ASEAN Journal of Educational Research and Technology

Journal homepage: https://ejournal.bumipublikasinusantara.id/index.php/ajert

Technology-driven Prevention of Examination Paper Leaks in High-Stakes Educational Assessment to Support Sustainable Development Goals (SDGs): A Bibliometric and Focused Literature Review

*Vishwas Pendse[1], Jaiprakash Paliwal[2], Manesh Palav[3], Abhay Bora[1], Atul Kumar[4], Srinivasa Rao Kasisomayajula[5], Sagar Nimbalkar[6], Shirish Raibagkar[7]**

[1]Sandip Institute of Technology and Research Centre, Nashik, India
[2]Symiosis Law School, Nagpur and Symbiosis International University, Pune, India
[3]Global Business School and Research Centre, Dr. D. Y. Patil Vidyapeeth, Pune, India
[4]Vikrant University, Gwalior, India
[5]Koneru Lakshmaiah Education Foundation (K L University), Guntur, India
[6]Vidya Pratishthan's Institute of Information Technology, Baramati, India
[7]The Institute of Cost Accountants of India, Kolkata, India
*Correspondence: E-mail: ssrssr696@gmail.com

ABSTRACT

Examination paper leaks threaten educational equity, public trust, and merit-based selection in high-stakes educational assessment. This study examines technology-driven prevention of examination paper leaks to support Sustainable Development Goals (SDGs) through a bibliometric and focused literature review. The review discusses blockchain-based question paper management, artificial intelligence (AI) proctoring, biometric authentication, cryptographic protection, digital watermarking, zero-knowledge proof frameworks, and generative AI-related academic integrity risks. Layered and policy-integrated technological approaches are needed to strengthen secure, fair, accountable, and SDG-oriented assessment systems.

ARTICLE INFO

Article History:
Submitted/Received 20 May 2026
First Revised 16 Aug 2026
Accepted 16 Aug 2026
First Available online 19 Aug 2026
Publication Date 01 Dec 2026

Keywords:
Academic integrity;
Artificial intelligence proctoring;
Biometric authentication;
Blockchain;
Examination paper leak.

1. INTRODUCTION

Examination paper leaks are a serious threat to fairness, public trust, and merit-based selection in high-stakes educational assessment. Such leaks are not limited to one country or one examination system, but occur in different contexts where competitive examinations determine access to limited educational and professional opportunities. Examination malpractice may involve impersonation, insider collusion, center-level misconduct, digital communication, paper theft, and organized fraud networks, showing that paper leakage is both an educational governance and security problem (Okpaka, 2026).

India's National Eligibility cum Entrance Test for Undergraduate admissions provides a highly visible example of this issue. The NEET-UG question paper leak attracted national attention because the examination functions as a major gateway to undergraduate medical education and involves a very large candidate population. Media reports, official inquiries, and policy discussions highlighted procedural vulnerabilities, organized malpractice, and the need for stronger examination security mechanisms. Examination paper leaks weaken students' trust in fairness, institutional credibility, and merit-based selection (Joshi *et al.*, 2025; Ranjan *et al.*, 2024).

Technology has increasingly been proposed for improving education (Al Husaeni *et al.*, 2022). Indeed, it can be used as a preventive mechanism for examination paper leaks and related malpractice. These technologies can operate across the examination lifecycle, including question paper creation, encryption, storage, distribution, candidate authentication, examination monitoring, result processing, and credential verification. The major technological domains include blockchain-based question paper management, artificial intelligence (AI) proctoring, biometric authentication, cryptographic protection, digital watermarking, zero-knowledge proof frameworks, and generative AI-related academic integrity risks (Bhabad, 2023; Roseela and Godhavari, 2020).

Each technology contributes differently to examination security. Blockchain can strengthen tamper-evident chain-of-custody records, AI can support proctoring and cheating detection, biometrics can reduce impersonation, cryptography can protect examination content, watermarking can trace leaked papers, and zero-knowledge proof systems can support privacy-preserving credential verification. However, these technologies also raise concerns about scalability, privacy, bias, fairness, transparency, and institutional readiness, especially in large-scale high-stakes assessment systems (Zhu and Cao, 2021).

The prevention of examination paper leaks is also relevant to Sustainable Development Goals (SDGs). Secure and fair assessment systems support SDG 4 by protecting quality education and equal opportunity. Technology-based prevention mechanisms support SDG 9 by encouraging innovation, digital infrastructure, and secure educational systems. Transparent examination governance supports SDG 16 by strengthening institutional trust, fairness, accountability, and public confidence. Therefore, examination security should be understood not only as a technical issue but also as part of sustainable educational governance.

This study used a bibliometric and focused literature review approach to examine technology-driven prevention of examination paper leaks in high-stakes educational assessment. The bibliometric component provides an overview of research development in examination security, while the focused literature review synthesizes technological prevention mechanisms across major domains. This approach is appropriate because the

topic connects education, information security, AI, biometrics, blockchain, cryptography, public policy, and academic integrity (Levy and Ellis, 2006; Webster and Watson, 2002; Xiao and Watson, 2019).

The novelty of this study lies in its integration of bibliometric evidence, technology-focused literature synthesis, and SDG-oriented educational assessment governance. Previous studies often discuss blockchain, AI proctoring, biometrics, watermarking, credential verification, or academic integrity separately. This study brings these domains together to highlight the need for layered, policy-integrated, and SDG-aligned examination security. Therefore, this study aims to examine how technology can contribute to preventing examination paper leaks and related assessment malpractice while identifying research trends, limitations, risks, and future directions for secure and sustainable assessment systems.

2. METHOD

This study used a bibliometric and focused literature review approach to examine technology-driven prevention of examination paper leaks in high-stakes educational assessment. The bibliometric component was used to describe the development of examination security research, while the focused literature review was used to synthesize key technological prevention mechanisms and their relevance to assessment governance. The bibliometric data were obtained from Scopus using the query TITLE-ABS-KEY (exam AND security). The search identified 1,266 documents published from 1981 to 2026. The dataset included 743 sources, 3,324 authors, 30,332 references, and various document types, including articles, conference papers, book chapters, reviews, and books. These data were used to describe publication trends, research growth, and the multidisciplinary scope of examination security studies. The focused literature review was guided by the question: how can technology contribute to the prevention of examination paper leaks and related assessment malpractice in high-stakes educational assessment? Relevant literature was organized into major technological domains, including blockchain-based question paper management, AI proctoring and cheating detection, biometric authentication, cryptographic protection, digital watermarking, zero-knowledge proof frameworks, and generative AI-related academic integrity risks. Peer-reviewed studies were used as the main evidence for the thematic synthesis. Contextual information related to the NEET-UG crisis was used only to frame the problem, while academic literature was used to support the analysis. The synthesis examined technological contributions, implementation challenges, limitations, and policy implications. The review also considered the relevance of examination security to SDG 4, SDG 9, and SDG 16.

3. RESULTS AND DISCUSSION

3.1. Bibliometric Overview of Examination Security Research

Examination security has developed into a multidisciplinary research area involving education, information security, AI, biometrics, blockchain, cryptography, and academic integrity. The main bibliometric information generated from the Scopus dataset is presented in **Figure 1**. The dataset covers publications from 1981 to 2026, indicating that examination security has been discussed for several decades but has become more visible with the expansion of digital assessment, online proctoring, biometric identity verification, blockchain-based credential systems, and concerns about technology-enabled academic misconduct.

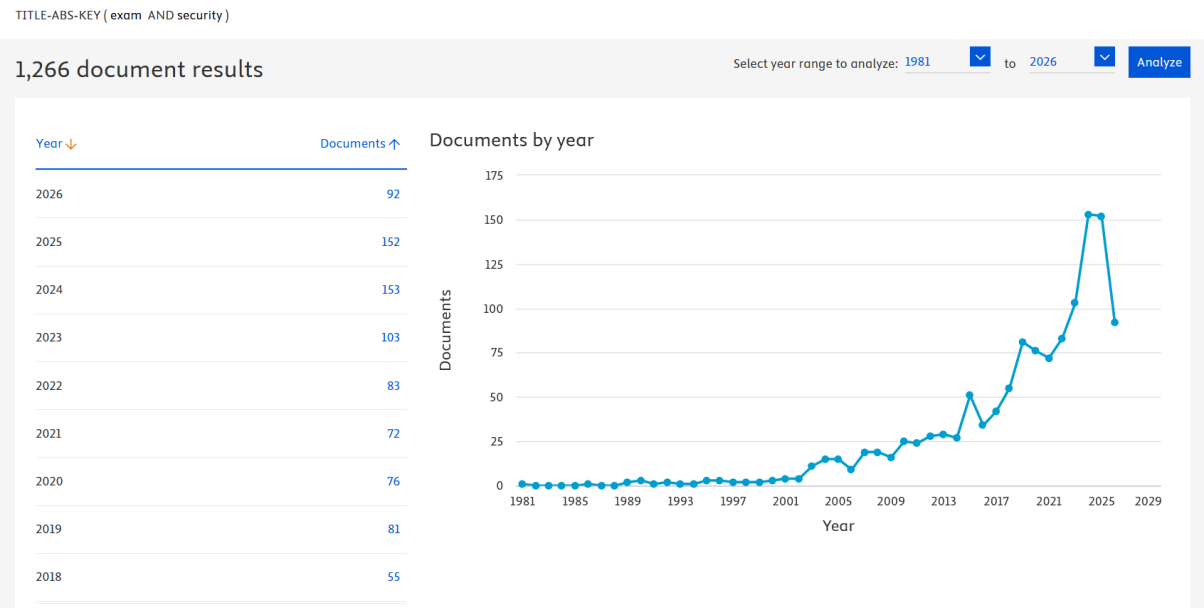

Figure 1. Scopus bibliometric dataset. Data were retrieved in August 2026.

3.2. Blockchain Technology for Secure Question Paper Management

Blockchain technology can strengthen examination security by creating tamper-evident records of question paper access, transfer, and modification. This function is important because question papers may be compromised during creation, printing, storage, transportation, digital distribution, or center-level handling. Blockchain-based systems reduce this risk by recording each access event in a distributed ledger, making unauthorized changes easier to detect and responsibility easier to trace (Bhabad, 2023).

Table 1 summarizes the main roles of blockchain in secure question paper management. Blockchain is useful not only for protecting the paper, but also for improving access control, accountability, and investigation after a suspected leak. Blockchain can support secure question paper management through encrypted storage, controlled access, distributed storage, and auditable access records. These features are relevant for high-stakes examinations because they can reduce dependence on physical paper transport, manual custody procedures, and centralized storage systems (Bhabad, 2023; Nagabushan *et al.*, 2025; Zhu and Cao, 2021).

Blockchain also supports transparency after a suspected leak. In conventional paper-based systems, it may be difficult to reconstruct who accessed the paper, when access occurred, and where the breach happened. A blockchain ledger can provide a time-stamped access history, making investigation more reliable and strengthening public confidence in institutional accountability (Nagabushan *et al.*, 2025). However, blockchain should not be treated as a complete solution. Many proposed systems are still prototypes, simulations, or small-scale pilots, so their effectiveness in national examinations with millions of candidates remains uncertain. Blockchain also requires infrastructure, interoperability standards, trained personnel, secure key management, and regulatory support. Therefore, blockchain is better understood as one layer in a broader examination security system that also includes cryptography, biometric authentication, AI proctoring, watermarking, and institutional governance (Zhu and Cao, 2021).

Table 1. Blockchain functions in secure question paper management.

BLOCKCHAIN FUNCTION	APPLICATION IN EXAMINATION SECURITY	MAIN BENEFIT	LIMITATION
Tamper-evident ledger	Records access, transfer, and modification of question papers	Improves traceability and accountability	Requires reliable digital infrastructure
Encrypted paper storage	Stores encrypted papers or hashed references on the ledger	Reduces unauthorized early access	Depends on secure key management
Smart contract access	Releases access keys only at the scheduled examination time	Limits premature paper exposure	Requires correct system configuration
Role-based permission	Gives different access rights to officials, centers, and authorized users	Reduces dependence on manual custody	Needs clear governance and user training
Distributed storage	Reduces reliance on a single central server	Minimizes single-point failure	May be difficult to scale nationally
Integration with biometrics	Links secure paper access with identity verification	Connects paper security and identity security	Requires strong privacy safeguards

3.3. AI and Machine Learning for Proctoring and Cheating Detection

AI and machine learning (ML) strengthen examination security by supporting candidate monitoring, abnormal behavior detection, object identification, facial movement analysis, eye-tracking, and incident review. In relation to paper leak prevention, AI does not directly protect question papers before the examination, but it reduces opportunities to use leaked materials, unauthorized devices, or external assistance during examination administration.

Table 2 summarizes the main functions of AI and ML in proctoring and cheating detection. AI can support both online and physical examination settings, but its use must be balanced with fairness, privacy, and human oversight. AI-based proctoring can operate through video monitoring, screen recording, audio analysis, browser activity tracking, and multimodal data integration. These systems can function as passive monitoring tools that flag suspicious behavior for later review or as active systems that intervene when serious irregularities are detected (Kosuri *et al.*, 2026).

AI-based cheating detection is also relevant in physical examination halls. Computer vision can help identify prohibited objects such as mobile phones, additional papers, and communication devices, while real-time object detection can support invigilators in environments with different lighting conditions and camera angles (Roa'a *et al.*, 2022; Alotaibi *et al.*, 2022).

AI can also improve investigation quality by identifying specific moments of suspicious behavior instead of classifying an entire examination session as problematic. This function is important in high-stakes assessment because disciplinary decisions require reviewable evidence, not only general risk scores (Liu *et al.*, 2024). However, AI proctoring has important limitations. Its accuracy depends on data quality, camera quality, internet connectivity, lighting, and candidate device capability. These requirements may create unequal conditions for candidates in low-resource or rural contexts (Duhaim *et al.*, 2022; Arianti *et al.*, 2023).

Table 2. AI and ML functions in proctoring and cheating detection.

AI/ML FUNCTION	APPLICATION IN EXAMINATION SECURITY	MAIN BENEFIT	LIMITATION
Behavior monitoring	Detects suspicious movements, repeated gaze changes, or unusual actions	Supports real-time or post-exam review	May produce false flags
Video-based proctoring	Monitors candidates through camera-based systems	Reduces dependence on manual invigilation	Depends on camera quality and lighting
Screen and browser tracking	Records screen activity, tab switching, and browser behavior	Detects unauthorized digital access	Raises privacy concerns
Object detection	Identifies mobile phones, notes, papers, or other prohibited items	Supports physical and online invigilation	Accuracy may vary by environment
Multimodal monitoring	Combines video, audio, screen, and browser data	Provides richer evidence for review	Requires stable devices and connectivity
Incident localization	Identifies specific moments of suspicious behavior	Supports fairer investigation	Needs human validation

AI-based cheating detection also raises concerns about fairness, privacy, and bias. Remote proctoring systems may affect candidates differently when face detection or behavior monitoring performs unevenly across demographic groups. Therefore, AI should be used as a decision-support tool with independent auditing, human review, clear appeal mechanisms, and transparent rules for identifying suspicious behavior (Liu *et al.*, 2024).

3.4. Biometric Authentication in Examination Security

Biometric authentication strengthens examination security by reducing candidate impersonation and unauthorized access. Conventional identity checks using photographs, identity cards, signatures, or manual invigilation can be weakened by human error, document substitution, photograph manipulation, or organized impersonation. Biometric systems address this risk by linking examination access to unique physiological or behavioral characteristics, such as fingerprints, facial features, iris patterns, or multimodal identity profiles.

Table 3 summarizes the main biometric authentication functions in examination security. Biometrics can support candidate verification, material control, and impersonation prevention, but their implementation requires strong privacy protection and fair verification procedures. Biometric authentication can support both candidate identity verification and examination material control. Biometric and RFID-based systems can connect candidate authentication with paper custody, while biometric protection can reduce unauthorized access and impersonation risks in examination settings (Roseela and Godhavari, 2020).

Facial recognition is widely relevant because it can be used at examination entry points, physical examination halls, and online proctoring platforms. Deep learning-based face recognition and AI-supported facial biometric systems can help verify whether the registered candidate is the person taking the examination (Fadlullah *et al.*, 2026; Mamun, 2023).

Table 3. Biometric authentication functions in examination security.

BIOMETRIC FUNCTION	APPLICATION IN EXAMINATION SECURITY	MAIN BENEFIT	LIMITATION
Fingerprint recognition	Verifies candidate identity before or during examination	Reduces impersonation	May fail due to damaged fingerprints or sensor issues
Facial recognition	Confirms candidate identity at entry points, exam halls, or online platforms	Enables real-time identity verification	Sensitive to lighting, camera quality, and demographic bias
RFID and biometric integration	Links candidate identity with examination material control	Connects identity security and paper custody	Requires integrated infrastructure
Multimodal biometrics	Combines fingerprint, face, iris, or other biometric signals	Improves verification reliability	Requires more data and stronger governance
Thermal-visible recognition	Uses visible and thermal facial data for authentication	Reduces spoofing risk	May be costly and technically complex
Fallback verification	Uses human review when biometric verification fails	Protects legitimate candidates from wrongful rejection	Requires clear operational procedures

Multimodal biometric authentication can improve reliability because single-modality systems may be affected by spoofing, poor image quality, damaged fingerprints, lighting problems, or environmental variation. Combining multiple biometric signals can strengthen verification, while thermal-visible face recognition can reduce dependence on visible-light conditions and make spoofing more difficult (Ammour *et al.*, 2023; Kowalski *et al.*, 2022). However, biometric authentication also creates serious governance concerns. Biometric data are sensitive personal data, so their use in educational assessment requires clear rules on consent, storage, access, retention, deletion, and secondary use. Responsible AI principles and ethical safeguards are especially important when biometric systems are used in large-scale educational assessment because biometric data involve sensitive identity information and possible verification bias (Ammour *et al.*, 2023; Kowalski *et al.*, 2022).

Bias and wrongful rejection are also important risks. Biometric systems may perform differently across age groups, gender, skin tone, disability status, and environmental conditions. Therefore, biometric authentication should include human review, fallback verification, transparent appeal mechanisms, and privacy protection. These safeguards are needed to prevent legitimate candidates from being unfairly excluded from examinations.

3.5. Cryptography, Digital Watermarking, and Secure Document Distribution

Cryptography and digital watermarking protect examination papers before, during, and after distribution. Cryptography secures the content of the question paper. Thus, intercepted files cannot be read without the correct key. Digital watermarking adds traceable information to the document, making it possible to identify the source of a leak if the paper is copied, printed, photographed, or shared without permission.

Table 4 summarizes the main functions of cryptography, digital watermarking, and secure document distribution. These technologies protect examination content and support leak tracing, but their effectiveness depends on secure key management, controlled access, and institutional procedures.

Table 4. Cryptography, digital watermarking, and secure document distribution in examination security.

SECURITY FUNCTION	APPLICATION IN EXAMINATION SECURITY	MAIN BENEFIT	LIMITATION
Encryption	Protects question papers during storage and transmission	Prevents unauthorized reading before access	Depends on secure key management
Multi-factor authentication	Controls access to examination materials	Reduces risk from stolen passwords	Requires user compliance and system reliability
IP address restriction	Limits access to authorized locations or devices	Reduces unauthorized remote access	May be difficult in flexible or distributed settings
Visible watermarking	Places visible marks on question paper copies	Discourages casual copying and sharing	May be removed or cropped
Invisible robust watermarking	Embeds hidden marks that survive printing, scanning, or compression	Supports forensic leak tracing	Requires technical expertise
Invisible fragile watermarking	Detects modification or tampering in documents	Supports evidence of document alteration	May be sensitive to normal file processing
Image encryption and hybrid watermarking	Protects scanned, photographed, or image-based question papers	Useful for papers circulated as images	May increase technical complexity

Secure document distribution requires more than ordinary file storage. Examination papers may pass through item writing, review, formatting, digital storage, printing, transportation, and center-level handling before reaching candidates. Each stage creates possible opportunities for unauthorized access. Thus, encryption, controlled access, and location-based restrictions are needed to reduce exposure (Shewale *et al.*, 2023; Kumar and Rohil, 2024).

Digital watermarking complements encryption because encrypted files may still be copied or photographed after authorized access. Watermarking allows each paper copy to carry visible or hidden identifying information, helping institutions trace the source of a leak after the paper has been distributed or opened.

Different watermarking techniques serve different purposes. Visible watermarks discourage casual copying, invisible robust watermarks support leak tracing after printing or scanning, and invisible fragile watermarks help detect document modification. A combination of robust and fragile watermarking is useful because examination systems need both traceability and tamper evidence (Shedole and Santhi, 2025).

Cryptography and watermarking are also relevant for question papers circulated as photographs, scans, or image-based files. Image encryption and hybrid-domain watermarking can strengthen protection against cropping, compression, scanning, and image manipulation (Mahalakshmi and Nagarajan, 2025; Ye *et al.*, 2025). However, these technologies do not work effectively without governance. Encryption can fail if keys are shared too early or handled by untrained personnel, while watermarking cannot prevent the first leak and only supports tracing after exposure. Therefore, cryptography and digital watermarking should be combined with controlled access, blockchain audit logs, biometric verification, and strict institutional procedures.

3.6. Zero-Knowledge Proof and Credential Verification

Zero-knowledge proof supports examination security by enabling privacy-preserving verification of academic records, candidate identity, and credentials. This technology allows one party to prove that a statement is valid without revealing the underlying data. In educational assessment, a qualification, registration status, or examination record can be verified without exposing unnecessary personal or academic information.

Table 5 summarizes the main functions of zero-knowledge proof in examination and credential security. Zero-knowledge proof is most relevant in the post-examination stage, especially for result processing, academic record verification, identity management, and cross-border credential recognition.

Table 5. Zero-knowledge proof functions in examination and credential security.

ZKP function	Application in examination security	Main benefit	Limitation
Privacy-preserving verification	Verifies academic records without revealing full data	Protects personal and academic privacy	Requires technical expertise
Credential authentication	Confirms the validity of certificates or qualifications	Reduces credential fraud	Depends on trusted digital infrastructure
Blockchain-based record verification	Links academic records with tamper-resistant verification systems	Improves trust and auditability	May require interoperability standards
Cross-border credential verification	Supports verification for study, employment, or licensing across countries	Helps international recognition	Requires institutional and legal alignment
Digital identity management	Verifies candidate eligibility or identity claims with limited data exposure	Reduces unnecessary data sharing	Needs strong governance and user control
Framework selection	Uses ZK-SNARKs, ZK-STARKs, Bulletproofs, or other models	Allows flexible system design	Involves trade-offs in speed, transparency, and computation

Zero-knowledge proof extends examination security beyond the test administration stage. High-stakes assessment also involves result processing, credential issuance, record sharing, and qualification verification. If academic records can be altered, forged, or misrepresented after the examination, the integrity of the assessment system remains vulnerable.

Different zero-knowledge proof frameworks involve trade-offs in proof generation time, verification speed, transparency, and computational requirements. These trade-offs are important because educational systems must be usable by institutions, candidates, employers, and credential evaluators, not only by technical specialists (Moya *et al.*, 2025; Rageshnithin *et al.*, 2025).

Zero-knowledge proofs can also support blockchain-based academic record verification. This approach allows a verifier to confirm that a candidate holds a valid qualification without accessing the complete academic record. It is relevant for employment, professional licensing, international study, and cross-border recognition (Moya *et al.*, 2025; Rageshnithin *et al.*, 2025).

In addition, zero-knowledge proofs can support digital identity management and candidate eligibility verification. This function can reduce unnecessary exposure of sensitive personal data during registration, identity checking, and institutional verification processes. However, zero-knowledge proof remains technically complex. Its use requires appropriate infrastructure, user-friendly interfaces, institutional trust, technical capacity, and governance support. Therefore, it should be viewed as a promising tool for secure credential verification and privacy protection, but not as a standalone solution for preventing paper leaks during examination administration.

3.7. Generative AI and Academic Integrity Risks

Generative AI creates new challenges for examination security because it can produce answers, explanations, essays, code, summaries, and problem-solving steps within seconds. In the context of examination paper leaks, generative AI increases both the speed and scale of malpractice because leaked questions can be rapidly processed into model answers and shared through digital communication channels. Therefore, paper leak prevention must address not only paper protection, but also the risk of AI-assisted exploitation after leaked materials enter circulation.

Table 6 summarizes the main generative AI-related risks in examination security. Generative AI affects examination integrity through answer generation, content amplification, detection limitations, assessment design, policy enforcement, and equity concerns. Generative AI expands examination security from paper protection to digital misuse prevention, assessment redesign, and academic integrity governance. Traditional detection-based approaches are insufficient because AI-generated answers may be difficult to identify reliably, especially when candidates edit, paraphrase, translate, or combine AI outputs with human writing (Yusuf *et al.*, 2024).

Table 6. Generative AI-related risks and responses in examination security.

GENERATIVE AI ISSUE	RISK FOR EXAMINATION SECURITY	POSSIBLE RESPONSE	LIMITATION
AI-generated answers	Leaked papers can be converted into model answers quickly	Strengthen paper protection and controlled access	Hard to control after public circulation
Rapid content amplification	Leaked questions and answers can spread through digital platforms	Use secure distribution and monitoring procedures	Digital sharing can occur instantly
Detection difficulty	AI-generated content may be edited, paraphrased, or translated	Combine detection with human review	Detection tools may produce false results
Assessment design risk	Recall-based questions are easier to exploit using AI	Use reasoning-based, randomized, or applied questions	Requires item bank redesign
Policy uncertainty	AI-assisted cheating may be difficult to define and sanction	Develop clear AI-use and misconduct policies	Requires consistent enforcement
Equity concern	Candidates with better AI access may gain unfair advantage	Protect equal opportunity through secure and fair assessment	Digital inequality may remain

Generative AI also requires changes in assessment design. High-stakes examinations should reduce overdependence on easily reproducible questions and strengthen randomisation, secure item banks, applied problem-solving, reasoning-based tasks, and professional judgement assessment. These strategies are important because secure technology must be supported by assessment formats that are less vulnerable to AI-assisted answer generation (Evangelista, 2025).

Policy governance is also necessary because generative AI-related misconduct cannot be managed only through technical detection. Examination authorities need clear rules on AI-assisted cheating, unauthorized tools, candidate responsibilities, invigilator procedures, evidence review, sanctions, and appeal mechanisms (Zia and Khan, 2023).

Generative AI also creates an equity risk. Candidates with better access to digital tools, paid AI platforms, private tutoring, or organized preparation networks may gain unfair advantages if examination papers are leaked. Therefore, generative AI strengthens the need for secure question paper management and fair assessment systems that protect equal opportunity in line with SDG 4.

3.8. Comparative Synthesis of Technology-Driven Examination Security

Each technology contributes to a different layer of examination security. Blockchain supports chain-of-custody records, AI supports monitoring and cheating detection, biometrics verify candidate identity, cryptography protects question paper content, watermarking supports leak tracing, zero-knowledge proof enables privacy-preserving verification, and generative AI governance addresses emerging academic integrity risks. Therefore, these technologies should be understood as complementary components of a layered examination security system.

Table 7 summarizes the main security function, lifecycle stage, strength, and limitation of each technology domain discussed in this review. No single technology can prevent all forms of paper leakage or examination malpractice. Each technology addresses a specific vulnerability, so effective prevention requires integration across the pre-examination, examination administration, and post-examination stages. At the pre-examination stage, security should focus on secure item development, cryptographic protection, blockchain-based access logging, and watermarking. During examination administration, biometric authentication and AI-assisted monitoring can reduce impersonation, unauthorized assistance, and suspicious behavior. At the post-examination stage, watermarking, audit logs, secure result processing, and zero-knowledge proof systems can support investigation, credential verification, and privacy protection.

Technology-driven prevention must be context-sensitive. Different examination systems require different levels of security depending on assessment scale, delivery mode, candidate diversity, infrastructure readiness, legal requirements, and public accountability needs. Therefore, technology should be selected and combined based on risk level rather than adopted as a single universal solution.

Table 7. Comparative synthesis of technology-driven examination security domains.

TECHNOLOGY DOMAIN	MAIN SECURITY FUNCTION	EXAMINATION LIFECYCLE STAGE	MAIN STRENGTH	MAIN LIMITATION
Blockchain	Tamper-evident access and custody record	Paper creation, storage, and distribution	Strong auditability and transparency	Scalability, infrastructure, and implementation readiness
AI and ML	Cheating detection and behavior monitoring	Examination administration	Real-time or semi-automated risk detection	Bias, privacy concerns, and false flags
Biometric authentication	Candidate identity verification	Registration, entry, and examination administration	Reduces impersonation and identity fraud	Sensitive data governance and demographic bias
Cryptography and digital watermarking	Secure paper protection and leak tracing	Paper storage, distribution, and post-leak investigation	Protects content and supports forensic traceability	Key management and post-decryption risks
Zero-knowledge proof	Privacy-preserving credential verification	Result processing and credential verification	Verifies authenticity while protecting privacy	Technical complexity and limited large-scale adoption
Generative AI governance	Prevention of AI-assisted cheating and misuse	Assessment design and administration	Responds to emerging academic integrity risks	Detection limits and policy uncertainty

3.9. SDG-Oriented Implications of Examination Security Technologies

Technology-driven examination security is closely related to educational equity, institutional trust, and sustainable governance. Examination paper leaks can weaken merit-based selection, reduce public confidence, and create unequal opportunities for candidates. Therefore, preventing paper leaks supports SDG 4, SDG 9, and SDG 16.

Table 8 presents the relationship between major examination security technologies and their relevance to the SDGs. Each technology domain contributes to secure, fair, innovative, and accountable assessment systems. SDG 4 is supported when examination systems protect fairness, equal opportunity, and credible assessment outcomes. SDG 9 is supported through secure digital infrastructure, innovation, and interoperable technologies for assessment protection. SDG 16 is supported through transparency, accountability, auditability, and stronger public trust in educational institutions. However, technology must be implemented responsibly. Examination security systems should not be evaluated only by technical performance, such as detection accuracy, encryption strength, or authentication speed. They should also be assessed through fairness, accessibility, privacy protection, transparency, and candidate rights. Therefore, SDG-oriented examination security requires both technological safeguards and strong institutional governance.

Table 8. SDG-oriented implications of examination security technologies.

TECHNOLOGY DOMAIN	SDG RELEVANCE	MAIN IMPLICATION FOR SUSTAINABLE ASSESSMENT
Blockchain	9 and 16	Strengthens secure digital infrastructure, auditability, transparency, and institutional accountability
AI and ML	4, 9, and 16	Supports cheating detection and monitoring, but requires fairness, transparency, and human oversight
Biometric authentication	4 and 16	Protects equal opportunity by reducing impersonation, but requires strong privacy and data governance
Cryptography and digital watermarking	9 and 16	Protects examination content, supports leak tracing, and strengthens secure institutional processes
Zero-knowledge proof	9 and 16	Enables privacy-preserving credential verification and reduces unnecessary exposure of personal data
Generative AI governance	4 and 16	Addresses AI-assisted cheating risks and supports ethical, fair, and accountable assessment practices

3.10. Gaps and Future Research Directions

Technology-driven prevention of examination paper leaks has developed across several promising domains, but several research and implementation gaps remain.

(i) Large-scale deployment. Many studies still present blockchain, biometric authentication, AI proctoring, watermarking, and zero-knowledge proof as prototypes, models, or conceptual frameworks. Future research should examine how these technologies perform in national high-stakes examinations involving large candidate populations, diverse geographical contexts, and complex administrative structures.

(ii) System integration. Many technologies are studied separately, although examination security requires a layered system. Future research should develop integrated models that connect pre-examination security, examination administration, and post-examination verification. These models should explain how different technologies interact, how responsibilities are distributed, and how security failures can be investigated.

(iii) Fairness, privacy, and bias. AI proctoring and biometric authentication can strengthen monitoring and identity verification, but they may also create risks of demographic bias, false accusations, surveillance anxiety, and unequal treatment. Future studies should include independent audits, candidate experience, accessibility analysis, human review, and appeal procedures.

(iv) Governance and regulation. Technology cannot prevent paper leaks if institutional procedures remain weak. Future research should examine how technical systems are supported by policy, legal frameworks, procurement standards, data protection rules, staff training, and accountability mechanisms. Public communication after security failures should also be studied because institutional trust depends on transparency and responsiveness.

(v) Generative AI risks. Examination systems are still adapting to AI-assisted cheating, AI-generated answers, and the rapid digital circulation of leaked materials. Future studies should examine secure item banks, randomized question delivery, AI-aware examination design, performance-based assessment, and clear policies for AI-related misconduct.

Examination security should be studied as a socio-technical system. Technology, policy, human behavior, institutional capacity, and candidate rights need to be analyzed together. Future research should move beyond single-tool solutions and develop evidence-based, scalable, ethical, and SDG-aligned models for secure high-stakes educational assessment.

4. CONCLUSION

Examination paper leaks require layered and technology-supported prevention. Examination security is a multidisciplinary and growing research area. Blockchain, AI, biometric authentication, cryptography, digital watermarking, zero-knowledge proof, and generative AI governance each contribute to different stages of the examination lifecycle. However, no single technology is sufficient. Effective prevention requires integration between secure infrastructure, institutional policy, human oversight, privacy protection, and accountability. Strengthening examination security also supports SDG 4, SDG 9, and SDG 16 by promoting fair, innovative, and trustworthy assessment systems.

5. ACKNOWLEDGMENTS

We thank Yogesh Wagh, Pune, India, for his help with language editing of the manuscript.

6. AUTHORS' NOTE

The authors declare that there is no conflict of interest regarding the publication of this article. The authors confirmed that the paper is free from plagiarism.

7. REFERENCES

Al Husaeni, D. F., Al Husaeni, D. N., Ragadhita, R., Bilad, M. R., Al-Obaidi, A. S. M., Abduh, A., and Nandiyanto, A. B. D. (2022). How language and technology can improve student learning quality in engineering? Definition, factors for enhancing students comprehension, and computational bibliometric analysis. *International Journal of Language Education*, *6*(4), 445-476.

Alotaibi, M. F., Omri, M., Abdel-Khalek, S., Khalil, E., and Mansour, R. F. (2022). Computational intelligence-based harmony search algorithm for real-time object detection and tracking in video surveillance systems. *Mathematics*, *10*(5), 733.

Ammour, N., Bazi, Y., and Alajlan, N. (2023). Multimodal approach for enhancing biometric authentication. *Journal of Imaging*, *9*(9), 168.

Arianti, A. S., Putra, M. A. S., and Nugraha, E. (2023). Designing an online examination system with object detection-based proctoring. *Computing and Education Technology Journal*, *3*(2), 1-12.

Bhabad, V. M. (2023). Block-chain framework for educational domain and its benefits. *International Journal of Advanced Research in Science, Communication and Technology*, 3(16), 586-593.

Duhaim, A. M., Al-Mamory, S., and Mahdi, M. S. (2022). Cheating detection in online exams during COVID-19 pandemic using data mining techniques. *Webology, 19*(1), 341-366.

Evangelista, E. D. L. (2025). Ensuring academic integrity in the age of ChatGPT: Rethinking exam design, assessment strategies, and ethical AI policies in higher education. *Contemporary Educational Technology*, *17*(1), ep559.

Fadlullah, S. Y., Hidayah, A. N., Saputra, Y., Negara, S. P. P. S., and Putra, S. (2026). SisCek: A deep learning-based face recognition system for real-time exam impersonation detection. *Jurnal Penelitian Sains Teknologi, 2*(2), 149-164.

Joshi, D., Chauhan, N., Gor, D., Shahu, A., and Telariya, B. (2025). A study of views from students about national competitive exam paper leaks in India. *International Journal for Multidisciplinary Research, 7*(3), 1-12.

Kosuri, S. T., Kumar, H., and Siri, V. (2026). A review on applications of artificial intelligence in online proctoring systems. *International Scientific Journal of Engineering and Management*, 5(4), 1-15.

Kowalski, M., Grudzien, A., and Mierzejewski, K. (2022). Thermal-visible face recognition based on CNN features and triple triplet configuration. *Sensors, 22*(13), 5012.

Kumar, N., and Rohil, H. (2024). Cheating detection and prevention techniques in online system for university examination. *International Research Journal on Advanced Engineering Hub, 2*, 2412-2428.

Levy, Y., and Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science: The International Journal of an Emerging Transdiscipline, 9*, 181-212.

Liu, Y., Ren, J., Xu, J., Bai, X., Kaur, R., and Xia, F. (2024). Multiple instance learning for cheating detection and localization in online examinations. *IEEE Transactions on Cognitive and Developmental Systems*, *16*(4), 1315-1326.

Mahalakshmi, K., and Nagarajan, S. (2025). Comprehensive review and analysis of image encryption techniques. *IEEE Access*, *13*, 109783-109813.

Mamun, M. A. (2023). Authentication system for exam halls using face biometrics by artificial intelligence. *Open Access Journal of Data Science and Artificial Intelligence, 1*(1), 20.

Moya, J. A. B., Ayoade, J., and Uddin, M. A. (2025). A zero-knowledge proof-enabled blockchain-based academic record verification system. *Sensors, 25*(11), 3450.

Nagabushan, P., Swayam, V., Megha, A. J., Bhattacharya, P., and Udupa, S. (2025). Decentralized ecosystem for secure question paper distribution. *International Research Journal on Advanced Engineering and Management, 3*(12):3430-3434.

Okpaka, C. (2026). Biometric fraud, syndicated collusion, and the governance of technology-enabled examination malpractice. *International Journal of Recent Trends in Multidisciplinary Research, 6*(3), 328-339.

Rageshnithin, A., Vanmathi, C., and Mangayarkarasi, R. (2025). Cross-border candidate credential verification using ZKP and blockchain Ethereum and Polygon perspectives: a scalable solution for authentic global corporate interviews. *Frontiers in Blockchain*, *8*, 1669666.

Ranjan, P., Kain, S., and Kumar, R. (2024). Call for reforms in the NEET-UG examination (National Eligibility cum Entrance Test-undergraduate): Addressing human resources in health for India, the world's most populous country. *Journal of Family Medicine and Primary Care*, *13*(12), 5453-5458.

Roa'a, M., Aljazaery, I. A., and Alaidi, A. H. M. (2022). Automated cheating detection based on video surveillance in the examination classes. *iJIM*, *16*(8), 125.

Roseela, J., and Godhavari, T. (2020). Biometric and RFID based authentication system for exam paper leakages detection. *Indonesian Journal of Electrical Engineering and Computer Science, 20*(3), 1271-1277.

Shedole, S. M., and Santhi, V. (2025). A comprehensive study on digital watermarking for security threats and research directions. *International Journal of Data Informatics and Intelligent Computing*, *4*(1), 54-72.

Shewale, C., Kadam, S., Shelke, P., Patil, R., Dedgaonkar, S., Banubakode, A. (2023). Multi factor authentication and IP address restriction based question paper delivery system. *International Journal on Recent and Innovation Trends in Computing and Communication, 11*(10), 390-396.

Webster, J., and Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly, 26*(2), xiii-xxiii.

Xiao, Y., and Watson, M. (2019). Guidance on conducting a systematic literature review. *Journal of Planning Education and Research, 39*(1), 93-112.

Ye, C., Tan, S., Wang, J., Shi, L., Zuo, Q., and Feng, W. (2025). Social image security with encryption and watermarking in hybrid domains. *Entropy, 27*(3), 276.

Yusuf, A., Pervin, N., and Roman-Gonzalez, M. (2024). Generative AI and the future of higher education: A threat to academic integrity? *International Journal of Educational Technology in Higher Education, 21*(1), 21.

Zhu, X., and Cao, C. (2021). Secure online examination with biometric authentication and blockchain-based framework. *Mathematical Problems in Engineering, 2021*, 5058780.

Zia, A., and Khan, M. M. (2023). Addressing contract cheating in Pakistani higher education: Strategies for upholding academic integrity. *Journal of Professional Research in Social Sciences*, *10*(2), 84-98.