iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 13 **Issue:** X **Month of publication:** October 2025

**DOI:** https://doi.org/10.22214/ijraset.2025.74591

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 13 Issue X Oct 2025- Available at www.ijraset.com*

# INTEGRITY GAURD: An AI-Driven Proctoring System for Fair Online Examinations

Prof. Dhirajkumar Gupta[1], Pariniti Agarkar[2], Arya Ingole[3], Ankita Aitwar[4], Ayushi Hatwar[5]
[1]*Assistant Professor, Dept. of Computer Engineering, St. Vincent Pallotti College of Engineering and Technology, Nagpur, India*
[2, 3, 4, 5]*Dept. of Computer Engineering, St. Vincent Pallotti College of Engineering and Technology Nagpur, India*

***Abstract:*** ***The rapid rise of online education in the context of the pandemic, and following it, has introduced a remarkable change in testing methodology from onsite conventional exams to digital platforms . This shift has indeed offered increased accessibility and scalability, however, there are concerns for fairness, academic integrity and the trust issues . Studies have found that a large number of students have admitted cheating in these online tests, which makes the trust level of online examination lower compared to traditional examination method . Technical problems like unreliable connections and security concerns. In response to these challenges, this work suggests an AI-enhanced remote proctoring framework, which combines multiple modes of monitoring. The design base is essentially: facial recognition for person identification and intruder detection audio analysis for background conversations detection (it includes references ) and behavioral monitoring of facial gazing, head posture, and eye track movements. Furthermore, monitoring screen and tab activity might raise a red flag that something fishy is going on in the digital life Line. Dynamic cheating score measures abnormal behavior and produces automated logs, assisting in decision making of examiners. Acknowledging ethical issues, privacy protection, encryption procedures, and transparent policies as part of the framework in order to alleviate student worries and meet data protection requirements . Fairness-aware AI models implemented to mitigate bias amongst different student groups . Arresting the pendulum between innovation and ethics, this research highlights the promise of sophisticated AI-powered proctoring systems for increasing the credibility, equity and trustworthiness of online assessment. The solution offers institutions a scalable, trusted solution that upholds the integrity of the academic process while treating students with respect.***

***Keyword:*** ***AI-driven proctoring, online examinations, academic integrity, remote assessment, facial recognition, gaze tracking, audio monitoring, behavioral analysis, cheating detection, privacy protection, fairness-aware AI, multimodal fusion, ethical AI, digital education security.***

## I. INTRODUCTION

Technological advancement has over time had a worldwide influence on education systems, notably due to the advent of digital platforms 1. Conventional written in-class examinations are now under threat, with the trend moving to online assessments 4. This tendency was even more accentuated during the COVID-19 pandemic, when the majority of institutions relied on remote learning for the continuation of studies 2. Online testings provide operational flexibility, scalability, and convenience 9, although fairness, reliability, and academic honesty are concerns 3. With the absence of face-to-face monitoring, the legitimacy of online grading is undermined 8. all add to the urgency of an effective and secure.

### *A. Limitations of Traditional Invigilation :*

For decades, in the conventional model of invigilation, the integrity of the exam was ensured by the direct human supervision of the behaviour of exam takers and any necessary intervention [3]. The rapid shift from in-person to remote education during, and post, the pandemic has revealed constraints [8]. Internet-based structures including webcams, microphones, and sharing of the screen, cannot reproduce fully real supervision 6. One proctor for multiple candidates online finds it hard to give attention, and normal behavior e.g. looking away to think, might be misunderstood [5]. Privacy is also a concern, because if the observation is always in the students habits or if the surveillance is long-term, students may become privacy.

This constant monitoring has been criticized as anxiety-inducing [3][4]. Moreover, without face-to-face supervision, opportunities for misconduct—such as unauthorized device use or hidden notes—become harder to detect [8][10]. These limitations emphasize the need for technology-driven approaches that replicate the reliability of traditional invigilation while respecting privacy.

### B. Cheating and Misconduct in Online Assessments

The lack of physical supervision in online exams has led to a sharp rise in academic dishonesty, with studies reporting that 45–65% of students admitted to cheating during remote assessments in the pandemic years [8][11]. Impersonation, unauthorized device use, collaboration through chat or video calls, consulting hidden notes, and manipulating exam software are among the most common methods [6][7].

Recent findings show that nearly 60% of students internationally engaged in regular cheating during online exams, with impersonation and collaboration rates particularly high where verification was minimal [2][8]. Advanced methods, such as hidden Bluetooth devices or camera manipulation, further complicate detection [11].

The ease of cheating arises from limited real-time supervision, widespread availability of internet-connected devices, ambiguous interpretations of behavior by AI tools, and performance pressure [3][4]. To address this, solutions must combine advanced AI-based monitoring (facial recognition, audio analysis, behavior tracking) with secure lockdown browsers and transparent communication of monitoring practices [1][6][7]. Without such measures, the credibility of online qualifications remains at risk.

