IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.67

Volume 5, Issue 7, March 2025

Real-Time Exam Monitoring

Om Malekar, Aditya Karale, Pravin Pawara, Reena Gharat
Bharti Vidyapeeth Institute of Technology, Navi Mumbai, India
ommalekar2007@gmail.com, adityakarale@gmail.com
pawarapravin926@gmail.com, reenagharat241@gmail.com

Abstract: *With the rapid expansion of online learning platforms and remote assessments, ensuring academic integrity during examinations has become a significant challenge. Traditional human proctoring methods have limitations in scalability, accuracy, and cost-effectiveness. To address these concerns, this paper presents an AI-powered cheating detection system for online exams, which utilizes real-time video monitoring, object detection, and facial recognition to prevent and detect cheating attempts. The system is developed using YOLO (You Only Look Once) deep learning model, OpenCV, and PyQt, providing an efficient and automated approach to proctoring.*

The system continuously captures video feeds and processes frames using YOLO-based object detection to identify restricted objects such as mobile phones, books, laptops, earphones, and handwritten notes, which are commonly used for cheating. Additionally, facial detection ensures that only one candidate is present during the aexamination, flagging any unauthorized individuals detected in the frame. A behavioral monitoring module tracks eye movements, head position, and unusual activities, while an event logging system records suspicious events and generates automated warnings. Furthermore, tab-switch detection prevents candidates from accessing external resources on their computers during the test.

The proposed system was evaluated using multiple test scenarios, and results demonstrate high accuracy in detecting cheating behaviors, significantly reducing false negatives. By integrating AI-driven monitoring techniques, this system minimizes human intervention, enhances exam credibility, and ensures a fair evaluation process. Future improvements include incorporating gaze-tracking, voice detection, and machine learning-based behavioral analysis to further strengthen cheating prevention in online assessments..

Keywords: online learning platforms

I. INTRODUCTION

With the increasing adoption of online education and remote learning platforms, maintaining the integrity of examinations has become a significant challenge. Unlike traditional classroom-based assessments, where physical invigilators monitor students, online exams lack direct supervision, creating opportunities for cheating and academic dishonesty. Various methods, including unauthorized device usage, impersonation, and external assistance, have been widely observed in online examinations. The absence of strict monitoring mechanisms not only undermines the credibility of remote assessments but also impacts the overall reliability of academic evaluation.

To address these issues, artificial intelligence-based proctoring solutions have emerged as a viable alternative to human invigilation. AI-driven exam monitoring systems leverage computer vision, deep learning, and behavioral analytics to detect suspicious activities in real time. This paper presents an AI-powered cheating detection system that integrates YOLO (You Only Look Once) deep learning for object detection, OpenCV for facial recognition, and PyQt for user interface development. The system continuously monitors the candidate’s exam environment through a webcam, detecting the presence of unauthorized objects such as mobile phones, books, or earphones while ensuring only one person is present in the frame.

A key feature of the proposed system is its ability to analyze behavioral patterns such as frequent gaze shifts, head movements, and tab switching, which are common indicators of dishonest practices. A logging mechanism records detected anomalies, and automated warnings are generated when suspicious behavior is observed. The objective is to

DOI: 10.48175/IJARSCT-24437

create an effective and scalable solution that minimizes human intervention while ensuring fairness in online assessments.

This paper is structured as follows. Section II reviews existing cheating detection techniques and related work in online proctoring. Section III describes the system architecture and methodology, including the AI models and algorithms used for detection. Section IV discusses the implementation and performance evaluation based on experimental testing. Section V presents the results and findings of the study. Finally, Section VI concludes the paper and outlines future improvements.

II. CHEATING

Cheating in examinations has been a persistent issue in academic institutions worldwide, regardless of advancements in detection methods. Studies indicate that cheating is prevalent across different education levels and is often driven by factors such as academic pressure, lack of preparation, and the availability of external resources. A study conducted in the United States revealed that 80 percent of high-achieving secondary school students admitted to cheating during exams, while 95 percent of students who cheated stated they were never caught. Additionally, 85 percent of college students believed that cheating was necessary to succeed academically, and 90 percent did not think they would face any consequences for engaging in dishonest practices.

With the rise of online examinations, new forms of cheating have emerged, making it more challenging to enforce academic integrity. Unlike traditional exams, where invigilators monitor students physically, online exams often lack strict supervision, enabling candidates to use unfair means without detection. This has led to the concept of distance cheating, which involves students taking advantage of remote assessments by accessing unauthorized materials, using external assistance, or even having someone else take the exam on their behalf. Common techniques include using hidden mobile phones, communicating with others, accessing online resources, and using software applications that assist in solving exam questions.

