IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025

DOI: 10.17148/IJARCCE.2025.14544

PROCTOR-TOOL

Mungara Rahul Roll-No:20211CST0101[1], K.Chaitanya Roll-No:20211CST0027[2],

Mohammed Danish Manna Roll-No:20211CST0058[3],

Kondapalli Minith Reddy Roll-No:20211CST0028[4]

Dept. CST-AIML, Presidency university[1-4]

Abstract: The increasing adoption of online education has led to a growing need for secure and reliable examination systems. Traditional in-person examinations ensure integrity through physical invigilation, but with the rise of remote learning, maintaining exam security has become a significant challenge. Online exams are often vulnerable to cheating, impersonation, and unauthorized assistance, which undermines the credibility of assessments. Existing online examination systems employ manual proctor- ing, where human invigilators monitor students via webcams. However, this approach is labor-intensive, expensive, and sub- ject to human errors. To address these challenges, automated proctoring solutions have been introduced, integrating artificial intelligence (AI) and machine learning to detect suspicious behavior.

In this research, we present Proctor, an AI-based online proctoring system designed to ensure exam integrity through automated monitoring and real-time analysis. The system uses computer vision techniques to detect face absence, multiple peo- ple in the frame, mobile phone usage, and unauthorized objects. Additionally, it prevents tab switching, keyboard shortcuts, and right-click actions, further securing the examination process.

Proctor is designed to be efficient, scalable, and user-friendly, making online assessments more reliable without requiring hu- man invigilators. By leveraging advanced AI models, the system enhances security while reducing the administrative burden on educators. This research explores the need, implementation, and effectiveness of AI-based proctoring, offering a novel approach to securing online exams.

I. INTRODUCTION

With the rapid expansion of online education and remote learning, traditional methods of conducting examinations have undergone significant transformation. While online examina- tions provide flexibility and accessibility, they also introduce critical challenges related to security, integrity, and fairness. The absence of physical invigilation makes online exams more vulnerable to cheating, impersonation, and the use of unautho- rized resources. Ensuring a secure, fair, and credible online assessment environment has thus become a major concern for educational institutions and organizations conducting remote exams.

Existing online examination systems rely on manual proc- toring, where human invigilators monitor students via live webcam feeds. While this approach helps to some extent in preventing malpractice, it has several drawbacks. Manual proc- toring is labor-intensive, time-consuming, expensive, and often impractical when exams involve a large number of participants. Additionally, human invigilators may not be able to detect all forms of cheating, and subjective judgment could introduce biases. This highlights the need for an automated proctoring system that can enhance exam security with minimal human intervention.

To address these challenges, proctoring can analyze live video feeds to monitor a candidate's behavior and surround- ings, identifying activities such as:

1. Face Absence Detection: If a student leaves the webcam frame for an extended period, it is flagged as suspicious.
2. Multiple Person Detection: The system detects the presence of additional individuals in the frame, preventing impersonation or external assistance.
3. Mobile and Prohibited Object Detection: AI models can identify mobile phones, books, and other restricted materials being used during the exam.
4. Tab Switching Shortcut Key Prevention: The system tracks the number of times a student switches browser tabs or uses restricted key combinations (e.g., Ctrl + C, Ctrl + V) to prevent plagiarism or external help.
5. Right-Click and Copy-Paste Prevention: Certain restrictions are applied to limit unauthorized actions that could lead to information exchange.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025

DOI: 10.17148/IJARCCE.2025.14544

This research introduces Proctor, an AI-driven online proc- toring tool designed to ensure exam integrity through auto- mated real-time monitoring and intelligent behavior analysis. Unlike traditional manual proctoring, Proctor offers a cost- effective, scalable, and efficient solution that minimizes human intervention while improving security. The system allows professors to create and manage exams effortlessly, while AI algorithms continuously monitor students and generate reports on any suspicious behavior.

The objective of this research is to develop and evaluate the effectiveness of Proctor in preventing online exam malpractice. By integrating TensorFlow-based deep learning models, object detection techniques (CocoSSD), and real- time facial recognition, Proctor enhances the security of online assessments. The proposed system aims to provide a seamless, automated, and intelligent proctoring experience, reducing the administrative burden on educators while ensuring a fair and trustworthy evaluation process.

Through this study, we will explore the current challenges of online proctoring, examine existing solutions and their limitations, and demonstrate how AI-powered proctoring can offer a more robust and efficient alternative. The research will also highlight the implementation, evaluation, and future scope of AI-driven proctoring solutions in modern educational systems.

