Multidisciplinary Journal of Research in Engineering and Technology

ISSN: 2348-6953

Volume 13 Issue 2s (2026) | Pages: 144-152

Privacy-Preserving On-Screen Activity Tracking and Classification in E-Learning using AI

Dewanand Meshram[1], Harish Mengade[2], Satyam Kale[3], Sanika Ahire[4], Swaraj Aghav[5]

[1,2,3,4,5]Department of Information Technology, RMD Sinhgad School of Engineering, Pune, Maharashtra, India

Peer Review Information

***Type**: Article*
***Received**: 27 March 2026*
***Revised**: 12 April 2026*
***Accepted**: 26 May 2026*
***Published**: 16 June 2026*

Abstract

The blistering development of online education has changed considerably the manner in which education, learning as well as scholarly analysis is given in academic institutions, instructional centers, and in professional education. Internet technologies have provided the flexibility in accessing learning materials regardless of geographical limits and thus learning institutions have been able to touch the greater and more varied populations of learners. Nevertheless, the task of making online assessment secure and trustworthy is a pressing challenge despite the fact that the process of content delivery has been developed at a remarkable pace. Invigilators monitor student behaviour directly in physical examination halls, confirm identity, limit unauthorised materials and compliance with examination regulations. It is much more challenging to provide the identical level of control within remote settings.

Somewhat towards this end, various scientists and organizations have been undertaking the study of learning intelligent proctoring systems which monitor student behaviour automatically in online exams. These are the systems that usually use the help of such tools as webcams, microphones, screen-capture functions, and behavioural analytics to detect suspicious behaviour like impersonation, collaborating with third parties, unusual gazes movement, multiple-people presence, using a hidden mobile phone, and constantly switching applications. Recent developments in artificial intelligence, particularly computer vision and machine learning, have enhanced the ability of such systems to scan facial expressions, head pose, attention patterns and environmental cues in real time.

Although these have some advantages, issues about privacy, lack of fairness and bias in algorithmic choices, over-surveillance and false charges have hindered universal adoption. Thus, the new generation of online monitoring tools needs to strike a balance between integrity in examinations and responsible data management. In this review, a detailed discussion will be made on privacy preserving activities tracked on-screen in e-learning assessment. It examines significant technologies, the current constraints, architectural design imperatives, ethical issues, and future research potential. An approach is also outlined that uses a privacy-conscious framework, where sensitive processing of data is carried out locally, but significant risk indicators and little encrypted evidence are sent to reviewers. These solutions are able to enhance trust, scalability and regulatory compliance of digital education e-mails.

Keywords: Intelligent Online Proctoring; Privacy-Preserving Assessment; Artificial Intelligence; Computer Vision; E-Learning Security; Behavioral Analytics.

How to Cite This Article

Meshram, D., Mengade, H., Kale, S., Ahire, S., & Aghav, S. (2026). Privacy-preserving on-screen activity tracking and classification in e-learning using AI. *Multidisciplinary Journal of Research in Engineering and Technology*, 13(2s), 144–152.

Introduction

The world education industry has made a significant shift towards digital transformation in the last decade. LMS, online classroom engines, mobile learning tools, and web-based teamwork platforms have taken the center stage in contemporary pedagogical endeavors. This change increased even more across periods of public health crises and widespread disruption, as institutions had to transition academic activities online. When conveying lectures, assignments, and learning content was accelerated, the assessment of student performance became one of the most problematic unsolved challenges.

Evaluation is important to assess the level to which learning goals have been attained. The results of examinations will affect further educational achievement, admission into a scholarship, selection to receive a job, and professional licensure. Thus, integrity of assessment is key to the credibility of any educational system. The traditional classroom ensures fairness by keeping environments controlled, identifying individuals and physically overseeing them. Though, in case of remote assessments, there might be attempts to take advantage of the lack of physical control in the students with unfair methods.

Some of the most frequent types of academic misbehaviour in online tests will be unauthorized note checking, opening hidden reasonable windows, communicating with fellow students by messaging, off camera help, use of secondary devices, or letting someone impersonate a student to take the test. Although the misconduct may be committed by few individuals in these situations, it will still cause a lack of confidence with the whole evaluation system. This puts the honest learners at a disadvantage and the institution may suffer reputational losses in case the authenticity of the assessments is put under question.

