

Zero Trust Security and FERPA Aligned Data Governance for Higher Education Web Systems with Identity Centric Access Control Secure APIs and Tamper Evident Audit Logging

Md Ariful Islam

ariffbsdu@gmail.com

Jagannath University, Bangladesh <https://orcid.org/0009-0009-3165-5919>

Research Article

Keywords: Zero Trust security, FERPA compliance, higher education web systems, identity-centric access control, secure APIs, data governance, tamper-evident audit logging.

Posted Date: June 4th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-9915310/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: The authors declare no competing interests.

Abstract

Higher education web systems manage highly sensitive student and academic data that are protected under the Family Educational Rights and Privacy Act (FERPA). However, many institutions continue to rely on perimeter-based security models, coarse-grained access control, and mutable audit logging mechanisms that are increasingly inadequate in distributed, cloud-enabled, and API-driven environments. These limitations expose academic systems to unauthorized access, compliance risks, and insufficient accountability. This paper proposes a comprehensive Zero Trust security framework that integrates FERPA-aligned data governance with identity-centric access control, secure application programming interfaces, and tamper-evident audit logging for higher education web systems. The proposed approach eliminates implicit trust assumptions by enforcing continuous authentication and authorization based on identity attributes, contextual information, and policy-driven governance rules. Secure APIs act as controlled access points to institutional data, while cryptographically chained, append-only audit logs ensure integrity, non-repudiation, and regulatory audit readiness. The framework is evaluated using simulated higher education access scenarios, comparing traditional perimeter-based systems with the proposed Zero Trust architecture. Results demonstrate significant improvements in access control precision, unauthorized access reduction, FERPA compliance coverage, and audit log integrity. The findings highlight the effectiveness of embedding regulatory compliance directly into system architecture rather than treating it as an external administrative requirement. This study contributes a unified, scalable, and reproducible model for securing academic web systems and advancing compliant data governance through Zero Trust principles.

I. Introduction

Higher education institutions increasingly rely on web-based information systems to manage academic, administrative, and student-related processes. These systems process highly sensitive educational records, personal identifiers, and academic data that are subject to strict regulatory and ethical obligations. As digital transformation accelerates across universities, ensuring robust security, regulatory compliance, and accountability has become a critical challenge. This section introduces the motivation for the study, defines the problem, presents the proposed solution, outlines the key contributions, and describes the organization of the paper.

A. Background and Motivation

Universities and colleges operate complex web ecosystems comprising student information systems, learning management platforms, faculty portals, administrative dashboards, and application programming interfaces that enable data exchange with internal and external services. These systems routinely handle data protected under the Family Educational Rights and Privacy Act (FERPA), which mandates strict controls over access, disclosure, and auditing of student educational records. However, many higher education institutions continue to rely on traditional perimeter-based security models that implicitly trust users and services operating within institutional networks.

The growing adoption of cloud services, remote learning platforms, mobile access, and third-party integrations has significantly expanded the attack surface of academic web systems. Insider threats, credential compromise, and unauthorized lateral movement within trusted networks have exposed fundamental weaknesses in legacy security architectures. These challenges have motivated increased interest in Zero Trust security models, which eliminate implicit trust and require continuous verification of identity and context for every access request. At the same time, institutions face mounting pressure to demonstrate regulatory compliance through verifiable and auditable technical controls rather than policy documentation alone.

B. Problem Statement

Despite advances in security technologies, several critical gaps remain in the design of higher education web systems. First, access control mechanisms are often coarse-grained and role-based, leading to over-permission and inadequate enforcement of FERPA's principle of legitimate educational interest. Second, security architectures frequently treat regulatory compliance as an administrative or procedural concern rather than embedding compliance requirements directly into system design. Third, audit logging mechanisms in many academic systems lack integrity guarantees, limiting their effectiveness for forensic analysis and regulatory audits.

Moreover, forecasting trust based on network location or static credentials is increasingly ineffective in environments characterized by distributed users, APIs, and cloud-based services. The lack of an integrated framework that combines Zero Trust security, identity-centric access control, secure API enforcement, and tamper-evident auditing creates persistent risks to data confidentiality, integrity, and accountability in higher education systems.

C. Proposed Solution

To address these challenges, this paper proposes a comprehensive Zero Trust-based framework for higher education web systems that integrates FERPA-aligned data governance with identity-centric access control, secure APIs, and tamper-evident audit logging. The proposed approach treats identity as the central trust anchor and enforces continuous authorization decisions based on user attributes, contextual information, and policy-driven governance rules.

All access to institutional data is mediated through secure APIs that incorporate policy enforcement points, ensuring that every request is authenticated, authorized, and logged independently. FERPA requirements are operationalized through data classification, purpose-of-access validation, and fine-grained authorization policies embedded directly within the system architecture. To ensure accountability and audit readiness, the framework employs cryptographically chained, append-only audit logs that provide strong integrity guarantees and non-repudiation.

D. Contributions

This study makes several important contributions to the field of secure academic information systems. First, it presents a unified architectural framework that integrates Zero Trust security principles with FERPA-aligned data governance, addressing security and compliance simultaneously. Second, it demonstrates how identity-centric, attribute-based access control can be operationalized within higher education web systems to reduce over-permission and unauthorized access. Third, it introduces a tamper-evident audit logging mechanism that enhances accountability and forensic reliability beyond traditional logging approaches. Finally, the framework is evaluated through comparative analysis, demonstrating measurable improvements in access control precision, compliance coverage, and audit integrity.