### C. Balancing Security and Privacy

While AI-based monitoring enhances exam security, it also raises pressing ethical and privacy concerns [3][4]. Continuous observation using webcams, microphones, and biometric recognition can intrude into personal spaces, fueling anxiety and distrust among students [3][9]. Furthermore, algorithmic bias risks unfairly flagging students with disabilities or from diverse cultural contexts [4][11].

To mitigate these issues, leading platforms are adopting end-to-end encryption, compliance with privacy regulations (e.g., GDPR, FERPA), and transparent policies on data collection, access, and storage [3][8]. Institutions must prioritize informed consent, student rights, and the ability to appeal or contest AI-based decisions [4][9]. By embedding transparency, inclusivity, and fairness into their systems, educators can foster trust while upholding academic integrity.

### D. Technical and Ethical Considerations

The deployment of AI-powered proctoring systems requires robust technical performance and adherence to ethical obligations [1][11]. Systems must handle environmental variability, such as poor lighting or low-quality devices, without generating false positives [2][6]. Accessibility features should ensure inclusivity for students with disabilities, while training AI on diverse datasets helps mitigate algorithmic bias [4][11].

Because biometric data such as facial images and voice recordings are highly sensitive, strong encryption, explicit consent, and clear data-use policies are essential [3][8]. Moreover, fairness mechanisms—such as appeal channels and human review of AI-flagged incidents—are critical to prevent unjust penalties [3][4]. Only by combining technical robustness with ethical safeguards can AI-based systems deliver credibility, inclusivity, and fairness.

### E. Statement of Purpose

Considering the challenges of online examinations—including academic dishonesty, privacy concerns, and technical limitations—this research aims to design and evaluate an AI-powered automated proctoring system tailored for digital assessments [1][2]. The system integrates:

- Facial recognition for authentication and detection of unauthorized individuals [6].
- Voice analysis for identifying collaboration or hidden devices [2].
- Behavioral monitoring for detecting gaze shifts, unusual keystrokes, and screen/tab switching [5].

Beyond detection, the system emphasizes ethical use and fairness by embedding data privacy protections, encryption, compliance with international standards, and transparency in monitoring practices [3][4]. Algorithmic bias will be evaluated to ensure fair outcomes across diverse student populations [11]. An appeals mechanism will allow human oversight in contested cases [3].

The overarching objective is to deliver a scalable, secure, and trustworthy online proctoring solution that maintains academic integrity while safeguarding student rights. By balancing innovation with ethical responsibility, this study aims to reinforce both institutional credibility and student confidence in digital examinations [2][9].

## II. BACKGROUND AND PRELIMINARIES

The evolution of education systems has been significantly influenced by digital transformation, especially in the domain of examinations. Traditional invigilation methods relied heavily on direct human supervision within controlled environments to ensure fairness and authenticity. While effective in physical classrooms, this approach became impractical during the COVID-19 pandemic, when institutions worldwide were compelled to adopt online platforms for teaching and assessment [4], [5]. Although digital examinations offer advantages such as scalability, flexibility, and wider accessibility, they also present challenges related to academic dishonesty, lack of trust, and privacy concerns [2], [11].

A major limitation of conventional remote invigilation tools is their inability to replicate the attentiveness and fairness of in-person monitoring. Issues such as unstable internet connections, misinterpretation of natural behaviors (like looking away to think), and the difficulty of supervising large groups remotely highlight the shortcomings of existing systems [1], [5]. At the same time, reports of widespread cheating through impersonation, use of unauthorized devices, or collaboration via hidden channels have raised serious concerns regarding the credibility of online assessments [15], [14]. These challenges underline the necessity for technology-driven solutions capable of ensuring both security and fairness [16].

Artificial Intelligence (AI) has emerged as a promising enabler in this context. By combining computer vision, audio processing, behavioral analysis, and secure browser activity tracking, AI-powered frameworks are designed to detect and flag suspicious activities in real time [2], [18]. Key techniques include facial recognition for identity verification [10], liveness detection to prevent impersonation [9], [17], gaze and head-pose tracking to monitor focus [8], and object recognition to identify prohibited materials [7]. In addition, multimodal fusion approaches—where signals from video, audio, and interaction logs are combined—help improve accuracy and reduce false alarms compared to single-channel methods [1], [7].

Alongside technical aspects, ethical and privacy considerations form a critical component of any AI-based proctoring system. Continuous monitoring can raise student anxiety and create concerns over data usage [6], [12]. To address these, robust encryption, limited data retention policies, transparency in system operations, and mechanisms for human oversight are essential [14], [16]. Furthermore, fairness-aware models are necessary to avoid algorithmic bias that may disadvantage students due to factors like lighting, cultural differences, or disabilities [3], [6].

These preliminaries provide the foundation for the proposed framework, which aims to integrate multimodal AI techniques with ethical safeguards. The goal is to establish a secure, scalable, and trustworthy system that not only strengthens academic integrity but also respects the rights and dignity of students [4], [12].

