International Journal of Computational Science and Engineering Research
ISSN: 3107 - 8605 (Online) , http://www.ijcser.com/
Regular Issue , Vol. 3, Issue. 2 (April– June) , 2026 , Pages: 14 - 26
Received: 21 August 2025 ; *Accepted:* 30 April 2026 ; *Published:* 29 April 2026
https://doi.org/10.63328/IJCSER-V3RI2P3
https://www.youtube.com/watch?v=uA1hmr-3kRk
https://archive.org/details/jsp-ijcser-v3ri2p3
Original Paper : Applied Research – Experimental Research Paper

A Risk-Aware Privacy-Preserving Online Examination System Using Behavioral Anomaly Detection Using Blockchain Technology

Nwosu Ogochukwu Fidelia

Department of Computer and Robotics Education, University of Nigeria, Nigeria; fidelia.nwosu@unn.edu.ng

** Corresponding Author: Nwosu Ogochukwu Fidelia ;* fidelia.nwosu@unn.edu.ng

Abstract: The fast implementation of online examination systems has yielded a dire requirement of proctoring solutions that safeguard and maintain privacy. Standard webcam-based surveillance systems improve detection rates and add serious privacy problems, excessive computing needs and reliance on a well-functioning network presence. In order to overcome these shortcomings, this paper suggests a risk-conscious and privacy-conscious online examination framework that gets rid of constant video surveillance by using the behavioural analysis of browsers, identifying anomalies, and recording the logs using blockchain technology. One of the systems identifies suspicious behaviour patterns like tab switching, inactivity, and patterns of abnormal interactions by a weighted risk-scoring model. Moreover, a lightweight anomaly detection system is incorporated to detect the violations of the regularity of behaviours. Critical events and examination results are safely stored in blockchain logging based on SHA-256 in order to guarantee data integrity and non-repudiation. Experimental outcomes show that the proposed system is highly accurate in detecting and has low latency without compromising user privacy. The structure offers an efficient, scalable and technically sound system to the current web-based test setting.

Keywords: Online Examination, Privacy-preserving Proctoring, Behavioral Anomaly Detection, Blockchain, SHA-256.

1. Introduction

The high rate of expansion of digital education platforms has greatly enhanced the online examination system in learning institutions and certification agencies. Although these systems are flexible, scalable, and accessible, they also create serious issues of upholding academic integrity. The issue of ensuring that candidates do not cheat in remote tests is still a big challenge since physical supervision will not be available. The traditional online proctoring involves constant web cameras, audio, and screen capture, whereby the activities are recorded and then analyzed to identify suspicious behaviors. Despite the fact that these methods provide better detection capability, they have some serious concerns associated with invasion of privacy, high computational cost, and reliance on a stable network infrastructure. Additionally, the constant video-based surveillance might not be possible in low resources settings and could adversely affect user acceptance because of the ethical implications [1],[2]. To overcome these restrictions, current studies have looked at non-invasive and privacy-friendly alternatives founded on system-level constraints and browser activity monitoring. Nevertheless, these strategies do not have clever decision-making processes and cannot offer good assurances of data integrity. Besides that, the majority of the current systems are based on centralized storage, which exposes the examination logs and results to manipulation, unauthorized alteration, and transparency deficiency [2],[3]. This paper presents a risk conscious privacy-sensitive online examination system that removes the concept of constant monitoring of webcams in favor of behavioral, anomaly, and blockchain-based secure logging. The system logs the candidate interactions like tab switching, time of inactivity, and limited command utilization and scores them according to a weighted risk-scoring model. An anomaly detection mechanism is introduced to detect the abnormality of the behavioral pattern in real time and is lightweight. To provide the integrity and non-repudiation of examination records, all the critical events are safely stored with a blockchain layer combined with a hash message-digest algorithm (SHA-256-cryptographic hashing) [4],[5]. The suggested framework attempts to provide a balance between security, privacy, and system efficiency and offers a scalable solution that can be applicable in contemporary examination environments

Jack Sparrow Publishers © 2026, IJCSER, All Rights Reserved
www.jacksparrowpublishers.com

ISSN: 3107 - 8605 (Online) , http://www.ijcser.com/ , Vol. 3, Issue 2 , 2026 , https://doi.org/10.63328/IJCSER-V3RI2P3

online. The key contributions of the same work are as follows: A non-video-monitored privacy-preserving proctoring system. A weighted behavioral risk-scoring model of real-time suspicious activity detection. An anomaly detection system that is lightweight and used to detect abnormal candidate behavior. Secure logging system with a blockchain based system guaranteeing tamper proof and audit records. A scalable and low-latency architecture that can be deployed on large scale. The rest of the paper will be structured as follows: Section II is the definition of problem statement, Section III is related work, Section IV is the proposed framework, Section V is the methodology, Section VI is mathematical models and the algorithm design, Section VII is the discussion of results and performance evaluation, and Section IX is the conclusion of the paper.

2. Research Methodology

The growing use of online examination systems has presented a major challenge of how academic integrity can be guaranteed in remote and uncontrolled conditions. The old proctoring techniques that rely on physical monitoring cannot be used in the virtual environment and as a result, automated monitoring solutions have been implemented. Nonetheless, the available methods have a number of vital flaws. Proctoring systems based on webcams are effective in the capture of the visual evidence but have severe issues connected with the invasion of privacy, great demands of bandwidth, and reliance on hardware. Nonstop video surveillance can be viewed as intrusive to the applicants and cannot be practiced in areas where the internet is scarce or where the devices are low-budget. Also these systems add to the computational overhead and they are not scalable to large user groups.

Conversely, lightweight browser-based monitoring systems are concentrated on monitoring activities like switching of tabs, copy-paste attempts and fullscreen violations. Although these techniques are less invasive, they do not provide analysis of intelligent behaviour and automated decision making which cannot detect more subtle or complex cheating patterns. In addition, such systems are usually based on centralized storage systems which can be easily tampered with, have the ability to be modified by unauthorized persons, and lack transparency, thus decreasing confidence in the process of examination. Lack of integrated systems that use privacy preservation, behavioral analysis, and secure data storage is another crucial weakness of existing systems. Most of the solutions handle these aspects separately, which leads to systems that are either secure yet intrusive, or privacy-friendly yet weak in the detection ability. Thus, it is necessary to have a privacy-friendly, intelligent, and secure online test model that is capable of By candidate interaction patterns rather than continuous video monitoring, detect suspicious behavior. Carry out automated and real-time of decision making by means of risk evaluation. Detect anomalous behavior by using anomaly detection methods. Ensuring that examination records are tamper proofed by secure and immutable logging.

3. Related Work

The issue of proctoring online exams and making them academically sound has been extensively researched, and multiple methods of proctoring have been developed and are based on the monitoring of browsers, artificial intelligence, and blockchain technologies. The three strategies are designed to identify cheating activities, create a level of fairness and uphold the integrity of the evaluation systems.

3.1. Proctoring Systems based on a browser

Early proctoring systems over the Internet used mainly browser-based monitoring methods to limit and monitor activities of users throughout exams [2],[3]. Such systems identify activities like switching tabs, copy-pasting, violation of fullscreen and time of inactivity. These solutions are not that bulky, simple to install, and do not demand extra hardware. They can however only do so much in tracking down more advanced forms of cheating like the use of external gadgets or collusion. As well, these systems do not have intelligent decision-making mechanisms, which means that the false positives are usually high or undetected violations.