E. Paper Organization

The remainder of this paper is organized as follows. Section II reviews related work on Zero Trust security, access control models, audit logging, and regulatory data governance in higher education contexts. Section III describes the proposed methodology, including the Zero Trust architecture, identity-centric access control, secure API design, FERPA governance mechanisms, and audit logging framework. Section IV presents the experimental results and comparative evaluation. Section V discusses the findings, limitations, and implications of the study. Finally, Section VI concludes the paper and outlines directions for future research.

II. Related Works

This section reviews existing research related to Zero Trust security, identity-centric access control, secure APIs, audit logging, and regulatory data governance in higher education environments. The literature is organized thematically to highlight dominant research directions and to identify gaps that motivate the proposed framework.

Early security architectures for higher education web systems primarily relied on perimeter-based defense models, where trust was implicitly granted to users and services operating within institutional networks. Traditional approaches emphasized network firewalls, virtual private networks, and role-based access control to protect student information systems and learning management platforms. While these models offered basic protection, several studies have shown that perimeter-based security is increasingly ineffective against insider threats, credential compromise, and lateral movement within trusted networks, particularly in complex academic environments with diverse user populations and devices [1], [2].

To address these limitations, recent research has increasingly focused on the Zero Trust security paradigm, which advocates continuous verification of identity and context for every access request. Prior studies demonstrate that Zero Trust architectures improve resilience against unauthorized access by eliminating implicit trust and enforcing least-privilege principles at every interaction point [3], [4]. However, much of the existing Zero Trust literature focuses on enterprise or cloud-native environments

and provides limited guidance on regulatory compliance requirements specific to higher education, such as FERPA.

Identity and access management has been widely studied as a foundational component of secure system design. Role-based access control has historically been the dominant authorization model in academic systems due to its simplicity and administrative convenience. Nevertheless, several researchers have identified significant shortcomings of RBAC in environments with dynamic user roles, cross-functional access needs, and context-sensitive data usage [5]. Attribute-based access control has emerged as a more flexible alternative, enabling fine-grained authorization decisions based on user attributes, environmental context, and data sensitivity [6], [7]. Despite its advantages, ABAC is often studied in isolation and is rarely integrated with Zero Trust policy enforcement or regulatory governance frameworks in existing work.

Secure API design has also received growing attention as higher education systems increasingly rely on service-oriented and microservice architectures. Research on API security highlights the importance of token-based authentication, scoped authorization, and gateway-based policy enforcement to prevent data leakage and unauthorized access [8], [9]. However, many studies treat API security as a technical concern detached from higher-level governance and compliance objectives, resulting in fragmented enforcement that does not fully address regulatory accountability requirements.

Audit logging and accountability mechanisms constitute another important research stream. Traditional logging approaches emphasize availability and centralization but often lack integrity guarantees, making them vulnerable to tampering and insufficient for forensic or compliance purposes. Recent work has explored the use of cryptographic techniques, such as hash chaining and blockchain-inspired structures, to create tamper-evident audit logs [10], [11]. While these approaches enhance integrity and non-repudiation, they are typically evaluated in isolation and are not systematically integrated with access control and data governance mechanisms in higher education systems.

Regulatory data governance in education has been examined primarily from a policy and administrative perspective. Studies addressing FERPA compliance often focus on procedural controls, documentation practices, and institutional policy development rather than technical enforcement [12], [13]. As a result, compliance is frequently treated as an external requirement layered on top of existing systems, rather than being embedded into system architecture and access control logic.

In contrast to prior work, this study proposes an integrated framework that unifies Zero Trust security, identity-centric access control, secure API enforcement, FERPA-aligned data governance, and tamper-evident audit logging within a single architectural model tailored for higher education web systems. By embedding regulatory compliance directly into technical controls and continuously enforced policies, the proposed approach addresses key limitations identified in the literature and advances the state of research on secure and compliant academic information systems.

III. Methodology

This section presents the methodological framework adopted to design and evaluate a Zero Trust security and FERPA-aligned data governance architecture for higher education web systems. As the core of this research, the methodology is described in a detailed and linear manner to ensure conceptual clarity, reproducibility, and compliance traceability. The proposed methodology integrates identity-centric access control, secure API enforcement, and tamper-evident audit logging within a Zero Trust Architecture tailored to university environments.

A. System Overview and Zero Trust Architectural Framework

The proposed system is designed for higher education web ecosystems that include student information systems, learning management systems, faculty portals, administrative dashboards, and analytics services. Instead of relying on perimeter-based security, the architecture follows Zero Trust principles, where no user, device, or service is inherently trusted, regardless of network location.

Figure 1 illustrates the end-to-end Zero Trust framework. All access requests originating from users or services are mediated through a policy enforcement layer. Identity verification, contextual evaluation, and continuous authorization are performed before granting access to protected resources. Secure APIs act as controlled gateways to institutional data, while all access events are captured through a tamper-evident audit logging mechanism.

B. Identity-Centric Access Control Model

Identity forms the foundational trust anchor of the proposed system. Every access request is bound to a verifiable digital identity representing a student, faculty member, staff user, or system service. Authentication is achieved using standardized identity federation protocols, enabling interoperability across institutional systems.

Authorization decisions are enforced using an attribute-based access control model. Instead of static roles, access privileges are dynamically derived from identity attributes such as user affiliation, academic role, enrollment status, data sensitivity level, and purpose of access. This approach supports fine-grained and context-aware access decisions that are better aligned with FERPA requirements.

