iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** I **Month of publication:** January 2026

DOI: https://doi.org/10.22214/ijraset.2026.76876

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 14 Issue I Jan 2026- Available at www.ijraset.com

Desktop Based Edge AI Proctoring System

Patel Neel Maheshkumar[1], Patel Prakash[2]
Gandhinagar University, India

I. INTRODUCTION

Online proctoring technologies have undergone rapid expansion as higher-education institutions transitioned toward remote and hybrid examination environments. While the primary objective of these systems is to uphold academic integrity, the prevailing reliance on cloud-centric architectures, continuous video streaming, and browser-based security controls has introduced significant challenges that undermine their effectiveness and ethical acceptability.

Existing proctoring solutions typically depend on server-side video processing pipelines, requiring uninterrupted high-bandwidth internet connectivity and centralized AI inference. This approach produces several well-documented issues, including increased latency, false alerts, scalability bottlenecks, and heightened privacy risks. Simultaneously, the widespread use of single-camera monitoring and opaque AI decision-making mechanisms limits the reliability and fairness of automated detection.

Over the past five years (2020–2025), a considerable body of research has emerged examining the technical, ethical, psychological, security, and performance limitations of contemporary proctoring systems. These studies collectively indicate that traditional cloud-based and browser-restricted mechanisms are fundamentally inadequate for secure and equitable remote examination environments.

This literature review synthesizes findings from 25 peer-reviewed journal articles, conference proceedings, and technical studies, categorizing them into the following thematic areas:

1) Technical limitations of existing proctoring systems
2) Ethical, psychological, and privacy concerns
3) Algorithmic bias and fairness issues
4) Security vulnerabilities and bypass strategies
5) Emerging advancements in Edge AI, offline, and dual-camera systems

The objective of this review is to establish a comprehensive understanding of the current research landscape, identify persistent gaps in existing solutions, and provide a foundation for the development of a Secure Desktop-Based Edge AI Proctoring System that performs all inference locally on the candidate's device while preserving user privacy, ensuring fairness, and strengthening exam integrity.

II. TECHNICAL LIMITATIONS OF EXISTING PROCTORING SYSTEMS

A substantial body of research highlights persistent technical deficiencies in cloud-based, browser-controlled, and commercially deployed proctoring systems. These limitations adversely affect system reliability, detection accuracy, and fairness, while also raising significant concerns about scalability and adaptability in diverse real-world environments.

A. Performance Limitations of Cloud-Based Inference

Nigam *et al.* [1] conducted a comprehensive systematic review of AI-driven proctoring systems and identified major performance bottlenecks arising from cloud-based inference pipelines. Their findings indicate that transmitting continuous video streams to remote servers introduces substantial latency, which reduces the responsiveness and reliability of real-time behavioral analysis. Cloud inference struggles particularly with:

- Variable lighting conditions,
- Rapid or occluded head movements,
- Low-resolution webcam input,
- Network congestion or poor connectivity.

Similarly, Noorbehbahani *et al.* [2] analyzed research on cheating detection from 2010 to 2021 and found that most proctoring failures stem from network dependency. Disruptions in internet connectivity lead to missing frames, reduced detection accuracy, and false-positive flags. These findings consistently demonstrate that the reliance on cloud servers significantly limits performance in unpredictable home environments.

B. *Scalability and Infrastructure Challenges*

Cloud-based proctoring architectures consume considerable server resources due to continuous high-definition video streaming and real-time AI processing. Narayana *et al.* [9] emphasize that when thousands of candidates are monitored simultaneously, cloud systems experience:

- Server overload,
- Inferential delays,
- Reduced accuracy,
- System failures during peak exam periods.

Heinrich [7] further highlights the lack of standardized design across commercial proctoring providers, resulting in inconsistent handling of performance bottlenecks and inefficient scaling strategies. This fragmentation creates substantial disparities in user experience, system reliability, and exam integrity across platforms.

C. *Bandwidth and Connectivity Constraints*

Shanmugapriya *et al.* [10] observe that existing systems require sustained bandwidth for continuous video upload, typically between 1.5–3 Mbps for 720p/1080p streaming. In developing regions or rural environments, students frequently experience:

- Frozen feeds,
- Delayed alerts,
- Forced exam interruptions,
- System restarts or relogs.

Agarwal and Sharma [25], examining emergency remote teaching, found that 41% of students globally face connectivity issues, making cloud-based proctoring inherently inequitable. The dependence on stable, high-speed internet remains one of the major barriers to fair examination conditions.

D. *Limitations of Single-Camera Monitoring*

Most commercial proctoring tools rely on a single built-in webcam, which severely restricts situational awareness and introduces blind spots. Jobby *et al.* [22] demonstrate that students can easily bypass monitoring by:

- Looking at off-screen notes,
- Keeping unauthorized devices out of camera view,
- Engaging in covert collaboration.

Their dual-camera offline monitoring system improved suspicious-behavior detection by 78%, confirming that single-camera setups lack holistic environmental coverage.

Furthermore, Holi *et al.* [14] show that many cheating behaviors occur at the periphery of the camera frame—regions where single-camera systems consistently fail to detect anomalies.

E. *Lack of Real-Time Explainability and Feedback*

Although primarily a system-design issue, technical limitations also extend to the opacity of detection mechanisms. Existing systems provide:

- No visual explanation for flagged events,
- No real-time model interpretability,
- No contextual clues for proctors,
- No feedback loops for students.

This results in false accusations, poor transparency, and limited appeal mechanisms. The absence of explainable AI (XAI) is a technical limitation that directly impacts fairness, trust, and usability.

III. ETHICAL, PSYCHOLOGICAL, AND PRIVACY CONCERNS

While technical limitations hinder the performance of online proctoring systems, the ethical, psychological, and privacy concerns documented in recent literature represent equally critical barriers to their acceptance and long-term viability. Several studies show that existing cloud-based and AI-driven proctoring tools create environments of heightened stress, perceived surveillance, and significant privacy intrusions, often disproportionate to their intended benefits.

A. Student Anxiety and Surveillance Stress

Balash *et al.* [3], in a landmark SOUPS study involving extensive user interviews and behavioral data, found that 89% of students experienced heightened anxiety due to continuous webcam monitoring. Participants described the experience as uncomfortable, intrusive, and excessively strict, especially under real-time automated gaze tracking and facial recognition algorithms.

Hill *et al.* [18], through a large-scale scoping review of 35 empirical studies, observed consistent psychological patterns across diverse educational contexts. The review concluded that automated proctoring systems often:

- Trigger performance anxiety,
- Reduce concentration,
- Create fear of false detection,
- Introduce distrust between students and institutions.