3.2. Proctoring, AI-based and vision-based

The recent research has involved the use of artificial intelligence and computer vision to proctor in order to surmount the shortcomings of browser-only monitoring. Such systems utilize face recognition, gaze tracking and object detection models to detect suspicious actions like impersonation, the existence of more than one person, or the utilization of unauthorized devices. Although these methods have notable contributions to the accuracy of detection, it also comes with a number of challenges, such as privacy problems, the high computation cost, and the reliance on the constant network connection. Constant webcam surveillance can also cause discomfort and ethical issues to the user and restrict their widespread use [15],[16].

3.3. Proctoring Approaches that Preserve Privacy

Other recent studies have been aimed at coming up with privacy preserving proctoring systems that minimize or do away with the use of constant video surveillance. These methods are based on behavioral cues, including interaction patterns, use of keyboard, and browser activity to assume suspicious activity. Though these approaches enhance usability and lessen the need of infrastructure, they do not have well-defined

Jack Sparrow Publishers © 2026, IJCSER , All Rights Reserved
www.jacksparrowpublishers.com

ISSN: 3107 - 8605 (Online) , http://www.ijcser.com/ , Vol. 3, Issue 2 , 2026 , https://doi.org/10.63328/IJCSER-V3RI2P3

analytical models and cannot offer high assurances of the accuracy of the detection and reliability of the system.

3.4. Examination Systems Based on Blockchain

The technology of blockchain has been actively studied in online examination systems to provide data integrity, transparency, and non-repudiation. The blockchain-based solutions ensure that examination records, logs, and results are not altered by unauthorized parties by storing them in a decentralized ledger through cryptographic hash algorithms like SHA-256, which ensures the provision of an audit trail that can never be tampered with. Nevertheless, the vast majority of the solutions available at the moment are more of secure storage and lack the mechanisms of real-time detection or intelligent monitoring [4]-[6].

3.5. Research Gap

Based on the discussion above, it can be seen that the current solutions focus on a single area of online examination security, be it monitoring, privacy or data integrity, and do not appear to have a cohesive framework that unites all these areas together. Browser based systems are lightweight and lack intelligence, AI based systems are precise but intrusive, and blockchain based systems are integrity assured and they do not support real-time detection.

3.6. Motivation of Proposed Work

In order to fill these gaps, this paper contains a risk-sensitive privacy-sensitive online examination framework that integrates: Non-Intrusive detection Behavioral monitoring. Risk-based automated decision making scoring. Abnormal patterns of anomaly detection. Logging on blockchain to ensure the safety and immutability of records. This combined scheme is expected to provide a balance between accuracy and privacy as well as security, which is why it can be applied to the scalable and real deployment.

4. Proposed Framework

The proposed system presents a risk-conscious and privacy-conscious online exam system that combines a behavioral surveillance system, anomaly detection system, and blockchain-based secure logging. In contrast to the traditional proctoring frameworks, which are based on the 24-hour webcam monitoring, the given framework presupposes the non-invasive monitoring of interactions between the user and the intelligent analysis of the data, which will help to identify any suspicious actions. The framework is built as a multi-layered framework comprising of the following major components:

4.1. Monitoring Layer on the Client-Side

The client-side monitoring layer has the responsibility of capturing the user interaction events in the course of the examination session. This layer works under browser and it has a minimum intrusion and gathers pertinent behavioral information. The activities that are followed include: Tab switching and change of window focus.

• Fullscreen exit attempts Copy-pasting and right-clicks: restrictions can be copied and pasted.

• Keyboard shortcut usage

• Inactivity duration tracking All the events detected are time-stamped and transferred to the backend processing modules to be processed further.

4.2. Behavioural Analysis and Risk Engine

The behavioral analysis module processes incoming event streams and evaluates them using a weighted risk-scoring mechanism. Each event is assigned a severity weight based on its potential impact on exam integrity.

- Low-risk events: short inactivity, minor delays
- Medium-risk events: occasional tab switching
- High-risk events: repeated violations, multiple suspicious actions

The cumulative risk score is continuously updated throughout the examination session. Based on predefined thresholds, the system classifies candidate behavior into:

- Normal
- Suspicious
- High Risk

This enables automated and real-time decision making, reducing dependency on manual supervision.

4.3. Detection of Anomaly Detection Module

The system is optimized with a light-weight behavioral anomaly detection module in order to increase its detection ability. This module involves a comparison of the behavior of the candidate with the normal behavioral patterns. The relevant parameters that were analyzed are:

- Frequency of tab switching.
- Duration of inactivity

Towards input consistency and pattern of interaction. The major aberrations of the baseline behavior would be reported as anomalies and sent to the risk engine to undergo further analysis. This module enhances the ability to detect cheating patterns which are subtle and non-obvious and may not be detected using rule-based monitoring.

4.4. Security Layer of Blockchain

In order to guarantee the integrity and security of the examination data, the framework

Jack Sparrow Publishers © 2026, IJCSER , All Rights Reserved
www.jacksparrowpublishers.com

ISSN: 3107 - 8605 (Online) , http://www.ijcser.com/ , Vol. 3, Issue 2 , 2026 , https://doi.org/10.63328/IJCSER-V3RI2P3

incorporates a blockchain based secure logging system. Rather than keeping the raw data, such critical events as violation records, risk scores, and final results are transformed into hashes with the help of the cryptographic algorithm of SHA-256.

The chain has blocks which include:

- Event data
- Timestamp
- Previous block hash
- Current hash This structure ensures:
- Data immutability
- Tamper detection
- Transparent audit trails

Any effort to alter existing storage records will create a disintegration of the hash values and any form of unauthorized impact can be readily identified.

4.5. Basic and Administrative Structure

The last layer offers a monitoring, reporting as well as administrative controlled interface. According to the analysis of risks:

- Candidates can get warning against suspicious behavior.
- High risk applicants can be identified or rejected.
- Final results and logs are safely stored and examined.
- Moreover, the candidate can be notified automatically about the exams and results. The administrators will be able to make decisions based on the detailed logs, level of severity and the audit trails.

4.6. Overall Framework Description

The suggested system integrates behavioral monitoring, smart analysis, and safe storage of data into one system which is non-invasive. The system balances privacy, accuracy and scalability by removing the constant webcam addiction and introducing the risk conscious decision process.

4.7. Face Verification Module

In order to achieve a high level of candidate authentication the system will have a light weight face verification module which will be used at critical points of the examination process. This module conducts periodic or event-based verification rather than using continuous webcam-monitoring as the case is in conventional proctoring systems which are in place to ensure user privacy. Face verification is activated when a candidate logs in, and is also activated optionally when examining. It takes a picture of the candidate and compares it to the registered reference image through an embedding model based on deep learning. A similarity score is generated based on a distance measure and the identity is confirmed when the value lies within an acceptable range. In case a mismatch is observed, the system notifies the event as a potential violation and sends it to the risk evaluation module. The cumulative risk score is based on repeated mismatches and can result in automatic termination of examination. This will provide a balance of security and privacy as identity is verified without constant monitoring.

