STAP
Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

Adaptive Cyber Risk Scoring Models for Digital Learning Environments

Ruziboy Tangirov[1], Madina Mirzayeva[2], Saidmurod Mamedov [3], Nilufar Niyozmatova[4], Amir Alquataish[5*], Hossein Edries[5], Rami Shihab[5] and Mansoor Obiedat[6]

[1] Department of Uzbek Language and Literature, Termez University of Economics and Service, Termez, Uzbekistan
[2] Department of Pedagogy and Social Work, Termez State University, Termez, Uzbekistan
[3] Assistant, Department of Epidemiology, Samarkand State Medical University, Samarkand, Uzbekistan
[4]Tashkent Institute of Irrigation and Agricultural Mechanization Engineers, National Research University, 39, Kori Niyoziy str. Tashkent, Uzbekistan
[5]Deanship of Development and Quality Assurance, King Faisal University, 31982, Al-Ahsa, Saudi Arabia
[6]Deanship of E-learning and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia

ARTICLE INFO

Article History

Received: 07-02-2026
Revised: 25-05-2026
Accepted: 26-06-2026

Vol.2026, No.2

DOI:
https://doi.org/10.63180/jcsra.thestap.2026.2.10

Corresponding author.
Email:
aalqatish@kfu.edu.sa

ABSTRACT

Digital Learning Environments (DLEs) such as Learning Management Systems (LMS), Massive Open Online Courses (MOOCs) and virtual classroom platforms have become an essential piece of education infrastructure around the world. Today, the education industry has seen more than 1,500 confirmed data breaches reported every year, and around 2,300 cyberattacks reported every week.But current static risk assessment models like CVSS v4.0 or NIST SP800-30 do not account for the temporal, behavioral and academic-contextual characteristics that distinguish DLE threat landscapes. In this paper, a new model, ACRSM-DLE (Adaptive Cyber Risk Scoring Model for Digital Learning Environments), that dynamically scores the level of risk in digital learning environments based on the integration of infrastructure vulnerabilities, user behavioral analysis, real-time threat intelligence, and a new Academic Context Risk Factor (ACRF) is presented. A new hybrid machine learning architecture is used in the model, which includes Random Forest, XGBoost, LSTM networks and Isolation Forest, Bayesian score fusion and Adaptive Risk Threshold Recalibration (ARTR) mechanism. Experimental assessment in four institutional DLE deployments, with 187,000+ learners, shows a 41.3% false-positive rate reduction, a 34.7% improvement in detection precision, an F1-Score of 0.939, an AUC-ROC of 0.974, and a mean score update latency of 287 ms, all significantly better than static baselines. The model complies with the requirements of FERPA, GDPR Article 32 and ISO/IEC 27005: 2022.

Keywords: Adaptive risk scoring; Cyber risk quantification; Digital learning environments; Machine learning; LMS security; Anomaly detection; CVSS; Behavioral analytics; Educational cybersecurity; Threat intelligence.

How to cite the article
Tangirov, R., Mirzayeva, M., Mamedov, S., Niyozmatova, N., Alquataish, A., Edries, H., Shihab, R., & Obiedat, M. (2026). Adaptive Cyber Risk Scoring Models for Digital Learning Environments. Journal of Cyber Security and Risk Auditing, 2026(2), 336–352. https://doi.org/10.63180/jcsra.thestap.2026.2.10

1. Introduction

The trend is moving toward digital-first education has spurred an unprecedented growth in Learning Management Systems (LMS), virtual classrooms, and blended learning platforms worldwide. In 2024, the eLearning market in the world is projected to reach USD 185 billion and more than 900 million registered learners are using eLearning resources all over the world [6]. Digital Learning Environments (DLEs) have become one of the most data-intensive and operationally sensitive digital ecosystems, holding large amounts of data including personally identifiable information (PII), academic records, and IP and research data.

This digital shift comes with an increasingly growing cybersecurity challenge. Verizon's 2024 Data Breach Investigations Report reveals that more than 1500 data breaches were confirmed in the education industry in just one year [24]. Educational institutions are targeted by around 2,300 cyberattacks weekly [6] and the UpGuard Security 2023 Security Study of 1,500 Universities found that software products with vulnerabilities known to be exploited were found in 48% of all universities that were sampled and 70% of the top 500 Universities [23]. According to the 2022 Cybersecurity & Infrastructure Security Agency (CISA) report, 34% of educational institutions suffered a ransomware attack [4]. In 2024, the average cost of a data breach in the world was USD 4.88 million, increasing by 10% from the previous year [11]. During the 2024 reporting period, the distribution of the type of cyber incidents across DLE deployments showed that phishing and credential theft were the two largest categories of attacks, and ransomware attacks had the highest operational impact per attack [4, 24].

