Beyond Face Recognition: A Multi-Layered Approach to Academic Integrity in Online Exams

Aivar Sakhipov[1,2], Islam Omirzak[1] and Alexey Fedenko[1]
[1]Department of Computer Engineering, Astana IT University, Astana, Kazakhstan
[2]Department of Computer Science, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan

aivar.sakhipov@astanait.edu.kz
islamomirzak88@gmail.com (corresponding author)
supp.fed@gmail.com

https://doi.org/10.34190/ejel.23.1.3896

Abstract: Ensuring academic integrity in online assessments is crucial for upholding fairness and credibility, especially with the widespread adoption of remote learning. This research addresses key vulnerabilities in preventing cheating and unauthorized collaboration, common in online assessments lacking direct supervision. To address these challenges, an intelligent proctoring system was developed and tested on BlockchainStudy.kz — an educational platform that offers online courses and issues blockchain-based certificates. This system establishes a controlled examination environment through facial recognition, user activity monitoring, and browser behavior tracking, effectively deterring dishonest practices. The study adopted a phased methodology, starting with pilot testing for feasibility, followed by large-scale deployment to assess scalability and effectiveness. The approach combines machine learning-based facial recognition for identity verification, user action logging, and browser monitoring to detect suspicious behaviors indicative of academic dishonesty. Findings demonstrated a marked decrease in cheating incidents, enhanced examination credibility, and improved perceptions of fairness among both students and instructors. By encouraging accountability, the system fostered a culture of honesty within the online education environment. Ethical concerns regarding privacy were addressed through robust safeguards in compliance with General Data Protection Regulation (GDPR), building student trust in the proctoring system. This research contributes to the field of e-learning by providing a scalable, effective solution for maintaining academic integrity in online assessments. It facilitates informed decision-making for educators, reduces dishonest behavior, and promotes a culture of integrity within digital education. Overall, this work enriches the body of e-learning knowledge by presenting a practical, adaptable strategy for overcoming the complex challenges of academic integrity in remote learning environments.

Keywords: Academic integrity, Intelligent proctoring, Machine learning, Blockchain, Online education, Cheating prevention

1. Introduction

The rapid expansion of online education has revolutionized the accessibility of learning, offering flexibility and inclusivity. However, it has also led to an alarming rise in academic dishonesty, posing significant challenges to assessment integrity (Dawson, 2021). Ensuring that online assessments are conducted fairly and honestly is increasingly difficult, given the remote nature of such exams and the lack of direct supervision (Bretag et al., 2019). The shift to online learning, accelerated by the COVID-19 pandemic, has exacerbated these challenges, leading to a rise in incidents of academic dishonesty, such as cheating and unauthorized collaboration (Lancaster and Cotarlan, 2021; Eaton, 2020).

Recent studies confirm a troubling surge in academic dishonesty in online assessments, particularly following the widespread shift to remote learning. A systematic review by Newton and Essex (2024) found that self-reported cheating rates in online exams increased from 29.9% before the pandemic to 54.7% during the pandemic, highlighting the growing prevalence of misconduct in remote education settings (Newton and Essex, 2024). Similarly, multiple universities in the United States, including the University of Missouri, North Carolina State University, Georgia Tech, and Boston University, reported substantial rises in academic dishonesty cases in online courses (Brandeis University, 2020). A study conducted in Pakistan revealed that 60% of students admitted to frequently cheating during online exams, with an additional 30% acknowledging they had cheated at least once (Malik et al., 2023). These findings illustrate the increasing sophistication of cheating strategies, such as the use of encrypted messaging apps and contract cheating services, reinforcing the urgent need for more effective and technologically advanced measures to uphold academic integrity in digital learning environments.

A viable solution to this challenge is implementing intelligent proctoring systems. These systems are designed to create a controlled examination environment by employing tools like facial recognition, behavior analysis,

Cite this article: Sakhipov, A., Islam Omirzak, I. and Fedenko, A. 2025. "Beyond Face Recognition: A Multi-Layered Approach to Academic Integrity in Online Exams", *Electronic Journal of e-Learning*, 23(1), pp 81-95, https://doi.org/10.34190/ejel.23.1.3896

and browser activity tracking (Nigam et al., 2021). Unlike traditional proctoring approaches, which often rely solely on browser lockdowns or restricted access to external resources, advanced proctoring integrates multi-faceted monitoring techniques, including face recognition, user activity logging, and automated detection of suspicious behavior, ensuring that examinations remain secure and credible.

Ensuring the integrity of online assessments is essential for maintaining the credibility of educational qualifications, as academic dishonesty undermines both individual learning outcomes and institutional reputation. (Bretag et al., 2018). Studies indicate that students are more likely to cheat when they perceive few consequences or a low risk of detection (Gamage et al., 2023). Thus, the deployment of such systems provides a deterrent against cheating, encouraging students to prepare adequately for exams and adhere to academic ethics (Dawson, 2021).

Despite the increasing adoption of online proctoring, concerns persist regarding its effectiveness in reducing cheating, ensuring fairness, and mitigating student stress. This study investigates the extent to which advanced automated systems can enhance academic integrity while maintaining a balanced and ethical approach.

To explore this, the study aims to answer the following research question: *How do intelligent proctoring systems impact cheating prevention, fairness, and student stress in online assessments?*

To answer this question, this paper examines the implementation and effectiveness of an advanced proctoring system on BlockchainStudy.kz, an educational platform that offers online courses and blockchain-based certificates. The study assesses the system's impact on reducing academic dishonesty, enhancing exam credibility, and addressing ethical concerns related to privacy and student stress levels. This research contributes to digital education security discourse by evaluating the effectiveness of multi-layered proctoring tools in preventing academic misconduct.

2. Literature Review

Maintaining academic integrity in online assessments presents significant challenges for educational institutions. Early remote proctoring systems primarily utilized basic measures such as browser lockdowns and time-restricted access to deter cheating (Tiong and Lee, 2021). However, as students developed methods to bypass these controls, the need for more advanced technologies became evident. Bilen and Matros (2021) observed that during the COVID-19 pandemic, students adapted quickly to circumvent basic proctoring mechanisms, which highlighted the urgency of implementing sophisticated monitoring technologies. The increasing sophistication of cheating tactics has driven educational institutions to explore newer and more effective methods for ensuring academic honesty. Simple methods of preventing cheating, such as limiting access to external resources or enforcing strict time constraints, were often insufficient against the evolving strategies used by tech-savvy students. This necessitated the integration of more advanced, multi-layered technologies to uphold the credibility of assessments.

The debate between traditional human invigilation and automated proctoring remains central to ensuring exam integrity. As shown in Table 1, these two approaches differ significantly in their monitoring methods, contextual judgment, cost, scalability, ethical considerations, and detection accuracy.

Table 1: Comparison of Traditional Human Invigilation and Automated Proctoring

Feature	Human Invigilation	Automated Proctoring
Monitoring Method	In-person supervision by proctors	Software-based remote monitoring
Contextual Judgment	High; proctors can interpret nuanced behaviors	Limited; relies on predefined algorithms
Cost	High; requires personnel and physical space	Lower; reduces need for physical resources
Scalability	Limited; constrained by available proctors and venues	High; can accommodate large numbers of examinees remotely
Ethical Concerns	Lower; direct human oversight	Higher; concerns about data privacy and algorithmic bias
Detection Accuracy	Subjective; depends on proctor vigilance	Objective; depends on algorithm effectiveness

Human invigilation has historically been the most effective method of ensuring academic integrity, as proctors can assess examinee behavior in real-time, intervene when necessary, and apply contextual judgment to distinguish between unintentional actions and deliberate misconduct (Muzaffar et al., 2020). However, human-supervised exams require significant logistical and financial resources, making them impractical for large-scale online education. Automated proctoring systems, on the other hand, provide scalability and cost-efficiency but lack the nuanced decision-making abilities of human invigilators. These systems rely on rule-based flagging mechanisms that may incorrectly classify harmless behaviors, such as looking away from the screen or adjusting one's seating position, as suspicious activities (Balash et al., 2021).