5. System Architecture

The suggested system architecture will be a pipeline based on processes in which candidate interactions will be captured, analyzed, evaluated, and stored safely. In contrast to the modular descriptions, such architecture focuses on the flow of data and decision-making in various components of the system in a sequence. The architecture is done according to a four stage workflow:

5.1. Stage of Acquiring the input

The steps will be initiating the process where the candidate will be invited to the examination platform via web-based interface. In the process, all the interactions involving the user are recorded in real time.
The inputs that have been captured are:

- Any switching of tabs, switching focus.
- Pattern of user interaction (keyboard and the use of the mouse).
- Duration of session activity (inactivity, response time)

These are the inputs that serve as the main source of data on analysis.

5.2. Processing Stage of behaviours

At this level, the events that are captured are converted into structured data of behaviours. The system takes the raw interaction logs as inputs and derives meaningful features which include:

- Incidences of suspicious behavior.
- Interaction time periods.
- Stability in user-behavior.

This change can make the system turn simple event logs into behavioral patterns that could be analyzed to make the basis of intelligent monitoring.

5.3. Evaluation of the Decision

The processed behavioural data is then measured with the help of two complementary mechanisms:

Risk Scoring: The cumulative risk score is a sum of the individual risk events identified with predetermined weights attached to every detected event. This enables the system to measure the degree of behaviours of the candidates.

Jack Sparrow Publishers © 2026, IJCSER , All Rights Reserved
www.jacksparrowpublishers.com

ISSN: 3107 - 8605 (Online) , http://www.ijcser.com/ , Vol. 3, Issue 2 , 2026 , https://doi.org/10.63328/IJCSER-V3RI2P3

Anomaly Detection: The system will match real-time behaviours with baseline patterns that are supposed to be. Any major deviations are perceived as anomaly which can be taken to mean wrongdoing.

- According to the aggregate assessment:
- Low score -Normal behavior.
- Medium score- Suspicious behavior. Score
- high - Malicious behavior.

This step will guarantee real-time and automated decision making.

5.4. Secure Storage Stage

After making the decisions, the critical events and results are logged safely with the help of blockchain-based logging mechanism.

Each event is:

- Turned into a hash with the help of SHA-256.
- Connected with the former block.
- Stored as a part of an unchangeable chain.

This ensures:

- Data integrity
- Tamper resistance
- Transparent auditing

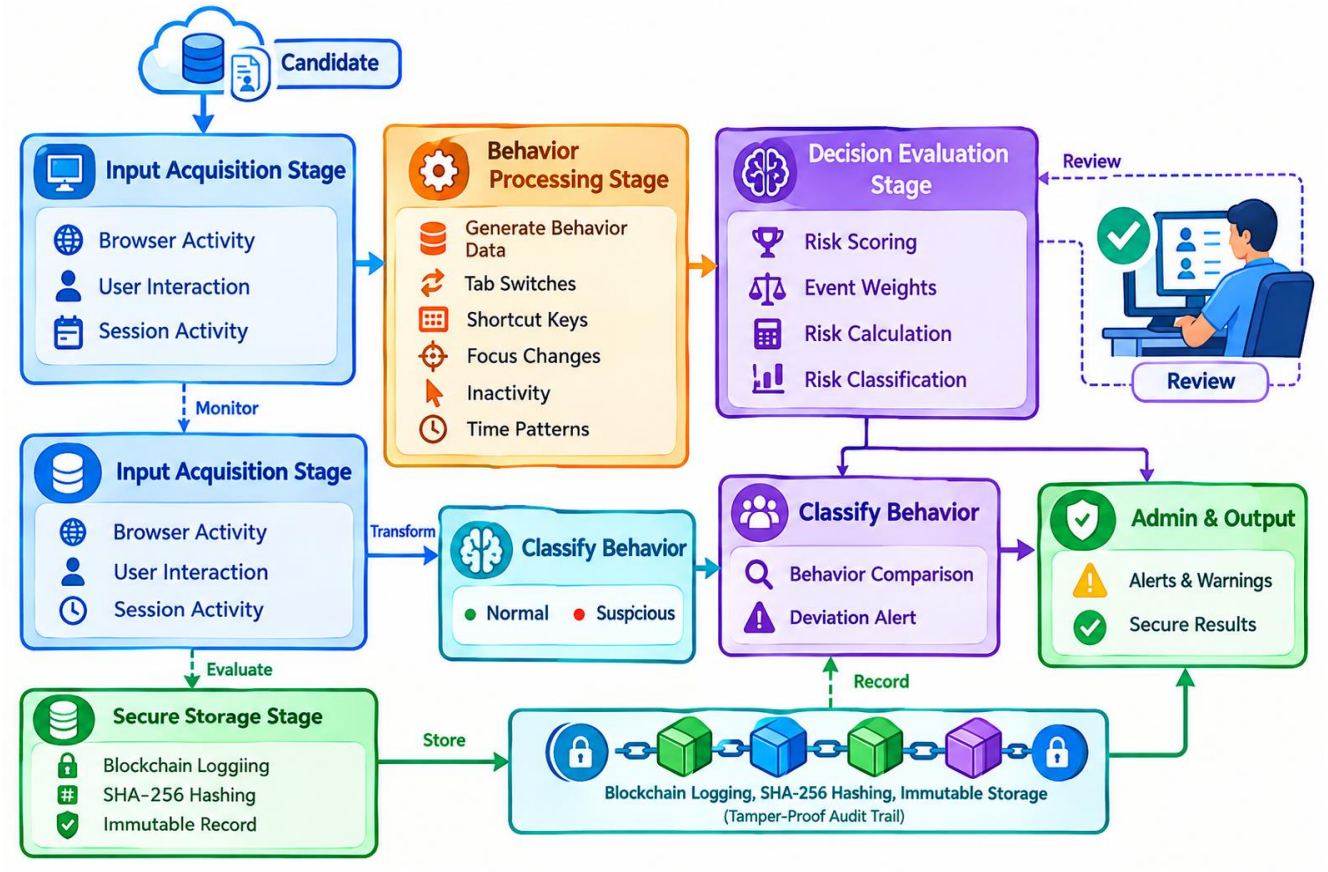


Figure 1. Architecture of the proposed privacy-preserving online examination framework.

5.5. Output and Administrative Control

The output of the last stage will be in the form of:

- Alerts and warnings
- Candidate status classification
- Secure examination results

Blockchain-supported records can be used to analyze candidates and verify their behaviours as well as review logs.

5.6. End-to-End Workflow Perspective

The architecture guarantees the uninterrupted flow of events capture to secure decision storage, which makes it

possible to have the privacy-preserving but efficient monitoring system. The system balances the accuracy, efficiency, and privacy of the user by concentrating on the behavioral cues rather than the intrusive approach.

Jack Sparrow Publishers © 2026, IJCSER , All Rights Reserved
www.jacksparrowpublishers.com

ISSN: 3107 - 8605 (Online) , http://www.ijcser.com/ , Vol. 3, Issue 2 , 2026 , https://doi.org/10.63328/IJCSER-V3RI2P3

6. Methodology and Algorithmic Implementation

The suggested framework integrates event monitoring on the browser, behavioral risk modelling, anomaly detection and blockchain-supported secure logging to offer privacy-enabling online examination monitoring. The methodology will convert unrefined interaction events into risk-conscious choices and inaccessible records. The general pipeline is comprised of five steps namely event acquisition, feature construction, risk evaluation, anomaly analysis, decision generation and secure storage.