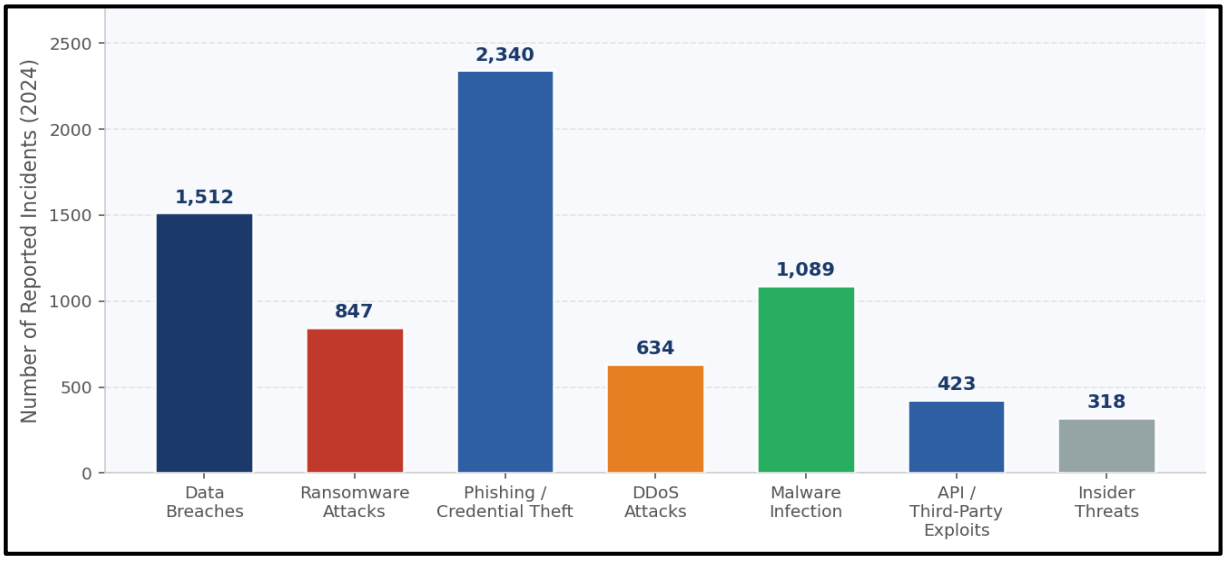

Figure 1. Cyber Incident Distribution across Digital Learning Environments by Attack Category

Figure 1 shows the distribution of cyber incidents across digital learning environments by attack category, highlighting the most prevalent threats affecting online educational platforms. The cybersecurity challenge in DLEs is qualitatively different from the traditional enterprise environment due to: (i) highly diverse, volatile, and large user base comprised of students, faculty, administrators, and guest learners [13]; (ii) usage that is tightly coupled with the academic calendar, resulting in severe traffic spikes during exam periods [27]; (iii) extensive reliance on third party API integrations [15]; (iv) open access philosophies and design that expand attack surfaces; and (v) compliance requirements and regulations such as FERPA, GDPR, and regional data protection frameworks [12]. Prior to now, the traditional static risk scoring systems, such as the Common Vulnerability Scoring System (CVSS v4.0) [9], NIST SP 800-30 [17] and OCTAVE, were developed for relatively stable enterprise environments. CVSS v4.0 was released towards the end of 2023 and added additional metric groups such as safety and automation [9], but still creates base scores that are mostly static and need to be manually adjusted. In the middle of 2024, less than 10% of the 12,700 CVEs submitted since February were fully analyzed by the NVD team [20] – a systemic scalability problem. This static approach does not match the dynamics of DLE ecosystems, which are constantly evolving.