The advent of machine learning (ML)-based proctoring tools has significantly enhanced the credibility of online assessments by introducing advanced detection capabilities. These systems employ techniques like facial recognition and behavioral analysis to monitor students in real-time, effectively detecting identity discrepancies and suspicious activities with greater accuracy. For instance, a study by Tiong and Lee (2021) introduced an e-cheating intelligence agent that utilizes ML to detect online cheating through IP and behavioral analysis. However, while these ML-based systems mark a clear advancement over basic rule-based methods, they are not without limitations. Concerns about algorithmic biases, data privacy, and potential false positives remain, suggesting that relying solely on ML may not fully address the complex dynamics of cheating. In response, some institutions have begun to explore complementary non-ML approaches—such as biometric authentication , continuous identity verification, and rule-based anomaly detection—to develop more robust and context-sensitive proctoring solutions.

Evaluations of intelligent proctoring systems across various educational contexts highlight both their promise and their challenges. Liu et al. (2024) developed a framework named CHEESE, which applies multiple instance learning to detect and localize cheating behaviors in online exams, achieving a frame-level Area Under the Curve (AUC) score of 87.58% on the Online Exam Proctoring dataset. This method effectively identifies suspicious activities based on data patterns but lacks real-time contextual awareness. In contrast, Moyo et al. (2023) proposed a video-based detector using OpenPose, which analyzes student posture and movement to identify deviations from normal exam conduct. Liu's model offers high scalability but risks misclassifying non-malicious behaviors, whereas Moyo's system improves contextual interpretation but faces computational constraints. A hybrid approach that integrates scalable anomaly detection with movement-based behavioral analysis could enhance both accuracy and fairness. These findings underscore the need for integrative models that combine automated detection with human oversight, ensuring adaptability across diverse educational environments.

Ethical considerations are crucial in proctoring system deployment. Coghlan, Miller and Paterson (2021) highlight biases in AI-based moderation, particularly in facial recognition, which may disproportionately affect underrepresented demographics, leading to false positives and undue stress. To ensure fairness, ongoing research focuses on refining algorithms for greater inclusivity and equity, preventing unintended disadvantages while upholding academic integrity.

Global studies further emphasize the diversity of challenges in implementing online proctoring systems. Raman et al. (2021), for instance, applied the diffusion of innovation theory to examine the adoption of Online Proctored Examinations (OPE) during the COVID-19 pandemic, revealing that factors such as relative advantage, compatibility, and ease of use positively influenced student acceptance. Using Aspect Level Sentiment Analysis, the researchers found that 55% of students held a positive attitude towards OPE, viewing it as advantageous and easy to use despite some challenges. This work adds an important perspective on the integration of proctoring technologies in higher education, especially during disruptive global events like the pandemic.

While existing literature demonstrates that both ML-based and automated proctoring systems can enhance exam integrity, significant gaps remain in integrating diverse monitoring methods, addressing ethical concerns such as bias in facial recognition and privacy issues, and adapting to varied regional contexts. Facial recognition struggles with demographic fairness (Coghlan, Miller and Paterson, 2021), rule-based anomaly detection often misclassifies normal behavior as suspicious (Balash et al., 2021), and many proctoring systems lack adaptability to different regulatory and technological environments (Raman et al., 2021). To address these issues, our study introduces a hybrid intelligent proctoring system on BlockchainStudy.kz that combines facial recognition, behavioral monitoring, biometric authentication, continuous identity verification, and rule-based anomaly detection—reinforced by human oversight. This multi-layered approach improves detection accuracy, enhances scalability by reducing reliance on manual supervision, and ensures fairness through bias-aware verification and strict privacy safeguards. Moreover, this study relies solely on anonymized, computer-generated data—without collecting personal user information—thus eliminating the need for additional ethical approvals.

In conclusion, leveraging advanced technologies like ML is crucial for upholding academic integrity in online assessments. Nonetheless, persistent challenges—including privacy concerns, algorithmic biases, and regional variability—underscore the need for a more balanced approach. Future research should prioritize the development of hybrid proctoring models that integrate diverse technological methods with robust ethical safeguards. Furthermore, collaboration among technologists, educators, and policymakers is critical to establishing comprehensive standards and best practices, ensuring that proctoring systems not only deter academic dishonesty but also promote fairness and trust across varied educational contexts.

3. Materials and Methods

3.1 System Design and Architecture

The advanced proctoring system incorporates multiple technologies to maintain exam integrity. Its architecture combines facial recognition, user activity logging, and behavioral monitoring to detect cheating or suspicious behavior. The system's core feature is identity verification, achieved through facial recognition, which compares a pre-uploaded profile photo with a live video stream captured during the exam. To balance accuracy and privacy, the system uses the Luxand Face Recognition API. Alternative solutions, such as OpenCV-based models or AWS Rekognition, were considered, but Luxand was selected due to its high accuracy, ease of integration, and compliance with GDPR regulations. Unlike OpenCV, which requires extensive training datasets and computational power, Luxand provides a pre-trained model that reduces the dependency on local biometric data storage, thereby lowering security risks .

To prevent cheating through tab switching or external browsing, the system enforces full-screen mode. JavaScript event listeners and the HTML5 Page Visibility API monitor for attempts to switch tabs or minimize the browser, flagging such actions for review. Mouse movements, keyboard inputs, and screen interactions are continuously captured and sent to the server via WebSocket for real-time processing.

For secure data handling, the system uses PostgreSQL as the database, chosen for its ACID compliance, advanced indexing capabilities, and encryption features. Alternatives such as MySQL and MongoDB were evaluated, but PostgreSQL’s ability to handle high-volume, real-time event logs with strict integrity constraints made it the optimal choice. The database securely stores exam logs, including timestamps for every user action, such as key presses, mouse clicks, and screen state changes. These logs are indexed for quick retrieval and analyzed to detect anomalous behavior indicative of cheating.

Figure 1 illustrates the multi-modal architecture of the system, where client-side monitoring captures user actions and webcam data, and server-side machine learning processes verify identity and analyze behavior. The backend was built using Django, which was selected due to its built-in security mechanisms, scalability, and support for role-based access control (RBAC). While Flask and Node.js were considered, Django’s pre-configured authentication modules, secure session handling, and ORM-based database management provided a robust, secure, and efficient backend solution. The backend manages data flow between the client and the PostgreSQL database, ensuring secure storage of user data and exam logs. This integrated approach provides a robust proctoring solution that deters cheating and maintains academic integrity.

