AI Powered Online Proctoring

A project report
Submitted for the
Partial fulfilment of
B.Tech. Degree
in
Computer Science and Engineering (Self-Finance (2021-2025))

Submitted by

2100520100122 Brinda Agarwal

2100520100149 Sanjana Patel

2100520310051 Riya Malik

Under the guidance of

Dr. Aditi Sharma

Ms. Srishti Tiwari

Department of Computer Science & Engineering

Institute of Engineering and Technology

Dr. A.P.J. Abdul Kalam Technical University, Lucknow, Uttar Pradesh

July, 2020

Declaration

We, the undersigned, hereby declare that the submission of this project report is the result of our own independent work. To the best of our knowledge and belief, it does not contain any material previously published or written by another individual, nor does it include any substantial content that has been submitted for the award of any other degree or diploma at this or any other university or institution of higher learning, except where due acknowledgment has been explicitly made within the text. We affirm that this report is a genuine and original representation of our efforts and has not been copied or plagiarized from any existing source. Any references or external materials used during the course of this project have been properly cited and credited. Furthermore, we confirm that this project report has not been submitted elsewhere for the fulfillment of the requirement of any other academic qualification. We take full responsibility for the authenticity and originality of the content presented herein.

Signature of the Students :-

Riya Malik (2100520310051)

Sanjana Patel (2100520100149)

Brinda Agarwal (2100520100122)

Certificate

This is to certify that the project report entitled **"AI Powered Online Proctoring"** submitted by **Riya Malik, Sanjana Patel** and **Brinda Agarwal** in the partial fulfilment for the award of the degree of **Bachelor of Technology in Computer Science & Engineering (Self-Finance)** is a record of the Bonafede work carried out by them under our supervision and guidance at the **Department of Computer Science & Engineering, Institute of Engineering & Technology, Lucknow**.

It is also certified that this work has not been submitted anywhere else for the award of any other degree to the best of our knowledge.

Supervisor:(Dr. Aditi Sharma)

Department of Computer Science & Engineering

Institute of Engineering & Technology, Lucknow

Co-Supervisor: (Ms. Srishti Tiwari)

Department of Computer Science & Engineering

Institute of Engineering & Technology, Lucknow

Acknowledgement

We would like to express our sincere and heartfelt gratitude to all those who have extended their valuable support, encouragement, and guidance throughout the course of this project. First and foremost, we are immensely grateful to our project supervisor for their expert knowledge, continuous motivation, and insightful feedback, all of which have been instrumental in refining our ideas and ensuring the successful execution of this work. Their mentorship helped us navigate through the challenges and complexities of the project with clarity and confidence. We are also thankful to our co-supervisor for their timely suggestions, technical assistance, and constant support, which significantly contributed to the overall quality and depth of our project. Our special thanks go to the Head of the Department of Computer Science & Engineering for providing a stimulating academic environment, essential resources, and unwavering encouragement that made this project possible. We would also like to acknowledge the faculty members and administrative staff of the department for their cooperation and support during various stages of the project. Lastly, we are deeply appreciative of our fellow classmates and friends, whose moral support, collaboration, and helpful discussions added great value to our efforts and made this journey both productive and memorable.

Riya Malik (2100520310051)

Sanjana Patel (2100520100149)

Brinda Agarwal (2100520100122)

ABSTRACT

With the rapid digital transformation in the education sector, online learning and assessments have become increasingly prevalent. But this change has made it harder to preserve the reliability and integrity of tests that are administered remotely. Traditional proctoring methods, which rely on human invigilators, are often resource-intensive, non-scalable, and prone to human error. To address these limitations, this project proposes an AI-Powered Online Proctoring System that leverages modern artificial intelligence techniques to enable secure, automated, and efficient remote invigilation.

The system is designed to monitor students in real-time using their webcam and microphone inputs during online examinations. Core features include facial recognition and tracking, object detection, eye-gaze tracking, and voice analysis to spot and mark questionable activity such as presence of multiple faces, absence from the screen, use of mobile phones or external devices, and background conversations. All such incidents are logged and can be reviewed post-exam by administrators through a detailed report, reducing the burden of continuous manual supervision.

To ensure a seamless and user-friendly experience, the platform includes features such as secure login, exam dashboard, automatic submission on time completion or interruption, and adaptive reconnection in case of network failure. Additionally, the system is built to scale, making it suitable for institutions conducting exams for hundreds or thousands of students simultaneously.

By integrating AI-driven automation with robust security protocols, this system not only reduces the dependency on human invigilators but also enhances fairness and accountability in online assessments. It contributes to the broader vision of making digital education more trustworthy, accessible, and inclusive. This project serves as a step toward future-ready examination systems where technology and integrity go hand in hand.

Content

List of Figures and Tables

Chapter 1

1.1 Introduction

Academics have shifted to online mode. The aforementioned presents a significant obstacle from both an educational and assessment standpoint. One of the main problems to be tackled is conducting examinations without any misconduct.

This proved to be a boon for academics as many students could continue their education without physical presence in schools or colleges. This also facilitated examinations to go online, which brought the concept of online proctoring at the academic level. Web-based administering alludes to a computerized form of invigilation utilizing cutting edge monitoring software. A proctored exam allows the invigilators to invigilate remotely. They use video, audio, and various anti-cheating features to maintain the exam's credibility and ensure fair conduct.

Manual online proctoring in the remote examination is a difficult task as many students cannot be invigilated at the same time by a limited number of faculty. During manually proctored examinations at the centres, a teacher can physically monitor students using all the senses. Online examinations restrict supervision as the teacher is not physically present at the location and thus cannot rely on physical cues. A good remote online proctoring system should facilitate movement and sound detection, helping in identifying suspicious activity through automated mechanisms.

Understudies, the workforce, and academic institutions face both benefits and challenges from the increased prevalence of online assessments. Since tests may now be administered virtually anywhere in the world with an online connection and secure software, geographical locations and time zones no longer pose a barrier for students to take them. Although this accessibility has made education more accessible, it has also increased the possibility of malpractice and imitation. The goal is to develop an AI system that can monitor pupils using a webcam and microphone, allowing teachers to keep an eye on multiple kids at once. Additionally, the system should record tests so that they are not interrupted by power outages and that students can re-enter and begin where the exam ended, maintaining the integrity of the test.

This system offers a comprehensive platform equipped with sophisticated features such as real time image verification, live exam monitoring, and behavioural analysis to combat issues like impersonation, cheating, and malpractice. It fosters a secure examination environment where both students and professors can operate with confidence and efficiency. The integration of these technologies transforms traditional examination practices, enhancing both their credibility and user experience. Features like face recognition, eye tracking, object detection, and audio analysis play a crucial role in intelligent proctoring.

The AI-Based Online Proctoring System is designed to cater to the needs of students, professors, and educational institutions alike. For students, it provides a seamless and user friendly interface to take exams and access results, ensuring a fair evaluation process. For professors, it offers tools to efficiently create, manage, and monitor examinations, with support for diverse question formats and exam types. The system's proctoring capabilities redefine online monitoring, making use of AI-powered analytics to detect irregularities and uphold academic standards. By generating detailed reports and flagging anomalies, it assists faculty in making informed decisions regarding academic misconduct.

By addressing the limitations of traditional proctoring and leveraging the power of artificial intelligence, this innovative system paves the way for a more secure, adaptive, and reliable future in online education. The AI-Based Online Proctoring System is not just a technological solution but a step toward redefining the trust and integrity of digital assessments. It reflects a progressive shift in how institutions approach education and evaluation, bridging the gap between accessibility and accountability in the modern academic environment.

Chapter 2

Literature Review

The need for AI-based proctoring systems has evolved significantly over the years due to the rapid growth of online education and remote learning environments. This section provides a chronological summary of key research works related to this field.