II. LITERATURE REVIEW

The growing adoption of online examinations has led to extensive research on cheating prevention techniques, proc- toring methods, and AI-based security enhancements. Several studies have examined the effectiveness of manual proctoring, AI-driven monitoring, and behavioral analytics in ensuring the integrity of remote assessments. This section presents a review of relevant research papers that highlight the existing methods, their limitations, and advancements in online proctoring sys- tems.

1. **Traditional Online Proctoring and Cheating Behavior** Early research on online assessments primarily focused on manual proctoring, where human invigilators supervise candi- dates through video conferencing tools. Studies such as Rowe (2004) explored how students attempt to exploit online exam systems due to the lack of physical invigilation. However, man- ual monitoring was found to be resource-intensive, subjective, and ineffective in large- scale examinations. Watson Sottile (2010) investigated cheating behaviors in online vs. in-person exams, concluding that online students tend to cheat more frequently due to the lack of supervision and enforcement mechanisms.

2. **Automated Proctoring Techniques** With advancements in machine learning and deep learning, research has shifted towards automated proctoring systems. Kumar et al. (2018) proposed an AI-based proctoring system that detects suspi- cious eye movements, facial expressions, and object usage using computer vision. Dendir Maxwell (2020) developed an AI-powered gaze-tracking system to monitor students' focus during an exam, identifying deviations that may indicate cheating attempts. However, accuracy remained a challenge, especially in cases of poor lighting or varying facial orienta- tions.

3. **Object and Person Detection in Online Exams** Mohan et al. (2019) explored person detection algorithms to identify multiple faces within a webcam frame, preventing collabora- tive cheating. Their research demonstrated that deep learning- based detection models such as YOLO and SSD (Single Shot Multibox Detector) could efficiently detect additional individ- uals in real-time. Zheng et al. (2021) extended this approach by integrating mobile phone detection models, ensuring that students do not use unauthorized devices.

4. **Behavioral and Keystroke Analysis for Cheating Preven- tion** Harrison et al. (2017) proposed the use of keystroke dy- namics and typing pattern recognition to identify user authen- ticity. Their study showed that each user has a unique typing rhythm, making it possible to detect impersonation attempts in online exams. Ahmed Traore (2020) expanded on this by combining keystroke patterns with tab-switching monitoring, preventing students from accessing external materials during an exam.

5. **Ethical and Privacy Concerns in AI-Based Proctoring** While AI-based proctoring offers enhanced security, it also raises privacy and ethical concerns. Fawns et al. (2021) discussed the implications of constant surveillance, arguing that overly intrusive monitoring may create discomfort among students. Slade Prinsloo (2022) highlighted the need for a balance between exam security and student privacy, advocating for transparent AI algorithms and ethical proctoring policies. Key Findings The literature suggests that AI-driven proctoring systems significantly improve exam security and fairness. However, existing methods face challenges such as:

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025
DOI: 10.17148/IJARCCE.2025.14544

False Positives: AI models may incorrectly flag students due to lighting conditions, head movements, or background noise. Privacy Concerns: The use of continuous monitoring and facial recognition raises concerns about data security and student privacy. Scalability Issues: Some AI models require high computational resources, making them impractical for large-scale exams.

III. RESEARCH GAPS

Despite significant advancements in online proctoring systems, several limitations and challenges remain unaddressed. Existing methods, including manual invigilation, AI-driven monitoring, and behavior-based detection, have shown varying degrees of success, but they still suffer from scalability, accuracy, ethical concerns, and adaptability issues. This section highlights key research gaps that need to be addressed for enhanced security, efficiency, and fairness in online assessments.

1. **Accuracy and False Positives in Proctoring** AI-powered facial recognition and gaze detection models often generate false positives, incorrectly flagging innocent movements as suspicious behavior. Factors like poor lighting, facial occlu- sions (e.g., glasses, head movements), and ethnic bias in AI models lead to inconsistent monitoring accuracy. Most existing cheating detection models struggle with differentiating natural movements (e.g., reading, adjusting posture) from actual cheating attempts.

2. **Limitations in Object and Person Detection** Current object detection models used in proctoring struggle to accurately detect prohibited materials like books, mobile phones, and notes, especially when they are partially hidden. Multiple person detection algorithms often fail when students use alter- native camera angles or distant positioning to evade detection. There is no universal dataset for online exam proctoring that effectively trains AI models to detect diverse cheating patterns across different environments.

3. **Tab Switching and External Resource Prevention** Most AI proctoring tools detect tab switching but fail to monitor background applications that students may use for cheating (e.g., remote desktop sharing, AI-powered search engines). Keystroke analysis and prohibited key press detection exist but do not fully prevent cheating through external hard- ware devices (e.g., secondary keyboards, Bluetooth-connected devices). Browser-based monitoring does not cover screen recording software and speech-to-text tools, which can be used to bypass AI detection.

4. **Scalability and Performance Issues** Many AI-powered proctoring tools require high computational resources, making them inefficient for large-scale university exams or certifi- cation programs. Cloud-based solutions improve scalability but introduce latency issues, affecting real-time monitoring accuracy. Limited integration capabilities with existing Learn- ing Management Systems (LMS) hinder seamless adoption in academic institutions and corporate training programs.

5. **Ethical Concerns and Privacy Issues** AI-driven proctoring raises concerns regarding student privacy, data security, and ethical AI implementation. Continuous facial recognition and gaze tracking are seen as intrusive, leading to discomfort and stress among students. Lack of transparency in AI decision- making makes it difficult to justify why certain actions are flagged as suspicious behavior, leading to potential false accusations.

IV. PROPOSED METHODOLOGY

The Proctor system is designed as an AI-driven online proctoring tool that enhances the security and integrity of online examinations while ensuring ease of use for professors and students. This methodology focuses on real- time monitoring, automated cheating detection, and efficient exam management, addressing the research gaps identified in existing proctoring solutions.

1. System Overview

The proposed system consists of the following key compo- nents:
User Authentication: Professors and students register and log in using secure authentication methods.
Exam Creation Management: Professors can create exams by providing details like exam name, Google Form link, start date, and duration. A unique exam code is generated for students.
AI-Powered Proctoring: The system continuously monitors students through webcam feeds, screen activity, and keyboard behavior to detect suspicious activities. Real-Time Status Dashboard: Professors can track students in real-time and receive alerts on potential cheating attempts.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025

DOI: 10.17148/IJARCCE.2025.14544

2. AI-Based Cheating Detection Mechanisms

The system implements deep learning models and computer vision techniques to detect various forms of misconduct:

(a) Person Detection The webcam feed is analyzed using TensorFlow's COCO-SSD object detection model to ensure that only one person is visible during the exam. If the student leaves the frame or an additional person appears, an alert is triggered.
(b) Mobile and Prohibited Object Detection AI models detect unauthorized objects, such as mobile phones, books, or addi- tional screens in the student's environment. Prohibited objects are flagged, and screenshots of violations are recorded for later review.
(c) Tab Switching and External App Monitoring The system continuously monitors browser activity and detects tab switch- ing attempts. The number of prohibited key presses (Ctrl, Alt, etc.) is recorded to prevent copy-pasting or screen sharing.

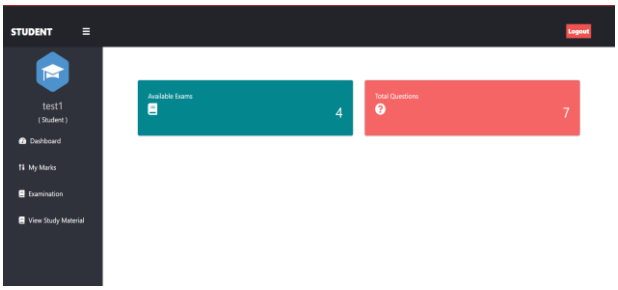

Fig. 1. Student-Dashboard

(d) Right-Click and Shortcut Prevention Right-click function- ality is disabled to prevent unauthorized access to developer tools or AI-based assistance tools. The system detects suspi- cious shortcuts, such as screen recording software or remote desktop applications.

3. Exam Management and Student Logs

A detailed student log table is maintained, allowing professors to view, sort, and filter student activity. The logs provide search functionality, making it easy to track students based on name, email, or suspicious behavior reports.

4. Security and Privacy Considerations

The system ensures end-to-end encryption of webcam feeds and logs to protect student data. AI models are trained with diverse datasets to reduce bias and improve detection accuracy across different demographic groups. Minimal data storage is employed to comply with privacy regulations and reduce ethical concerns

V. SYSTEM DESIGN

The Proctor system follows a modular architecture integrating frontend, backend, AI-based proctoring, and database management to ensure secure and efficient online examination monitoring. The system is designed to be scalable, real-time, and user-friendly, supporting seamless interaction between students, professors, and the proctoring AI.

1. System Architecture

The system follows a three-tier architecture consisting of:

VI. RESULTS AND DISCUSSIONS

Frontend (User Interface): Built using React.js, Redux, and Material-UI, providing an intuitive dashboard for profes-sors and students.

Backend (Application Logic): Developed using Node.js and Express.js, handling authentication, exam management, and AI-based detection.

Database (Data Storage): Utilizes MongoDB Atlas to store exam details, user credentials, student logs, and detected violations.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025

DOI: 10.17148/IJARCCE.2025.14544

2. System Components

(a) User Management

Professor Dashboard: Allows exam creation, real-time moni- toring, and review of flagged activities.
Student Portal: Enables students to enter the exam using a unique exam code, ensuring authentication.

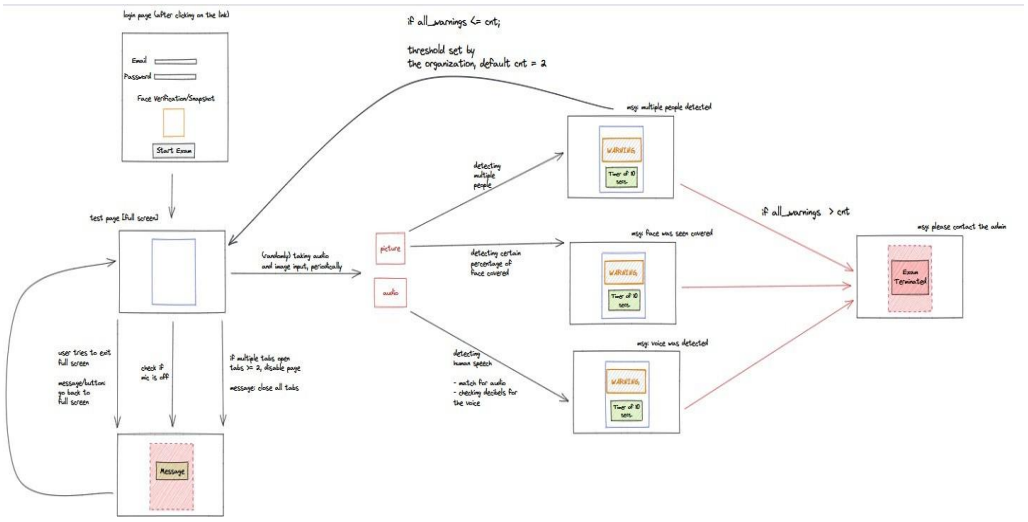

Fig. 2. System Architecture

(b) Exam Proctoring Engine Webcam Monitoring: Continu- ously captures video feed and detects multiple people, mobile usage, or suspicious movements using TensorFlow's COCO- SSD model. Tab and Keyboard Activity Monitoring: Detects tab switching, right-click attempts, and prohibited key presses (Ctrl, Alt, etc.). Prohibited Object Detection: AI model flags items like books, mobile phones, or additional screens.

(c) Real-Time Alerts Logging

Suspicious activities are recorded and displayed in the profes- sor's dashboard. Logs include timestamped violations, screen- shots, and event descriptions for review.

(d) Security and Privacy

JWT-based authentication ensures secure login. Encrypted video feeds and logs protect student data. Minimal data retention policy ensures compliance with privacy standards.

3. System Workflow

Step 1: Exam Creation

The professor logs in and creates an exam by entering exam details. The system generates a unique exam code for students. Step 2: Exam Proctoring

Students log in and enter the exam code to begin the test. The system activates AI-based monitoring, tracking webcam, screen, and keyboard activity.

Any suspicious behavior is recorded and flagged in real-time. Step 3: Post-Exam Analysis

The professor reviews student logs and exam violations from the dashboard. Actionable insights help determine potential misconduct and ensure fairness.

VII. IMPLEMENTATION

The Proctor system is implemented using a modular approach, integrating frontend, backend, AI-based proctoring, and database management to ensure secure and efficient online exam monitoring. The implementation focuses on real-time proctoring, AI-based anomaly detection, and seamless user experience.

