International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3711-3718
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0486

A Secure Online Proctoring System for Academic Integrity

Karthica N[1], Kanishka shree T[2], Monika S T[3], Mythili N[4]
[1]Associate professor, Dept. of CSE, Paavai Engineering College, Namakkal , TamilNadu , India
[2,3,4] UG -Computer Science and Engineering, Paavai Engineering College, Namakkal , TamilNadu , India
Emails: *karthicanatesanpec@paavai.edu.in [1], kanishkashree.t55@gmail.com[2], stmonika15@gmail.com[3], mythilin980@gmail.com4*

Abstract
The fast development of online education has made the use of secure and reliable online examination systems more desired. Conventional internet-based exams in most cases encounter the problem of academic dishonesty and inefficiency in monitoring the exams. The current paper explains a proctoring system utilizing AI to examine learners online and guarantee academic integrity by observing the student behavior throughout the exams. The suggested system combines a web-based test platform and artificial intelligence and computer vision algorithms to identify suspicious activities on time. The webcam frames are analyzed by the system to detect behaviours that include, absence of faces, detection of multiple faces, and head pose deviation, movement of eyes and existence of illegitimate objects. Further, the activity of browsers like tab switching is tracked and cheating is discouraged. Rather than keeping recordings of large videos the system produces event logs with lists of timestamps, detected events, and risk scores which minimize storage space and facilitate viewing by instructors. In case the cumulative risk score goes beyond a specified limit, the system may automatically end the examination session. The architecture is made of a React based frontend, a Node.js based backend, and a Python based machine learning service based on computer vision libraries like OpenCV and YOLO. The offered system offers both efficient and scalable and privacy-aware to the system to undertake secure online tests and help educators to detect suspicious activity.

Keywords—*Artificial Intelligence, Online Examination, Automated Proctoring, Computer Vision, Face Detection, Eye Tracking, Object Detection, Academic Integrity, Event Logging, Risk Score Analysis.*

1. Introduction

The online education has grown at a high rate in the last few years especially because of the growth in the utilization of the digital learning platforms. The learning institutions have made academic integrity one of the largest issues because of online exams. Traditional means of supervising exams are not easy to use in distant places and this increases the possibilities of cheating and malpractices. It is therefore clear that there is great need of secure and intelligent systems that can be utilized to monitor students in online examination. Real-time student behavior monitoring can be addressed with the help of computer vision and Artificial Intelligence (AI). The AI-controlled proctoring software can detect suspicious actions such as screen look-away, multiple faces, using unauthorized objects and changing the browser tabs. These technologies may be taken to ensure that the registered student is doing the exam and applying the rules of the exam. The proposed paper is a proposal of a Secure AI-Based Online Examination Proctoring System, which is intended to be utilized to provide academic integrity in online examination. The system consists of a web-based analysis engine and machine learning algorithms that scan web camera frames and detect suspicious activities. Instead of storing big video records, the system stores event records and calculates a risk score by using the identified behaviors. The system can automatically terminate a test in the event that the score of a risk is greater than a specified limit. The proposed system will also provide various interfaces of the administrators, teachers and students, therefore effective exam management and monitoring. The system provides a reliable and scalable system of conducting secure online examinations that is accomplished by incorporating the real-time tracking, computer vision technique, and automated risk analysis.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3711-3718
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0486

