Recibido: 05-05-2025 / Revisado: 01-08-2025
Aceptado: 04-08-2025 / Publicado: 31-01-2026

Cybersecurity in educational platforms: threats, challenges, and best practices

Ciberseguridad en las plataformas educativas: amenazas, desafíos y mejores prácticas

Juan Carlos Castro-Ortiz[1,2], Francisco José Martínez-López[1]

[1] University of Huelva, Spain
[2] CISO and Head Of Cybersecurity, Spain

juancarlos.castro@alu.uhu.es , francis@uhu.es

ABSTRACT. Los ciberataques a instituciones educativas públicas son cada vez más frecuentes, poniendo en riesgo grandes volúmenes de datos sensibles. La información personal, los registros académicos e incluso los datos financieros suelen quedar expuestos a ransomware, brechas de seguridad y interrupciones del servicio. A pesar de esta amenaza creciente, muchas plataformas operan con medidas de seguridad obsoletas o carecen de una estrategia de protección bien definida debido a limitaciones presupuestarias y técnicas.

En este estudio, adoptamos un enfoque estructurado para evaluar la seguridad de las plataformas educativas. Nuestro análisis destaca vulnerabilidades clave en la seguridad de las aplicaciones, en la implementación de criptografía y en los entornos contenedorizados. Además, evaluamos el Acceso a la Red de Confianza Cero (ZTNA, por sus siglas en inglés) como una alternativa viable a los marcos de seguridad tradicionales. A diferencia de las estrategias de seguridad aisladas, este trabajo integra múltiples capas de protección en un modelo integral que mejora la seguridad en entornos educativos.

Para abordar estas deficiencias, este estudio proporciona una lista de verificación de ciberseguridad diseñada específicamente para plataformas educativas. Este marco ofrece recomendaciones prácticas sobre desarrollo seguro de aplicaciones, buenas prácticas criptográficas, refuerzo de infraestructura y mecanismos de control de acceso. Al implementar estas medidas, las plataformas educativas pueden mejorar su postura de ciberseguridad, mitigar amenazas emergentes y establecer un modelo de seguridad estructurado que se alinee con las mejores prácticas del sector y los requisitos regulatorios, garantizando una resiliencia digital a largo plazo en el sector educativo.

RESUMEN. Cyberattacks on public educational institutions are becoming more frequent, putting large volumes of sensitive data at risk. Personal information, academic records, and even financial details are often exposed to ransomware, data breaches, and service disruptions. Despite this growing threat, many platforms operate with outdated security measures or lack a well-defined protection strategy due to budget limitations and technical constraints.

In this study, we take a structured approach to evaluate the security of educational platforms. Our analysis highlights key vulnerabilities in application security, cryptographic implementations, and containerized environments. Furthermore, we assess Zero Trust Network Access (ZTNA) as a viable replacement for traditional security frameworks. Unlike isolated security strategies, this work integrates multiple security layers into a comprehensive model that enhances protection in educational settings.

To address these deficiencies, this study provides a cybersecurity checklist tailored for educational platforms. This framework offers actionable guidance on secure application development, cryptographic best practices, infrastructure hardening, and access control mechanisms. By implementing these measures, educational platforms can enhance their cybersecurity posture, mitigate evolving threats, and establish a structured security model that aligns with industry best practices and regulatory requirements, ensuring long-term digital resilience in the education sector.

KEYWORDS: Cybersecurity, Educational platforms, Moodle, Risk assessment.

PALABRAS CLAVE: Ciberseguridad, Plataformas educativas, Moodle, Evaluación de riesgos.

Castro-Ortiz, J. C.; Martínez-López, F. J. (2026). Cybersecurity in educational platforms: threats, challenges, and best practices. *Campus Virtuales*, 15(1), 191-213. https://doi.org/10.54988/cv.2026.1.1700

1. Introduction

The increasing reliance of educational platforms like Moodle has made them prime targets for sophisticated cyberattacks. These platforms manage vast amounts of sensitive data, including personally identifiable information (PII), academic records, and financial transactions, making them highly attractive to cybercriminals. As a result, ransomware incidents, data breaches, and denial-of-service (DoS) attacks have surged, often leading to severe operational disruptions.

A primary cause of these security weaknesses is the over-reliance on regulatory compliance frameworks, such as ISO 27001, which focus on policy enforcement rather than technical security implementations. While these certifications provide a baseline for security governance, they fail to guarantee actual protection against evolving cyber threats. Recent reports indicate that the education sector has experienced a 75% year-over-year increase in cyberattacks, averaging 3,574 attacks per week, primarily due to outdated infrastructure, unpatched vulnerabilities, and reliance on third-party integrations with minimal security oversight (Checkpoint, 2025).

Moreover, cybercriminals increasingly exploit these gaps to exfiltrate sensitive data, disrupt platform operations, and demand hefty ransoms, further straining already limited IT funds. As highlighted by Microsoft, "attackers focus on exploiting these vulnerabilities to steal sensitive data, disrupt operations, and demand hefty ransoms, further crippling already strained IT budgets" (Microsoft, 2024). Given the increasing sophistication of cyber threats, educational institutions must transition from reactive security postures to proactive, risk-based defense strategies.

This study introduces a multi-layered security assessment framework, integrating Static and Dynamic Application Security Testing (SAST & DAST), cryptographic evaluations, container audits, and Zero Trust Network Access (ZTNA). Unlike previous studies that focus exclusively on compliance adoption or isolated security techniques, this research presents a comprehensive empirical analysis of real-world vulnerabilities in educational platforms.

To bridge the gap between regulatory compliance and actual security effectiveness, this study also introduces a Self-Diagnosis Checklist (Appendix A), a risk-weighted assessment tool that quantifies security deficiencies often overlooked in conventional audits. By providing actionable insights based on empirical security evaluations, this checklist enables institutions to prioritize technical remediations beyond compliance-driven security models.

2. Literature review

La This study has examined and compared 23 prior research efforts on cybersecurity in the educational sector. While these studies have addressed key aspects such as vulnerabilities, compliance, and threat management, most adopt fragmented approaches that fail to provide a comprehensive security perspective.

Unlike previous research, this study introduces a multi-layered security framework that integrates several critical domains. It encompasses security assessment across multiple layers, ensuring a thorough evaluation of risks from different perspectives. Additionally, it strikes a balance between regulatory compliance and technical security implementation, aligning with established standards such as ISO 27001 and NIST CSF.

A fundamental component of this framework is the adoption of Zero Trust Network Access (ZTNA) to enhance segmentation and access control, minimizing the attack surface. Risk prioritization is reinforced through the MITRE ATT&CK framework, providing a structured approach to identifying and mitigating threats based on their real-world impact.

Furthermore, the study emphasizes the protection of containerized and server environments, addressing vulnerabilities specific to deployment infrastructures. AI-powered threat detection is also incorporated as a key element, enabling proactive identification and response to evolve cyber threats. Lastly, a comprehensive

Castro-Ortiz, J. C.; Martínez-López, F. J. (2026). Cybersecurity in educational platforms: threats, challenges, and best practices. *Campus Virtuales,* 15(1), 191-213. https://doi.org/10.54988/cv.2026.1.1700

cybersecurity diagnostic checklist has been developed to offer an actionable tool for assessing and improving the security posture of educational platforms.

By integrating all these elements, this study presents the most comprehensive cybersecurity framework to date, bridging the gap between risk assessment and the practical implementation of robust security measures to protect educational institutions from emerging threats.

3. Methodology

This study employs a multi-layered security methodology to provide a comprehensive risk assessment of public educational platforms. Unlike traditional compliance-based evaluations, this approach integrates both technical security controls and strategic security governance. The methodology encompasses automated security testing, manual penetration testing, cryptographic analysis, network security assessments, and infrastructure auditing to capture a holistic view of security risks. The approach follows established cybersecurity frameworks, including Zero Trust Network Access (ZTNA), identity-based access controls, and MITRE ATT&CK-based risk assessment methodologies, ensuring a structured and reproducible security analysis.

The study focused on five virtual campuses, selected based on infrastructure complexity, third-party integrations, and operational scale. Security assessments were conducted through direct evaluations of authentication mechanisms, access control models, and exposure to common attack vectors. Meetings were held with security directors and IT administrators to analyse platform configurations and review known security challenges. Due to confidentiality agreements under the National Security Framework (ENS) in Spain, specific results and identifying information remain undisclosed.

Security Evaluation Techniques Overview

The methodology integrated automated scanning tools and manual security validation techniques to conduct a comprehensive security assessment across multiple infrastructure layers. The evaluation encompassed SAST, DAST, Zero Trust security evaluations, cryptographic analysis, container and server security assessments, and infrastructure audits, as illustrated in Figure 1. This step-by-step approach identifies and mitigates vulnerabilities effectively, following a structured path.

Figure 1 outlines the nine key stages of the security assessment methodology, beginning with Static Application Security Testing (SAST) and concluding with Advanced Monitoring. This visual representation highlights the interconnectedness of each stage, ensuring a holistic evaluation of security controls.

The findings from these evaluations were systematically mapped against ISO 27001, NIST CSF, and MITRE ATT&CK, aligning the results with industry best practices. To provide a structured measurement of security effectiveness, a Self-Diagnosis Checklist (Appendix A) was introduced as a practical tool for institutions to measure and improve their security posture. Unlike conventional compliance frameworks, this checklist translates security gaps into actionable insights, allowing institutions to prioritize critical vulnerabilities and track improvements over time.

By integrating this checklist into routine cybersecurity audits, educational platforms can establish a continuous security monitoring approach, moving beyond one-time compliance checks.

Security assessments were conducted across multiple public educational institutions, ensuring diverse deployment environments were analysed. The results were aggregated and anonymized, providing a comparative evaluation of security maturity trends while preserving institutional confidentiality. Any additional data requests must comply with Non-Disclosure Agreements (NDAs) with the respective institutions.

This structured methodology, illustrated in Figure 1, ensures a rigorous, reproducible, and quantifiable assessment of cybersecurity in educational platforms, addressing both policy-based compliance and technical security enforcement.

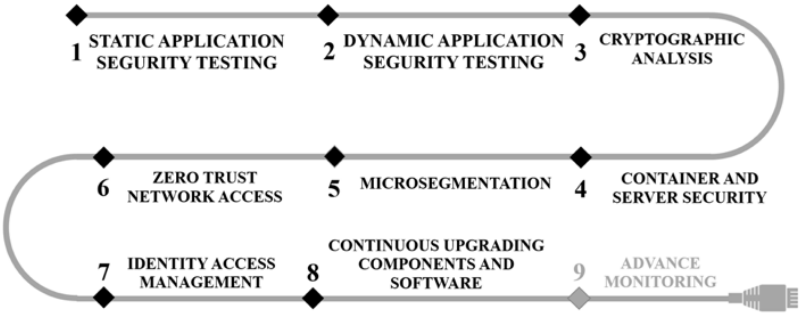

Figure 1. AST reviewing methodology developed by the author. Source: Own elaboration.

3.1. Static Application Security Testing (SAST)

Static Application Security Testing (SAST) is a critical approach for identifying vulnerabilities in educational platforms by analysing their source code. Given the complexity of reviewing thousands of lines of code manually, specialized tools are indispensable for effective SAST execution. As defined in recent research, "SAST tools are defined as a set of techniques that analyse the source code scan without having to execute the code, operating as a white-box approach. They can identify potential errors present in the code, code smells, and security vulnerabilities" (Herrera Jerónimo Adrián, 2024). These tools help trace application inputs, intermediate code changes, and outputs to ensure that vulnerabilities do not emerge at any stage.

3.1.1. Specialized Tools for SAST

Specialized tools for SAST have evolved to become indispensable in modern security workflows. "SAST tools have evolved significantly over time, moving from small lexical analyses to a set of complex techniques that allow for more sophisticated and comprehensive feedback" (Herrera Jerónimo Adrián, 2024). Today, leading solutions such as Veracode, Checkmarx, Synopsys, or Snyk efficiently detect vulnerabilities, streamline code analysis, and align with Common Weakness Enumeration (CWE) standards.

3.1.2. Selection Guidance

Choosing the right tool is essential for achieving comprehensive coverage. It is recommended to consult industry frameworks like the Forrester Wave or Gartner Magic Quadrant, which provide insights into the strengths and weaknesses of various solutions. This ensures that the chosen tool aligns with the institution's specific requirements.

3.1.3. Key Focus Areas

SAST tools focus on:

1. Input Traceability: Ensuring that all inputs are sanitized to prevent injection attacks.
2. Intermediate Code Changes: Analysing transformations within the application to detect potential vulnerabilities.
3. Output Validation: Verifying that sensitive data is not exposed or mishandled.

3.1.4. Common CWE Vulnerabilities in Static Analysis in Educational platforms

The vulnerabilities detected through SAST are as diverse as the 900+ entries listed in the CWE database. However, the most common issues in static analysis for educational platforms include:

1. CWE-79: Cross-Site Scripting (XSS)
2. CWE-89: SQL Injection
3. CWE-22: Path Traversal
4. CWE-200: Information Exposure
5. CWE-732: Incorrect Permission Assignment
6. CWE-611: XML External Entity (XXE)
7. CWE-327: Use of a Broken or Risky Cryptographic Algorithm
8. CWE-918: Server-Side Request Forgery (SSRF)
9. CWE-502: Deserialization of Untrusted Data
10. CWE-94: Code Injection

3.1.5. Challenges in SAST Implementation

While SAST provides extensive benefits, its adoption comes with challenges such as false positives, where the analysis may flag non-critical issues as vulnerabilities, creating noise for developers. Additionally, scalability can be a concern for platforms with extensive customizations, such as Moodle plugins. Furthermore, coverage limitations mean certain vulnerabilities, like logic flaws, may not be detected solely through static analysis, necessitating complementary testing methods.

Despite these challenges, SAST remains invaluable for early detection of vulnerabilities. As highlighted in research, "The SAST scan can detect vulnerabilities early in the software development process and can be initiated as soon as the code is considered feature complete" (Yusof Darus Mohamad, 2023). By integrating SAST during the initial phases of software development, educational institutions can proactively address security issues and significantly reduce the attack surface of their platforms. However, it is essential to complement these findings with dynamic testing approaches to achieve a comprehensive security posture.

Specific SAST Methodology Proposed

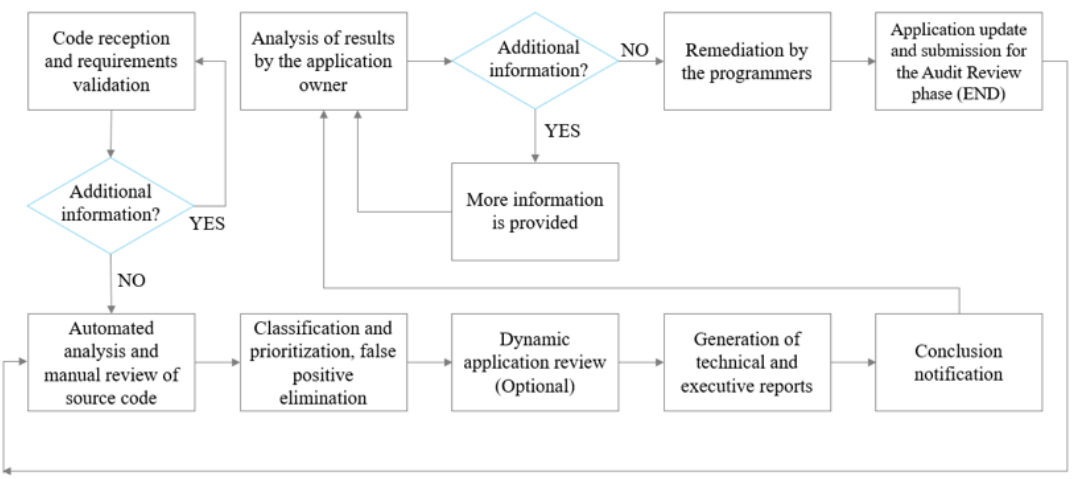

Figure 2. Methodological Diagram Proposed and Designed by the Author. Source: Own elaboration.

The methodology outlined in the diagram (Figure 2) is specifically designed to address Common Weakness Enumeration (CWE) vulnerabilities detected by automated security tools. It emphasizes the need for specialized team and qualified vendor support to ensure accurate detection, classification, and remediation of these vulnerabilities. Below is a detailed explanation of each step:

1. Code Reception and Requirements Validation

This initial phase involves collecting the full source code of the application, including all its dependencies.

This step is crucial as it ensures a comprehensive scope of analysis. Additionally, a detailed inventory of the programming languages used in the application is created, which may include PHP, Java, Python, JavaScript, or others. This information is fundamental for tailoring the security assessment to the application's architecture and aligning it with industry standards like OWASP or CWE.

2. Automated and Manual Source Code Review
Automated tools are used to identify vulnerabilities related to CWE categories like SQL Injection or Cross-Site Scripting (XSS). Additionally, manual reviews are conducted by experts to identify complex flaws not detectable by automated methods.

3. Classification and Prioritization of Vulnerabilities
Vulnerabilities are classified according to their severity, exploitability, and potential impact. This stage requires advanced knowledge of CWE classifications to eliminate false positives and streamline the remediation process.

4. Optional Dynamic Application Review
Dynamic testing complements static analysis by simulating runtime attack scenarios. This step is optional but critical for identifying vulnerabilities that manifest only during application execution.

5. Analysis of Results by the Application Owner
The application owner evaluates the findings to determine if additional clarification or context is needed. If so, the team loops back to collect more information or refine the analysis.

6. Remediation by Programmers
A specialized development team, often supported by the vendor, works on resolving vulnerabilities, focusing on the most critical issues first. This includes implementing secure coding practices and adhering to CWE remediation guidelines.

7. Audit Review and Reporting
The updated application undergoes a final audit review, ensuring all vulnerabilities have been addressed. Comprehensive technical and executive reports are generated to document findings, remediation efforts, and residual risks.

8. Conclusion Notification
The process concludes with a formal notification, confirming the application's compliance with predefined security standards.

This proposed methodology provides a structured approach that leverages specialized expertise and advanced tools to ensure a thorough and effective assessment of security vulnerabilities.

3.2. Dynamic Application Security Testing (DAST)

Static Application Security Testing (SAST) plays a crucial role in securing educational platforms by analysing their source code before execution. This white-box approach enables security teams to detect vulnerabilities early in the development process, making it a valuable tool for preventing security flaws before deployment. However, SAST has inherent limitations, as it focuses on code-level weaknesses but cannot identify security flaws that manifest only during runtime, such as session mismanagement, authentication weaknesses, or insecure API interactions.

To address these gaps, Dynamic Application Security Testing (DAST) offers a complementary approach by assessing applications during execution. Unlike SAST, which strictly analyzes source code, DAST simulates real-world attack scenarios, interacting with the application just as an attacker would. As (Brown, 2024)

describes.

"DAST is a methodology to assess the security of web applications and APIs while running. Unlike Static Application Security Testing (SAST), which analyzes the application's source code", DAST examines the application by interacting with the application in real time, mimicking the behaviour of an attacker. This allows DAST tools to identify runtime vulnerabilities." This makes DAST particularly effective in detecting authentication flaws, session hijacking risks, and improper data exposure, which are often missed by static analysis alone. By integrating both SAST and DAST, educational institutions can achieve a more robust security posture, mitigating risks at both the code and runtime levels.

3.2.1. Specialized Tools for DAST

The following tools are widely used in dynamic testing: OWASP ZAP, Burp Suite, Acunetix, or Netsparker, for example. These tools simulate real-world attack scenarios, such as injection attacks, cross-site scripting (XSS), and misconfigured authentication. By interacting with the live application, DAST tools provide a more comprehensive view of the security posture.

These tools simulate real-world attack scenarios, such as injection attacks, cross-site scripting (XSS), and misconfigured authentication. By interacting with the live application, DAST tools provide a more comprehensive view of the security posture.

3.2.2. Selection Guidance

To select the most effective DAST tool, institutions should consider factors such as scalability, ease of integration with CI/CD pipelines, and reporting capabilities.

3.2.3. 2Key Focus Areas

DAST tools concentrate on identifying authentication flaws, including weak or misconfigured authentication mechanisms. They also detect session management vulnerabilities, such as improper session handling, session fixation, or lack of secure cookies. Additionally, they evaluate runtime data exposure, assessing how sensitive information is handled during application execution.

3.2.4. Common CWE Vulnerabilities in Dynamic Analysis

The most frequently encountered vulnerabilities in DAST for educational platforms includes:

1. CWE-352: Cross-Site Request Forgery (CSRF)
2. CWE-601: Open Redirects
3. CWE-119: Buffer Overflow
4. CWE-287: Improper Authentication
5. CWE-384: Session Fixation
6. CWE-502: Deserialization of Untrusted Data
7. CWE-307: Improper Restriction of Excessive Authentication Attempts
8. CWE-613: Insufficient Session Expiration
9. CWE-640: Weak Password Recovery Mechanism
10. CWE-311: Missing Encryption of Sensitive Data

3.2.5. Challenges in DAST Implementation

Despite its advantages, implementing DAST presents several challenges. One of the primary concerns is performance impact, as testing on live systems may affect application performance. Additionally, while false positives are fewer compared to SAST, dynamic analysis requires the technical expertise of a skilled Red Team professional to validate findings and effectively uncover nuanced vulnerabilities. DAST is most effective when integrated as part of a broader security testing strategy within the software development lifecycle (SDLC). As

noted in research, "The testing phase under a secured SDLC will in-volve a series of scans including SCA, Interactive Application (binary) Security Testing (IAST), Dynamic Application (binary) Security Testing (DAST), and Penetration Test to make sure no severe bugs make it to production" (Chen, 2022). Lastly, coverage limitations remain a challenge, as some vulnerabilities may only surface under specific conditions, necessitating extensive testing scenarios.

By incorporating DAST into their security practices, educational institutions can uncover runtime vulnerabilities and ensure robust application security. However, combining DAST with SAST provides a more comprehensive approach to safeguarding educational platforms.

3.3. Cryptographic Analysis

Cryptographic analysis is a cornerstone of securing educational platforms, as it ensures the confidentiality, integrity, and authenticity of sensitive data exchanged within the system. "Cryptography involves using code to secure data and communications, allowing only the intended recipient to read them. Conventional cryptography algorithms and ciphers enable both the encryption and decryption of data" (Iffath Tanjim Moon, 2023). In this study, cryptographic implementations were evaluated to verify compliance with industry standards such as TLS 1.3 and robust encryption protocols like AES-256.

3.3.1. Tools for Cryptographic Analysis

The following tools were employed to assess cryptographic protocols and configurations:

- Qualys SSL Labs: Used to audit SSL/TLS configurations and identify misconfigurations or vulnerabilities, such as the use of outdated protocols (e.g., SSL 3.0, TLS 1.0).
- OpenSSL: Utilized to verify the strength and correctness of cryptographic implementations, including key lengths and algorithm usage.

3.3.2. Key Focus Areas

1. SSL/TLS Configurations:
Ensuring proper implementation of TLS 1.3, the latest and most secure protocol version, to prevent eavesdropping and man-in-the-middle (MITM) attacks.
Detecting weak cipher suites and protocols that could compromise the security of communication channels.

2. Certificate Validation:
Verifying that SSL certificates are properly issued, valid, and not self-signed unless explicitly required.
Identifying the use of weak certificate signatures, such as SHA-1, which has been deprecated.

3. Data Encryption Standards:
Ensuring that sensitive data, such as user credentials and financial transactions, is encrypted using robust algorithms like AES-256 and RSA-2048.

4. Key Management Practices:
Evaluating the storage, rotation, and lifecycle management of encryption keys is critical to ensuring secure operations in educational platforms. Best practices involve the proper handling of cryptographic keys throughout their lifecycle, from generation to secure destruction. "NIST SP 800-57 is a standard from the National Institute of Standards and Technology (NIST) that provides guidelines and recommendations for cryptographic key management. This standard encompasses the entire key lifecycle, from generation, distribution, storage, and usage to destroying cryptographic keys, ensuring their security and integrity" (Nasywa Rayhan Brian, 2024). Adherence to such standards helps prevent unauthorized access, mitigates risks of key misuse, and ensures that encryption mechanisms remain robust and effective.

3.3.3. Common Cryptographic Vulnerabilities

Cryptographic weaknesses identified in educational platforms often align with CWE entries. Key vulnerabilities include:

1. CWE-319: Cleartext Transmission of Sensitive Information.
2. CWE-326: Inadequate Encryption Strength.
3. CWE-295: Improper Certificate Validation.
4. CWE-310: Cryptographic Issues.
5. CWE-331: Insufficient Entropy in Cryptographic Algorithms.
6. CWE-328: Reversible One-Way Hash.
7. CWE-345: Insufficient Verification of Data Authenticity.

3.3.4. Challenges in Cryptographic Implementation

While modern cryptographic standards provide robust security, their effectiveness is highly dependent on proper implementation. Misconfigurations, insecure protocol usage, and poor key management practices often introduce vulnerabilities that can be exploited by attackers. "Cryptographic implementation errors in popular open-source libraries (e.g., OpenSSL, GnuTLS, BotanTLS, etc.) and the misuses of cryptographic primitives have been the major source of vulnerabilities in the wild" (Yao, 2017).

Backward compatibility also remains a challenge, as maintaining support for older clients can lead to the retention of deprecated protocols and weaker cipher suites, undermining security. Additionally, improper handling of encryption keys—such as storing them in plaintext—remains one of the most critical vulnerabilities affecting cryptographic security.

Importance of Cryptographic Analysis

A thorough cryptographic analysis mitigates risks associated with data exposure, interception, and manipulation. Educational platforms, which handle sensitive student and institutional data, must prioritize strong encryption practices and regular audits to maintain trust and compliance with regulatory standards.

3.4. Risk Assessment with the MITRE Calculator

Effective cybersecurity management requires prioritizing vulnerabilities to allocate resources efficiently. The MITRE Risk Calculator (MRC) serves as a robust tool for assessing and quantifying risks, enabling educational institutions to adopt a proactive approach in securing their platforms. "The risk assessment of the system is to quantify the possibility of attack on the system through the algorithm used in the risk assessment model, so as to objectively analyse the weaknesses of the system and realize risk early warning" (Li, 2021). By converting these factors into measurable risk scores, institutions can focus on addressing high-priority vulnerabilities first.

3.4.1. Key Features and Methodology

The MRC evaluates risks based on several parameters, such as threat likelihood, impact, and exposure level. By converting these factors into measurable risk scores, institutions can focus on addressing high-priority vulnerabilities first. This tool integrates seamlessly with frameworks like Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) to ensure a comprehensive evaluation.

3.4.2. Application in Educational Platforms

The MRC is highly applicable to educational platforms like Moodle, where sensitive data and diverse user bases require rigorous security. By leveraging this tool, institutions can identify critical threats such as SQL injection or improper access control, focusing on the most impactful risks. The tool also supports contextual risk analysis, taking into account user behaviour, network configurations, and platform dependencies, enabling

a tailored approach to vulnerability management. Furthermore, it helps optimize resource allocation, allowing IT teams to focus on the most pressing issues, improving efficiency and security outcomes.

3.4.3. Advantages for Educational Institutions

Educational institutions benefit significantly from using the MITRE Risk Calculator due to its ability to enhance decision-making through a quantitative approach. "By lever-aging the structured representation of attack trees and the wealth of knowledge in the MITRE framework, informed decisions can be taken in a systematic way such that organizations optimize their security strategies and bolster their overall cybersecurity resilience" (Husseis Anas, 2023). By removing ambiguity, institutions can develop clear and data-driven strategies that prioritize the highest-impact risks and ensure compliance with regulatory standards such as ISO 27001 and GDPR.

3.4.4. Challenges and Mitigation Strategies

Despite its benefits, effective use of the MITRE Risk Calculator requires technical expertise and accurate data input. This can pose challenges for institutions with limited IT resources or knowledge gaps. To overcome these challenges, it is essential to provide targeted training for IT and security staff, ensuring they can maximize the tool's potential. "By applying our methodology to a specific SDVN use case, we effectively identified and mitigated potential attack vectors" (Wissem Chorfa, 2023). Additionally, institutions should establish processes to regularly update vulnerability databases and contextual information, maintaining the accuracy and relevance of risk assessments over time.

3.5. Container and Server Security

The increasing reliance on containerized environments for deploying educational platforms has introduced both opportunities and challenges in cybersecurity. Containers, while efficient and scalable, require robust security practices to prevent exploitation.

3.5.1. Tools for Container and Server Security

To assess the security of containerized and server infrastructures, several tools were utilized. Docker Bench for Security is an automated script designed to check for best practices and common security misconfigurations in Docker environments. Kubebench evaluates Kubernetes clusters against the Center for Internet Security (CIS) benchmarks to ensure compliance with established security standards. Aqua Security provides runtime protection and vulnerability scanning for containers, adding an additional layer of defense. Finally, Falco monitors containerized environments in real time, detecting unexpected behaviours and potential threats.

"Mitigating security risks by integrating Linux Security Modules (LSMs) with suitable profiles has emerged as a promising approach to enhance Docker's security. Additionally, cloud orchestration tools like Ansible, Puppet, and Chef are explored to streamline secure container deployment at scale" (Mandela, 2023). Combining these tools with automated vulnerability scanning and real-time security monitoring can significantly reduce the risk of misconfigurations and unauthorized access, ensuring a more resilient containerized infrastructure for educational platforms.

Furthermore, research on lightweight container security frameworks emphasizes the importance of trusted computing, transparent encryption, and microservice isolation to mitigate container escape attacks and prevent privilege escalation. A lightweight container security enhancement framework, based on hardware virtualization isolation, cloud trust, and transparent encryption and decryption of container data, has been proposed to strengthen container security in cloud-native environments (Wei Liu, 2021). This approach strengthens security boundaries while maintaining performance efficiency, making it an essential consideration for modern cloud-native environments.

3.5.2. Key Focus Areas

1. Container Hardening: Ensuring that containers run with the least privileges necessary, disabling unnecessary capabilities, and using minimal base images to reduce the attack surface.
2. Network Segmentation: Configuring container networks to restrict unnecessary communication between containers and external entities.
3. Monitoring and Logging: Enabling detailed logging to detect suspicious activity, such as privilege escalation or unauthorized API calls, and monitoring runtime behaviour using tools like Falco to identify anomalous activities.
4. Server Security and Bastioning: Applying operating system hardening techniques, such as disabling unused services and applying security patches promptly and configuring firewalls and intrusion detection/prevention systems to secure server environments.

3.5.3. Common Vulnerabilities in Containers and Servers

The following vulnerabilities were frequently observed during the assessment:

1. CWE-798: Use of Hardcoded Credentials.
2. CWE-77: Improper Neutralization of Commands in Shells.
3. CWE-502: Deserialization of Untrusted Data.
4. CWE-94: Improper Control of Code Generation.
5. CWE-20: Improper Input Validation.

3.5.4. Challenges in Securing Containers and Servers

Securing containers and orchestrators, such as Kubernetes, presents several challenges. One key issue is complexity, as securing these environments requires specialized knowledge, which can be a significant barrier for institutions with limited IT resources. Additionally, the dynamic nature of containers makes tracking vulnerabilities and applying patches a continuous effort. As highlighted in research, "If a zero-day vulnerability is released to the public, its exploitability risk increases since attackers are likely to use it to attack vulnerable systems." (Roumani, 2021). This is particularly concerning in containerized environments where unpatched vulnerabilities in base images or orchestration misconfigurations can introduce severe security gaps. Lastly, misconfigurations pose a critical risk; for instance, simple oversights, such as exposing the Docker daemon to the internet, can result in severe security breaches.

3.5.5. Server Security

Securing containers and servers is a critical component of a holistic cybersecurity strategy. Educational platforms, which often operate in multi-tenant environments, must prioritize container and server security to protect sensitive data and maintain system integrity. Regular audits, adherence to CIS benchmarks, and leveraging real-time monitoring tools can significantly reduce risks. With the growing use of containers in deploying educational platforms, this study assessed Docker and Kubernetes environments using tools like Docker Bench for Security and Kubebench. Key findings included misconfigured container privileges, exposed APIs, and insufficient monitoring of server activities.

3.6. Zero Trust Implementation: A Modern Framework for Educational Security

The limitations of VPNs in educational environments are increasingly evident, as these tools are cumbersome, provide insufficient security, and fail to meet the demands of modern cloud-centric networks. Zero Trust Network Access (ZTNA) offers a transformative alternative, replacing implicit trust with strict access controls based on identity and context. This model is especially relevant for educational platforms, where secure access to resources across distributed environments is critical.

3.6.1. Why Replace VPNs with ZTNA?

The growing dependence on home networks and personal devices, many of which lack robust security measures, has significantly increased the need for comprehensive cybersecurity frameworks. As a recent report emphasizes, "the increased reliance on home networks and personal devices, which often lack robust security measures, has heightened the need for comprehensive cybersecurity frameworks." (Rey, 2024). This challenge is particularly evident in educational institutions, where outdated VPN setups are still widely used. Traditional VPNs grant users broad access to entire networks once authenticated, creating a large attack surface that is highly vulnerable to breaches and lateral movement by attackers.

In contrast, ZTNA provides a more secure and efficient alternative. "Zero trust (ZT) refers to an evolving cybersecurity concept and model that have emerged in response to the changing nature of cyber threats and network environments. It moves cybersecurity defense from traditional perimeter-based security models to a more dynamic and adaptive security posture, with the premise that implicit trust is never given but needs to be continually assessed" (Zhang, 2025). Unlike perimeter-based security, ZTNA assumes that implicit trust is never granted but must be continually verified, which is particularly crucial in educational environments where access conditions frequently change. By integrating granular, identity-based access controls, institutions can significantly reduce unauthorized access and mitigate the risks associated with compromised credentials or insecure personal devices. Furthermore, ZTNA's seamless integration with multi-cloud environments addresses the growing adoption of cloud-based educational tools, enabling institutions to benefit from both flexibility and enhanced security. By replacing outdated VPN solutions with ZTNA, educational institutions can not only mitigate existing vulnerabilities but also build a more resilient cybersecurity posture that aligns with modern operational demands.

3.6.2. Core Principles of ZTNA

The first step in implementing ZTNA in educational platforms is establishing a microsegmented network. Traditional network architectures, particularly those relying on VPNs, expose entire infrastructures once access is granted, making them vulnerable to lateral movement and privilege escalation. Microsegmentation addresses this risk by isolating workloads and restricting access based on identity, device posture, and contextual policies. This ensures that even if an attacker gains access, they cannot move freely within the system, significantly reducing the attack surface and preventing unauthorized access to critical educational resources. By integrating microsegmentation with Zero Trust, institutions can build a resilient security model, where each access request is verified before granting permissions, rather than assuming implicit trust.

Zero Trust principles redefine network security by eliminating implicit trust, even within the institutional perimeter. Access is granted dynamically based on user roles, device compliance, and predefined security policies. For educational platforms, this ensures that only authenticated and authorized users can access sensitive systems, minimizing risks from compromised credentials or unauthorized devices. Additionally, ZTNA incorporates robust encryption protocols, safeguarding data during transmission and ensuring compliance with educational data protection regulations.

Zero Trust Architecture (ZTA) is a token-based architecture based on the principles of zero trust access or on the concept that nothing can be trusted. ZTA is a set of guidelines that strengthens the security for the design of the systems and operations to protect the assets of an enterprise (Farhan A Qazi, 2022).

The next diagram illustrates the ZTNA authentication and access control process, whether deployed on-premises or in the cloud. The process begins with the registration of applications in the ZTNA Gateway, which acts as a secure intermediary. The ZTNA Broker then establishes a connection with the Identity Access Management (IAM) provider, such as Okta, Azure or Ping Identity, for example, to manage authentication and identity validation.

When a user attempts to access the system, they must first undergo user verification and device validation,

ensuring that only trusted identities and compliant devices can connect. Once verified, the ZTNA Broker authenticates the user through an Identity and Access Management (IAM) system, such as Okta, Azure AD, Ping Identity, etc.

IAM is critical in Zero Trust security, enforcing strict access controls, multi-factor authentication (MFA), and least privilege principles to prevent unauthorized access and privilege escalation. By integrating IAM with ZTNA, educational platforms can dynamically manage identity-based access, monitor authentication attempts, and strengthen protection against credential theft. Once validated, the ZTNA Broker establishes a secure session, granting access only to authorized resources, minimizing exposure, and reducing the risk of lateral movement across the network.

This approach enhances security by eliminating direct user access to applications, ensuring that applications remain undetectable from the internet, and preventing infra-structure from being scanned by attackers. Additionally, it safeguards applications from threat exploitation, reinforcing a Zero Trust security posture. By implementing ZTNA, educational institutions can restrict access to authenticated and validated users while protecting sensitive digital assets from unauthorized exposure (Figure 3).

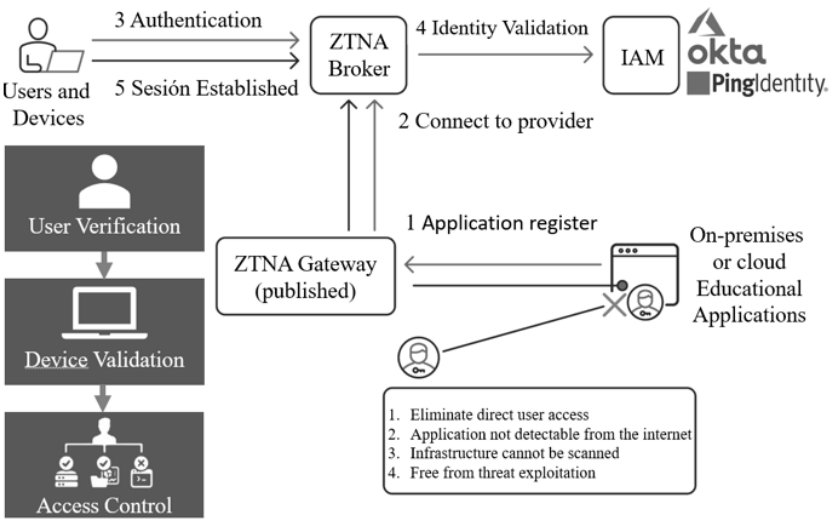

Figure 3. ZTNA Interaction Diagram by the Author. Source: Own elaboration.

3.6.3. Summary of ZTNA Benefits

The application of ZTNA principles in the analysed educational platforms significantly reduced unauthorized access incidents and improved security policy enforcement. The transition from VPN-based access to identity-centric controls minimized attack surfaces, particularly in multi-campus environments. These findings demonstrate that ZTNA not only enhances security but also facilitates compliance with cybersecurity frameworks such as ISO 27001 and NIST CSF. Its first approach encryption protects sensitive academic and administrative data, making it an indispensable component of a holistic cybersecurity strategy for education. The principles of Zero Trust Network Access (ZTNA) were evaluated by simulating case studies where traditional perimeter-based security was replaced with micro-segmentation and identity-based access control. This approach significantly reduced the attack surface and minimized unauthorized access incidents.

3.7. Updating Platform Components

A critical aspect of securing educational platforms involves the continuous monitoring and updating of platform components and containerized environments. Many vulnerabilities stem from outdated dependencies, unpatched software, or misconfigured container systems. Ensuring these are regularly updated and maintained

is essential for mitigating risks.

3.7.1. Component Updates for Platform Security

Regularly scanning and updating platform components is crucial for identifying and remediating vulnerabilities catalogued in databases such as the Common Vulnerabilities and Exposures (CVE). Educational platforms often rely on open-source plugins and libraries, which, if left unpatched, can serve as entry points for attackers. Automated scanning tools enable the detection of outdated dependencies, prioritization of updates based on vulnerability severity, and monitoring of third-party code to maintain a secure software supply chain.

3.7.2. Benefits of Regular Updates

Regular updates significantly reduce the attack surface by patching known vulnerabilities, ensuring compliance with security standards like ISO 27001 and CIS Benchmarks, and enhancing platform performance through improvements in functionality and additional security features.

Regular updates and monitoring are key to strengthening cybersecurity in educational institutions and protecting sensitive data.

4. Results

This section may be divided by subheadings. It should provide a concise and precise description of the experimental results, their interpretation, as well as the experimental conclusions that can be drawn. The evaluation of cybersecurity in public educational platforms confirms that these systems exhibit vulnerabilities commonly recognized in global security frameworks such as the OWASP Top Ten, while also facing additional risks specific to their operational environments. Many platforms remain highly dependent on legacy systems and third-party plugins, which significantly expand the attack surface.

Among the most critical weaknesses are SQL Injection (CWE-89), Cross-Site Scripting (CWE-79), and Improper Input Validation (CWE-20), all of which persist due to inadequate security validation practices. Furthermore, misconfigurations in server setups, unprotected APIs, and insufficient network segmentation further expose these platforms to exploitation. These risks are compounded by the reliance on open-source components, which, in many cases, lack timely security updates.

Beyond these well-documented vulnerabilities, a structured empirical assessment was conducted using the Self-Diagnosis Checklist (Appendix A) to measure the actual implementation of security controls across educational platforms. The checklist highlights systemic weaknesses that extend beyond basic misconfigurations, revealing critical failures in cryptographic management, network segmentation, and access controls.

The Self-Diagnosis Checklist (Appendix A) provides an empirical assessment that quantifies the lack of enforcement of security frameworks in educational platforms. The evaluation highlights areas with particularly low compliance scores, confirming that security weaknesses extend beyond common misconfigurations and into fundamental deficiencies in technical security governance.

Cryptographic key management was one of the weakest areas, with an average compliance of 30 percent, primarily due to poor key rotation policies and insecure storage mechanisms. Network segmentation and Zero Trust implementation scored 35 percent, indicating minimal adoption of microsegmentation and identity-based access controls. Access review and privilege management remained at 40 percent, as many entities failed to conduct periodic audits of user permissions, significantly increasing the risk of unauthorized access escalation. Additionally, injection attack vulnerabilities, including SQL Injection (SQLi) and Cross-Site Scripting (XSS), scored 45 percent, reflecting inadequate input validation in web applications and APIs.

These findings suggest that while many institutions adhere to regulatory frameworks such as ISO 27001 and NIST CSF, their technical implementations often fall short. The Self-Diagnosis Checklist offers a structured approach to identifying these gaps beyond standard compliance audits. With an average cybersecurity compliance score of 52 percent, it becomes evident that certification alone does not guarantee resilience. Future studies should explore how to bridge this gap through continuous validation and adaptive security measures.

Educational platforms like Moodle encounter distinct challenges due to their reliance on open-source components and plugins. These dependencies, frequently outdated and seldom reviewed for vulnerabilities, create multiple entry points for exploitation. Authentication mechanisms and session management protocols often lack adequate security controls, making unauthorized access to sensitive student and institutional data a recurring risk.

Beyond the standard vulnerabilities outlined by OWASP, several additional risks were identified. Many platforms suffer from insecure plugin ecosystems, where plugins lack proper maintenance and remain unpatched for extended periods, creating long-term security risks. Cryptographic practices in these environments are often inadequate, with outdated encryption protocols such as TLS 1.0 still in use, leaving sensitive information vulnerable to man-in-the-middle (MITM) attacks. Unpatched servers and core system components further contribute to the attack surface, as many operating systems and web servers lack timely security updates. Additionally, misconfigured containerized environments frequently provide attackers with excessive privileges, enabling lateral movement within the system.

These findings highlight a recurring pattern of security misconfigurations and outdated components in public institutions, increasing their exposure to cyber threats. Ad-dressing these vulnerabilities requires not only periodic audits but also proactive security reinforcement and real-time threat monitoring to reduce exploitation risks.

5. Navigating the AI revolution in cybersecurity

The integration of Artificial Intelligence (AI) into cybersecurity presents both significant challenges and transformative opportunities. AI is a double-edged sword; while it enhances security measures, it also enables cybercriminals to conduct more sophisticated and automated attacks. Platforms such as ChatGPT, DeepSeek, or Pentest GPT exemplify this duality, being used for both defensive cybersecurity efforts and malicious exploits. As Zhang et al. highlight, "The rapid development of large language models (LLMs) has opened new avenues across various fields, including cybersecurity, which faces an evolving landscape and demand for innovative technologies" (Zhang, 2025). This evolution underscores the increasing reliance on AI-driven security solutions while raising concerns about their potential misuse.

5.1. AI as a Weapon: Emerging Threats

Cybercriminals increasingly leverage AI to bypass security measures and automate attacks at an unprecedented scale. AI-generated phishing emails, AI-driven malware development, and automated vulnerability exploitation are now commonplace.

"The advent of artificial intelligence (AI) tools such as ChatGPT has significantly enhanced security capabilities while also equipping cybercriminals with sophisticated means to launch cyberattacks." (Dingzong Zhang, 2024).

5.2. Some of the key challenges AI presents include:

Automated Exploitation: Tools like Pentest GPT enable rapid identification of vulnerabilities, which, if used maliciously, can facilitate large-scale attacks. AI-driven cyber threats can continuously learn and modify their behaviour in real time to avoid detection. Additionally, AI-generated messages closely mimic legitimate communication, making phishing attacks harder to detect and mitigate. Platforms like DeepSeek, which has

demonstrated superior performance in programming and mathematics, can also be leveraged for cybersecurity research, both ethical and malicious. Although DeepSeek operates within regulatory constraints, its pure reinforcement learning model introduces new challenges regarding oversight and control.

5.3. AI for Ethical Cybersecurity: Strengthening Defenses

While AI presents risks, it also enables cybersecurity professionals to bolster their defenses. By automating repetitive security tasks and enhancing threat detection, AI significantly improves response times and overall security posture.

"Large language models (LLMs) like ChatGPT have exhibited remarkable advancements in software engineering tasks such as code review and vulnerability detection." (Fu Michael, 2023).

5.4. Some key benefits include:

- Automated Threat Analysis: AI enhances real-time log analysis, detecting attack patterns and facilitating proactive defense.
- Vulnerability Identification: AI-powered penetration testing tools can simulate attacks, helping organizations address security gaps before they are exploited.
- Malware Detection and Classification: AI models, including DeepSeek, assist in analysing malware signatures and identifying anomalies in network traffic.
- Code Analysis for Security Weaknesses: AI can review application code to identify vulnerabilities, including improper API calls to back-end systems through POST requests, incorrect parameter handling, and potentially dangerous queries.

For public institutions and educational platforms, AI-driven security solutions offer a cost-effective means of fortifying cybersecurity defenses, particularly in environments with constrained budgets.

5.5. Balancing AI's Potential: Ethical and Security Considerations

While AI-powered security tools improve defense mechanisms, ethical concerns and regulatory challenges must be addressed. Open-source AI models like DeepSeek provide transparency, allowing researchers to audit code for vulnerabilities. However, their unrestricted use poses security risks.

5.6. Positive Impact:

- Transparency and Security: Open-source AI models enable independent audits and early vulnerability detection.
- Data Privacy: AI models that run locally reduce risks associated with cloud-based data processing.
- Threat Intelligence: AI facilitates advanced malware detection and response.
- Accessibility: AI-driven security tools offer cost-effective protection for institutions with limited resources.

5.7. Negative Impact:

- Potential for Malicious Use: Open-source AI can be modified for nefarious purposes, such as automating cyberattacks and crafting undetectable phishing content.
- Lack of Oversight: Unlike corporate AI models, open-source systems lack centralized regulation, allowing unrestricted deployment.
- Security Risks: Open-source transparency enables attackers to identify and exploit weaknesses before patches are implemented.

5.8. Strategic AI Integration: A Forward-Thinking Approach

For public institutions and enterprises, responsibly integrating AI into cybersecurity strategies is critical. AI

should be deployed with safeguards that emphasize privacy, ethical considerations, and regulatory compliance. To maximize its benefits, organizations should enhance Threat Intelligence using AI-driven predictive analytics, automate Security Monitoring to improve response efficiency, and implement Ethical AI Training to ensure responsible use within cybersecurity frameworks. As AI continues to evolve, its role in cybersecurity will only expand. While it introduces risks, its responsible adoption holds the potential to revolutionize digital defense mechanisms. By leveraging AI wisely, organizations can fortify their security postures while mitigating emerging threats in an increasingly AI-driven world.

6. Discussion

6.1. Challenges

Public educational institutions face several systemic challenges that hinder their ability to secure their digital platforms effectively. These challenges arise from resource limitations, lack of comprehensive oversight, and gaps in technical expertise, creating vulnerabilities that often remain unaddressed.

One significant issue is budget constraints. Limited financial resources mean that cybersecurity often competes with other operational priorities, leaving minimal room for investments in advanced tools, training programs, or regular audits. This lack of funding results in outdated systems and reactive approaches to threats, which increase the likelihood of breaches.

Another challenge is incomplete visibility of components. Many institutions lack a full understanding of their IT environments, including unmanaged devices, third-party dependencies, and shadow IT. Without this visibility, they struggle to identify vulnerabilities or implement comprehensive security measures, leaving critical gaps in their defenses. Additionally, the human factor plays a crucial role in cybersecurity effectiveness, particularly when users face external stressors or environmental challenges. As noted in research, "Some of our employees were more distracted by other stressful events, found the rapid transition from home to work challenging, and were not given adequate support to adopt effective cybersecurity when working from home." (Whitty Monica, 2024) This issue extends beyond corporate environments to educational institutions, where faculty members and students must adapt to rapidly evolving security policies without sufficient training or support. Addressing these human and operational challenges is just as critical as implementing technical security measures.

Additionally, there is often a lack of professionalism in audit practices. Cybersecurity audits in public institutions are frequently superficial, viewed as procedural requirements rather than opportunities for meaningful improvement. This issue stems from limited technical expertise and the absence of standardized frameworks for assessing platform vulnerabilities. Consequently, critical risks are overlooked, and remediation efforts lack focus and direction.

Lastly, failure to address risks exacerbates these issues. Even when vulnerabilities are identified, institutions frequently fail to act due to a lack of understanding or misplaced confidence in existing security measures. Many rely on "defense in depth" strategies without ensuring that individual layers of defense are adequately configured. This over confidence often leads to high priority risks being ignored, leaving platforms exposed.

6.2. Opportunities

Despite these challenges, public educational institutions have significant opportunities to enhance their cybersecurity posture through strategic changes:

1. Resource Optimization: Institutions can maximize their limited budgets by leveraging cost-effective solutions such as open-source tools, government-funded training programs, and partnerships with cybersecurity organizations. Frameworks like OWASP and free tools like the MITRE Risk Calculator offer valuable resources for improving security without significant financial investment.

2. Adopting Zero Trust Frameworks: Transitioning to Zero Trust Network Access can address many of the limitations associated with traditional perimeter-based defenses. By enforcing strict identity and access management protocols, ZTNA reduces the risk of lateral movement within networks and provides granular control over user permissions.
3. Collaboration and Knowledge Sharing: Partnerships with governmental cybersecurity agencies, private sector experts, and academic institutions can provide access to expertise, tools, and shared resources. These collaborations can also foster a culture of continuous improvement and innovation within public institutions.
4. Building a Culture of Cybersecurity Awareness: Training staff and students to recognize and respond to cybersecurity threats can significantly reduce human error, which remains a leading cause of breaches. Awareness programs can also help institutions better prioritize cybersecurity as a core operational concern.
5. Monitoring: Implementing continuous monitoring and real-time threat detection is essential for securing educational platforms against evolving cyber threats. Security Information and Event Management (SIEM) systems, behaviour-based anomaly detection, and threat intelligence platforms enable proactive risk identification and rapid response.

While the challenges facing public educational institutions are substantial, they are not insurmountable. By addressing resource gaps and fostering a culture of awareness and collaboration, these institutions can move from reactive measures to proactive strategies. This shift is essential for ensuring the security and integrity of digital platforms in the face of evolving cyber threats.

7. Conclusions

This study confirms that educational platforms face significant security risks due to outdated infrastructure, weak access controls, and common misconfigurations, making them vulnerable to threats such as SQL injection (CWE-89), session management flaws (CWE-384), and weak TLS configurations (CWE-295). The heavy reliance on third-party plugins and reactive security strategies further amplifies these risks, underscoring the limitations of traditional perimeter-based security models. Future research should investigate adaptive security frameworks and dynamic trust mechanisms to enhance resilience in educational environments.

The findings demonstrate that a multi-layered security approach, integrating SAST, DAST, container audits, and Zero Trust Network Access (ZTNA), is essential to mitigating threats that conventional assessments often overlook. The ZTNA framework, in particular, significantly reduces attack surfaces by enforcing strict identity-based access controls and limiting lateral movement. Additionally, the security checklist developed in this study provides a structured method for educational platforms to assess vulnerabilities and align security efforts with ISO 27001, NIST CSF, and MITRE ATT&CK standards.

Beyond technical solutions, this research underscores the need for a paradigm shift in cybersecurity governance, where security is embedded into the architecture, development lifecycle, and operational strategies of educational platforms. Cybersecurity in digital education is not merely a technical requirement but a fundamental pillar of platform trust and operational continuity. Without proactive, risk-centric security strategies, educational platforms will remain prime targets for cybercriminals. By adopting scalable security frameworks, continuous monitoring, and AI-driven threat intelligence, they can transition from being vulnerable targets to resilient, security-first environments in an evolving threat landscape.

8. Limitations and future research

While this study has addressed key cybersecurity challenges in educational platforms, several critical areas require further investigation. Identity and Access Management (IAM) remains a pressing issue, as platforms increasingly adopt federated identities and multi-cloud environments. Future research should explore how Zero Trust principles can be integrated into IAM to enhance authentication and privilege management.

Advanced monitoring and detection with SIEM and XDR is another key area, as traditional SIEM solutions

struggle in highly distributed educational ecosystems. The role of AI-driven threat intelligence in improving behavioural anomaly detection while minimizing resource constraints warrants further study. Similarly, incident response automation through SOAR could optimize threat mitigation, yet its real-world integration in educational settings remains underexplored.

Further research is needed on Web Application Firewalls (WAFs) as compensatory control in legacy environments with weak SDLC practices. Many educational platforms rely on third-party plugins, increasing security risks, yet the tradeoffs between WAF effectiveness, performance, and false positives are not well documented.

Lastly, hybrid and multi-cloud security presents growing challenges. As educational platforms expand across on-premises and cloud infrastructures, research should focus on granular access control, real-time risk assessment, and compliance enforcement in dynamic cloud environments.

Addressing these gaps is essential for developing scalable, adaptive security models that strengthen the resilience of educational platforms against evolving cyber threats.

Acknowledgements
The authors extend their gratitude to colleagues and institutions that provided insights and feedback during the research process.

Funding
No external funding was received for this research.

Appendix A

Justification and Context:

Traditional cybersecurity audits, such as those based on ISO 27001, NIST CSF, and CIS Controls, provide a regulatory framework but often fail to reflect the actual technical security posture of an organization. Multiple security assessments have revealed that even certified entities exhibit significant gaps in critical security controls, leading to a false sense of security.
This appendix introduces a technical self-diagnosis checklist designed to provide an assessment based on empirical evidence and concrete technical validations of infrastructure and operational security. Unlike conventional security certifications, this methodology evaluates the actual implementation of security controls rather than relying solely on documented policies.
By incorporating a weighted scoring system (W_i), this methodology ensures that more critical security measures contribute more significantly to the final compliance score, highlighting vulnerabilities that traditional audits may overlook.

Formula Explanation

To quantify the security maturity of the evaluated entities, the following formula calculates a weighted cybersecurity compliance score, considering the importance ( ) of each evaluated control:

$$S = \frac{\sum_{i=0}^{n}(P_i W_i)}{\sum_{i=0}^{n} W_i} x \frac{1}{100}$$

Where:

s is the final cybersecurity score.
p_i represents the compliance percentage (0-100) for control i.
w_i is the assigned weight for control iii, reflecting its importance.
n is the total number of evaluated controls.

Interpretation:

1. Each control's compliance level p_i is weighted according to its assigned importance w_i.
2. The sum of weighted compliance scores is divided by the sum of all weights to obtain a normalized average.
3. The final result is scaled down by 100 to express it as a percentage between 0 and 1.
4. The weights w_i have been assigned subjectively by the author of this study, based on the perceived impact on the security of the evaluated entity. These weights reflect the relative importance of each security control in mitigating risks, preventing cyber threats, and ensuring operational resilience.
5. However, the assigned weights are not absolute and may be modified in future research to accommodate different organizational priorities, risk profiles, or evolving cybersecurity frameworks. Researchers and practitioners applying this methodology are encouraged to adjust the weight distribution based on their specific threat landscape and security objectives.

Future Validation and Adaptability

The weighting system used in this study has been empirically tested across five educational entities, providing an initial validation of its applicability. The results demonstrate clear disparities in cybersecurity maturity between institutions and confirm that certain security controls play a crucial role in overall security resilience. However, additional testing in larger samples and different sectors (e.g., finance, healthcare, or government infrastructures) could further refine these weight distributions. Future research may leverage historical security incidents, statistical modelling, and comparative analysis to determine if specific security measures should carry greater or lesser weight based on real world attack patterns and breach data.
By iteratively refining the model through expanded case studies and quantitative analysis, this methodology can evolve into a more universally applicable cybersecurity assessment framework.

Table A1. Results

Nº	Category	Checklist Item	Description	Control	Entity A	Entity B	Entity C	Entity D	Entity F	Weight
1	Container and Cloud Security	Image Scanning	Scan Docker images and base layers for known vulnerabilities.	What percentage of container images are scanned for vulnerabilities before deployment to production?	0	0	80	50	50	1
2	Container and Cloud Security	Kubernetes Security	Apply RBAC policies and enforce CIS benchmarks for Kubernetes clusters.	What percentage of Kubernetes clusters have automated controls that verify compliance with CIS benchmarks?	50	70	70	100	30	1
3	Container and Cloud Security	Cloud Access Management	Restrict access to cloud resources using role-based policies and MFA.	What percentage of accesses to cloud resources are protected by role-based policies (RBAC) and multi-factor authentication (MFA)?	100	80	90	90	100	2
4	Cryptographic Practices	SSL/TLS Configuration	Audit SSL/TLS certificates to enforce compliance with TLS 1.3 and identify deprecated algorithms.	SSL Labs score converted to a scale from 0 to 100 (A = 100, F = 0)	75	60	65	75	75	5
5	Cryptographic Practices	Data Encryption	Confirm sensitive data is encrypted using robust standards like AES-256 or RSA-2048.	Percentage of sensitive data stored with strong encryption (AES-256, RSA-2048, or equivalent).	90	80	100	90	95	2
6	Cryptographic Practices	Key Management	Enforce regular key rotation, secure storage, and proper lifecycle management.	Percentage of keys with documented rotation and management in the past year.	30	0	70	50	60	2
7	Dynamic Application Security	Runtime Vulnerability Testing	Use tools like OWASP ZAP or Burp Suite to identify runtime vulnerabilities under simulated attacks.	Percentage of applications analyzed with DAST tools after deployment to production or a critical update.	70	50	50	60	40	5

Castro-Ortiz, J. C.; Martínez-López, F. J. (2026). Cybersecurity in educational platforms: threats, challenges, and best practices. *Campus Virtuales,* 15(1), 191-213. https://doi.org/10.54988/cv.2026.1.1700

Nº	Category	Checklist Item	Description	Control	Entity A	Entity B	Entity C	Entity D	Entity F	Weight
8	Dynamic Application Security	Input Validation Testing	Validate user input against strict rules to prevent injection attacks such as SQLi and XSS.	Percentage of user inputs validated against strict rules to prevent injection vulnerabilities.	80	50	50	50	15	2
9	Dynamic Application Security	Authentication and Session Control	Verify that sessions expire appropriately, and tokens are securely handled.	On a scale from 0 to 100, to what extent has it been verified that sessions expire correctly and tokens are securely protected?	100	80	70	70	70	3
10	Dynamic Application Security	Authorization Flows	Ensure role-based access control (RBAC) prevents privilege escalation.	Percentage of roles and permissions reviewed in the last 6 months to prevent privilege escalation.	20	20	20	20	40	2
11	Identity & Access Management (IAM)	Role-Based Access Control (RBAC)	Enforce RBAC policies to restrict access based on user roles and responsibilities.	Percentage of systems with RBAC configured without excessive privileges or improper assignments.	30	40	20	40	35	2
12	Identity & Access Management (IAM)	Multi-Factor Authentication (MFA) Enforcement	Require MFA for all users, particularly for privileged accounts and remote access.	Percentage of users with MFA enabled for critical access points, privileged accounts, and remote access.	50	70	75	65	85	4
13	Network Micro-Segmentation	Policy-Based Network Access	Ensure network access is granted dynamically based on user identity, device compliance, and risk level.	Percentage of accesses dynamically managed based on identity, device compliance, and risk level.	15	0	0	15	25	4
14	Network Micro-Segmentation	Zero Trust Segmentation Audits	Conduct periodic audits to verify proper enforcement of network segmentation.	Percentage of network segmentations audited in the past year.	35	25	40	35	50	1
15	Network Security & Micro-Segmentation	Network Segmentation Strategy	Apply micro-segmentation to isolate critical assets and minimize lateral movement risks.	Percentage of network segments implemented with Zero Trust policies, including critical systems.	50	45	40	30	40	5
16	Network Security & Micro-Segmentation	Policy-Based Network Access	Restrict network access dynamically based on user identity, device compliance, and risk level.	Percentage of accesses dynamically restricted based on identity, device compliance, and risk level.	30	40	20	40	35	2
17	Policy and Compliance	Data Protection Policies	Ensure compliance with GDPR, FERPA, or other applicable data protection regulations.	Percentage of compliance with applicable data protection regulations (GDPR, FERPA, or others)	90	100	95	90	100	2
18	Policy and Compliance	Secure Development Lifecycle (SDLC)	Integrate security controls at every stage of the software development lifecycle.	Percentage of projects incorporating security controls from the design phase.	40	35	50	25	5	2
19	Policy and Compliance	Access Control Reviews	Periodically review and update access control policies to align with organizational changes.	Percentage of user permissions reviewed in the past year.	30	20	40	40	45	2
20	Risk Management	Vulnerability Prioritization	Use the MITRE Risk Calculator to evaluate the impact of vulnerabilities and prioritize remediation.	Percentage of high and critical vulnerabilities remediated in the past month.	80	75	85	75	100	5
21	Risk Management	Awareness and Training	Conduct phishing simulations and provide staff with training on modern cyber threats.	Percentage of users who correctly identified and did not interact with phishing attempts in the latest simulation.	70	75	70	75	75	1
22	Server and Infrastructure Security	Operating System Hardening	Apply CIS Benchmarks for Windows and Linux to disable unnecessary services and enforce security.	Percentage of CIS Benchmark controls implemented on Windows and Linux servers.	50	60	70	0	0	5
23	Server and Infrastructure Security	Server Patch Management	Regularly update OS and server applications to address critical vulnerabilities.	Percentage of servers with security patches applied in the last 30 days.	50	20	80	50	80	5
24	Server and Infrastructure Security	Log Aggregation and Monitoring	Centralize logs and set alerts for anomalous activities using tools like Splunk or ELK Stack.	Percentage of virtual campus information sources monitored through logs and security alerts.	50	75	70	90	95	5
25	Server and Infrastructure Security	Backup and Disaster Recovery	Implement backup solutions with encrypted data storage and regular recovery drills.	Percentage of backups performed according to best practices across the entire virtual campus infrastructure.	40	100	75	90	90	5

Nº	Category	Checklist Item	Description	Control	Entity A	Entity B	Entity C	Entity D	Entity F	Weight
26	Static Application Security	Code Analysis Tools	Integrate SAST tools like Microfocus, Checkmarx, or Veracode to detect and fix vulnerabilities early.	Percentage of applications analyzed with SAST tools before deployment to production or after a critical update.	20	0	10	20	35	5
27	Static Application Security	Secure Code Reviews	Conduct manual reviews to identify logic flaws and confirm automated findings.	On a scale from 0 to 100, to what extent have manual reviews been conducted to identify logic flaws and validate automated findings?	0	10	15	10	25	2
28	Static Application Security	Dependency Scanning	Regularly audit third-party libraries and plugins to identify vulnerabilities using CVE databases.	Percentage of third-party libraries and plugins audited in the past year for vulnerabilities or outdated components.	70	50	50	60	40	4
29	Static Application Security	Coding Standards	Implement secure coding practices aligned with OWASP guidelines.	Percentage of projects that have followed OWASP recommendations during requirements gathering and the development phase.	70	40	50	40	40	3
30	Zero Trust Security	Zero Trust Implementation	Adopt Zero Trust principles for access control, ensuring verification at every access attempt.	Percentage of authenticated and dynamically verified accesses based on Zero Trust principles	50	30	40	40	50	2
31	Zero Trust Security	Identity-Based Access	Implement ZTNA to grant access based on identity and compliance rather than location.	On a scale from 0 to 100, to what extent has ZTNA been implemented to grant access based on identity and conditional access?	50	50	65	60	70	3
32	Zero Trust Security	ZTNA Implementation	Implement Zero Trust Network Access (ZTNA) to enforce identity-based access control.	Percentage of authenticated and dynamically verified accesses based on Zero Trust principles.	50	50	65	60	70	2
33	Zero Trust Security	Least Privilege Enforcement	Ensure all users and services have only the minimum privileges required for their tasks.	Percentage of accounts reviewed and adjusted according to the principle of least privilege.	20	30	30	35	20	2
34	Zero Trust Security	Continuous Access Monitoring	Monitor access attempts and anomalies in real time to detect unauthorized access.	On a scale from 0 to 100, to what extent are failed access attempts, logins from suspicious locations, impossible travel scenarios, and anomalous patterns monitored and responded to in real time?	70	70	65	60	60	2
				RESULTS	**52%**	**49%**	**56%**	**53%**	**56%**	

Cómo citar este artículo / How to cite this paper

Castro-Ortiz, J. C.; Martínez-López, F. J. (2026). Cybersecurity in educational platforms: threats, challenges, and best practices. *Campus Virtuales,* 15(1), 191-213. https://doi.org/10.54988/cv.2026.1.1700

References

Brown, A. T. (2024). Harnessing the Power of LLMs: LLM Summarization for Human-Centric DAST Reports. In 2024 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC).

Checkpoint. (2025). https://www.checkpoint.com. (https://www.checkpoint.com/security-report/?flz-category=items&flz-item=report-cyber-security-report-2025).

Chen, S.-J. (2022). The Impact of the Practical Security Test during the Software Development Lifecycle. In International Conference on Advanced Communications Technology(ICACT), 2.

Dingzong Zhang, K. J. (2024). Guarding Against ChatGPT Threats: Identifying and Addressing Vulnerabilities. In 2024 IEEE 7th International Conference on Multimedia Information Processing and Retrieval (MIPR).

Farhan A Qazi. (2022). Study of Zero Trust Architecture for Applications and Network Security.

Fu Michael, C. (. (2023). ChatGPT for Vulnerability Detection, Classification, and Repair: How Far Are We?. In 2023 30th Asia-Pacific Software Engineering Conference (APSEC).

Herrera Jerónimo Adrián, P. M. (2024). Techniques of SAST Tools in the Early Stages of Secure Software Development: A Systematic Literature Review. In 2024 IEEE International Conference on Engineering Veracruz (ICEV) (pp. 1-8). Boca del Rio, Veracruz, Mexico.

https://doi.org/10.1109/ICEV63254.2024.10766004, 1.
Husseis Anas, J. L. (2023). Enhancing Cybersecurity Proactive Decision-Making through Attack Tree Analysis and MITRE Framework. In IEEE International Carnahan Conference on Security Technology (ICCST).
Iffath Tanjim Moon, A. M. (2023). Cryptographic Analysis: Popular Social Media Applications and Mitigations of Vulnerabilities. In 2023 26th International Conference on Computer and Information Technology (ICCIT).
Li, T. H. (2021). A Model and Method of Information System Security Risk Assessment based on MITRE ATT&CK. In 2021 2nd International Conference on Electronics, Communications and Information Technology (CECIT).
Mandela, D. M. (2023). Evaluating Docker Container Security through Penetration Testing: A Smart Computer Security. In International Conference on Communication, Security and Artificial Intelligence (ICCSAI).
Microsoft. (2024). https://www.microsoft.com. (https://www.microsoft.com/en-us/security/blog/2024/10/10/cyber-signals-issue-8-education-under-siege-how-cybercriminals-target-our-schools/).
Nasywa Rayhan Brian, M. M. (2024). Design of Web-based Key Management System Application Based on NIST SP 800-57 recommendations. In International Conference on Electrical Engineering and Computer Science (ICECOS) 2024.
Rey, M. J. (2024). Beyond the Firewall: Strategies in Securing Remote Work Environment. In 14th International Conference on Software Technology and Engineering (ICSTE).
Roumani, Y. (2021). Patching zero-day vulnerabilities: an empirical analysis. Journal of Cybersecurity, 2021, 1-13.
Wang, R. L. (2025). Zero-trust based dynamic access control for cloud computing. Cybersecurity. https://doi.org/10.1186/s42400-024-00320-x.
Wei Liu, J. Y. (2021). A lightweight Container Security Framework adapted to power cloud Platform.
Whitty Monica, T. N. M. (2024). Cybersecurity when working from home during COVID-19: considering the human factors.
Wissem Chorfa, N. B. (2023). Threat Modeling with Mitre ATT&CK Framework Mapping for SD-IOT Security Assessment and Mitigations. Wissem Chorfa 1 , Nihel Ben Youssef. IEEE Senior Member2, Abderrazak Jemai 1, 4.
Yao, S. R. (2017). Program Analysis of Cryptographic Implementations for Security. In 2017 IEEE Cybersecurity Development.
Yusof Darus Mohamad, M. F. (2023). 8th IEEE International Conference and Workshops on Recent Advances and Innovations in Engineering- ICRAIE. (IEEE Record #59459).
Zhang, J. B. (2025). When LLMs meet cybersecurity: a systematic literature review. https://doi.org/10.1186/s42400-025-00361-w.