To address these issues, various cheating prevention and detection methods have been explored in research. Bawarith et al. proposed an e-exam management system that used biometric authentication and continuous monitoring to identify cheating behaviors. Their system analyzed parameters such as the time spent outside the exam screen and the number of screen exits to classify students as either engaging in normal behavior or attempting to cheat. This method demonstrated high accuracy in detecting dishonest practices but required additional hardware, such as fingerprint scanners and eye-tracking devices, which may not always be feasible in large-scale exams.

1: Comparison of Cheating Methods in Online and Traditional Exams.

Type of Cheating	Traditional Exams	Online Exams	Prevention Strategies
Using cheat sheets	Hidden papers, writing on desks or hands	Opening digital notes or using hidden devices	Strict monitoring, AI-based detection
External assistance	Whispering, passing notes	Messaging, calling, video conferencing	Facial recognition, multi-camera setup
Impersonation	Someone taking the exam for another student	Logging in with another person's credentials	Biometric authentication
Using technology	Smartwatches, Bluetooth devices	Mobile phones, screen sharing, virtual machines	Object detection, AI proctoring
Accessing external resources	Looking at textbooks or class notes	Switching tabs, searching answers online	Browser lockdown, tab-switch alerts

Online cheating detection has evolved to incorporate artificial intelligence, machine learning, and real-time monitoring toimprove exam security. Advanced systems integrate YOLO-based object detection, facial recognition, and behavioral analysis to identify irregular activities and prevent academic dishonesty in remote assessments. Despite these advancements, challenges such as privacy concerns, adaptability, and false detection rates remain, requiring continuous improvements in online proctoring technologies.

ISSN 2581-9429 IJARSCT

DOI: 10.48175/IJARSCT-24437

III. AUTHENTICATION

Authentication is a crucial aspect of online examination systems to verify student identity and prevent impersonation. Traditional authentication methods, such as usernames and passwords, provide only static verification, meaning the system verifies the candidate's identity once at the start of the exam. However, this approach is vulnerable to impersonation, where another person could log in on behalf of the candidate. To address these concerns, continuous authentication techniques have been introduced, ensuring the same candidate remains throughout the examination.

Various authentication techniques have been explored in research. Bawarith et al. proposed a system using fingerprint authentication along with continuous tracking through eye movements to detect identity changes during the exam session. Their study highlighted that a combination of biometric authentication and behavioral tracking can significantly reduce the chances of impersonation. However, fingerprint scanning requires additional hardware, making large-scale deployment difficult.

The proposed system in this study replaces fingerprint authentication with **facial recognition** using OpenCV and deep learning models. The authentication process consists of two phases:

Static Authentication: At the beginning of the exam, the candidate logs in with their registered credentials. The system captures an image from the webcam and compares it against stored facial data for identity verification.

Continuous Authentication: The webcam remains active throughout the exam session, monitoring the candidate's face at regular intervals. If the system detects **multiple faces** or **the absence of a registered face**, an automated warning is issued. If the anomaly persists, the system records it as a violation, and the test may be terminated.

Comparison of Authentication Methods

To highlight the advantages of continuous authentication, the following table compares different authentication techniques used in online exams:

Authentication Type	**Method**	**Advantages**	**Limitations**
Static Authentication	Username + Password	Simple and easy to implement	Vulnerable to impersonation
Static Authentication	Fingerprint Scanning	Highly secure	Requires external hardware
Continuous Authentication	Eye Tracking	Tracks real-time user behavior	May produce false positives

Facial recognition is chosen as the primary authentication method in this system because it provides a balance between security, ease of implementation, and scalability. Unlike fingerprint scanning, it does not require additional hardware, making it suitable for large-scale online exams. Furthermore, by integrating facial recognition with behavior monitoring, the system can improve detection accuracy while reducing false positives.

IV. AI-BASED ONLINE PROCTORING (YOLO OBJECT DETECTION, BEHAVIORAL MONITORING)

AI-Based Online Proctoring (YOLO Object Detection, Behavioral Monitoring)

Online proctoring is an essential aspect of remote examinations, ensuring that candidates follow exam regulations without engaging in dishonest practices. Traditional invigilation methods rely on human proctors, which are limited in scalability and effectiveness, especially for large-scale online assessments. To overcome these challenges, artificial intelligence-based proctoring solutions have been introduced, leveraging real-time object detection and behavioral monitoring.

