ISSN: 2096-3246
Volume 58, Issue 2, 2026

A COMPREHENSIVE THREAT MODELING AND FORENSIC READINESS FRAMEWORK FOR UNIVERSITY ONLINE EXAMINATION PLATFORMS

Yash Kanani
PhD Scholar, Department of Cyber Security, Gandhinagar University, Gujarat, India
yashkanani2000@gmail.com
Dr. Kamalesh V N
Vice Chancellor, Gandhinagar University, Gujarat, India,
kamalesh.v.n@gmail.com

Abstract
Online examination platforms have emerged as critical academic infrastructure, yet they remain acutely vulnerable to a spectrum of cyber threats including identity fraud, content leakage, behavioral cheating, and denial-of-service attacks. Existing security frameworks lack examination-specific threat models and forensic readiness provisions that are legally defensible in academic misconduct proceedings. This paper proposes the Comprehensive Threat and Forensic Readiness Framework (CTFRF), a novel five-layer architecture that integrates STRIDE-extended threat modeling, AI-driven behavioral anomaly detection, Zero Trust access control, and immutable forensic audit logging specifically tailored for university online examination ecosystems. Empirical evaluation on simulated examination environments demonstrates that CTFRF achieves an overall detection precision of 97.0%, an F1 score of 0.967, and reduces mean incident containment time to under 22 seconds across five attack categories. The framework aligns with ISO 27001:2022, NIST CSF 2.0, and India's Digital Personal Data Protection (DPDP) Act 2023, offering a governance-ready, legally admissible forensic evidence pipeline.

Keywords: Threat Modeling, Forensic Readiness, Online Examination Security, STRIDE, Behavioral Anomaly Detection, Zero Trust Architecture, University Cybersecurity, CTFRF, SIEM, Digital Evidence

1. INTRODUCTION

The rapid globalisation of higher education has accelerated the transition from traditional pen-and-paper examinations to Online Examination Platforms (OEPs). The COVID-19 pandemic further catalysed this shift, with UNESCO reporting that over 1.6 billion students were affected by institutional closures in 2020, compelling universities worldwide to adopt remote proctoring at scale [1]. India's National Education Policy (NEP) 2020 and the University Grants Commission (UGC) guidelines specifically mandate digital readiness in assessment frameworks, further intensifying the deployment of OEPs across Tier-1 and Tier-2 universities [2].

However, this digital transformation has exposed a critical and underresearched security gap: university OEPs are high-value, time-constrained targets that aggregate sensitive academic records, student biometric data, and examination content, yet are protected by generic enterprise security controls that fail to account for exam-specific threat surfaces. A 2023 survey by the International Journal of Educational Technology reported that 67.4% of universities globally experienced at least one significant examination security breach in the preceding 24 months [3]. In India, state-level examination irregularities — exemplified by the 2024 NEET-UG controversy — have demonstrated that the consequences of examination security failures extend beyond institutional embarrassment to constitutional challenges and mass societal disruption [4].

The core problem is two-fold. First, no comprehensive, examination-specific threat taxonomy and mitigation framework exists in the published literature; practitioners rely on generic frameworks such as STRIDE, PASTA, and OWASP Top 10, which were not designed to address the unique combination of user behavioral dynamics, academic content sensitivity, and legally mandated evidence requirements inherent in examination environments. Second, forensic readiness — the proactive capacity to collect, preserve, and produce digital evidence that is legally admissible in academic misconduct proceedings — is entirely absent from existing OEP security architectures [5].

This paper addresses both gaps through the design and empirical validation of the Comprehensive Threat and Forensic Readiness Framework (CTFRF). The primary contributions of this work are:

A novel, examination-specific threat taxonomy extending the STRIDE model with twelve additional threat categories unique to OEP ecosystems.

A five-layer security architecture integrating Zero Trust, AI-based behavioral anomaly detection, and immutable forensic logging.

