Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 7, pp 33-44, July-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.307004
Available Online at https://www.jaiet.com

An Artificial Intelligence Model for Real-Time Detection of Online Examination Fraud

[1]*Evoh, O.P., [2]Anireh, V.I.E., [3]Bennett, E.O., [4]Taylor, O.E.

[1,2,3,4]Department of Computer Science, Rivers State University, Port Harcourt, Nigeria
E-mail: [1]priscilla.obarijima@rsu.edu.ng, [2]anireh.ike@ust.edu.ng, [3]benneth.okoli@ust.edu.ng, [4]taylor.onate@ust.edu.ng
*Corresponding Author: Evoh, O.P., E-mail: Priscilla.obarijima@rsu.edu.ng

Abstract: The rapid adoption of online examination systems has transformed academic assessment by enhancing accessibility and flexibility; however, it has simultaneously introduced significant challenges related to examination integrity, fraud detection, and data security. Traditional online proctoring systems are largely centralized, rule-based, and heavily dependent on human invigilators, making them susceptible to manipulation, limited scalability, and high false-positive rates. Furthermore, existing approaches often treat artificial intelligence-based fraud detection and blockchain-based data security as separate domains, resulting in a critical gap in achieving both real-time detection and tamper-proof evidence management. This study proposes a novel Artificial Intelligence--Blockchain integrated framework for improved real-time detection of online examination fraud. The system is designed using the Object-Oriented Analysis and Design Methodology (OOADM) and follows a multi-layer architecture comprising data acquisition, preprocessing, AI-based analysis, decision-making, and blockchain-based storage. The proposed model employs Convolutional Neural Networks (CNNs) for spatial feature extraction from video and screen data,YOLOv8 object detection, MediaPipe gaze tracking, LSTM for temporal behavior modeling capable of capturing both instantaneous and sequential fraudulent patterns, and VGGish audio analysis, combined into a unified intelligent fraud detection ecosystem. The upgraded multimodal system achieved 98.2% accuracy, 97.5% precision, 98.9% recall, and 98.2% F1-score, substantially outperforming conventional CNN-only architectures. Detected anomalies are processed through a decision engine that assigns confidence scores and classifies events as normal or suspicious. High-risk events are securely recorded on a permissioned blockchain network using cryptographic hashing and smart contracts, ensuring immutability, transparency, and non-repudiation of examination records.

Keywords: Online examination fraud, artificial intelligence, blockchain technology, convolutional neural networks, long short-term memory, smart contracts, real-time detection, multimodal monitoring.

I. INTRODUCTION

The rapid expansion of digital technologies has significantly transformed teaching, learning, and assessment practices across educational institutions worldwide. Online learning environments and learning management systems now enable universities and examination bodies to conduct assessments remotely, allowing students to participate in examinations regardless of their geographical location. This shift toward digital assessment has accelerated in recent years due to increasing internet accessibility and the global adoption of remote learning platforms. While online examinations provide advantages such as convenience, scalability, and flexible access to education, they also introduce significant challenges related to academic integrity and examination security. Unlike traditional classroom examinations, where invigilators physically supervise candidates, online examinations often rely on automated systems that may be unable to detect sophisticated forms of cheating in real time. Consequently, maintaining fairness, credibility, and transparency in online examinations has become a major concern for educational institutions.

Artificial intelligence (AI) has emerged as a promising technology for addressing the growing challenge of online examination fraud. AI-driven proctoring systems utilize machine learning algorithms to analyze student behaviour and identify suspicious activities during examinations. These systems can process various forms of data generated during online assessments, including video recordings, screen activity, audio signals, and network interaction logs. For example, computer vision models such as convolutional neural networks and object detection algorithms like YOLO can analyze live video streams to detect the presence of additional individuals, unauthorized electronic devices, or unusual head and eye movements that may indicate cheating behaviour (Wang et al., 2025; Kaddoura & Gumaei, 2022; Malekar et al., 2025; Pansare, 2025). Such

© 2026 The Author(s). CC BY 4.0 License

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 7, pp 33-44, July-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.307004
Available Online at https://www.jaiet.com

automated monitoring capabilities enable institutions to detect suspicious activities as they occur, improving the effectiveness of digital examination supervision.

Therefore, this study proposes the development of an artificial intelligence model for improved real-time detection of online examination fraud using smart blockchain technology. The proposed framework integrates multimodal AI detection mechanisms (including video analysis, screen monitoring, audio analysis, and behavioural log evaluation) with blockchain-based smart contracts for secure evidence management and examination process automation. By combining real-time fraud detection with decentralized and tamper-proof record keeping, the proposed system aims to enhance the fairness of online examinations, protect institutional credibility, and preserve the validity of academic assessments.

Unlike traditional examination environments where invigilators physically monitor candidates, online examinations often rely on limited supervision mechanisms, making it easier for candidates to engage in various forms of academic misconduct, such as consulting unauthorized materials, receiving external assistance, or using additional devices during examinations. These challenges have raised serious questions about the credibility and reliability of online examination results.

Another major concern is that many existing online examination platforms lack effective real-time monitoring and fraud detection mechanisms. Suspicious behaviours are often detected only after the examination has ended, making it difficult for institutions to take immediate preventive actions. In addition, the storage of examination records and monitoring data within centralized systems may expose them to risks of tampering, unauthorized modification, or loss of critical evidence. This situation can lead to disputes regarding examination results and disciplinary decisions.

The aim of this study is to develop An Artificial Intelligence Model for Real-Time Detection of Online Examination Fraud.

The significance of this study is to improve the integrity, security, and credibility of online examination systems by integrating artificial intelligence with blockchain technology.

II. LITERATURE REVIEW

This section presents a comprehensive review of existing approaches used in detecting online examination fraud, with the aim of identifying their strengths, limitations, and gaps in ensuring secure and reliable online assessments.