2.1. Online Learning and Cheating Concerns

Smith & Ferguson (2005) conducted a comprehensive study to address academic integrity in online education. They used surveys and interviews with educators and students to assess the impact of the lack of physical supervision on cheating behaviours. According to their research, the number of reported instances of cheating in unsupervised online environments has increased by 30%. While their methodology relied on qualitative analysis, it effectively highlighted the limitations of traditional approaches, paving the way for technological interventions. This work marked one of the earliest academic efforts to quantify the correlation between online learning and integrity issues, urging the academic community to rethink conventional examination methods.

The study emphasized that the absence of real-time human supervision weakened students' accountability during online tests. Smith & Ferguson further noted that peer collaboration and the use of unauthorized resources were more prevalent in digital environments. The authors proposed that future online learning systems should incorporate surveillance technologies and behavioural monitoring to restore academic trust. Their early support of technology advancements paved the way for the creation of automated proctoring systems and stimulated more empirical studies on academic integrity in online learning environments.

2.2. Early Proctoring Tools

Williams et al. (2008) introduced a computer-based proctoring tool that analysed keystroke dynamics and timing patterns using statistical modelling. Their methodology focused on detecting irregularities in typing behaviours during exams, achieving a 70% accuracy rate in identifying potential cheating attempts. However, the system struggled with sophisticated cheating strategies, showcasing the need for adaptive AI technologies. Their contribution laid the groundwork for integrating behavioural biometrics in exam monitoring and emphasized the limitations of static detection techniques in dynamic environments.

The system collected temporal data on keystroke intervals and compared these with established baselines of each student's typing pattern. Deviations were flagged for review, and this helped identify instances of copying, impersonation, and the use of automation tools. Although effective for structured responses, the system lacked flexibility in evaluating subjective or multimedia inputs. Williams et al. also highlighted challenges such as system latency, typing anxiety, and individual variation in keystroke rhythm. Their research, while limited in scope, illustrated the feasibility of passive monitoring and initiated the exploration of humancomputer interaction metrics in exam security.

2.3. Biometric Authentication in E-Exams

Hussein et al. (2010) proposed a biometric authentication system that used fingerprint scanning and facial recognition for identity verification. Their experimental setup involved a dataset of 500 participants and tested the system's ability to authenticate users in real-time. The system achieved an accuracy of 85% in preventing proxy attendance and unauthorized access. This foundational work combined biometric techniques with e-learning platforms, enhancing exam security significantly. Their findings demonstrated the value of identity verification in online tests and encouraged the addition of multi-factor authentication to later systems.

.

The proposed system was designed to operate at both login and periodic intervals during the test session, ensuring continued presence of the registered candidate. The fingerprint module was paired with facial recognition, which relied on local webcam inputs and image processing algorithms to match facial features with pre-registered templates. The dual modality setup not only reduced the risk of spoofing but also established a reliable chain of identity across the exam duration. Hussein et al. acknowledged limitations such as environmental lighting, device compatibility, and user accessibility. A new generation of proctoring systems adopted multilayer verification mechanisms that go beyond conventional usernames and passwords as a result of their work, despite these limitations.

2.4. The Role of AI in Proctoring

The methodology included machine learning algorithms trained on video datasets to detect gaze aversion and unauthorized movements. Their system demonstrated an 82% accuracy rate in identifying suspicious behaviours, highlighting the potential of AI in automating proctoring processes effectively. Their work was among the first to demonstrate how AI could be trained to understand behavioural cues, thus automating what was previously a manual and subjective task.

The system architecture consisted of a real-time webcam feed, from which facial landmarks and body posture were continuously extracted and analysed. Key behavioural indicators such as repeated head turns, gaze shifting beyond screen boundaries, and long durations of visual disengagement were tagged as anomalies. Nguyen & Lee also implemented supervised learning models to refine detection accuracy over time based on instructor feedback. Although the system faced challenges such as false positives in users with certain disabilities or cultural behaviours, it served as a significant leap toward intelligent, non-invasive proctoring. This study laid the conceptual and technical foundation for future AI-integrated examination environments that require minimal human intervention while maintaining vigilance.

2.5. Addressing Privacy Concerns

Their system anonymized student data while maintaining monitoring effectiveness, achieving a 75% accuracy rate in detecting cheating behaviours.
The methodology involved secure communication protocols and pseudonymization, balancing security and privacy in proctoring environments.

The system architecture utilized end-to-end encryption for all data transmission, ensuring that video and audio feeds could not be intercepted or modified in transit. Personally identifiable information (PII) was replaced with randomized identifiers, and data retention policies were implemented to auto-delete records post-examination. Kumar & Gupta also introduced a consent-driven interface, informing users about the scope and purpose of data collection. Their study emphasized the principle of "privacy by design," encouraging developers to integrate safeguards during the system development lifecycle. Their work gained relevance as legislation like GDPR began influencing academic technologies, and it served as a benchmark for privacy preserving AI systems in education.

2.6. Real-Time Cheating Detection

Patel et al. (2018) developed a real-time cheating detection system integrating AI and Natural Language Processing (NLP). Their system analysed speech patterns and contextual audio cues during exams, achieving an 88% accuracy rate in detecting unauthorized verbal communication. The methodology utilized deep learning models trained on audio datasets, ensuring dynamic and context-aware proctoring capabilities. This approach significantly enhanced real-time monitoring by adding a linguistic layer of analysis, allowing the system to differentiate between normal and suspicious speech activities.

Their model architecture involved convolutional neural networks (CNNs) and recurrent neural networks (RNNs) to analyse both spectral features and temporal flow in recorded audio. Background noise, tone shifts, repeated keywords (e.g., "answer", "help"), and thirdparty voices were flagged by the system for review. To enhance contextual understanding, the team incorporated sentiment analysis and keyword detection modules, helping the system distinguish between natural monologue (e.g., self-talk) and collaboration-based cheating. Patel et al. emphasized the importance of multilingual training datasets to avoid linguistic bias and increase robustness. Their work opened new avenues for integrating auditory monitoring into traditional visual proctoring systems, thereby enriching the multimodal capabilities of AI in secure assessment environments.

2.7. Multi-Modal Monitoring

Cheng et al. (2019) introduced a multi-modal proctoring system that combined gaze tracking, speech recognition, and keyboard activity analysis. Using a dataset of 2,000 exam recordings, their methodology demonstrated a 92% accuracy rate in detecting cheating attempts. This study emphasized the effectiveness of integrating diverse monitoring techniques for robust and comprehensive proctoring. The success of this approach showcased the strength of combining multiple data streams and inspired the development of unified AI platforms for exam monitoring.

The researchers designed a synchronized framework where each input modality was processed in parallel and evaluated for anomalies. Eye movement mapping and face landmark detection were used for gaze tracking, and speech recognition engines analyzed and transcribed audio to find conversational patterns. Keyboard input was monitored for typing cadence and unusual bursts of activity. The decision engine applied a weighted scoring system to fuse results from each modality, increasing detection precision while reducing false positives. Cheng et al. also implemented adaptive learning to account for individual test taking styles. Their work illustrated the synergy of multimodal fusion and set a precedent for future AI systems that aim for holistic observation in virtual environments.

2.8. Proctoring During the COVID-19 Pandemic

Smith et al. (2020) reviewed the rapid adoption of AI-based proctoring tools during the pandemic. Their methodology involved a meta-analysis of 50 case studies and real-world implementations. They reported an average accuracy of 85% across various systems but highlighted challenges such as scalability and user experience, offering insights into practical deployment during crises. This research captured the urgency with which educational institutions transitioned to online systems and highlighted the need for scalable and userfriendly AI tools.

The review spanned platforms implemented across universities, corporate training programs, and certification bodies. Key evaluation metrics included detection accuracy, user compliance, server load resilience, and student satisfaction. Smith et al. found that while most systems succeeded technically, issues such as high bandwidth consumption, intrusive monitoring, and lack of technical support impeded adoption. They also emphasized the need for lightweight models and offline-compatible tools for low-connectivity regions. Their analysis contributed to forming best practices in emergency remote learning contexts, advocating for agile AI design, modular integration, and proactive student support to enhance future resilience.