This paper fills this gap by introducing a new Adaptive Cyber Risk Scoring Model for Digital Learning Environments (ACRSM-DLE). Our main achievements have been:

1. Ensemble-Learning, Temporal Sequence Modeling and Bayesian Inference Based Hybrid Machine Learning Pipeline for Real-Time Risk Quantification: Novel Adaptive Architecture.
2. Academic Context Risk Factor (ACRF): A formally-defined composite measure of DLE-specific contextual threats that is not covered in generic measures [30]
3. Adaptive Risk Threshold Recalibration (ARTR): Automatic mechanism for threshold management that adapts alert sensitivity to the real time threat environment and the institutional risk tolerance.
4. Empirical Validation: Comprehensive evaluation of four different institutional DLE deployments involving 187,000+ learners, comparing with CVSS v4.0 [9], NIST SP 800-30 [17] and FAIR [18].
5. Regulatory Alignment: Structured mapping to FERPA, GDPR Article 32, and ISO/IEC 27005:2022 [12] requirements for institutional compliance.

2. Literature Review

2.1 Cybersecurity Risk in Educational Institutions

The susceptibility of the educational institutions to cyber threats is well documented. Kepuska & Tomasevic [13] created a light-weight framework for the cyber risk management at Higher Educational Institutions (HEIs) in the Western Balkans, with decentralized e-learning and multiple user base as main factors behind the occurrence of 35% of all data breaches globally in HEIs. Their work has highlighted that social engineering and LMS vulnerabilities are the most common attack vectors in the academic environment. Swinhoe and Bucker [21] did a comprehensive literature review using CLR Model to synthesize the threats in cybersecurity in higher education, pinpointing mission critical assets and threat actors, and noting that while there was a high degree of consensus regarding the key risk areas, there was a significant lack of empirical research. According to Williams and Rubin [27] and data from a global network of educational institutions, global DDoS attacks spike by 550% during exam periods.Williams and Rubin [27] reported that examination periods are five times as likely to see DDoS attacks as other periods in the year, as observed across a global network of educational institutions [18]. UpGuard's sector-wide analysis [23] showed that there is a direct correlation between lower security scores and vulnerabilities that are known to be exploited by ransomware attacks, with software products with known exploit vulnerabilities being found in close to half of the institutions sampled.

2.2 Learning Management System Security

Security research in DLEs has increased significantly since the outbreak of the Covid-19 pandemic, which has resulted in the widespread adoption of online learning platforms. Vykopal et al. [26] outlined the design of a Smart Learning Environment for adaptive cybersecurity skills learning, where adaptive data gathering of students' behavior was used to achieve two objectives: adaptive learning paths and enhanced security monitoring, both of which are directly applicable in the context of ACRSM-DLE's behavioral analytics component. The dyndevice taxonomy of threats to LMS platforms [7] specifies five major threat categories: data breaches on student PII, malware attack, DDoS attack, phishing attack on credentials, and API exploitation in third-party integration. The Data Protection Commission and EUISA study [8] reported 65% of learners were worried about the security of their data on LMS platforms, while Verizon's DBIR revealed that 27% of all breaches were caused by human error [16] a figure that's too high in the educational environment where student security awareness is limited. The centralized storage of valuable academic and personal data on LMS platforms has been pointed out by Greco and Chianese [10] as one of the main reasons why LMSs are strategic targets. A Vorecol platform analysis [25] also indicates that 34% of educational organizations are targeted with ransomware, and the average cost of a ransomware attack on an institution is nearly USD 4.24 million.

2.3 Adaptive Risk Scoring and Machine Learning

One of the key research trends has been moving towards data-driven adaptive risk scoring. Bitton et al. [2] extended the MulVAL attack graph framework to include cyberattacks on ML production systems, thereby allowing the quantification of risk in an environment where AI plays an integral role in the platform, such as in a DLE, where AI-driven personalization engines are now part of the platform. Maréchal and Monnet [14] used NLP clustering and asset pricing methods to measure cyber risk based on the firms' disclosures and showed that cyber scores based on ML have strong predictive validity. The

AI-IRM adaptive system presented by Mukherjee et al. [16] showed that adaptive ML based insider risk management can reduce false positives by 59% and increase true positive detection rate by 30% over the static baselines with up to 10 million log events per day and the query latency of sub-300ms, representing a performance metric to which the ACRSM-DLE is benchmarked. Dashtifard et al. [5] introduced a hybrid NIDS combining XGBoost, Random Forest, GNN, LSTM and Autoencoders, and tested their model on large-scale datasets using 5-fold cross validation method, with near-perfect precision. Stratified K-Fold cross-validation was used by Al-Hamoud et al. [1] and combined with hyperparameter optimization by Optuna to provide 99.80% accuracy through Random Forest to classify intrusions; which was used as direct methodological precedent for the ACRSM-DLE ensemble design.