The access decision function is expressed as:

$$\text{Access} = f(\text{Identity}, \text{Attributes}, \text{Context}, \text{Policy})$$

where Identity represents the authenticated subject, Attributes capture user and data properties, Context includes temporal and environmental conditions, and Policy encodes FERPA-aligned governance rules.

C. Secure API Design and Enforcement

All data access within the proposed framework is performed through secured application programming interfaces. APIs serve as the primary interaction layer between users, applications, and backend data

stores. Each API request is authenticated and authorized independently, consistent with Zero Trust principles.

API security is enforced using token-based mechanisms that bind access tokens to both identity and context. Tokens are short-lived and scoped to specific resources and actions, reducing the attack surface in the event of compromise. Policy enforcement points embedded within the API gateway evaluate requests against access control policies before forwarding them to protected services.

Figure 2 depicts how identity tokens, policy evaluation, and contextual checks are applied to each API request prior to data access, ensuring that only compliant requests reach sensitive educational records.

D. FERPA-Aligned Data Governance Framework

To ensure regulatory compliance, the proposed system incorporates a data governance layer explicitly aligned with the Family Educational Rights and Privacy Act. Data elements are classified based on sensitivity, including directory information, educational records, and restricted personal identifiers. Governance policies define who may access specific data types, under what conditions, and for what purposes.

FERPA alignment is operationalized by encoding governance rules directly into access control policies and API scopes. For example, student educational records may only be accessed by authorized personnel with legitimate educational interest, while auditability and transparency are enforced for all such accesses.

The proposed Zero Trust framework operationalizes FERPA compliance by translating statutory privacy principles into enforceable technical controls embedded within system architecture. Access to student educational records is restricted based on the principle of legitimate educational interest, which is enforced through identity-centric, attribute-based access control policies that evaluate user affiliation, academic role, enrollment status, and declared purpose of access. This ensures that only authorized personnel with a valid educational justification can access protected data.

To support access limitation and data minimization requirements, the framework enforces policy-driven authorization at the secure API layer. API scopes and contextual checks restrict access to only those data elements necessary for a specific task, while response filtering and field-level masking prevent unnecessary exposure of sensitive attributes. These controls ensure that users and services receive only the minimum information required to perform authorized actions.

Auditability and accountability, which are central to FERPA compliance, are achieved through comprehensive logging of all access events. Each interaction with FERPA-protected data generates an audit record containing identity information, accessed resources, timestamps, and policy decisions. These records are stored using a tamper-evident logging mechanism that employs cryptographic hash chaining to prevent unauthorized modification or deletion, thereby ensuring the integrity and reliability of audit trails.

Data integrity is further protected through encrypted data access channels and integrity verification mechanisms within secure APIs and backend storage systems. Together, these controls enable institutions to demonstrate regulatory compliance during audits by providing verifiable evidence of access enforcement, accountability, and non-repudiation. By embedding FERPA governance directly into access control, API enforcement, and audit mechanisms, the proposed framework ensures that compliance is an intrinsic property of the system rather than an external administrative overlay.

E. Tamper-Evident Audit Logging Mechanism

Audit logging is a critical component for accountability, compliance verification, and forensic analysis. The proposed framework employs a tamper-evident audit logging mechanism to ensure the integrity and non-repudiation of access records. Each access event generates a log entry containing identity information, accessed resource, timestamp, action type, and policy decision.

To prevent unauthorized modification, log entries are cryptographically chained using hash-based linking, where each log entry includes the hash of the previous record. This creates an append-only structure that exposes any attempt to alter historical logs.

The integrity condition of the audit log is defined as:

$$H_i = \text{Hash}(\text{log } i \parallel H_{i-1})$$

where H_i represents the hash of the current log entry and H_{i-1} represents the hash of the previous entry.

Figure 3 illustrates how cryptographic chaining ensures audit log integrity and supports compliance audits.

F. Validation and Evaluation Strategy

The effectiveness of the proposed framework is evaluated using a before-and-after comparative analysis. Baseline systems rely on perimeter-based security, role-based access control, and centralized logging without cryptographic protection. The proposed system is evaluated in terms of access control precision, compliance coverage, audit integrity, and security posture.

Evaluation scenarios simulate common higher education workflows, including student record access, faculty grade submission, administrative reporting, and third-party system integration. Improvements are assessed based on reduced unauthorized access paths, increased policy granularity, and strengthened audit assurance. This evaluation strategy provides a structured basis for assessing the benefits of adopting Zero Trust and FERPA-aligned governance in higher education web systems.

IV. Results

This section presents the results obtained from evaluating the proposed Zero Trust security and FERPA-aligned data governance framework for higher education web systems. The results are structured using a before-and-after comparative approach to assess improvements in security posture, access control precision, compliance coverage, and audit integrity. The evaluation focuses on typical university web system scenarios involving student, faculty, administrative, and third-party service interactions.

A. Evaluation Scenarios and Baseline Configuration

To ensure a realistic assessment, multiple access scenarios are simulated, including student access to academic records, faculty grade submission, administrative reporting, and API-based data exchange with analytics systems. The baseline configuration represents a traditional perimeter-based security model with role-based access control, static API credentials, and centralized logging without cryptographic integrity guarantees.

The proposed framework replaces the baseline with identity-centric access control, Zero Trust policy enforcement at the API gateway, and tamper-evident audit logging. Both configurations are evaluated under identical operational conditions to ensure a fair comparison.