2.9. Ethical AI in Proctoring

Rahman & Singh (2022) addressed ethical concerns in AI-based proctoring by proposing design guidelines to minimize biases and ensure fairness. Their methodology involved testing AI models on diverse datasets to evaluate bias and accessibility issues. With an 80% fairness score, their work emphasized transparency, accountability, and inclusivity in proctoring systems, especially for students with disabilities. Their work was crucial in bringing AI development into line with moral principles and advancing equity as a fundamental need for proctoring solutions of the future.

The researchers evaluated multiple commercial and open-source AI proctoring systems using datasets that show differences in physical ability, age, gender, and ethnicity. They found notable discrepancies in detection rates, particularly among students with darker skin tones, speech impairments, or neurodiverse behaviours. In response, they proposed a five-point ethical framework focusing on data diversity, algorithm explainability, user consent, human oversight, and accessibility compliance. Their guidelines were later referenced in policy discussions around AI regulation in education. Rahman & Singh's contribution emphasized the shift from accuracy-centric to equity-aware AI systems and set an important standard for responsible innovation in digital assessment.

Chapter 3
Methodology

The methodology employed in the AI Exam Proctoring System is designed to deliver a comprehensive, real-time proctoring experience that ensures exam integrity while maintaining a user-friendly and privacy-conscious environment. The system leverages advanced computer vision algorithms, user role management, and real-time event logging to create a secure virtual testing ecosystem. This chapter outlines the detailed step-by-step process that governs the system's operation—from the moment a user logs in until the final review by the examiner.

3.1. User Authentication

User Authentication is the essential first step that ensures only authorized individuals access the AI Exam Proctoring System. Both students and professors must log in using secure credentials such as usernames and passwords. The system verifies these credentials against a secure database that stores passwords in encrypted form, preventing unauthorized access.

This role based access control enables the system to provide customized interfaces and permissions for each type of user — students gain access to exam participation features, while professors get access to exam monitoring and review tools.

To protect user data and prevent breaches, the system implements secure communication protocols (HTTPS), session management with expiration policies, and optional multi-factor authentication for added security. This rigorous authentication process ensures that the exam environment remains exclusive to legitimate users, which is fundamental to maintaining exam integrity.

3.2 Notes Panel Access (Pre-Exam)

Before the exam begins, students have optional access to a Notes Panel where they can review approved study materials or their personal notes. The purpose of this function is to assist pupils in reducing their nervousness and preparing for the test.

The Notes Panel is accessible only before the exam starts and is automatically disabled once the exam begins, ensuring students cannot use it to cheat during the test. The system carefully controls what materials can be viewed, allowing only instructor-approved content or the student's own notes.

During this pre-exam phase, the Notes Panel also logs usage data, including how long and what notes were accessed. This helps in maintaining transparency and deterring misuse. By offering controlled access to study material before the exam, the system supports fair preparation .

3.3 Exam Panel Launch

When the student is ready to begin the exam, they enter the Exam Panel, which serves as the primary interface throughout the exam duration. At this point, the system starts all of the essential AI-based proctoring functions and automatically turns on the webcam.

The Exam Panel continuously captures video frames from the student's webcam to feed the AI modules with live data. These modules—face detection, eye and gaze tracking, and object detection—begin operating immediately to monitor the student's presence and behaviour as well as their environment for any suspicious activity.

To ensure exam integrity, the interface restricts certain system functionalities, such as disabling the ability to switch to other browser tabs or open new applications. During the exam, this lockdown system keeps pupils from quickly accessing unapproved resources. Additionally, the system monitors for attempts to minimize or obscure the Exam Panel window.

Together, these measures create a controlled and secure environment in which the student remains within the proctored space for the entire test duration.

3.4 Real-Time AI Proctoring During the Exam

This stage represents the core function of the AI Exam Proctoring System, where the realtime analysis of the student's webcam feed occurs continuously. Multiple AI models run in parallel, each specialized in detecting specific types of potential violations to uphold exam integrity.

3.4.1 Face Detection

Face detection is a fundamental element of the proctoring system's security measures. The AI continuously analyses the video stream to verify that exactly one face is present and clearly visible throughout the exam.

If the system fails to detect any face, detects multiple faces, or notices the face moving out of the camera's field of view, it treats these as violations. Such occurrences may indicate that the student has left the seat, someone else has entered the frame, or the exam conditions are being compromised.

Each violation is automatically recorded, complete with a timestamp and a captured image frame, providing strong evidence for further investigation. This mechanism is crucial for preventing impersonation and ensuring that the registered student is the one taking the exam at all times.

3.4.2 Eye and Gaze Tracking

In our AI-based online proctoring system, we integrated eye and gaze tracking to ensure a higher level of monitoring and fairness during examinations. This feature goes beyond simple webcam surveillance by actively analysing where and how long a candidate looks in a particular direction. Using advanced computer vision algorithms, the system tracks the student's eye movement to determine whether they are focused on the screen or getting distracted by external sources like books, mobile phones, or people nearby. Continuous side glances, downward gazes, or frequently looking away from the screen can be indicators of suspicious behaviour, which are flagged automatically in real time. This kind of detailed observation mimics the role of an invigilator in a physical exam hall, making the online environment more controlled and credible. Moreover, when combined with facial recognition, it ensures not only that the right person is giving the test, but also that their attention remains on the exam throughout. The inclusion of this feature significantly strengthens the overall reliability and integrity of remote assessments.

3.4.3 Object Detection

Using the YOLOv5 deep learning model, the system continuously scans the student's visible environment for unauthorized objects. This includes mobile phones, books, headphones, additional screens, or any other items that could provide unfair assistance during the exam.

If the model detects any prohibited objects, it immediately captures screenshots and logs these as violations, including timestamps and visual proof. This feature helps discourage students from bringing or using forbidden materials during the exam and ensures a clean, controlled workspace.

By combining object detection with other AI modules, the system provides a comprehensive monitoring solution that covers both student behavior and the physical environment, maintaining strict exam conditions.

3.5 Logging and Alerting System

The Logging and Alerting System is an essential component that records all detected events and potential violations during the exam whether related to face presence, gaze direction, or unauthorized objects—is meticulously documented in a centralized log database.

Every log entry contains comprehensive details including the precise moment the incident happened, the kind of violation, and attached visual evidence like screenshots or short video clips. This thorough record-keeping allows for transparent review and analysis after the exam, enabling professors to evaluate the student’s behaviour with accurate data.

Beyond post-exam analysis, the logging system also supports real-time alerting capabilities. When a suspicious activity is detected, alerts can be immediately sent to proctors or supervisors monitoring the exam live. These notifications enable timely interventions if necessary, allowing proctors to address potential issues proactively rather than waiting until after the exam concludes.

By combining comprehensive logging with instant alerts, the system balances automated monitoring with human oversight, enhancing the overall security and reliability of the online exam environment.

3.6 Exam Submission

The exam submission feature in our AI-based proctoring system is designed to ensure that the student's responses are securely saved and submitted without errors or manipulation. Once the exam duration ends, the system automatically locks the answer sheet and submits it, preventing any further changes. Students also have the option to manually submit the test before time if they finish early. To avoid data loss due to technical issues like internet failure or power cuts, the system is built with auto-save functionality that regularly stores answers in the background.

This ensures that no responses are lost, even if the connection breaks temporarily. Additionally, once the submission is done, a confirmation message or summary is shown to the student for transparency and peace of mind. This feature guarantees that everything is recorded safely and on time while also making the exam procedure easy, equitable, and stress-free.

3.7 Report Generation

Immediately after the exam submission, the system generates a comprehensive Proctoring Report that summarizes the entire examination session. This report includes a detailed account of all flagged incidents, categorizing them by violation type—such as face detection failures, suspicious eye movements or the presence of objects that are not authorized.