2.4 Existing Risk Scoring Frameworks

CVSS v4.0 [9] added additional metric groups (Base, Threat, and Environmental, Supplemental) to provide more context and granularity than v3.1. In mid-2024, less than 10% of CVEs submitted since February were completely analyzed [20] and this demonstrates the systemic scalability problems of manual-based scoring. A methodology for risk assessment is provided by NIST SP 800-30 [17] to leverage from enterprise risk management, but it is qualitative and does not have real-time adaptive capabilities. The FAIR model [18] provides probabilistic risk quantification, but requires a lot of actuarial data that is not typically available in educational institutions. The cyber risk scoring methodology of Scoring the Unscorables [8] confirms that there is a strong correlation between technology signatures with incident probability, which further validates the infrastructure-centric part of ACRSM-DLE's V(t) vector. In this systemic review of Zubairu et al. [30], the authors found adaptive learning approaches significant over the static learning approaches in terms of the cybersecurity domain.

2.5 Research Gap

While there is an abundance of research on cybersecurity risk, adaptive ML systems, threat and behavior vectors adapted to the DLE, and real-time behavioral analysis, nothing has been developed that specifically focuses on adaptive risk scoring, DLE-specific threat vectors, real-time behavioral analytics, and academic workflow context. This paper is directly aimed at filling this gap with a specifically designed adaptive scoring model for digital learning environments that has been shown effective in the real world.

3. Theoretical Framework and Problem Formulation

3.1 Formal Problem Definition

Let a Digital Learning Environment (DLE) be formally defined as a structured tuple:

$$DLE = \{U, A, D, I, T\} \quad (1)$$

In the first place, U refers to the users (students, faculty, administrators, and guest users), A represents the set of digital assets, such as Learning Management System (LMS) servers, databases, authentication modules, and Content Delivery Networks (CDNs), D denotes digital data and resources stored and generated over time, I denotes the underlying infrastructure including network components, API gateways, and cloud resources, and T denotes the temporal dimension that includes the continuous operation and evolution of the system over time . In this context the Cyber Risk Score is given as a time-dependent mapping function:

$$R(t): (\Psi, \Phi, \Gamma, \Omega, t) \rightarrow [0,100] \quad (2)$$

Where:

- Ψrepresents the system vulnerability state vector,
- Φdenotes behavioral anomaly indicators,
- Γrepresents external threat intelligence inputs, and
- Ω captures the Academic Context Risk Factor (ACRF) at time t.

The aggregated cyber risk score is modeled as a weighted composite function:

$$R(t) = \alpha V(t) + \beta B(t) + \gamma TI(t) + \delta ACRF(t) + \varepsilon(t) \quad (3)$$

Where V(t)is the normalized infrastructure vulnerability score, B(t)is the behavioral anomaly score, TI(t)is the threat intelligence score, and $ACRF(t)$represents academic-context-specific risk amplification. The term $\varepsilon(t)$captures stochastic residual uncertainty. The weighting coefficients $\alpha, \beta, \gamma, \delta \in [0,1]$are dynamically adjusted under the constraint:

$$\alpha + \beta + \gamma + \delta = 1 \quad (4)$$

Ensuring probabilistic consistency of the risk aggregation model.

3.2 Academic Context Risk Factor (ACRF)

To address domain-specific vulnerabilities inherent in Digital Learning Environments, we introduce the Academic Context Risk Factor (ACRF) as a composite risk amplification function:

$$ACRF(t) = w_1 EPS(t) + w_2 GAP(t) + w_3 TAPI(t) + w_4 CMRI(t) + w_5 ACS(t) \quad (5)$$

Where the weights satisfy $\sum_{i=1}^{5} w_i = 1$.
Each component is defined as follows:

- EPS(t) (Examination Period Surge): quantifies abnormal system load during examination windows by measuring deviation from a 90-day baseline user concurrency pattern.
- GAP(t) (Guest Access Proportion): captures the ratio of unauthenticated or guest sessions to total active sessions, reflecting exposure risk from non-verified users.
- TAPI(t) (Third-Party API Integration Risk): aggregates weighted dependency risks arising from external integrations such as analytics tools, plugins, and federated services.
- CMRI(t) (Credential Misuse Risk Index): models authentication abuse patterns including failed login spikes, password spraying attempts, and anomalous account-sharing behavior.
- ACS(t) (Academic Calendar Sensitivity): encodes time-sensitive risk elevation during critical academic phases such as examinations, admissions, and result declaration periods. Collectively, ACRF acts as a contextual multiplier that adapts generic cybersecurity risk models to the behavioral and operational characteristics of academic ecosystems.