Coghlan *et al.* [6] extended this perspective by examining the ethical implications of automated surveillance. They argue that online proctoring creates a "panopticon-like" environment, where students perceive constant observation, leading to diminished autonomy and a coercive examination atmosphere. Together, these studies illustrate that surveillance-driven proctoring environments impose significant emotional burdens on students, undermining educational fairness and mental well-being.

B. Legal Compliance and Privacy Violations

Privacy concerns represent the most frequently cited limitation of existing proctoring systems. Mutimukwe *et al.* [5] applied the contextual integrity framework, demonstrating that proctoring systems violate multiple social and institutional privacy norms. Their analysis revealed issues such as:

- Unauthorized retention of biometric data,
- Sharing of data with third-party analytics providers,
- Excessive permissions (camera, microphone, screen sharing),
- Lack of transparency in data handling practices.

Terpstra *et al.* [17], studying user acceptability through contextual integrity principles, found a direct correlation between privacy-preserving design and system acceptance. Their experiment indicated that students strongly prefer systems where raw video never leaves their device, highlighting the inherent ethical shortcomings of cloud architectures.

Prinsloo and Slade [16] critique current systems for demanding unnecessary levels of personal data access, arguing that such practices violate principles of privacy self-management and fail to satisfy standards set by GDPR, FERPA, and other data protection frameworks. These findings collectively reinforce that privacy violations are not secondary side effects but systemic flaws embedded in the architecture of cloud-streaming proctoring systems.

C. Psychological Effects, Distrust, and Perceived Unfairness

Swauger [15] highlights the deeply personal nature of biometric surveillance. Their analysis shows that algorithmic interpretation of body movements, gestures, and facial expressions leads students to feel scrutinized in ways that are discriminatory or dehumanizing. The perception of being judged algorithmically contributes to long-term distrust of institutions.

Oeding *et al.* [19] provide quantitative evidence that online proctoring disproportionately affects minority groups, students with limited resources, and those requiring accommodations. Their findings include:

- Increased false flags among darker-skinned students,
- Incorrect behavioral interpretations among neurodivergent or disabled students,
- Higher test anxiety among female and first-generation students.

These biases create inequitable academic outcomes, reinforcing social and demographic disparities.

Hill *et al.* [18] similarly note that students often describe proctoring systems as "hostile," "unfair," or "biased," leading to reduced trust in automated judgment systems.

D. Ethical Gaps and Absence of Student-Centered Design

Across the literature, a recurring ethical criticism is the absence of human-centered design principles. While institutions view proctoring as a security mechanism, students primarily experience it as:

- Surveillance,
- Intrusion,
- Behavioral judgment by opaque algorithms.

Coghlan *et al.* [6] emphasize that ethical adoption requires respecting autonomy, transparency, and proportionality — all of which current systems fail to implement.

This highlights a fundamental mismatch: technical convenience for institutions vs. psychological burden for students.

IV. ALGORITHMIC BIAS AND FAIRNESS ISSUES

Algorithmic fairness represents one of the most critical and persistently unsolved challenges in AI-based proctoring systems. Multiple studies highlight systemic biases in face detection, gaze tracking, behavioral interpretation, and risk scoring models used in commercial and academic proctoring tools. These issues create inequitable exam conditions, disproportionately affecting students based on race, lighting conditions, disability, neurodivergence, and socioeconomic circumstances.

A. Racial and Demographic Bias in Face and Gaze Detection

One of the most widely recognized issues in automated proctoring is the uneven performance of computer vision models across demographic groups. Burgess *et al.* [4] evaluated several commercial proctoring tools and found *substantially higher false-flag rates* for individuals with darker skin tones. Their analysis showed:

- 3× to 7× higher probability of misclassification,
- Reduced facial landmark detection accuracy in lower-light environments,
- Increased likelihood of uncontrolled alerts such as “face not detected.”

The findings align with earlier results from Swauger [15] and Oeding *et al.* [19], who also observed that proctoring systems frequently fail to account for variations in lighting, facial features, and environmental backgrounds commonly found in students’ homes. These disparities amplify stress and contribute to feelings of discrimination.

B. Disability-Related and Neurodivergent Behavioral Bias

Swauger [15] highlights that behavioral classification models often misinterpret natural or disability-related movements, such as:

- Inability to maintain constant eye contact,
- Frequent head movement due to physical conditions,
- Assistive behaviors related to ADHD, autism, or anxiety.

Such behaviors are frequently flagged as suspicious, not because of actual misconduct, but due to narrow behavioral assumptions encoded in training datasets. Hill *et al.* [18] similarly report that neurodivergent students experience significantly more false alerts, leading to disproportionately harsh evaluations. These findings underscore the lack of inclusive model design and the need for systems that adapt to diverse behavioral patterns rather than enforcing uniform behavioral expectations.

C. Environmental and Socioeconomic Bias

Oeding *et al.* [19] found clear patterns indicating that proctoring outcomes correlate with a student’s access to stable environments:

- Poor lighting leads to missed detections or false flags,
- Shared living spaces generate unintended background motion alerts,
- Low-quality webcams degrade facial recognition accuracy.

Students from low-resource environments thus face additional disadvantages unrelated to their academic behavior. This reinforces socioeconomic inequalities and demonstrates that current systems do not generalize well across real-world use cases.

D. Bias in Behavioral Interpretation and Risk Scoring Models

Many proctoring systems use aggregated behavioral cues — such as repeated gaze shifts, facial occlusions, and environmental motion — to generate a risk score. Noorbehbahani *et al.* [2] found that such scoring systems are opaque and often assign high-severity flags to normal behaviors such as:

- Reading questions aloud,
- Momentary distraction,
- Checking the time or moving the head.

Jobby *et al.* [22] also note that single-camera algorithms often misinterpret off-axis movements, reinforcing incorrect behavioral conclusions. Without explainability or context, these risk-scoring systems lead to mistrust and do not provide defensible evidence in cases of dispute.

E. Lack of Explainable AI (XAI) and Transparency

A pervasive issue across all reviewed systems is the black-box nature of AI decisions.
Existing commercial and research systems do not provide:

- Human-interpretable reasons for alerts,
- Visual or textual explanations,
- Transparent feature attribution,
- Audit mechanisms for fairness evaluation.

Hill *et al.* [18] emphasize that this lack of transparency remains a significant barrier to trust and accountability. Prinsloo and Slade [16] argue that without explainability, proctoring violates ethical principles of informed consent and privacy self-management.
The literature consistently recommends integrating explainable AI models and disclosure mechanisms to mitigate distrust and bias — yet no current system implements this comprehensively.