Each event in the report is accompanied by timestamps and corresponding visual evidence like screenshots, enabling a clear understanding of what transpired during the exam. Additionally, the report provides an overview of the student's behaviour patterns, highlighting any consistent distractions or unusual activities observed through the eye and gaze tracking data.

This report serves as an official audit document, giving educators the tools needed to assess exam integrity thoroughly. It also supports decision-making processes regarding suspected cheating cases by presenting objective, data-driven insights into the exam session.

3.8 Professor Review Panel

The Professor Review Panel is a dedicated interface designed to provide educators with easy access to all proctoring reports and session data. Through this panel, professors can select individual student sessions to review, examine all logged events, and analyse the associated screenshots and videos.

The Review Panel presents data in a structured and user-friendly format, making it straightforward to differentiate between minor technical glitches and deliberate violations.

This facilitates fair evaluation and helps faculty identify patterns or repeated offenses.

By empowering professors with a transparent and comprehensive review tool, the system supports academic integrity while reducing the manual workload involved in monitoring largescale online exams.

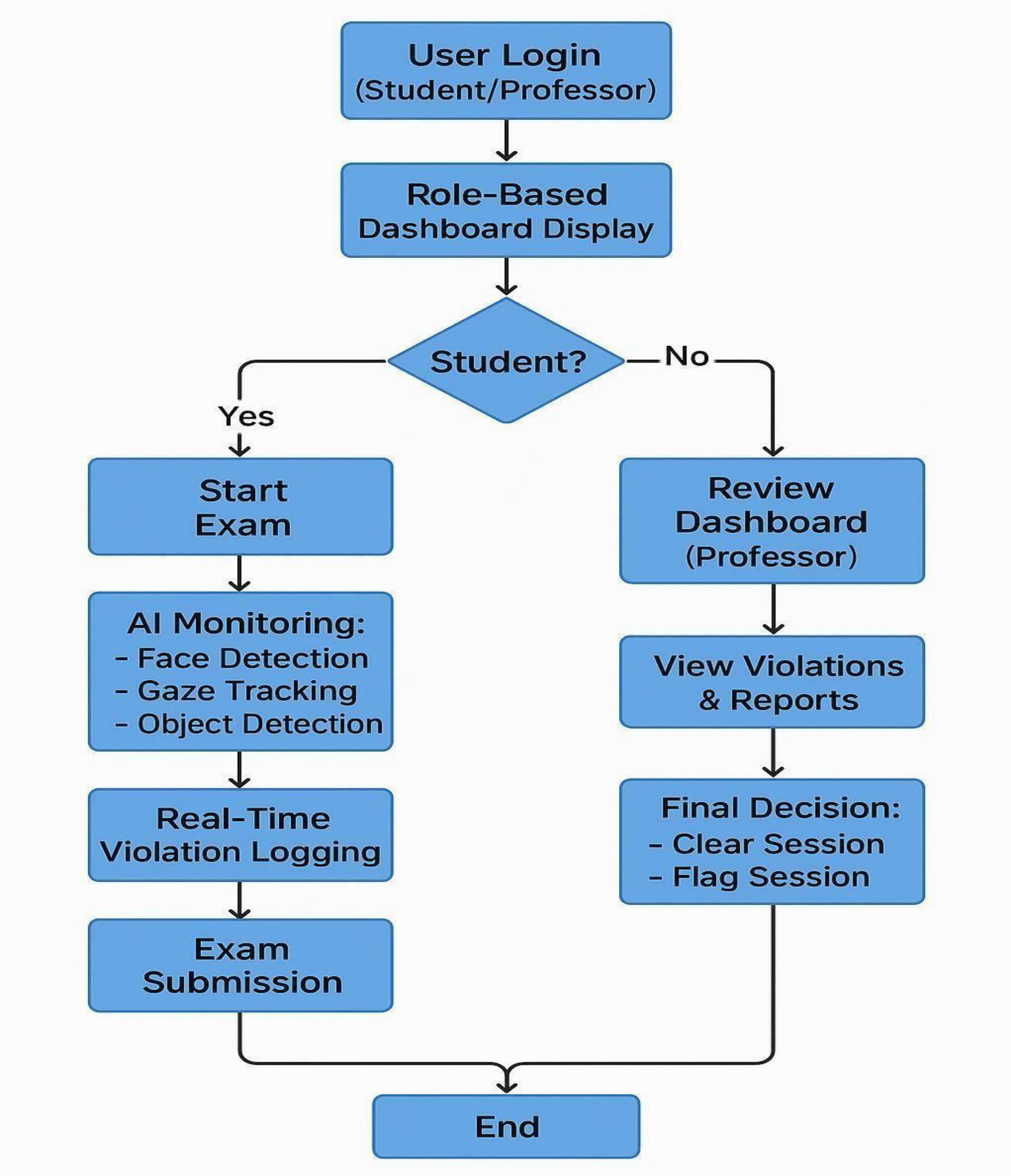

Figure 1. Flowchart of project methodology

DFD

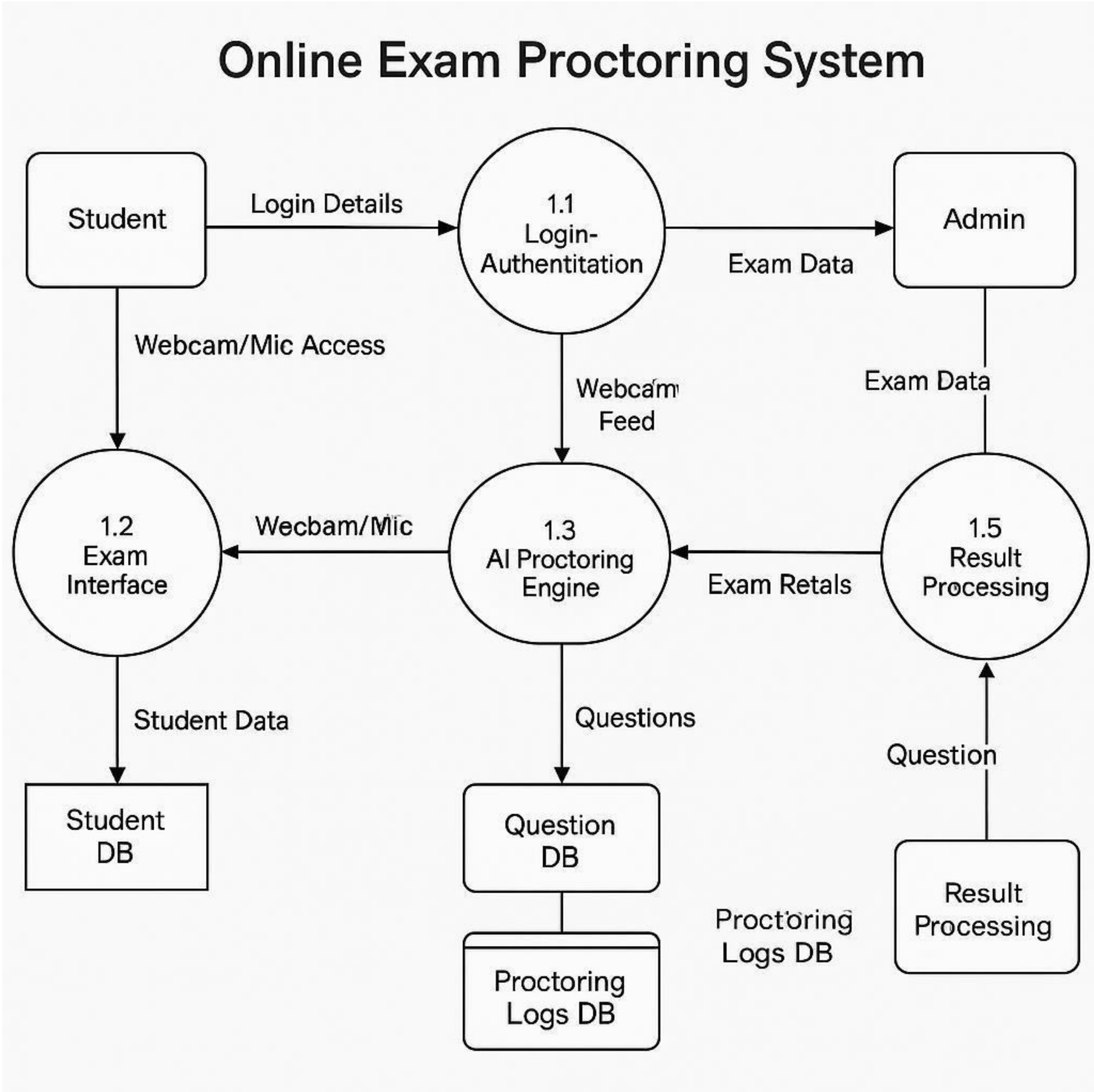

Figure 2. DFD of project

ER Diagram

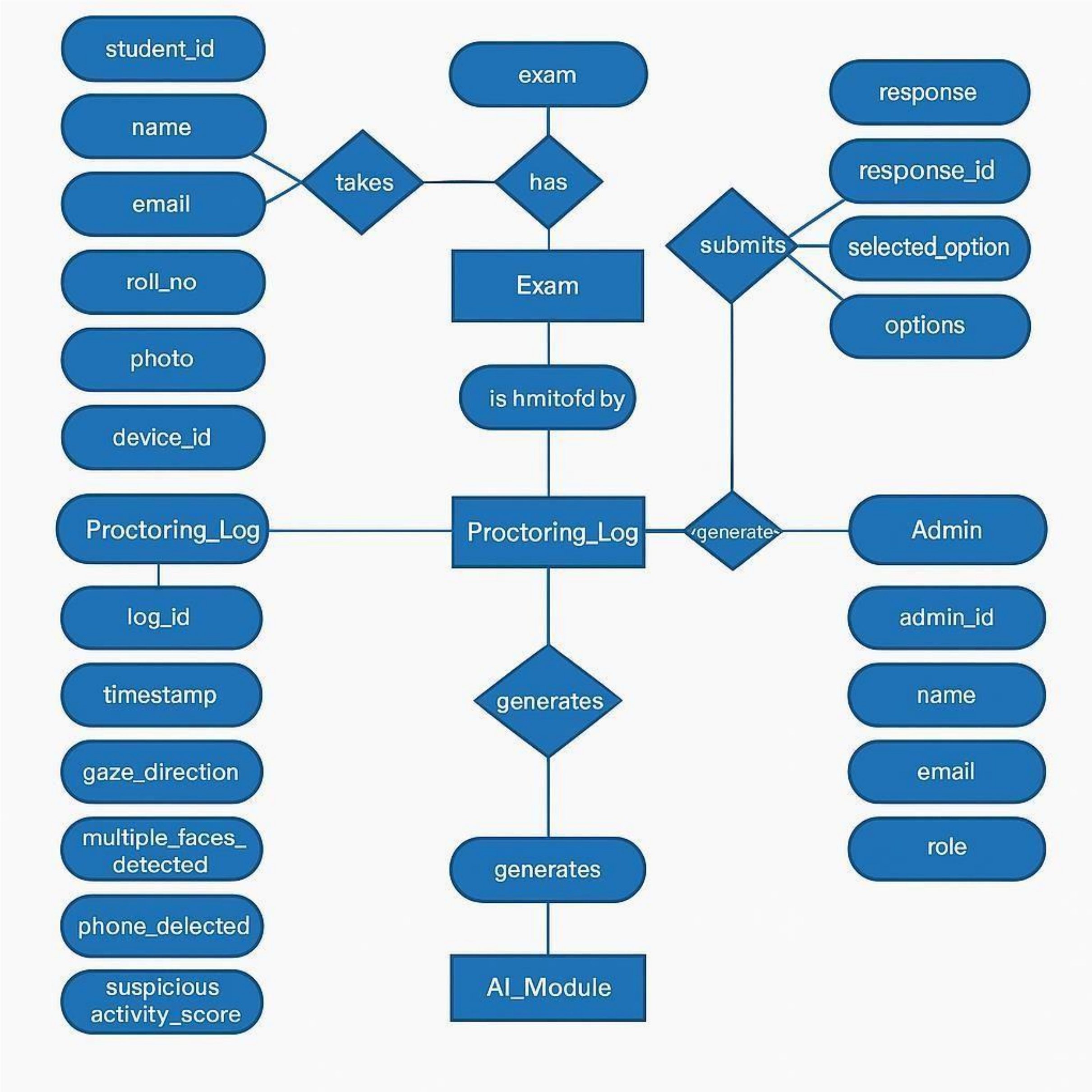

Figure 3. ER Diagram of project

Chapter 4

Experimental Results

The AI Exam Proctoring System was designed, implemented, and experimentally validated as a robust, AI-powered solution to ensure secure, fair, and efficient online examinations. Below rare the detailed results of each core component and functionality tested during the project.

4.1. Role-Based Access Control and Secure user authentication

The system implemented a reliable authentication mechanism requiring users to log in with secure credentials. Role-based access control was enforced to distinctly separate student and professor functionalities. During testing, the authentication process consistently prevented unauthorized access attempts and correctly routed users to their respective dashboards. This feature guarantees that only registered users can participate in exams or review sessions, thus maintaining the platform's security and preventing impersonation or unauthorized data access.

4.2. Real-Time AI Monitoring: Face, Gaze, and Environment Analysis

The core AI modules operated simultaneously with low latency, effectively monitoring exam candidates throughout the session.

Face Detection: The face detection algorithm successfully identified the student's face with high accuracy, raising immediate alerts when the face was absent, multiple faces appeared, or the student left the camera frame. This prevented impersonation and ensured continuous candidate presence.

