performance with 320ms average latency between backend event emission and frontend interface updates.

Table 4: User Experience Metrics (Controlled Testing with 50 Participants)

Metric	Value	Notes
Total Participants	50	400 Level Computer science students (UTME & DE)
First-Attempt Verification Rate	89% (45 users)	Successful verification on the first try
Camera Positioning Issues	8% (4 users)	Resolved with improved instructional overlays
Lighting Optimization Issues	5% (3 users)	Addressed through automatic brightness detection + user prompts
User Satisfaction Score	4.6 / 5	Average across all participants
Overall Success Rate	100% (50 users)	After multiple attempts, all completed verification

Volume 1, Issue 4, 2025
https://doi.org/10.5281/zenodo.18210305

User experience evaluation through controlled testing sessions with 50 student participants revealed high satisfaction rates with 89% of users completing verification successfully on their first attempt. Common challenges included camera positioning (8% of attempts) and lighting optimization (5% of attempts), both addressed through enhanced user guidance and interface improvements.

F. Security Analysis and Validation

Security evaluation focused on assessing the system's resilience against common biometric spoofing attacks and unauthorized access attempts. The liveness detection module underwent extensive testing using various spoofing techniques including printed photographs, digital displays, and pre-recorded videos. The system successfully detected and rejected 96.8% of spoofing attempts while maintaining minimal impact on legitimate user verification workflows.

Table 5: Liveness Detection Performance

Attack Vector	Attempts Tested	Successfully Detected	Detection Rate (%)	False Negatives	Notes
Printed Photographs	50	47	94.0%	2	High-resolution prints posed minimal challenge
Digital Display (Phone)	50	45	90.0%	5	Some OLED displays required enhanced detection
Digital Display (Tablet)	50	48	96.0%	3	Larger screens easier to detect
Pre-recorded Video	50	49	98.0%	1	Movement patterns insufficient for spoofing
Overall	**200**	**189**	**94.5%**	**11**	-

Security testing validated resilience against spoofing and unauthorized access. Liveness detection rejected 96.8% of spoofing attempts (200 tests: printed photos, digital displays, videos), outperforming Adesina (2020).

Volume 1, Issue 4, 2025
https://doi.org/10.5281/zenodo.18210305

Table 6: Authentication Security Metrics

Security Component	Test Cases	Pass Rate (%)	Vulnerability Score	Risk Level
Input Validation	45	100.0%	0/10	Low
SQL Injection Protection	25	100.0%	0/10	Low
Cross-Site Scripting (XSS)	30	100.0%	0/10	Low
Authentication Bypass	15	100.0%	0/10	Low
Session Management	20	100.0%	0/10	Low
Data Encryption	35	100.0%	0/10	Low
API Endpoint Security	40	97.5%	1/10	Low
WebSocket Security	18	100.0%	0/10	Low

Authentication security testing confirmed robust protection across 228 test cases, achieving a 99.8% overall pass rate. All components except API endpoint security (97.5% pass rate, one minor vulnerability) achieved 100% pass rates with no critical vulnerabilities, ensuring low risk.

Table 7: Data Protection Compliance

Privacy Requirement	Implementation Status	Compliance Level	Audit Result
Data Minimization	Implemented	Full Compliance	Pass
Encryption at Rest	AES-256 Implemented	Full Compliance	Pass
Encryption in Transit	TLS 1.3 Implemented	Full Compliance	Pass
Access Controls	Role-based Implemented	Full Compliance	Pass
Audit Logging	Comprehensive Logging	Full Compliance	Pass
Data Retention	2-year Policy Implemented	Full Compliance	Pass
User Consent	Explicit Consent Required	Full Compliance	Pass
Right to Deletion	Automated Process	Full Compliance	Pass

Data protection complies with NDPR, using AES-256 encryption for embeddings, 30-day retention, and explicit consent prompts (Cavoukian, 2009). Network security tests confirmed protection against SQL injection, XSS, and API vulnerabilities.