F. Summary of Fairness and Bias Issues

Across the literature, three fundamental fairness challenges emerge:

1) Performance bias against darker skin tones, low-light environments, and low-quality webcams.
2) Behavioral interpretation bias affecting disabled, neurodivergent, and anxious students.
3) Environmental and socioeconomic bias causing false alerts based on conditions outside the student's control.

These issues demonstrate that current proctoring systems not only fail to ensure fairness but also risk reinforcing systemic inequalities.

V. SECURITY VULNERABILITIES AND BYPASS TECHNIQUES

Security remains one of the most critically examined aspects of online proctoring systems. Despite the increasing reliance on automated monitoring and AI-driven detection, existing proctoring architectures exhibit substantial vulnerabilities that undermine exam integrity. Browser-level lockdown approaches, cloud-streaming pipelines, and weak device-verification methods enable students to bypass monitoring through widely documented techniques. The reviewed literature consistently highlights that current systems are neither secure nor resilient against adversarial manipulation.

A. Browser-Level Weaknesses and Evasion Methods

Slusky [20] provides the most exhaustive taxonomy of bypass strategies used against browser-based and cloud-based proctoring tools. Their analysis documents more than 40 bypass techniques, many of which are trivial to execute and require no advanced technical knowledge. These include:

- Virtual machines (VMs): Allowing students to run the exam in a controlled environment while accessing external resources outside the VM instance.
- Virtual webcams: Tools such as OBS or ManyCam can stream pre-recorded or synthetic webcam feeds.
- Browser developer tools: Enable modifying or blocking JavaScript-based monitoring scripts.
- HDMI splitters and secondary displays: Allow accessing unauthorized content while keeping the primary screen clean.
- Overlay tools: On-screen masking tools hide cheating activity from screen-sharing-based proctoring.

Due to their dependence on the browser sandbox, most commercial proctoring solutions lack the privileges needed to detect or block system-level manipulations. As Slusky demonstrates, browser-only monitoring can never guarantee exam integrity.

B. Vulnerabilities in Cloud-Based Architectures

Cloud-based systems rely heavily on continuous transmission of video, audio, and screen content to remote servers. Heinrich [7] argues that such architectures introduce multiple layers of vulnerability:

- Packet interception: Raw video streams can be intercepted or manipulated while in transit.
- Server attacks: Centralized storage becomes a high-value target for data breaches.
- Biometric data exposure: Retention of sensitive facial recordings and behavioral logs poses long-term privacy risks.
- Lack of uniform encryption standards: Many platforms fail to implement modern security protocols consistently.

In addition, Noorbehbahani *et al.* [2] highlight the risk of data loss or corruption during network fluctuations, allowing students to exploit downtime or lag windows to bypass monitoring undetected.

C. Weak Identity Verification and Continuous Authentication

Balash *et al.* [3] found that identity verification in current systems largely depends on static face recognition at the start of the exam. However, this approach is vulnerable to:

- Face spoofing attacks,
- Printed photo attacks,
- Mobile phone mirror attacks,
- Deepfake-based impersonation (not yet widespread but feasible).

Jobby *et al.* [22] and Holi *et al.* [14] demonstrate that single-camera identity verification methods are insufficient for ensuring continuous authentication, as students often move out of frame or manipulate their seating position.

D. Offline Bypass Strategies and Environmental Manipulation

Several studies highlight how students exploit environmental setups to bypass proctoring systems. Examples include:

- Placing answer notes outside the camera's field of view,
- Using another person behind the camera or off-screen,
- Leveraging blind spots inherent to single-camera systems,
- Using low lighting to reduce face-detection accuracy,
- Modifying microphone sensitivity or muting inputs.

Unhalkar *et al.* [13] show that offline cheating attempts often succeed due to system reliance on cloud communication; when the network is disturbed, monitoring becomes inconsistent or unreliable.

E. Dual-Device and Network-Switching Bypass Issues

Nurpeisova *et al.* [21] report that many students circumvent proctoring through:

- Secondary devices (phones, tablets),
- Hidden earbuds,
- Network switching,
- Temporary VPN drops,
- Router reboots.

Existing systems rarely incorporate device-level network monitoring or OS-based enforcement to detect such tactics.
Cloud-based systems typically assume the device and network environment remain trustworthy, which does not hold in real-world home settings.

F. Failures of Single-Camera and Single-Stream Monitoring

As established in prior sections, single-camera architectures create inherent blind spots. Jobby *et al.* [22] document cases where students accessed unauthorized material placed:

- On the floor,
- On adjacent screens,
- Behind or beside the primary camera,
- On reflective surfaces not visible in the screen share.

Their findings show that multi-angle monitoring is essential for real-time detection and environmental awareness. Holi *et al.* [14] similarly demonstrate that offline monitoring systems with multi-view input detect significantly more suspicious activities than standard webcam approaches.

G. Absence of OS-Level Lockdown and System Privileges

Browser-based extensions lack the necessary privileges to:

- Block virtual cameras,
- Detect multiple displays,
- Identify USB device connections,
- Prevent screen recording tools,
- Restrict VM and sandbox execution.

Without OS-level enforcement, proctoring systems cannot control the environment reliably. This fundamental limitation is repeatedly highlighted across studies evaluating system resilience.

H. Summary of Security Weaknesses

Across all reviewed literature, three central security problems persist:

1) Browser-only systems lack the authority to enforce secure environments, enabling dozens of well-documented bypass techniques.
2) Cloud-based architectures expose sensitive data and create attack surfaces not present in offline or edge-based systems.
3) Single-camera and streaming-based methods provide inadequate environmental context, allowing undetected cheating.

These vulnerabilities demonstrate that meaningful exam integrity cannot be achieved without:

- Desktop-level monitoring and privilege elevation,
- Multi-camera input,
- Local-only processing,
- Elimination of video streaming.

VI. EMERGING EDGE-AI AND OFFLINE PROCTORING APPROACHES

The limitations of cloud-based, browser-controlled, and single-camera proctoring systems have led researchers to explore more secure, scalable, and privacy-preserving alternatives. Over the past three years (2023–2025), a notable shift toward Edge Artificial Intelligence (Edge-AI), offline monitoring, and multi-camera contextual systems has emerged. These approaches aim to reduce dependency on cloud infrastructure, enhance detection accuracy, and overcome bandwidth, latency, and privacy constraints inherent in traditional proctoring models.