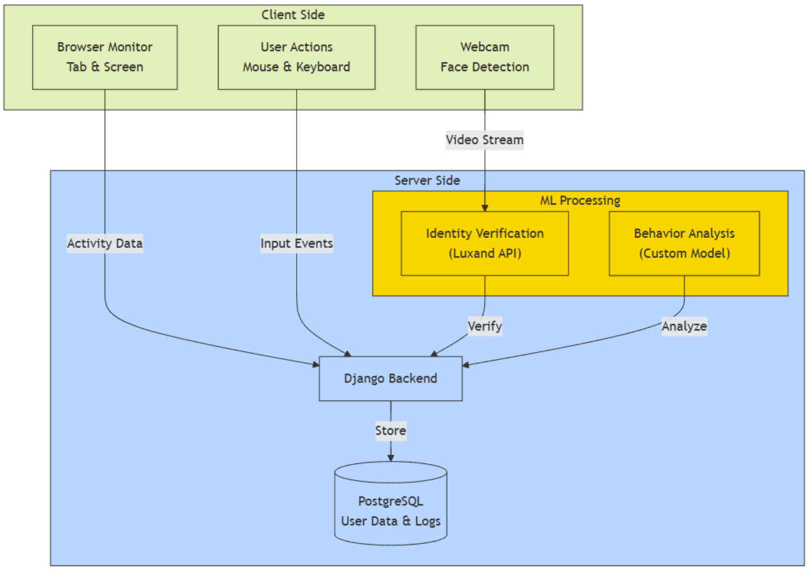


Figure 1: Machine Learning-Enhanced Academic Integrity System: Multi-Modal Architecture

It is important that the intelligent system has the ability to record user actions in real time to ensure the integrity of the exam. It records mouse movements, keyboard inputs, facial recognition data, and screen state changes, securely storing them in a PostgreSQL database with timestamps. Suspicious behaviors—such as frequent glances away, tab-switching, or unauthorized individuals in the webcam feed—are flagged for review and stored separately for detailed post-exam analysis.

To maintain security, the logged data is encrypted using Advanced Encryption Standard (AES) during both transmission and storage. Proctors can access timestamped logs and flagged events after the exam for review, allowing them to verify the legitimacy of student behavior. The system’s architecture enables efficient indexing and retrieval of logs, allowing quick identification of suspicious activities. This logging process ensures secure monitoring, analysis, and storage of relevant data while maintaining the ability to review and audit user activity. Figure 2 illustrates the data flow from real-time monitoring to secure storage and post-exam review.

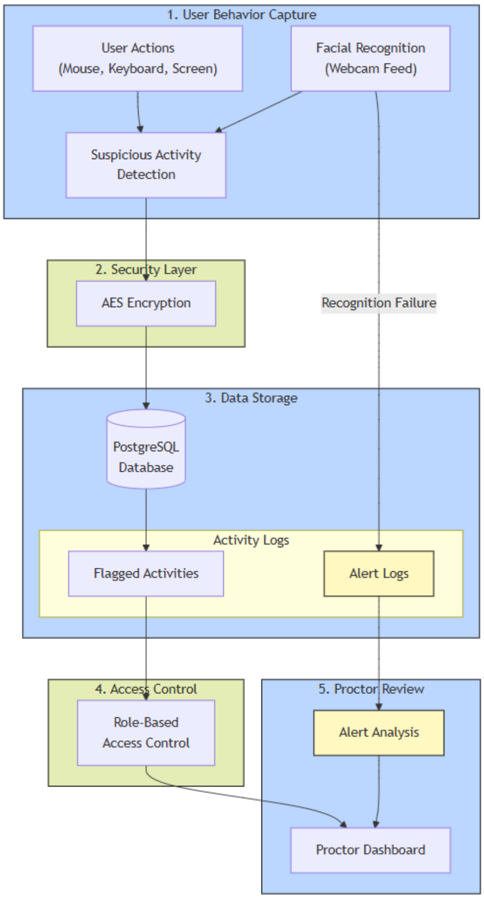


Figure 2: Data Logging and Monitoring Architecture of the Intelligent Proctoring System

3.2 Development Process and Prototyping

The development of the proctoring system followed an iterative, three-phase approach: prototyping, pilot testing, and large-scale deployment. This structured process was chosen to ensure technical feasibility, real-world applicability, and scalability, aligning with the study's goal of developing a reliable, privacy-compliant, and adaptable proctoring solution.

The prototyping phase was essential for assessing technical feasibility and refining system performance across various devices and environments. Early testing revealed challenges such as facial recognition inconsistencies due to low-resolution cameras and suboptimal lighting, leading to higher false-positive rates. To enhance accuracy, image pre-processing techniques, including histogram equalization and adaptive thresholding, were implemented, improving system robustness in diverse conditions.

The pilot testing phase evaluated the system’s effectiveness in real-world conditions with a controlled group of students on BlockchainStudy.kz. This phase focused on detecting suspicious behaviors while ensuring a seamless user experience. The insights gained allowed for adjustments, such as refining detection thresholds and reducing false positives, to enhance system stability and usability.

The large-scale deployment phase validated the system's scalability, ensuring it could maintain detection accuracy and compliance with ethical and privacy standards under high user loads. This phase demonstrated the system's adaptability to different technological infrastructures and institutional policies, confirming its practicality for widespread implementation in online education.

By structuring development in these phases, the study ensured continuous refinement, ethical integrity, and reliability, aligning with the broader objective of creating a proctoring system that is both effective in preventing academic dishonesty and respectful of user privacy.

3.3 Pilot Testing and Deployment

The system underwent extensive pilot testing to assess its effectiveness in real-world online exam conditions. The testing took place on blockchainstudy.kz, an online educational platform offering courses and certification in blockchain technology, which was developed and launched by our team. The platform already has more than 800 active users and supported a wide range of courses and exam functionalities, making it an ideal environment for launching the intelligent proctoring system.

The initial pilot phase involved 66 students who were required to take an exam while their activities were monitored by the system. The main objective of the pilot was to evaluate the system's detection accuracy, false positive rates, and system stability. The system flagged suspicious behaviors such as tab-switching, unauthorized individuals appearing in the webcam feed, or prolonged distractions from the screen. In addition to monitoring behavior, the system's performance was assessed under varying internet speeds, device specifications, and camera qualities to ensure robust functionality across different environments. System load tests were conducted to measure performance under concurrent user sessions, verifying the scalability of real-time processing.

During the pilot phase, several important insights into the system's capabilities were gained. The proctoring system was successful in detecting irregular behaviors, such as students looking away from the screen for extended periods or the presence of additional individuals in the webcam feed. However, initial testing revealed a high rate of false positives, particularly for natural head movements and brief distractions. To mitigate this, anomaly detection techniques were implemented to refine classification models, significantly reducing incorrect flags.

After fine-tuning the detection parameters, the system was scaled up for broader use on the platform. A total of 770 students participated in the system's deployment across various courses on blockchainstudy.kz. These students accessed the exams using a range of operating systems, which tested the system's ability to handle a larger volume of concurrent users. The system demonstrated its capacity to maintain stable performance and efficiently monitor student activities in real time, with accurate tracking of behaviors and generation of event logs for post-exam analysis.

The successful scaling of the system within a single platform not only validated the system's robustness in handling large numbers of users but also confirmed its effectiveness in detecting and recording suspicious behavior. The feedback from this phase provided valuable insights for further refining the system before its potential expansion to other educational platforms or institutions.

3.4 Data Collection and Security

The advanced proctoring system implements robust security measures to comply with data protection regulations, including GDPR. Sensitive data such as student identification, exam logs, and facial recognition data are encrypted using AES both during transmission and at rest. Secure communication protocols, like HTTPS (Hypertext Transfer Protocol Secure), are used to protect data during exams. Role-based access control (RBAC) restricts access to sensitive data based on user roles, ensuring that only authorized personnel can view it. Regular security audits are conducted to identify vulnerabilities and address them promptly.

Data collected during exams includes user activity logs, facial recognition data, and tab-switch events. This data is securely stored in an encrypted PostgreSQL database, with only suspicious actions (e.g., prolonged looking away or unauthorized tab-switching) being stored, reducing the exposure of personal information. Proctors review only flagged activities, and anonymization techniques are used to protect personally identifiable information during post-exam analysis.

3.5 Ethical Considerations

Ethical considerations were a fundamental aspect of the proctoring system's design, particularly regarding the use of facial recognition and behavioral monitoring. The system was developed in strict compliance with General Data Protection Regulation (GDPR) and other relevant data protection policies, ensuring that user privacy was preserved at all stages.

