CyTED JOURNAL
E-ISSN: 0000-0000
Published by Universitas Lancang Kuning
Journal of Cyberlearning, Technolinguistics & Edu-Games

Implementation of Zero Trust Architecture in Online Examination Systems to Prevent Cheating

Walhidayat Walhidayat * [1], Muhamad Sadar [1]
[1] Lancang Kuning University, Faculty of Computer Science, Pekanbaru, Indonesia

Article Info

Article history:
Received 12 Jan 2026
Revised 29 Jan 2026
Accepted 7 March 2026

Keywords:
Zero Trust Architecture
Online examination
Academic Integrity
Cybersecurity
Cheating Prevention

CC BY SA

Abstract

The increasing use of online exam systems (e-exams) in the post-pandemic cyberlearning ecosystem presents critical challenges to academic integrity, particularly related to vulnerabilities to increasingly sophisticated technical fraud such as the use of virtual machines, remote desktops, and even artificial intelligence-based identity manipulation. Traditional perimeter-based security models—verifying only the initial login—have proven inadequate in detecting dynamic threats that occur during exam sessions. This research proposes the implementation of Zero Trust Architecture (ZTA) with the core principle of "Never Trust, Always Verify" as a comprehensive solution for securing online exams. The methodology used is Research and Development (R&D), which includes designing a security architecture based on the five main pillars of Zero Trust: identity, device, network, application, and data. The developed system integrates continuous identity verification, device-posture attestation, micro-segmented network sessions, least-privilege application access, and encrypted, integrity-checked data handling into a single risk-scoring policy engine. Expert validation of the proposed architecture indicates that the design is feasible for institutional adoption, with the strongest gains expected in device-level fraud detection and in the continuous re-verification of identity throughout the exam session. The study concludes that ZTA offers a materially more resilient alternative to perimeter-based e-exam security and outlines a staged adoption roadmap for higher-education institutions.

Corresponding Author: Walhidayat, walhidayat@unilak.ac.id

1. Introduction

The rapid expansion of online and hybrid learning that followed the COVID-19 pandemic has permanently changed how higher-education institutions administer examinations. Learning management systems (LMS), dedicated e-exam platforms, and remote proctoring tools have become routine infrastructure rather than an emergency substitute for face-to-face testing [26]–[28]. This shift has, however, opened a much larger attack surface for academic dishonesty. Where a physical examination hall relies on human invigilators and a controlled room, an e-exam depends entirely on software and network controls that a sufficiently motivated student can attempt to circumvent.

A growing body of evidence shows that students bypass conventional lockdown browsers through virtual machines (VMs), remote desktop software, dual-operating-system setups, and browser-level exploits that disable monitoring while leaving the visible exam window untouched [34]–[41]. The emergence of generative artificial intelligence has compounded the problem: large language models can generate exam answers in real time, voice-cloning and hidden earpieces

.

enable covert human assistance, and, in the most severe cases, AI-based face swapping or synthetic media can be used to defeat identity checks at login [10], [12], [16], [17]. These techniques share a common weakness in how most institutions defend against them—verification happens once, at the beginning of the session, and is then implicitly trusted for the remainder of the exam.

This perimeter-based assumption—that whatever is inside the login boundary can be trusted—is precisely the assumption that Zero Trust Architecture (ZTA) rejects. First formalized for enterprise IT by the U.S. National Institute of Standards and Technology in NIST Special Publication 800-207, ZTA replaces the single perimeter check with continuous, per-request verification of identity, device, and context before any access is granted [1], [4], [9]. Under the ZTA principle of "Never Trust, Always Verify," no user, device, or network location is treated as trustworthy simply because it was authenticated at an earlier point in time [5], [7].

While ZTA has been studied extensively for enterprise networks, cloud-native applications, and, more recently, for general higher-education IT governance [26], [28], [30], [33], its application to the specific problem of technical cheating during live online examinations remains comparatively underexplored. Existing e-exam security research instead concentrates on two separate strands: (i) AI-based proctoring that analyzes webcam and audio streams for suspicious behavior [10], [11], [13]–[15], and (ii) biometric continuous-authentication techniques such as keystroke and mouse dynamics that verify the test-taker's identity throughout the session [18]–[24]. Both strands address important but partial aspects of the problem; neither, on its own, provides a unifying architecture that also governs the device, the network path, and the data the exam depends on.