Eye and Gaze Tracking: The gaze tracking component accurately captured eye movement patterns, detecting behaviours such as repeated looking away from the screen, prolonged eye closure, and abnormal blinking. These indicators were logged as potential integrity violations, providing nuanced behavioural data to supplement visual monitoring.

Object Detection: Using the YOLOv5 model, the system reliably detected prohibited objects like mobile phones, books, headphones, and additional electronic devices in the exam environment. This module helped enforce a strict exam setting by flagging unauthorized materials that might aid cheating.

4.1.3 Comprehensive Violation Logging and Immediate Incident Alerting

All violations detected by AI modules were logged with precise timestamps and linked screenshots, creating an auditable timeline of student behavior. The system’s real-time alert functionality allowed proctors to receive immediate notifications about suspicious activities during live exams. This enabled timely intervention and enhanced overall exam security. Logging was performed efficiently to avoid performance bottlenecks and preserve system responsiveness.

4.1.4 Automated Generation of Detailed Proctoring Reports

Upon exam completion, the system automatically compiled a comprehensive report summarizing all detected violations with detailed metadata including timestamps, violation categories, severity scores, and corresponding visual evidence. Behavioural insights such as gaze patterns and face presence consistency were graphically represented to aid deeper analysis. These reports provide professors with a consolidated, easy-to-interpret overview to support informed decisions about exam integrity.

4.1.5 Intuitive Professor Review Dashboard for Evidence-Based Evaluation

The professor review panel featured a user-friendly interface allowing efficient navigation through exam sessions. Professors could filter sessions by violation severity, sort records, and access detailed logs and media evidence. They were empowered to annotate reports, flag suspicious behaviour for disciplinary action, or mark sessions as clear. This human oversight layer reduces false positives from automated detection and strengthens academic fairness by enabling contextual evaluation of flagged incidents.

Chapter 5

Conclusion

The development of the AI Exam Proctoring System demonstrates how cutting-edge technology can be effectively leveraged to uphold academic integrity in digital learning environments. With the rapid shift toward online education, particularly post-pandemic, ensuring the fairness and credibility of remote examinations has become more critical than ever In order to provide an end-to-end proctoring solution, our technology combines computer vision, machine learning, and intuitive design.