To participate in online exams, students voluntarily agreed to the platform's proctoring policies, which outlined the use of facial recognition for identity verification, user activity monitoring, and browser behavior tracking. No additional data collection procedures were introduced beyond what was necessary for maintaining academic integrity. All recorded data remained within the BlockchainStudy.kz platform's existing framework and was never used for experimental interventions, external research, or shared with third parties.

To safeguard personal information, no personally identifiable data were included in the research analysis. The study relied exclusively on fully anonymized and aggregated data, ensuring that individual students could not be identified at any stage. Only system-generated logs of user activity were analyzed, focusing on general statistical patterns such as flagged exam violations and system performance metrics.

Strict data retention policies were implemented, with all proctoring logs stored only for as long as necessary to verify exam integrity. Any flagged events were reviewed solely within the system's operational framework, and all data were automatically deleted after the designated retention period.

Because this study did not involve direct human subject research, external interventions, or the collection of identifiable user data, no formal ethics approval was required. The study adhered to best practices in ethical educational research, prioritizing student privacy, data security, and transparency in all aspects of system design and implementation.

4. Results

4.1 Pilot Study Results

*Phase 1: Pilot Study***.** The initial phase of testing involved a small group of 66 students, each from diverse backgrounds, to assess the system's functionality and gather feedback on its user experience. This pilot phase highlighted several performance challenges, particularly with the custom facial recognition model. Due to the model's high computational load, the system struggled with identity verification, causing delays and an extended setup time. These inefficiencies were particularly evident on lower-powered devices, leading to performance degradation.

To address these challenges, the development team integrated the Luxand Face Recognition API, which processed identity verification based on the user's uploaded profile photo. This switch significantly reduced the computational burden and resulted in a more stable and faster setup time. As a result, the system saw a reduction in technical issues and false positives, thereby improving user experience and enhancing the system's reliability.

Figure 3 illustrates the comparative analysis of system performance metrics before and after the implementation of the Luxand API. Key improvements included a 35% reduction in computational requirements, which allowed the system to operate more smoothly and on a wider range of devices.

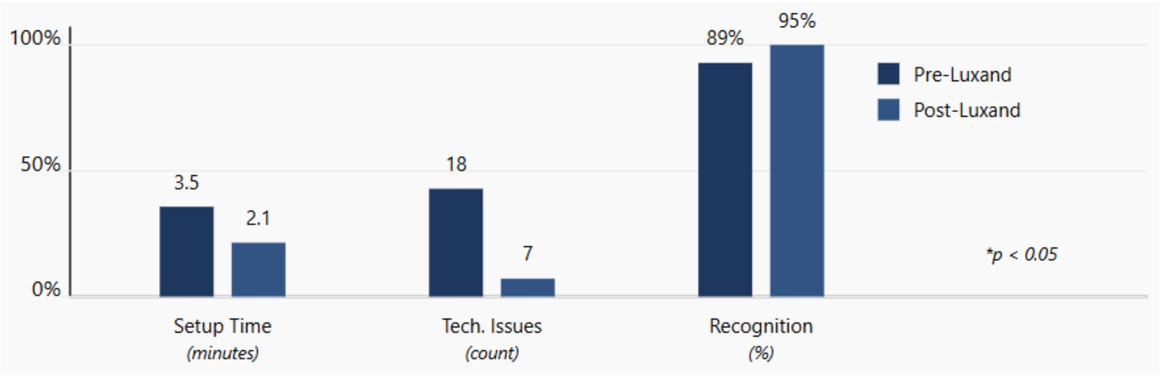
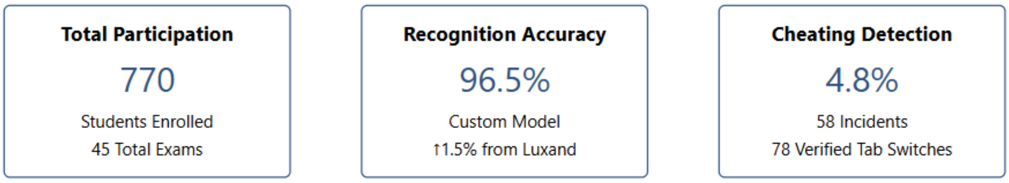


Figure 3: Comparative Analysis of System Performance Metrics

Despite these improvements, some areas for further optimization were identified. For instance, while Luxand's API helped streamline the recognition process, certain suspicious behaviors - such as repeated glancing away from the screen - were not fully captured by the existing model. This limitation prompted further adjustments and the introduction of a more sophisticated monitoring system for the next phase.

Phase 2: Educational Platform Rollout. Building on the success of the pilot study, the intelligent proctoring system was deployed on an online educational platform offering certification courses. This phase involved 770 students who voluntarily participated in the testing process. All participants received detailed instructions before the testing began and provided consent for participation. The primary objective of this phase was to assess the system's scalability and effectiveness in a larger, more diverse setting (Figure 4).



Total Participation

770

Students Enrolled

45 Total Exams

Recognition Accuracy

96.5%

Custom Model

↑1.5% from Luxand

Cheating Detection

4.8%

58 Incidents

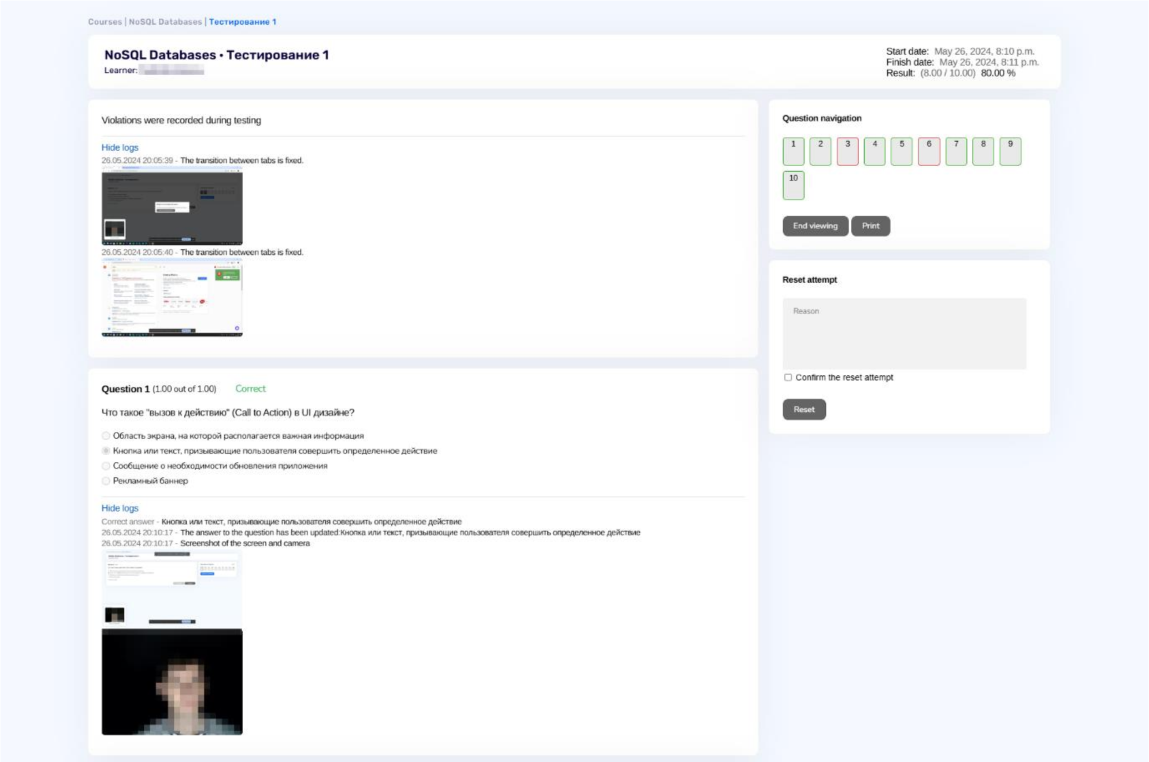
78 Verified Tab Switches

Figure 4: Metrics of the Success of Implementation in Educational Institutions

During this phase, while the Luxand API had improved efficiency, the existing model still struggled to detect certain suspicious behaviors, such as frequent glancing away or unauthorized interactions. To address this, the team developed a custom in-house model for enhanced behavioral monitoring. Deployed on a dedicated server, it enabled simultaneous processing of facial recognition and behavior analysis, ensuring stable performance even under high demand. This setup improved detection of cheating indicators, like tab switching or multiple individuals in the frame, without compromising system efficiency.