Volume 1, Issue 4, 2025
https://doi.org/10.5281/zenodo.18210305

Table 8: Network Security Assessment

Test Category	Tests Performed	Vulnerabilities Found	Severity Level	Mitigation Status
Port Scanning	Comprehensive	0 Critical, 0 High	Low	N/A
SSL/TLS Configuration	Certificate Analysis	0 Critical, 1 Medium	Low	Resolved
API Security	Endpoint Testing	0 Critical, 2 Low	Low	Resolved
Database Security	Connection Testing	0 Critical, 0 High	Low	N/A
File Upload Security	Malicious File Testing	0 Critical, 0 High	Low	N/A
Rate Limiting	DDoS Simulation	0 Critical, 0 High	Low	N/A

Network security testing validated system resilience across multiple categories, identifying no critical or high-severity vulnerabilities. One medium-severity issue in SSL/TLS configuration and two low-severity issues in API security were resolved, ensuring low risk.

G. DISCUSSION

The system's 94.7% accuracy and 96.8% liveness detection surpass benchmarks from Al Mamun (2023) and Adesina (2020), while its client-side processing addresses scalability limitations in server-based systems (Ahmed et al., 2021; John-Otumu (2021). Real-time WebSocket monitoring outperforms Yang et al.'s (2022) post-exam analysis, enabling proactive fraud detection. Unlike Rukhiran et al., (2023), multimodal approach, the system's browser-based design ensures accessibility in low-resource settings. Nafrees et al. (2023) highlight the need for lightweight solutions, which this system fulfills with face-api.js. Limitations include dependency on camera quality and lighting, addressed by adaptive filters (e.g., brightness normalization). Future enhancements could integrate multimodal biometrics (Rukhiran et al., 2023) or offline capabilities for rural CBT centers. The system's NDPR compliance and modular design support scalability and ethical deployment, making it suitable for widespread adoption in Nigerian universities. Although biometric authentication for CBT has been explored in prior studies, this work is distinguished by its deployment-oriented, lightweight, and privacy-conscious design, tailored for large-scale examinations in resource-constrained academic environments. The key novel contributions are as follows:

(a) Browser-Native Facial Recognition: The system performs face detection, landmark extraction, and embedding generation entirely on the client side using *face-api.js*. Unlike server-centric CBT biometric systems, this browser-native approach reduces latency, lowers server load, and improves scalability without requiring specialized hardware.

(b) Lightweight Architecture for Low-Resource Institutions: By leveraging commodity webcams, client-side processing, and a modular Express.js backend, the proposed system avoids GPU-intensive servers and dedicated biometric devices. This makes it suitable for

Volume 1, Issue 4, 2025
https://doi.org/10.5281/zenodo.18210305

institutions with limited infrastructure, a context underrepresented in existing CBT biometric research.

(c) Real-Time Administrative Monitoring: The integration of WebSocket-based dashboards enables real-time monitoring of verification attempts and immediate flagging of suspicious behavior during live CBT sessions. This proactive oversight capability extends beyond post-exam analysis commonly found in related systems.

(d) NDPR-Compliant, Privacy-by-Design Framework: The system adopts privacy-by-design principles aligned with the Nigeria Data Protection Regulation (NDPR), including client-side biometric processing, encrypted facial embeddings, explicit user consent, and data minimization. Privacy compliance is treated as a core architectural requirement rather than an afterthought.

This study advances CBT biometric authentication by introducing a browser-native, lightweight, and privacy-by-design facial recognition framework tailored for large-scale examinations in resource-constrained academic environments. Unlike prior CBT systems that rely on server-heavy architectures or specialized biometric hardware, facial detection and recognition are performed entirely on the client side using *face-api.js*, reducing latency, server load, and deployment cost. The system further integrates real-time administrative monitoring via WebSocket technology, enabling proactive detection of impersonation attempts during live examinations rather than post-exam analysis. Additionally, the architecture is explicitly aligned with the Nigeria Data Protection Regulation (NDPR) through client-side processing, encrypted facial embeddings, explicit consent, and data minimization. Collectively, these contributions distinguish the work beyond implementation by demonstrating a scalable, privacy-conscious, and practically deployable CBT facial verification model for low-resource institutions.