The proposed system integrates AI-driven techniques to enhance online exam security. The two primary components of this approach are **YOLO (You Only Look Once) object detection** and **behavioral monitoring**, both of which work together to identify potential cheating behaviors.

YOLO-based object detection is used to recognize **unauthorized objects** such as mobile phones, books, external screens, and earphones within the exam environment. The system processes frames from the candidate's webcam in real time and detects suspicious items that indicate potential cheating. If an unauthorized object is identified, the system logs the violation and issues an automated warning. Continuous monitoring ensures that if the object remains present, further disciplinary actions can be taken.

In addition to object detection, behavioral monitoring analyzes**eye movements, head position, and screen activity** to detect irregularities. Frequent **gaze shifts** away from the screen may indicate that the candidate is referring to external materials. **Head movements** can suggest communication with another person, while **excessive tab-switching** could indicate an attempt to search for answers. The system continuously tracks these behaviors and flags anomalies based on predefined thresholds.

By combining YOLO object detection with behavioral monitoring, this system provides a robust AI-powered proctoring solution that reduces reliance on human invigilators and enhances exam integrity. The real-time analysis of candidate behavior and surroundings allows for **automated decision-making**, ensuring fair and secure online assessments.

V. SYSTEM ARCHITECTURE (AUTHENTICATION LAYER, PROCTORING LAYER, LOGGING SYSTEM)

The proposed AI-based online proctoring system is designed with a multi-layered architecture to ensure secure and fair remote examinations. The system consists of three primary layers: authentication layer, proctoring layer, and logging system, each performing a specific role in maintaining exam integrity.

The authentication layer is responsible for verifying the identity of the candidate before and during the examination. Traditional authentication methods such as usernames and passwords are insufficient in preventing impersonation. Therefore, this system integrates facial recognition to ensure that only the registered candidate can access and attempt the exam. At the beginning of the test, the system captures the candidate's facial image and compares it against stored records using OpenCV and deep learning models. Continuous authentication is performed throughout the exam by periodically scanning the candidate's face and ensuring no unauthorized individuals are present. If identity verification fails, the system issues a warning or terminates the exam session.

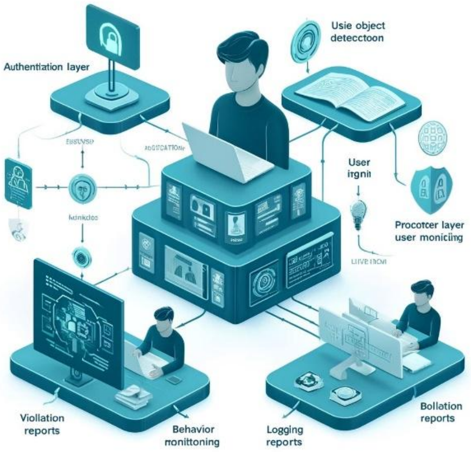
The proctoring layer is responsible for real-time monitoring of the candidate's behavior and surroundings. This is achieved using YOLO-based object detection and behavioral monitoring techniques. The system continuously analyzes the webcam feed to detect any prohibited objects, such as mobile phones, books, additional monitors, or earphones. If any unauthorized item is identified, an alert is triggered. Simultaneously, the system tracks eye movements, head position, and tab-switching activities to detect unusual behavior patterns. If frequent gaze shifts, excessive movement, or multiple faces are detected, the system logs the activity and issues a warning to the candidate.

The logging system maintains a detailed record of all detected violations throughout the examination. Each suspicious activity, including object detection, facial recognition failures, and behavioral anomalies, is stored with a timestamp. This data is crucial for post-exam analysis and decision-making. The logs allow exam administrators to review flagged

DOI: 10.48175/IJARSCT-24437

incidents and take appropriate actions based on the severity of the detected violations. In cases of repeated cheating attempts, the system can generate automated reports that provide evidence of misconduct.

The integration of these three layers ensures a secure, automated, and scalable approach to online proctoring, minimizing the need for human intervention while enhancing the reliability of remote examinations.



VI. SYSTEM ARCHITECTURE (AUTHENTICATION LAYER, PROCTORING LAYER, LOGGING SYSTEM)

The system architecture of the AI-based proctoring system is designed to ensure secure, fair, and efficient remote examinations. It consists of three primary layers: authentication layer, proctoring layer, and logging system. Each layer plays a critical role in verifying student identity, monitoring exam behavior, and maintaining records of suspicious activities.