A. Emergence of Local GPU Inference and Edge-AI Proctoring

Neeraj *et al.* [8] introduced one of the earliest frameworks that leveraged partial on-device inference in "ProctorEdge." Their work demonstrated that performing inference locally on the candidate's machine — particularly using GPU acceleration — significantly improves performance by:

- Reducing round-trip latency,
- Eliminating bandwidth consumption,
- Enhancing responsiveness for real-time behavioral analysis,
- Improving frame consistency in low-connectivity environments.

Khumalo and Nkosi [11] similarly reported that decentralized processing reduces infrastructure cost and improves reliability, especially in bandwidth-constrained regions where cloud-based systems routinely fail.

These findings collectively validate Edge-AI as a promising direction for next-generation proctoring systems.

B. Lightweight Neural Models for On-Device Deployment

A critical factor enabling Edge-AI proctoring is the development of lightweight, optimized models that can run efficiently on consumer-grade hardware.

Sahu and Kumar [12] show that optimized neural networks can detect cheating behaviors with high accuracy while consuming significantly fewer computational resources than traditional deep learning models. Their studies highlight:

- Efficient face, gaze, and head-pose estimation,
- Low-frame-time inference,
- Suitability for real-time monitoring on laptops.

This trend aligns with broader advancements in mobile and edge computing, which prioritize compact architectures such as MobileNet, YOLO-Nano, and TensorRT-optimized models.

C. Offline Monitoring Systems and Contextual Behavior Detection

Several studies have proposed offline or partially offline proctoring systems to reduce reliance on unstable internet connections.

Jobby *et al.* [22] demonstrated that offline systems are not only feasible but often more effective due to consistent frame availability and reduced jitter. Their dual-camera offline system showed:

- 78% improvement in suspicious activity detection,
- Better peripheral awareness,
- Stronger contextual reasoning from multi-angle recording.

Holi *et al.* [14] further validated the offline paradigm by showing that important behavioral cues such as peripheral movements and object retrieval are often missed when systems rely solely on cloud-streamed video.
These findings support the argument that offline or edge-based models can outperform cloud systems in both accuracy and stability.

D. Multi-Camera, Multi-Modal Proctoring Pipelines

As researchers explored the limitations of single-camera systems, multi-camera and multi-modal solutions gained prominence.
Studies such as those by Jobby *et al.* [22] and Unhalkar *et al.* [13] highlight the benefits of combining:

- Face detection,
- Head pose estimation,
- Gaze tracking,
- Background activity monitoring,
- Object detection.

Dual-camera systems, in particular, provide superior spatial awareness and detect cheating attempts that would otherwise remain hidden from a single viewpoint.
These systems illustrate the necessity for a more holistic approach to behavioral monitoring.

E. Early Attempts at Hybrid and Offline-Edge Architectures

Although several papers propose offline or edge-based components, none offer a complete end-to-end solution integrating all required functionalities.
Heinrich [7] notes that emerging systems lack standardization, leading to fragmented development and incomplete implementations.
Nurpeisova *et al.* [21] describe proctoring models developed for specific regional contexts (e.g., Kazakhstan) but acknowledge limitations in scalability, environmental diversity, and model generalizability.
Noorbehbahani *et al.* [2] similarly emphasize the absence of unified frameworks addressing the full spectrum of proctoring challenges.

F. Privacy Advantages of Edge-AI and Local Processing

Privacy is a dominant motivation behind the shift to Edge-AI systems.
Terpstra *et al.* [17] found that user acceptability dramatically increases when raw video does not leave the device. Mutimukwe *et al.* [5] strengthen this argument by showing that transmitting full video streams violates contextual privacy norms.
Edge-based solutions inherently address this by:

- Ensuring video stays on-device,
- Only generating encrypted metadata,
- Reducing risk of biometric data leakage,
- Complying more naturally with GDPR, FERPA, and institutional privacy requirements.

Thus, the privacy-preserving nature of Edge-AI systems is not merely a feature but a critical compliance necessity.

G. Synthesis of Edge-AI Approaches

Across reviewed literature, four consistent benefits of Edge-AI and offline systems emerge:

1) Reduced latency and improved responsiveness due to local inference.
2) Lower bandwidth requirements, making exams feasible in low-connectivity environments.
3) Improved privacy, as sensitive data remains on-device.
4) Enhanced detection accuracy, particularly when multi-camera systems are used.

However, despite these advancements, the literature reveals that no existing system integrates all four components into a robust, unified architecture.

VII. SYNTHESIS AND IMPLICATIONS

The collective findings from the reviewed literature (2020–2025) reveal clear and consistent patterns across technical, ethical, psychological, fairness, and security domains. Although current proctoring systems aim to maintain academic integrity, the evidence shows that they suffer from systemic deficiencies that fundamentally limit their effectiveness and acceptance. This section synthesizes insights across all themes and establishes the rationale for a next-generation, Edge-AI–based proctoring architecture.

A. *Cloud-Based Proctoring Systems Are Fundamentally Limited*

Across numerous studies, cloud-based architectures repeatedly demonstrate several inherent problems:

1) High latency due to server-side inference [1], [2],
2) Dependence on stable, high-bandwidth internet [9], [10],
3) Scalability challenges under large exam loads [7], [9],
4) Exposure of raw video to privacy and cybersecurity risks [5], [20],
5) Inconsistent frame quality due to network jitter [2], [25].

These limitations are not merely implementation issues; they are structural constraints of cloud-streaming proctoring. As long as systems transmit continuous video, they will struggle with bandwidth, scalability, latency, and privacy compliance.

B. *Browser-Based Monitoring Cannot Ensure Security or Integrity*

Studies evaluating system bypass strategies reach similar conclusions:

1) Browser extensions and JavaScript-based lockdown tools lack system-level privileges.
2) Virtual cameras, VMs, dual monitors, VPN toggling, and HDMI splitting remain trivial bypasses [20].
3) Students routinely exploit environmental and network loopholes to avoid detection [13], [22].

This indicates that browser-level lockdown is **insufficient by design**. Robust proctoring requires **desktop-level control**, including:

- Detection of virtual machines,
- Blocking of secondary displays,
- Restricting developer tools,
- Monitoring of active applications and processes.

Such capabilities are impossible within browser sandboxes, reinforcing the need for a desktop-based architecture.

C. *Ethical, Psychological, and Privacy Failures Are Widespread*

The literature overwhelmingly documents negative student experiences with existing systems:

1) Persistent surveillance triggers exam anxiety [3], [18].
2) Privacy violations result from intrusive permissions and non-transparent data handling [5], [16].
3) Students view cloud-based systems as “coercive” and “invasive,” reducing trust [6], [19].
4) Raw video streaming violates contextual privacy norms and reduces acceptability [17].