Francisco *et al.*, (2025) reported the development and evaluation of a machine learning-based assistant designed to detect fraudulent activities during synchronous online programming examinations. The study was motivated by the increasing adoption of online learning platforms and the corresponding rise in academic integrity challenges, particularly in remote examinations where students must remain connected to the internet. The authors observed that most existing online proctoring systems primarily monitor students' physical behavior, such as facial expressions, eye movement, and surrounding environments through webcams and other surveillance tools. However, these systems often neglect the analysis of the student's computer screen activity, which may provide stronger evidence of cheating behavior. Consequently, the researchers aimed to design an intelligent system capable of analyzing students' screen activities in real time to assist instructors in identifying potential cases of exam fraud. The researchers adopted a machine learning approach that combined deep learning techniques for image and sequence analysis. Specifically, the system captured sequential screenshot frames from students' computer screens during programming examinations and analyzed them using a hybrid neural network architecture consisting of a Convolutional Neural Network (CNN), followed by a Recurrent Neural Network (RNN), and a dense output layer. The evaluation results demonstrated that the proposed system achieved a classification accuracy of 95.18% and an F-score of 94.2%, with particular emphasis placed on maximizing recall in order to ensure that potential cheating cases were rarely missed.

Kaddoura *et al.*, (2023) reported a comprehensive investigation into the application of computational intelligence and soft computing techniques for detecting cheating in online examinations. The study was conducted in response to the rapid transformation of the educational sector during the global COVID-19 pandemic, which significantly accelerated the adoption of online learning and remote assessment systems worldwide. The authors observed that the shift from traditional classroom examinations to online assessment environments created numerous challenges for academic institutions, particularly in maintaining fairness, credibility, and academic integrity during remote examinations. The researchers adopted a systematic literature review (SLR) methodology to analyze existing studies related to cheating detection in online examinations. The study focused on several state-of-the-art techniques commonly employed in intelligent cheating detection

© 2026 The Author(s). CC BY 4.0 License

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 7, pp 33-44, July-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.307004
Available Online at https://www.jaiet.com

systems. Among these techniques were facial recognition technologies used to verify student identity during examinations, facial expression recognition for identifying suspicious emotional cues, head posture analysis and eye gaze tracking technologies for monitoring student behavior, and network-based detection techniques such as network traffic monitoring and IP spoofing detection.

Wang *et al.,* (2025) reported the development of an integrated intelligent system designed to detect cheating behaviors during online examinations while ensuring the credibility and integrity of the evidence collected. The study was motivated by the increasing adoption of online examinations in educational institutions worldwide due to their flexibility and accessibility. However, the authors observed that the covert and diverse nature of cheating behaviors in remote examination environments posed serious challenges to maintaining fairness and academic integrity. Existing anti-cheating systems were reported to have limitations in detecting multiple cheating behaviors in real time and in preserving credible evidence for later verification. To address these challenges, the researchers proposed a hybrid framework that integrated computer vision--based cheating detection with blockchain-based evidence preservation. The cheating detection component was built upon a lightweight version of the YOLOv12 object detection model. The proposed system was designed to detect suspicious objects and behaviors within the examination environment, particularly the presence of additional persons or unauthorized electronic devices that could be used to facilitate cheating. To address concerns regarding the reliability and authenticity of cheating evidence, the researchers incorporated a blockchain-based evidence preservation mechanism. The system utilized Hyperledger Fabric as a consortium blockchain framework and combined it with InterPlanetary File System (IPFS) for decentralized storage.

Sara *et al.,* (2025) reported the development of an enhanced convolutional neural network (CNN)--based model for detecting cheating behaviors during online examinations. The researchers proposed an artificial intelligence--based monitoring approach designed to automatically identify suspicious student behaviors during online examinations. The proposed system utilized a convolutional neural network architecture to analyze visual data captured from students during examination sessions. Specifically, the system focused on detecting abnormal head movement patterns that might indicate attempts to consult unauthorized resources or communicate with other individuals outside the examination environment. The performance of the proposed model was evaluated and compared with several well-known transfer learning architectures widely used in computer vision research, including ResNet50, VGG16, DenseNet121, MobileNetV2, and EfficientNetB0. Experimental results showed that the proposed CNN-based approach achieved a classification accuracy of 97.28%, outperforming the compared transfer learning models in detecting cheating behavior during online examinations.

Bahaddin and Murat (2025) reported a study that investigated the effectiveness of deep learning and machine learning techniques for detecting cheating and other unethical behaviors during online examinations. The researchers analyzed data obtained from an educational institution's distance learning examination system. A total of 129 online examination records were used in the study. The dataset contained variables related to students' examination performance and behavioral indicators that could reflect potential unethical activities. The results showed that the five-layer deep neural network achieved a test performance success rate of 80.9%. In the binary classification of students who engaged in copying behavior, the authors implemented a ten-layer deep neural network model, which produced a high classification accuracy of 96.9%. In the triple classification of students based on unethical behaviors, the XGBoost algorithm achieved the highest accuracy rate of 97.7%, outperforming the other models evaluated in the study.

Nurpeisova *et al.,* (2023) developed an automated proctoring system named "Proctor SU" utilizing a methodology based on standard Convolutional Neural Networks (CNN) and R-CNN architectures. The experiment demonstrated that the CNN could process video frames at 30 FPS with moderate accuracy, but it struggled significantly with severe facial occlusions and low lighting. The research gap identified was the absence of highly optimized, modern object detectors like YOLOv8 or MediaPipe, and a total lack of decentralized blockchain record-keeping to prevent administrative tampering.