6.1. Event Acquisition and Preprocessing

The system is able to capture the browser level activities continuously during the examination session without necessarily reporting them via continuous use of webcams. Some of the observed events are tab switching, loss of browser focus, fullscreen exit attempts, key shortcut, copy-pasting, right-click triggers and idle time. All events are stored in the form of a structured tuple:

$$e_i = (t_i, type_i, value_i)$$

and t_i denotes the time of the event, $type_i$ denotes the type of event, and $value_i$ denotes the magnitude or number of times an event has taken place. Raw events are normalized into session behavioral features like: to minimize noise and allow the analysis to proceed efficiently, including:

- table number of tab switches
- total inactive duration, frequency of limited orders
- average response interval
- focus-loss count.

The behavioural vector of the candidate is made up of these features:

$$B = [b_1, b_2, b_3, \dots, b_n]$$

and where b_j rep is a normalized measure of behavioural measure obtained during the session.

6.2. Weighted Behavioural Risk Model

The system employs a weighted cumulative risk model in order to measure the level of suspiciousness of the behaviours. All the types of events have the predetermined severity weight based on their possible effects on the integrity of the examinations. The risk score is summed up to obtain the cumulative risk score:

$$R = \sum_{i=1}^{m} w_i \, x_i$$

where x_i is the indicator of the frequency or occurrence of the i^{th} suspicious event and w_i is the severity weight. As an example, one full screen exit can have a smaller weight than a series of switching tabs, and several limited command attempts can be used to add a greater penalty. Depending on the threshold values T_1 and T_2, candidate behaviours is rated as:

$$\text{Normal, if } R < T_1$$
$$\text{Suspicious, if } T_1 \le R < T_2$$
$$\text{High Risk, if } R \ge T_2$$

This model offers a basic and yet effective way of risk assessment in real time and aids in the same way automated decision making.

6.3. Detection of Anomaly of Behaviour

Although risk scoring, which is based on rules, can identify the event of explicit suspiciousness, the subtle irregularity may go undetected. To deal with this, the proposed framework has an anomaly detection phase which is lightweight and compares the present behavior vector with a desired baseline pattern. Where $B^{(c)}$ refers to the current candidate behavioral vector and $B^{(n)}$ refers to the normal behavioral baseline. The deviation score is :

$$A = \| B^{(c)} - B^{(n)} \|$$

where $\|\cdot\|$represents a distance metric such as Euclidean distance or absolute deviation aggregation.
If the deviation exceeds a predefined threshold δ, the behaviours is marked as anomalous:

$$A > \delta \Rightarrow \text{Anomaly Detected}$$

This anomaly score is combined with the weighted risk score to enhance reliability in the detection of anomaly. This way the system will be able to detect the direct violations as well as the concealed behavioural inconsistencies.

6.4. Fusion of Decisions and Decision Severity

The rule-based risk score is added to the anomaly score to come up with the final decision. Where R means the cumulative risk score and A means the anomaly score. A composite decision is a function that is defined as follows:

$$D = \alpha R + \beta A$$

In which α and β are weighting factors that regulate the proportional effects of explicit event violations and behavioural abnormalities. The values of D is were plotted

Jack Sparrow Publishers © 2026, IJCSER , All Rights Reserved
www.jacksparrowpublishers.com

ISSN: 3107 - 8605 (Online) , http://www.ijcser.com/ , Vol. 3, Issue 2 , 2026 , https://doi.org/10.63328/IJCSER-V3RI2P3

against one of the following categories:

Low Severity: the session is not interrupted.

Medium Severity: warning is generated and recorded.

High Severity: candidate is flagged and this session can be ended.

The advantage of this fusion approach is that it enhances the robustness of the monitoring approach by not relying excessively on one monitoring signal.

6.5. Blockchain-Based Secure Logging

In order to ensure that examination records are integrity guaranteed and auditable, all the essential outputs of the decision engine are stored in a hash chain inspired by blockchain [11],[12]. To compute block hash of each important event final result record M k, the system calculates:

$$H_k = \text{SHA-256}(H_{k-1} \parallel M_k \parallel t_k)$$

H_{k-1} is the hash of the previous block, M_k is the current event data, and t_k is the time. This chained design makes sure that any alteration of a previous record alters all the following hashes exposing any attempt towards tampering.

The stored payload may include:

- candidate identifier,
- event type,
- computed risk score,
- anomaly flag,
- decision label,
- timestamp.

This is done to guarantee immutability, non-repudiation as well as clear verification of examination logs.

6.6. Secure Credential Protection

Besides examination integrity, the framework provides the user credentials with salted hashing.. For a user password P and random salt S, the stored value is:

$$C = \text{SHA-256}(P \parallel S)$$

To prevent rainbow table and brute-force attacks on stored credentials, this technique can be used to make sure that the same passwords do not generate the same stored hash.

6.7. Face Verification Model

A deep learning based embedding model is used to implement the face verification module [16] which projects facial images into a high dimension feature space. Let F(r) be the reference embedding and F(c) be the current captured embedding. The distance metric is used to calculate the similarity between the two:

$$D = ||F(r) - F(c)||$$

In the event that distance D is smaller than a threshold τ which has been set, identity is checked. Otherwise, it is categorized in the system as a mismatch. This method makes it possible to verify the identity efficiently and accurately in a range of conditions like lighting and face positioning.

The model will be used to make sure that it is only the authorized candidate who proceeds with the examination and any deviation will lead to the necessary actions. Face verification outcome is incorporated in the total risk scoring system. Several mismatches raise the risk score and add to the ultimate decision, which ensures a solid detection of impersonation attempts.

6.8. Algorithmic Implementation

The framework is practically implemented into four main algorithms, which are the event monitoring, risk evaluation, anomaly detection [17], and secure block generation.

Algorithm 1: Event Monitoring and Feature Extraction

Input: Browser activity stream

Output: Behavioural feature vector B

Step - 1 : Start examination session.

Step - 2 : Initialize counters for tab switches, focus loss, inactivity, and restricted actions.

Step - 3 : For each browser event:

(a). capture timestamp and event type,

(b). update the corresponding counter,

(c). append event to session log.

Step - 4 : At fixed intervals, normalize counters into behavioural features.

Step - 5 : Construct behaviours vector B.

Step - 6 : Forward B to the risk and anomaly modules.

Algorithm 2: Weighted Risk Score Computation

Input: Event counts $x_1, x_2, \ldots, x_m$

Output: Risk score R, severity label

Step - 1 : Initialize $R = 0$.

Step - 2 : For each event type i:

(a). retrieve weight w_i,

(b). compute contribution $w_i x_i$,

(c). update $R = R + w_i x_i$.

Step - 3 : Compare $R$with thresholds $T_1$and T_2.

Step - 4 : Assign label:

(a). Normal if $R < T_1$,

(b). Suspicious if $T_1 \leq R < T_2$,

(c). High Risk if $R \geq T_2$.

Step - 5 : Forward the output to the decision layer.