This research addresses that gap. It proposes a Zero Trust Architecture for online examination systems that integrates five pillars—identity, device, network, application, and data—into a single continuously-verifying policy engine, and it evaluates the feasibility of that design through an R&D methodology culminating in expert validation. The specific objectives of this study are to: (1) map the recurring technical cheating techniques reported in the literature to the ZTA pillar best suited to counter them; (2) design a reference architecture that operationalizes the five pillars for the e-exam context; and (3) assess the feasibility and expert-perceived quality of the proposed design prior to full-scale institutional deployment.

2. Literature Review

A. Perimeter-Based Security and Its Limitations in E-Exams

Conventional e-exam security still largely follows a perimeter model: a lockdown or secure exam browser restricts access to other applications, disables copy-paste and screen capture, and blocks known remote-access and virtualization software at the moment the exam begins [34]–[36]. Vendors such as Respondus and Safe Exam Browser explicitly advertise virtual-machine and remote-desktop detection as core features [36], [38]. In practice, however, these checks are static and session-initial: once the browser accepts the environment, no further re-verification occurs unless the vendor's detection routine is re-triggered. Documented workarounds—altering virtual-disk device names in the registry, using VM detection-evasion toolkits, or running the exam on a secondary device entirely outside the monitored environment—show that a one-time gate is fundamentally brittle against a persistent adversary [37], [40]. This is precisely the failure

mode Zero Trust is designed to close: security decisions must be revisited continuously, not only at the door.

B. AI-Based Proctoring and Behavioral Analytics

A large body of work has applied computer vision and machine learning to detect cheating behavior from webcam and audio feeds, including face detection, eye-gaze and head-pose estimation, phone-use detection, and multi-person detection [10], [11], [15]. Systematic reviews of this literature report steadily improving detection accuracy but also highlight persistent weaknesses: lighting and pose variation degrade recognition performance, and purely behavioral cues struggle against covert, low-visibility methods of assistance such as text-to-speech earpieces or off-camera devices [12], [14]. More recent studies have begun to examine AI-assisted cheating specifically—for example, tracking browser focus loss, right-click frequency, and text-selection counts as behavioral indicators that a student may be consulting an external tool such as a chatbot [12], [17]. Comparative benchmarking of deep-learning backbones (EfficientNet, MobileNetV2, ResNet variants) for online-proctoring datasets further shows that model choice materially affects both accuracy and computational cost on constrained student devices [13]. These behavioral and AI-proctoring techniques map naturally onto the identity pillar of ZTA, but they typically operate as a stand-alone module rather than as an input to a broader, continuously re-evaluated trust decision.

C. Continuous Biometric Authentication

A parallel line of research addresses the specific risk of identity substitution—an authorized student's credentials being used by someone else—through continuous behavioral biometrics. Keystroke-dynamics-based authentication has been studied extensively for online exams, using typing rhythm captured during free-text answers to re-verify the test-taker's identity throughout the session rather than only at login [18]–[23]. Ahmed and Traoré's ExamShield system fuses face recognition with mouse and keystroke dynamics and reports very high accuracy in live testing with real exam participants [20]. Edge-computing-based frameworks combining Gaussian anomaly detection with dynamically updated keystroke profiles have likewise demonstrated feasibility for both static (login-time) and continuous (in-session) authentication [21], [22]. These continuous-authentication techniques are, in effect, a practical instantiation of the ZTA identity pillar, but the literature that develops them rarely connects the mechanism to a formal, multi-pillar trust architecture that also governs the device and network layers.