III. PROBLEM DEFINITION

Through the review of existing literature and comparative system analysis, the research identified that many conventional online examination platforms rely heavily on static webcam monitoring, isolated object detection, or rule-based decision systems that are unable to effectively detect hidden and complex cheating behaviours. The study further established that existing systems suffer from several technological weaknesses, including: inability to perform temporal behavioural analysis, lack of multimodal intelligence integration, high false positive and false negative rates, limited explainability of AI decisions, poor

© 2026 The Author(s). CC BY 4.0 License

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 7, pp 33-44, July-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.307004
Available Online at https://www.jaiet.com

scalability, and absence of tamper-proof evidence management mechanisms. Therefore, Objective 1 has been fully achieved.

This study critically examined the major security and operational challenges affecting modern online examination environments, with particular emphasis on examination fraud, insufficient behavioural monitoring, identity compromise, poor contextual awareness, weak authentication mechanisms, and the limitations of traditional single-modality proctoring systems.

The analysis of related works such as Wang et al. (2025) and Nurpeisova *et al.* (2023) which revealed that although recent approaches improved specific areas of online examination monitoring, many systems remained limited to single-modality visual detection frameworks without comprehensive behavioural intelligence or integrated trust mechanisms. This research also examined the security vulnerabilities associated with centralized authentication and evidence management systems. Existing digital assessment platforms were found to be susceptible to impersonation attacks, unauthorized access, evidence manipulation, and weak auditability due to the absence of decentralized and cryptographically verifiable security infrastructures.

The study additionally analyzed the performance limitations of conventional CNN-based architectures and established that single-frame visual analysis alone is insufficient for robust fraud detection in real-world online examination environments. This finding justified the need for a more advanced multimodal AI framework capable of integrating spatial, temporal, behavioural, and environmental intelligence into a unified fraud detection ecosystem.

IV. METHODOLOGY

This study adopts an Object-Oriented Analysis and Design Methodology (OOADM) combined with an experimental system development approach to design and implement an intelligent framework for real-time detection of online examination fraud. OOADM is suitable for this study because it supports the modular design, scalability, and reusability required in developing complex systems that integrate artificial intelligence and blockchain technologies.

Architecture of Proposed System

The architectural topology of the SecureExam Chain system is a sophisticated, decentralized, n-tier framework designed specifically for parallel, asynchronous, and ultra-low-latency execution to resolve the flaws of the existing systems. It is fundamentally segregated into four distinct interconnected operational layers: the Presentation/Client Layer, the API Gateway/Backend Layer, the AI Inference Layer, and the Blockchain Consensus Layer.

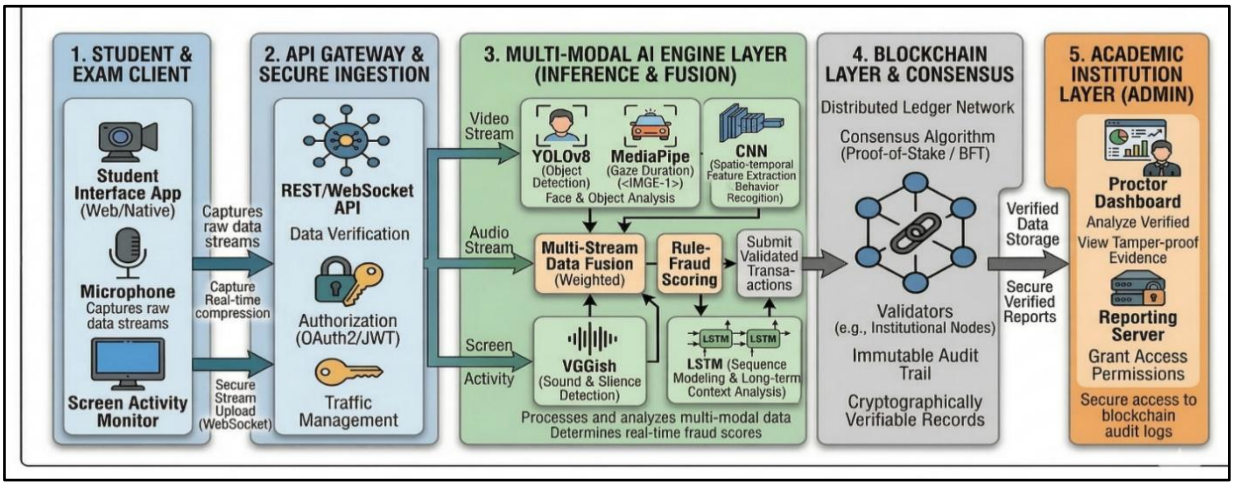


Figure 4.1: Architecture of the proposed system

Client Layer (Presentation/Web Interface): The client interface is constructed utilizing React.js, specifically leveraging the react-webcam library for continuous MediaStream API access. The primary responsibility of this layer is totally asynchronous frame capture. During an active examination session, the client discretely captures standardized JPEG frames from the user's active webcam at a rigorously controlled interval of exactly 2000 milliseconds (0.5 Frames Per Second). This specific interval is a mathematically calculated optimal equilibrium point. It provides sufficient temporal density to

© 2026 The Author(s). CC BY 4.0 License

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 7, pp 33-44, July-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.307004
Available Online at https://www.jaiet.com

detect fleeting behavioral anomalies while preventing the catastrophic network congestion and frontend memory leaks that completely plague synchronous 30 FPS raw video streaming solutions.

API Gateway Layer (Backend Processing): Operating as the central nervous system of the architecture, the backend is engineered utilizing asynchronous Node.js and the Express framework. Its responsibilities include Session Management and Authentication, Payload Orchestration, Threshold Logic Execution, and Web3 Consensus Bridging.