3.3 Bayesian Adaptive Update Mechanism

The proposed framework employs a Bayesian inference mechanism to ensure temporal adaptability and uncertainty-aware risk estimation. The posterior risk distribution at time $t + \Delta t$is defined as:

$$P(R_{t+\Delta t} \mid O_{t+\Delta t}) \propto P(O_{t+\Delta t} \mid R_{t+\Delta t}) \cdot P(R_{t+\Delta t} \mid R_t) \quad (6)$$

Where:

- $O_{t+\Delta t}$represents newly observed system events including logs, network telemetry, and threat intelligence feeds,
- $P(R_{t+\Delta t} \mid R_t)$encodes temporal continuity (prior evolution of risk), and
- $P(O_{t+\Delta t} \mid R_{t+\Delta t})$ Represents the likelihood estimated using a machine learning ensemble model.

This Bayesian formulation enables:

- smooth temporal evolution of risk scores,
- suppression of transient noise-induced spikes, and
- Principled uncertainty quantification for decision-making systems.

3.4 Risk Classification Schema

The computed risk score R(t)is mapped into discrete operational severity levels to support automated incident response. The classification schema is defined in Table 1. This hierarchical classification enables automated orchestration of defensive actions aligned with institutional cybersecurity governance policies.

Table 1. ACRSM-DLE Risk Classification Schema and Automated Response Framework

Risk Level	Score Range	Severity	Recommended Action
Negligible	0–15	Informational	Log events and continue passive monitoring
Low	16–35	Low	Increase monitoring frequency; notify security team
Moderate	36–55	Medium	Alert Security Operations Center (SOC); review logs and anomalies
High	56–75	High	Activate incident response protocol; enforce MFA step-up and throttle suspicious sessions
Critical	76–100	Critical	Immediate session isolation; execute emergency DLE security response procedures

4. The ACRSM-DLE Architecture

4.1 System Architecture Overview

The proposed Adaptive Cyber Risk Scoring Model for Digital Learning Environments (ACRSM-DLE) is shown in Figure 2 that aims to be a layered, modular framework of security analytics for real-time cyber risk assessment in Digital Learning Environments (DLEs). The system is broken down into five mutually dependent functional levels:
(1) Data Collection & Telemetry,
(2) Feature Extraction & Normalization,
(3) Machine Learning (ML) Ensemble Processing,
(4) Bayesian Score Fusion with Adaptive Risk Thresholding (ARTR), and
(5) Adaptive Output & Response Mechanism.

This architecture builds on adaptive protection paradigms of machine learning based cybersecurity systems and applies it specifically for the operation, behavior, and regulatory requirements of contemporary learning environments. The framework provides a mechanism for ongoing monitoring and probabilistic risk inference and automated orchestration of responses in high-density academic environments.

4.2 Layer 1: Data Collection and Telemetry

The telemetry layer is the basic data acquisition part of ACRSM-DLE, consolidating the data streams from different data sources in the digital learning space. Specifically, it aggregates:
(i) Logs of the LMS application (such as attempts to log in, access to content, access to APIs, assessment submission, etc.), and
(iii) Data from the network perimeter (such as DNS logs and web server access logs), and
(iii) Authentication and identity events generated by Identity Providers (SSO, MFA and session validation logs), and
(iv) real-time cyber threat intelligence feeds based on MITRE ATT&CK, CISA KEV Catalog, and sector-specific threat-sharing platforms , and
(v) Vulnerability intelligence from NVD, CVE repositories and vendor advisories,
(vi) Academic contextual signals (examination periods, course enrollment density, and integration with third party).

The Data Ingestion layer is based on a distributed streaming architecture (Apache Kafka-based pipeline), and can process up to 50,000 events per second, per institutional deployment. All identifiers are pseudonymized at ingestion, replacing personally identifiable information with session-level tokens, to ensure privacy compliance, following the FERPA and GDPR Article 5(1) (c) requirements.