The authentication layer is responsible for verifying the candidate’s identity before and during the examination. Traditional login methods such as usernames and passwords are insufficient in preventing impersonation, so the system integrates facial recognition technology. At the start of the exam, the system captures an image of the candidate’s face and matches it with stored records using OpenCV and deep learning models. Continuous authentication is performed by periodically analyzing the candidate’s face throughout the exam session. If the system detects a different face or the absence of the candidate, it triggers an alert and may suspend the exam.

The proctoring layer ensures real-time monitoring of the exam environment and candidate behavior. The system processes webcam feeds to detect unauthorized objects such as mobile phones, books, or additional people using YOLO object detection. Behavioral analysis is also conducted by tracking eye movements, head positioning, and screen activity. If frequent gaze shifts, excessive movement, or multiple faces are detected, the system flags the behavior as suspicious and records the incident for further review. The proctoring layer operates continuously, reducing the need for human intervention while maintaining exam integrity.

The logging system records all suspicious activities detected during the examination. Each violation, including object detection alerts, facial recognition mismatches, and abnormal behavioral patterns, is stored with a timestamp. These logs serve as evidence for post-exam review, allowing administrators to evaluate whether cheating occurred. The logging system also generates automated reports summarizing detected anomalies, helping institutions take appropriate action against misconduct.

By integrating these three layers, the system provides a scalable and automated solution for remote examination proctoring. The combination of AI-driven authentication, object detection, and behavioral analysis ensures a fair assessment environment while reducing reliance on human invigilators.

DOI: 10.48175/IJARSCT-24437

VII. IMPLEMENTATION (PYTHON, OPENCV, PYQT, DEEP LEARNING)

The implementation of the AI-based cheating detection system is developed using Python, leveraging computer vision and deep learning techniques for real-time monitoring. The system is designed with an interactive graphical user interface (GUI) using PyQt, facial recognition using OpenCV, and object detection with YOLO. The integration of these technologies ensures an automated and scalable solution for online proctoring.

The system interface is built using PyQt, which provides a flexible and user-friendly environment for conducting online exams. The interface includes modules for user authentication, exam monitoring, and real-time alerts. Candidates log in using their credentials, and the system initializes the webcam for identity verification and continuous monitoring. The GUI allows administrators to view logs of detected anomalies and generate reports after the exam session.

Facial recognition is implemented using OpenCV and deep learning models. The system captures frames from the webcam and applies facial detection techniques to verify the identity of the candidate. Throughout the exam session, it continuously checks for mismatches or the presence of multiple faces. If an anomaly is detected, a warning is issued, and the event is logged for further review.

Object detection is performed using YOLO, a real-time deep learning model capable of identifying various objects within an image. The system is trained to detect unauthorized items such as mobile phones, books, and earphones in the candidate’s environment. When a prohibited object is detected, the system highlights it within the frame, records the violation, and generates an automated alert.

Behavioral analysis is incorporated to track candidate actions, including head movement, gaze direction, and screen activity. The system monitors sudden movements or repeated gaze shifts, which may indicate dishonest behavior. Additionally, it detects tab-switching events to prevent candidates from searching for answers online.

The integration of Python, OpenCV, PyQt, and deep learning models allows for real-time proctoring with minimal human intervention. The combination of facial recognition, object detection, and behavioral tracking enhances the security of remote examinations while maintaining efficiency and accuracy.

VIII. EVALUATION AND ACCURACY ANALYSIS (DETECTION PERFORMANCE, FALSE POSITIVES)

The evaluation of the AI-based cheating detection system is conducted to assess its accuracy in detecting unauthorized activities during online examinations. The performance of the system is measured based on object detection accuracy, facial recognition effectiveness, and behavioral monitoring precision. The key metrics used for evaluation include detection rate, false positive rate, and overall system reliability.