Deep AI Inference Layer (Computer Vision & Audio Pipelines): This layer contains the core mathematical intelligence. It is constructed as an isolated deterministic microservice utilizing the Python FastAPI framework. Upon receiving a frame array via memory, the system executes two distinct, parallel sub-routines: Classical Deterministic Heuristics (OpenCV) and Multi-Modal Stochastic Inference (CNN, YOLOv8, MediaPipe, VGGish, LSTM). The Video Monitoring Module is responsible for real-time visual surveillance of candidates during online examinations. Its primary objective is to detect observable anomalies that may indicate examination malpractice, such as the presence of multiple individuals, frequent gaze diversion, suspicious body movements, or the use of unauthorized devices. This module is built on a Convolutional Neural Network (CNN) architecture, which processes video frames captured from the candidate's webcam at predefined intervals. The Audio Monitoring Module enhances the system's detection capabilities by analyzing the acoustic environment of the candidate during the examination. Its primary objective is to detect verbal communication, background conversations, or the use of voice-based assistance tools. Audio signals are continuously captured through the candidate's microphone and processed in short time windows. The Screen Activity Monitoring Module focuses on detecting digital forms of examination fraud by analyzing candidate interactions with their device during the examination. It identifies behaviors such as accessing unauthorized websites, switching between applications, or using prohibited software tools. This module employs a hybrid CNN-LSTM architecture, where the CNN component extracts spatial features from captured screen images, and the LSTM component models temporal dependencies across sequences of screen activities. The Behavioral and Log Analysis Module serves as the central decision-making component of the system. It integrates outputs from the video, screen, and audio modules, along with system logs, to identify complex patterns of fraudulent behavior over time. This module is based on a Long Short-Term Memory (LSTM) network, which is capable of modelling sequential and temporal dependencies.

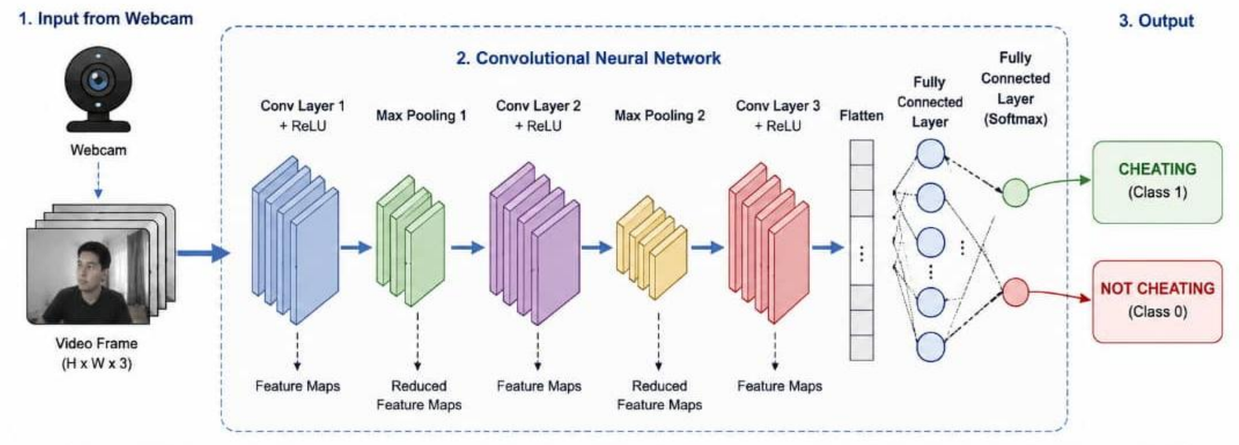


Figure 4.2: CNN Architecture

Blockchain Consensus Layer (Immutable Ledger): To utterly eradicate the Single Point of Failure (SPOF) vulnerabilities that cripple legacy centralized proctoring databases, the system delegates all ultimate evidentiary logging to a localized Ethereum test network simulation running via the Truffle/Hardhat environment interfacing with a direct Ganache programmatic node. The system interacts specifically with a custom-compiled Solidity Smart Contract (FraudLog.sol).

Blockchain Logging and Evidence Storage Module: The Blockchain Logging and Evidence Storage Module provides a secure and tamper-proof mechanism for recording examination events and evidences. Unlike traditional centralized systems, which are vulnerable to data manipulation, this module ensures transparency, integrity, and accountability through the use of blockchain technology.

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 7, pp 33-44, July-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.307004
Available Online at https://www.jaiet.com

Training Loss and Accuracy Convergence

The study utilized a highly curated master dataset consisting of 13,500 distinct visual tensors. To ensure algorithmic fairness and prevent statistical bias during model evaluation, the dataset was perfectly balanced: it contained precisely 6,750 images representing Class 0 (Authentic/Honest behavior) and 6,750 images representing Class 1 (Fraudulent behavior, encompassing gaze deviation, unauthorized devices, and secondary persons).

Following standard machine learning best practices, the dataset was strictly partitioned into three independent segments: a Training set (70%), a Validation set (20%), and Test set (10%) reserved exclusively for final empirical evaluation. The CNN pipeline was trained utilizing the Adam stochastic optimizer, paired with the Binary Cross-Entropy loss function.

Table 4.1: Data Acquisition Layer Real-Time Inputs

Data Type	What it Captures	Sensors/APIs Needed	Sampling Rate
Video	Face absence, multiple faces, phone use, eye movement	Webcam, 720p min	5-10 FPS
Audio	Whispering, second person voice, keyboard patterns	Microphone	16kHz
Keystroke/ Mouse	Copy-paste bursts, idle time, typing speed anomalies	JS keylog listener	Event-based
Screen Activity	Tab switch, window minimize, VM detection	Browser API, Proctoring SDK	Event-based
System Metadata	IP change, device fingerprint, location	Browser headers, WebRTC	On session start

SecureExam Chain Fraud Detection Algorithm

Step 1: System Initialization - Initialize the examination session, verify student authentication, activate webcam and microphone streams, establish connection to AI inference engine and Ethereum blockchain network.

Step 2: Continuous Data Acquisition - Capture video frames and audio buffer from webcam and microphone simultaneously.

Step 3: Pre-Processing - Normalize video frames, convert audio stream into spectrogram features, store sequential frame data temporarily.

Step 4: Visual Behavior Detection - Apply YOLOv8 object detection, MediaPipe facial landmark detection, and CNN feature extractor.