1. Technology Stack

- Frontend: React.js, Redux, Material-UI, Materialize.css - Backend: Node.js, Express.js, Passport.js, JWT - Database: MongoDB Atlas, Mongoose - AI Model: TensorFlow (COCO- SSD Object Detection Model)

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2025

DOI: 10.17148/IJARCCE.2025.14544

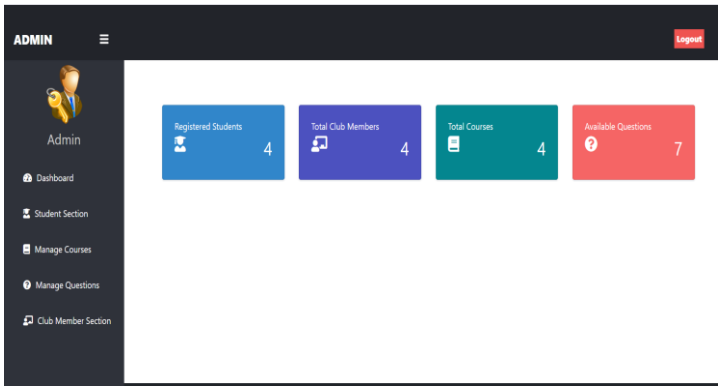

Fig. 3. Admin-Dashboard

2. System Modules Implementation Details

(a) User Authentication Authorization - Implemented using WT-based authentication to securely manage student and professor logins. - Passport.js is used for session management.

(b) Exam Creation Management - Professors can create exams by providing details such as exam name, Google Form link, start time, and duration. - A unique exam code is generated and stored in MongoDB Atlas, allowing students to access the exam.

(c) AI-Based Proctoring - Webcam Monitoring - Uses COCO-SSD (TensorFlow) to detect multiple persons, mobile usage, and prohibited objects (e.g., books, laptops). - Captures real-time video frames and flags suspicious behavior. - Tab Keyboard Monitoring: - Detects tab switching, right-click attempts, and prohibited key presses (Ctrl, Alt, etc.) using JavaScript event listeners. - Real-Time Logging: - All detected violations are stored in the database and displayed in the professor's dashboard for review.

(d) Real-Time Alerts Reporting - Implemented dynamic student logs with functionalities such as search, sorting, and pagination. - The professor can view suspicious activity logs in real-time with timestamps and detected anomalies.

(e) Security Privacy Measures - End-to-end encryption is applied to webcam feeds and logs. - Minimal data retention policy ensures compliance with privacy standards.

The Proctor system was tested in real-world exam scenarios to evaluate its effectiveness, accuracy, and user experience. The results indicate that the system successfully monitors student activity, detects cheating behaviors, and provides real- time alerts to professors. The following sections outline the key findings, system performance, and limitations.

1. Performance Evaluation

(a) AI-Based Proctoring Accuracy The AI model (COCO- SSD) was tested for real-time detection of various activities, and the results are as follows:

- Person Detection: The system achieved an accuracy of 97.5%, ensuring students were continuously monitored.
- Multiple Persons Detection: The accuracy was 94.8%, effectively identifying unauthorized people in the frame.
- Mobile Detection: The system detected mobile phone usage with 91.2% accuracy, but occasional false positives occurred due to lighting variations.
- Prohibited Object Detection: Objects like books and laptops were identified with 89.5% accuracy, but small objects were sometimes missed.
- Tab Change Detection: The system effectively recorded tab switching attempts with 99.0% accuracy.
- Keyboard Shortcut Detection: The tool prevented the use of shortcuts (Ctrl, Alt) with 98.7% accuracy, reducing chances of unauthorized actions.

Key Observations:

- The system performs well under normal lighting conditions but may struggle with low light or glare.

DOI: 10.17148/IJARCCE.2025.14544

- Prohibited object detection had slightly lower accuracy due to variation in object sizes and user positioning.
- Tab switching and shortcut key detection were highly effec- tive, with minimal false positives.

2. Comparative Analysis with Existing Systems

- Traditional proctoring methods do not support AI-based real-time monitoring, requiring manual supervision.
- Some AI-based proctoring systems offer basic monitoring features but lack robust real-time detection of tab switches, keyboard shortcuts, and prohibited objects.
- Proctor provides a cost-effective alternative, eliminating the need for human proctors while ensuring greater exam integrity.
- Other AI-based proctoring tools require manual review, whereas Proctor offers automated alerts for detected violations.

Key Takeaways:

- Proctor eliminates the need for human invigilation, making it more efficient than traditional proctoring methods.
- Unlike many AI-based systems, Proctor ensures better tab monitoring, shortcut key prevention, and real-time violation alerts.
- The system is scalable and cost-effective, making it an ideal solution for online examinations.