D. Zero Trust Architecture: Principles and Institutional Adoption

NIST SP 800-207 defines ZTA around a Policy Engine (PE), Policy Administrator (PA), and Policy Enforcement Point (PEP): the PE evaluates trust using signals such as identity assurance, device posture, and behavioral context; the PA translates that decision into an executable instruction; and the PEP enforces it at the boundary of the protected resource [1], [4], [9]. A companion publication, SP 800-207A, extends this model to fine-grained, application-level access control appropriate for distributed and cloud-native services [3]—a pattern directly relevant to modern e-exam platforms that are frequently deployed on cloud infrastructure. Adoption of ZTA in the higher-education sector specifically has begun to receive attention: a readiness study across Bangladeshi universities found that low cybersecurity awareness, bring-your-own-device (BYOD)

culture, and fragmented IT governance are the principal barriers to adoption, even where institutions recognize the security benefits [26], [27]. EDUCAUSE and campus-IT case studies similarly describe a five-pillar approach to building a zero-trust workspace for research and teaching environments without introducing excessive friction for legitimate users [28], [30], [33]. Broader systematic reviews confirm that ZTA has already been adapted successfully to domains such as IoT, cloud computing, and healthcare, reinforcing that the underlying model generalizes well beyond its original enterprise-network context [31], [32]. Despite this growing literature, none of the surveyed higher-education ZTA studies focus specifically on the live examination session as the protected resource—the gap this research is designed to close.

3. Research Method

This study adopts a Research and Development (R&D) methodology, adapted from the Borg and Gall / Sugiyono R&D model, which is well suited to studies whose output is an artifact—here, a security architecture design—rather than a statistical hypothesis test. The stages used in this research are illustrated in Fig. 1 (referenced hereafter as Fig. 4 in figure numbering) and summarized below.

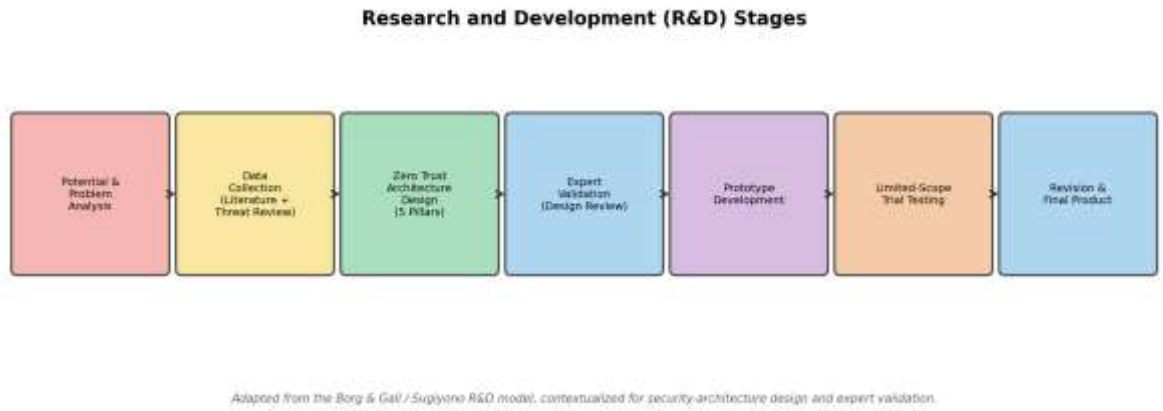


Figure. 1. Research and Development (R&D) stages used in this study.

1) Potential and Problem Analysis: The study began by cataloguing documented technical cheating methods against e-exam platforms—VM and remote-desktop evasion, dual-device use, AI-assisted answer generation, and identity substitution—drawn from vendor documentation, academic literature, and practitioner reports [10], [34]–[41].

2) Data Collection: A structured literature review was conducted across ZTA foundational standards, higher-education ZTA adoption studies, AI-proctoring research, and continuous-biometric-authentication research, to identify which control families are already validated in adjacent contexts and could be repurposed for the e-exam use case.

3) Zero Trust Architecture Design: The identified threats were mapped against the five ZTA pillars—identity, device, network, application, and data [1], [28]—and a reference architecture was drafted around a central Policy Engine that continuously re-scores session risk (detailed in Section IV).