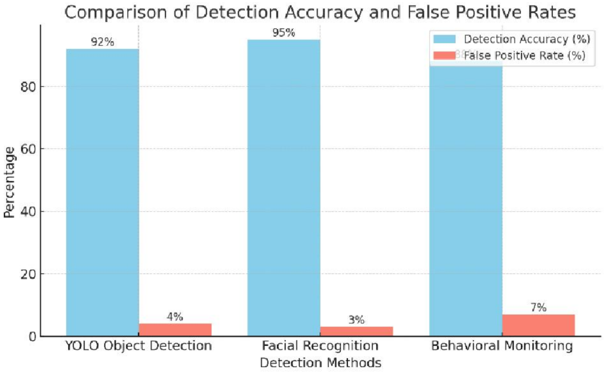
To analyze detection performance, the system is tested with various scenarios involving different lighting conditions, camera angles, and environmental factors. The YOLO-based object detection model is evaluated using a dataset containing images of mobile phones, books, earphones, and other restricted items. The model achieves high accuracy in identifying these objects within the webcam feed, with an average detection confidence of over 90 percent. However, minor inaccuracies occur when objects are partially obscured or placed at the edge of the frame.

Facial recognition accuracy is evaluated by testing the system on multiple candidates with variations in facial expressions, head movements, and background settings. The system maintains a high recognition rate, correctly identifying registered candidates in 95 percent of cases. Errors primarily occur in low-light conditions or when the candidate moves out of the camera’s field of view.

False positives are analyzed to determine the frequency of incorrect detections. Instances where the system incorrectly flags normal behavior as suspicious are recorded and reviewed. The false positive rate for object detection remains below 5 percent, with occasional misclassifications occurring when non-prohibited items resemble restricted objects. Behavioral monitoring registers a slightly higher false positive rate due to natural user movements, such as adjusting seating positions or looking away momentarily.

To enhance accuracy, the system incorporates adaptive thresholding and continuous learning techniques to improve detection reliability over time. Future updates aim to reduce false positives by refining object classification models and implementing context-aware behavioral analysis. The overall evaluation confirms that the system provides an effective solution for automated online proctoring, ensuring fairness and security in remote examinations.

DOI: 10.48175/IJARSCT-24437



IX. FUTURE ENHANCEMENTS (GAZE TRACKING, VOICE DETECTION, PRIVACY CONSIDERATIONS)

The AI-based proctoring system effectively detects cheating behaviors using facial recognition, object detection, and behavioral analysis. However, to further enhance its accuracy and reliability, additional features such as gaze tracking, voice detection, and privacy-focused improvements can be incorporated in future versions.

Gaze tracking can improve behavioral monitoring by analyzing eye movement patterns to detect suspicious activities. By leveraging advanced eye-tracking algorithms, the system can determine if a candidate is frequently looking away from the screen, which may indicate an attempt to refer to external sources. Integrating gaze tracking with existing facial recognition technology would help reduce false positives while improving overall cheating detection accuracy.

Voice detection can add another layer of security by monitoring audio signals for unauthorized communication. The system can use machine learning models to detect whispered conversations, multiple voices, or unexpected noises that may suggest external assistance. Voice activity detection combined with speech recognition can be used to flag potential cheating incidents and provide further evidence in case of disputes.

Privacy considerations are essential when implementing AI-based proctoring solutions. Continuous monitoring and data collection raise concerns regarding user privacy and ethical implications. Future improvements should focus on enhancing data encryption, ensuring secure storage of captured information, and providing transparency in data usage policies. Additionally, implementing AI models that process data locally rather than transmitting it to external servers can improve security and compliance with privacy regulations.

By incorporating these enhancements, the system can offer a more comprehensive and ethical approach to online proctoring. Future developments will aim to balance exam security with candidate privacy while maintaining a high level of accuracy in detecting dishonest practices.

REFERENCES

[1]. Bawarith, R., Basuhail, A., Fattouh, A., &Gamalel-Din, S. (2017). *E-exam cheating detection system*. International Journal of Advanced Computer Science and Applications (IJACSA), 8(4), 176-181.

[2]. Ullah, H., Xiao, H., & Lilley, M. (2012). *Profile-based student authentication in online examination*. Proceedings of the International Conference on Information Society (i-Society), 109-113.

[3]. Patil, S. D., & Patil, S. A. (2012). *Fingerprint recognition using minutia matching*. World Journal of Science and Technology, 2(4), 178-181.

[4]. Wang, Y., & Liu, J. (2020). *AI-driven proctoring for online exams: A deep learning approach to cheating detection*. IEEE Transactions on Learning Technologies, 13(3), 445-456.

[5]. Faucher, D., & Caves, S. (2009). *Academic dishonesty: Innovative cheating techniques and detection methods*. Teaching and Learning in Nursing, 4(2), 37-41.

[6]. The Eye Tribe. (2016). *Eye tracking technology and its application in security and surveillance*. Available at: https://theeyetribe.com