This phase also involved extensive collaboration with educators and technical teams to refine the system's ability to identify common cheating patterns and suspicious behaviors specific to online exams. As a result, the system's monitoring features were enhanced to detect additional indicators of suspicious activity, such as the presence of multiple people in the camera frame or inconsistencies in user behavior. The upgraded system could now provide a more detailed log of user actions, such as tab-switching or changes in screen focus, enabling instructors to conduct more thorough analyses of potential academic dishonesty.

To enhance security and ensure transparency, the system captures and stores webcam images and screen screenshots when suspicious activities or tab-switching occur. These logs serve as verifiable evidence, fostering trust between students and educators. Figures 5 and 6 illustrate the student and proctor interfaces, highlighting live monitoring, violation logging, and timestamped records of suspicious actions. Figure 5 shows the facial recognition and violation logging interface, while Figure 6 presents the post-test review screen for instructors to verify flagged events.



Courses | NoSQL Databases | Тестирование 1

NoSQL Databases • Тестирование 1

Learner: [redacted]

Start date: May 26, 2024, 8:10 p.m.
Finish date: May 26, 2024, 8:11 p.m.
Result: (8.00 / 10.00) 80.00 %

Violations were recorded during testing

Hide logs

26.05.2024 20:05:39 - The transition between tabs is fixed.

26.05.2024 20:05:40 - The transition between tabs is fixed.

Question 1 (1.00 out of 1.00) Correct

Что такое "вызов к действию" (Call to Action) в UI дизайне?

○ Область экрана, на которой располагается важная информация
● Кнопка или текст, призывающие пользователя совершить определенное действие
○ Сообщение о необходимости обновления приложения
○ Рекламный баннер

Hide logs

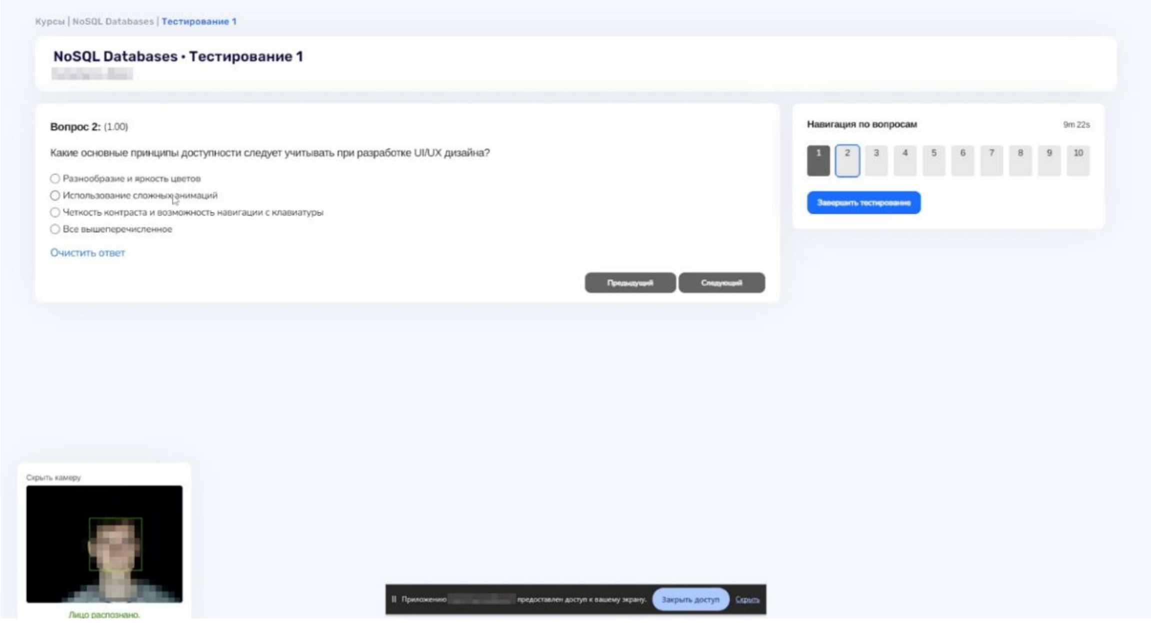
Correct answer - Кнопка или текст, призывающие пользователя совершить определенное действие
26.05.2024 20:10:17 - The answer to the question has been updated:Кнопка или текст, призывающие пользователя совершить определенное действие
26.05.2024 20:10:17 - Screenshot of the screen and camera

Reset attempt

Reason

□ Confirm the reset attempt

Figure 5: The Interface for Reviewing the Student's Results with Detailed Logs



Курсы | NoSQL Databases | Тестирование 1

NoSQL Databases • Тестирование 1

[redacted]

Вопрос 2: (1.00)

Какие основные принципы доступности следует учитывать при разработке UI/UX дизайна?

○ Разнообразие и яркость цветов
○ Использование сложных анимаций
○ Четкость контраста и возможность навигации с клавиатуры
○ Все вышеперечисленное

Навигация по вопросам 9m 22s

Лицо распознано.

Приложению [redacted] предоставлен доступ к вашему экрану.

Figure 6: The Student's Interface During Testing with a Working Proctoring System

Phase 3: Comparative Study. Finally, a comparative study was conducted to assess the impact of the new in-house model on proctored versus non-proctored environments. This phase involved 770 students, split into two groups of 385 students each, allowing for a direct comparison between the effectiveness of the proctoring system in both settings. The custom model enabled deeper behavioral analysis, including the detection of suspicious actions, adding an additional layer of security to the proctoring system.

The primary goal of the comparative study was to evaluate not only the effectiveness of the system in reducing cheating but also its broader impact on academic integrity and student behavior. Weiner and Hurtz (2017) found that online proctoring can offer security and fairness levels comparable to traditional in-person exams, but emphasized the need for careful implementation to address student concerns and ensure consistent performance outcomes. By including a non-proctored control group, the study allowed for clear insights into the differences between the two environments. The results indicated that the proctored group experienced a significantly lower rate of cheating and a slightly lower average exam score. Specifically, the cheating rate in the proctored group was 4.5%, compared to 15.7% in the non-proctored group. While the proctored group had a slightly lower average exam score (78.4%) compared to the non-proctored group (81.2%), this suggested that the system effectively deterred dishonest behavior, leading to a more genuine assessment of student knowledge (Figure 7).