2. Related Work

As more people switch to online learning platforms, the question of academic integrity in the process of online examination has become a critical issue. Artificial intelligence, machine learning and computer vision have been employed in the proposal of various online proctoring systems where different researchers track and identify cheating behavior by students. There has been a number of studies that have concentrated on the development of AI-based automated proctoring to monitor online examinations. Das et al. [1] came up with an AI-proctoring system, which involves the application of machine learning algorithms to track student behavior and suspicious activities detected during online examinations. On the same note, Jain and Gupta [2] came up with a computer vision-based automated proctoring framework that can track students in real time through the analysis of webcams. Another significant element of online examination security is identity verification. In a study by Rahman et al. [3], a face recognition-based examination system was introduced online, which checks the identity of the student during and before the exam to ensure that they do not impersonate users. Sharma and Singh [4] were also able to suggest an AI-based e-proctoring that combines facial recognition and behavior analysis in order to implement safe online exams. Cheat detection in machine learning has also been extensively applied. In the article by Patel et al. [5], a smart examination system was devised to analyze the activities of students with the help of machine learning models. Nguyen et al. [6] suggested a deep learning framework that can identify suspicious actions in real-time video streams when conducting online exams. The use of eye-tracking and gaze detection methods has also been studied to identify abnormal behaviors by students. Li and Zhang [7] suggested a proctoring system, which integrates face recognition and eye-tracking devices to track student attention and prevent any possible attempts at cheating. In the same way, Kumar and Verma [8] used object detection algorithms based on deep learning to detect illegal devices like mobile phones or books in the test room. Some other studies have also concentrated on enhancing scalability and efficiency of remote proctoring systems. The system described by Lee et al. [9] is an AI-based remote proctoring to be used on e-learning platforms with a large number of students. Brown and Wilson [10] wrote about the safe web-based test systems and emphasized on the automation of the monitoring with in massive online classes. Suspicion in examination has also been suggested to be detected by vision-based monitoring techniques. Ahmed et al. [11] came up with a vision-based monitoring system, which examines facial movements and posture to detect possible cheating behavior. Gupta and Arora [12] proposed a system of monitoring based on head pose estimation and gaze tracking to identify abnormal student behaviors. More developments have been aimed at combining behavioral analysis with artificial intelligence. The Srinivas and Reddy [13] developed a smart e-proctoring system, which integrates monitoring based on AI usage and automated report generation. Smith and Wang [14] came up with the machine learning strategy to learn the behavioral pattern of the students when undertaking online exams. Chatterjee and Banerjee [15] invented a scalable AI-based proctoring system that incorporates various monitoring methods that include face recognition, object detection, and behavioral analysis to increase the credibility of online tests. Though such systems have good monitoring capabilities, most of the systems that are available today use the continuous video recording heavily which needs high storage and privacy issues. Thus, the suggested system is oriented at real-time identification of the suspicious behavior and retention of only the event logs and risk scores, as opposed to complete video footage, which enhances the efficiency and scalability.

3. Proposed Methodology

The suggested system will also help to create a safe and trustful online testing platform with an amalgamation of web technologies and the methods of artificial intelligence and computer vision. The system keeps checking students in the process of taking online examinations and it automatically identifies suspicious activities that could be as a result of cheating. The methodology as a whole is based on real time monitoring, behavior analysis and risk-based decision making. The proposed system has three primary parts in its architecture, including the

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3711-3718
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0486

frontend layer, the backend layer, and the machine learning service. The frontend layer serves to give user interface to students, teachers and administrators. It works with the examination interface, enables the webcam and transmits the obtained frames to the server. This interface enables students to log in to the system and choose the given examination and take the test. The backend layer handles operations in the system like authentication, examination, event logging and communication with machine learning module. It also accepts frontend requests and inserts appropriate information into the database. The monitoring records and risk score calculations are also implemented in the backend, which assesses risk-identified events in the course of the examination. The machine learning service analyses webcam frames in real-time with the help of computer vision algorithms. As the test starts, the system goes on to start the web camera of the student and records frames on a continued basis. These frames are being forwarded to the machine learning module where a number of monitoring techniques are used. The system is used to detect a face so that it prevents a scenario where the face of the student is not visible during the examination. The identity of the student is verified by face recognition and also helps in deterring the impersonation. Monitoring of how the student is gazing and tracking suspicious movements, like looking away frequently, is done by use of head pose detection and eye tracking. Object detection algorithms also are used in the system to distinguish unauthorized objects like mobile phones or books that can be used to cheat. Besides visual surveillance, the system can monitor the activities of the browser including tab switching or the minimization of the examining window which can mean that he/she is trying to get access to other websites. Any suspicious activity identified by the system creates an event log that will have information about the student ID, exam ID, date, type of suspicious activity, and a risk score. The severity of such events is assessed with the help of a risk scoring mechanism. The system automatically ends the examination session when the cumulative risk score goes above a specific threshold to avoid cases of additional misbehavior. The proposed methodology would allow conducting secure online examinations and ensuring academic integrity by integrating artificial intelligence, real-time monitoring, and automated risk analysis, which will be efficient and scalable.

4. System Design/Architecture

The offered AI-based online examination proctoring system aims at providing a secure and reliable remote exam system by combining web technologies with the approach of artificial intelligence and computer vision shown in figure 1. The system is based on three-layer architecture which includes Frontend Layer, Backend Layer, and Machine Learning Layer. The components collaborate to track students in exams and distinguish suspicious activity as it occurs.

4.1. Frontend Layer

The front-end layer will be the interface of all system users whether they are administrators, teachers and students. This layer is created with the help of the latest web technologies like React in order to provide the interactive and responsive interface. This interface allows students to log in into the system, consult appointed examinations, and access the examination environment. Once the exam is started, the front end starts the web camera of the student and captures image frames in the continuous mode. These frames are forwarded to the back server where they are processed further. Through the application, teachers are able to design examinations, post question papers, give tests to a particular group of students, and manage the sessions of the tests. Administrators are in charge of user accounts, student approving and system level administration.

4.2. Backend Layer

The backend layer serves as the hub which takes care of operations of the system as well as communicating with the frontend and machine learning service. This layer is provided via the use of Node.js and Express. The backend has a number of significant functions that include user authentication, schedule events, data management, and event logging. The frontend sends it webcam frames and browser activity information which it transmits to the machine learning module to analyze it. Once the analysis is done, the backend logs the identified events in the database with additional information on the student ID, exam ID, and timestamp, event type, and risk score. The backend also makes the total risk score when the

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3711-3718
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0486

examination is underway and whether to proceed with the exam session or to terminate it.

4.3. Machine Learning Layer

The machine learning layer will be the one that analyses webcam frames and determines suspicious activities through the application of computer vision algorithms. The code to execute this module is written in Python and includes such libraries as OpenCV, MediaPipe, DeepFace, and YOLO shown in Figure 1.

The machine learning module carries out several monitoring functions, such as:

- Face Detection in order to make sure the face of the student can be seen during the exam.
- Face Recognition to confirm the identity of the student.
- Head Pose Detection to detect unusual head movements.
- Gaze monitoring using Eye Tracking.
- Object Detection to detect illegal objects like book or mobile phones.

4.4. Risk Score System and Event Logging

The system has an event-based logging system as opposed to continuous video logging. Detection of every suspicious behavior results in an event log with the identified behavior, the time of occurrence, and a predefined risk score. Risk scores are represented by the absence of faces, switching of tabs, screen aversion and multiple face recognition. The system further estimates the overall risk score of each student as long as the student is undergoing the examination.

4.5. Automatic Exam Termination

In a case when the total risk score is more than a certain set threshold value, the system automatically ends the examination session. This feature can stop serious cases of cheating, and provides fairness when conducting online tests.

4.6. System Workflow

- The student enters the system and clicks on the exam given.
- On beginning the exam, the webcam is switched on.
- The system constantly takes the webcam frames.
- The frames are forwarded to the machine learning service to be analyzed.
- Suspicious behavior is detected by AI algorithms.
- Events detected are made available into the backend server.
- The risk score is updated and the event logs are captured on the backend.
- In case the risk score is more than the threshold, the test will be automatically canceled.