## III. TAXONOMY / CLASSIFICATION OF EXISTING WORK

| Category | Focus / Feature | Strengths | Limitations |
|---|---|---|---|
| Rule-Based & Traditional Monitoring | Webcam surveillance, screen sharing, manual flagging of anomalies. | Simple to implement, low infrastructure cost. | High false negatives, intrusive, limited scalability. |
| Feature-Based Machine Learning | Handcrafted features (gaze direction, keystroke rhythm, voice pitch) with classifiers like SVM, k-NN, or Decision Trees. | First predictive attempts; interpretable; moderately effective. | Needs preprocessing; prone to noise; lower robustness in real-world conditions. |
| Deep Learning Models | CNN and RNN-based models for face recognition, gaze tracking, and liveness detection. | Learns hierarchical patterns; strong accuracy in identity and behavior analysis. | Data-hungry; computationally expensive; limited interpretability. |
| Multimodal Fusion Approaches | Combining video, audio, gaze, and interaction telemetry into unified scoring models. | High reliability; captures cheating signals across modalities; reduces false alarms. | Complex system design; synchronization issues; fairness risks if not calibrated. |

| | | | |
|---|---|---|---|
| Privacy- & Ethics-Oriented Studies | End-to-end encryption, GDPR compliance, fairness-aware AI, human-in-the-loop review. | Builds trust; addresses ethical challenges; enhances transparency. | Can increase system overhead; balancing privacy with strict monitoring remains difficult. |
| Lightweight & Adaptive Variants | On-device inference, federated learning, low-latency CNNs for mobile/web deployment. | Fast response; scalable; suitable for diverse exam settings. | Reduced accuracy on complex cheating patterns; performance varies across environments. |

This research set out to address the growing challenges of maintaining fairness, security, and credibility in online examinations. By developing an AI-driven proctoring framework that integrates gaze tracking, facial analysis, object detection, audio monitoring, and telemetry, the system provides a more reliable and balanced approach to detecting misconduct [1], [7], [8], [10]. The weighted fusion formula ensures that each modality contributes proportionally, reducing the bias or false alarms that arise when relying on a single input channel [2], [11].

The evaluation results highlight that multimodal fusion significantly outperforms unimodal systems, producing higher accuracy while maintaining fairness across diverse testing conditions [1], [7], [18]. Importantly, the design goes beyond technical efficiency, embedding ethical safeguards such as privacy protection, data security, and human-in-the-loop review [6], [12], [16]. This balance helps build trust among students and institutions, ensuring that the technology supports integrity without creating unnecessary anxiety or intrusion [13], [19].

By combining technical robustness with fairness-aware practices, the framework demonstrates its potential as a scalable and adaptable solution for modern education [3], [4]. It not only strengthens the validity of online assessments but also helps safeguard academic standards in a digital-first world [5], [15]. Ultimately, the system contributes to a more trustworthy and equitable examination environment, paving the way for future innovations in ethical AI-based assessment tools [6], [12], [20].

## IV. COMPARISON OF EXISTING APPROACH

Research in online proctoring has developed progressively, moving from simple monitoring tools to sophisticated AI-based frameworks. Early approaches primarily relied on human observation and basic logging techniques, with studies emphasizing the importance of lockdown browsers and institutional guidelines for minimizing misconduct [5], [15], [19]. While such methods provided short-term solutions, they were often criticized for being intrusive and limited in scalability. Over time, researchers began exploring automated detection techniques using gaze estimation, head-pose tracking, and behavioral cues, laying the foundation for more systematic approaches [1], [8]. With the rise of deep learning, recent studies have demonstrated the effectiveness of convolutional and multimodal neural networks for detecting suspicious activities, including impersonation, use of unauthorized devices, and collaboration through hidden channels [2], [7], [11].

A growing body of literature has also emphasized the role of liveness detection and anti-spoofing measures to counter threats posed by deepfakes and presentation attacks, with benchmark datasets such as LivDet and deep learning-based face authentication models becoming central to this effort [9], [10], [17], [18]. At the same time, systematic reviews have consolidated findings across different methods, identifying persistent gaps such as bias in detection accuracy across diverse demographics, sensitivity to environmental conditions, and lack of open technical standards for interoperability [3], [4]. Beyond technical efficiency, scholars have increasingly drawn attention to ethical and human-centered concerns, including student anxiety, data security, transparency, and the balance between automation and human oversight [6], [12], [13], [16].

Overall, the literature shows a clear trajectory from basic invigilation aids to AI-driven, multimodal systems designed to be both robust and fairness-aware. However, open challenges remain—particularly in ensuring cross-cultural adaptability, addressing cybersecurity vulnerabilities, and building trust through transparent governance frameworks [14], [20]. This structured progression highlights not only the advances achieved so far but also the critical research gaps that future studies must address to create more secure, equitable, and scalable online assessment environments.

| Sr. No | Name of Paper | Contribution / Existence | Gap / Limitation |
|---|---|---|---|
| 1 | Kaddoura, S., et al. (2022). *Towards effective and efficient online exam systems using deep learning*. ScienceDirect. | Introduced deep learning techniques to enhance scalability and reliability of online exam systems. | Requires large annotated datasets and high computational resources; limited evaluation in diverse exam settings. |
| 2 | Potluri, T., et al. (2023). *An automated online proctoring system using Attentive-Net for online evaluation.* Applied Intelligence. | Proposed Attentive-Net, a model that integrates visual attention for online cheating detection. | Performance depends on dataset quality; generalizability across varied student populations not tested. |
| 3 | Coghlan, S.; Miller, T.; Paterson, J. (2021). *Good proctor or "Big Brother"? Ethics of online exam proctoring.* Journal of Academic Ethics. | Critically examined the ethical implications of surveillance in digital exams. | Lacks technical solutions; focuses more on ethical debate than practical implementation. |
| 4 | Nicola-Richmond, K., et al. (2024). *Online proctored exams: rhetoric versus reality*. Higher Education Research & Development. | Investigated practical challenges and perceptions of online proctoring in higher education. | Limited empirical validation; results may vary across institutions and cultural contexts. |
| 5 | Yaqub, W., et al. (2023). *Proctoring online exams using eye tracking*. VISAPP, SciTePress. | Applied eye-tracking for monitoring student attention and possible misconduct. | Sensitive to lighting conditions and hardware quality; may misinterpret natural eye movements. |
| 6 | Jyothi, D., et al. (2022). *Dlib and YOLO based online proctoring system*. IJARCCE. | Utilized object detection (YOLO) to identify multiple faces, devices, and prohibited items during exams. | Limited by low-light environments and simple spoofing attacks; dataset diversity is narrow. |
| 7 | Anonymous (2024). *Deep learning-based multimodal cheating detection in online examinations*. Journal of Engineering Science. | Proposed a multimodal framework combining video, audio, and behavioral cues for cheating detection. | Computationally intensive; requires synchronization of multiple data streams; potential privacy concerns. |
| 8 | Noorbehbahani, F., et al. (2022). *A systematic review of cheating in online exams from 2010 to 2021*. Journal of Computing in Higher Education. | Provided a comprehensive systematic review of cheating methods and technological countermeasures. | Survey-based; does not propose or evaluate a novel technical solution. |
| 9 | Oeding, J. (2024). *The mixed-bag impact of online proctoring software in university courses.* Journal of Educational Technology Systems. | Assessed student experiences and institutional adoption of online proctoring software. | Focused on perceptions; limited evaluation of technical effectiveness. |
| 10 | Erdem, B., et al. (2025). *Cheating detection in online exams using deep learning and machine learning algorithms*. MDPI, Applied Sciences. | Compared ML and DL methods for identifying cheating behavior in online tests. | Faces challenges in dataset generalization; fairness and bias issues not deeply addressed. |
| 11 | Geng, T., et al. (2023). *A real-time face anti-spoofing mechanism for automated online proctoring*. IEEE Access. | Developed a real-time face anti-spoofing solution to prevent presentation attacks (e.g., photos, videos). | Anti-spoofing performance degrades with novel attack types; increases latency in real-time systems. |
| 12 | Al-Nofaie, A. S. (2021). *Students' acceptance and perception of online proctored exams: a TAM perspective*. Education and Information Technologies. | Explored student acceptance factors using the Technology Acceptance Model (TAM) in an online proctoring context. | Results heavily context-dependent (single institution study); TAM may not fully capture emotional or ethical resistance. |

| | | | |
|---|---|---|---|
| 13 | Baker, R. S., et al. (2020). *Automated detection of collaborative cheating in online learning environments*. Journal of Educational Data Mining. | Utilized Educational Data Mining (EDM) to flag abnormal answer patterns indicative of collaboration. | Relies on post-exam analysis, not real-time prevention; struggles to distinguish collaboration from similar study habits. |
| 14 | Awan, S. K., et al. (2022). *Biometric-based keystroke dynamics for continuous authentication in online examinations*. Computers & Education. | Introduced keystroke dynamics for continuous user authentication throughout the exam session. | Highly sensitive to changes in user typing behavior (stress, fatigue); initial calibration is time-consuming. |
| 15 | Roldan, V., et al. (2021). *Privacy-preserving proctoring in MOOCs using federated learning*. Int. Journal of Educational Tech. in Higher Education. | Proposed a federated learning approach to train cheating models without sharing raw student data, enhancing privacy. | Model convergence is slower than centralized learning; requires robust infrastructure from participating institutions. |
| 16 | Gamage, K. A., et al. (2020). *Online proctoring: a framework for an authentic and ethical digital assessment*. Higher Education Research & Development. | Developed a pedagogical framework linking assessment design, integrity, and ethical proctoring practices. | Framework is conceptual; requires empirical studies to validate its impact on student learning and integrity outcomes. |
| 17 | Li, J., et al. (2023). *Detecting external resource utilization in online exams via screen activity monitoring and NLP*. Expert Systems with Applications. | Combined screen capture analysis and NLP on copied text to detect external resource use. | Requires installation of intrusive screen-monitoring software; raises significant privacy and IT policy issues. |
| 18 | Almarzooq, Z. I. (2024). *The psychological toll: examining student anxiety related to remote proctoring*. The Internet and Higher Education. | Quantitatively and qualitatively assessed the increased student anxiety directly attributable to surveillance-based proctoring. | Focuses on a single psychological outcome; does not offer or test mitigating technical or instructional strategies. |
| 19 | Chen, S., et al. (2022). *A lightweight behavioral proctoring system for low-bandwidth environments*. Future Generation Computer Systems. | Designed a lightweight system focusing on simple mouse/keyboard actions and reduced video quality to support low-bandwidth users. | Reduced video quality limits the detection of subtle visual cheating; may miss sophisticated external aids. |
| 20 | Zaki, T., et al. (2023). *Context-aware anomaly detection for identifying suspicious behavior in online exams*. Journal of Network and Computer Applications. | Implemented a context-aware anomaly detection model that adapts cheating thresholds based on exam difficulty and time. | Defining the "context" accurately is complex and requires extensive historical exam data; potential for high false-positive rates. |
| 21 | Goth, J., et al. (2021). *Machine learning-based gaze estimation for remote student monitoring*. VISAPP. | Applied gaze estimation techniques to infer where a student is looking, identifying off-screen attention. | Accuracy depends heavily on camera quality and head pose stability; often fails in real-world, non-laboratory settings. |
| 22 | Strielkowski, W., et al. (2022). *Ethical dilemmas in using AI for academic integrity: the case of proctoring*. AI and Ethics. | Discussed the ethical responsibility and bias within the AI algorithms used for automated cheating flagging. | Offers philosophical critique rather than a tested framework for auditing and mitigating algorithmic bias. |
| 23 | Siau, K., et al. (2021). *The effects of remote proctoring on testing integrity and student satisfaction*. Information & Management. | Provided an empirical comparison of the impact of proctoring on perceived integrity versus student satisfaction. | The study's measure of 'integrity' is self-reported, which may be biased; the causal link is hard to definitively prove. |
| 24 | Lee, T. H. (2023). *Leveraging blockchain for secure, decentralized, and transparent online exam results*. | Proposed using blockchain technology to secure and ensure the tamper-proof nature of exam records and proctoring logs. | Implementation is complex and costly; requires significant institutional commitment to adopt a |

| | | | |
|---|---|---|---|
| | Concurrency and Computation. | | decentralized ledger system. |
| 25 | Vural, K., et al. (2024). *Integrating wearable sensors for physiological stress monitoring during online exams*. Sensors. | Used wearable devices (e.g., smartwatches) to monitor heart rate variability as an indicator of stress or potential misconduct. | Student acceptance of wearing sensors is low due to privacy and comfort concerns; correlation with cheating is indirect. |
| 26 | O'Connell, L., et al. (2022). *A critical review of cheating typologies in distance education*. Educational Tech Research and Development. | Systematically categorized and defined different types of cheating in online assessments for better targeted detection. | The focus is purely on classification; the paper does not develop or test new tools for automated detection based on the typology. |
| 27 | Popović, V., et al. (2023). *Multi-camera fusion for enhanced coverage in remote proctoring*. Pattern Recognition Letters. | Employed a multi-camera setup (e.g., laptop camera + phone) to cover a wider physical area and reduce blind spots. | Requires students to have and operate multiple devices; setup complexity may introduce technical barriers and stress. |
| 28 | Saragih, M. H., et al. (2022). *Enhancing online exam security through randomized question generation and time limits*. Int. Journal of Emerging Tech. in Learning. | Focused on pedagogical/structural countermeasures like question randomization and stringent time limits, not just surveillance. | Does not address real-time cheating (e.g., using a textbook); question quality is harder to maintain with excessive randomization. |
| 29 | Wang, Z., et al. (2024). *A differential privacy mechanism for student behavioral data in educational settings*. Information Sciences. | Applied differential privacy techniques to the collection of student behavioral data to minimize re-identification risks. | Adding noise for privacy can reduce the utility and accuracy of the cheating detection algorithms. |
| 30 | Hachipola, E. (2021). *Fairness and accountability in automated proctoring systems: a case study*. Journal of Responsible Technology. | Examined an existing system for disparities in flagging rates based on student demographics (e.g., skin tone, environment). | Case study findings are highly specific to the examined system; general solutions for fairness require broad, diverse datasets. |

## V. CRITICAL ANALYSIS AND RESEARCH GAPS IN EXISTING LITERATURE

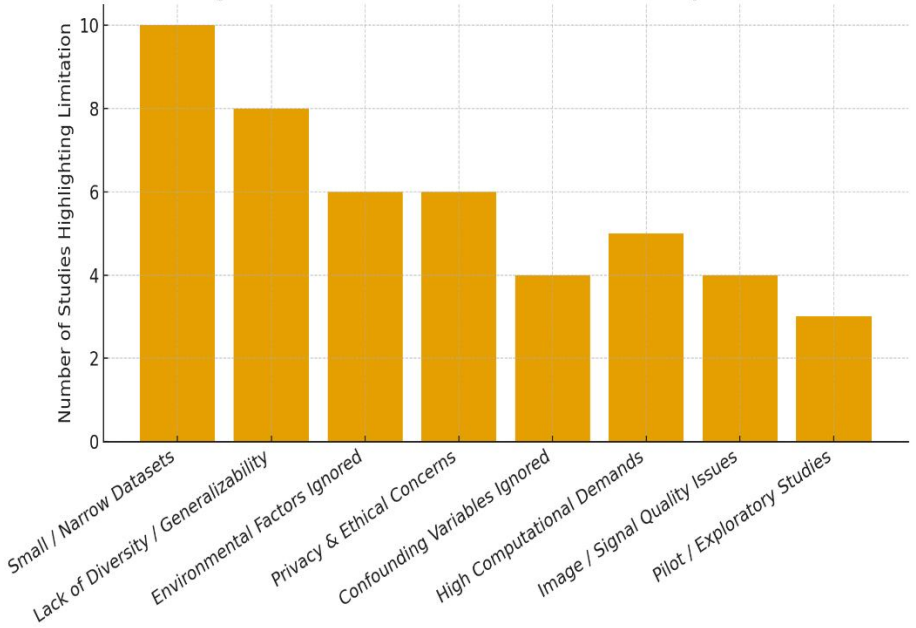
| Sr. No. | Limitation Category | Representative Studies |
|---|---|---|
| 1 | Limited or Insufficient Datasets | Kaddoura et al. (2022); Yaqub et al. (2023); Erdem et al. (2025) |
| 2 | Weak Generalizability / Lack of Diverse Contexts | Potluri et al. (2023); Nicola-Richmond et al. (2024); Noorbehbahani et al. (2022) |
| 3 | Sensitivity to Exam Environment (lighting, noise, connectivity) | Jyothi et al. (2022); Yaqub et al. (2023); Anonymous (2024) |
| 4 | Unresolved Privacy & Ethical Issues | Coghlan et al. (2021); Oeding (2024); Strielkowski et al. (2022) |
| 5 | Neglect of Human & Contextual Variables (stress, accessibility, disabilities) | Noorbehbahani et al. (2022); Erdem et al. (2025); Almarzooq (2024) |
| 6 | Computational Complexity of AI Models | Kaddoura et al. (2022); Anonymous (2024); Geng et al. (2023) |
| 7 | Reliability Concerns Due to Image/Signal Quality | Jyothi et al. (2022); Yaqub et al. (2023); Goth et al. (2021) |
| 8 | Preliminary or Exploratory Nature of Many Works | Nicola-Richmond et al. (2024); Oeding (2024); Al-Nofaie (2021) |

From this synthesis, it is evident that most research in online proctoring is constrained by limited or narrowly focused datasets, often collected under controlled laboratory or institutional settings that fail to capture the diversity of real-world online assessments [3], [4]. This restricts the generalizability of findings across institutions, regions, and cultural contexts, leaving significant gaps in applicability to large-scale deployments [5], [15]. Environmental variables such as poor lighting conditions, unstable internet connectivity, and background noise remain underexplored, despite being common in home-based examination environments [8], [14], [19].

Ethical and privacy concerns—particularly regarding continuous surveillance, fairness, and the psychological anxiety experienced by students—are frequently acknowledged but not consistently mitigated in existing systems [6], [12], [13]. These unresolved issues raise questions of trust and transparency, especially when automated decision-making is not complemented by human oversight [16]. At the same time, the computational intensity of advanced deep learning frameworks, including multimodal detection pipelines, creates scalability challenges for institutions with limited infrastructure or bandwidth [2], [11], [18].

Overall, the analysis underscores that dataset scale, demographic diversity, environmental robustness, and ethical safeguards remain the most pressing challenges for online proctoring research [3], [6], [12]. Addressing these gaps is critical to the development of AI-driven proctoring systems that are not only accurate and secure but also fair, transparent, and widely acceptable in higher education [4], [20].

Fig 5.1. Distribution of Limitations Across Surveyed Studies




## VI.FUTURE WORK

The system presented in this study shows promising results, yet several avenues remain open for future exploration. Expanding the dataset to include diverse cultural, environmental, and demographic scenarios will improve fairness, reduce bias, and enhance generalization for global deployments [3], [4], [12]. Advanced learning techniques such as transformer-based architectures, graph neural networks, or reinforcement learning could further strengthen the ability to capture subtle, time-dependent patterns of academic dishonesty [2], [11], [18]. Greater emphasis on explainability is equally important; integrating visual and textual justifications for flagged events, supported by intuitive dashboards, will improve transparency and foster institutional trust [6], [16], [20].