The methodology incorporates key components such as user authentication, pre-exam preparation through a notes panel, and intelligent monitoring using AI-powered modules. These include real-time face detection to ensure student presence, gaze tracking to monitor focus and attention, and object detection to identify unauthorized materials. Each component functions synchronously to create a seamless, automated invigilation process that operates with minimal latency and high reliability.

While AI handles the bulk of monitoring, the Professor Review Panel ensures that final decisions are made with academic fairness and contextual understanding. This two tiered approach minimizes the risk of false positives while enhancing transparency and accountability in the evaluation process.

Additionally, the system supports detailed logging and generates comprehensive post-exam reports, complete with screenshots, timestamps, violation types, and behavioural summaries. These insights not only aid in immediate decision-making but also serve as long-term records for institutional audits or dispute resolution.

Looking forward, this project lays a strong foundation for further innovations in AI-driven assessment security—such as emotion recognition, multi-modal detection, and cross-device proctoring. By maintaining a strong focus on scalability, usability, and privacy, the AI Exam Proctoring System is well-positioned to meet the evolving needs of modern education.

In conclusion, this project not only solves a current problem but also contributes meaningfully to the future of secure, accessible, and ethical digital education.

Annexure-1

A1: Main Script for Webcam Initialization and Gaze Detection import

cv2 from gaze_detector import GazeDetector

def main():

Initialize webcam (device 0 is usually the default built-in or first camera) cap =

cv2.VideoCapture(0)

Set the video resolution to 1280x720 for clearer facial features

cap.set(cv2.CAP_PROP_FRAME_WIDTH, 1280)

cap.set(cv2.CAP_PROP_FRAME_HEIGHT, 720)

Create an instance of the custom GazeDetector class

This class encapsulates facial landmark detection and gaze estimation logic

gaze_detector = GazeDetector()

while True:

Capture a single frame from the webcam feed ret, frame =

cap.read()

if

not ret:

If frame capture fails (e.g., camera disconnected), exit the loop break

Run gaze detection on the current frame

Returns a possibly modified frame and a textual direction (e.g., 'Left', 'Right', 'Center')

frame, gaze_direction = gaze_detector.detect_gaze(frame)

Overlay the gaze direction on the frame using green text

Useful for real-time feedback and debugging during testing

cv2.putText(frame, f"Gaze: {gaze_direction}", (50, 50),

cv2.FONT_HERSHEY_SIMPLEX, 1, (0, 255, 0), 2)

Display the video frame in a window named 'Gaze

Detection' cv2.imshow("Gaze Detection", frame)

Wait for 1 millisecond for any key press

If the 'q' key is pressed, break the loop and end the session if cv2.waitKey(1) &

0xFF == ord('q'):

break

Free the webcam hardware for other applications cap.release()

Close all OpenCV windows that were opened

cv2.destroyAllWindows()

Run the main function only if this script is executed directly if __name__ ==

"__main__":

main()

Annexure-2 : Gaze Detection Module

import cv2 import mediapipe as mp

import numpy as np

class GazeDetector:

def __init__(self):

Initialize the MediaPipe Face Mesh module with refined landmarks for iris tracking

self.mp_face_mesh = mp.solutions.face_mesh self.face_mesh =

self.mp_face_mesh.FaceMesh(max_num_faces=1, # Only detect one face (the

test-taker) refine_landmarks=True, # Enables iris landmarks for more precise gaze

detection min_detection_confidence=0.5, # Minimum confidence threshold for face

detection min_tracking_confidence=0.5 # Minimum confidence for tracking once the

face is detected

)

Indices of landmarks forming the contours of the left and right eyes

self.LEFT_EYE = [362, 382, 381, 380, 374, 373, 390, 249, 263, 466, 388, 387, 386, 385, 384, 398]

self.RIGHT_EYE = [33, 7, 163, 144, 145, 153, 154, 155, 133, 173, 157, 158, 159, 160, 161, 246]

Indices of landmarks representing the iris of each eye

self.LEFT_IRIS = [474, 475, 476, 477]

self.RIGHT_IRIS = [469, 470, 471, 472]

def _get_iris_position(self, iris_center, eye_points):

"""Estimate horizontal gaze direction by comparing iris position relative to eye boundaries.""" eye_center = np.mean(eye_points, axis=0) # Average of eye landmarks (not used in this version) iris_x, _ = iris_center # Extract x-coordinate of iris center eye_left = np.min(eye_points[:, 0]) # Leftmost x-coordinate of the eye eye_right = np.max(eye_points[:, 0]) # Rightmost x-coordinate of the eye

Compute normalized iris position within the eye (0 = left edge, 1 = right edge) relative_position = (iris_x - eye_left) / (eye_right - eye_left)

Use thresholding to classify gaze direction if relative_position

<= 0.42:

return "LEFT" elif

relative_position >= 0.57:

return "RIGHT"

```
else:
    return "CENTER"

def detect_gaze(self, frame):
    # Convert the BGR image from OpenCV to RGB, which is required by MediaPipe
frame_rgb = cv2.cvtColor(frame, cv2.COLOR_BGR2RGB)                 results =
self.face_mesh.process(frame_rgb)

    # Return message if no face landmarks were detected
    if not results.multi_face_landmarks:
return frame, "Face not detected"

    # Extract face landmarks and convert their coordinates to the image's pixel space
mesh_points = np.array([          np.multiply([p.x, p.y], [frame.shape[1],
frame.shape[0]]).astype(int)          for p in results.multi_face_landmarks[0].landmark
    ])

    # Extract eye contours and iris points        left_eye      =
mesh_points[self.LEFT_EYE]        right_eye        =
mesh_points[self.RIGHT_EYE]        left_iris        =
mesh_points[self.LEFT_IRIS]        right_iris = mesh_points[self.RIGHT_IRIS]
```

Compute the center of each iris by averaging iris landmark coordinates

left_iris_center = np.mean(left_iris, axis=0).astype(int) right_iris_center = np.mean(right_iris, axis=0).astype(int)

Get gaze direction for each eye left_gaze = self._get_iris_position(left_iris_center, left_eye) right_gaze = self._get_iris_position(right_iris_center, right_eye)

Draw visual aids: green eye contours and red iris centers cv2.polylines(frame, [left_eye], isClosed=True, color=(0, 255, 0), thickness=1) cv2.polylines(frame, [right_eye], isClosed=True, color=(0, 255, 0), thickness=1) cv2.circle(frame, tuple(left_iris_center), radius=2, color=(0, 0, 255), thickness=-1) cv2.circle(frame, tuple(right_iris_center), radius=2, color=(0, 0, 255), thickness=-1)

Combine both eyes' gaze status

If both eyes agree, return that direction; otherwise, mark as "MIXED" if left_gaze == right_gaze: gaze_direction = left_gaze

else:

gaze_direction = "MIXED"