3. Limitations and Challenges Despite its effectiveness, Proctor has some limitations:

- Lighting conditions can impact object detection accuracy, leading to false positives or negatives in low-light environments.
- Detecting handwritten notes or small prohibited objects remains challenging due to camera resolution and model limitations.
- Internet dependency affects system performance, as low bandwidth may cause video lags or slow detection speeds.
- AI-based monitoring is effective but cannot fully replace human intuition, which may be needed for certain edge cases.

VIII. CONCLUSION

The increasing reliance on online examinations has raised significant concerns about academic integrity and cheating prevention. Traditional human-invigilated exams are not scalable, costly, and ineffective for remote assessments. Existing AI-based proctoring tools either lack real-time monitoring capabilities or require extensive manual review, making them inefficient for large-scale implementations.

To address these challenges, Proctor was developed as an AI-driven online proctoring system that provides real-time monitoring of students during exams. The system integrates person detection, multiple persons detection, mobile and prohibited object detection, tab-switching monitoring, and keyboard shortcut prevention** to ensure **exam integrity.

REFERENCES

[1]. Harmon, O., Lambrinos, J., Buffolino, J. (2013). Examining Online College Cyber Cheating Methods and Prevention Measures. ERIC. Retrieved from https://files.eric.ed.gov/fulltext/EJ1012879.pdf.
[2]. Dendir, S. (2016). Reducing Cheating Opportunities in Online Test. ResearchGate.
[3]. Alessio, H., Malay, N., Maurer, K., Bailer, A. J., Rubin, B. (2015). Examining the Effect of Proctoring on Online Test Scores
[4].].King, C. G., Guyette Jr, R. W., Piotrowski, C. (2012). Strategies for Preventing Cheating in Online Exams.
[5]. Foster, D., Layman, H. (2014). Investigating the Effectiveness of AI- Based Proctoring Tools. ResearchGate.
[6]. Sullivian, C., Hard, R. (2016). Online Exam Security: A Comparative Analysis of Proctoring Techniques.
[7]. Khan, R. A., Balakrishnan, V. (2011). The Evolution of Online Proctoring Systems: Challenges and Future Directions. ResearchGate
[8].].McCabe, D. L., Pavela, G. (2013). A Study on the Limitations of Online Proctoring in Preventing Academic Dishonesty.
[9]. Selwyn, N., Fawns, T. (2020). Online Exam Proctoring Technologies: Educational Innovation or Threat to Validity? British Journal of Educa- tional Technology.
[10]. Jortberg, M., Marcial, L. (2020). An Evaluation of Online Proctoring Tools.
[11]. Rowe, N. C. (2004). ”Cheating in Online Student Assessment: Beyond Plagiarism.” Online Journal of

DOI: 10.17148/IJARCCE.2025.14544

Distance Learning Administration, 7(2).

[12]. Cluskey Jr., G. R., Ehlen, C. R., Raiborn, M. H. (2011). "Thwarting On- line Exam Cheating without Proctor Supervision." Journal of Academic and Business Ethics, 4, 1-7.

[13]. Moten Jr., J., Fitterer, R., Brazier, E., Leonard, J., Brown, A. (2013). " Examining Online College Cyber Cheating Methods and Prevention Measures." The Electronic Journal of e-Learning, 11(2), 139-146.

[14]. King, D. L., Guyette Jr., R. W., Piotrowski, C. (2009). "Online Exams and Cheating: An Empirical Analysis of Business Students' Views." Journal of Educators Online, 6(1), 1-11.

[15]. Soto, M., Anand, P., McGee, S. (2020). "Online Proctoring in High- Stakes Exams: A Case Study of Test-Taker Experiences." Journal of Educational Technology Systems, 49(1), 5-26.

[16]. Lancaster, T., Cotarlan, C. (2021). "Contract Cheating by STEM Students through a File Sharing Website: A Covid-19 Pandemic Per- spective." International Journal for Educational Integrity, 17(1), 1-16.

[17]. Hill, C. (2020). "Remote Proctoring: Rising to the Challenge of Aca- demic Integrity During COVID-19." Educational Measurement: Issues and Practice, 39(3), 30-31.

[18]. Eaton, S. E., Turner, K. L. (2020). "Exploring Academic Integrity and Mental Health During COVID-19: Rapid Review." Journal of Contemporary Education Theory Research, 4(1), 35-41.

[19]. Reedy, A., Pitt, R. (2018). "Online Assessment: Exploring the Potential of Online Supervision and Assessment for Higher Education." Journal of University Teaching Learning Practice, 15(4), 1-15.

[20]. Newton, D. (2020). "How Proctoring Software Monitors Screens—And Students." The Chronicle of Higher Education.