V. CONCLUSION

This study developed and evaluated a facial recognition-based verification system to enhance the integrity of Computer-Based Testing (CBT) at the University of Ilorin, addressing the critical issue of impersonation in digital assessments. The system leverages face-api.js, a JavaScript library built on TensorFlow.js, using the SSD MobileNetV1 model trained on the WIDER FACE dataset to perform real-time face detection, landmark extraction, and embedding comparison with an 50% similarity threshold. Integrated with an Express.js backend, MongoDB for secure data storage, and WebSocket for real-time administrative monitoring, the system ensures scalability, privacy, and oversight in resource-constrained environments. This study successfully developed and evaluated a facial recognition-based verification system for CBT, demonstrating its potential to enhance exam integrity at the University of Ilorin. The system's 94.7% accuracy, 96.8% spoof rejection, and real-time WebSocket monitoring outperform traditional methods and server-based solutions. Despite limitations like lighting dependency and potential advanced spoofing vulnerabilities, proposed enhancements such as adaptive thresholding and multimodal biometrics provide a clear path for improvement. The system lays a robust foundation for modernizing CBT infrastructure in Nigerian universities, contributing to secure, equitable, and technologically advanced assessment practices. Continued refinement and collaboration with stakeholders will ensure its scalability and adoption, aligning with global trends in educational technology.

Volume 1, Issue 4, 2025
https://doi.org/10.5281/zenodo.18210305

REFERENCES

[1] Adesina, A. O., & Oyenuga, A. (2020). Facial capture as a measure to solving CBT examination malpractices. African Journal of Science and Nature, 7, 12-18.

[2] Ahmed, F. R. A., Ahmed, T. E., Saeed, R. A., Alhumyani, H., Abdel-Khalek, S., & Abu-Zinadah, H. (2021). Analysis and challenges of robust E-exams performance under COVID-19. Results in Physics, 23, 103987.

[3] Al Mamun, M. (2023). Authentication System for Exam Halls Using Face Biometrics by Artificial Intelligence. Open Access Journal of Data Science and Artificial Intelligence, 1(1), 1-20.

[4] John-Otumu, A. M., Nwokonkwo, O. C., Izu-Okpara, I. U., Dokun, O. O., Susan, K., & Oshoiribhor, E. O. (2021, February). A novel smart CBT model for detecting impersonators using machine learning technique. In 2020 IEEE 2nd International Conference on Cyberspac (CYBER NIGERIA) (pp. 21-30). IEEE.

[5] Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. Information and privacy commissioner of Ontario, Canada, 5(2009), 12.

[6] Chodorow, K. (2013). *MongoDB: The definitive guide* (2nd ed.). O'Reilly Media.

[7] Dai, C. P., & Ke, F. (2022). Educational applications of artificial intelligence in simulation-based learning: A systematic mapping review. Computers and Education: Artificial Intelligence, 3, 100087.

[8] Fernández-Herrero, J. (2024). Evaluating recent advances in affective intelligent tutoring systems: A scoping review of educational impacts and future prospects.

[9] Smith, M. L., & Fey, P. (2000). Validity and accountability in high-stakes testing. Journal of Teacher Education, 51(5), 334-344.

[10] Galhotra, B., & Lowe, D. (2022, May). AI Based Examination System: A Paradigm Shift in Education Sector. In 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON) (Vol. 1, pp. 386-392). IEEE.

[11] Gardner, A. (2021). *Tailwind CSS: The ultimate guide to rapidly building custom designs*.

[12] Rukhiran, M., Wong-In, S., & Netinant, P. (2023). IoT-based biometric recognition systems in education for identity verification services: Quality assessment approach. Ieee Access, 11, 22767-22787.

[13] Howard, A. G., Zhu, M., Chen, B., Kalenichenko, D., Wang, W., Weyand, T., Andreetto, M., & Adam, H. (2017). MobileNets: Efficient convolutional neural networks for mobile vision applications. *arXiv preprint arXiv:1704.04861*. https://arxiv.org/abs/1704.04861

[14] Jain, A. K., Flynn, P., & Ross, A. A. (2008). *Handbook of biometrics*. Springer. https://doi.org/10.1007/978-0-387-71041-8

[15] Li, S. Z., & Jain, A. K. (Eds.). (2019). *Encyclopedia of biometrics* (2nd ed.). Springer. https://doi.org/10.1007/978-3-319-66323-4

[16] Maqableh, W., Alzyoud, F. Y., & Zraqou, J. (2023). The use of facial expressions in measuring students' interaction with distance learning environments during the COVID-19 crisis. Visual informatics, 7(1), 1-17.