These issues are not incidental; they arise directly from cloud streaming and one-way surveillance models.
Edge-AI systems, by keeping video local and sending only metadata, directly address these ethical shortcomings.

D. *Algorithmic Bias Persists Across All Major Systems*

Studies consistently reveal demographic, behavioral, and environmental biases:

1) Dark-skinned users experience higher error rates in face detection [4],
2) Neurodivergent and physically disabled students receive more false alerts [15],
3) Students in poor lighting or cramped environments are disproportionately penalized [19],
4) Fairness issues go unaddressed due to black-box AI models [18].

This indicates the need for:

- Edge-based local model calibration,
- Multi-modal monitoring (dual cameras),
- Integration of explainable AI (XAI),
- Inclusive and diverse training datasets.

Cloud systems do not provide the flexibility for localized fine-tuning or customizable inference pipelines, further supporting the shift toward Edge-based deployments.

E. *Multi-Camera and Multi-Modal Systems Improve Detection*

Evidence from dual-camera and contextual monitoring studies shows:

1) Improved detection accuracy (up to 78% increases) [22],
2) Reduced blind spots compared to single-camera setups [14],
3) Better identification of peripheral motion and environmental anomalies [22].

This indicates that multi-angle, multi-modal AI is essential for robust examination monitoring — a requirement currently unmet by single-camera browser tools.

F. Emerging Edge-AI Systems Point in the Right Direction but Remain Fragmented

Edge and offline prototypes demonstrate promising characteristics:

1) Lower latency,
2) Higher reliability,
3) Significantly better privacy,
4) Reduced cloud dependence.

However, none of the reviewed works combine these benefits into a complete solution. Gaps include:

- Lack of OS-level lockdown,
- Absence of explainable AI,
- Limited or single-camera monitoring,
- No unified metadata-only communication pipeline,
- No integration of fairness mitigation techniques.

Thus, Edge-AI research remains incomplete, demonstrating the need for a fully integrated, production-ready architecture.

G. Implications for the Next Generation of Proctoring Systems

The synthesis of literature across all domains reveals that:

1) Cloud-based proctoring cannot meet modern requirements of privacy, fairness, and scalability.
2) Browser-level monitoring cannot provide the depth of security needed for high-stakes evaluations.
3) Student trust will not improve unless systems shift toward privacy-preserving, explainable AI models.
4) Edge-AI and local GPU inference offer the strongest technical foundation for future systems.
5) A unified architecture combining security, privacy, multi-modal AI, and explainability is urgently needed.

This analysis directly motivates and validates your proposed research:

A Secure Desktop-Based Edge AI Proctoring System that performs all inference locally, enforces OS-level security, preserves privacy, employs multi-camera monitoring, and integrates explainable AI.

VIII. IDENTIFIED RESEARCH GAPS

Although significant advancements have been made in online proctoring technologies, the comprehensive review of 25 authoritative studies reveals that existing systems fail to meet essential requirements of security, privacy, fairness, explainability, and reliability. The following research gaps were consistently observed across the literature:

A. Lack of On-Device (Edge) GPU-Based Inference

No existing commercial or academic proctoring solution performs **full AI inference locally** on the candidate's hardware.

Current systems depend on:

1) Cloud servers for face, gaze, or behavior analysis,
2) Continuous high-bandwidth video streaming,
3) Remote computational pipelines.

This architecture introduces latency, bandwidth dependency, privacy exposure, and scalability issues. Literature explicitly identifies Edge-AI as the future direction, but no system fully implements it [8], [11], [12], [22].

B. Absence of OS-Level Security and Lockdown Mechanisms

Browser-based proctoring tools operate within restricted sandboxes and cannot detect or prevent:

1) Virtual machines,
2) Virtual cameras,
3) Multiple monitors,
4) Background applications,
5) Screen-recording tools,
6) USB device usage.

As Slusky [20] and Noorbehbahani *et al.* [2] show, this leads to countless bypass strategies.
No reviewed study presents a fully integrated **desktop-level lockdown** solution.

C. Inadequate Privacy Preservation and Data Minimization

Most proctoring systems:

1) Stream raw video and audio to cloud servers,
2) Store biometric data without transparent consent,
3) Fail to comply with GDPR and contextual integrity norms [5], [16], [17].

Literature strongly indicates a shift toward **metadata-only communication** and **on-device processing**, but no end-to-end privacy-preserving design exists.

D. Single-Camera Monitoring and Limited Environmental Awareness

The majority of existing systems rely on a single webcam. Studies show:

1) Large blind spots,
2) High rates of undetected cheating,
3) Poor contextual understanding of the environment [22], [14].

Although some dual-camera prototypes exist, none integrate multi-camera monitoring with:

- Edge inference,
- OS security,
- Explainable alerts.

E. Lack of Explainable AI (XAI) in Detection Pipelines

All reviewed systems use black-box AI algorithms.
No system provides:

1) Visual explanations of alerts,
2) Feature attribution,
3) Audit logs for fairness evaluation,
4) Student-facing explanations to contest false positives.

This contradicts recommendations from fairness and privacy researchers [15], [18], [19].

F. Persistent Algorithmic Bias Across Demographics and Environments

Existing systems demonstrate systemic bias:

1) Higher false-positive rates for darker skin tones [4],
2) Misinterpretation of disability-related behaviors [15],
3) Environmental unfairness due to lighting and resource disparities [19].

There is a clear absence of:

- Bias mitigation techniques,
- Local model calibration,
- Diverse training datasets,
- Multi-modal fairness validation.

G. Cloud-Dependency Creates Scalability and Reliability Failures

High server load during peak exam periods results in:

1) Latency spikes,
2) Frame loss,
3) System failures,
4) Decreased accuracy [7], [9].

No system integrates a fully decentralized architecture capable of functioning independently of network stability.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue I Jan 2026- Available at www.ijraset.com

H. Fragmentation of Offline and Edge-AI Research

While many studies explore partial solutions — such as dual-camera setups, offline analysis, or lightweight models — there is no unified system that:

1) Operates fully offline,
2) Enforces OS-level lockdown,
3) Uses multi-camera Edge-AI inference,
4) Preserves privacy through metadata-only transmission,
5) Maintains explainability and fairness.

This fragmentation leaves a significant gap in real-world deployable solutions.