Automated proctoring systems have gotten the attention to overcome these risks. Such systems aim at simulating invigilation with sensors and smart algorithms. Webcam can check the attendance of the right student. Looking: It is possible to determine whether the candidate keeps looking away at the screen through gaze analysis. Conversations or other weird sounds can be detected through the use of a microphone input. Monitors placed on the desktops are able to detect suspect application switches or even blocked browsing undertakings. The system will create alerts to be reviewed by taking a combination of these signals.

Nevertheless, acceptance and fairness cannot be assured solely through technological monitoring. Concerns have been raised amongst many students and teachers that constant capturing of faces, voices, individual rooms, and desktop usage can be too invasive. Moreover, errors of algorithms can falsely indicate innocent behaviour, like normal eye movement, temporary problems with the net, or noise. Otherwise, these systems may cause stress and lack of trust, unless designed properly.

In these regards, the new direction of research has been identified: privacy-conscious intelligent proctoring. Rather than sending all raw data to central servers, current methods seek to process sensitive data where a student is, and retain only necessary risk indicators and have a human reviewer make a final decision. The review looks at latest advances in that space and how safe, scalable and ethically sound assessment systems can be engineered in future e-learning ecologies.

Literature Survey

Various related fields such as identity verification, behavioural analytics, multimedia fusion, anomaly detection and privacy-preserving systems structure define the literature grounded on online examination monitoring. Current contributions show considerable improvement, still portraying some unresolved technical and ethical difficulties.

Vision-Based Monitoring Systems

A big category of research involves applying computer vision to monitor student behaviour in the form of webcam feeds. The verification of the existence of a candidate during examination is usually done using face detection models. After the face has been recognized, further algorithms can determine the head orientation, facial features, and gaze direction. Making repeated turn left and right turns, being out of the frame for a long period, or constantly looking away during the frame or out of the frame may be a sign of suspicious activity, e.g. use of external material or communication with someone else.

This has been demonstrated in a number of papers that indicate that temporal analysis enhances stability in detection. Sequential models examine the movement patterns over time, rather than single, separated frames. This minimizes false alarms occasioned by short natural movements like blinking, stretching or adjusting seating position.

Identity Assurance and anti-impersonation.

One significant problem with distant testing is identity fraud. Researchers have come up with face verification systems to help in this situation by matching the image of a candidate at the time with that of an identity record that has been registered. Other liveness detection algorithms study blinking behaviour, depth information, pattern of texture or motion to eliminate image, video or mask spoofing.

Certain frameworks also carry out periodic re-authentication in the course of the examination instead of authenticating the identity on one occasion on login. This comes in handy when a candidate steps off briefly out of the screen and somebody is trying to take their place.

Audio and Environmental Analysis.
All forms of misconduct cannot be identified with visual monitoring. Numerous systems, therefore, use audio streams that are obtained using microphones. Conversations, whispering or repeated background voices can be detected using speech activity. Other possible suspicious events that can be identified by acoustic event recognition include typing on a keyboard on a second device or activating voice assistants.

The environmental surveillance can also involve scanning the surrounding room or the presence of other cameras to monitor the area. Although it may decrease blind spots, this also poses practical and ethical issues in privacy and affordability of hardware.

Screen and Application Activity Tracking
The other significant area of study is concerned with direct contact with the examination apparatus. These systems track running windows, browser tabs, clipboard actions, keyboard shortcuts and unauthorized software usage. Switching out of the exam interface a lot might reflect either searching using the interface or communicating with the outside world.

Screen analytics may be able to show clearer evidence of rule violations compared to camera-based monitoring. But continuous monitoring of the desktops could reveal personal data that has nothing to do with the examination.

Multi-Modal Decision Systems
Recent research is beginning to support multi-modal architectures, which integrate video information, audio information and device behaviour into a single risk model. This method proves to be more strong since it is very rare that suspicion is portrayed through one signal. In the case of a candidate, who views sideways several times, one should not necessarily assume that he/she is cheating, yet, a sideways gaze and a speech and tab swapping might possibly be viewed as reason enough to revisit a particular candidate.

These signals have been combined with machine learning models, which, when used in fusing behavioural patterns, include support vector machines, random forests, convolutional neural networks, recurrent networks, and transformer-based networks.

Privacy-Aware Proctoring
Through more current literature, big-monitoring has been known to be accompanied by big-privacy. A number of strategies have been suggested:

- Local device inference as opposed to cloud analysis.
- Summary instead of recordings of events.
- Coding of evidence delivered.
- Short storage durations of data.
- Notice of user consent and transparency.
- Before punishments, human validation must be done.

These changes illustrate the slow transformation of surveillance-based systems towards trust-based systems.

Limitations of Current Online Examination Practices

Whereas remote examinations have been embraced in most institutions, when it comes to real-life application, they are barely developed. Ordinary learning management systems or generic meeting tools are most often provided without dedicated safeguards over integrity. This establishes various weaknesses.

- Inability to control the environment: They use homes, hostels, offices including public places, unlike physical exam halls, students are involved. The presence of noise, interruptions, and poor light, as well as changes in camera positions, mitigate the quality of monitoring and hinder the possibility of fair evaluation.
- Able to access outside resources with ease: Students can have notes as close as possible, use mobile phones when out-of-view, consult internet sources on other devices or use some hidden channels to talk to another person. These activities can hardly be identified with traditional software.
- Technical Inequality: Not every learner has a good web camera, fast internet access and a fast computer. Students with poor technical capabilities might be disadvantaged by heavy proctoring software.
- Psychological Stress: Continuous surveillance can increase anxiety. The students might be afraid that even innocent behavior, like look away, thinking about something, etc., will be considered vice. High levels of stress may have a detrimental impact on true performance.

- Privacy Risks: Any types of recording bedrooms, personal conversations, family movement, or irrelevant desktop content would pose vital questions of privacy. Poor security measures can lead to exposing delicate student information.

The limitations indicate the necessity of balanced solutions that do not infringe on student rights but guard integrity.

Shortcomings Of the Existing Practices of Online Examination

Despite the high adoption of remote exams in most educational institutions, most have not been fully implemented and have inconsistent operations. Most universities use either generic video conferencing services, or simple learning management systems that were not initially developed as an assessment tool but as a form of communication and delivery of content. These platforms often do not have specific processes of identity assurance, behavioural tracking, anomaly detection, and evidence management as an outcome. Lack of integrity controls taking specific forms exposes possible weaknesses to undermine fairness, credibility and trust among students in the exam process.

Lack of Controlled Environment

In traditional testing rooms, organizations control the sitting pattern, oversee mobility, limit socialization, and ensure consistent testing conditions to everyone taking a test. Such control can not be easily replicated in remote assessments since students may be taking examinations in different settings like homes, hostels, offices, libraries, or even in public areas. These places vary significantly in terms of lighting, background noises, the quality of internet connection, disruptions and workspace. Unwanted individuals may accidentally get into the room, or yield to the camera and display inadequate views of candidate behaviour, and ill positioning of the camera can make candidate behaviour less visible or visible. These environmental discrepancies render it hard to create an equal condition to all students and can decrease the efficiency of automated monitoring systems.

Easy Access to External Resources

The possibility to obtain illicit help is one of the strongest issues with online examinations. Students can have printed materials next to the computer, leave the mobile phone outside the camera shot, find answers using other devices, or use hidden typing programs to contact other students. Others might be verbally instructed by a second individual just out of sight, yet within the reach of hearing. Most of these activities are not in the immediate field of view of the web camera or within the monitored device, thus the traditional software products might not recognize them correctly. This gives an unfair distinguishability to deceitful participants and diminishes belief in remote assessment results.

Technical Inequality

Remote assessment relies on the assumption that students will have sufficient technological infrastructure, which is not always the case. Communication Some learners work with old-outdated computers, poor resolution webcams, poor microphones or insecure internet connectivity. Other people might use devices with their family or rely on insufficient data plans on their mobile devices. Proctoring applications that require a lot of resources may bring about a high use of processor load, bandwidth usage and system crash during exams. As a result, students who have less robust technical means could be interrupted, even late in their submissions, or receive false alerts that do not relate to academic misconduct. This digital divide brings inequity on the way of assessment.

Psychological Stress

The psychological pressure faced by a lot of students can be developed due to continuous monitoring with the help of webcams, microphones, and tracking of the screens. Applicants might not enjoy being captured all through the test especially during the evaluation by the assessing bodies in their personal confidential rooms. Anxiety can be elevated by fear of being improperly signalled as to abnormality (e.g., simply turning his head to think, fidgeting, reacting to the inevitable disturbances of the environment). Stress levels may be high and have adverse effects on focus, time management and general grades. As such, systems that aim to ensure fairness should be sensitive to how they are impactful on learners in terms of their emotions.

Privacy Risks

One of the most controversial problems of remote proctoring is privacy. The examination systems can store the facial images, voice recording, room, back room, background as well as desktop activities beyond the assessment itself. There are even instances when institutional systems come to see highly personal spaces like bedrooms or family rooms. When such data have been stored in an insecure manner, have been stored without reason, or have been viewed without authorization, then students can encounter huge privacy violations. The perception of intrusive surveillance can already decrease resistance and trust to online assessment technologies even in the case of no breach.

All of these restrictions prove that successful remote examinations cannot be done only with the help of a digital connection. The solutions in the future need to safeguard academic integrity and at the same time provide fairness, accessibility, transparency and respect of the rights of students.

On-Screen Activity Tracking Framework that is privacy-preserving

The current e-learning monitoring system should be able to detect behavioural risk in case of online exams and at the same time should not interfere with the privacy of the students. Traditional remote proctoring software tends to rely on constant recording and storing sensitive personal information that can raise issues around surveillance, information privacy violation, and legal control. Conversely, a privacy-conscious system this will aim to reduce unwarranted exposure to data by intelligently running the data, only retaining necessary evidence, and automated analysis is to be used in supporting human judgment and not in its place. The conceptual architecture proposed is divided into five primary functional units: secure authentication of the candidates, a local behavioural intelligence engine, context-specific risk scoring, privacy protection layer and human review dashboard.

Secure Candidate Authentication

Determining that the person taking the assessment is the registered candidate is the initial need of any online examination system. The student undergoes an authentication process via institutional logins and identity records as well as live facial verification before the exam time starts. The live image obtained is compared with the profile enrolled by the candidate to determine a consistent identity. Nevertheless, matching images is not enough since photos can be used, or recorded videos or online impersonating devices can be utilized to defraud the system. This is why the liveness detection systems are introduced to identify whether a subject under observation is a real and physically present person. Such mechanisms can examine the behaviour of blinking, natural facial movements, depth variation, head movement, or reaction to random prompting. Collectively, identity verification and liveness analysis provide a greater defence against impersonation and unauthorized substitution.

Local Behavioural Intelligence Engine

After the authentication, the system will trigger a behavioural monitoring module that will work on the device directly of the candidate. Instead of streaming unprocessed webcam imagery, sound, and recordings to an offsite server, the offered framework works with real-time analysis on-site by means of an in-built intelligence engine. Such a design encourages a high level of privacy since data that are sensitive are kept under local control unless certain anomalies are indicated that may lead to further research.

There are numerous sources of information, which the local engine processes. Facial presence, head orientation, stare direction and objects visible on the candidate are studied using the webcam images. Silent examinations are conducted by microphone input eavesdropping of on-ya-speak or suspicious sounds in the environment. The interactions on the screens are tracked to identify changes on the windows, open tabs in the exam, unauthorized access to applications, clipboard activity, or other banned online activities.

Diverse and possibly suspicious behaviours can be identified using this combined analysis by the module. As an example, it can recognize extended intervals when the student is not on the screen, recurrent non-screen staring implying that he/she is referring to external material, the presence of multiple faces in a camera view, frequent head turning towards side positions, uses copy-pasting tools against the purpose, audible voice activity during limited sessions, or visible banned things like cell phones, books, or handwritten text. This analysis is done locally, so only the results that are relevant and not full personal records are required to be disseminated outwards.

Context-Aware Risk Scoring

The behavioural events observed in an examination cannot be taken out of context. Most natural activities including momentarily looking aside during thought or changing the sitting positions can be perceived to be of suspicion when captured without the background. Thus, in the given framework a context-based risk scoring system, as opposed to on-the-spot rule-based punishment, is used.

A weighted contribution is given to each of the detected events based on its type, duration, frequency, when it occurs during the exam and how it relates to other events occurring at the same time. A single look out of the screen might be given a insignificant weight but a repeated shift of eyes and watching multiple tabs and speaking might be telling. In the same way, microphone noise that comes temporarily due to the environment should not be handled the same way as a conversation that lasts a long time.

Cumulative risk score is changing during the examination session. The system only raises an important alarm when several signals are detected to be the same or to have suspicious combinations. The methodology minimises false accusation, enhances fairness as well as being assured that the processes of decision-making demonstrate the presence of a behavioural pattern and not a single incident.

Privacy Protection Layer

The proposed architecture is based on privacy protection as opposed to a secondary feature. The privacy module is in charge of how the data are stored, transmitted, accessed, and retained during the examination lifecycle. The main aim of it is to make sure that the personal information is treated in regard to the principles of necessity, proportionality and security.

According to this model, raw video and audio streams are not transferred to the candidate device unless there is a high-risk incident that needs evidence retention. In these situations the only event-based clips or little contextual snapshots the system will store are provided, and

no recordings of the entire session will be stored. In transmission to institutional servers, behaviour logs and alert summaries as well as related evidence are encrypted. Access controls are very strong in order to have access to flagged content only by a specific group of authorized faculty members or individuals designated to do so in case of an examination.

The framework helps minimize unauthorized surveillance, data hoarding, and unintentional disclosure of sensitive student details by integrating these controls into the system design.

Human Review Dashboard

Even though artificial intelligence will help to identify abnormalities effectively, academic judgments must not be assigned to machines completely. Context, judgement and procedural fairness in examination are human-judged issues, which necessitate human supervision. Due to this fact, the last element of the framework is a review dashboard on a human basis that is applied by instructors, administration or designated examination officers.

The dashboard displays flagged events in an organized and comprehensible way. The reviewers will be able to access time stamps, type of event, and confidence ratings, behavioural summaries, and evidence clips related to every alert. As opposed to turning all of the examination captures, they concentrate on sessions in which significant anomalies have been recognized. This will minimize the workload and allow more attentive consideration of high priority cases.

Human reviewers may then be able to take into consideration contextual issues like technical issues, environmental issues, accommodations of disabled or other valid reasons before issuing judgments. By doing so, the dashboard safeguards procedural fairness since automated detection will act as assistance in making decisions and not as the final arbiter.

Architecture

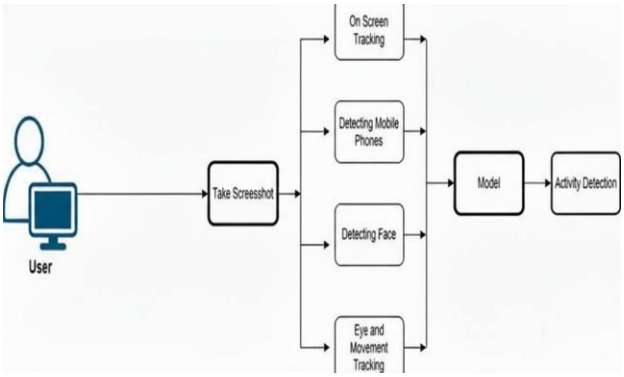

Fig. 1. *Architecture of Proposed System*

Proposed System

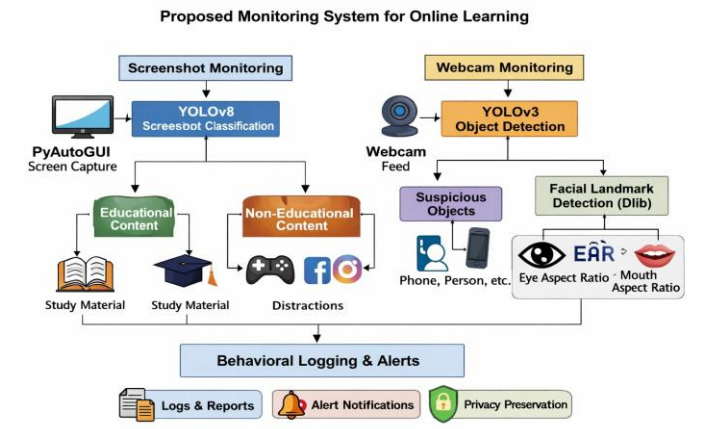

Fig. 2. *Monitoring System for Online Learning*

Benefits of Privacy-Conscious Intelligent Proctoring.

Privacy-conscious intelligent proctoring is a fairer alternative to traditional remote monitoring to provide not only examination security and responsible use of personal information. Instead of depending on surveillance that is unrestricted, these systems are structured to gather only

that information that is necessary to ensure integrity with minimum intrusion that is not warranted. This kind of approach is an advantage to both the institutions and learners because it enhances efficiency in operations, evenhandedness, trust, and scalability over time.

- Scalable Examination Management: Schools have a large number of students they tend to test at once, hundreds or even thousands of students. Invigilation on this scale is labor intensive (requiring a large number of staff members) and time consuming (involving scheduling and administration) to do manually. Large groups of candidates can be monitored by use of automated behavioural detection and prioritized alerts, privacy aware intelligent proctoring. The human examiners are thus able to devote their attention to high-risk cases rather than continually monitoring all the participants. This enhances significantly the viability of carrying out massive online tests.
- Improved Fairness: An automated system that has been developed properly utilizes the behavioral criteria of all the candidates thus minimizing recurring inconsistencies that might come up under human judgement. Suspicious activities like a recurring mismatch of identity, extended absence, or unauthorized application switching can be systematically analyzed. Put with human-review of events that are flagged, this makes the process more balanced and transparent where honest learners are not compromised but potential maleficence is dealt with adequately.
- Reduced Data Exposure: Among the key benefits of privacy-aware systems, there is the minimization of the unnecessary amount of personal data collection. Rather than repeatedly uploading unfiltered video and audio streams, most contemporary frameworks do analysis on the student machine and only submit event summaries, scores of confidence, or encrypted evidence when necessary. This greatly reduces the chances of abuse, information leakage or unnecessary holding of sensitive data.
- Operational Efficiency: Old review techniques might indle instructors to view lengthy examination records manually, which is not only time-consuming but also is ineffective. The automatic filtering can be done by intelligent systems to filter the routine ones and only flag those with suspicious patterns or rules being breached. Consequently, faculty members get to spend their time reading relevant evidence instead of combating huge quantities of unproductive recordings. This saves time on administration and speed up a post examination decision.
- Better User Trust: When students are informed about the types of data that are monitored, the manner in which choices are made, and privacy is safeguarded, then they are more likely to accept digital monitoring systems. Clear consent procedures, readable policies, understandable warnings, and restrictions on the data retention are also beneficial to enhanced trust in the examination process. Privacy-conscious systems will yield higher cooperation and decrease opposition among the learners compared to the opaque system of surveillance.

Open Research Challenges

Even after tremendous advances in technology, privacy-preserving online proctoring is a developing area and there are a number of research challenges that are yet to be solved. These issues need to be tackled to come up with systems that are accurate, equitable, are legally bound, and are generally acceptable within the circles of education.

- False Positives: Human behaviour that is normal may be taken as supporting suspicious activity by automated systems. Learners also tend to avert their eyes to the computer when they are remembering something, discovering that they change their posture during a long test, or they lean their voices when they are brainstorming on a problem. Alerts can also be caused by environmental disturbances like movement of the background or unexpected sounds. False positives that are high may destroy confidence in the system and unnecessarily cause stress to the candidates. Any future models have to be more discriminative between nuisance behaviour and actual misbehavior.
- Equity amongst a wide range of users.: Detecting models need to be able to work well in different student groups and testing environments. System performance can be influenced by variations in the skin tone, facial features, lighting quality, camera resolution, internet speed, disability, potentially different cultural communication styles. The evaluation will be discriminating in the case of algorithms being more effective in some groups than others. Fairness should then be ensured by the inclusion of datasets, auditing of bias and adaptive model design.
- Adversarial Cheating: With the advancement of the monitoring technologies, new types of cheating are introduced. Candidates can make efforts to circumvent detection with the help of virtual cameras, earpieces, or secondary screens, deepfake identity substitution, or AI-based assistance features. With such adversarial algorithms, there is a continuous technological arms race between evasion schemes and detection. The future work should come up with excellent protection mechanisms against new and more advanced threats.
- Legal Compliance: Educational establishments fall under various legal jurisdictions and laws with different regulations on consent, processing of biometric data, storage and transfer of information across borders. What may be deemed as a system that is agreeable in one area will infringe on the law of privacy in another. This means that the technical solutions should be deserving enough to address national legal frameworks and different institutional policies.

- Explainability: The students and administrators must understand the reason behind raising a red flag on a given exam session. When opaque machine learning models are applied in making decisions, and they are not presented in a clear manner, users will wonder the validity of the process. Explainable artificial intelligence techniques are capable of assisting to provide perceivable reasons, confidence, and evidences of each alert.
- Benchmark Datasets: Advances in this field are constrained by the few publicly available benchmark data of realistic online examination behaviour under privacy preserving constraints. In the absence of shared datasets and evaluation criteria, comparisons of competing approaches become hard, and results in literature hard to reproduce. Creation of anonymized datasets based on concerns for ethical collections continues to be a priority.

Future Scope

The future of secure online assessment is systems, which are technologically mature and ethically conscious. There are a number of new research lines that can greatly enhance the existing ones.

By facilitating distributed learning among institutions, federated learning can help institutions design more effective detection models without sharing raw student data and hence maintain privacy, but still get the benefit of distributed data of a larger scale. Low-latency local inference can be assisted by edge artificial intelligence to intelligently utilize student devices without relying on cloud computing to enhance responsiveness on live examinations.

Feel-aware analytics can be used to differentiate between suspicious behaviour and normal stress, so that affected systems can offer assistance, but not condemn unjustly anxious students. The audit systems based on blockchains have the potential of giving auditlogs that cannot be altered, enhancing accountability and trust in audit decisions.

Adaptive monitoring plans can also vary the intensity of supervision based on type of examination, length of examination or level of risk rather than overall surveillance to all situations. The use of multilingual speech analysis has the potency of enhancing equity in learning settings that are distributed worldwide since students can have varying languages and accents. Accessibility can be achieved by including interface design to cater to students with disabilities or special learning needs.

It is also anticipated that future platforms will be smoothly integrated with learning management systems, student information systems and institutional enterprise software to develop cohesive academic ecosystems. Finally, the task of the future study cannot be absolute surveillance, but the design of virtual assessment conditions which are safe, transparent, fair, and humane.

Conclusion

The study comes to the conclusion that automated proctoring systems that use computer vision and artificial intelligence are successful in preserving fairness during online tests and e-learning. By examining a student's face, eye movements, and gestures in real time, these systems can identify instances of cheating. They provide a clever, scalable, and sequestration-friendly method of covering exams in the absence of mortal invigilators. All things considered, comparable technology promotes academic integrity and guarantees confidence in online learning.

References

1. Jay Mayekar, Shubham Pal, Aditya Pandey, Bikra Pani, and Prof. Preeti Mishra, “Automated Proctoring System,” *International Research Journal of Engineering and Technology (IRJET)*, e-ISSN: 2395-0056, vol. 10, no. 4, Apr. 2023.
2. Simon Wenig, Michael Suriyah, Freiber Rojas, Kevin Schönleber, and Thomas Leibfried, “Simulation Framework for DC Grid Control and AC–DC Interaction Studies Based on Modular Multilevel Converters,” *IEEE*, 2016.
3. Aiman A. Turani, Jawad H. Alkhateeb, and Abdul Rahman A. Alsewari, “Students Online Exam Proctoring: A Case Study Using 360 Degree Security Cameras,” *2020 Emerging Technology in Computing, Communication and Electronics (ETCCE)*, 2020.
4. Asep Hadian Sudrajat Ganidisastra and Yoanes Bandung, “An Incremental Training on Deep Learning Face Recognition for M-Learning Online Exam Proctoring,” *2021 IEEE Asia Pacific Conference on Wireless and Mobile (APWiMob)*, 2021.
5. “Automated Proctoring System Using Computer Vision Techniques,” *Conference Paper*, July 2021, doi: 10.1109/ICSCAN53069.2021.9526411.
6. Renuka Devi and Gowri Srinivasa, “Detection of Anomalous Behavior in an Examination Hall Towards Automated Proctoring,” 2017. Available: https://www.researchgate.net/publication/321260760
7. Yousef Atoum, Liping Chen, Alex X. Liu, Stephen D. H. Hsu, and Xiaoming Liu, “Automated Online Exam Proctoring,” *IEEE Transactions on Multimedia*, 2015.
8. Yusep Rosmansyah, “Impersonation Attack-Defense Tree,” doi: 10.3991/ijet.v15i19.12699.
9. Aditya Nigam, Rhitvik Pasricha, Tarishi Singh, and Prathamesh Churi, “A Systematic Review on AI-Based Proctoring Systems: Past, Present and Future,” *Education and Information Technologies*, vol. 26, pp. 6421–6445, 2021.

10. Tejaswi Potluri, Venkatramaphanikumar S., and Venkata Krishna Kishore K., "An Automated Online Proctoring System Using Attentive-Net to Assess Student Mischievous Behavior," *Multimedia Tools and Applications*, vol. 82, pp. 30375–30404, 2023.
11. A. Sun and X. Chen, "Online Education and Its Effective Practice: A Research Review," *Journal of Information Technology Education: Research*, vol. 15, pp. 157–190, 2016.
12. E. Allen and J. Seaman, "Digital Learning Compass: Distance Education Enrollment Report," *Babson Survey Research Group*, Tech. Rep. 2017-1, 2017.
13. S. I. U. Rehman, H. S. Ullah, and A. Akhtar, "Consumption of Social Media and Academic Performance: A Cross-Sectional Survey of Perception of Students in KP Universities," *Global Mass Communication Review*, vol. 4, pp. 57–71, 2020.
14. K. Sohail and N. A. Nabaz, "The Influence of Social Media on Student's Academic Performance: A Case Study of Lebanese French University," *Modern Management Theory and Practice*, vol. 25, no. 2, pp. 117–127, 2019.
15. Goet, "Impact of Social Media on Academic Performance of Students," *KIC International Journal of Social Science and Management*, vol. 1, no. 1, pp. 35–42, Dec. 2022.
16. S. I. U. Rehman, H. S. Ullah, and A. Akhtar, "Consumption of Social Media and Academic Performance: A Cross-Sectional Survey of Perception of Students in KP Universities," *Global Mass Communication Review*, vol. 5, no. 4, pp. 57–71, Dec. 2020.
17. C. Li and F. Lalani, *The COVID-19 Pandemic Has Changed Education Forever. This Is How*, World Economic Forum, Geneva, Switzerland, 2020.
18. E. Vayena, A. Blasimme, and I. G. Cohen, "Machine Learning in Medicine: Addressing Ethical Challenges," *PLOS Medicine*, vol. 15, no. 11, Art. no. e1002689, Nov. 2018.
19. B. Imler and M. Eichelberger, "Using Screen Capture to Study User Research Behavior," *Library Hi Tech*, vol. 29, no. 3, pp. 446–454, 2011.
20. P. Krieter and A. Breiter, "Track Every Move of Your Students: Log Files for Learning Analytics from Mobile Screen Recordings," in *Proceedings of DeLFI 2018*, pp. 1–12, 2018.
21. B. J. Ferdosi, M. Sadi, N. Hasan, and M. A. Rahman, "Tracking Digital Device Utilization from Screenshot Analysis Using Deep Learning," in *International Conference on Data Science Applications (ICDSA)*, Singapore: Springer, 2023, pp. 661–670.
22. C. Dwork, "Differential Privacy," in *International Colloquium on Automata, Languages, and Programming*, Berlin, Germany: Springer, 2006, pp. 1–12.
23. X. Yi, R. Paulet, and E. Bertino, "Homomorphic Encryption," in *Tutorials on the Foundations of Cryptography*, Cham, Switzerland: Springer, 2014.
24. O. Goldreich, "Secure Multi-Party Computation," Manuscript, Preliminary Version, vol. 78, no. 110, pp. 1–108, 1998.
25. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated Learning: Strategies for Improving Communication Efficiency," 2016.
26. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep Learning with Differential Privacy," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA: ACM, 2016, pp. 308–318.
27. W. Dai, S. Wang, H. Xiong, and X. Jiang, "Privacy Preserving Federated Big Data Analysis," in *Guide to Big Data Applications*, 2018, pp. 49–82.
28. H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y. Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," arXiv:1602.05629, 2016.
29. S. J. Pan and Q. Yang, "A Survey on Transfer Learning," *IEEE Transactions on Knowledge and Data Engineering*, vol. 22, no. 10, pp. 1345–1359, Oct. 2009.
30. R. Varshney, "Trustworthy Machine Learning and Artificial Intelligence," *XRDS: Crossroads, The ACM Magazine for Students*, vol. 25, no. 3, pp. 26–29, Apr. 2019.