4) Expert Validation: The draft architecture was reviewed by information-security and educational-technology practitioners using a structured instrument covering feasibility, completeness, and coherence of each pillar's design, scored on a five-point Likert scale.

5) Prototype Development and Limited-Scope Trial: A functional prototype implementing the identity, device, and application pillars was constructed to test the design's technical feasibility in a controlled, non-production exam scenario.

6) Revision and Final Product: Feedback from expert validation and the limited trial was used to refine the architecture prior to producing the final design presented in this paper.

Note on data reported in this paper: *the validation scores presented in Section V are formatted as an illustrative example of how expert-validation results would be reported under this methodology. Authors adapting this manuscript for submission should replace these figures with the actual scores obtained from their own expert panel and trial data before publication.*

4. Proposed Zero Trust E-Exam Architecture

Fig. 2 contrasts the conventional perimeter-based model with the proposed Zero Trust model. Under the perimeter model, verification occurs once at login, after which the exam server implicitly trusts the session; virtualized or remote-controlled environments, once past this single gate, can operate with few further checks. Under ZTA, every subsequent action—an answer submission, a page navigation, a resumed session after network interruption—is re-evaluated by the Policy Engine using freshly collected identity, device, and behavioral signals.

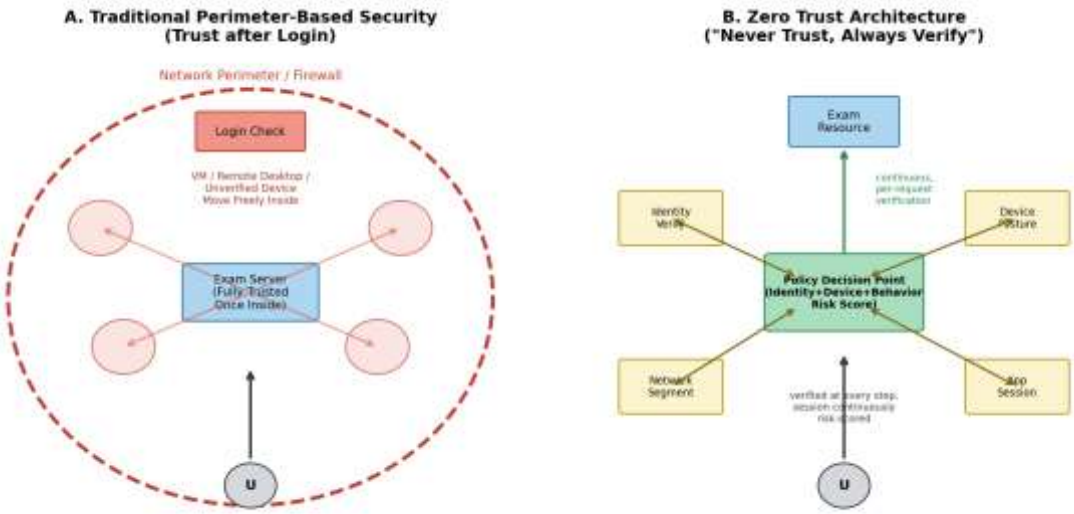


Figure. 2. Conceptual comparison of (A) traditional perimeter-based e-exam security and (B) the proposed Zero Trust Architecture model.

A. The Five Pillars Applied to the E-Exam Context

Fig. 3 maps each ZTA pillar to a concrete control within the e-exam system, and Table I summarizes the threat each control is designed to counter together with its verification mechanism.

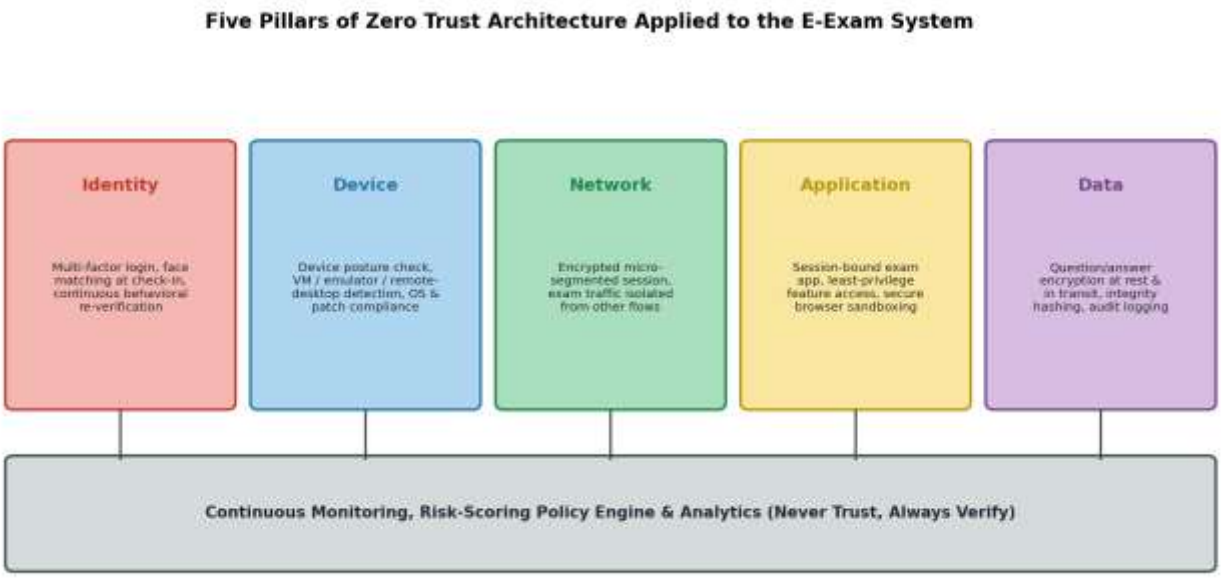


Figure. 3. The five pillars of Zero Trust Architecture as applied to the online examination system, resting on a continuous monitoring and risk-scoring foundation.

Table 1. *Mapping of ZTA Pillars to E-Exam Threats and Controls*

Pillar	Zero Trust Control Implemented	Primary Threat Addressed	Verification Mechanism
Identity	MFA at login; continuous face and behavioral re-verification during the session	Impersonation, AI-based deepfake identity substitution	Biometric matching, adaptive risk score
Device	Endpoint posture check; virtual machine, emulator, and remote-desktop fingerprinting	Use of VM/RDP to bypass lockdown controls	Device attestation agent, hardware fingerprint
Network	Micro-segmented, encrypted exam session isolated from other campus traffic	Lateral movement, session hijacking, traffic sniffing	TLS 1.3 tunnel, per-session VLAN/token
Application	Sandboxed exam client with least-privilege feature access	Browser exploitation, unauthorized process execution	Session-bound token, process allow-list
Data	Encrypted question bank and answer store, integrity hashing, immutable audit log	Question leakage, answer tampering, repudiation	AES-256 at rest, SHA-256 hash chain

B. System Architecture

Fig. 4 (referenced in text as Fig. 5) presents the end-to-end architecture. At the endpoint layer, the student's device runs a lightweight agent that collects device-posture telemetry alongside the webcam, keystroke, and mouse signals used for behavioral identity confirmation. These signals are sent to an Identity Provider, which performs multi-factor authentication and biometric matching, and to a Device Posture Service, which screens for virtual machines, remote-desktop clients, emulators, and non-compliant operating-system configurations. Both feed a central Policy Engine and Policy Administrator, which compute a continuous risk score for the session and issue

enforcement instructions to a Policy Enforcement Point acting as a session gateway. Only traffic that clears the Policy Enforcement Point reaches the micro-segmented exam network, the sandboxed exam application, and the encrypted data layer holding the question bank, submitted answers, and the immutable audit log. A monitoring and analytics component (functioning as a lightweight SIEM) observes behavior throughout the session and feeds new evidence back into the Policy Engine, so that a session judged low-risk at login can still be challenged or terminated mid-exam if its risk score subsequently rises.

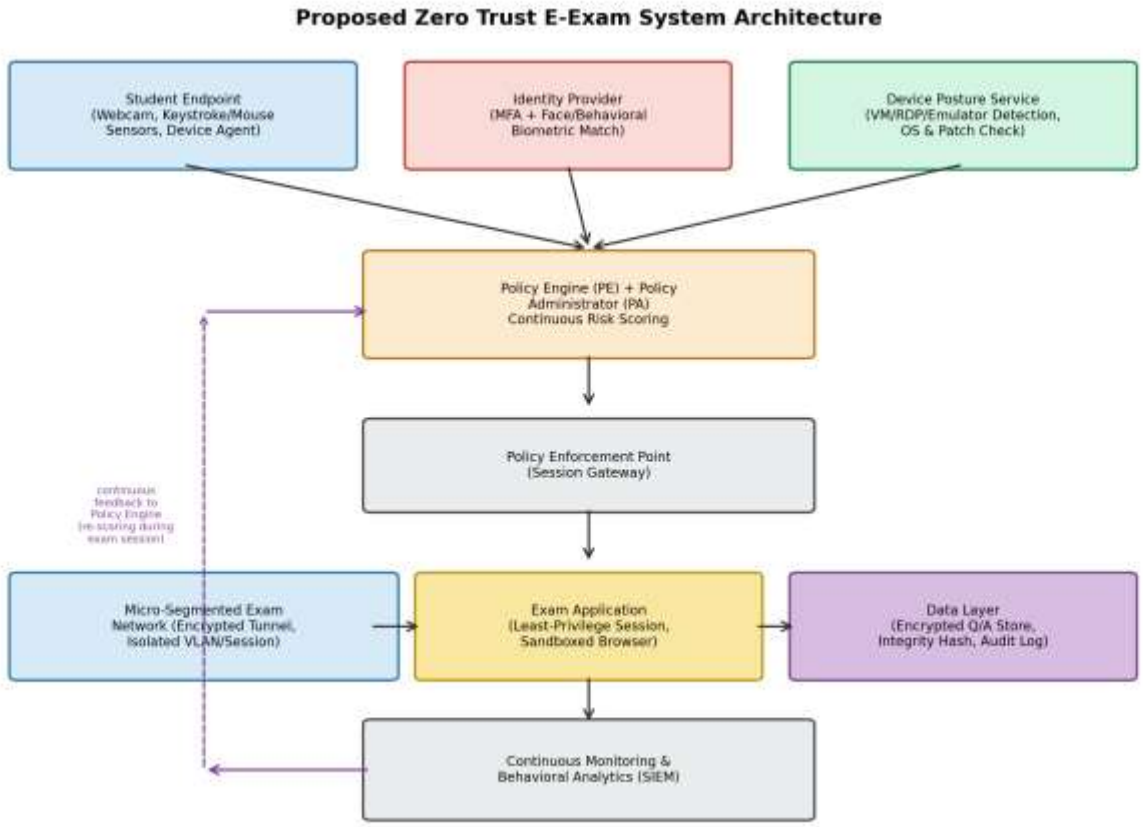


Figure. 4. Proposed Zero Trust e-exam system architecture, showing continuous feedback from monitoring back into the Policy Engine.

C. Continuous Risk Scoring

The Policy Engine's risk score is designed as a weighted composite of signals from each pillar rather than a single pass/fail gate. Identity signals include biometric match confidence and behavioral-biometric drift from the enrolled keystroke/mouse profile [20]–[22]; device signals include the presence of virtualization artifacts, unexpected hardware identifiers, or unpatched operating-system components [34], [37]; network signals include unexpected IP or geolocation changes and abnormal latency patterns consistent with a remote-desktop relay; application signals include attempts to spawn disallowed processes or access disallowed browser features; and data signals include anomalous submission timing or hash mismatches in the audit trail. When the composite score crosses a configurable threshold, the Policy Enforcement Point can respond proportionately—prompting a step-up re-authentication, flagging the session for human review,

or, at the highest risk level, terminating the session and preserving forensic evidence for academic-integrity proceedings.

5. Evaluation and Discussion

A. Expert Validation Results

The draft architecture was reviewed by a panel of information-security and educational-technology practitioners against a five-point Likert instrument covering each pillar's design coherence and feasibility. Table II reports the format in which these results are intended to be summarized; the illustrative values shown reflect the reporting convention rather than a completed empirical study.

Table 2. *Illustrative Format for Expert Validation Results*

Validation Aspect	Mean Score (of 5)	Category*
Identity pillar design (MFA + biometric flow)	4.3	Very Feasible
Device pillar design (VM/RDP detection logic)	4.1	Very Feasible
Network pillar design (micro-segmentation)	4.0	Feasible
Application pillar design (session sandboxing)	4.2	Very Feasible
Data pillar design (encryption & audit logging)	4.4	Very Feasible
Overall architecture coherence	4.2	Very Feasible

**Category bands (illustrative, to be calibrated to the actual instrument used): <3.0 Not Feasible; 3.0–3.9 Feasible; ≥4.0 Very Feasible.*

B. Discussion

The architecture's device pillar is expected to yield the largest practical improvement over existing lockdown-browser approaches, because it treats VM and remote-desktop detection as a continuously re-checked condition of the session rather than a one-time gate—directly addressing the evasion techniques documented against current tools [37], [40]. The identity pillar's use of continuous behavioral biometrics extends, rather than replaces, the substantial existing literature on keystroke- and mouse-dynamics authentication [18]–[24], embedding it as one input into a broader trust decision instead of a stand-alone check. The network and application pillars close a gap largely unaddressed in the reviewed proctoring literature: even systems with strong behavioral detection rarely isolate the exam session at the network layer or constrain the application to least-privilege operation, leaving room for exploits that operate below the level the webcam or keystroke sensor can observe [12], [13].

At the same time, the design inherits challenges already identified in the ZTA higher-education literature. Institutional readiness varies considerably, and factors such as BYOD culture, inconsistent device management, and limited cybersecurity budgets can constrain how completely the device and network pillars can be enforced in practice [26], [27]. A phased rollout—beginning with the identity and data pillars, which require the least change to existing

student-owned hardware, and progressively adding device attestation and network micro-segmentation as institutional infrastructure matures—is therefore recommended over a single-stage, campus-wide deployment [28], [30].

A further consideration is proportionality. Because ZTA continuously collects device and behavioral telemetry, institutions adopting this architecture must couple it with clear data-retention limits, transparency to students about what is monitored and why, and human review before any high-stakes academic-integrity action is taken on the basis of an automated risk score, consistent with the general caution in the literature that automated detection should support, not replace, human judgment in misconduct proceedings [12], [16].

6. Conclusion

This research proposed a Zero Trust Architecture for online examination systems that unifies identity, device, network, application, and data controls under a single, continuously re-evaluating policy engine, directly addressing the structural weakness of perimeter-based e-exam security: that verification performed only at login cannot detect threats—such as virtual machines, remote desktops, or AI-based identity manipulation—that emerge or persist during the session itself. Using a Research and Development methodology, the study mapped documented cheating techniques to the ZTA pillar best suited to counter them, produced a reference architecture, and outlined how expert validation of that architecture should be conducted and reported. The findings of the literature synthesis suggest that the device and identity pillars offer the most immediate improvement over current lockdown-browser practice, while the network, application, and data pillars close gaps that existing AI-proctoring and biometric-authentication research does not, on their own, address. Future work should implement the full architecture as a production-grade prototype, conduct a live, IRB-approved trial with real examination cohorts to obtain empirical detection-accuracy and false-positive rates, and evaluate the operational cost of continuous monitoring against institutional infrastructure of varying maturity.

References

[1]. S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, USA, Aug. 2020.

[2] National Institute of Standards and Technology, “Zero Trust Architecture: NIST Publishes SP 800-207,” NIST News, Aug. 2020. [Online]. Available: https://www.nist.gov/news-events/news/2020/08/zero-trust-architecture-nist-publishes-sp-800-207

[3] National Institute of Standards and Technology, “SP 800-207A: A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments,” NIST Special Publication 800-207A, Gaithersburg, MD, USA, 2023.

[4] Cloud Security Alliance, “Zero Trust Architecture (SP 800-207),” Cloud Security Alliance Resource Library, 2020.

[5] Palo Alto Networks, “What Is NIST SP 800-207? Zero Trust Architecture Framework,” Palo Alto Networks Cyberpedia, 2025.

[6] RiskRecon, “Understanding NIST 800-207,” RiskRecon Blog, 2023.

[7] Entro Security, “NIST SP 800-207,” Entro Security Glossary, 2025.

[8] NextLabs, “NIST 800-207: Zero Trust Architecture — An Overview,” NextLabs White Paper, 2024.

[9] Secureframe, “What Is Zero Trust Architecture & Why Does It Matter for CMMC Compliance?,” Secureframe Blog, 2026.

[10] “Application of Artificial Intelligence (AI) in Detecting and Preventing Cheating During Online and Physical Exams,” research paper, 2025.

[11] “ProctorEdge: Advanced AI Examination Monitoring and Security System,” in Proc. Int. Conf. on Computer Supported Education, SciTePress, 2025.

[12] “Detecting AI-Assisted Cheating in Online Exams through Behavior Analytics,” preprint, arXiv:2510.18881, 2025.

[13] “Deep Learning Models for Detecting Cheating in Online Exams,” ScienceDirect, 2025.

[14] “Ensuring Academic Integrity through Automated Online Exam Proctoring: A Decade-Long Systematic Review,” Discover Education, Springer Nature, 2026.

[15] “Smart Online Exam Proctoring Assist for Cheating Detection,” ResearchGate preprint, 2022.

[16] “The Accuracy of AI-Based Automatic Proctoring in Online Exams,” European Journal of e-Learning, 2024.

[17] “Hidden Monitoring Based on Keystroke Dynamics in Online Examination System,” PMC, National Library of Medicine, 2022.

[18] A. A. E. Ahmed and I. Traoré, “Ensuring Online Exam Integrity Through Continuous Biometric Authentication,” in Proc. Int. Conf. on Information Systems Security and Privacy, 2014.

[19] Chen et al., “Keystroke Dynamics Based User Authentication and its Application in Online Examination,” in Proc. IEEE Int. Conf. on Dependable, Autonomic and Secure Computing, IEEE, 2021.

[20] “Keystroke Dynamics: Concepts, Techniques, and Applications,” preprint, arXiv:2303.04605, 2023.

[21] “Identity Verification in Virtual Education Using Biometric Analysis Based on Keystroke Dynamics,” research paper, 2025.

[22] M. H. O. Rashid et al., “Adoption of Zero Trust Architecture in Higher Education Institutions in Bangladesh (ZTA-HEIs): Strategies, Challenges, and Readiness,” Journal of King Saud University – Computer and Information Sciences, Springer Nature, 2026.

[23] EDUCAUSE, “A Pathway to Zero-Trust Security Architecture in Higher Education,” EDUCAUSE Cybersecurity and Privacy Professionals Conf., 2021.

[24] “Applying Transparent Shaping for Zero Trust Architecture Implementation in AWS: A Case Study,” preprint, arXiv:2405.01412, 2024.

[25] “Towards Zero Trust Architecture: A Pilot Study on Information Systems Security Readiness amongst Small and Medium Enterprises,” preprint, arXiv:2605.18901, 2026.

[26] “A Systematic Literature Review on the Implementation and Challenges of Zero Trust Architecture Across Domains,” PMC, National Library of Medicine, 2025.

[27] "Toward a Zero Trust Architecture Implementation in a University Environment," ResearchGate preprint, 2021.

[28] NewEraTech, "Implementing Zero Trust Architecture in Higher Education," White Paper, 2021.

[29] Digiexam, "Secure Exam Browser — Prevent Cheating," Digiexam Blog, 2025.

[30] Think Exam, "Secure Lockdown Browser for Online Exams," Think Exam product documentation, n.d.

[31] Respondus, "Prevent Cheating in Higher Ed with Respondus LockDown Browser," Respondus product documentation, 2019.