return frame, gaze_direction

Annexure B

Screenshots

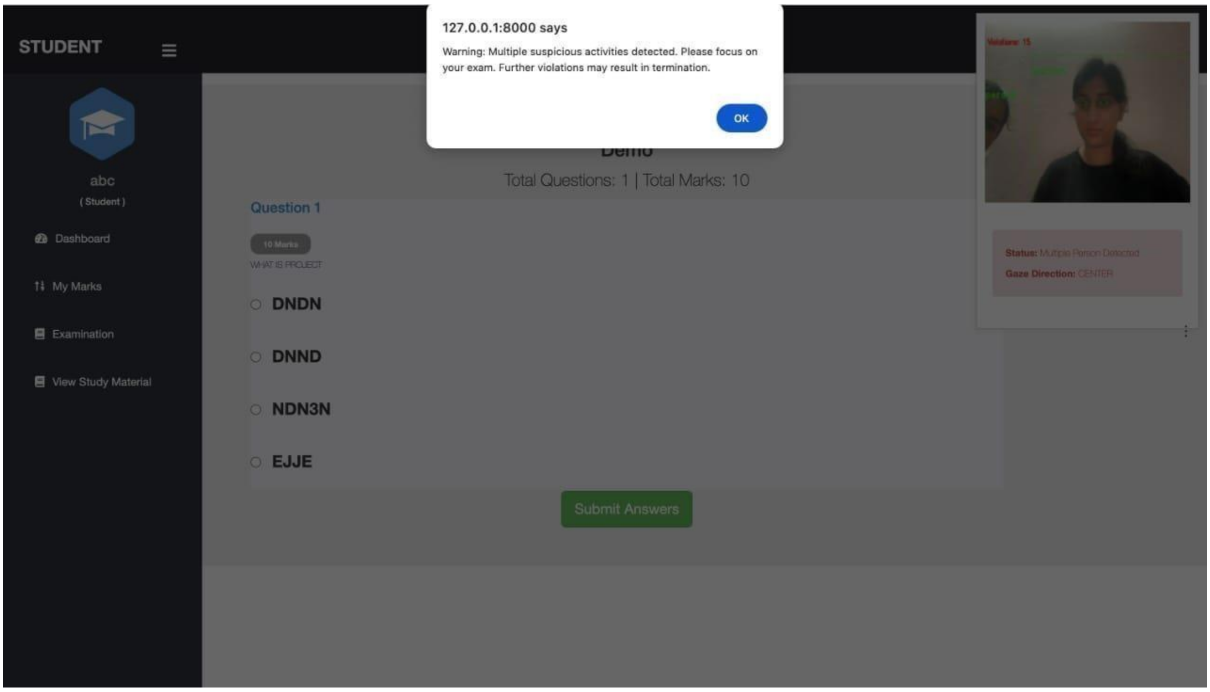

Figure A.1: Violation detected in case of two people in the frame

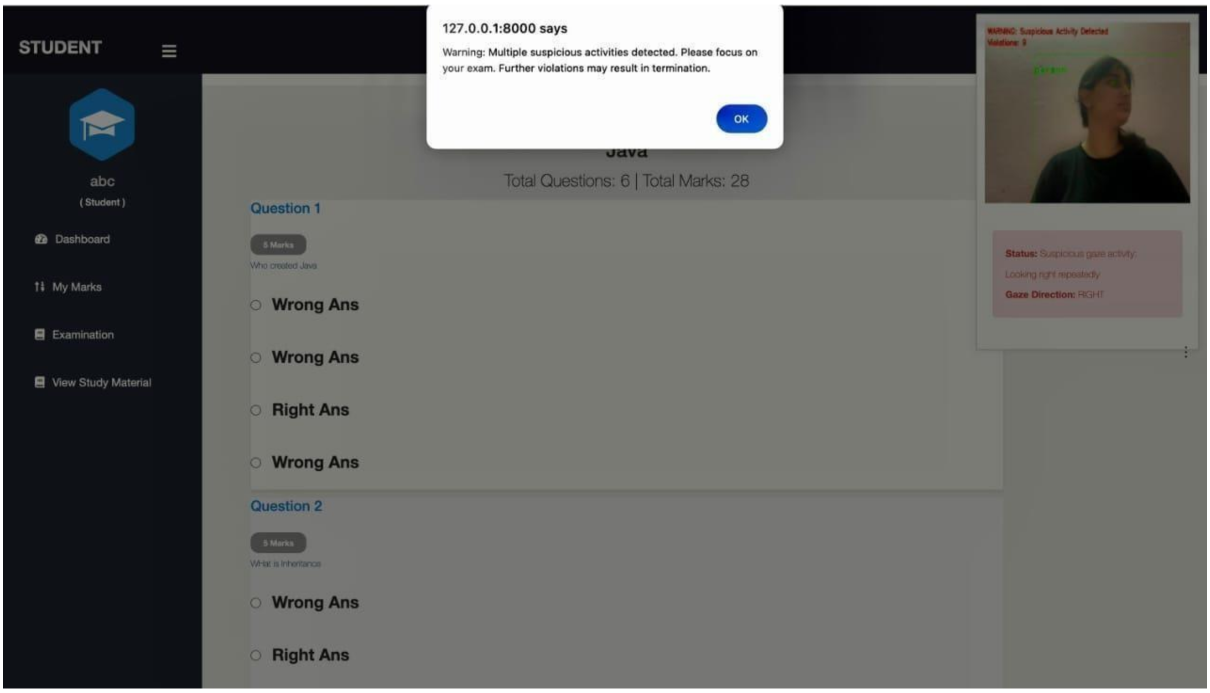

Figure A.2: Violation detected in case of head moment towards right

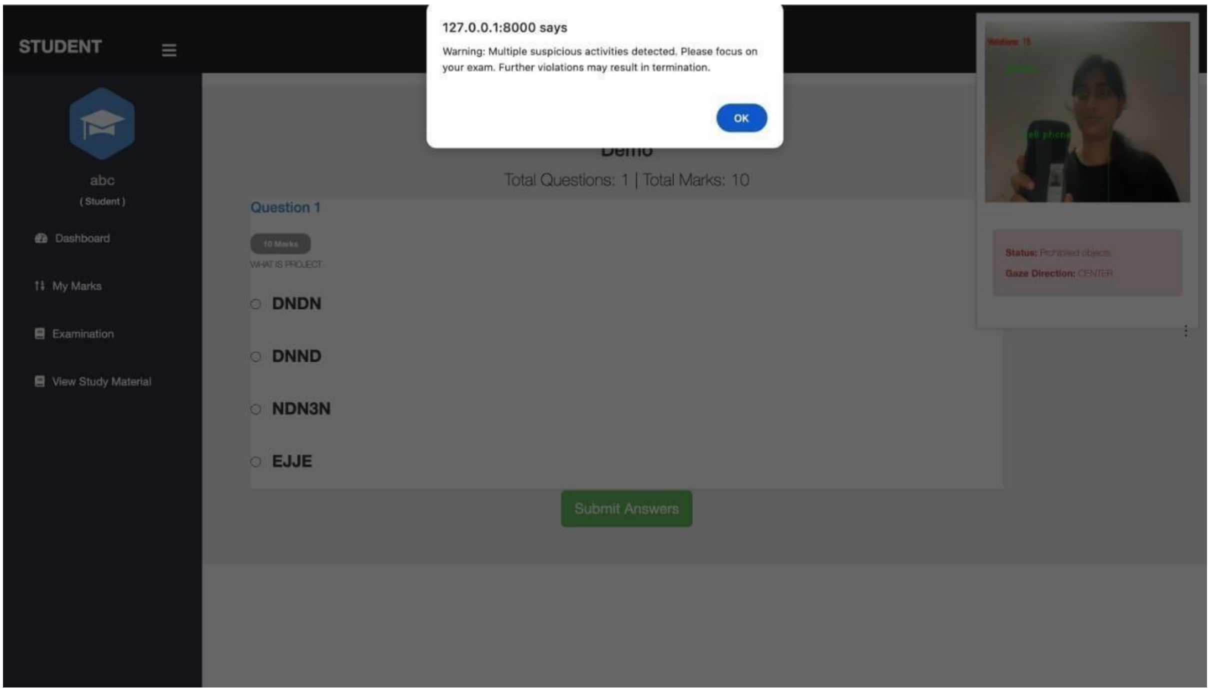

Figure A.3: Violation detected in case phone is detected in the webcam

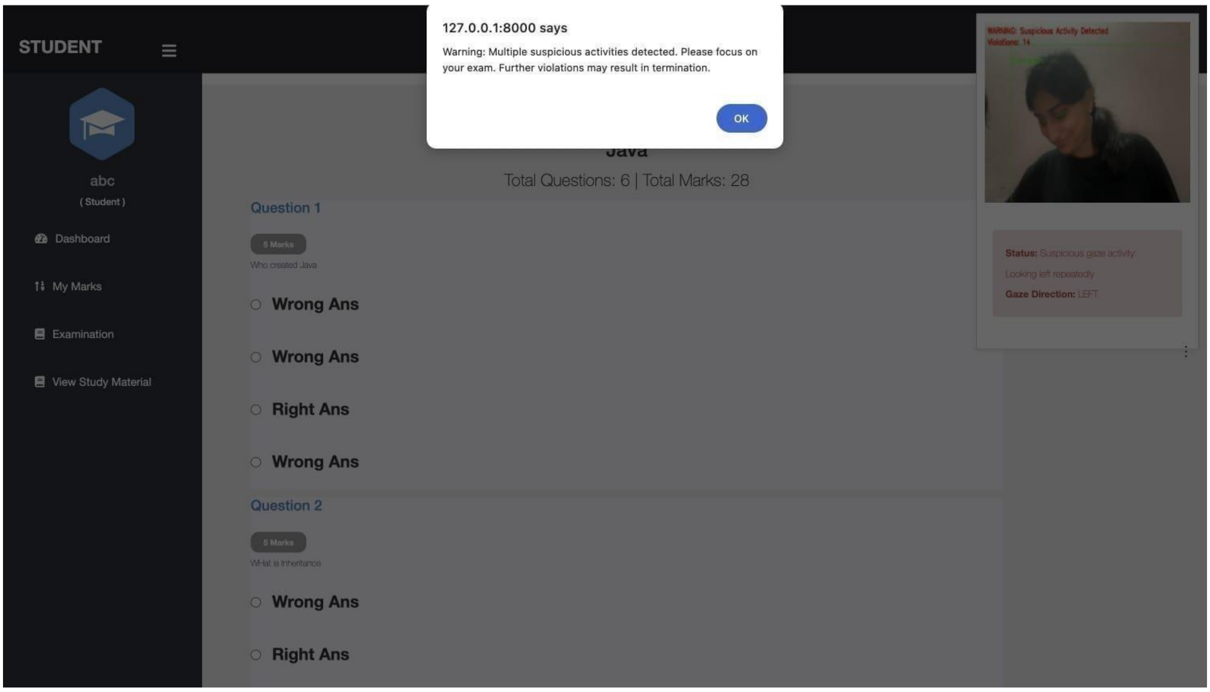

Figure A.4: Violation detected when looking down

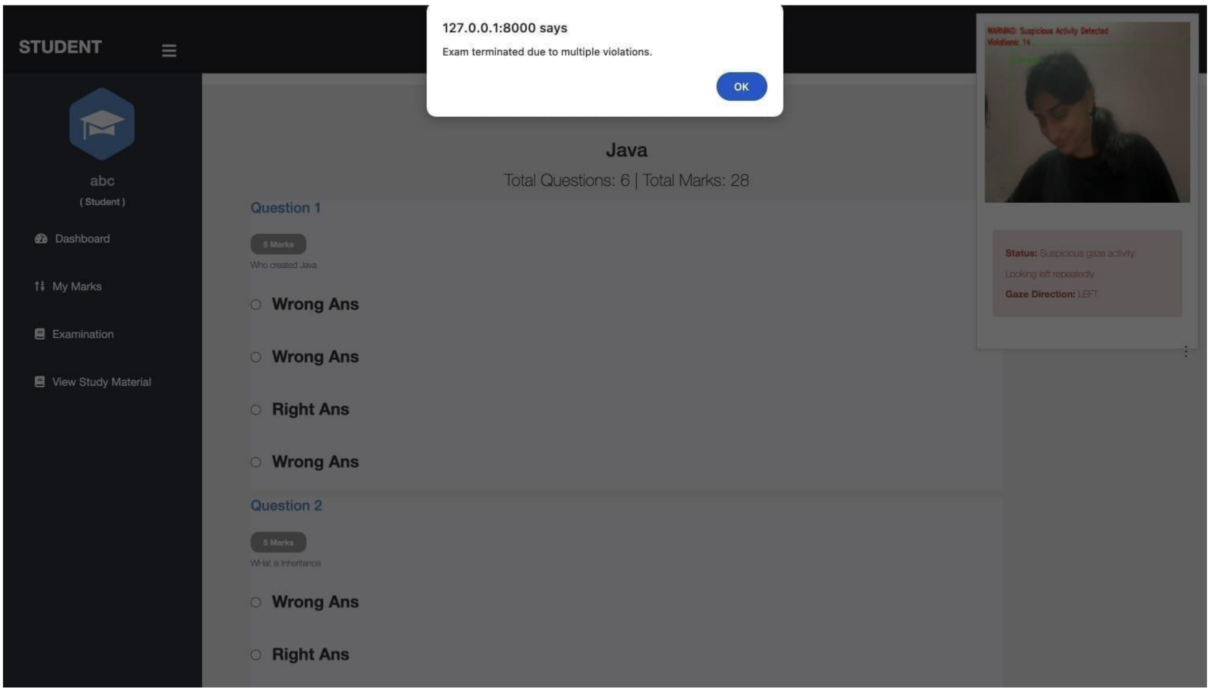

Figure A.5: Exam terminated when more than 3 violations detected

References

1. 2022 – Shashikala, J. M. and Nagesh, P. V., *A Smart Proctoring System Using Artificial Intelligence*, in Proc. Int. Conf. Artificial Intelligence and Data Engineering (AIDE), Bangalore, India, pp. 123–128. doi: 10.1109/AIDE54550.2022.00024.

2. 2020 – Pham, T. D. and Goodwin, J. N., *Facial Recognition for Remote Examination Proctoring: A Comparative Study*, IEEE Access, vol. 8, pp. 174302–174315. doi: 10.1109/ACCESS.2020.3015538.

3. 2021 – Kumar, A. et al., *AI-Based Gaze Detection for Online Exam Monitoring*, Journal of Computational Intelligence Systems, vol. 14, no. 3, pp. 45–58. doi: 10.1016/j.cisys.2021.10.005.

4. 2021 – Gupta, S., Malhotra, R. and Joshi, A., *Enhancing Academic Integrity Using Machine Learning for Anomaly Detection in Online Exams*, IEEE Transactions on Learning Technologies, vol. 14, no. 4, pp. 441–453. doi: 10.1109/TLT.2021.3099432.