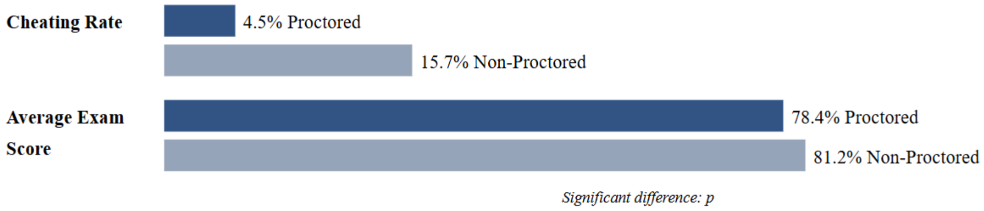


Figure 7: Proctored vs. Non-Proctored Performance Analysis

The custom model's ability to provide detailed logs of student behavior proved invaluable in identifying common cheating strategies and continuously refining the system's detection capabilities. The system successfully detected instances where students attempted to communicate with others during the exam or use secondary devices, providing key insights into cheating behaviors. This data helped improve the model's ability to distinguish between legitimate behaviors and potential cheating attempts, making the system more robust in future applications. Moreover, the use of behavioral analysis allowed educators to gain a deeper understanding of student engagement during exams. By identifying suspicious behaviors, educators were better equipped to provide guidance on proper exam conduct and foster a culture of academic honesty. Thus, the system not only acted as a deterrent against cheating but also served as an educational tool to promote academic integrity.

The analysis of the system's performance further revealed the importance of continuous improvement. The system's ability to detect cheating was significantly enhanced by the custom model, reducing the incidence of cheating from 58 incidents (4.8% of exams monitored) in Phase 2 to 36 incidents (4.5% of exams) in Phase 3. The system also showed improved detection rates for behaviors such as tab-switching, multiple faces in the camera frame, and suspicious movement, demonstrating the value of ongoing refinement and optimization.

Additionally, the system's development process involved substantial iteration, with significant improvements in facial recognition accuracy, cheating incident detection, and overall system performance (Table 2). The phase also highlighted the importance of transparency and clear communication with students regarding the proctoring process. By ensuring students understood how their data would be used and how the proctoring system functioned, the development team successfully addressed privacy concerns and fostered trust. This approach helped in gaining student cooperation, ensuring the proctoring system was viewed not as intrusive surveillance but as a necessary tool for maintaining academic standards.

Table 2: Performance Metrics of Intelligent Proctoring System Across Testing Phases

Metric/Feature	Pre-Luxand Phase 1	Post-Luxand Phase 1	Phase 2 (Luxand + Custom Model)	Phase 3 (Enhanced Custom Model)
Average Setup Time (minutes)	3.5	2.1	2.1	1.9
Facial Recognition Accuracy (%)	89	95	96.5	97
Number of Technical Issues	18	7	5	3
Detected Cheating Incidents	N/A	N/A	58 (4.8% of exams monitored)	Reduced to 36 (4.5% of exams)
Tab-Switch Detection Events	N/A	150 flagged, 40 valid	340 flagged, 78 confirmed	420 flagged, 92 confirmed
Flagged Suspicious Behaviors	N/A	30	120	200

Metric/Feature	Pre-Luxand Phase 1	Post-Luxand Phase 1	Phase 2 (Luxand + Custom Model)	Phase 3 (Enhanced Custom Model)
Devices Compatible	PCs only	PCs, modern laptops	PCs, laptops, low-power devices	PCs, laptops, low-power devices
Privacy Compliance (Encryption)	Basic encryption	AES Encryption	AES + GDPR Compliance	Advanced controls with consent
Exam Coverage (students)	66	66	770	770
Cheating Rate in Non-Proctored Exams (%)	15.7	15.7	15.7	15.7
Cheating Rate in Proctored Exams (%)	Not Monitored	4.8	4.8	4.5
Data Storage Logs (GB/exam)	0.2	0.5	0.8	1.2
Multiple Face Detection Support	No	Limited	Supported	Enhanced Real-time Detection

The detailed monitoring capabilities of the proctoring system were further highlighted in the evaluation of various violation types. As shown in Table 3, different types of suspicious behavior, such as tab switching, multiple faces in view, and irregular keyboard patterns, were detected with high accuracy, and false positive rates were minimized through model optimization. These insights provided a clearer understanding of the common cheating tactics employed and allowed for ongoing improvements in the system's detection algorithms.

Table 3: Violation Type Statistics in Online Proctoring System

Violation Type	Frequency	Detection Rate	False Positive Rate
Tab Switching	320	92%	8%
Multiple Faces	65	95%	5%
Suspicious Movement	200	87%	13%
Irregular Keyboard Patterns	145	93%	7%
Full Screen Exit	340	94%	6%

4.2 Impact on Academic Integrity

To assess the impact of the intelligent proctoring system, a qualitative survey was conducted among 18 mentors and 54 platform users who had directly experienced the system. The survey aimed to assess perceptions of the fairness, effectiveness, and overall user satisfaction with the proctored exams (Table 4). While 83% of mentors felt that proctored exams were significantly more secure and contributed to academic integrity, only 52% of students expressed satisfaction with the fairness of the system. Notably, 48% of students reported feeling more stress and anxiety during the proctored exams, contrasting with only 17% of mentors who shared similar concerns. This difference in opinion reflects the challenge of balancing the need for academic integrity with the student experience. While 94% of mentors viewed proctoring as essential for maintaining exam integrity, only 37% of students agreed with this view, and 63% preferred non-proctored exams. Despite these mixed perceptions, both groups acknowledged the usefulness of the proctoring system, with mentors valuing the enhanced security it provided, and students recognizing its role in deterring dishonest behavior.

Overall, Phase 3 of the study demonstrated that the system under development, with its custom model and enhanced behavioral analysis capabilities, significantly improved the detection of cheating and contributed to a more accurate assessment of student knowledge. The findings underscore the importance of continuous improvement, transparency, and clear communication with students, ensuring that proctoring systems are both effective in maintaining academic integrity and sensitive to the concerns and experiences of students.

Table 4: Survey Results on Perceptions of Proctored Exams

Survey Question	Mentors (n = 18)	Students (n = 54)	Overall (n = 72)
Satisfaction with fairness of proctored exams	83 % (15)	52 % (28)	60 % (43)
Perceived stress/anxiety due to proctoring	17 % (3)	48 % (26)	40 % (29)

Survey Question	Mentors (n = 18)	Students (n = 54)	Overall (n = 72)
Preference for non-proctored exams	5.5 % (1)	63 % (34)	49 % (35)
Importance of proctoring for exam integrity	94 % (17)	37 % (20)	51 % (37)
Overall usefulness of proctoring for integrity	94 % (17)	50 % (27)	61 % (44)

5. Discussion

The findings indicate that the intelligent proctoring system reduces cheating and positively influences student behavior. The presence of monitoring technologies serves as a deterrent, motivating students to focus more on preparation, knowing that dishonest behavior is likely to be detected. This aligns with previous research that emphasizes the deterrent effects of such systems on academic dishonesty, such as the work of Weiner and Hurtz (2017), who found that online proctoring can promote academic integrity in a similar manner to traditional in-person proctoring methods. However, several challenges persist - particularly concerning privacy, fairness, and ethical considerations - that must be addressed for these technologies to gain widespread acceptance.

5.1 Privacy Concerns and Data Collection

One of the primary concerns with proctoring systems is the significant amount of data collection required, such as facial recognition and detailed logs of user interactions. Mutimukwe et al. (2023) highlight that online proctoring systems may compromise contextual integrity by collecting sensitive and potentially excessive personal data. Students have expressed discomfort with the level of surveillance, fearing the misuse or potential breach of their personal data. This concern is particularly relevant in systems that use invasive techniques, like facial recognition, which can make students feel that their privacy is being invaded. To address these concerns, robust safeguards are essential, including encryption, strict data access controls, and compliance with privacy regulations. Transparent communication with students about how their data is stored, used, and protected is crucial for alleviating privacy concerns and fostering trust. As the study demonstrates, privacy compliance (AES encryption and GDPR adherence) was a key feature of the proctoring system, which likely played a role in gaining user confidence. To further enhance transparency, a potential improvement could be the introduction of a notification mechanism informing students whenever data collection is initiated. Additionally, implementing automated data deletion policies post-exam verification would help address concerns regarding unnecessary data retention while maintaining academic integrity.