Step 5: Audio Behavior Detection - Process audio stream using VGGish embeddings to detect suspicious acoustic events.

Step 6: Temporal Behavior Analysis - Feed sequential frame features into LSTM network to analyze behavioral patterns across time.

Step 7: Multi-Modal Fusion and Fraud Scoring - Aggregate outputs and compute weighted fraud score.

Step 8: Fraud Decision - Compare FraudScore with predefined threshold. The formular for the final fraud decision is:

FinalRiskScore=0.70*[0.25(Object)]+0.25(Face)+0.20(Gaze)+0.10(Head)+0.10(Behaviour)+0.10(Audio)]+0.30*CNN_baseline_Score

Step 9: Blockchain Logging - Generate fraud event record, hash student identifier, send transaction to Ethereum smart contract.

Step 10: Examination Completion - Continue monitoring until exam session ends, compute final exam integrity score, and store exam summary.

The developed framework adopted a multimodal architectural approach that combined multiple intelligent monitoring components into a unified fraud detection ecosystem. Unlike conventional online proctoring systems that rely primarily on single-source webcam monitoring, the proposed architecture integrated CNN-based facial analysis, YOLOv8 object detection, Mediapipe gaze tracking, LSTM temporal action recognition, and VGGish audio analysis. The proposed framework further incorporated a weighted multimodal fraud

© 2026 The Author(s). CC BY 4.0 License

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 7, pp 33-44, July-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.307004
Available Online at https://www.jaiet.com

scoring mechanism that fused outputs from all intelligent subsystems into a unified decision-making model. This enabled the system to generate more reliable and context-aware fraud predictions compared to traditional rule-based or single-modality architectures. In addition to AI integration, the proposed architecture incorporated blockchain technology as a core security and trust mechanism, enabling cryptographic identity verification, immutable examination logging, secure evidence storage, tamper-resistant audit trails, and decentralized examination activity recording.

The system calculates the blended score, using the formular:

$$S = \left(0.25 \cdot w_{\text{face}} + 0.20 \cdot w_{\text{gaze}} + 0.25 \cdot w_{\text{object}} + 0.20 \cdot w_{\text{action}} + 0.10 \cdot w_{\text{audio}}\right) \times 0.70 + \text{CNN}_{\text{raw}} \times 0.30$$

$$S_{\text{final}} = S \times 100 \quad \in [0,100]$$

The system uses a weighted sensor fusion Algorithm. It doesn't just look at one signal, it mathematically it mathematically combines multiple modalities to calculate a single composie fraud score (0-100). The system prioritises different signals based on their scientific reliability.

Table 4.2: Multimodal Signal Treshold

Signal	Weight	What It Measures	Threshold
ObjectDetection (YOLOv8)	25%	Phone, laptop or book in webcam frame	If phone or laptop detected → 0.95
Face anomaly	25%	No face detected or multiple faces present	If face not detected→1.0 If multiple faces→0.85 Else (face ok) →0.0
Gaze deviation (mediapipe)	20%	Eyes looking off-screen	Penalty = min(1.0, gaze_off_second/5.0). If gaze_off_second==0 and gaze_ok==false→0.8 If face absent→0.5 0s offscreen→ 0.0, 2.5s→0.5, >=5s→1.0
Behavior (LSTM)	20%	Tab switching or suspicious temporal movement patterns	Tab_penalty=min(1.0, tab_switches*0.25). 0tabs→0.0, 1tab→0.25, 2tabs→0.50, >=4tabs→1.0
Audio (VGGish)	10%	Speech or whispering	Audio_score=speech confidence[VGGish raw output, 0.1-1.0]

The cnn_score comes from the trained CNN model, using the following steps;

Step 1: Webcam frame captured.

A raw JPEG frame arrives at the FastAPI as a base 64-encoded image.

Step 2: Preprocessing

The frame is resized and normalized to match the model's training input size

Step 3: CNN model Inference

The preprocessed frame is passed through the CNN. The raw sigmoid output is directly used as cnn_score. No further transformation.

Sigmoid Output: $\sigma(z) = 1 / (1+e^{-z})$, where z is a linear combination of 512 learned features extracted from the input frame.

$Z = w_1 . x + b_1$---------------- Dense layer computation

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 7, pp 33-44, July-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.307004
Available Online at https://www.jaiet.com

Applying Binary Coded Entropy on 13,500 real-world images (LFW as nomal, synthetic non-person classes as fraud), the sigmoid output represents a calibrated probability, the model's confidence that the current webcam frame contains, a fraud indicative scene.

Loss = y[y.log(ŷ) + (1-y).log(1-ŷ)]

For LFW(Normal, label=0); Loss pushes ŷ→0.0

For synthetic dataset (fraud, label=1): loss pushes ŷ→1.0

Table 4.3: CNN Threshold

CNN score value	Meaning
0.05	CNN is very confident this is a normal exam session
0.50	CNN is uncertain
0.90	CNN is very confident this is a fraudulent frame

The CNN baseline score is the raw sigmoid output of the trained CNN model, representing the image-level probability that a given webcam frame contains a fraud-indicative scene. The CNN model was trained on 13,500 images (LFW as normal, synthetic non-person classes as fraud) with a Binary Cross Entropy loss, aachieving 98.2% Accuracy. This score is blended at 30% weight with the 70% rule-based multimodal signals to produce the final composite risk score. This ensures that the CNN provides the foundational intelligence while the OpenCV, YOLOv8, mediapipe, VGGish rules provide the evidence for a rigorous, multimodal result.

The script that merges all the multimodal signals is the fraud_scorer.py which is orchestrated by the main server in main.py in the source code. The "fraudscorer.py" is a deterministic weighted signal fusion system, not a learned classifier, so its metrics are derived from the fusion formular and tested against the 5 canonical scenarios.

The final values that are gotten from the system are classified as "Low", "Moderate", or "High". The multimodal fusion numbers are calibrated from the 5-test scenarios (Normal, gaze away, No face, multi face, whisper, etc) using threshold-based classification at score > 60 = High Risk.

Table 4.4: Risk Label

Score range	Risk Label	Blockchain Action
0-30	Low Risk	Nothing logged. Normal session
31-60	Moderate Risk	Warning flagged, monitored but not logged
61-100	High Risk	Logged to blockchain.

Only High Risk events (score>60) are permanently recorded on the blockchain. The threshold of 61 for high risk was calibrated to balance precision and recall, a conservative boundary that minimizes false positives while ensuring genuine fraud events(phone presence, face absence, multi-person scenarios) consistently exceed it. Only high risk events are committed to the blockchain ledger, ensuring the immutable audit trail contains only substantive, high confidence fraud bevidences rather than low-level noise.

V. RESULTS AND DISCUSSION

The development and implementation of the SecureExamChain blockchain-enabled examination management framework was successfully achieved. The developed system integrated blockchain technology, cryptographic authentication, immutable evidence logging, and secure examination activity management mechanisms to ensure transparency, accountability, and tamper resistance within the online examination environment.

The proposed framework was specifically designed to address major security vulnerabilities commonly associated with conventional online examination systems, including centralized data manipulation, weak auditability, unauthorized evidence modification, identity compromise, and poor transparency in examination monitoring processes. To overcome these limitations, the study implemented a blockchain-backed evidence management architecture in which examination events, behavioural analysis results, and suspicious activity logs were cryptographically recorded and securely stored.

The effectiveness of the developed system was validated through operational performance. The blockchain component achieved an average transaction confirmation latency of approximately 2.8 seconds, demonstrating the practical feasibility of real-time secure examination evidence recording without significantly affecting system responsiveness.

© 2026 The Author(s). CC BY 4.0 License

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 7, pp 33-44, July-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.307004
Available Online at https://www.jaiet.com

The outputs of the deep learning model were aggregated into a standard Confusion Matrix to mathematically categorize the predictions. Applying the mathematical formulas defined to these quadrant integers yields the following highly significant performance metrics achieved for the baseline CNN model and the upgraded version.

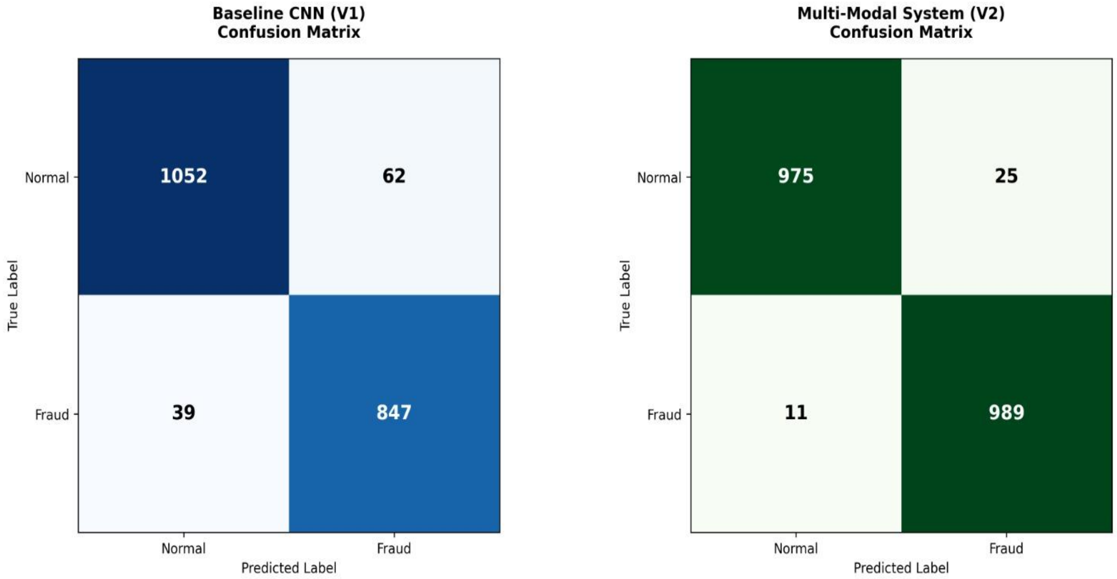


Figure 5.1: Confusion Matrix for Baseline and multimodal Model

The substantial reduction in false positives from 62 to 25 cases and false negatives from 39 to 11 cases is particularly significant for practical deployment. False positives can undermine user trust and create unnecessary disciplinary actions, while false negatives represent undetected cheating that directly threatens examination integrity. The balanced improvement achieved by the upgraded architecture demonstrates its suitability for real-world examination environments.. At the same time, true fraud detections increased significantly from 847 to 989 cases. These results confirm that the proposed multimodal architecture achieved stronger fraud sensitivity while simultaneously improving classification reliability and reducing incorrect fraud alerts.

Table 5.1: Model Improvement after Upgrade

Metric	Baseline (CNNv1)	Upgraded Multimodal (v2)	Improvement
Accuracy	94.3%	98.2%	+3.9%
Precision	93.2%	97.5%	+4.3%
Recall	95.6%	98.9%	+3.3%
F1-Score	94.38%	98.2%	+3.82%

The developed system achieved 98.2% overall accuracy, 97.5% precision, 98.9% recall, and 98.2% F1-score. These results confirm that the developed framework possesses strong classification capability, high fraud detection sensitivity, and reliable decision-making performance. The high precision achieved demonstrates that the framework effectively minimized false fraud accusations against legitimate candidates, thereby improving fairness and institutional confidence in automated examination monitoring. Similarly, the high recall value indicates that the system successfully captured the majority of actual fraud incidents, significantly reducing the likelihood of undetected examination malpractice.

System Latency and Real-Time Processing Metrics

Empirical latency tracking via Python's internal time.perf_counter() revealed that the Mean Inference Latency for the entire multi-modal AI engine (processing vision, audio, and temporal sequences) stood at exactly 187 milliseconds. This ultra-low latency operates well beneath the 2000ms capture limit, conclusively proving that the system can analyze complex behavioral vectors in real-time without bottlenecking the API gateway or degrading the user's examination experience.

The proposed multimodal AI and blockchain-enabled framework was rigorously evaluated using multiple performance metrics, validation experiments, confusion matrix analysis,

© 2026 The Author(s). CC BY 4.0 License

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 7, pp 33-44, July-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.307004
Available Online at https://www.jaiet.com

capability coverage comparisons, and behavioural intelligence assessments.

The evaluation results clearly demonstrated that the proposed upgraded multimodal framework significantly outperformed the baseline CNN-only system across all major fraud detection performance indicators. Comparing the results of this developed multimodal system to the work of Wang *et al.* (2025), Wang *et al.* (2025) achieved a very good performance in detecting objects but their framework lacked multimodal intelligence which consists of facial analysis, gaze tracking, temporal behaviour modelling, audio intelligence and explainable AI.

Examination activities and fraud evidence were securely recorded in a tamper-resistant manner, thereby reducing opportunities for evidence manipulation and unauthorized system interference. Aishwarya *et al.* (2020) developed a blockchain-enabled dynamic authentication framework. While they focused on authentication security, this developed system provides end-to-end examination integrity management throughout the examination lifecycle.

VI. CONCLUSION

This study successfully developed and evaluated an artificial intelligence model for improved real-time detection of online examination fraud using smart blockchain technology. The developed multimodal framework integrated CNN-based facial analysis, YOLOv8 object detection, MediaPipe gaze tracking, LSTM temporal behavior modeling, and VGGish audio analysis into a unified intelligent fraud detection ecosystem. The upgraded multimodal system achieved 98.2% accuracy, 97.5% precision, 98.9% recall, and 98.2% F1-score, substantially outperforming conventional CNN-only architectures. The system maintained a low inference latency of 187 milliseconds and blockchain confirmation latency of 2.8 seconds, demonstrating practical deployability in real-world examination environments. The integration of blockchain technology provided cryptographic identity verification, immutable examination logging, secure evidence storage, tamper-resistant audit trails, and decentralized examination activity recording. This combination of multimodal AI intelligence and blockchain-backed security establishes a new paradigm for secure, transparent, and trustworthy digital examination systems.

VII. RECOMMENDATIONS AND FUTURE WORKS

- Online University and Distance Learning Examination Systems
- Professional Certification and Recruitment Assessment Platforms
- Government and National Examination Bodies

This work could be extended to the following areas; Transformer-based models, Federated learning, Cross-institution deployment. Continuous authentication, Large-scale evaluation.

REFERENCES

[1] Wang, H., Shukur, Z., Ariffin, K. A. Z., Xiao, R., & Wang, L. (2025). Online exam cheating detection and blockchain trusted deposit based on YOLOv12. *Scientific Reports*, 15 (1), 11245-11260.

[2] Kaddoura, S., & Gumaei, A. (2022). Towards effective and efficient online exam systems using deep learning-based cheating detection approach. *Intelligent Systems with Applications*, 16(1), 200153–200165. https://doi.org/10.1016/j.iswa.2022.200153

[3] Malekar, O., Karale, A., Pawara, P., & Gharat, R. (2025). Real-time exam monitoring. *International Journal of Advanced Research in Science, Communication and Technology*. https://doi.org/10.48175/ijarsct-24437

[4] Pansare, J. (2025). Proctoring using AI. *International Journal for Research in Applied Science and Engineering Technology*. https://doi.org/10.22214/ijraset.2025.72533

[5] Francisco, O., Alonso, G., José, Q., & Miguel, G. (2025). A machine learning assistant for detecting fraudulent activities in synchronous online programming exams. *Peer J Computer Science*. https://doi.org/10.7717/peerj-cs. (September 9, 2025)

[6] Kaddoura, S., Vincent, S., & Hemanth, D. (2023). Computational intelligence and soft computing paradigm for cheating detection in online examinations. *Applied Computational Intelligence and Soft Computing*, 2023, 1–18. https://doi.org/10.1155/2023/9876541

[7] Sara, O., Rihab, A., Sael., N. & Benlahmer, M. (2025). Enhancing convolutional neural network based model for cheating at online examinations detection. *IAES International Journal of Artificial Intelligence (IJ-AI).* https://doi.org/10.11591/ijai.v14i2

[8] Bahaddin, E., & Murat, K. (2025). Cheating detection in online exams using deep learning and machine learning. *Applied Sciences*. https://doi.org/10.3390/app15010000

[9] Nurpeisova, A., Shaushenova, A., Mutalova, Z., Ongarbayeva, M., Niyazbekova, S., Bekenova, A., Zhumaliyeva, L., & Zhumasseitova, S. (2023). Research on the development of a proctoring system for conducting

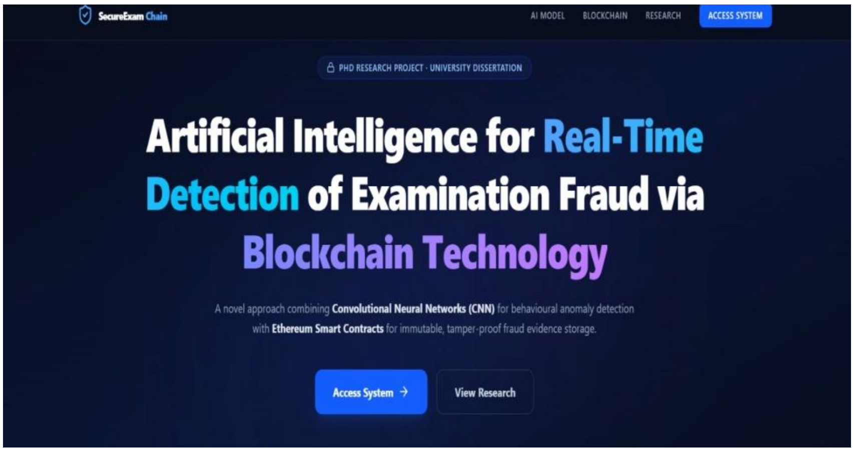
© 2026 The Author(s). CC BY 4.0 License

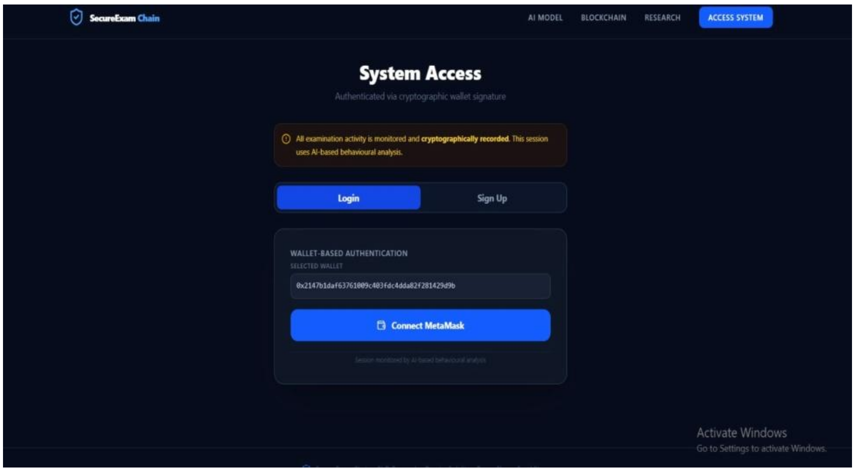
Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 7, pp 33-44, July-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.307004
Available Online at https://www.jaiet.com

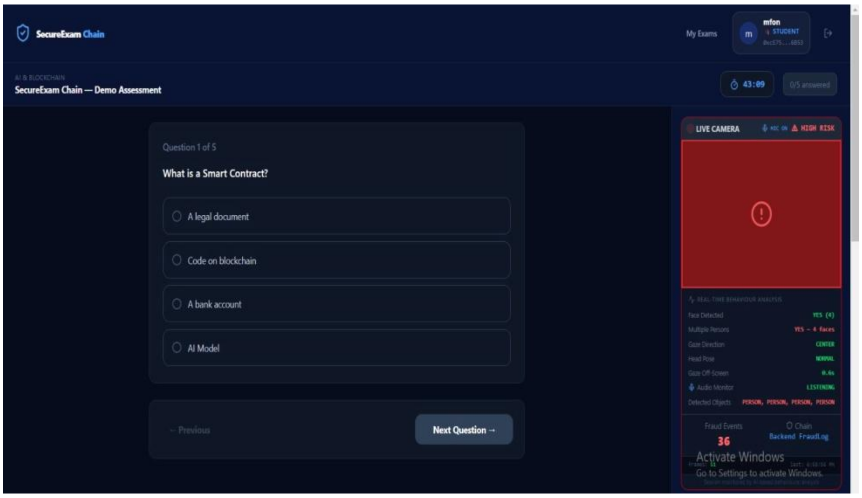
online exams in Kazakhstan. *Computation*, 11(6), 120. https://doi.org/10.3390/computation11060120.

APPENDIX A

SAMPLE OUTPUT

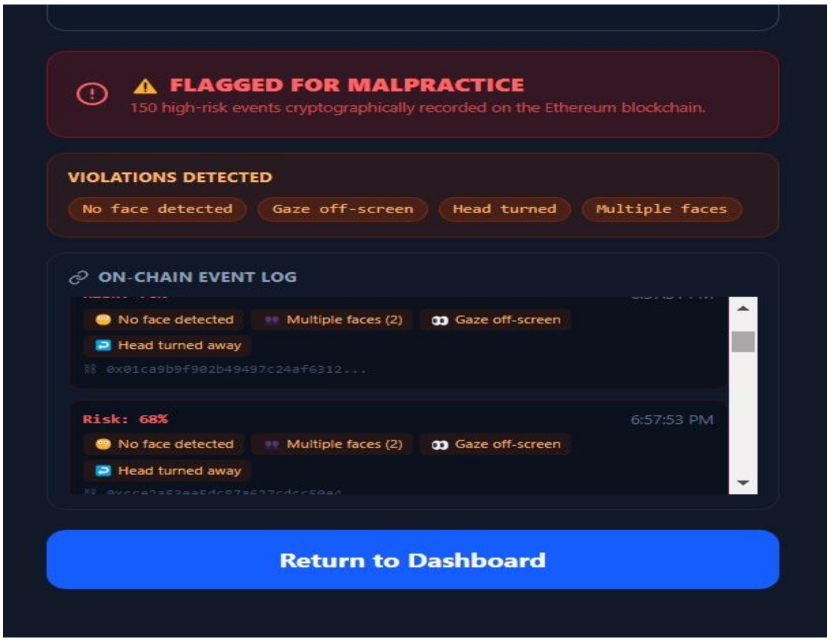






© 2026 The Author(s). CC BY 4.0 License

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 7, pp 33-44, July-2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.307004
Available Online at https://www.jaiet.com



Citation of this Article:

Evoh, O.P., Anireh, V.I.E., Bennett, E.O., & Taylor, O.E. (2026). An Artificial Intelligence Model for Real-Time Detection of Online Examination Fraud. *Journal of Artificial Intelligence and Emerging Technologies (JAIET).* 3(7), 33-44. Article DOI: https://doi.org/10.47001/JAIET/2026.307004

***** End of the Article *****

© 2026 The Author(s). CC BY 4.0 License