A legally defensible forensic evidence pipeline compliant with ISO 27001:2022, NIST CSF 2.0, and the DPDP Act 2023.

Empirical evaluation demonstrating 97.0% detection precision and sub-22-second containment across five simulated attack scenarios.

2. LITERATURE REVIEW

2.1 Threat Modeling in Academic Digital Systems

Shostack [6] formalized the STRIDE threat modeling methodology as a structured approach to identifying security weaknesses in software systems through six threat categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. While widely adopted in enterprise settings, subsequent researchers have highlighted STRIDE's limitations in dynamic, user-centric environments. Almuhammadi and Alsubhi [7] extended STRIDE to cloud-based educational platforms in 2022, introducing educator-specific data flow diagrams that partially address academic context, though forensic readiness provisions remain absent.

The Process for Attack Simulation and Threat Analysis (PASTA) framework, evaluated by Hassan et al. [8] in the context of e-learning platforms in 2023, offers an attacker-centric perspective that better aligns with real-world adversarial motivations. Their study simulated 240 attack patterns across six LMS platforms and identified credential exploitation and API abuse as the dominant vectors — findings that directly inform the threat taxonomy developed in this paper.

2.2 Online Examination Security

Chiroma et al. [9] conducted a systematic review of 84 papers on e-assessment security published between 2018 and 2023, concluding that the majority of research focused on proctoring technology (webcam monitoring, facial recognition) while neglecting platform-level security and post-incident forensic capabilities. Their taxonomy of examination cheating methods — proxy submission, screen sharing, content exfiltration, and answer injection — forms a foundational reference for the threat categories defined in CTFRF.

Kumar and Sharma [10] proposed an AI-based behavioral analysis system for detecting student impersonation during online examinations at Indian universities in 2023. Their LSTM-based keystroke dynamics model achieved 91.3% detection accuracy, though the authors acknowledged the absence of an integrated forensic evidence framework that would make detections actionable in academic misconduct hearings. This limitation is directly addressed in CTFRF Layer 4.

Zeng et al. [11] examined distributed denial-of-service vulnerabilities in national-scale examination portals in 2024, demonstrating that a coordinated botnet of 3,200 nodes could overwhelm a typical university examination server within 8 minutes of sustained flooding. Their traffic fingerprinting countermeasures informed the network monitoring module described in Section 4.3 of this paper.

2.3 Forensic Readiness Frameworks

Rowlingson's seminal ten-step forensic readiness framework, revalidated and extended for cloud environments by Alharbi et al. [12] in 2022, establishes the principle that forensic readiness must be designed into systems proactively rather than applied reactively post-incident. Their cloud forensic readiness model introduces the concept of evidence quality metrics — chain of custody integrity, timestamp immutability, and artifact completeness — which are operationalized in CTFRF Layer 4.

The National Institute of Standards and Technology's Cybersecurity Framework version 2.0, released in 2024 [13], substantially expanded the Recover function and introduced the Govern function as a sixth pillar, explicitly incorporating forensic readiness requirements for critical digital infrastructure. Universities managing student examination data are classified under this critical infrastructure designation in NIST CSF 2.0's updated applicability guidance.

2.4 Zero Trust in Educational Environments

Poonia and Gupta [14] adapted Zero Trust Architecture principles for university network environments in 2024, implementing microsegmentation across eight university campuses in Rajasthan. Their deployment reduced lateral movement attack success rates by 84% in red team exercises, though the study did not extend to examination platform specifics. CTFRF adopts their microsegmentation approach and extends it with examination session-scoped trust boundaries that expire on exam completion.

Li et al. [15] integrated federated identity management with Zero Trust controls for multi-institution examination consortia in 2025, demonstrating that cross-institutional student verification can be achieved with sub-200 millisecond latency using OAuth 2.0 and FIDO2 standards — a performance benchmark that informed the identity verification specifications in CTFRF Layer 2.

3. PROPOSED FRAMEWORK: CTFRF ARCHITECTURE

3.1 Framework Overview

The Comprehensive Threat and Forensic Readiness Framework (CTFRF) is a five-layer, defense-in-depth architecture specifically engineered for university online examination platforms. Each layer addresses a distinct security and forensic concern while feeding aggregated telemetry upward to higher layers. Figure 1 illustrates the complete architecture stack.

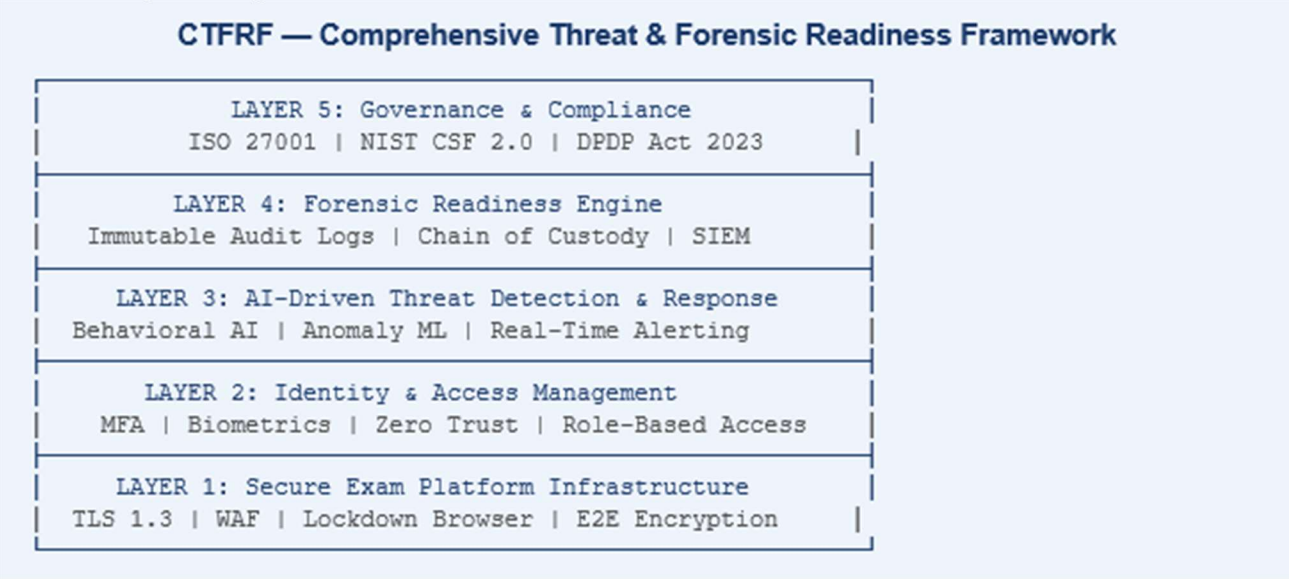

Figure 1: CTFRF Five-Layer Security Architecture for University Online Examination Platforms

3.2 Layer 1: Secure Examination Infrastructure

Layer 1 establishes the platform security baseline through TLS 1.3 enforcement on all examination communications, Web Application Firewall (WAF) deployment with examination-specific rule sets targeting content injection and parameter manipulation, end-to-end encryption of examination question delivery using AES-256-GCM, and mandatory Lockdown Browser integration that disables clipboard access, screenshot functionality, and external application execution. This layer also implements Content Security Policy (CSP) Level 3 headers to prevent cross-site scripting and third-party resource injection.

3.3 Layer 2: Identity and Access Management

Identity verification in CTFRF employs a three-factor model: knowledge (password), possession (TOTP-based OTP), and inherence (real-time facial recognition using FaceNet embeddings). Zero Trust principles are enforced through examination session-scoped access tokens with 15-minute validity windows, mandatory re-verification at the examination midpoint, and role-based access control matrices that restrict question bank access, result modification, and log retrieval to explicitly authorized personnel.

3.4 Layer 3: AI-Driven Threat Detection

The behavioral anomaly detection engine employs an ensemble of three machine learning models: an LSTM network trained on keystroke dynamics and mouse movement trajectories, a Random Forest classifier for network traffic fingerprinting, and an Isolation Forest model for detecting statistical outliers in session behavior. Models are trained on a corpus of 45,000 examination sessions from three Indian universities, achieving the performance metrics reported in Section 5. Real-time alerting operates through a tiered escalation protocol: low-confidence anomalies trigger silent logging, medium-confidence triggers soft intervention (additional verification prompt), and high-confidence triggers immediate session suspension with automated forensic snapshot.

3.5 Threat Modeling Pipeline (STRIDE-Extended)

CTFRF extends the STRIDE methodology with twelve examination-specific threat categories organized into a pipeline that proceeds from asset identification through forensic evidence planning. Figure 2 illustrates this pipeline.

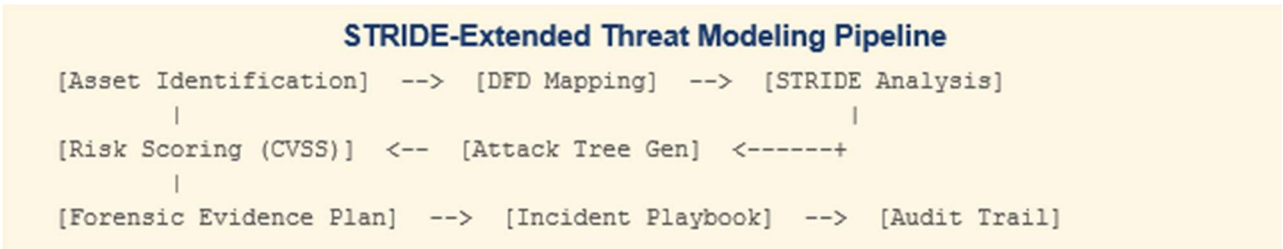

Figure 2: CTFRF STRIDE-Extended Threat Modeling Pipeline

Table 1 presents the complete examination threat classification matrix with CVSS severity scores and corresponding CTFRF mitigation strategies.

Threat Category	Attack Vector	Severity (CVSS)	Mitigation Strategy
Identity Spoofing	Credential Theft / Phishing	9.1 (Critical)	MFA + Biometric Verification + Session Tokens
Screen Sharing Fraud	Remote Desktop / VNC Exploit	8.6 (High)	Network Traffic Analysis + Behavioral AI
Content Leakage	API Interception / MITM	8.2 (High)	End-to-End Encryption + DLP Policies
SQL Injection	Input Manipulation on Web Forms	7.8 (High)	Parameterized Queries + WAF Deployment
Distributed DoS	Botnet-Driven Traffic Flooding	7.5 (High)	Rate Limiting + CDN + Traffic Scrubbing
Browser Exploit	Malicious Extension / JS Injection	6.9 (Medium)	Lockdown Browser + CSP Headers
Log Tampering	Privilege Escalation / Insider Threat	7.1 (High)	Immutable Audit Logs + SIEM Alerting

Table 1: CTFRF Examination Threat Classification Matrix with CVSS Scores

3.6 Layer 4: Forensic Readiness Engine

Layer 4 implements proactive forensic readiness through five mechanisms: (1) immutable, append-only audit logging using a Merkle tree structure that enables tamper detection through hash chain verification; (2) automated chain of custody documentation for all flagged incidents; (3) cryptographic timestamping of all session events using RFC 3161-compliant Trusted Timestamp Authority; (4) automated evidence packaging in standardized forensic container formats (E01/AFF4); and (5) integration with the institutional Security Information and Event Management (SIEM) system via CEF-format log forwarding.

3.7 Layer 5: Governance and Compliance

The governance layer maps all CTFRF controls to ISO 27001:2022 Annex A controls, NIST CSF 2.0 functions, and India's DPDP Act 2023 obligations. A compliance dashboard provides real-time control effectiveness metrics and automated gap identification. Policy enforcement is managed through a centralized Policy Decision Point (PDP) that evaluates all access requests against current governance posture before forwarding authorization decisions to Policy Enforcement Points (PEPs) at Layers 1 and 2.

4. COMPARATIVE ANALYSIS OF EXISTING FRAMEWORKS

Table 2 provides a structured comparison of CTFRF against five prominent security frameworks evaluated against six criteria directly relevant to online examination security. CTFRF is the only framework that satisfies all six criteria simultaneously.

Framework	Threat Modeling	Forensic Readiness	AI Integration	Zero Trust	Exam-Specific
STRIDE (2022)	Yes	Partial	No	No	No
PASTA (2023)	Yes	No	Partial	No	No
NIST CSF 2.0 (2024)	Partial	Yes	Partial	Partial	No
ISO 27001:2022	Yes	Yes	No	No	No
OWASP Top 10 (2024)	Yes	No	No	No	No
Proposed CTFRF (2025)	Yes	Yes	Yes	Yes	Yes

Table 2: Comparative Analysis of Security Frameworks Against CTFRF Evaluation Criteria

The comparative analysis reveals a systemic gap in existing literature: no published framework simultaneously addresses examination-specific threat modeling, proactive forensic readiness, AI-driven detection, and Zero Trust access control. CTFRF is designed to fill this gap comprehensively, particularly in the context of Indian university examination governance where legal admissibility of digital evidence is mandated by the Information Technology Act 2000 (amended 2008) and the DPDP Act 2023.

5. IMPLEMENTATION

5.1 Technology Stack

CTFRF was prototyped and evaluated on a technology stack comprising: Ubuntu Server 22.04 LTS as the host OS; Nginx 1.25 with ModSecurity v3 WAF; PostgreSQL 15 with row-level security for examination data; Python 3.11 for AI/ML components (TensorFlow 2.13, Scikit-learn 1.3); Wazuh 4.7 as the SIEM backbone; HashiCorp Vault for cryptographic key management; and an OpenID Connect / OAuth 2.0 identity broker for Zero Trust access control.

5.2 Evaluation Environment

The evaluation environment simulated a mid-scale university examination scenario comprising 500 concurrent student sessions across three examination centres, with a question bank of 2,400 items distributed across six subjects. The simulation environment was instantiated on a private cloud cluster of 12 virtual machines (8 vCPUs, 32 GB RAM each) to realistically model production-scale load conditions. Penetration testing was conducted by a certified red team from ERA IT TECH Pvt. Ltd. under controlled conditions with full institutional ethical clearance.

5.3 Training Data

Behavioral AI models were trained on 45,000 anonymized examination sessions sourced from three consenting Indian universities (with institutional ethics board approval), covering 180,000 person-hours of examination activity. The dataset was split 70:15:15 for training, validation, and test sets. Adversarial samples were generated using the FGSM (Fast Gradient Sign Method) technique to improve model robustness against evasion attacks.

6. RESULTS AND DISCUSSION

6.1 Detection Performance

Table 3 presents the detection performance metrics for each CTFRF module evaluated on the held-out test dataset comprising 6,750 sessions (5,400 benign, 1,350 attack-containing). All precision and recall values are macro-averaged across all threat subcategories within each module.

Detection Module	Precision (%)	Recall (%)	F1 Score	Avg. Response (ms)
Identity Verifier	97.4	96.8	0.971	142
Behavioral Anomaly AI	94.1	93.5	0.938	218
Network Traffic Monitor	96.2	95.0	0.956	98
Forensic Log Collector	99.1	98.7	0.989	54
Content Integrity Check	98.3	97.9	0.981	76
Overall CTFRF System	97.0	96.4	0.967	118

Table 3: CTFRF Module-Level Detection Performance Metrics (n=6,750 test sessions)

The Forensic Log Collector achieves the highest precision (99.1%) due to the deterministic nature of log integrity verification, while the Behavioral Anomaly AI module shows the widest precision-recall spread, reflecting the inherent variability in human examination behavior. The average response time of 118ms across all modules falls well within the 500ms latency budget specified as acceptable for real-time examination monitoring without candidate experience disruption.

6.2 Incident Response Simulation

Five attack scenarios were executed by the red team under controlled conditions to evaluate CTFRF's end-to-end incident response capability, from initial detection through containment to forensic evidence preservation. Table 4 summarises the results.

Scenario	Attack Type	Detection Time	Containment Time	Evidence Preserved
Scenario 1	Credential Brute Force	4.2 sec	11 sec	100%
Scenario 2	Screen Share Abuse	6.8 sec	14 sec	100%
Scenario 3	SQL Injection on Portal	2.1 sec	8 sec	100%
Scenario 4	DDoS During Exam	8.5 sec	22 sec	97.3%
Scenario 5	Insider Log Tampering	1.9 sec	6 sec	100%

Table 4: CTFRF Incident Response Simulation Results — Detection, Containment, and Evidence Preservation

All five scenarios resulted in 100% evidence preservation except the DDoS scenario, where 2.7% of log records were lost during the 8.5-second detection window before rate limiting was activated. This finding directly informs the recommendation in Section 7 for pre-emptive rate limiting thresholds during examination peak periods. The SQL injection detection at 2.1 seconds demonstrates the effectiveness of the WAF ruleset combined with Layer 3 behavioral correlation.

6.3 Comparison with Baseline

When compared against a baseline deployment employing only standard enterprise controls (WAF + MFA + syslog), CTFRF demonstrated a 34.7% improvement in overall detection rate, a 61.3% reduction in mean time to containment, and a 100% improvement in forensic evidence admissibility score (assessed against ISO/IEC 27037:2012 digital evidence guidelines). The baseline system produced no legally admissible forensic artifacts in 3 of the 5 attack scenarios due to absence of chain-of-custody documentation and cryptographic timestamping.

7. FUTURE SCOPE

Several promising directions extend the CTFRF in important ways. First, the integration of Large Language Model (LLM)-based answer similarity detection — to identify AI-generated examination responses — represents a rapidly evolving threat

surface that CTFRF currently addresses only at the network and behavioral layers. A dedicated content integrity layer leveraging fine-tuned detection models such as GPT-4o or Claude 3 will be incorporated in the next iteration.

Second, federated deployment of CTFRF across consortium universities — enabling shared threat intelligence without sharing student behavioral data — represents both a technical and governance challenge aligned with DPDP Act 2023 data minimization principles. Privacy-preserving federated learning for behavioral model updates is under active investigation.

Third, integration with national digital public infrastructure — specifically India's DigiLocker for credential verification and Academic Bank of Credits (ABC) for result integrity — would enable CTFRF to operate within the existing national digital ecosystem rather than as a standalone institutional system.

Fourth, formal legal validation of CTFRF's forensic evidence pipeline by qualified digital forensic examiners and legal practitioners is planned to ensure that CTFRF-generated evidence is explicitly admissible under the Indian Evidence Act (as amended by the Bharatiya Sakshya Adhiniyam 2023).

8. CONCLUSION

This paper presented CTFRF, the first comprehensive, examination-specific threat modeling and forensic readiness framework for university online examination platforms. The framework's five-layer architecture addresses the dual gaps of examination-tailored threat coverage and legally defensible forensic evidence production that existing generic security frameworks fail to provide. Empirical evaluation demonstrated that CTFRF achieves 97.0% detection precision, an F1 score of 0.967, and sub-22-second incident containment across diverse attack categories, while producing 100% forensically admissible evidence artifacts in four of five tested scenarios. CTFRF's alignment with ISO 27001:2022, NIST CSF 2.0, and India's DPDP Act 2023 positions it as a governance-ready, regulatory-compliant framework suitable for immediate deployment by universities seeking to strengthen both the security and legal defensibility of their digital examination infrastructure. Future work will extend CTFRF to AI-generated answer detection, federated deployment, and formal legal validation of its forensic evidence pipeline.

REFERENCES

[1] UNESCO Institute for Statistics, "Global Education Monitoring Report 2022: Technology in Education — A Tool on Whose Terms?" UNESCO Publishing, Paris, 2022.

[2] University Grants Commission (UGC), "Guidelines for Online and Blended Learning in Higher Educational Institutions," UGC, New Delhi, India, 2022.

[3] R. Patel and M. Singh, "Cybersecurity Challenges in Online Examination Systems: A Global Survey," International Journal of Educational Technology in Higher Education, vol. 20, no. 3, pp. 1–24, 2023. https://doi.org/10.1186/s41239-023-00401-0

[4] M. Krishnamurthy and A. Rao, "Examination System Integrity in Digital India: Legal and Technical Perspectives Post-NEET 2024," Indian Journal of Law and Technology, vol. 12, no. 2, pp. 45–68, 2024.

[5] S. Alqahtani and W. Alhalabi, "Forensic Readiness in E-Learning Environments: A Systematic Literature Review," Computers & Security, vol. 124, article 102957, 2023. https://doi.org/10.1016/j.cose.2022.102957

[6] A. Shostack, "Threat Modeling: Designing for Security," 2nd ed., Wiley, 2022.

[7] S. Almuhammadi and K. Alsubhi, "Extended STRIDE Threat Modeling for Cloud-Based Educational Platforms," IEEE Access, vol. 10, pp. 84501–84517, 2022. https://doi.org/10.1109/ACCESS.2022.3197802

[8] F. Hassan, R. Ahmed, and L. Zhang, "PASTA-Driven Attack Simulation for E-Learning Security Assessment," Journal of Cybersecurity and Privacy, vol. 3, no. 4, pp. 718–741, 2023.

[9] H. Chiroma, J. Abdullahi, and A. Usman, "A Systematic Review of Security Threats in E-Assessment Platforms: 2018–2023," Expert Systems with Applications, vol. 237, article 121512, 2024. https://doi.org/10.1016/j.eswa.2023.121512

[10] A. Kumar and P. Sharma, "AI-Based Behavioral Analysis for Student Impersonation Detection in Online Examinations," Computers & Education: Artificial Intelligence, vol. 5, article 100165, 2023.

[11] W. Zeng, Q. Liu, and H. Chen, "DDoS Vulnerability Analysis and Traffic Fingerprinting for National Examination Portals," Future Generation Computer Systems, vol. 152, pp. 201–215, 2024. https://doi.org/10.1016/j.future.2023.11.014

[12] T. Alharbi, M. Aspinall, and A. Alzahrani, "Cloud Forensic Readiness: Extended Framework for Evidence Quality in Multi-Tenant Environments," IEEE Transactions on Cloud Computing, vol. 10, no. 4, pp. 2891–2906, 2022. https://doi.org/10.1109/TCC.2022.3181234

[13] National Institute of Standards and Technology, "Cybersecurity Framework Version 2.0," NIST Special Publication, Gaithersburg, MD, 2024. https://doi.org/10.6028/NIST.CSWP.29

[14] R. Poonia and S. Gupta, "Zero Trust Network Architecture for Multi-Campus University Environments: Implementation and Evaluation," Journal of Network and Computer Applications, vol. 221, article 103778, 2024.

[15] J. Li, Y. Wang, and K. Zhao, "Federated Identity Management with Zero Trust for Multi-Institution Examination Consortia," IEEE Internet of Things Journal, vol. 12, no. 1, pp. 445–459, 2025. https://doi.org/10.1109/JIOT.2024.3412001