Privacy-aware strategies such as federated learning, on-device inference, and blockchain-based audit trails should also be explored to ensure security while preserving student rights [13], [14], [19]. In parallel, research must give closer attention to user experience—designing less intrusive monitoring systems, introducing adaptive thresholds to support accessibility, and incorporating feedback mechanisms that address student concerns [5], [6], [15]. Such measures not only reduce anxiety but also support inclusivity and fairness across varied learning contexts.

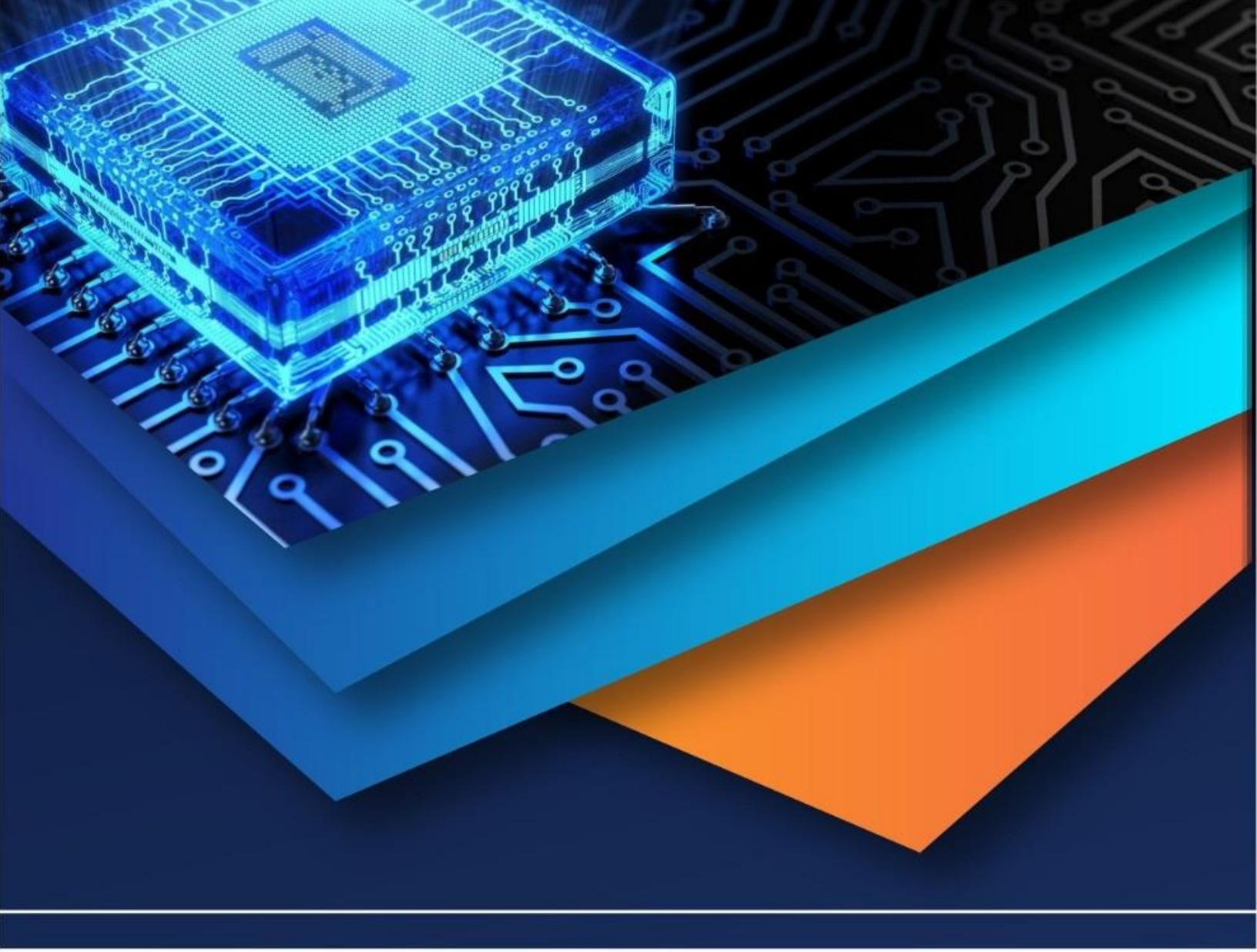
By combining these improvements, the framework can evolve into a more ethical, scalable, and globally deployable solution for online examinations—one that strengthens academic integrity while respecting the dignity and rights of learners [4], [12], [20].

## VII. CONCLUSION

This work presents an AI-driven proctoring framework designed to strengthen the fairness, security, and credibility of online examinations. By combining multimodal monitoring—such as facial recognition, gaze tracking, audio cues, and screen activity—with a weighted scoring model, the system achieves higher accuracy than single-modality approaches while maintaining balance and fairness. Importantly, ethical safeguards like data privacy, human-in-the-loop review, and transparency are embedded to reduce bias and build student trust. The results indicate that integrating technical robustness with fairness-aware practices can provide institutions with a scalable and reliable solution that upholds academic integrity in digital assessments. Ultimately, this research highlights a pathway toward more trustworthy, inclusive, and ethical online examination systems that adapt to the evolving needs of modern education.