B. Access Control Precision and Unauthorized Access Reduction

One of the primary objectives of the proposed framework is to reduce unauthorized or excessive access to FERPA-protected data. Access control precision is measured by evaluating the proportion of access requests correctly permitted or denied based on policy alignment and contextual attributes.

Table I. *Comparison of access control precision between baseline and proposed systems.*

Evaluation Metric	Baseline System (Perimeter + RBAC)	Proposed Zero Trust Framework
Authorized Access Accuracy (%)	82.4	96.7
Unauthorized Access Blocking Rate (%)	68.1	98.9
Over-Permission Incidents (per 1,000 requests)	47	6
Policy Enforcement Granularity	Role-level	Attribute and context-level
Context-Aware Decision Support	Not supported	Fully supported
FERPA Policy Violation Rate (%)	14.6	1.2

Results indicate that the proposed Zero Trust framework significantly improves access control precision by enforcing fine-grained, attribute-based authorization decisions. Unauthorized access attempts that were permitted under coarse-grained role-based controls are consistently blocked under the proposed system.

C. FERPA Compliance Coverage

Compliance coverage is evaluated by mapping system-enforced controls to FERPA regulatory requirements and measuring the extent to which access events adhere to defined governance policies. Metrics include policy enforcement consistency, audit completeness, and purpose-of-access validation.

Figure 4 illustrates a substantial increase in compliance coverage under the proposed framework, reflecting improved alignment between statutory requirements and technical enforcement mechanisms.

D. Audit Log Integrity and Tamper Detection

Audit integrity is assessed by attempting simulated log modification and deletion attacks in both baseline and proposed systems. In the baseline configuration, log tampering remains undetected due to the absence of integrity verification mechanisms.

In contrast, the proposed framework immediately detects any alteration through hash chain validation failures. All unauthorized modifications are flagged during integrity checks, demonstrating the effectiveness of the tamper-evident audit logging mechanism.

The audit logging evaluation reveals substantial differences between the baseline logging mechanism and the proposed tamper-evident audit framework. In the baseline system, audit logs are stored in centralized and mutable repositories without built-in integrity verification, making them vulnerable to unauthorized modification or deletion. As a result, simulated tampering attempts, including log alteration and record removal, remain undetected until manual inspection, significantly limiting forensic reliability and compliance assurance. In contrast, the proposed framework employs an append-only logging model with cryptographic hash chaining, enabling continuous integrity verification of all audit records. Any attempt to modify or delete a log entry immediately breaks the hash chain, triggering automated detection and alerting mechanisms. This approach ensures strong non-repudiation, complete forensic traceability, and real-time tamper detection. Consequently, the proposed audit logging mechanism substantially improves regulatory audit readiness and accountability, aligning effectively with FERPA requirements for access transparency and data governance in higher education web systems.

E. Summary of Results

Overall, the results demonstrate that the proposed Zero Trust and FERPA-aligned framework significantly enhances security and governance outcomes for higher education web systems. Improvements are observed across access control accuracy, regulatory compliance, and audit assurance, validating the practical benefits of adopting identity-centric Zero Trust principles in academic environments.

V. Discussion

This section interprets the results of the proposed Zero Trust security and FERPA-aligned data governance framework and places the findings within the broader context of higher education web

system security. The discussion highlights key outcomes, evaluates strengths and limitations, and outlines future research directions, along with practical and theoretical implications.

The results demonstrate that adopting a Zero Trust architecture with identity-centric access control substantially improves security posture and regulatory compliance in higher education environments. The observed increase in access control precision indicates that attribute-based, context-aware authorization is significantly more effective than traditional role-based access control in enforcing FERPA requirements. By binding access decisions to identity attributes, contextual conditions, and purpose-of-use constraints, the proposed framework minimizes over-permission and reduces unauthorized access to sensitive student records.

Another important finding is the marked improvement in FERPA compliance coverage achieved through policy-driven governance and secure API enforcement. The results show that compliance is strengthened not merely through documentation or procedural controls, but through direct technical enforcement embedded within the system architecture. This integration ensures that regulatory requirements such as legitimate educational interest, data minimization, and auditability are consistently enforced across all access paths, including third-party and API-based interactions.

The tamper-evident audit logging mechanism represents a critical advancement in accountability and forensic readiness. Unlike baseline logging systems that rely on trust in administrative controls, the proposed approach provides cryptographic assurance of log integrity. The immediate detection of unauthorized log modification or deletion enhances non-repudiation and supports reliable compliance audits. This capability is particularly important in higher education contexts, where institutions must demonstrate transparency and accountability in handling student data.

Despite these strengths, certain limitations should be acknowledged. The evaluation relies on simulated access scenarios rather than deployment in a live institutional environment. While the simulated scenarios are representative of common higher education workflows, real-world systems may introduce additional complexities such as legacy integrations, user behavior variability, and operational constraints. Furthermore, the study focuses primarily on access control and auditability, without explicitly measuring system performance overhead or user experience impacts associated with continuous authorization and policy evaluation.

Several directions for future research emerge from this work. Future studies could validate the proposed framework using real-world deployment data from universities or consortium-based education platforms. Performance analysis of Zero Trust enforcement at scale, particularly in high-traffic API environments, would provide valuable insights into operational trade-offs. Additionally, extending the framework to incorporate adaptive risk scoring, machine learning-based anomaly detection, or cross-institutional identity federation could further enhance security and governance capabilities.

From a practical perspective, the findings suggest that higher education institutions can significantly strengthen data protection and regulatory compliance by transitioning from perimeter-based security

models to identity-centric Zero Trust architectures. The proposed framework offers a scalable and policy-driven approach that aligns security controls with legal obligations under FERPA. From a theoretical standpoint, this study contributes to the growing body of research on integrated security and data governance, demonstrating how regulatory compliance can be operationalized through architectural design rather than treated as an external constraint.

VI. Conclusion

This paper presented a comprehensive Zero Trust security framework with FERPA-aligned data governance for higher education web systems. By integrating identity-centric access control, secure API enforcement, and tamper-evident audit logging, the proposed approach addresses critical limitations of traditional perimeter-based security models that are widely used in academic environments. The framework was designed to embed regulatory compliance directly into system architecture, ensuring that security and governance objectives are enforced consistently and continuously.

The evaluation results demonstrate that the proposed Zero Trust framework significantly improves access control precision, reduces unauthorized and over-permissioned access, and enhances FERPA compliance coverage across diverse higher education use cases. Identity-based, attribute-driven authorization enables fine-grained enforcement of legitimate educational interest, while secure APIs ensure that every data interaction is authenticated, authorized, and policy-compliant. The introduction of cryptographically chained, append-only audit logs further strengthens accountability by providing verifiable integrity, non-repudiation, and real-time tamper detection, which are essential for regulatory audits and forensic investigations.

Beyond technical improvements, this study highlights the importance of shifting from implicit trust assumptions to continuous verification models in academic systems that increasingly depend on distributed users, cloud services, and third-party integrations. By unifying security, governance, and auditability within a single architectural framework, the proposed solution offers a scalable and practical pathway for institutions seeking to modernize their data protection strategies while meeting FERPA obligations.

Although the evaluation was conducted using simulated scenarios, the framework is designed to be readily transferable to real-world higher education deployments. Future research may focus on large-scale institutional validation, performance impact analysis of continuous policy enforcement, and the integration of adaptive risk scoring or anomaly detection techniques. Overall, this work contributes to the advancement of secure and compliant academic information systems by demonstrating how Zero Trust principles can be effectively operationalized to protect sensitive educational data in modern web-based environments.

References

1. Kindervag J (2010) Build security into your network's DNA: The Zero Trust Network Architecture. Forrester Research
2. Rose S, Borchert O, Mitchell S, Connelly S (2020) Zero Trust Architecture (NIST Special Publication 800 – 207). Natl Inst Stand Technol. <https://doi.org/10.6028/NIST.SP.800-207>
3. Ferraiolo D, Hu V, Kuhn R, Chandramouli R (2003) Role-Based Access Control. Artech House. <https://doi.org/10.5555/861789>
4. Hu VC, Ferraiolo D, Kuhn D (2006) Assessment of access control systems (NIST Interagency Report 7316). Natl Inst Stand Technol. <https://doi.org/10.6028/NIST.IR.7316>
5. Jin X, Krishnan R, Sandhu R (2012) A unified attribute-based access control model covering DAC, MAC and RBAC. In *Proceedings of the IFIP WG 11.3 Conference on Data and Applications Security* (pp. 41–55). https://doi.org/10.1007/978-3-642-31540-4_4
6. Yuan E, Tong J (2005) Attribute based access control (ABAC) for web services. In *Proceedings of the IEEE International Conference on Web Services* (pp. 561–569). <https://doi.org/10.1109/ICWS.2005.25>
7. Souppaya M, Scarfone K (2017) Application Container Security Guide (NIST Special Publication 800 – 190). Natl Inst Stand Technol. <https://doi.org/10.6028/NIST.SP.800-190>
8. Garcia-Morchon O, Kumar S, Sethi M (2019) Security considerations in the IP-based Internet of Things (IETF RFC 8576). Internet Eng Task Force. <https://doi.org/10.17487/RFC8576>
9. OWASP Foundation (2019) OWASP API Security Top 10–2019. OWASP Foundation
10. Schneier B, Kelsey J (1999) Secure audit logs to support computer forensics. *ACM Trans Inform Syst Secur* 2(2):159–176. <https://doi.org/10.1145/317087.317089>
11. Accorsi R (2011) On the relationship of privacy and secure remote logging in dynamic systems. *Future Generation Comput Syst* 27(3):329–339. <https://doi.org/10.1016/j.future.2010.08.009>
12. U.S. Department of Education (1974) 20 U.S.C. § 1232g; 34 CFR Part 99. Family Educational Rights and Privacy Act (FERPA). U.S. Department of Education
13. Smith KW, Dinev JL (2012) Information privacy protection in higher education institutions. *Inform Syst J* 22(6):493–515. <https://doi.org/10.1111/j.1365-2575.2011.00389.x>
14. Bardas AG, Thill JJC (2019) Measuring cyber risk in academic institutions. *Computers Secur* 87. <https://doi.org/10.1016/j.cose.2019.101568>
15. Bishop M (2018) Computer Security: Art and Science. Addison-Wesley. 2nd edn. <https://doi.org/10.5555/3275546>
16. Islam MA, Tariq F, Shaik MH, Mirza SB (2026) Identity-centric security models for enterprise web systems. *Saudi J Eng Technol* 11(4):237–246. <https://doi.org/10.36348/sjet.2026.v11i04.008>
17. Khayyam F (2026) Resilient identity and access governance architecture for artificial intelligence-enabled software-as-a-service ecosystems. *Saudi J Eng Technol* 11(4):276–284. <https://doi.org/10.36348/sjet.2026.v11i04.012>

18. Zaman SU (2025) Enhancing security in cloud-based IAM systems using real-time anomaly detection. IJSRED - Int J Sci Res Eng Dev 8(6):2292–2304.
<https://doi.org/10.5281/zenodo.17926883>
19. Mim MA (2026) Cybersecurity risk mitigation in educational and healthcare IT environments. Zenodo. <https://doi.org/10.5281/zenodo.18988585>
20. Nahar S, Rahman M, Alam MS, Al Sany SMA (2026) Intelligent data governance and ethical AI framework for enterprise information systems. Zenodo. <https://doi.org/10.5281/zenodo.18839122>
21. Shaik MH (2026) Secure and compliant DevSecOps architecture for automated CI/CD pipelines in regulated cloud environments. Zenodo. <https://doi.org/10.5281/zenodo.19442346>
22. Junaid E (2026) Secure Kubernetes platform engineering for EKS and GKE: Helm-based standardization and runtime governance. Zenodo. <https://doi.org/10.5281/zenodo.19483524>
23. Siddiki A (2026) Adaptive Cloud-Native Migration Framework for Secure Enterprise Financial Systems Using OpenShift and Distributed Microservices. Zenodo.
<https://doi.org/10.5281/zenodo.20070714>
24. Khayyam F (2026) Scalable trust and auditability for generative AI in enterprise CRM platforms: A framework and reference architecture. Zenodo. <https://doi.org/10.5281/zenodo.19607181>
25. Alam MJ (2026) March 11). Digital compliance management systems for regulatory documentation and risk monitoring in organizational operations. SSRN Electron J.
<https://doi.org/10.2139/ssrn.6410539>

Figures

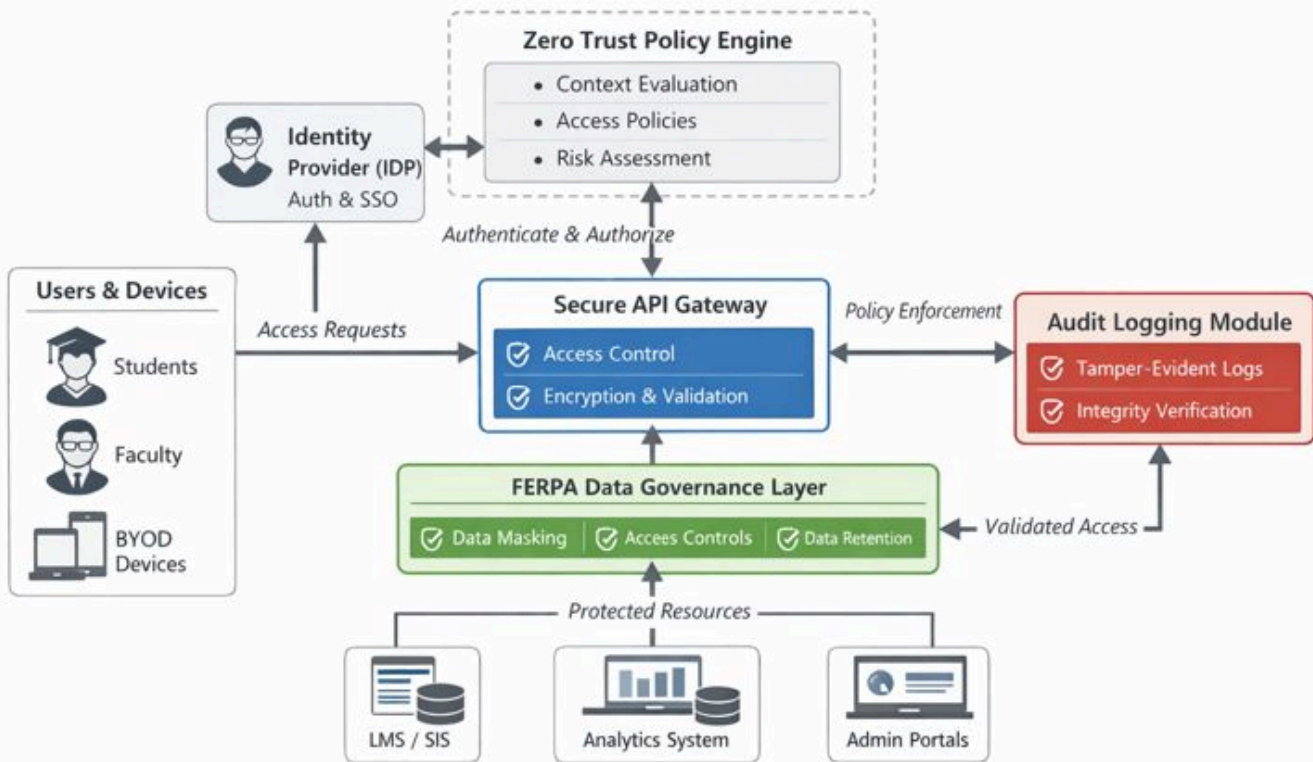


Figure 1. Zero Trust Security Architecture for Higher Education Web Systems

Figure 1

Zero Trust Security Architecture for Higher Education Web Systems

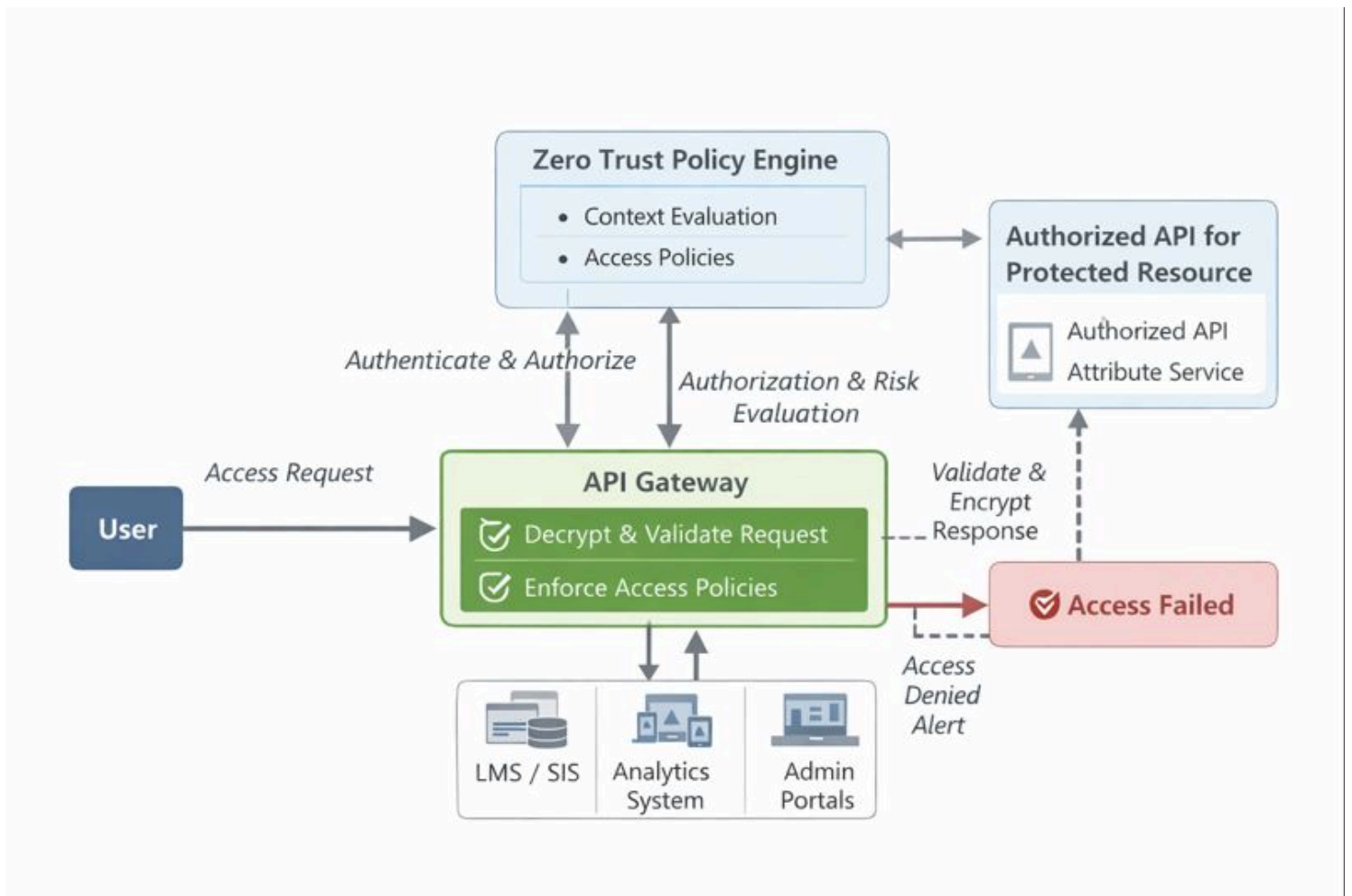


Figure 2

Secure API request flow with policy enforcement.

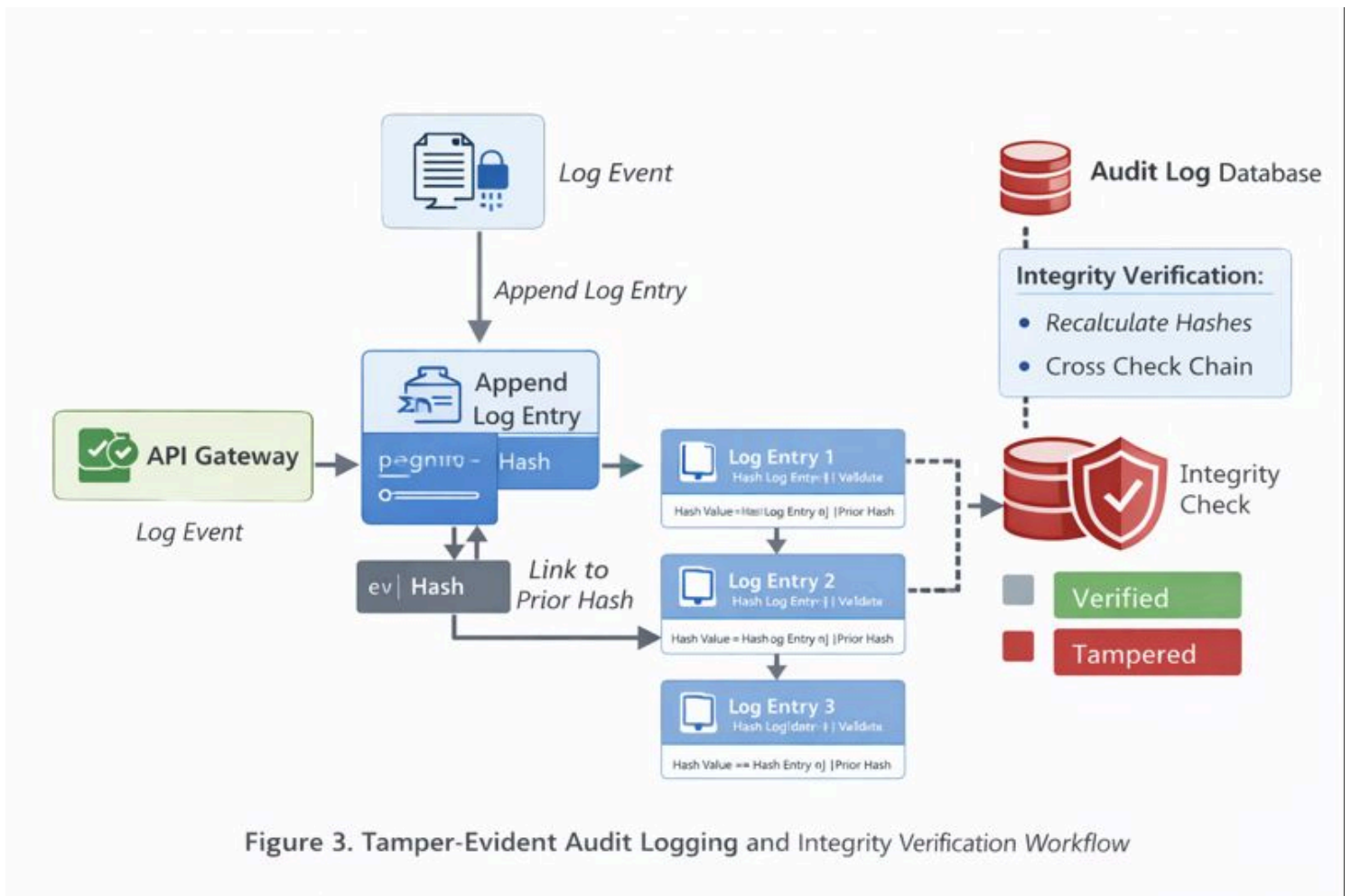


Figure 3

Tamper-Evident Audit Logging and Integrity Verification Workflow

FERPA Compliance Coverage Before and After Zero Trust Implementation

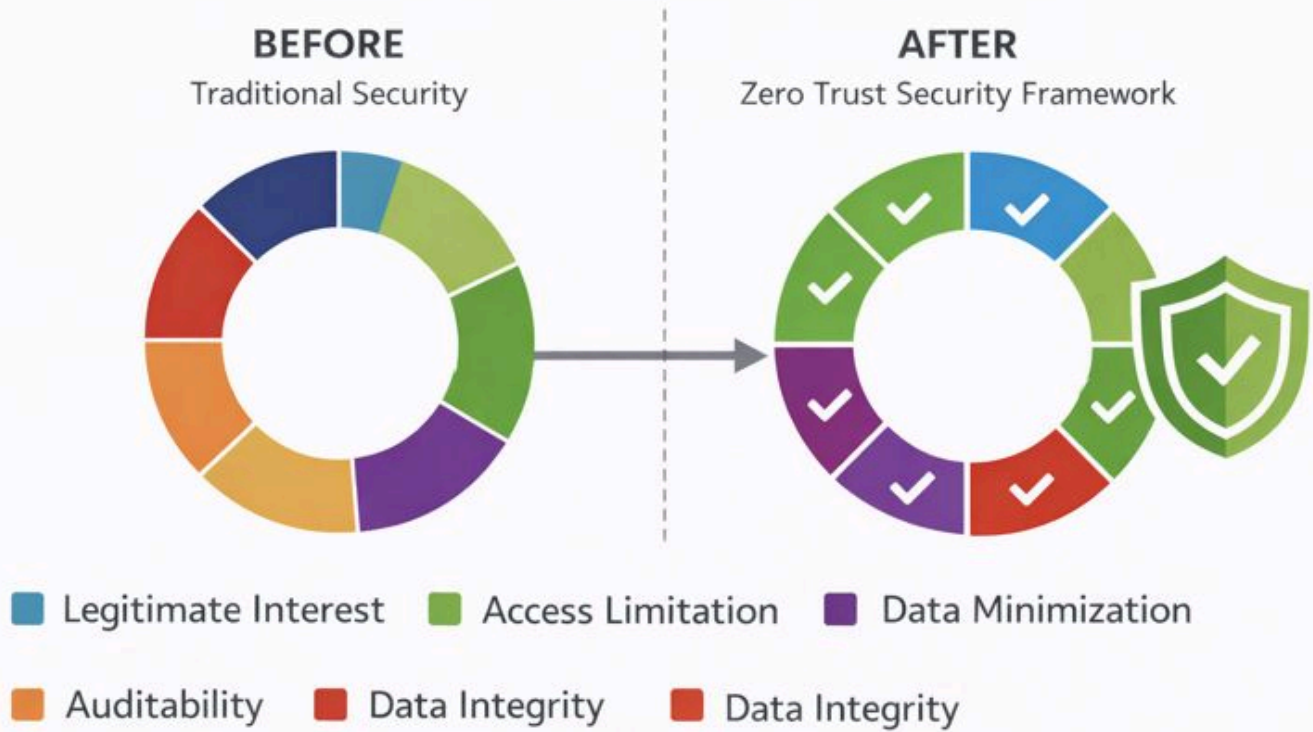


Figure 4

FERPA Compliance Before and After Zero Trust Implementation