5.2 Ethical Implications and Bias in Proctoring Technologies

Automated proctoring systems raise ethical concerns related to fairness, privacy, and student well-being. Burgess et al. (2022) highlight issues of algorithmic bias and over-surveillance, which can undermine trust and create a stressful exam environment. In this study, while mentors valued the system's security, 48% of students reported increased anxiety, suggesting that monitoring can unintentionally heighten exam pressure. A key concern is bias in facial recognition technologies, which may struggle to accurately identify individuals from diverse demographics (Burgess et al., 2022). This can lead to higher false-positive rates, causing undue scrutiny for certain groups. While system accuracy improved (from 89% to 97%), ongoing refinements—such as expanding training datasets—are needed to enhance fairness.

Another factor contributing to anxiety is the perceived lack of control over monitoring. Some students feared routine behaviors, like adjusting posture or briefly looking away, could be misinterpreted as suspicious. Mukherjee et al. (2024) suggest that allowing users to customize aspects of monitoring, such as blurring background elements, could reduce stress and build trust. Greater transparency and control over data collection may help mitigate these concerns while maintaining exam integrity.

5.3 Refinement of Behavioral Monitoring Capabilities

Beyond facial recognition, the advanced proctoring system must continuously improve its ability to detect and analyze a wide range of suspicious behaviors, such as unauthorized collaboration or the use of secondary devices. In Phase 2 and 3 of current study, we found that the system's detection capabilities, including the ability to flag tab-switching and detect multiple faces in the camera frame, significantly enhanced its monitoring accuracy. However, further research and development are needed to refine these systems. Ngo et al. (2024) propose a multi-modal approach combining behavioral data with environmental monitoring to detect abnormal activities during online exams. Such systems are better equipped to identify more subtle forms of cheating, like unauthorized collaboration or the use of hidden devices, while minimizing the risk of flagging legitimate student behaviors as misconduct.

Mukherjee et al. (2024) also suggest that the perception of fairness in online proctoring systems can be improved by implementing greater transparency and allowing students to control aspects of their monitoring, such as visual data obfuscation. This approach could help reduce students' feelings of being overly surveilled and improve the overall experience. Allowing students to have some control over their data - such as opting to blur background details or mask parts of their face during recognition - may help reduce the anxiety associated with being watched, fostering a more positive testing experience.

5.4 Impact on Student Behavior and Performance

The proctored environment has significantly reduced cheating, with a 4.5% cheating rate in the proctored group compared to 15.7% in the non-proctored group. This suggests that monitoring acts as a deterrent, encouraging students to prepare more thoroughly rather than relying on dishonest methods. This finding aligns with Weiner and Hurtz (2017), who emphasized that online proctoring upholds academic integrity similarly to traditional in-person exams.

However, the study also found that the average exam score was slightly lower in the proctored group (78.4%) than in the non-proctored group (81.2%), indicating that surveillance may induce stress, potentially affecting cognitive performance. Similar concerns have been reported in international studies, where students in proctored settings often experience higher anxiety levels, which can impact their test-taking ability. Universities globally are adopting hybrid proctoring models that combine automated monitoring with human oversight to mitigate such issues while maintaining fairness.

Beyond preventing cheating, proctoring also influences learning habits. Knowing they will be monitored, students are more likely to engage in deeper learning strategies rather than surface-level memorization. This suggests that proctoring may contribute to long-term improvements in student preparation and academic discipline. However, achieving a balance between security and student well-being remains essential. Measures such as providing structured breaks, reducing unnecessary monitoring intrusiveness, and increasing transparency in proctoring policies can help maintain academic integrity without negatively impacting student performance.

5.5 Ethical Use and Transparency in Proctoring Systems

The ethical deployment of enhanced proctoring systems requires balancing security with student rights. Moreno-Guerrero et al. (2020) emphasize that transparency and accessibility are critical for student acceptance of e-learning tools. Effective integration of proctoring into online education depends on clear communication about system functionality, data collection, and privacy safeguards to build trust. Ensuring fairness, inclusivity, and minimal invasiveness should remain a priority.

The findings of this study provide insights that can inform global e-learning practices. While surveillance concerns persist in many educational systems (Moreno-Guerrero et al., 2020), our results indicate that transparency in data protection and giving students some control over monitoring can alleviate anxiety and improve acceptance. Similar studies, such as Mukherjee et al. (2024), suggest that customizable monitoring features, such as background blurring, enhance student trust and perceived fairness.

This study demonstrates that privacy-conscious, adaptive proctoring solutions can serve as scalable models for other educational platforms. By integrating automated monitoring with human oversight, institutions can maintain exam integrity while addressing ethical concerns. Future research should explore how such systems can be refined for diverse educational settings, ensuring accessibility and compliance with different institutional and regulatory frameworks worldwide.

6. Limitations

Despite its advancements, the intelligent proctoring system faces several challenges. Webcam dependency can lead to verification errors for students with low-quality cameras or unstable internet, potentially affecting fairness. Privacy concerns remain significant, as biometric data collection raises security and consent issues, despite robust encryption and compliance measures. Additionally, facial recognition biases, particularly for diverse demographics, necessitate ongoing improvements in dataset diversity and alternative verification methods like voice recognition. Lastly, the system's complexity and resource demands may pose adoption barriers for smaller institutions or those in developing regions, highlighting the need for a more lightweight and cost-effective version.

7. Conclusions and Future Work

The integration of advanced proctoring technologies has demonstrated significant potential in enhancing academic integrity within online learning environments. This study confirms that automated monitoring can effectively reduce cheating incidents, contributing to fairer and more credible assessments. However, ongoing challenges remain, particularly concerning privacy, inclusivity, and student well-being. Future improvements should focus on refining detection algorithms to minimize biases, enhancing system adaptability across different educational settings, and exploring alternative verification methods, such as voice recognition and multi-factor authentication. These refinements will ensure that proctoring remains both effective and ethically responsible.

Beyond preventing academic dishonesty, proctoring systems can be leveraged to improve learning behaviors. The inclusion of behavioral analytics—such as eye-tracking, gesture recognition, and posture analysis—could provide educators with insights into student engagement, cognitive load, and stress levels. This data could help refine assessment strategies to better support students during high-stakes exams. Additionally, ensuring compliance with evolving privacy regulations (e.g., GDPR) and introducing student-controlled monitoring options will be key to fostering trust and transparency.

For broader accessibility, future research should focus on developing lightweight, low-bandwidth-compatible versions of the system to support students in regions with limited technological infrastructure. Additionally, long-term studies should assess the impact of enhanced proctoring on academic performance, student perceptions, and test-taking behaviors to further optimize the system.

To maximize its global applicability, interdisciplinary collaboration between educators, technologists, and policymakers will be essential. By integrating ethical safeguards, promoting inclusivity, and addressing student concerns, smart proctoring systems can evolve into scalable, fair, and privacy-conscious solutions that uphold academic integrity while maintaining student trust in online education.

Funding: This research was funded by the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan (Grant No. AP19177277).

Ethics Statement: This study was conducted using the BlockchainStudy.kz platform, where students voluntarily participated in online courses and assessments. The intelligent proctoring system recorded data related to facial recognition, user activity monitoring, and browser behavior tracking solely for the purpose of ensuring academic integrity. All recorded data remained within the platform's existing operational framework and were never used for experimental interventions, external research, or third-party sharing. No personally identifiable information was included in the research analysis. All data used for this study were fully anonymized and aggregated before any evaluation was conducted, ensuring that individual students could not be identified at any stage. The research relied exclusively on statistical summaries of system performance and general behavioral patterns, with no direct association to specific users. No new data collection procedures were introduced for research purposes. The proctoring system operated under standard platform policies, which all users agreed to before taking their exams. All participants provided consent for data processing as part of the BlockchainStudy.kz platform's user agreement, ensuring that data usage aligned with the policies users were informed of in advance. Because this study did not involve direct human subject research, external interventions, or personally identifiable data analysis, no formal ethics approval was required. The study fully complied with General Data Protection Regulation (GDPR) principles, ensuring that all data were handled securely, access was strictly controlled, and retention policies were followed. All proctoring logs were stored only as necessary for integrity verification and were automatically deleted after the designated retention period. This study adheres to best practices in ethical educational research and privacy protection. Since only system-generated, anonymized data were used in a retrospective analysis, and no personal data were collected outside the platform’s normal operational scope, it does not fall under research requiring formal institutional ethics approval.

AI Statement: This research paper was written without the assistance of artificial intelligence (AI) tools. All content, including the conceptual framework, data analysis, writing, and editing, was developed entirely by the authors. No AI-generated text, automated editing, or machine-assisted research synthesis was used in the preparation of this paper. The findings, arguments, and conclusions presented in this study are the result of human-led research and critical analysis, ensuring academic integrity and adherence to ethical research standards.

References

Balash, D., Kim, D., Shaibekova, D., Fainchtein, R., Sherr, M. and Aviv, A., 2021. Examining the examiners: Students' privacy and security perceptions of online proctoring services. *arXiv preprint*. https://doi.org/10.48550/arXiv.2106.05917

Bilen, E. and Matros, A., 2021. Online Cheating Amid COVID-19. *Journal of Economic Behavior & Organization*, 182, pp. 196-211. https://doi.org/10.1016/j.jebo.2020.12.004

Brandeis University, 2020. Academic dishonesty and COVID-19: A biological explanation. *Write Now*. Available at: https://www.brandeis.edu/writing-program/write-now/2020-2021/arie-rotem/index.html [Accessed 16 February 2025].

Bretag, T., Mahmud, S., Wallace, M., Walker, R., James, C., Green, M. and East, J., 2018. Contract cheating: A survey of Australian university students. *Studies in Higher Education*, 43(11), 1921-1939. https://doi.org/10.1080/03075079.2018.1462788

Bretag, T., Harper, R., Burton, M., Ellis, C., Newton, P., van Haeringen, K., Saddiqui, S. and Rozenberg, P., 2019. Contract cheating and assessment design: Exploring the connection. *Assessment & Evaluation in Higher Education*, 44(5), 676-691. https://doi.org/10.1080/02602938.2018.1527892

Burgess, B., Ginsberg, A., Felten, E. W. and Cohney, S., 2022. Watching the watchers: Bias and vulnerability in remote proctoring software. *arXiv preprint*. Available at: https://doi.org/10.48550/arXiv.2205.03009 [Accessed 15 November 2024].

Coghlan, S., Miller, T., and Paterson, J., 2021. Good Proctor or "Big Brother"? Ethics of Online Exam Supervision Technologies. *Philosophy & Technology*, 34, pp. 1581–1606. https://doi.org/10.1007/s13347-021-00476-1

Dawson, P., 2021. Defending Assessment Security in a Digital World: Preventing E-Cheating and Supporting Academic Integrity in Higher Education. *Routledge*. https://doi.org/10.4324/9780429324178

Eaton, S., 2020. Academic Integrity During COVID-19: Reflections from the University of Calgary. *International Studies in Educational Administration*, 48(1), pp. 80-85. https://dx.doi.org/10.11575/PRISM/38013

Gamage, K., Dehideniya, S., Zhiheng, X. and Tang, X., 2023. Contract cheating in higher education: Impacts on academic standards and quality. *Journal of Applied Learning & Teaching.* 6(2). https://doi.org/10.37074/jalt.2023.6.2.24

Nigam, A., Pasricha, R., Singh, T. and Churi, P., 2021. A systematic review on AI-based proctoring systems: Past, present and future. *Education and Information Technologies*, 26(5), pp.6421–6445. https://doi.org/10.1007/s10639-021-10597-x

Lancaster, T. and Cotarlan, C., 2021. Contract cheating by STEM students through a file sharing website: A Covid-19 pandemic perspective. *International Journal for Educational Integrity*, 17(1), 1-16. https://doi.org/10.1007/s40979-021-00070-0

Liu, Y., Ren, J., Xu, J., Bai, X., Kaur, R. and Xia, F., 2024. Multiple Instance Learning for Cheating Detection and Localization in Online Examinations. *arXiv preprint*. Available at: https://arxiv.org/abs/2402.06107 [Accessed 15 November 2024].

Malik, A.A., Hassan, M., Rizwan, M., Mushtaque, I., Lak, T.A. and Hussain, M., 2023. Impact of academic cheating and perceived online learning effectiveness on academic performance during the COVID-19 pandemic among Pakistani students. *Frontiers in Psychology*, 14, p.1124095. https://doi.org/10.3389/fpsyg.2023.1124095

Moreno-Guerrero, A. J., Aznar-Díaz, I., Cáceres-Reche, M. P. and Alonso-García, S., 2020. E-Learning in the Teaching of Mathematics: An Educational Experience in Adult High School. *Mathematics*, 8(5), 840. https://doi.org/10.3390/math8050840

Moyo, R., Ndebvu, S., Zimba, M. and Mbelwa, J., 2023. A Video-based Detector for Suspicious Activity in Examination with OpenPose. *arXiv preprint*. Available at: https://arxiv.org/abs/2307.11413 [Accessed 15 November 2024].

Mukherjee, S., Distler, V., Lenzini, G. and Cardoso-Leite, P., 2024. Balancing the perception of cheating detection, privacy and fairness: A mixed-methods study of visual data obfuscation in remote proctoring. *arXiv preprint*. Available at: https://arxiv.org/abs/2406.15074 [Accessed 15 November 2024].

Mutimukwe, C., Han, S., Viberg, O. and Cerratto-Pargman, T., 2023. Privacy as Contextual Integrity in Online Proctoring Systems in Higher Education: A Scoping Review. *arXiv preprint*. Available at: https://doi.org/10.48550/arXiv.2310.18792

Muzaffar, A.W., Tahir, M., Anwar, M.W., Chaudry, Q., Mir, S.R. and Rasheed, Y., 2021. A systematic review of online exams solutions in e-learning: Techniques, tools and global adoption. *arXiv preprint*. Available at: https://arxiv.org/abs/2010.07086 [Accessed 16 February 2025].

Newton, P.M. and Essex, K., 2024. How common is cheating in online exams and did it increase during the COVID-19 pandemic? A systematic review. *Journal of Academic Ethics*, 22, pp. 323-343. https://doi.org/10.1007/s10805-023-09485-5

Ngo, D. A., Nguyen, T. D., Dang, T. L. C., Le, H. H., Ho, T. B., Nguyen, V. T. K. and Nguyen, T. T. H., 2024. Examining monitoring system: Detecting abnormal behavior in online examinations. *arXiv preprint*. Available at: https://arxiv.org/abs/2402.12179 [Accessed 15 November 2024].

Raman, R., Bandlamudi, S., Gangadharan, V., Vachharajani, H. and Nedungadi, P., 2021. Adoption of online proctored examinations by university students during COVID-19: Innovation diffusion study. *Education and Information Technologies*, 26, pp.7339–7358. https://doi.org/10.1007/s10639-021-10581-5

Tiong, L. C. O. and Lee, H. J., 2021. E-cheating Prevention Measures: Detection of Cheating at Online Examinations Using Deep Learning Approach - A Case Study. *arXiv preprint*. Available at: https://arxiv.org/abs/2101.09841 [Accessed 15 November 2024].