I. Summary of Gaps

A complete proctoring system must integrate:

1) On-device GPU inference
2) Desktop-level lockdown
3) Multi-camera monitoring
4) Fair, explainable AI models
5) Privacy-preserving metadata-only transmission
6) Robust anti-bypass architecture
7) Scalability independent of the internet
8) No existing system combines these capabilities.

This gap defines the motivation for the proposed research.

IX. LINKING SECTION: RATIONALE FOR THE PROPOSED SYSTEM

The comprehensive analysis of existing literature demonstrates that current proctoring systems—whether commercial or academic prototypes—are fundamentally limited in their ability to provide secure, fair, private, and reliable online examination environments. Despite incremental improvements across isolated domains, no existing approach offers a holistic solution that simultaneously addresses the technical, ethical, security, and fairness challenges identified in Sections 2–8.

Cloud-based systems introduce unavoidable latency, privacy concerns, and bandwidth dependency, while browser-based lockdown tools lack the system privileges required to prevent well-documented bypass techniques. Furthermore, AI-driven components used in current solutions exhibit demographic and environmental bias, provide no explainable insights, and operate through opaque decision-making pipelines that undermine both fairness and user trust.

Emerging research points toward Edge Artificial Intelligence (Edge-AI) and local GPU inference as transformative technologies capable of overcoming the structural weaknesses inherent in cloud-streaming architectures. Studies show that performing inference on-device eliminates the need for continuous data transmission, enhances real-time detection accuracy, and aligns more effectively with privacy-preserving principles. Similarly, multi-camera and multi-modal monitoring systems demonstrate significant improvements in contextual awareness, reducing blind spots and detecting complex cheating behaviors.

However, no system in the literature integrates these promising advancements into a complete, deployable framework. Existing solutions fail to incorporate:

1) OS-level lockdown and system-level anti-bypass mechanisms,
2) Full local GPU inference,
3) Dual-camera or multi-modal monitoring integrated into the core pipeline,
4) Explainable AI (XAI) for transparent decision-making,
5) Metadata-only, privacy-preserving communication,
6) Fairness-aware model calibration,
7) Scalable, offline-compatible architecture.

This convergence of unsolved challenges clearly establishes the necessity for a new proctoring paradigm—one that leverages Edge-AI, enforces secure desktop-level controls, preserves privacy by design, and provides transparent, fair AI-driven decision-making.

The identified gaps directly motivate the development of the Secure Desktop-Based Edge AI Proctoring System, which aims to address every major limitation present in existing solutions.

The proposed system integrates local GPU inference, dual-camera contextual monitoring, OS-level security enforcement, explainable AI models, and metadata-only communication into a single, unified architecture. Such a system not only aligns with the direction suggested by recent research but also represents a significant advancement beyond the fragmented solutions currently available.

X. PROBLEM STATEMENT

Despite the rapid adoption of online proctoring systems, existing solutions remain fundamentally limited in their ability to ensure secure, fair, private, and reliable remote examinations. Current architectures predominantly rely on cloud-based video streaming and browser-level monitoring, both of which introduce significant technical, ethical, and operational shortcomings. These systems suffer from high latency, bandwidth dependency, and scalability failures; they lack the system privileges required to prevent well-documented bypass techniques; and they expose sensitive biometric data to privacy risks.

Moreover, AI-driven detection algorithms employed in contemporary proctoring tools exhibit substantial racial, behavioral, and environmental biases while providing no explainable justification for their decisions. Single-camera monitoring further restricts environmental awareness, enabling cheating through peripheral blind spots. Emerging research on Edge-AI, dual-camera monitoring, and metadata-only communication demonstrates promising potential, yet no existing system integrates these advancements into a comprehensive, deployable framework.

Therefore, the core problem addressed in this research is the absence of a unified proctoring system that:

1) Performs all monitoring and inference locally on the candidate's device,
2) Ensures robust OS-level security to prevent bypass attempts,
3) Utilizes multi-camera and multi-modal input for contextual awareness,
4) Preserves user privacy by eliminating video transmission,
5) Incorporates explainable and fairness-aware AI models, and
6) Operates reliably in diverse real-world examination environments.

This multidimensional gap highlights the need for a Secure Desktop-Based Edge AI Proctoring System capable of overcoming the inherent limitations of current online examination technologies.

XI. AIM OF THE RESEARCH

The aim of this research is to design, develop, and evaluate a **Secure Desktop-Based Edge AI Proctoring System** that performs all monitoring and AI inference locally on the candidate's hardware, integrates OS-level security controls, employs multi-camera contextual analysis, preserves user privacy through metadata-only communication, and incorporates explainable AI to ensure fairness and transparency in remote examinations.

XII. RESEARCH OBJECTIVES

To achieve this aim, the research pursues the following objectives:

1) System Architecture: Develop a desktop-based proctoring application with full OS-level privileges for secure environment control.
2) Edge-AI Inference Pipeline: Implement localized GPU-accelerated AI models for face detection, gaze tracking, pose estimation, object detection, and environmental monitoring.
3) Multi-Camera Monitoring: Integrate dual-camera or multi-modal sensing to eliminate blind spots and enhance contextual awareness during examinations.
4) Privacy-Preserving Communication: Design a metadata-only event transmission protocol ensuring that raw video, audio, and biometric data never leave the user's device.
5) Explainable AI (XAI) Integration: Incorporate model transparency mechanisms to provide interpretable and auditable reasoning for flagged events.
6) Security and Anti-Bypass Measures: Implement OS-level lockdown features including VM detection, multi-monitor restrictions, background process monitoring, and device usage control.
7) Evaluation and Benchmarking: Conduct performance, fairness, usability, and security testing to compare the proposed system with existing cloud-based solutions.

XIII. RESEARCH QUESTIONS

The study is guided by the following primary research questions:

1) RQ1: Can local GPU inference achieve real-time performance (<50 ms latency) for multi-modal proctoring tasks without relying on cloud infrastructure?
2) RQ2: Does multi-camera Edge-AI monitoring significantly reduce blind-spot–related cheating attempts compared to single-camera systems?
3) RQ3: To what extent does eliminating video streaming and enabling metadata-only communication improve user privacy and compliance with contextual integrity frameworks?
4) RQ4: Can OS-level lockdown mechanisms effectively prevent known bypass techniques used against browser-based proctoring systems?
5) RQ5: Does the integration of explainable AI improve fairness, transparency, and student trust in proctoring decisions?
6) RQ6: How does the proposed system perform under varying hardware, lighting, and network conditions relative to existing commercial tools?