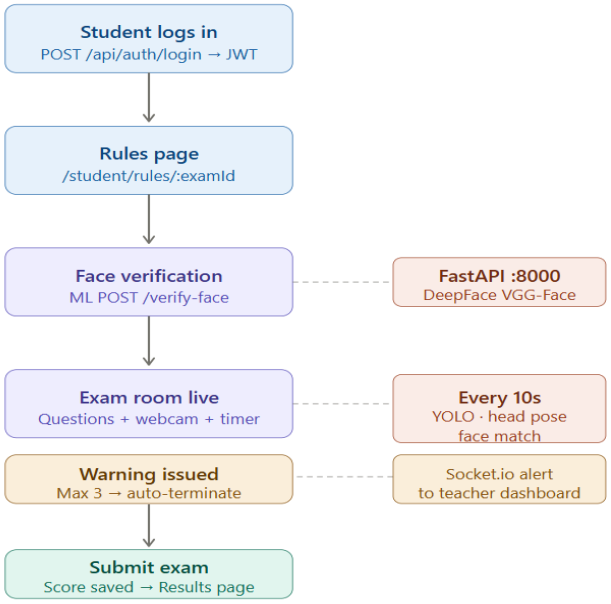

Figure 1 Architecture Diagram

5. Implementation

5.1. Implementation Overview

The Online Examination Proctoring System is an AI based platform that has been implemented with the use of both the web technologies and machine learning services. The system will be developed in a way that it will be used to screen students taking online tests and in real time to detect suspicious activities as well. Its application has 3 layers, frontend and backend layer, and machine learning service. Every element has some functions to be performed in a way that the monitoring could be effective and analysis control could be ensured. It is characterized by the system capturing the webcam frames during the exam and using the computer vision algorithms on the webcam frames and storing

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3711-3718
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0486

the suspicious activities in the form of event logs instead of storing the continuous video streams.

5.2.Frontend Implementation

This was done on the front end by React that provides an interactive and responsive user interface to all users of the system including administrators, teachers and students.

The salient elements of the frontend are:

- User authentication and the user login.
- Displaying examinations to students.
- Interface of question answering examination.
- Turning on Webcams and frame capture.
- Frame relaying to the backend server.
- Detecting tab switching in the browser.

As soon as the student opens an examination, the system will switch on the web camera and frame it at a certain period. These frames are directed to the server in the back-end where these frames are examined by the machine learning module to an even greater extent. It also possesses various user dashboards in the frontend. Instructors can create, manage exams, meanwhile the administrators can create user accounts and system configuration.

5.3. Backend Implementation

The back-end layer was implemented based on the Node.js and Express. The major role played by this layer is to coordinate the system operation and the interaction between the frontend interface and the machine learning service.

Major backend responsibilities are:

- Authentication and authorization of the user.
- Development and planning of exams.
- Student batch management
- Event logging
- Risk score calculation
- Connection with machine learning service.
- Exam session control

When the web frontend sends pictures of the webcam or web browser activity information, the backend forwards the information to the machine learning service to be processed. The backend logs an event in the database in the event of any suspicious activity. Each log record will contain the student identifier, exam identifier, time-stamp, identified type of event and risk score assigned. The backend sequentially gives the risk score with the total risk score prior to the examination. It has an automatic alarm which terminates the examination session when the cumulative risk score surpasses the preset threshold score.

5.4. Realization of Machine Learning Service.

The machine learning module was implemented in Python and using several computer vision libraries including OpenCV, MediaPipe, DeepFace, and YOLO. The module will focus on scanning of webcam frames and detecting suspicious actions that may indicate cheating during an online test. Some of the monitoring methods installed are:

5.4.1. 5Face Detection

The latter is face detection which ensures that the face of the student is visible during examination. This is because when the system fails to identify a face over a duration of time an event is activated.

5.4.2. Face Recognition

The face recognition is used to identify the face of the student by comparing a picture of the student with the list of registered students. When there is a mismatch, a mismatch identity event is detected in the system.

5.4.3. Multiple Face Detection

The system will rely upon whether there are more than one face in the camera frame. This is perceived as being suspicious due to the presence of other individuals during the exam.

5.4.4. Head Pose Detection

The Head pose estimation is also utilized in order to find out whether the student is somewhat looking away frequently out the screen which can be viewed as the potential cheating behavior.

5.4.5. Eye Tracking

Eye tracking refers to the examination of eyewitness movements with the view of diagnosing the anomalous eye gaze patterns.

5.4.6. Object Detection

The algorithms developed based on YOLO- (You Only Look Once) are used to detect objects such as a mobile phone or a book in the surroundings of the student. The machine learning service will analyze the frames of the webcam and send the events it recognizes to the server.

5.5. Database Implementation

The system depends on MongoDB which is the primary database of data storage of the system.

The following information is contained in the

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3711-3718
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0486

database:

- Verified clients (students, teachers, administrators)
- Details of the exam and question papers.
- Student batch information
- Greats made at examinations.
- Supervising the reports of final exams.

Instead of storing large video records, event logs are the only ones stored in the system. This will significantly reduce the storage areas and still the teachers will access the suspicious activities. All event logs contain the following fields:

- Student ID
- Exam ID
- Timestamp
- Event type
- Assigned risk score

5.6. Event Logging Mechanism

The system has a mechanism used in logging, which is an event-driven mechanism rather than a continuous video recording. In a case of suspicion that has been discovered, an event record is appended into the database by the system.

The following are examples of logged events:

- Face not detected
- Looking away from screen
- Browser tab switching
- Multiple face detection
- Identity mismatch
- Illegal object detection.

This kind of solution will ensure that storage is used efficiently and also the review process can be made easier to instructors.

5.7. Risk Score Calculation

Risk scores will be determined beforehand based on the severity of all suspicious events shown in Table 1. Examples of the risk score assignments include:

Table 1 Event Logging Mechanism

Event	Risk Score
Face Missing	+10
Looking Away	+15
Tab Switching	+10
Multiple Face Detection	+40
Identity Mismatch	+50

The system sums up the total score of the risk in the examination session.

5.8. Automatic Exam Termination

The exams have an automatic termination of the tests in the system to prevent severe cases of cheating. The backend server transmits an instant kill command to the examination session when the cumulative risk score exceeds a threshold value which has been previously programmed. This ensures unscrupulous practices are checked in real time basis and integrity of the examination process is maintained.

5.9. Examination System Review In Batch

Educators will be able to develop tests and allocate them to a certain group of students. The questions to be examined can be uploaded in excel files which are handled by the back-end server and stored in the database. Students can only access examination after they have been assigned to a specific batch. This feature is useful in handling a large population of students.

5.10. Exam Monitoring Report

Once the examination is complete, the teachers are able to look through monitoring logs that the system produces.

The final report includes:

- Student identification data.
- Exam information
- Table of identified suspicious events.
- Final calculated risk score
- Overall exam status

Example report:
Student ID: ST101
Test: Database Management System.
Events:
10:10 – Looking Away
10:12 – Tab Switch
10:20 – Multiple Face Detected
Final Risk Score: 65
Status: Suspicious
This report enables instructors to study the behavior of students and make sound decisions concerning academic integrity.

6. Results and Discussion

6.1. Experimental Evaluation

The online proctoring system based on AI was experimented within a simulated online exam setting

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3711-3718
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0486

to assess its capacity to identify suspicious behavior of students. This system was used to constantly scan the frames of the webcams at the time of the exam and to scan the results with computer vision algorithms like face detection, gaze tracking, and object detection. Various habits like facing off the screen, switching tabs, multi-face view and identity misfit were emulated during the assessment. The system was able to identify these events and produced event logs which included timestamps and the risk scores associated with those events.

6.2. Discussion

The findings indicate that online examination can be successfully used to screen suspicious behaviors through the use of the system. The event-based logging system enables the system to record only the captured events rather than entire video recordings which considerably decreases the storage needs. Risk scoring mechanism assists in the assessment of the intensity of identified activities. When the cumulative risk score is more than a pre-determined threshold, the system notifies the examination session is automatically ended. This prevents the severe cases of cheating. In general, the suggested system is an effective and scalable way of ensuring academic integrity during online examinations due to real-time tracking and artificial intelligence analysis.