Jack Sparrow Publishers © 2026, IJCSER , All Rights Reserved
www.jacksparrowpublishers.com

ISSN: 3107 - 8605 (Online) , http://www.ijcser.com/ , Vol. 3, Issue 2 , 2026 , https://doi.org/10.63328/IJCSER-V3RI2P3

Algorithm 3: Behavioural Anomaly Detection [15]
Input: Current behaviours vector $B^{(c)}$, baseline vector $B^{(n)}$
Output: Anomaly score A, anomaly flag.

Step - 1 : Compute deviation:
$A = \| B^{(c)} - B^{(n)} \|$
Step - 2 : Compare $A$with threshold δ.
Step - 3 : If $A > \delta$, set anomaly flag to True.
Step - 4 : Else set anomaly flag to False.
Step - 5 : Send anomaly result to the fusion module.

Algorithm 4: Secure Log Block Generation
Input: Event payload M_k, previous hash H_{k-1}, timestamp t_k
Output: Current block hash H_k

Step - 1 : Concatenate H_{k-1}, M_k, and t_k.
Step - 2 : Apply SHA-256 hashing:
$H_k = \text{SHA-256}(H_{k-1} \| M_k \| t_k)$
Step - 3 : Store $H_k$with current record metadata.
Step - 4 : Link the block to the next generated block.
Step - 5 : Preserve the chain for later audit verification.

6.9. Implementation Discussion

The machine code implementation is lightweight and appropriate in web-based examination set-up. The framework is not based on continuous video analysis and, therefore, has less computation overhead and is scalable.

Meanwhile, the weighted scoring, analysis of anomalies, and logging supported by blockchain enhance the detection functionality and integrity of the records. This renders the framework technically sound, privacy conscious and apt to deploy secure online examination.

7. Analysis of Results and Performance

The effectiveness of the suggested privacy-saving online examination system is assessed regarding its performance on the detection of suspicious activity, real-time reaction, and integrity of secure records.

The following section gives the analysis of the important performance factors such as behavioural risk assessment, detection accuracy, system latency, and realistic system outputs. The findings show that risk-based scoring, anomaly detection, and blockchain-based logging integration can help to ensure the efficient monitoring with the maintenance of the privacy of users.

7.1. Behavioral Risk Evaluation

The efficiency of the suggested system is also estimated according to the capacity to assess the conduct of the candidates and calculate the cumulative risk score in the process of the examination session dynamically. Fig. 2 displays the variation of risk score with regards to the detected events.

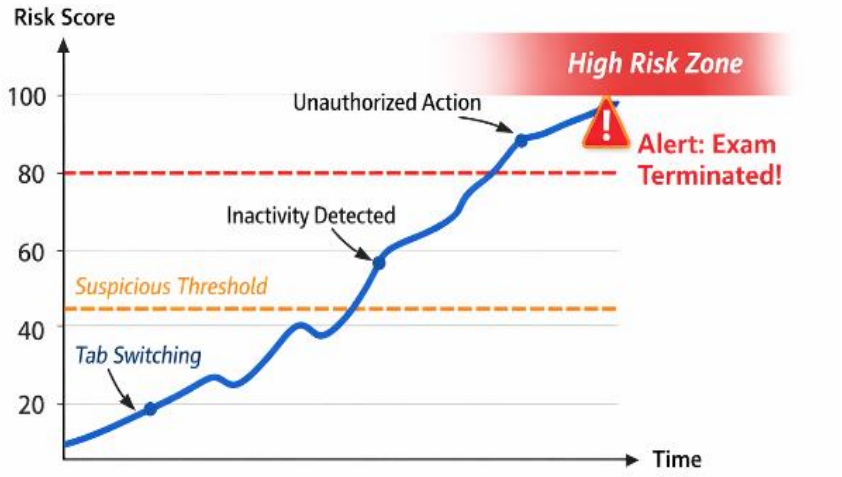


Figure 2. Risk score variation during an examination session.

The risk score is also raised when suspicious activities like tab switching, idleness and unauthorized activities are identified. Once the score goes past predetermined level, the system categorizes the candidate behaviour as suspicious or high risk. This shows how the risk model is able to assess behavioral patterns at any given moment.

7.2. Detection Performance Analysis

Risk scoring and anomaly detection are used to increase the detection capability of the proposed system. In Fig. 3 a comparative study is made with the traditional methods of monitoring. The graph shows that the proposed system is more efficient than the traditional methods of monitoring since it implements behavioural risks analysis and anomaly detection systems.

Jack Sparrow Publishers © 2026, IJCSER , All Rights Reserved
www.jacksparrowpublishers.com

ISSN: 3107 - 8605 (Online) , http://www.ijcser.com/ , Vol. 3, Issue 2 , 2026 , https://doi.org/10.63328/IJCSER-V3RI2P3

Table.1 Detection Accuracy Comparison of Different Proctoring Systems

METHOD	Detection accuracy (%)	Privacy Level	Computational Cost
Traditional Browser Monitoring	78	Medium	Low
Basic Proctoring System	85	Medium	Medium
Webcam-Based Proctoring	91	Low	High
Proposed System	94	High	Medium

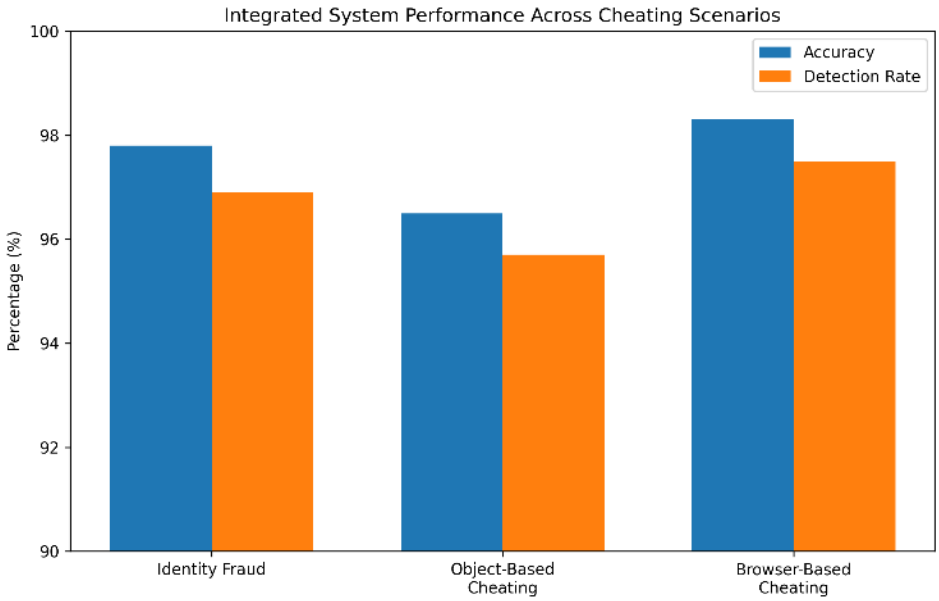


Figure 3. Detection accuracy comparison of different proctoring approaches.

The system proposed has greater accuracy of detection than the traditional methods and also has greater degree of privacy and reasonable computational cost.

7.3. System Output and Validation

The real-world use of the developed system proves that it is capable of identifying suspicious activity and delivering the results that can be acted upon.

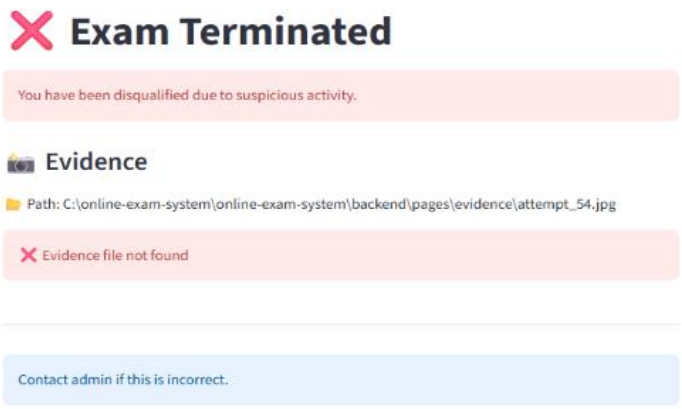


Figure 4. Automatic termination of examination upon detection of high-risk behavior.

The fig. 4 shows that the system automatically ends the examination once the cumulative risk score gets out of the predefined threshold. This supports the usefulness of real time monitoring and automatic decision-making systems in deterring malpractice.

Jack Sparrow Publishers © 2026, IJCSER , All Rights Reserved
www.jacksparrowpublishers.com

ISSN: 3107 - 8605 (Online) , http://www.ijcser.com/ , Vol. 3, Issue 2 , 2026 , https://doi.org/10.63328/IJCSER-V3RI2P3

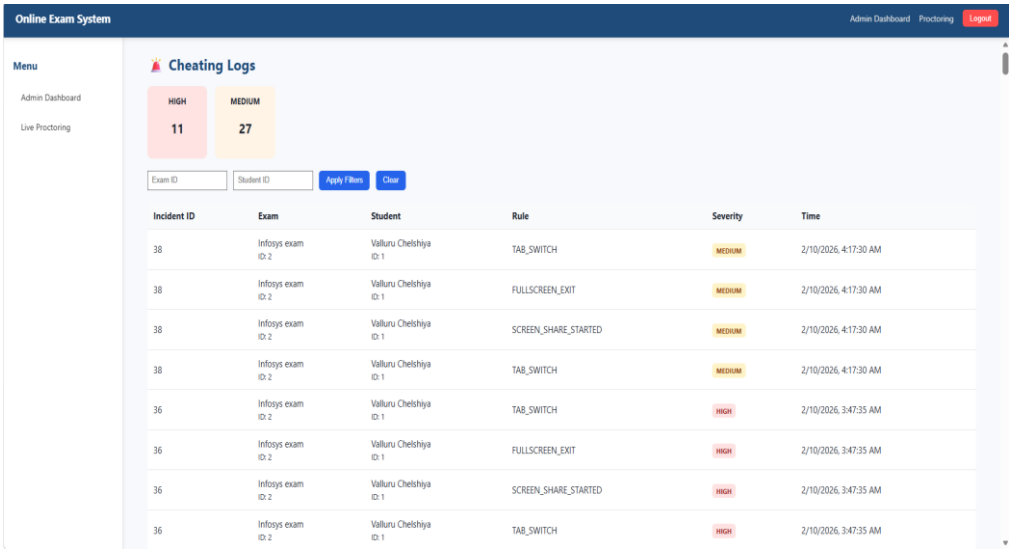


Figure 5. Administrative dashboard displaying candidate activity logs and violation records.

The fig 5. Shows the administrative interface gives a summary of the activity of the candidate, the violations identified, the level of severity, and the final result. This allows effective control and checking of integrity of examinations.

Incident ID	Exam	Student	Rule	Severity	Time	Result
1	INFOSYS	VALLURU CHELSHIYA ID: 1	TAB_SWTICH	MEDIUM	2/10/2026, 4:17:30PM	PASS
2	INFOSYS	SHANIVARAPU CHARAN ID: 2	NIL	LOW	2/10/2026, 4.30:00PM	PASS
3	INFOSYS	ADIL JAIWANT ID: 3	MOBILE DETECTED	HIGH	2/10/2026, 4:15:30PM	FAIL
4	INFOSYS	SAI PRASANNA ID:4	FULL_SCREEN EXIT	MEDIUM	2/10/2026, 4.05.15PM	PASS
5	INFOSYS	HEMANTH ID:5	SCREEN_SHARED	HIGH	2/10/2026, 4.10.30PM	FAIL

Figure 6. List of Unauthorized or Terminated access user detection during the Exam Session

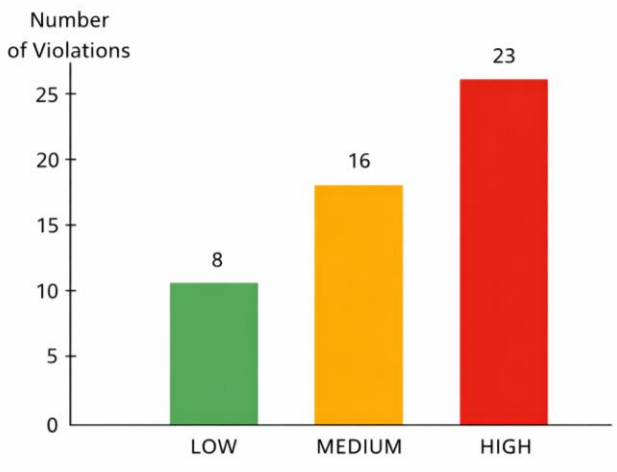


Figure 7. Severity classification of detected violations during the examination session.

List of Unauthorized or terminated access user detection in the Exam Session .The identified examination cases recorded by the system and the information like identification of the exam, student, the type of violation, the level of severity, time of occurrence, and the final outcome.

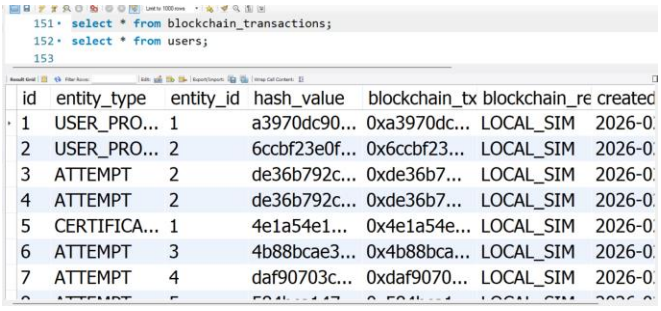


Figure 8. Blockchain transaction records with hashed values for secure and immutable storage.

Figure 8. Records of transaction using the blockchain with the use of hashed values to store data safely and impartially. The fig 8. shows the blockchain transaction logs created by the system, every element of which is associated with an event that is stored, i. e. user activity, attempt data, or certification details.

Jack Sparrow Publishers © 2026, IJCSER , All Rights Reserved
www.jacksparrowpublishers.com

ISSN: 3107 - 8605 (Online) , http://www.ijcser.com/ , Vol. 3, Issue 2 , 2026 , https://doi.org/10.63328/IJCSER-V3RI2P3

All records have a distinct hash value and blockchain transaction identifiers which make them safe and impossible to tamper with. SHA-256 hashing and chained records are used to ensure that the information is intact, and any alteration on the information stored would lead to a discrepancy in the hash chain. This shows the ability of the system to have unalterable and auditable logs to be used during audits and validation.