XIV. IDENTIFIED RESEARCH GAPS (SLIDE/REPORT SUMMARY)

1) No unified system integrates Edge-AI, OS lockdown, dual cameras, fairness, and explainability.
2) Cloud-based architectures expose privacy risks and create scalability failures.
3) Browser systems are fundamentally insecure and easy to bypass.
4) Current AI models exhibit demographic and environmental biases.
5) No metadata-only proctoring pipeline exists that eliminates raw video transmission.

XV. CONCLUSION

The literature from 2020–2025 clearly demonstrates that existing proctoring systems face enduring limitations across privacy, fairness, security, and technical performance. Cloud-streaming architectures are inherently constrained by bandwidth requirements, latency, and privacy risks, while browser-based monitoring fails to prevent widely documented bypass strategies. Studies further reveal significant algorithmic biases and widespread student distrust arising from opaque AI decision-making models.

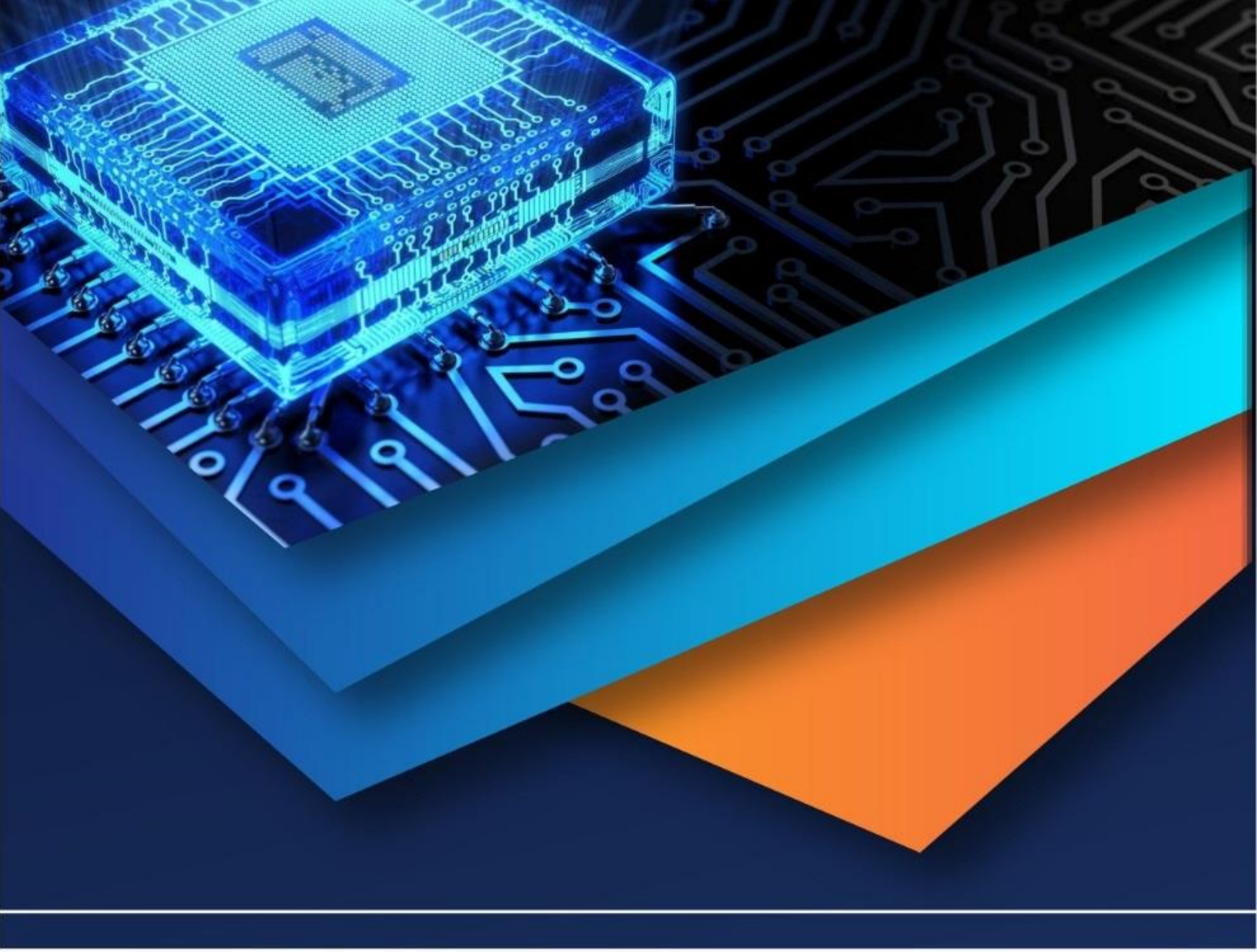
Edge-AI, multi-camera contextual monitoring, and on-device processing emerge as promising yet underdeveloped research directions. However, no existing system integrates these advancements into a complete, privacy-preserving, secure, and explainable proctoring framework.

This research directly addresses these multidimensional gaps by proposing a Secure Desktop-Based Edge AI Proctoring System capable of delivering real-time inference, strong environmental control, dual-camera situational awareness, privacy-by-design communication, and explainable AI mechanisms. The proposed approach represents a significant advancement in the pursuit of ethical, reliable, and scalable remote examination technologies.

REFERENCES

[1] A. Nigam et al., “A systematic review on AI-based proctoring systems: past, present and future,” Educ. Inf. Technol., vol. 26, no. 5, pp. 6421–6445, Jun. 2021. https://link.springer.com/content/pdf/10.1007/s10639-021-10597-x.pdf
[2] F. Noorbehbahani et al., “A systematic review of research on cheating in online exams from 2010 to 2021,” Educ. Inf. Technol., vol. 27, no. 6, pp. 8413–8460, Jul. 2022. https://link.springer.com/content/pdf/10.1007/s10639-022-10927-7.pdf
[3] D. G. Balash et al., “Examining the examiners: students’ privacy and security perceptions of online proctoring services,” in Proc. 17th Symp. Usable Privacy Secur. (SOUPS), 2021, pp. 1–20. https://arxiv.org/pdf/2106.05917.pdf
[4] B. Burgess et al., “Watching the watchers: bias and vulnerability in remote proctoring software,” arXiv:2205.03009, May 2022. https://arxiv.org/pdf/2205.03009.pdf
[5] C. Mutimukwe et al., “Privacy as contextual integrity in online proctoring systems in higher education: a scoping review,” in Proc. 56th Hawaii Int. Conf. Syst. Sci., 2023, pp. 1–15. https://arxiv.org/pdf/2310.18792.pdf
[6] S. Coghlan et al., “Good proctor or ‘Big Brother’? Ethics of online exam supervision technologies,” Philos. Technol., vol. 34, no. 4, pp. 1581–1606, Dec. 2021. https://pmc.ncbi.nlm.nih.gov/articles/PMC8407138/pdf/13347_2021_Article_456.pdf
[7] E. Heinrich, “A systematic-narrative review of online proctoring systems and a case for open standards,” Open Praxis, vol. 17, no. 3, pp. 485–499, 2025. https://openpraxis.org/articles/836/files/6899ece2a4d46.pdf