Conclusion

The proposed AI-based online proctoring will provide the plausible solution to the effective administration of online tests in a safe manner and maintenance of academic integrity. This system will involve integration of web technologies combined with the applications of artificial intelligence and computer vision to monitor the behavior of students taking exams. Using live monitoring of the webcam frames allows the system to detect suspicious actions such as lack of face, several faces, tab changes, and explicitly illicit use of an item. Continuous video recordings are not stored in the system, rather event based logging system captures ongoing events, timestamps and risk scores. This does not require a high degree of storage but is applicable to review effectively the suspicious conduct of the teachers. Another addition that the system makes to the mechanism of risk scores is that the risk score is automatic in stopping the exam sessions in case of severe results of cheating. Overall, it can be seen that the provided system demonstrates how AI-based surveillance, including the automated analysis of risks, can significantly improve the security and reliability of web-based tests. The system provides a powerful and scalable platform to learning institutions that perform remote assessment.

References

[1]. Das, P. K. Mishra, and S. Kumar, “AI-based online proctoring system for remote examinations,” International Journal of Computer Applications, vol. 183, no. 12, pp. 25–31, 2021.
[2]. S. Jain and R. Gupta, “Automated online exam proctoring using computer vision techniques,” in Proceedings of the International Conference on Artificial Intelligence and Data Engineering, 2022, pp. 145–150.
[3]. M. A. Rahman, T. Ahmed, and S. Hossain, “Face recognition-based secure online examination system,” IEEE Access, vol. 9, pp. 120345–120356, 2021.
[4]. P. Sharma and N. Singh, “AI-driven e-proctoring system for online examinations,” International Journal of Advanced Computer Science and Applications, vol. 12, no. 6, pp. 320–326, 2021.
[5]. R. Patel, S. Shah, and K. Mehta, “Smart online examination system using machine learning,” in Proc. IEEE International Conference on Smart Computing, 2020, pp. 212–217.
[6]. H. Nguyen, D. Nguyen, and T. Tran, “Real-time cheating detection in online exams using deep learning,” IEEE Transactions on Learning Technologies, vol. 14, no. 3, pp. 358–370, 2021.
[7]. Y. Li and X. Zhang, “Online proctoring system based on facial recognition and eye tracking,” Journal of Educational Technology Systems, vol. 50, no. 1, pp. 45–60, 2021.
[8]. A. Kumar and R. Verma, “Deep learning-based object detection for cheating prevention in online examinations,” Procedia Computer Science, vol. 167, pp. 196–205, 2020.
[9]. S. Lee, J. Kim, and H. Park, “AI-powered

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3711-3718
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0486

remote proctoring system for e-learning platforms," in Proc. IEEE International Conference on Big Data and Smart Computing, 2022, pp. 101–106.

[10]. D. Brown and M. Wilson, "Secure web-based examination systems and online proctoring," Computers & Education, vol. 157, 2020.

[11]. T. Ahmed, M. Rahman, and K. Hasan, "Vision-based monitoring system for online examination environments," IEEE Access, vol. 10, pp. 55822–55835, 2022.

[12]. P. Gupta and S. Arora, "Automated student monitoring using head pose estimation and gaze tracking," International Journal of Computer Vision and Applications, vol. 11, no. 2, pp. 89–97, 2020.

[13]. K. R. Srinivas and M. R. Reddy, "Design of intelligent e-proctoring system using artificial intelligence," in Proc. IEEE International Conference on Information Technology, 2021, pp. 278–283.

[14]. J. Smith and L. Wang, "Behavior analysis in online examination systems using machine learning," IEEE Access, vol. 9, pp. 96543–96555, 2021.

[15]. S. Chatterjee and A. Banerjee, "Secure and scalable AI-based proctoring framework for online assessments," International Journal of Emerging Technologies in Learning, vol. 17, no. 4, pp. 102–115, 2022.