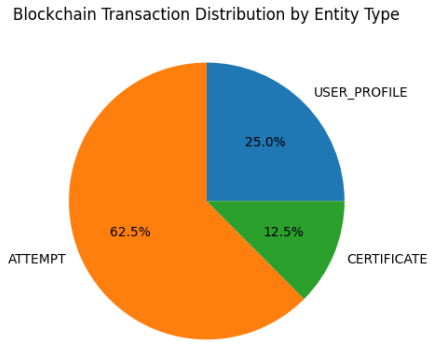


Figure 9. Breakdown of blockchain transactions by the type of entities.

The pie chart shows how the blockchain transaction records are distributed according to the types of entities that are stored in the system.

The transactions are associated with a particular event like user registration, attempt at examination or generation of the certificate. As it can be seen, most of the transactions are also linked with attempts to examine, since every candidate interaction creates a number of records. This distribution emphasizes the active character of the blockchain logging system, in which all important events are safely stored. The existence of the various entity types reflects how the system can be used to store a wide variety of data and maintain integrity by using cryptographic hashing.

The figure 10. shows the face verification and monitoring component performance in various examination situations. First, the candidate has his or her facial image taken and registered prior to the examination. In the test, the system conducts real-time identity checks where the candidate is successfully checked in the normal course of things. Nonetheless, in the case of face being covered or failing to match the stored reference, the system identifies discrepancy and sends alerts. Cumulative risk score is based on repeated violations and results in the automatic termination of examination. These findings demonstrate the strength of the suggested system in impersonation prevention and integrity of examinations.

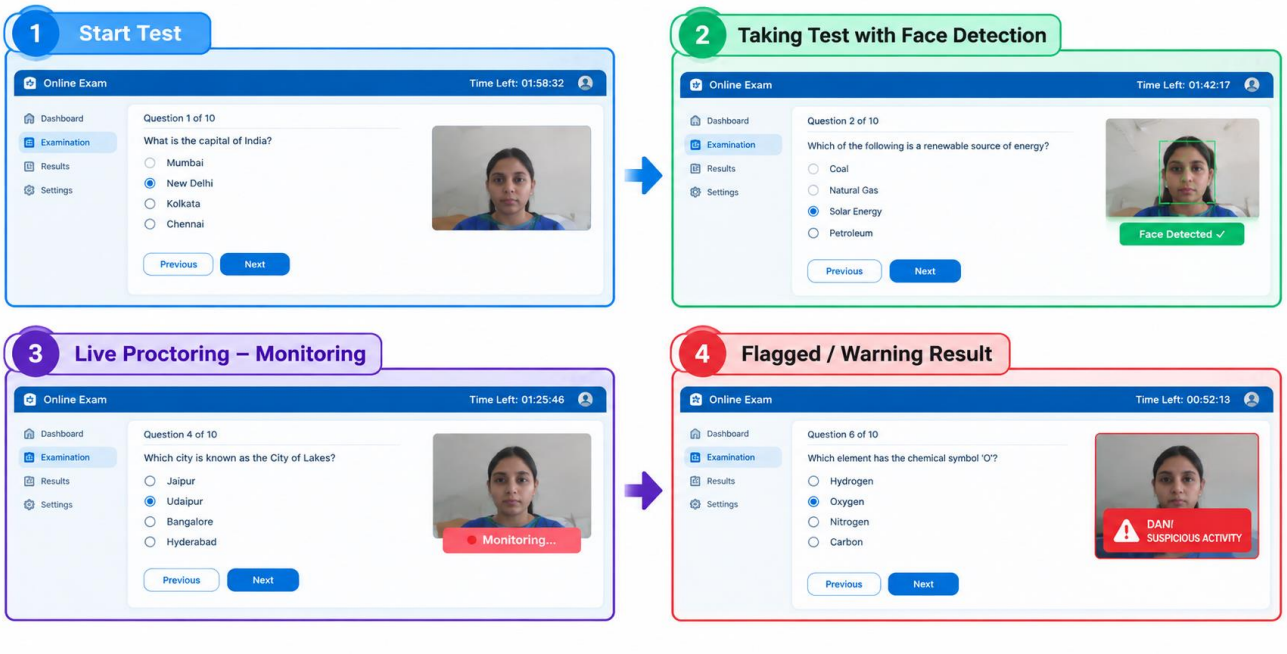


Figure 10. The results presented in face verification and violation detection, indicate registered identity capture, successful verification,mismatch detection and automatic termination of exams.

7.4. Overall System Performance

The findings confirm that the suggested framework manages to balance the accuracy, efficiency, and privacy protection. The proposed method, in contrast to the traditional webcam based systems, gets rid of the persistent video surveillance, but does not decrease the detection efficiency. Behavioral risk scoring and anomaly detection enhanced the performance of detection, whereas the blockchain-based logging system guarantees safe and impeccable storage of examination records.

7.5. Limitations

The given framework is mostly based on behavioural monitoring through the use of a browser, which might fail

Jack Sparrow Publishers © 2026, IJCSER , All Rights Reserved
www.jacksparrowpublishers.com

ISSN: 3107 - 8605 (Online) , http://www.ijcser.com/ , Vol. 3, Issue 2 , 2026 , https://doi.org/10.63328/IJCSER-V3RI2P3

to identify all types of cheating, especially the ones that utilize the use of external devices or support through offline means. The system does not have any visual verification because it does not involve constant use of the webcam to maintain privacy. Moreover, the usefulness of risk evaluation model is dependent on the preset weights and thresholds, which might need tuning to various examination settings. Moreover, the anomaly detecting system operates under simplified behavioural patterns and might not be able to represent even highly diverse user behavior. Although the logging layer is blockchain-based, it adds extra storage and computation costs, although the data is not lost or modified. These could have scalability and performance implications in a large-scale real-world deployment.

8. Conclusion and Future Work

This paper presented a risk-aware privacy-preserving online examination framework that integrates behavioural monitoring, anomaly detection, and blockchain-based secure logging to ensure academic integrity in remote assessments. Unlike traditional proctoring systems, the proposed approach eliminates continuous webcam surveillance and instead relies on intelligent analysis of candidate interactions, thereby addressing privacy concerns while maintaining effective monitoring [5].

The weighted risk-scoring model enables real-time evaluation of user behaviours, while the anomaly detection mechanism enhances the system's ability to identify subtle irregular patterns. Additionally, the blockchain-based logging layer ensures secure, immutable, and verifiable storage of examination events, providing transparency and auditability. The results demonstrate that the proposed system achieves a balanced performance in terms of detection accuracy, low latency, and privacy preservation, making it suitable for scalable deployment in modern online examination environments. Overall, the framework provides a reliable and efficient solution for secure and non-intrusive examination monitoring.

Future work can focus on enhancing the adaptability and intelligence of the proposed framework by incorporating machine learning and deep learning-based anomaly detection models for improved behavioural analysis. Dynamic threshold optimization techniques can also be introduced to automatically adjust risk levels based on varying examination scenarios.

The integration of smart contracts within the blockchain layer can further automate result validation, certification, and audit processes. Additionally, extending the system to support cross-session behavioural profiling can improve long-term detection of irregular patterns. Further improvements may include optimizing system performance for large-scale deployments, enhancing user experience, and integrating secure browser environments to strengthen resistance against advanced cheating techniques.

References

[1]. M. J. C. Samonte, M. G. E. Artista, A. S. M. Oliveros, and N. P.Solivio,"Analyzing the Integration of Intrusion Detection Systems in Online Learning Applications as an Anti-Cheat Measure," in Proc. 4th Int. Conf. Computer Systems (ICCS), Hangzhou, China, Sep. 2024.
DOI: 10.1109/ICCS62594.2024.10795850.

[2]. X. Duan, X. Ye, and S. Manoharan, "An Online System for Creating Personalized Assessments to Mitigate Cheating," in Proc. IEEE Int. Conf. Teaching, Assessment and Learning for Engineering (TALE), Bengaluru, India, Dec. 2024.
DOI : 10.1109/TALE62452.2024.10834362.

[3]. U. Desai, S. Naik, S. Tari, S. Dessai, and P. Shetgaonkar,"Unauthorised Activity Detection during Online Exam," in Proc. 15th Int. Conf. Computing, Communication and Networking Technologies (ICCCNT), Kamand, India, Jun. 2024.
doi: 10.1109/ICCCNT61001.2024.10724172.

[4]. R. Ramani, S. Gangadhar, A. Balaganesh, and M. Ganganathan, "CryptoProctor in Elevating Online Exams through Blockchain Technology," in Proc. Int. Conf. Computing and Data Science (ICCDS), Chennai, India, Apr. 2024.
doi: 10.1109/ICCDS60734.2024.10560403.

[5]. M. Abdelsalam, M. Shokry, and A. M. Idrees, "A Proposed Model for Improving the Reliability of Online Exam Results Using Blockchain," IEEE Access, vol. 12, pp. 7719–7733, Aug. 2023.
doi: 10.1109/ACCESS.2023.3304995.

[6]. N. V. Toutova, A. P. Gaeva, V. L. Agamirov, L. V. Agamirov, and I. A. Andreev, "Blockchain in Education: A New Approach to Storing and Verification of Academic Works," in Proc. Int. Conf. Intelligent Technologies and Electronic Devices in Vehicle and Road Transport Complex (TIRVED), Moscow, Russia, Nov. 2024.
doi: 10.1109/TIRVED63561.2024.10769792.

[7]. E. Ebrahimi, M. Sober, A.-T. Hoang, C. U. Ileri, W. Sanders, and S. Schulte, "Blockchain-based Federated Learning Utilizing Zero-Knowledge Proofs for Verifiable Training and Aggregation," in Proc. IEEE Int. Conf. Blockchain, Copenhagen, Denmark, Aug. 2024.
Doi: 10.1109/Blockchain62396.2024.00017.

[8]. "Implementing Blockchain and Smart Encryption for Immutable Purchase and Generates Digital Ownership Certificates," in Proc. 3rd Int. Conf. Artificial Intelligence for Internet of Things (AIIoT), Vellore, India, May 2024.

Jack Sparrow Publishers © 2026, IJCSER , All Rights Reserved
www.jacksparrowpublishers.com

ISSN: 3107 - 8605 (Online) , http://www.ijcser.com/ , Vol. 3, Issue 2 , 2026 , https://doi.org/10.63328/IJCSER-V3RI2P3

Doi: 10.1109/AIIoT58432.2024.10574657.

[9]. Q. Xia, J. Gao, I. A. Obiri, K. O. Asamoah, and D. A. Worae, "Blockchain Technology," in Blockchain and Its Applications, Wiley-IEEE Press, 2024, pp. 95–123. doi: 10.1002/9781119989387.ch7.

[10]. M. Pandita, D. H. Patil, K. Kashid, M. Malve, and S. Raina, "Securing Blockchain Database System: An Integrated Approach Using PCA and Isolation Forest for Intrusion Detection,"in Proc. 5th Int. Conf. Emerging Technology (INCET), Belgaum, India, May 2024
doi: 10.1109/INCET61516.2024.10593196.

[11]. K. Sattaiah and K. Chinnaiah, "Providing Security in Genesis and Other Blocks of Blockchain Technology Using SHA256 Algorithm," in Proc. 3rd Int. Conf. Innovation in Technology (INOCON), Bangalore, India, Mar. 2024. doi: 10.1109/INOCON60754.2024.10511929.

[12]. S. S. Dhole, P. N. Chatur, A. V. Deorankar, and K. Waghmare, "Improved Hashing Algorithm for Data Integrity and Security," in Proc. 3rd Int. Conf. Electrical, Electronics, Information and Communication Technologies (ICEEICT), Trichirappalli, India, Jul. 2024. doi: 10.1109/ICEEICT61591.2024.10718623.

[13]. Z. Wang, Y. Wang, C. Yuan, N. Ruan, J. Li, and J. Lou, "Taking Attacks to the Next Level: A Framework for Front-Running Attacks on Blockchain Systems," in Proc. IEEE Global Blockchain Conf. (GBC), Shanghai, China, Jun. 2025.
Doi: 10.1109/GBC60041.2025.11134471.

[14]. V. Chandola, A. Banerjee, and V. Kumar, "Anomaly Detection: A Survey," ACM Computing Surveys, vol. 41, no. 3, pp. 1–58, Jul. 2009. doi: 10.1145/1541880.1541882.

[15]. J. R. Koza, "Machine Learning and Behavioral Pattern Analysis for Anomaly Detection," IEEE Trans. Knowledge and Data Engineering, vol. 35, no. 4, pp. 2150–2162, Apr. 2023.
doi: 10.1109/TKDE.2022.3145678.

[16]. F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," Proc. IEEE CVPR, 2015.

[17]. V. Chandola, A. Banerjee, and V. Kumar, "Anomaly Detection: A Survey," ACM Computing Surveys, vol. 41, no. 3, 2009.

How To Cite:

Nwosu Ogochukwu Fidelia , " A Risk-Aware Privacy-Preserving Online Examination System Using Behavioral Anomaly Detection Using Blockchain Technology ", International Journal of Computational Science and Engineering Research (IJCSER) , Volume 3, Issue 2, pp 14–24, April 2026.

CrossRef DOI: https://doi.org/10.63328/ijcser-v3ri2p3

Declaration

Conflicts of Interest: The authors declare no conflict of interest.

Author Contribution: All authors wrote the main manuscript text and also consent to the submission.

Ethical approval: Not applicable.

Consent to Participate: All authors consent to participate.

Funding: Not applicable, and No funding was received

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Personal Statement: We declare with our best of knowledge that this research work is purely Original Work and No third party material used in this article drafting. If any such kind material found in further online publication, we are responsible only for any judicial and copyright issues.

Generative AI Statement: The authors declare that generative AI was not used in the preparation or creation of this manuscript. The alternative text (alt text) accompanying the figures in this article was generated by Frontiers with the assistance of artificial intelligence. Reasonable efforts have been made to ensure the accuracy and appropriateness of the generated alt text, including review by the authors wherever possible. If you identify any inaccuracies or issues, please contact the editorial team.

Publisher's Note: The statements, opinions, and claims presented in this article are exclusively those of the authors and do not necessarily reflect the views of their affiliated institutions, the publisher, editors, or reviewers. Any products discussed or evaluated, as well as any claims made by their manufacturers, are not warranted, approved, or endorsed by the publisher.

Acknowledgements

We thank everyone who inspired our work

Jack Sparrow Publishers © 2026, IJCSER , All Rights Reserved
www.jacksparrowpublishers.com