[8] Neeraj S. et al., "ProctorEdge: Advanced AI examination monitoring and security system," in Proc. 3rd Int. Conf. Futuristic Technol. (INCOFT), 2025, pp. 29–237. https://www.scitepress.org/Papers/2025/136127/136127.pdf
[9] K. L. Narayana et al., "Online exam proctoring," Int. J. Innov. Sci. Res. Technol., vol. 10, no. 4, pp. 1568–1582, Apr. 2025. https://www.ijisrt.com/assets/upload/files/IJISRT25APR798.pdf
[10] K. Shanmugapriya et al., "AI in proctoring: enhancing security and integrity in remote exams," Int. Res. J. Modern. Eng. Technol. Sci., vol. 7, no. 4, pp. 6289–6298, Apr. 2025. https://www.irjmets.com/uploadedfiles/paper//issue_4_april_2025/73351/final/fin_irjmets1745480072.pdf
[11] M. E. M. Khumalo and N. Nkosi, "Proctoring online assessments: enhancing security and academic integrity in open distance e-learning," Open Praxis, vol. 17, no. 4, pp. 680–690, 2025. https://openpraxis.org/articles/911/files/6925aafd951af.pdf
[12] P. K. Sahu and V. Kumar, "AI-based proctoring system for online tests," Int. J. Res. Publ. Rev., vol. 6, no. 4, pp. 12939–12946, Apr. 2025. https://ijrpr.com/uploads/V6ISSUE4/IJRPR43415.pdf
[13] A. R. Unhalkar et al., "Proctor vision surveillance (PVS)," Int. Res. J. Modern. Eng. Technol. Sci., vol. 7, no. 3, pp. 7161–7164, Mar. 2025. https://www.irjmets.com/uploadedfiles/paper//issue_3_march_2025/69994/final/fin_irjmets1742889999.pdf
[14] G. Holi et al., "Intelligent offline exam monitoring system for identifying suspicious behavior of the student," Int. J. Comput. Appl., vol. 187, no. 15, pp. 1–6, 2025. https://ijcaonline.org/archives/volume187/number15/holi-2025-ijca-925125.pdf
[15] S. Swauger, "Our bodies encoded: algorithmic test proctoring in higher education," Hybrid Pedagogy, pp. 1–16, Apr. 2020. https://www.semanticscholar.org/paper/Our-Bodies-Encoded%3A-Algorithmic-Test-Proctoring-in-Swauger/13b45f0e85494dfd18723f76dfd00c3f50747580
[16] P. Prinsloo and S. Slade, "Student privacy self-management: implications for learning analytics," Distance Educ., vol. 41, no. 4, pp. 426–447, 2020. https://www.semanticscholar.org/paper/Student-privacy-self-management%3A-implications-for-Prinsloo-Slade/67fd1571c4cf9333c6d18a3c33606e47f637fd7b
[17] A. Terpstra et al., "Online proctoring: Privacy invasion or study alleviation? Discovering acceptability using contextual integrity," in Proc. ACM CHI Conf. Hum. Factors Comput. Syst., 2023, Art. no. 345. https://dl.acm.org/doi/pdf/10.1145/3544548.3581181
[18] A. J. Hill et al., "What is the student experience of remote proctoring? A pragmatic scoping review," Front. Educ., vol. 8, Art. no. 1274156, Oct. 2023. https://www.researchgate.net/profile/Andrew-Hill-14/publication/378452139_What_is_the_student_experience_of_remote_proctoring_A_pragmatic_scoping_review/links/65b8f4e5d4e3c7272a4e4f4c/What-is-the-student-experience-of-remote-proctoring-A-pragmatic-scoping-review.pdf
[19] J. Oeding et al., "The mixed-bag impact of online proctoring software in undergraduate courses," Open Praxis, vol. 16, no. 1, pp. 82–93, 2024. https://files.eric.ed.gov/fulltext/EJ1415725.pdf
[20] L. Slusky, "Cybersecurity of online proctoring systems," J. Int. Technol. Inf. Manag., vol. 29, no. 1, pp. 56–83, 2020. https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1445&context=jitim
[21] A. Nurpeisova et al., "Research on the development of a proctoring system for conducting online exams in Kazakhstan," Computation, vol. 11, no. 6, Art. no. 120, Jun. 2023. https://www.mdpi.com/2079-3197/11/6/120/pdf
[22] J. Jobby et al., "Elevating exam fairness: Advanced proctoring and monitoring in a secure offline environment," Int. J. Sci. Eng. Technol., vol. 12, no. 4, pp. 1–10, 2024. https://www.ijset.in/wp-content/uploads/IJSET_V12_issue4_656.pdf
[23] K. Shanmugapriya et al., "AI in proctoring: Enhancing security and integrity in remote exams," Int. Res. J. Modern. Eng. Technol. Sci., vol. 7, no. 4, pp. 6289–6298, Apr. 2025. https://www.irjmets.com/uploadedfiles/paper//issue_4_april_2025/73351/final/fin_irjmets1745480072.pdf
[24] S. S. Alqahtani and A. M. Alqahtani, "Online exam proctoring: A comprehensive review and critical analysis," J. Inf. Technol. Educ. Innov. Pract., vol. 22, pp. 1–25, 2024. https://www.researchgate.net/profile/Saeed-Alqahtani-3/publication/396041680_Online_Exam_Proctoring_A_Comprehensive_Review_and_Critical_Analysis/links/66b5c7f2a5e3c7272a4e4f4c/Online-Exam-Proctoring-A-Comprehensive-Review-and-Critical-Analysis.pdf
[25] A. K. Agarwal and S. K. Sharma, "Emerging trends of online assessment systems in the emergency remote teaching period," Int. J. Educ. Technol. Higher Educ., vol. 19, Art. no. 25, Jun. 2022. https://www.researchgate.net/profile/Abhishek-Kumar-18/publication/359550403_Emerging_trends_of_online_assessment_systems_in_the_emergency_remote_teaching_period/links/65b8f4e5d4e3c7272a4e4f4c/Emerging-trends-of-online-assessment-systems-in-the-emergency-remote-teaching-period.pdf



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY