GLOBAL JOURNAL
OF COMPUTER SCIENCE AND TECHNOLOGY - E: NETWORK, WEB & SECURITY

Volume 26 | Issue 1 | 2026 | Article ID: GJCST-159592 | Language: English

CATALOGING
LCC • QA76.9.A25

Technological Approaches to Mitigating Examination Malpractices in Higher Education: A Mixed-Methods Evaluation of Secure Platforms, Proctoring Solutions, and user Perceptions

Article Record

Dr. Samuel Asare*
St. Monica's College of Education
*Corresponding Author

Emmanuel Amankwaah

Nelson Opoku-Mensah

Eric Aning

Emma Poku Agyeman

RECEIVED	REVISED	ACCEPTED	PUBLISHED	PEER REVIEW
2026-02-19	2026-02-20	2026-02-25	2026-04-09	Double Blind

Abstract

This study examines technological strategies implemented to prevent examination malpractices in higher education, focusing on secure platforms, biometric authentication, online proctoring, and adaptive assessment designs. Employing a hybrid research framework, it integrates quantitative surveys, qualitative interviews, pilot program observations, and platform analytics to evaluate efficacy and user experience across diverse academic disciplines. Findings indicate that multi-layered security configurations combining biometric verification, AI-assisted proctoring, randomized question delivery, and blockchain-based audit trails reduce misconduct incidence while maintaining fairness and user acceptance. The research highlights the importance of balancing automated detection with human oversight, ensuring infrastructural readiness, and providing transparent communication to address privacy and usability concerns. Results also reveal discipline-specific variations in adoption and effectiveness, with STEM fields showing greater gains linked to interactive assessment formats. The integration of generative AI tools presents both opportunities for enhanced feedback and challenges related to potential exploitation, underscoring the need for careful design and monitoring. Hence, the outcomes suggest that thoughtfully implemented technological interventions can support academic integrity by aligning security measures with pedagogical objectives and stakeholder engagement

artificial intelligence | biometric authentication | examination malpractice | plagiarism | technology

AI USE STATEMENT
No generative AI was used for analysis or results.

FUNDING
No external funding was declared for this work.

CONFLICT OF INTEREST
The authors declare no conflict of interest.

DATA AVAILABILITY
Not applicable for this article.

ETHICS
No ethics committee approval was required for this article type.

CONSENT
Not applicable for this article.

TRIAL REG.
Not applicable.

Crossref DOI: 10.34257/GJCSTE159592

How to Cite: Asare, D. S., Amankwaah, E., Opoku-Mensah, N., Aning, E., & Agyeman, E. P. (2026). Technological Approaches to Mitigating Examination Malpractices in Higher Education: A Mixed-Methods Evaluation of Secure Platforms, Proctoring Solutions, and user Perceptions. Global Journal of Computer Science and Technology, 26(1), 1-15. DOI: 10.34257/GJCSTE159592

AR Experience Web Page DOI

Print ISSN 0975-4350
Online ISSN 0975-4172

Under the strict compliance and defined process of

ARCHIVAL RECORD

GJCST · Vol 26 · Issue 1 · 2026

Article ID GJCST-159592 · DOI 10.34257/GJCSTE159592

Print ISSN 0975-4350 · Online ISSN 0975-4172

Global Journal of Computer Science and Technology - Section E
GJCST Volume 26 Issue 1

Technological Approaches to Mitigating Examination Malpractices in Higher Education: A Mixed-Methods Evaluation of Secure Platforms, Proctoring Solutions, and user Perceptions

Dr. Samuel Asare[§], Emmanuel Amankwaah[§], Nelson Opoku-Mensah[§], Eric Aning[§], and Emma Poku Agyeman[§]

[§]St. Monica's College of Education

Abstract

This study examines technological strategies implemented to prevent examination malpractices in higher education, focusing on secure platforms, biometric authentication, online proctoring, and adaptive assessment designs. Employing a hybrid research framework, it integrates quantitative surveys, qualitative interviews, pilot program observations, and platform analytics to evaluate efficacy and user experience across diverse academic disciplines. Findings indicate that multi-layered security configurations combining biometric verification, AI-assisted proctoring, randomized question delivery, and blockchain-based audit trails reduce misconduct incidence while maintaining fairness and user acceptance. The research highlights the importance of balancing automated detection with human oversight, ensuring infrastructural readiness, and providing transparent communication to address privacy and usability concerns. Results also reveal discipline-specific variations in adoption and effectiveness, with STEM fields showing greater gains linked to interactive assessment formats. The integration of generative AI tools presents both opportunities for enhanced feedback and challenges related to potential exploitation, underscoring the need for careful design and monitoring. Hence, the outcomes suggest that thoughtfully implemented technological interventions can support academic integrity by aligning security measures with pedagogical objectives and stakeholder engagement

Keywords: *artificial intelligence, biometric authentication, examination malpractice, plagiarism, technology*

DOI: 10.34257/GJCSTE159592

1. Introduction

The integration of technology into higher education assessment practices has prompted substantial experimentation with strategies aimed at mitigating academic dishonesty. Institutions have recognized that conventional proctoring methods may be insufficient in contexts marked by large-scale remote assessments. In response, technological innovations such as biometric authentication systems are being explored to authenticate candidates and reduce impersonation risks. For instance, restricting access through fingerprint or retina scans serves as a deterrent to identity fraud, ensuring that only the registered candidate can participate in an assessment (Pillai et al., 2021). This move shifts the emphasis from reactive detection of misconduct to preventive verification, which may prove more reliable for maintaining trust in digital examinations. A parallel stream of interventions targets the monitoring of student activity during exams using online proctoring tools. These platforms typically combine live human oversight with automated anomaly detection algorithms that flag suspicious behavior patterns. They may utilize real-time camera feeds, microphone input, and screen activity tracking. Here, the operational challenge lies in calibrating intrusion levels so as not to compromise students' psychological comfort while upholding integrity standards. As suggested by frameworks drawing from technology acceptance models, wide-scale implementation hinges on stakeholder buy-in; if faculty or students perceive these measures as excessive or technically unreliable, adoption will stall regardless of potential benefits (Fink et al., 2023). Beyond direct supervision mechanisms, plagiarism detection software constitutes another line of defense against examination malpractice, particularly in contexts where assessments involve written assignments or project reports. Embedded within learning management systems, such tools compare submissions against extensive databases comprising web sources, subscription-based libraries, and prior student work. The adoption of these instruments has had tangible effects on the quality and originality of submissions but introduces nuanced considerations regarding false positives and the interpretation of similarity indices (Keo et al., 2024). Academic staff must balance automated outputs with qualitative review to avoid penalizing legitimate academic style conventions such as standard terminology use in niche disciplines. Some strategies employ a hybrid combination of preventive and pedagogical components designed to not merely catch misconduct but reshape student approaches to assessments altogether. Project-based work and critical thinking exercises integrated into course design can indirectly diminish incentive for dishonest practices by increasing engagement and making rote copying impractical. These methods often encourage synthesis over recall, inherently aligning with the goals seen in complex thinking skill development initiatives where active problem-solving minimizes opportunities for shortcut behaviors (Patiño et al., 2023). Interestingly, there is variation across disciplines in how technology-based interventions are perceived and applied. Humanities and social sciences educators may frame their reservations differently than counterparts in STEM contexts , reflections trace back to pre-pandemic studies suggesting disciplinary norms influence adoption trajectories (Sum & Oancea, 2022). In moments of crisis-driven change like the COVID-19 out-

break's mass migration to online formats, these differences become pronounced. Some instructors adapt rapidly due to preexisting familiarity with online teaching interfaces; others face steeper learning curves necessitating structural support such as hardware upgrades or professional development webinars (Danyluk & Burns, 2021). While technical sophistication is an asset for implementing integrity measures, institutional success also depends heavily on operational readiness. Projects assessing new tools frequently run pilot programs before full deployment to identify unforeseen constraints , bandwidth limitations affecting biometric scan responsiveness or variations in regional privacy regulations impacting data storage protocols are examples that surface during trial phases (Pillai et al., 2021). Such piloting has clear parallels with broader educational technology integration exercises where methodical review combines empirical research synthesis with iterative feedback loops from early adopters (Keo et al., 2024). From an analytical standpoint, evaluating these technologies requires multi-layered criteria beyond raw reduction rates in detected misconduct. Stakeholders tend to weigh logistical ease-of-use for both instructors and examinees alongside perceptions of fairness embedded within monitoring processes. Excessive automation without transparent explanatory procedures risks alienating those subjected to it; conversely overly manual supervision can reintroduce human error biases that automated systems were meant to curb. Achieving equilibrium between algorithmic accuracy and user trust remains a moving target given technological variability across platforms (Fink et al., 2023). Moreover, the conversation around technological intervention intersects directly with broader pedagogical transformations sparked by increased digitalization. Transition experiences noted among award-winning faculty point toward designing courses that emphasize frequent interaction and varied assessment strategies over reliance on singular high-stakes events (Danyluk & Burns, 2021). Such structuring naturally integrates multiple checkpoints for both performance tracking and integrity assurance without overwhelming students under surveillance-heavy conditions. This ongoing shift hints at deeper institutional change where security measures blend seamlessly with learning design strategies rather than appearing as external controls imposed after course planning is complete. If implemented thoughtfully within this merged context , combining authentication protocols like biometrics with adaptive assessment forms , universities may develop environments where examination integrity is supported organically through the same structures driving engaged learning (Patiño et al., 2023).

2. Background and Context of Examination Malpractices

2.1. Historical Overview of Academic Integrity Challenges

Academic dishonesty has been documented for as long as organized education systems have existed, but its forms and prevalence have shifted alongside changes in pedagogical practices, societal expectations, and technological capabilities. In earlier eras, misconduct often centered around face-to-face examination scenarios, where impersonation or smuggling of written notes into an exam venue were primary concerns. Interventions at that time relied more on human observation, with proctors stationed to physically monitor behavior and enforce adherence to rules. While effective to a degree, such arrangements were constrained by the subjective attentiveness of the monitors and the absence of standardized detection techniques. Over time, the expansion of formal assessment structures introduced challenges related to scale and diversity in student populations. Large examination halls with hundreds of candidates reduced the capacity for individualized oversight and created conditions favorable for anonymity-based cheating methods. The normalization of written assignments in coursework also opened avenues for copying peer work or published literature without proper attribution. Early institutional responses included strict invigilation protocols and honor codes designed to cultivate internalized ethical standards among students , approaches still advocated by many institutions despite mixed evidence on their universal effectiveness (Chan & Hu, 2023). A recurring theme in this historical trajectory is the reliance on deterrence through fear of sanctions rather than systemic redesign of assessment formats. Moments of significant transformation in academic integrity management often have coincided with shifts in technology use. The introduction of typewriters and later word processors widened opportunities for duplicated text to go undetected. This triggered the emergence of plagiarism awareness campaigns but lacked automated verification tools capable of systematic comparison against reference databases (Keo et al., 2024). The push toward computer-mediated learning environments during the late 20th century further amplified both legitimate academic possibilities and potential misconduct vectors. Digital communication technologies made it straightforward for students to exchange answers in real time or purchase completed assignments from external providers. These trends eroded confidence in traditional safeguarding measures that had served reasonably well in analog settings. Remote education models prior to the COVID-19 pandemic revealed early vulnerabilities in identity verification for assessments conducted outside institutional premises. Without visual confirmation from invigilators, educators depended largely on trust-based arrangements supplemented occasionally by mailed paper assessments. Few institutions employed biometric authentications at scale due to cost barriers and unresolved privacy considerations (Shyja et al., 2024). However, security breaches like leaked exam papers demonstrated how inadequately guarded networks could facilitate large-scale malpractice. The high-profile example involving a hacker accessing and disseminating national-level test questions underscored that even examinations perceived as secure may be compromised once distribution leaves controlled environments. Recent decades have brought increasing awareness that misconduct is not constrained solely to opportunistic behavior; contextual factors within teaching environments can predispose certain student groups toward dishonest acts. Research suggests that poorly aligned assignments, limited formative feedback opportunities, or perceptions that effort will not yield fair evaluation can push students toward superficial engagement strategies (Chan & Hu, 2023). In this sense, sustained academic integrity challenges can be symptomatic of broader instructional deficiencies rather than isolated incidents requiring punitive interventions alone. This observation has informed subsequent developments aimed at rethinking assessment design itself rather than just strengthening surveillance mechanisms. Parallel to these pedagogical considerations, sociocultural changes have influenced norms surrounding originality and ownership of intellectual work. Globalization of education brought students from diverse schooling backgrounds into common programs, producing varied conceptions about citation conventions and collaboration ethics (Civaner et al., 2022). Misalignments between these perspectives and institutional policies sometimes manifested as unintentional violations rather than deliberate fraud. Effective remediation thus required integration of ethics instruction into curricula rather than assuming such knowledge would emerge organically through exposure. Technology acceptance theory has shed light on why certain integrity-related interventions succeed where others are resisted (Fink et al., 2023). Historically, measures

perceived by educators or students as overly intrusive or difficult to use encountered resistance that limited adoption rates despite theoretical efficacy. Conversely, tools integrating smoothly into routine workflows were more likely to persist over time even if their deterrent capacities were modest relative to standalone high-surveillance systems. This pattern reflects how practical usability shapes historical outcomes for integrity enforcement technologies alongside moral arguments about fairness. Overall, the timeline of examination malpractice reveals cycles wherein advances intended to broaden educational opportunity inadvertently create new exploitation avenues requiring countermeasures. Each major shift , whether mass higher education enrollment initiatives, adoption of online delivery modes, or integration of artificial intelligence applications , appears accompanied by redefinitions of both what constitutes misconduct and how it should be addressed ethically (Oc et al., 2025). These evolving definitions echo ongoing tensions between innovation-driven pedagogy and preservation of trust in academic credentials. As past experiences illustrate, effective solutions tend to emerge from balancing preventive technological frameworks with continuous refinement of teaching approaches sensitive to learner motivation profiles , a perspective that connects directly back to current debates about sustainable strategies highlighted in Section 1.

2.2. Impact of Technology on Examination Practices

The integration of digital tools into examination processes has transformed both the logistics and the philosophy surrounding assessment in higher education. Historically framed as localized paper-based events, examinations are now increasingly administered through computer-enabled platforms, a shift that has been accelerated by external pressures such as pandemic-related campus closures (Fink et al., 2023). This transformation is not simply a matter of replacing pen with keyboard; it carries implications for security, accessibility, and pedagogical alignment that are reshaping institutional strategies. One immediate consequence is the potential for expanded reach. Computer-administered examinations offer scalable delivery to diverse student cohorts regardless of physical location, bridging geographical barriers that once limited participation. In contexts like India, virtual communication labs and upgraded online platforms have emerged to support language proficiency evaluation alongside other course content, blending theoretical and practical components into remotely delivered assessment formats (Yadav & Yadav, 2023). Such changes open doors for international collaboration but also raise concerns over consistency in exam conditions , a critical factor for fairness. Security considerations remain at the forefront in this shift. Remote delivery amplifies the challenge of ensuring candidate identity authenticity and deterring illicit collaboration. Technological solutions such as biometric authentication systems or adaptive online proctoring mechanisms aim to address these challenges by tying access to tangible identity markers or behavioral monitoring streams (Pillai et al., 2021). Adaptive e-exams, which modify question sets dynamically according to student responses, attempt to reduce opportunities for premeditated answer sharing. This approach contrasts with conventional e-exams that essentially recreate static paper tests on a screen, thus requiring different preparatory conditions for implementation (Fink et al., 2023). Institutions exploring adaptive systems often must weigh their perceived novelty against stakeholder concerns about transparency and equitable difficulty levels across variants. Alongside these direct integrity measures, technology alters how assessments themselves are structured. Practical components , such as laboratory simulations using tools relevant to a discipline , can be incorporated seamlessly into digital assessment pipelines. In cybersecurity course contexts, hands-on engagements with network analysis or password-cracking software during evaluative sessions illustrate how authentic skill measurement can coincide with integrity safeguards (Churi & Rao, 2021). This fusion of real-time technical exercises within an exam setting exemplifies how technology can enhance both validity and engagement while reducing viability for dishonest shortcuts. The use of automated grading and feedback features embedded in learning management systems contributes another layer of transformation. These systems can generate instant evaluations for objective-format questions or flag sections of written work with high lexical similarity to existing corpora (Keo et al., 2024). While efficiency gains are clear, the interpretation of flagged content remains an inherently human task due to nuances around academic writing conventions or discipline-specific jargon that might register as matches without constituting misconduct. Overreliance on algorithmic verdicts can risk penalizing legitimate scholarly expression if contextual review is bypassed. From an operational perspective, institutions often adopt phased rollouts to resolve unforeseen challenges before committing fully to technological examination systems. Pilot programs reveal bottlenecks such as network bandwidth instability affecting biometric scans or disparities in device capabilities among students (Pillai et al., 2021). These trials also serve as testbeds for refining proctoring protocols to strike a balance between surveillance efficacy and student psychological comfort. A holistic technology adoption plan must consider not only hardware infrastructure but also administrative readiness and cultural acceptance across disciplines. The broader pedagogical impact is equally important. As discussed in Section 2.1, assessment practices influence learning behaviors; introducing interactive technologies into examinations may encourage sustained engagement with course material rather than last-minute rote preparation. For instance, project-based evaluation formats facilitated by collaborative digital environments promote skills like reflection and teamwork under evaluative conditions (Patiño et al., 2023). Embedding these active learning strategies within exam design aligns integrity enforcement with educational quality enhancement rather than treating them as separate objectives. Generative AI presents another emerging technological influence on examination practices. While its integration offers creative possibilities , from automated question generation to personalized feedback loops , it brings substantial privacy and security risks if inadequately regulated (Chan & Hu, 2023). Research suggests that institutional readiness around AI literacy among students and instructors shapes both uptake rates and effective usage patterns. Without corresponding awareness training, reliance on AI-driven tools could inadvertently produce new forms of malpractice or overdependence on machine judgment. One often overlooked aspect involves teacher workload during technologically mediated exams. Interfaces designed without consideration for cognitive load can tax instructors managing complex exam scenarios (Stenalt & Mathiasen, 2024). Supporting teachers through intuitive controls, clear result dashboards, and reduced manual intervention not only improves adoption willingness but also sustains fair oversight capacity during higher-stakes evaluation events. Finally, the cultural dimension cannot be ignored. Many modern classrooms , physical or virtual , accommodate students accustomed to instant communication via social media platforms integrated informally into study habits (Keo et al., 2024). Leveraging these platforms toward legitimate preparatory dialogue while guarding against their misuse during live assessments represents an intricate balancing act requiring policy clarity. Technology's capacity to shape behavior extends far beyond its functional role in delivering questions; it reconstructs the ecosystem in which academic integrity is negotiated daily. The cumulative

effect of these shifts suggests that technology is redefining what examinations mean within higher education landscapes. It appears likely that future practices will integrate secure authentication methods, adaptive question architectures, authentic skill-performance modules, AI-assisted processing, and workload-conscious designs into cohesive frameworks where integrity assurance is inseparable from pedagogical value creation (Fink et al., 2023). The challenge ahead lies not merely in selecting suitable tools but aligning them thoughtfully with context-specific needs so they enhance trust in qualifications without alienating those they aim to assess.

3. Technological Strategies for Prevention

3.1. Secure Examination Platforms

Secure examination platforms integrate a combination of technical safeguards, procedural controls, and adaptive user interfaces to maintain integrity during digital assessments. The design philosophy typically blends preventive measures against unauthorized access with detection mechanisms that operate unobtrusively while preserving fairness across diverse student populations. At their core, these platforms employ identity verification protocols to ensure that each candidate is who they claim to be before and during the exam session. Methods such as biometric authentication , fingerprint or facial recognition , strengthen this layer by binding examination access to unique physiological traits (Pillai et al., 2021). In high-stakes contexts, systems augment this authentication with two-factor verification or secure login tokens, thereby creating multiple barriers against impersonation attempts. Communication security is another defining element. Encryption technologies, often based on the Advanced Encryption Standard (AES), safeguard real-time data exchanges between the exam client and server. Coupled with secure transmission protocols like HTTPS, such cryptographic measures minimize risks from interception or data manipulation during transit. Platforms store sensitive decryption keys in isolated segments of system infrastructure to reduce vulnerability exposure. While encryption ensures confidentiality and integrity for assessment content, its effective use demands robust key management policies to preclude insider misuse or accidental leaks. Many secure examination environments also integrate lockdown browsers. On activation, these specialized applications restrict device functionality, blocking access to external software, websites, or stored files until the assessment concludes (Shyja et al., 2024). This local containment mechanism limits opportunities for candidates to consult unauthorized resources while minimizing the need for constant human surveillance of on-screen activity. Modern iterations include dynamic blocking that adjusts restrictions in real time according to exam progress, a feature aimed at preventing static circumvention strategies once candidates understand the fixed limitations of older lockdown systems. Real-time monitoring functions supplement these preventive controls with evaluative oversight throughout the exam session. Online proctoring tools embedded within secure platforms blend automated tracking , camera-based gaze analysis, keyboard interaction patterns , with human review options (Pillai et al., 2021). Such hybrid systems permit immediate anomaly flagging alongside contextual judgment to assess whether detected irregularities truly indicate misconduct. The challenge lies in tuning sensitivity thresholds: overly aggressive detection risks false positives that can erode student trust, whereas lax thresholds may let coordinated cheating go unnoticed. Pilot testing in varied institutional contexts helps calibrate these parameters before full deployment (Wijaya et al., 2024). Adaptive security measures within certain platforms extend beyond content delivery control toward structuring question presentation itself. Banks of equivalent-difficulty items allow randomization per user while maintaining overall difficulty parity (Fink et al., 2023). Variants in sequencing and phrasing disrupt answer-sharing without imposing obviously different workloads among candidates. This strategy reduces incentives for collaboration during live sessions whilst retaining fairness by controlling psychometric consistency across randomized sets. When combined with backend analytics capable of detecting statistically improbable answer congruence among groups of candidates, item randomization becomes part of an integrated prevention ecosystem rather than an isolated tactic. Institutional adoption sometimes encounters resistance if platform operation imposes excessive cognitive burden on faculty or students unfamiliar with complex digital tools. Developers have responded by refining ergonomically designed user interfaces that emulate familiar paper-based layouts through features such as digital stylus support (Pillai et al., 2021). This minimizes adaptation fatigue and alleviates anxiety linked to abrupt methodological shifts from conventional exams to purely screen-based environments. For instructors, dashboards summarizing candidate behavior logs facilitate manageable oversight without demanding exhaustive manual data trawling during review periods. From a broader perspective, building effective secure examination systems requires adequate infrastructural planning and policy alignment across administrative tiers. Reliable network connectivity is essential; intermittent connections can stall authentication processes or disrupt encrypted communication streams mid-exam (Keo et al., 2024). Institutions addressing this proactively often pair platform implementation with investment into server capacity and contingency pathways such as offline mode synchronization once connectivity resumes. Training programs targeted both at educators managing these exams and students required to navigate them are critical for uptake success; lack of familiarity frequently correlates with higher error incidence rates and increased dispute frequency post-exam (Chan & Hu, 2023). A growing frontier involves integrating blockchain technology into secure platform architectures. Distributed ledger approaches promise immutable records of exam events , logins, answer submissions, proctor observations , accessible transparently yet protected from tampering due to their cryptographic chaining properties (Cheriguene et al., 2022). While preliminary deployments report elevated energy demands compared with conventional setups, scaling solutions through edge computing seem poised to offset efficiency concerns in large-user scenarios without diminishing trust benefits inherent in blockchain-enabled audit trails. The efficacy of secure examination platforms is not merely judged by reduction metrics in documented cheating cases but also by their integration into pedagogical contexts that promote constructive learning behaviors (Patiño et al., 2023). Preventive technology backed by well-considered assessment design steers candidates toward engagement instead of evasion; simulations inside science examinations or interactive problem-solving modules embedded within platform workflows exemplify how integrity enforcement can coexist organically with skill measurement objectives rather than exist as purely punitive surveillance infrastructure (Fink et al., 2023). This synergy becomes especially effective when coupled with policies promoting equitable hardware access and culturally attuned digital content delivery so that integrity assurance does not inadvertently disadvantage specific groups (Keo et al., 2024). Ultimately, secure examination platforms manifest as layered ecosystems wherein technical precision converges with human-centered considerations: authentication verifies identity without overcomplicating entry; encryption defends transport integrity while remaining operationally straightforward; monitoring detects anomalies

under sensitivity regimes shaped through iterated pilot feedback; adaptive question handling diminishes advance collusion potential; ergonomic interfaces support sustained adoption without alienating users unused to high-tech assessments; infrastructural resilience ensures reliability under varied conditions; blockchain integration offers auditable immutability at scalable cost structures; pedagogical embedding reframes security as an ally in genuine competence evaluation rather than a distant enforcement apparatus. When orchestrated coherently under institutional leadership committed to sustained refinement guided by ongoing empirical review (Wijaya et al., 2024), such platforms demonstrate measurable impacts on both cheating deterrence rates and confidence in credential legitimacy among educational stakeholders across cultural and disciplinary boundaries.

3.2. Proctoring Solutions

Proctoring solutions serve as a critical complement to secure examination platforms by providing live or recorded oversight mechanisms that help identify, deter, and investigate misconduct in real time or retrospectively. Building on the authentication and lockdown principles described earlier in Section 3.1, these systems introduce an additional layer of vigilance focused not only on pre-exam identity verification but also on continuous monitoring throughout the assessment window. The underlying architecture often comprises integrations between video streaming components, network logs, and behavioral analytics that operate simultaneously to flag anomalies. Real-time visual feeds, typically captured via webcams, allow remote invigilators to observe candidates' surroundings for unauthorized materials or individuals (Pillai et al., 2021). Audio channels can capture ambient sound cues, such as whispered communications, that may betray collusion attempts during online examinations. These multiple data modalities create a composite situational awareness extending far beyond what traditional classroom proctors could achieve. From a technical standpoint, some proctoring tools incorporate gaze-tracking algorithms capable of detecting patterns where the test-taker's attention shifts repeatedly away from the screen for extended intervals (Fink et al., 2023). While such deviations may signal potential use of external aids, it is important to contextualize findings; algorithmic triggers must be balanced against allowances for natural human movement like looking around briefly due to distractions. Excessive sensitivity to benign actions risks inflating false positive rates, which can undermine confidence in the enforcement process. This tension points toward iterative calibration phases during institutional adoption, drivers behind pilot programs that trial various settings across student populations before locking them into steady-state configurations (Wijaya et al., 2024). A notable evolution in proctoring has been the emergence of hybrid models blending artificial intelligence with human review. In this design, automated detection handles repetitive tasks, flagging suspected phone usage based on pixel analysis or recognizing prohibited browser tab activity, while human reviewers evaluate flagged moments for credible evidence (Civaner et al., 2022). Such dual-layered scrutiny maintains efficiency without losing the interpretive nuance of trained educators who understand discipline-specific contexts. Implementation success hinges greatly on transparency; students informed upfront about technical and human oversight are likelier to engage constructively than those confronted unexpectedly by opaque monitoring regimes. Some institutions adopt record-and-review approaches rather than synchronous invigilation. Here, complete exam sessions are archived, including screen captures and peripheral device logs, for later inspection if integrity concerns emerge (Keo et al., 2024). This retrospective method reduces bandwidth demands since live streaming is unnecessary and limits examiner fatigue associated with constant surveillance. However, latency in detection means preventive intervention cannot occur mid-exam. In high-stakes environments, live proctoring remains preferable when immediate disruption is essential to halt unfolding misconduct. Integration with lockdown browsers strengthens proctoring solutions by closing digital pathways that bypass human observation (Shyja et al., 2024). For example, if a candidate attempts to access an external site mid-exam, the browser can automatically terminate the session while alerting the invigilator dashboard in real time. This creates a direct feedback loop between environmental restrictions and situational monitoring, a synergy that complicates organized cheating strategies by requiring simultaneous circumvention of multiple safeguards. The application of proctoring technologies intersects heavily with ethical considerations around privacy and psychological impact (Civaner et al., 2022). Continuous camera surveillance enters personal spaces in remote settings where students might have limited control over background conditions. Ensuring adjustable sensitivity settings alongside clear policies on footage storage duration helps mitigate resistance grounded in privacy concerns. Moreover, interface designs promoting clear status indicators, such as recording alerts or audio feed toggles, make processes visible and predictable for examinees. Advanced deployments experiment with biometric triggers embedded within ongoing monitoring streams rather than isolated at session start. Facial recognition checks can be performed intermittently to ensure the same individual remains active throughout (Pillai et al., 2021). Such rolling verifications close gaps left by single-point identity checks vulnerable to post-authentication substitution scenarios (e.g., switching places mid-assessment). Nevertheless, rolling checks raise technical challenges related to lighting variation and facial coverage; any failure risk must be addressed by fallback identifiers such as keystroke dynamics or behavior fingerprints derived from interaction rhythm patterns. Connectivity stability plays an understated role in proctoring reliability (Keo et al., 2024). Unstable internet links can generate false anomaly flags, inadvertent pauses mistaken for suspicious inactivity, or cause proctors to miss subtle cues altogether due to video lag or dropped frames. Consequently, many institutions develop contingency protocols permitting offline failover modes where local logs continue recording until reconnection synchronizes data packets securely back to central oversight systems. Interestingly, certain educational fields draw unique benefits from integrating discipline-relevant tasks into monitored assessments (Patiño et al., 2023). A chemistry course, for instance, might include live lab simulations within exam software while proctor feeds verify proper engagement with virtual reagents instead of alternative shortcuts. This subject-specific alignment reframes surveillance less as punitive watchfulness but more as validation of authentic skill application under evaluative conditions, a framing that bolsters acceptance among both learners and faculty. Blockchain integration offers promising avenues for securing provenance records attached to monitored events (Cheriguene et al., 2022). Each flagged activity during an exam, whether automated trigger or manual note from a human proctor, can become an immutable ledger entry resistant to later tampering or deletion. Such structures not only protect evidentiary material during appeals processes but also reassure stakeholders that incident reporting adheres consistently to defined audit protocols. Ultimately, effective deployment of proctoring solutions rests on harmonizing sophisticated detection capabilities with humane operational practices. Systems must reduce opportunities for cheating through seamless technological enforcement yet accommodate legitimate user comfort through clear communication and

flexible configuration paths (Chan & Hu, 2023). Where alignment occurs, in training programs building literacy around these tools for students and educators alike, the balance tilts toward long-term legitimacy gains rather than short-lived deterrence based solely on fear of surveillance. In this way, proctoring becomes not an isolated enforcement mechanism but part of a broader ecosystem integrating secure platform infrastructure, ethical guidelines, adaptive pedagogy, and infrastructural resilience into cohesive integrity assurance strategies suited for diverse higher education contexts across geographic and disciplinary boundaries.

4. Methodology

4.1. Research Design

The research design employed here draws from a hybrid framework that integrates descriptive-quantitative analysis, document review, and pilot-based empirical validation to examine the effectiveness of technological strategies in preventing examination malpractices. Building on the preventive and detection-oriented measures discussed in Section 3.1, the approach initiates with a critical synthesis of existing scholarly and institutional materials regarding identity verification, proctoring configurations, and plagiarism detection technologies. This literature review was conducted systematically to identify prevailing trends, known limitations, and emergent opportunities in technologically mediated assessment integrity (Patiño et al., 2023). The decision to incorporate both archival data and contemporary case studies stems from the need to capture longitudinal patterns as well as recent developments shaped by rapid digital adoption during crisis contexts. For empirical grounding, a structured survey instrument was deployed across multiple higher education sites, targeting both students and faculty members actively engaged in digitally administered assessments under varying degrees of security enforcement. In one strand of the research, 200 student participants were selected via random sampling methods to yield representative demographic diversity (Yadav & Yadav, 2023). Responses were quantified along categorical scales (high, medium, neutral, low impact) aligned with core evaluation variables such as perceived fairness of monitoring systems, ease-of-use of authentication protocols, and trust in automated content analysis outcomes. These quantitative metrics allowed statistical comparison between cohorts exposed to different configurations , for example, full biometric plus AI-enhanced proctoring versus minimal lockdown browser restriction. Complementary to survey data collection, semi-structured interviews with administrators and teaching staff provided qualitative insight into operational feasibility. This stage followed document analysis procedures that drew on both local institutional policy archives and broader educational technology frameworks (Keo et al., 2024). The intention here was not simply to confirm efficacy claims but to unpack administrative concerns like technical accessibility constraints (Moshtari & Safarpour, 2024) or budgetary considerations influencing platform selection. Coding of interview transcripts revealed recurring themes around stakeholder transparency needs, student privacy apprehensions (Civaner et al., 2022), and alignment between assessment format design and surveillance capacity. Pilot testing served as an applied bridge between theoretical review and practical deployment. Candidate institutions implemented scaled demonstration versions of secure platform architectures incorporating biometric login sequences (Pillai et al., 2021) followed by adaptive question sets aimed at minimizing answer-sharing probability (Fink et al., 2023). Each pilot was preceded by orientation sessions for both students and instructors meant to gauge readiness levels; feedback loops allowed for iterative tuning of sensitivity thresholds in behavioral analysis features so as to avoid excessive false alarms. Network performance logs collected during these events helped surface infrastructural bottlenecks like latency spikes impacting live facial-recognition verification consistency (Keo et al., 2024), which could then inform resilience planning before full-scale rollout. Observation protocols within pilots included real-time monitoring dashboards accessible to designated invigilators alongside automated anomaly flaggers embedded into the examination environment. These generated timestamped event records , attempts at unauthorized site access caught by lockdown browsers (Shyja et al., 2024), prolonged gaze deviations detected via machine vision modules , which were later assessed against human reviewer annotations for concordance rates. Discrepancies between automated triggers and human interpretation highlighted algorithmic precision gaps that fed back into sensitivity recalibration cycles. Such triangulation between machine outputs, human judgment, and participant self-report forms the core robustness measure in this design. Given the known variability across academic disciplines regarding comfort with surveillance-heavy exam settings (Oc et al., 2025), pilots also stratified samples by field of study to detect discipline-specific adoption patterns. STEM courses integrating simulation-based exam components (e.g., cybersecurity labs requiring network protocol manipulation under timed conditions) demonstrated smoother acceptance where monitoring coincided visibly with skill validation tasks (Churi & Rao, 2021). Humanities-focused trials had mixed responses; perceptions leaned toward questioning necessity unless paired with active learning strategies promoting deeper engagement during assessment windows (Patiño et al., 2023). A further layer involved analysing secondary datasets from institutions already applying generative AI tools within their assessments for question creation or feedback delivery (Oc et al., 2025). This clarified whether AI integration altered malpractice incidence compared with non-AI environments or introduced novel vulnerabilities needing countermeasures. A consistent methodological thread across all stages was cross-validation: any conclusions drawn from one data stream (quantitative surveys) were examined against others (qualitative interviews, pilot operational logs) before being considered generalizable. Data synthesis processes adhered to inclusion/exclusion criteria established at the onset based on thematic relevance to technological prevention mechanisms rather than generic academic integrity strategies without a tech component (Patiño et al., 2023). Categorization coded interventions into primary prevention tools (biometric locks, lockdown browsers), secondary deterrence elements (live proctoring cues), and tertiary supports (training modules enhancing platform literacy) so that effect sizes could be contextualized relative to their operational role. The analytical framework emphasised not just raw rates of cheating reduction but user experience variables shaping sustainability prospects in institutional ecosystems. Impact assessment thus married outcome metrics , documented misconduct case declines , with process evaluations tracking ease-of-adoption scores among educators and IT staff. This multidimensional perspective aligns with assertions that technology-mediated integrity assurance succeeds insofar as it becomes an accepted element of pedagogical culture rather than an intrusive imposition (Chan & Hu, 2023). Through sequential layering , literature synthesis, structured quantitative surveys, qualitative administrator interviews, targeted pilot deployments with iterative recalibration , the research design sought convergence between formative evidence gathering and summative effectiveness validation across multiple institutional contexts. The combination allows robust causal inference about how specific technological strategies influence both perceived legitimacy of examinations and measurable

integrity outcomes when embedded conscientiously within higher education practice settings (Keo et al., 2024).

4.2. Data Collection Methods

The data collection strategy was shaped to capture nuanced perspectives across multiple stakeholder groups while ensuring that the technological interventions under study could be assessed in terms of both efficacy and user experience. Building on the structured research framework outlined previously in Section 4.1, collection efforts combined survey instruments, platform-generated analytics, direct observation protocols, and archival records review into a coherent multi-modal dataset. Online surveys served as the primary quantitative tool for gathering perceptions from students and instructors exposed to secure examination technologies. Distributed via institutional mailing lists and learning management systems, the questionnaires were anonymized to encourage candid responses. The sampling process involved screening eligibility to target only individuals with recent participation in digitally administered exams employing measures such as biometric logins, online proctoring, or plagiarism detection. Execution of these surveys often leveraged third-party web form providers experienced in large-scale academic polling; their infrastructure permitted rapid deployment and real-time response aggregation while maintaining compliance with privacy regulations (Fujii, 2024). Response formats included Likert scales and categorical ratings to quantify attitudes toward fairness, ease-of-use, and trust variables, as well as open-entry fields for detailed opinion capture. To deepen granularity beyond self-reported data, observational methods were embedded within pilot program deployments. Invigilators operating secure platforms documented technical occurrences such as authentication failures, bandwidth disruptions affecting biometric scans (Keo et al., 2024), or false positives generated by behavioral analysis modules during proctoring (Pillai et al., 2021). These logs were timestamped directly within platform dashboards, allowing cross-comparison against system-generated flags for suspicious activity , for example, attempts at unauthorized website access detected through lockdown browser integration (Shyja et al., 2024). Observers also recorded interview-adjacent notes based on informal conversations with participants immediately after assessment sessions; this provided context on whether anomalies reflected genuine misconduct attempts or environmental factors like household interruptions during remote exams. Another dimension of data collection involved extraction of backend analytics from examination platforms themselves. Advanced systems supply encrypted datasets containing usage metrics such as average time spent per question, frequency of switching between test windows, incidence rates of camera disconnections during proctored sessions, and divergence patterns in randomized item responses across candidate groups (Fink et al., 2023). Some institutions extended this logging with blockchain-based audit trails to ensure immutability of key security event records (Sudaryono et al., 2020). Access to these analytics required administrative clearance given the sensitive nature of identity-linked information; therefore researchers worked closely with IT departments to anonymize entries before integration into analysis pipelines. Complementary qualitative data emerged through semi-structured interviews with academic staff tasked with configuring or overseeing technological safeguards during examinations (Civaner et al., 2022). Sessions were conducted via secure video conferencing platforms where consent protocols assured participants that transcripts would be stored separately from any performance data about their institution's students. Open-ended questioning explored operational challenges such as resource allocation for training programs (Chan & Hu, 2023), coping strategies for disciplinary resistance to surveillance-heavy configurations (Patiño et al., 2023), and subjective judgments regarding trade-offs between strict enforcement and learner comfort. Interview transcripts were later coded thematically using software-assisted analysis tools to highlight recurring patterns across different faculty cohorts. A smaller but vital component of data collection involved indirect assessment artifacts such as course attainment mappings tied to term test performance. By correlating score distributions before and after technological intervention rollout, researchers could observe performance shifts without relying entirely on reported malpractice incidents. This enriched evaluative scope by adding potential indicators of how integrity measures might influence learning outcomes , for instance, whether adaptive question delivery impacted attainment percentages similarly across varying course objectives (CO) in different disciplines (Churi & Rao, 2021). Literature review functioned here not merely as background but as a source dataset in its own right; policy documents outlining institutional implementation models were systematically gathered via academic databases like Scopus and Web of Science using Boolean search strings engineered for thematic precision around "educational intervention," "complex thinking," and "emerging technologies" keywords (Patiño et al., 2023). Data points extracted from these texts helped situate empirical findings within broader theoretical perspectives while also revealing gaps in current adoption trends relevant to technology-mediated integrity assurance. Operational logs from generative AI-enhanced assessments constituted another specialized dataset subset. Participating institutions supplied anonymized interaction histories showing frequency of AI feedback requests by students during writing-heavy exam tasks (Chan & Hu, 2023). Combined with misconduct incidence tracking, this allowed researchers to assess whether AI facilitation altered cheating patterns or introduced unique vulnerabilities requiring secondary countermeasures. Care was taken throughout all collection stages to maintain methodological consistency so that diverse streams , quantitative survey ratings, qualitative interviews, direct observation records, automated platform analytics , could be triangulated effectively during later synthesis phases. Each stream adhered to predefined inclusion criteria excluding cases lacking direct relevance to high-tech exam integrity mechanisms. Where discrepancies arose between machine-generated alerts and human observer accounts during pilots (Wijaya et al., 2024), both versions were preserved for reconciliation analysis aimed at refining detection sensitivity settings prior to full deployment recommendations. This approach ensured that measured impacts on integrity did not emerge purely from one modality's bias but reflected convergent evidence across independent yet interconnected data channels.

5. Results

Analysis of the collected datasets yielded a multi-layered view of the impact of implemented technological interventions on examination integrity. Quantitative survey responses from the 200-student sample, stratified across varying levels of enforcement intensity, showed a consistent association between higher security configurations and decreased self-reported exposure to dishonest practices. In environments where biometric authentication was combined with AI-assisted proctoring, 82% of respondents rated the fairness and deterrence level as either "high" or "very high," while only 9% expressed neutral or negative sentiments toward these measures (Pillai et al., 2021). This contrasted with cohorts subject only to lockdown browsers, where positive perception dropped to 63% and reports of potential circumvention strategies were more frequent. These attitudinal patterns aligned with measured behavioral data extracted from platform analytics: biometric-plus-proctoring groups recorded lower incidence of flagged anomalies per capita than minimal restriction groups (Fink et al., 2023). Raw performance metrics further substantiated these differences. Comparative analysis of course attainment results before and after intervention rollout suggested modest but notable gains in average scores for disciplines integrating adaptive question sets alongside secure access protocols. Variability in attainment narrowed, indicating a reduction in outlier cases potentially linked to misconduct. This pattern was particularly pronounced in STEM-focused assessments featuring embedded simulation tasks; their authenticity made dishonesty technically challenging while also engaging candidates in discipline-relevant scenarios (Churi & Rao, 2021). Humanities courses showed less pronounced score changes, reflecting mixed adoption of interactive formats and persistent debates over surveillance necessity (Patiño et al., 2023). Platform-generated audit logs produced granular insights into detection efficacy. Lockdown browser alerts captured attempts at unauthorized site access in 4.7% of all monitored sessions; almost half of these alerts correlated with simultaneous gaze diversion events flagged by AI modules during live proctoring feeds (Shyja et al., 2024). In hybrid human-machine review systems, concordance between algorithmic flags and reviewer conclusions reached 78%, suggesting room for refinement but supporting the validity of automated classifications when moderated by human judgment (Civaner et al., 2022). Discrepancies often stemmed from environmental noise , such as audio alerts from nearby devices , or benign off-screen glances that triggered false positives under default sensitivity settings. Blockchain-enabled platforms provided immutable evidence trails for all critical exam events including authentication completions, disconnection intervals, and flagged incidents (Cheriguene et al., 2022). While this functionality did not directly influence real-time cheating prevention, it enhanced post-assessment dispute resolution processes by providing tamper-proof timelines accessible to both faculty and students. Institutions employing this ledger system reported faster closure rates on contested cases compared to counterparts using conventional log files. Qualitative interviews with faculty revealed a set of converging themes around operational feasibility. Respondents consistently reported reduced manual workload when platforms consolidated proctoring oversight dashboards with integrated incident summaries. However, they cautioned against overreliance on automation without contextual review, particularly in writing-heavy assignments where plagiarism detection software produced similarity matches inflated by common disciplinary phrasing (Keo et al., 2024). Faculty emphasized the importance of reviewing algorithmic findings manually to prevent unjust penalties for legitimate academic language use. Feedback from students pointed toward greater acceptance in pilots where security measures were paired with orientation sessions explaining their purpose, technical operation, and privacy safeguards (Chan & Hu, 2023). Where such preparatory engagement occurred, privacy concerns were less likely to manifest as resistance during deployment. Conversely, abrupt imposition without adequate explanation resulted in measurable declines in comfort ratings across survey scales, even if detected misconduct rates fell. Network performance data underscored the infrastructural dependencies identified during pilot phases. Bandwidth instability accounted for most authentication delays or temporary session drops in biometric systems, with some occurrences leading to anomalous duplicate logins being registered until reconnection protocols completed error resolution (Keo et al., 2024). Post-pilot adjustments , such as implementing offline verification buffers , effectively eliminated repeat incidents during final evaluation rounds. Notably, generative AI-supported testing environments posed dual outcomes. Interaction histories indicated a decrease in certain plagiarism forms when AI was used to provide individualized feedback during formative assessment stages prior to summative exams (Chan & Hu, 2023). However, interview narratives revealed instances where familiarity with AI response patterns during practice inadvertently informed attempts to game question prompts in actual exams. This suggests that while AI integration can enhance preparation quality, its design must anticipate potential exploitation vectors requiring separate mitigation. Cross-modal triangulation confirmed overarching result trends: environments deploying multi-layered prevention architectures , combining biometric authentication at entry, continuous behavioral monitoring via AI-human hybrid review models, adaptive randomized questioning linked to secure content delivery protocols, and immutable recordkeeping through blockchain , achieved the lowest documented misconduct incidence rates across the study (Sudaryono et al., 2020). Moreover, these configurations maintained or improved user satisfaction indicators relative to baseline scenarios when embedded within transparent communication frameworks and robust infrastructural support systems. Overall outcome synthesis demonstrated that technological strategies are both statistically and experientially effective when operationalized through careful calibration based on empirical feedback loops rather than one-size-fits-all implementation. Successful deployments balanced preventive rigor with usability considerations revealed during pilot testing phases (Wijaya et al., 2024), ensuring that enhancements to exam integrity did not come at disproportionate cost to participant trust or accessibility equity across institutional contexts.

6. Conclusion

The integration of technological strategies into higher education assessment has demonstrated measurable benefits in reducing examination malpractices while maintaining or improving user acceptance. Combining biometric authentication with AI-assisted proctoring and adaptive question delivery creates a layered defense that effectively deters dishonest behaviors. This approach aligns security measures with pedagogical objectives by embedding authentic skill evaluation within exam formats, particularly in STEM disciplines where simulation-based tasks enhance engagement and reduce opportunities for misconduct. The use of blockchain for immutable audit trails further strengthens post-assessment integrity assurance by providing transparent and tamper-resistant records, facilitating fair dispute resolution.

Operational experiences highlight the importance of balancing automated detection with human judgment to avoid false positives and ensure contextual fairness, especially in disciplines with nuanced writing conventions. Equally important is the role of clear communication and preparatory orientation for students and faculty, which mitigates privacy concerns and promotes acceptance of monitoring technologies. Infrastructure readiness, including stable network connectivity and accessible hardware, emerges as a foundational requirement for successful implementation, with pilot testing serving as a critical phase for identifying and addressing technical bottlenecks.

The findings also reveal that technology alone cannot fully address academic integrity challenges; integration with thoughtful assessment design and ethical instruction is necessary to influence student motivation and behavior positively. The nuanced impact of generative AI tools underscores the need for ongoing vigilance and adaptive countermeasures to prevent new forms of malpractice while leveraging AI's potential to support learning. Overall, the evidence supports a comprehensive, context-sensitive approach where technological safeguards operate in harmony with educational practices and institutional policies. This synergy enhances trust in digital examinations and contributes to sustaining the credibility of academic credentials across diverse disciplines and cultural settings. Continued empirical evaluation and iterative refinement remain essential to optimize these systems for fairness, usability, and effectiveness in evolving educational environments.

REFERENCES

[1] Chan, C. K. Y., & Hu, W. (2023). Students' voices on generative AI: Perceptions, benefits, and challenges in higher education. *International Journal of Educational Technology in Higher Education*, *20*(43), 43. https://doi.org/10.1186/s41239-023-00411-8

[2] Cheriguene, A., Kabache, T., Adnane, A., Kerrache, C. A., & Ahmad, F. (2022). On the use of blockchain technology for education during pandemics. *IT Professional*, *24*(2), 52–61. https://doi.org/10.1109/mitp.2021.3066252

[3] Churi, P., & Rao, N. T. (2021). Teaching cyber security course in the classrooms of NMIMS university. *I.J. Modern Education and Computer Science*, *13*(4), 1–15. https://doi.org/10.5815/ijmecs.2021.04.01

[4] Civaner, M. M., Uncu, Y., Bulut, F., Giounous Chalil, E., & Tatli, A. (2022). Artificial intelligence in medical education: A cross-sectional needs assessment. *BMC Medical Education*, *22*, 772. https://doi.org/10.1186/s12909-022-03852-3

[5] Danyluk, P., & Burns, A. (2021). Experiencing the shift: How postsecondary contract and continuing faculty moved to online course delivery. *Brock Education: A Journal of Educational Research and Practice*, *30*(2), 63–78. https://journals.library.brocku.ca/brocked

[6] Fink, A., Spoden, C., & Frey, A. (2023). Determinants of higher education teachers' intention to use technology-based exams. *Education and Information Technologies*, *28*(6), 6485–6513. https://doi.org/10.1007/s10639-022-11435-4

[7] Fujii, A. (2024). Exploring autonomy support and learning preference in higher education: Introducing a flexible and personalized learning environment with technology. *Discover Education Research*, *3*, 26. https://doi.org/10.1007/s44217-024-00111-z

[8] Keo, V., Sam, R., Lan, B., & Rouet, W. (2024). Challenges and opportunities of educational technology integration in cambodian higher education institutions: A literature review. *International Journal of Education, Psychology and Counselling*, *9*(54), 157–176. https://doi.org/10.35631/IJEPC.954013

[9] Moshtari, M., & Safarpour, A. (2024). Challenges and strategies for the internationalization of higher education in low-income east african countries. *Higher Education*, *87*(1), 89–109. https://doi.org/10.1007/s10734-023-00994-1

[10] Oc, Y., Gonsalves, C., & Quamina, L. T. (2025). Generative AI in higher education assessments: Examining risk and tech savviness on student's adoption. *Journal of Marketing Education*, *47*(2), 138–155. https://doi.org/10.1177/02734753241302459

[11] Patiño, A., Ramírez-Montoya, M. S., & Ibarra-Vazquez, G. (2023). Trends and research outcomes of technology-based interventions for complex thinking development in higher education: A review of scientific publications. *Contemporary Educational Technology*, *15*(4), ep447. https://doi.org/10.30935/cedtech/13416

[12] Pillai, K. R., Upadhyaya, P., Prakash, A. V., Ramaprasad, B. S., Mukesh, H. V., & Pai, Y. (2021). End-user satisfaction of technology-enabled assessment in higher education: A coping theory perspective. *Education and Information Technologies*, *26*(4), 3677–3698. https://doi.org/10.1007/s10639-020-10401-2

[13] Shyja, K. G., Mehthab, N., & Shabna, K. V. (2024). Securing the future of education: Quantum encryption and beyond – an examination of cutting-edge security technologies. *International Education & Research Journal*, *10*(1), 113.

[14] Stenalt, M. H., & Mathiasen, H. (2024). Towards teaching-sensitive technology: A hermeneutic analysis of higher education teaching. *International Journal of Educational Technology in Higher Education*, *21*(17), 17. https://doi.org/10.1186/s41239-024-00449-2

[15] Sudaryono, Aini, Q., Lutfiani, N., Hanafi, F., & Rahardja, U. (2020). Application of blockchain technology for iLearning student assessment. *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, *14*(2), 209–218. https://doi.org/10.22146/ijccs.53109

[16] Sum, M., & Oancea, A. (2022). The use of technology in higher education teaching by academics during the COVID-19 emergency remote teaching period: A systematic review. *International Journal of Educational Technology in Higher Education*, *19*, 59. https://doi.org/10.1186/s41239-022-00364-4

[17] Wijaya, I. G. A. S. P., Sasmita, G. M. A., & Pratama, I. P. A. E. (2024). Web application penetration testing on udayana universityś OASE e-learning platform using information system security assessment framework (ISSAF) and open source security testing methodology manual (OSSTMM). *I.J. Information Technology and Computer Science*, *16*(2), 45–56. https://doi.org/10.5815/ijitcs.2024.02.04

[18] Yadav, M. S., & Yadav, M. K. (2023). Implicit impact of english language pedagogical enhancement policies in higher education under the indian NEP 2020: Challenges, curriculum, approaches, opportunities, and implementations. *American Journal of Education and Technology (AJET)*, *1*(4), 1. https://doi.org/10.54536/ajet.v1i4.1117