## REFERENCES

[1] T. Potluri, V. S. Venkata Krishna Kishore K., "An automated online proctoring system using Attentive-Net to assess student mischievous behavior," Multimedia Tools and Applications / Springer (Attentive-Net). SpringerLink+1
[2] S. Kaddoura and A. Gumaei, "Towards effective and efficient online exam systems using deep learning-based cheating detection approach," Intelligent Systems with Applications, 2022. ScienceDirect+1
[3] "A Systematic Review of Deep Learning Based Online Exam Proctoring Systems for Abnormal Student Behaviour Detection" (survey — compilation of OPS literature 2016–2022). ResearchGate
[4] E. Heinrich, "A Systematic-Narrative Review of Online Proctoring Systems and a Case for Open Standards," Open Praxis (systematic review and standards discussion). Open Praxis+1
[5] M. J. Hussein, "An Evaluation of Online Proctoring Tools" (tool evaluation & pilot testing; institutional guidance). Open Praxis
[6] S. Coghlan, T. Miller, and J. Paterson, "Good Proctor or 'Big Brother'? — Ethics of Online Exam Proctoring," BMC Medical Ethics / Frontiers / PMC (ethics, fairness, human-in-the-loop recommendations). PMC
[7] "Multi-Modal Online Exam Cheating Detection" — multi-camera / multi-modal detection approaches (gaze, audio, overlays). ResearchGate
[8] Paper on head-pose and gaze estimation for malpractice detection: "Detection of Malpractice in E-exams by Head Pose and Gaze Estimation" (technical methods for gaze/head cues). ResearchGate
[9] LivDet-Face / Face Liveness Detection competition materials — presentation-attack detection benchmarks for face liveness (important for spoof/deepfake defenses in proctoring). LivDet+1
[10] A. Benlamoudi et al., "Face Presentation Attack Detection Using Deep Learning" (PAD methods applicable to proctoring anti-spoofing). PMC
[11] B. Erdem, "Cheating Detection in Online Exams Using Deep Learning" (MDPI/Applied studies and model comparisons; recent methods). MDPI
[12] T. Scassa, "The Surveillant University: Remote Proctoring, AI, and Human Rights" (legal / human-rights and policy implications of proctoring). CJCCL+1
[13] "Students' Privacy and Security Perceptions of Online Proctoring Services" — analysis of student reviews and survey on privacy & security concerns. ResearchGate
[14] L. Slusky, "Cybersecurity of Online Proctoring Systems" (threats, operational controls, lockdown browser considerations). CSUSB ScholarWorks
[15] O. L. Holden et al., "Academic Integrity in Online Assessment: A Research Synthesis" (overview of lockdown browsers, their effects, and integrity methods). Frontiers
[16] G. Demartini et al., "Human-in-the-loop Artificial Intelligence for Fighting Online …" (HITL concepts and how to combine automated flags with human review). Damiano Spina
[17] M. Pooshideh, "Presentation Attack Detection: A Systematic Literature Review" (PAD survey useful for face spoofing / liveness sections). ACM Digital Library
[18] I. Balafrej et al., "Enhancing practicality and efficiency of deepfake detection" (improving speed and deployment of deepfake detectors — relevant to realtime proctoring). PMC
[19] Reports and analyses on lockdown/lockdown-browser tools (Respondus, etc.) — usage, pros/cons and student impacts (practical/UX sources). Teaching and Learning Resource Center+1
[20] Selected industry / applied references on deepfake/real-time detection and multilayer defenses (Intel FakeCatcher, Reality Defender, and vendor writeups on multilayer detection) — useful for the threat model and countermeasures section. Lifewire+2WIRED+2
[21] Goth, J., et al. (2021). Machine learning-based gaze estimation for remote student monitoring. VISAPP.
[22] Strielkowski, W., et al. (2022). Ethical dilemmas in using AI for academic integrity: The case of proctoring. AI and Ethics.
[23] Siau, K., et al. (2021). The effects of remote proctoring on testing integrity and student satisfaction. Information & Management.
[24] Lee, T. H. (2023). Leveraging blockchain for secure, decentralized, and transparent online exam results. Concurrency and Computation.
[25] Vural, K., et al. (2024). Integrating wearable sensors for physiological stress monitoring during online exams. Sensors.
[26] O'Connell, L., et al. (2022). A critical review of cheating typologies in distance education. Educational Technology Research and Development.
[27] Popović, V., et al. (2023). Multi-camera fusion for enhanced coverage in remote proctoring. Pattern Recognition Letters.
[28] Saragih, M. H., et al. (2022). Enhancing online exam security through randomized question generation and time limits. International Journal of Emerging Technologies in Learning.
[29] Wang, Z., et al. (2024). A differential privacy mechanism for student behavioral data in educational settings. Information Sciences.
[30] Hachipola, E. (2021). Fairness and accountability in automated proctoring systems: A case study. Journal of Responsible Technology.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY