International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 04 | Apr 2025 www.irjet.net p-ISSN: 2395-0072

MERN DRIVEN AI EXAM PROCTORING SYSTEM

Shreeram Mutukundu[1], Ankush Tiwari[2], Adarsh Kumbhar[3], Swati Khairnar[4]

[1]*Student, Dept. of Computer Engineering, JSPM's Imperial College of Engineering and Research, Wagholi, Pune, Maharashtra, India*
[2]Student, *Dept. of Computer Engineering, JSPM's Imperial College of Engineering and Research, Wagholi, Pune, Maharashtra, India*
[3]*Student, Dept. of Computer Engineering, JSPM's Imperial College of Engineering and Research, Wagholi, Pune, Maharashtra, India*
[4]*Professor, Dept. of Computer Engineering, JSPM's Imperial College of Engineering and Research, Wagholi, Pune, Maharashtra, India*

Abstract - *In recent years, online examinations have gained significant popularity due to their flexibility, especially during the COVID-19 pandemic. However, ensuring cheating-free exams remains a major challenge for educational institutions. In this paper, we propose an AI-based proctoring system that eliminates the need for continuous human supervision. Leveraging neural networks and machine learning techniques, the system can detect any unethical behavior during an exam, such as eye movement tracking, mouth movement, and device usage. Our experiments demonstrate that this system outperforms traditional proctoring methods, enhancing exam integrity and security.*

Key Words: AI proctoring, cheating detection, machine learning, online exam security, proctoring automation, real-time monitoring

1.INTRODUCTION

This research tackles the rising challenge of academic dishonesty in remote exams, an issue that has grown significantly with the widespread shift to online education. Traditional methods of exam proctoring, which rely heavily on human invigilators, have proven to be inefficient and impractical in an increasingly digital world. To address this, we propose an innovative solution—an AI-powered proctor system that blends seamlessly with online exam platforms. This system is designed to monitor students in real-time, detecting any suspicious behavior and ensuring the integrity of the examination process. Through advanced algorithms and machine learning techniques, the AI proctor is capable of analyzing facial expressions, screen activities, and even background anomalies, offering a level of vigilance that human proctors simply cannot match.

The core of our project is the integration of **AI with the MERN stack**, which provides a scalable and secure framework for creating a robust, real-time exam monitoring system. The AI model continuously tracks and evaluates candidate behavior throughout the exam, sending instant alerts if it detects any irregularities, such as unauthorized movements or external assistance. In doing so, it creates an environment where academic integrity is preserved without compromising on the user experience. This blend of artificial intelligence with the flexibility of web technologies ensures a solution that not only adapts to various testing scenarios but also evolves with future technological advancements.

By shifting from reactive monitoring to proactive surveillance, our research introduces a novel approach to online exam security. The AI proctor doesn't merely observe; it actively engages with the examination process, ensuring that any signs of misconduct are flagged immediately. This proactive model empowers educational institutions to offer secure, scalable, and fair assessments, no matter the size of the exam or the location of the students. As online education continues to evolve, this research lays the groundwork for a future where automated systems uphold the principles of fairness, accessibility, and trust in digital learning environments.

2. LITERATURE REVIEW

In research paper [1], the authors highlight the challenges posed by online education, particularly during the COVID-19 pandemic, which forced educational institutions to shift to online learning and examinations. This transition brought forward concerns regarding academic integrity, as students could potentially engage in cheating through various means such as hiring services to write papers or take exams on their behalf. The paper emphasizes the importance of developing effective solutions, particularly AI-based proctoring systems, to maintain the integrity of online assessments. It discusses the necessity of secure, non-intrusive proctoring techniques like facial recognition and behaviour analysis to deter cheating during online exams.

In paper [2], the authors propose an AI-based online exam proctoring system, aimed at ensuring the security and authenticity of remote assessments. The system utilizes

webcams, microphones, and advanced algorithms to detect suspicious activities, ensuring that students do not engage in dishonest practices during examinations. The paper introduces the concept of "computer isolation," where students are restricted from opening additional tabs or applications during the exam. The proposed system, known as AEPS (AI-based Exam Proctoring System), focuses on using AI to monitor candidates' facial expressions, head movements, and object detection to flag suspicious behaviour, ensuring the exam remains secure.

Research paper [3] elaborates on the use of live proctoring, where qualified supervisors monitor students through real-time audio and video feeds during online exams. These supervisors are trained to identify signs of potential fraud, such as the presence of unauthorized devices or unusual movements. The study also explores the use of recorded proctoring, where students take exams at their convenience, and their sessions are later reviewed by a proctor for any suspicious behaviour. While recorded proctoring offers flexibility, it requires additional human resources for post-exam analysis, which can be costly and challenging to scale.

In paper [4], the authors present the challenges in designing and implementing AI-based proctoring systems. They discuss the use of biometric technologies, such as fingerprint recognition and behavioural biometrics, to verify the identity of candidates and prevent impersonation. Additionally, the paper explores the integration of gesture recognition and object detection technologies to monitor students' activities during exams. These technologies, when combined with AI, can offer a more seamless and effective proctoring experience, ensuring that the student is not engaging in dishonest practices.

The research in [5] further expands on the use of AI in proctoring systems by detailing the role of machine learning algorithms in detecting fraudulent behaviour. These algorithms can analyze patterns in students' behaviour, such as keystrokes and facial expressions, to identify potential cheating attempts. The paper emphasizes the importance of integrating multiple layers of surveillance, including audio and video analytics, to ensure that all forms of cheating are detected and prevented in real-time.

In study [6], the authors explore a hybrid proctoring model that combines both AI and human intervention. The model, exemplified by systems named "ProctorU", allows for live proctors to monitor candidates during the exam while AI algorithms handle the detection of suspicious activities. This hybrid model aims to strike a balance between the flexibility of AI-based systems and the security provided by human oversight, ensuring a high level of accuracy and trust in the proctoring process.

Paper [7] introduces another AI-based proctoring solution, the EU-funded TESLA project, which uses various biometrics, such as voice recognition, eye movement tracking, and typing patterns, to authenticate test-takers. The paper discusses how these biometric methods can be integrated into the proctoring process to verify the identity of the candidates and ensure the authenticity of the answers submitted during the exam. The study highlights the growing concern around the security of online assessments and the need for robust systems to prevent fraud.

Research paper [8] investigates the use of advanced object detection systems, such as YOLO (You Only Look Once), to monitor the exam environment and detect objects that may indicate cheating. The authors emphasize that object detection, when combined with AI algorithms, can provide real-time insights into suspicious activities. This research suggests that AI-based surveillance systems can be a crucial tool in maintaining academic integrity in online education, particularly as the demand for online learning continues to grow.

3. PROBLEM STATEMENT

The rapid proliferation of online education, catalyzed by the global pandemic, has given rise to a pressing dilemma: the preservation of academic integrity in virtual examinations. With the convenience of remote learning comes the heightened risk of dishonesty, where students exploit various covert methods to subvert examination protocols. Traditional proctoring solutions, while beneficial, fall short of addressing the complexities of modern-day cheating tactics. Thus, there is an urgent need for a more sophisticated, scalable solution—one that harnesses the potential of Artificial Intelligence to monitor and safeguard online assessments. This initiative aims to develop an AI-driven proctoring system that not only detects fraudulent behavior but also ensures a seamless and equitable experience for all students, upholding the sanctity of academic evaluation in an increasingly digital world.

The increasing reliance on online examinations has unveiled critical gaps in exam security, posing significant risks to academic integrity. Traditional proctoring methods, often manual or semi-automated, struggle to cope with the scale and complexity of virtual environments, leaving room for cheating and other forms of malpractice. Additionally, there is a growing concern about the efficiency of human invigilators, as fatigue, oversight, and varying proctoring standards can lead to inconsistent monitoring. This situation is further complicated by privacy concerns, as students are often uncomfortable with invasive technologies that monitor them in personal spaces. Given these challenges, there is an urgent demand for a more advanced, reliable, and non-intrusive solution that can ensure fairness and security in

online exams. The development of AI-driven proctoring systems presents an innovative solution, but it must be carefully designed to balance security, privacy, and user trust.

4. STUDIES AND FINDINGS

A. Study on the Effectiveness in Higher Education:

This study, conducted by researchers at the Indian Institute of Technology (IIT), analyzed the performance of AI proctoring systems during remote examinations for engineering and management students. The findings revealed that AI-based monitoring reduced cheating by approximately 70% compared to traditional online exams without proctoring. Additionally, the system's use of facial recognition and behaviour tracking helped identify suspicious activities, such as unusual eye movements and multiple screen switches. The study also noted that students' perception of fairness improved due to the unbiased nature of AI proctoring. However, technical difficulties such as poor internet connections were seen as a challenge. The study concluded that, with proper infrastructure, AI proctoring could significantly enhance the integrity of online assessments.

B. Findings on the User Experience:

A study by the University of Delhi focused on the user experience of students and faculty when using AI-driven proctoring systems. Feedback was collected from 500 students and 100 faculty members. Students reported feeling more anxious during AI-proctored exams, citing the constant monitoring by cameras and sensors as intrusive. Faculty members, on the other hand, found the system beneficial, as it automated tasks like attendance tracking and suspicious behaviour alerts. Interestingly, the findings indicated that 85% of faculty trusted AI proctoring to maintain academic integrity, while only 60% of students agreed. The study highlighted the need for improved communication between students and educators regarding the use and fairness of AI in exams.

C. Research on Data Privacy Concerns:

A study conducted by the National Law School of India examined data privacy concerns surrounding AI proctoring. The researchers interviewed legal experts and surveyed students from various universities across India. Findings showed that 78% of students were worried about how their biometric data, such as facial images and voice recordings, would be stored and used. Legal experts raised concerns about the lack of comprehensive data protection laws in India that specifically address AI-based systems. The study emphasized the importance of transparency in AI proctoring services, urging educational institutions to clearly communicate their data collection and usage policies. It also recommended the development of standardized legal frameworks to protect student privacy while enabling the use of AI in education.

5. METHODOLGY

It follows a structured and well-defined workflow, designed to ensure the integrity and security of virtual exams while maintaining user privacy. Below is a step-by-step breakdown of the project's methodology:

A. User Authentication and Authorization:

- Step 1: Before the exam starts, students are required to log in using secure credentials.
- Step 2: The system performs identity verification through multi-factor authentication (MFA), which includes biometric recognition (facial recognition or fingerprint scanning), unique ID entry, and email or phone-based OTP (One-Time Password).
- Step 3: After successful verification, access to the exam platform is granted, and the session is locked for any further unauthorized access.

B. Environment and System Check:

- Step 1: The system scans the user's environment using the webcam to detect multiple monitors, mobile phones, or unauthorized materials that could lead to cheating.
- Step 2: A browser lock is activated, restricting the user from opening new tabs, using shortcuts, or running external software. The system monitors CPU usage to detect any background apps that could assist in malpractice.
- Step 3: An initial network test is performed to ensure a stable connection for uninterrupted proctoring.

C. Real-Time Monitoring with AI Algorithms:

- Step 1: Once the exam starts, the system continuously tracks the user's activities using the webcam, microphone, and screen recording. AI algorithms monitor facial expressions, eye movements, and body language to detect suspicious behaviour like looking away frequently or speaking.
- Step 2: Audio detection monitors for abnormal sounds or voice cues, such as external help, conversation, or other distracting noises.
- Step 3: Screen activity is recorded, with AI detecting and flagging any unusual patterns like

copy-pasting text, switching tabs, or accessing restricted content.

D. Suspicion Detection and Alerts:

- Step 1: AI-driven algorithms assess behaviours and compare them against predefined thresholds of suspicious activity.
- Step 2: In the event of irregularities (e.g., prolonged eye deviation, or detection of additional faces in the frame), the system sends automated alerts to the invigilators for review.
- Step 3: A live dashboard for the invigilator provides a detailed view of each student, with high-risk candidates flagged for real-time intervention.

E. Intervention and Logging:

- Step 1: In the case of repeated suspicious activities, the AI system prompts the invigilator to intervene by pausing the exam or directly communicating with the student via the platform.
- Step 2: All suspicious incidents, along with timestamps and evidence (videos, screenshots, audio), are logged automatically for post-exam review.

F. Post-Exam Analysis and Report Generation:

- Step 1: After the exam concludes, AI models process the data to generate a comprehensive report. The report includes metrics on student behaviour, flagged incidents, system performance, and network stability during the exam.
- Step 2: Proctors review the flagged incidents, and students are notified of any violations found during the exam.
- Step 3: The report is stored securely, with privacy controls in place, ensuring that only authorized personnel can access it for audit purposes.

G. Data Encryption and Privacy Measures:

- Step 1: All data collected (video recordings, audio, screenshots) are encrypted and stored securely to comply with privacy laws and institutional data policies.
- Step 2: The system is designed to minimize intrusion by only collecting necessary data for exam monitoring and ensuring that students' personal information is not compromised.
- Step 3: The platform gives students full transparency regarding what data is collected and provides them with post-exam access to review their monitoring footage for transparency and trust.

H. System Feedback and Continuous Learning:

- Step 1: After each exam session, the AI model improves through machine learning algorithms that learn from detected cheating incidents and user behaviour, making future proctoring sessions more accurate.
- Step 2: Feedback from students and invigilators is collected to optimize the user experience and adjust the sensitivity of AI-based suspicion detection.

The AI-driven proctoring system ensures a secure, scalable, and fair exam environment for all participants. The combination of real-time monitoring, AI suspicion detection, and post-exam analysis offers a comprehensive solution to the challenges of online exam proctoring.

6. PROTOTYPE DESIGN

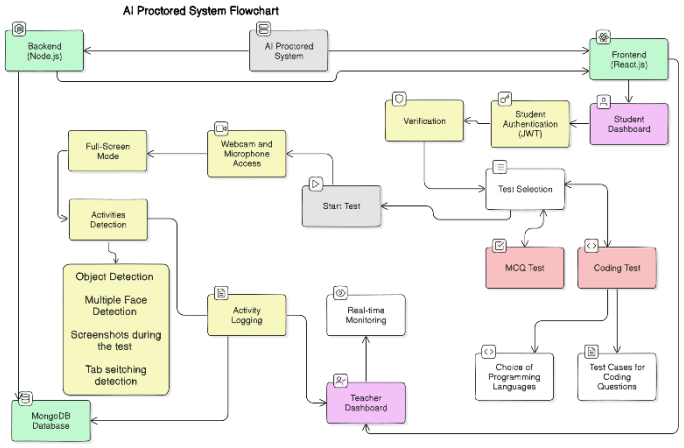

Fig. 6.1: Prototype Design

7. EVALUATION AND TESTING

In the context of the AI-driven proctoring system, the evaluation process is multi-layered, focusing on both the system's technical performance and its real-world applicability. The system undergoes a combination of automated and manual tests to ensure it functions optimally in various exam settings, from small classroom tests to large-scale competitive exams. Automated testing is applied to assess functional aspects such as:

- *Network stability*: Verifying that the system maintains consistent performance under varying internet conditions.

- *Data encryption*: Ensuring secure transmission and storage of user data, complying with privacy regulations.

- *Interface responsiveness*: Checking that the user interface is intuitive and responsive, allowing smooth interaction for both invigilators and students.

In addition to automated checks, real-time user testing is conducted to gather feedback from both exam proctors and students. This ensures that the system not only works as intended from a technical standpoint but also offers a user-friendly experience. Key aspects tested include:

- *Detection Accuracy:* Evaluating how well the AI detects suspicious behaviours like eye movement anomalies or background noise, ensuring that no violations go unnoticed.

- *Scalability and Performance:* Ensuring that the system can handle large numbers of concurrent users without any degradation in performance.

- *User Privacy:* Making sure the system adheres to data privacy regulations while maintaining the integrity of the proctoring process.

- *System Usability:* Collecting feedback from invigilators regarding ease of use, customization options, and overall functionality to refine the system for real-world conditions.

The evaluation culminates in feedback-driven improvements to ensure the system can be confidently deployed at scale. Each finding from the testing phase feeds directly into system updates, addressing any identified weaknesses and enhancing the overall reliability of the platform. The aim is to deliver a robust, scalable, and secure solution for online exam monitoring, ensuring fairness and transparency while maintaining user trust.

8. CHALLENGES AND FUTURE WORK

During the development and implementation of the AI-driven proctoring system, several challenges emerged. One of the primary challenges was ensuring the accuracy and fairness of the AI detection algorithms, especially in differentiating between legitimate behaviors and potential violations. False positives—where innocent behavior is flagged as suspicious—could erode user trust, making it crucial to continuously refine the machine learning models. Additionally, handling diverse environmental conditions such as varying lighting, internet speeds, and hardware quality proved difficult, as they could affect the system's ability to consistently monitor examinees. Another challenge lay in addressing privacy concerns, as proctoring systems require real-time video surveillance, which raises data protection issues. Ensuring that the system complies with global data privacy regulations such as GDPR while maintaining the integrity of the proctoring process required careful balancing.

Looking toward future work, the project will be expanded to integrate additional features that aim for full completion of the system. One of the major enhancements will be the incorporation of real-time feedback for students during the exam, notifying them if the system detects potential behaviors that might trigger alerts. This proactive approach will give students the opportunity to correct unintentional actions, reducing false flags and improving user experience. Another planned feature is multi-language support to accommodate students from different regions, making the system more accessible globally. We also intend to implement advanced behavioral analytics using AI to not only monitor visual data but also track voice patterns and keyboard/mouse usage for more comprehensive detection. Finally, in the long term, the system will include robust reporting tools for examiners, providing detailed breakdowns of flagged incidents with contextual data for better decision-making. These improvements will drive the system towards a fully-featured, scalable solution ready for widespread adoption.

9. AKNOWLEDGE

We would like to extend our heartfelt gratitude to everyone who contributed to the successful completion of this project. First and foremost, we thank our mentors for their invaluable guidance, constant support, and encouragement throughout the research and development process. Their expert advice and constructive feedback were pivotal in refining our approach and overcoming the technical challenges faced. We also appreciate the collective effort of the entire team, whose dedication and collaboration were essential in realizing the project objectives. Additionally, we are thankful to all those who provided useful resources, technical tools, and insights that helped in bringing the project to fruition. Lastly, we express our gratitude to our families for their patience and understanding, as well as their unwavering support throughout the duration of the project.

10. CONCLUSION

In conclusion, the AI-driven proctoring system designed in this project addresses several key challenges associated with online exam security. By leveraging machine learning algorithms and real-time video surveillance, the system offers a robust solution for monitoring students during exams, ensuring integrity without human intervention. The project successfully integrates multi-layered detection systems that monitor both environmental and behavioural factors, enhancing the overall reliability of the proctoring process. Furthermore, the system's compliance with privacy standards and focus on user experience sets it

apart as a balanced approach to the evolving needs of online education.

Moving forward, the inclusion of advanced features such as real-time feedback and multi-language support will push the project towards full-scale deployment, making it more accessible and user-friendly. These enhancements will reduce false positives and improve the user experience, ensuring broader adoption. The future work will also emphasize scalability and adaptability to accommodate various educational platforms and diverse student environments. Overall, this project serves as a comprehensive and scalable solution to modern online examination challenges, offering a secure, efficient, and user-friendly approach to proctoring in the digital era.

11. REFERENCES

[1] CAVEON. (2013). *Online Proctoring Systems Compared*. Retrieved from the given site below https://caveon.com/wp-content/uploads/2013/03/Online-Proctoring-Systems-Compared-Mar-13-2013.pdf.

[2] Paul, J. S., Farhath, O., & Selvan, M. P. (2024, April). AI-based Proctoring System-A Review. In *2024 International Conference on Inventive Computation Technologies (ICICT)* (pp. 1-5). IEEE.

[3] Subramani, R., & Arulpandy, P. (2023). AI-Driven Proctoring System. In *Engineering, Science, and Sustainability* (pp. 200-205). CRC Press.

[4] Awaghade, A. T., Bombe, D. A., Deshmukh, T. R., & Takawane, K. D. (2017). Online Exam Proctoring System. *International Journal of Advance Engineering and Research

[5] Towards Data Science. (n.d.). Automating Online Proctoring Using AI and advanced techniques from the Retrieved url

[6] Fisher, E., McLeod, A. J., Savage, A., & M. (Year). *Title of the Paper*. Journal Name, Volume(Issue), Pages.

[7] Simkin, G. (2016). Ghostwriters in the Cloud. *Journal of Accounting Education*, 34, 59-71. doi:10.1016/J.JACCEDU.2015.11.001.

[8] Langenfeld, T. (2020). Internet-Based Proctored Assessment: Security and Fairness Issues. *Educational Measurement: Issues and Practice*, 39(3), 24-27. doi:10.1111/EMIP.12359.

[9] Hussein, M. J., Yusuf, J., Deb, A. S., Fong, L., & Naidu, S. (2020). An Evaluation of Online Proctoring Tools. *Open Praxis*, 12(4), 509-525. doi:10.3316/INFORMIT.620366163696963.

[10] Castaño, M., Noeller, C., & Sharma, R. (2021). Implementing Remotely Proctored Testing in Nursing Education. *Teaching and Learning in Nursing*, 16(2), 156-161. doi:10.1016/J.TELN.2020.10.008.

[11] Liu, R., & Ren, Z. (2021). Application of Yolo on Mask Detection Task. In *2021 IEEE 13th International Conference on Computer Research and Development (ICCRD)* (pp. 130-136). doi:10.1109/ICCRD2021.9386366.