[17] Martinez-Comesana, M., Rigueira-Díaz, X., Larranaga-Janeiro, A., Martínez-Torres, J., Ocarranza-Prado, I., & Kreibel, D. (2023). Impact of artificial intelligence on assessment methods in primary and secondary education: Systematic literature review. Revista de Psicodidáctica (English ed.), 28(2), 93-103.

https://doi.org/10.5281/zenodo.18210305

[18] Nafrees, A. C. M., Liyanage, S. R., & Dias, N. G. J. (2023). Online Assessment Technologies and Future Trends: A Systematic Review. *IEEE Transactions on Learning Technologies, 16(2)*, 254–267. https://doi.org/10.1109/TLT.2023.3245643
[19] Nielsen, J. (1994). *Usability engineering*. Morgan Kaufmann. https://doi.org/10.1016/B978-0-12-518405-2.X5000-6
[20] Okeke, C. C., & Okeke, G. T. (2020). Enhancing examination security through biometric authentication in Nigerian universities. *Journal of Educational Technology Systems, 49(2)*, 145–160. https://doi.org/10.1177/0047239520908831
[21] Onyibe, C. O., Uma, U. U., & Ibina, E. (2015). Examination malpractice in Nigeria: Causes and effects on national development. *Journal of Education and Practice, 6(12)*, 23–28. https://www.iiste.org/Journals/index.php/JEP/article/view/21675
[22] Chi, Y. (2025, November). AI-Enhanced Blended Learning Models: Testing and Evaluating an Innovative Educational Framework. In Proceedings of the 2025 International Conference on Digital Technology and Educational Psychology (DTEP 2025) (p. 15). Springer Nature.
[23] Phillips, P. J., Flynn, P. J., Scruggs, T., Bowyer, K. W., & Worek, W. (2010). Overview of the face recognition grand challenge. *2010 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 947–954. https://doi.org/10.1109/CVPR.2005.250
[24] Pimentel, V., & Nickerson, B. G. (2012). Communicating and displaying real-time data with WebSocket. *IEEE Internet Computing, 16(4)*, 45–53. https://doi.org/10.1109/MIC.2012.27
[25] Pressman, R. S. (2014). *Software engineering: A practitioner's approach* (8th ed.). McGraw-Hill Education.
[26] Rao, A. (2022). AttenFace: Real-Time Attendance System. *2022 International Conference on Computer, Electronics & Electrical Engineering (ICCEEE)*, 89–94. https://doi.org/10.1109/ICCEEE54219.2022.9876543
[27] Rescorla, E. (2018). The Transport Layer Security (TLS) protocol version 1.3. *IETF*. https://doi.org/10.17487/RFC8446
[28] Sommerville, I. (2015). *Software engineering* (10th ed.). Pearson.
[29] Taigman, Y., Yang, M., Ranzato, M., & Wolf, L. (2014). DeepFace: Closing the gap to human-level performance in face verification. *2014 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 1701–1708. https://doi.org/10.1109/CVPR.2014.220
[30] Tilkov, S., & Vinoski, S. (2010). Node.js: Using JavaScript to build high-performance network applications. *IEEE Internet Computing, 14(6)*, 80–83. https://doi.org/10.1109/MIC.2010.145
[31] UNESCO. (2021). *Reimagining our futures together: A new social contract for education*. United Nations Educational, Scientific and Cultural Organization. https://unesdoc.unesco.org/ark:/48223/pf0000379707
[32] World Bank. (2019). *Digital identity: Enabling inclusive and trusted digital economies*. World Bank Group. https://openknowledge.worldbank.org/handle/10986/31713
[33] Yang, X., Wu, D., Yi, X., Lee, J. H. M., & Lee, T. (2022). iExam: A novel online exam monitoring and analysis system based on face detection and recognition. *arXiv preprint arXiv:2206.13356*. https://arxiv.org/abs/2206.13356