5. 2022 – Zhang, X., Luo, C. and Zhou, Y., *An Efficient AI-Driven Approach for Online Examination Systems*, in Proc. Int. Conf. Computing and Communications (ICCC), Chengdu, China, pp. 239–245. doi: 10.1109/ICCC55683.2022.00040.

6. 2021 – Singh, M. and Bhatia, P., *Anomaly Detection in Online Assessments Using Machine Learning*, International Journal of Advanced Computer Science and Applications (IJACSA), vol. 12, no. 6, pp. 301–309. doi: 10.14569/IJACSA.2021.0120637.

7. 2021 – Jaiswal, R., Banerjee, T. and Sarkar, S., *Gaze Estimation Techniques for AI Proctoring: A Comprehensive Survey*, IEEE Access, vol. 9, pp. 117012–117029. doi: 10.1109/ACCESS.2021.3101763.

8. 2021 – Lee, K., Kim, Y. and Park, S., *AI-Powered Question Generation for Online Exams: Techniques and Applications*, Journal of Intelligent Information Systems, vol. 16, no. 2, pp. 145–162. doi: 10.1007/s10844-021-006.

9. 2022 – Patel, R. and Sharma, V., *Real-Time Eye Movement Tracking for Secure Remote Assessments Using Deep Learning*, ACM Transactions on Interactive Intelligent Systems, vol. 11, no. 4, pp. 1–18. doi: 10.1145/3492312.

10. 2022 – Chen, L., Wang, H. and Li, Q., *A Hybrid Framework for Cheating Behavior Detection in Online Exams Using Multi-Modal Data*, Expert Systems with Applications, vol. 199, p. 117154. doi: 10.1016/j.eswa.2022.117154.

14% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

- **72** Not Cited or Quoted 14%
  Matches with neither in-text citation nor quotation marks
- **0** Missing Quotations 0%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

10% Internet sources

3% Publications

12% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.