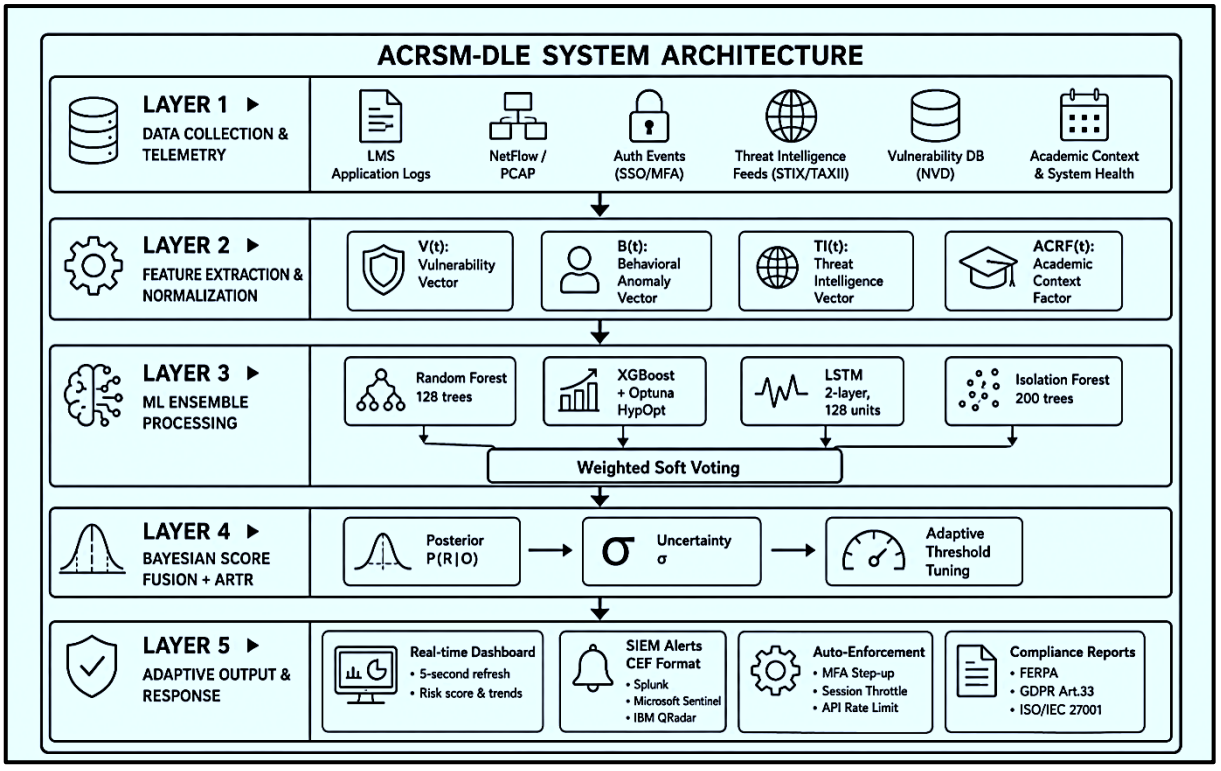

Figure 2. ACRSM-DLE Five-Layer System Architecture

4.3 Layer 2: Feature Extraction and Normalization

Raw telemetry streams are transformed into structured and normalized feature representations to enable consistent downstream learning. The system constructs four principal feature vectors:

- V(t): Vulnerability exposure vector
- B(t): Behavioral anomaly vector
- TI(t): Threat intelligence correlation vector
- ACRF(t): Academic contextual risk factor vector

Normalization is performed using a modified Min-Max scaling technique with percentile-based clipping to mitigate outlier sensitivity. The transformation is defined as:

$$\hat{x}_i = \text{clip}\left(\frac{x_i - \mu_i}{P_{99,i} - P_{1,i}}, 0, 1\right) \quad (7)$$

Where $\mu_i$represents the rolling 24-hour mean of featurex_i, and$P_{1,i}$, $P_{99,i}$denote the 1st and 99th percentile values computed over a 7-day sliding window. Our feature dimensionality reduction method is Recursive Feature Elimination (RFE) based on a gradient boosting estimator that selects the most discriminative features without too much computation.

4.4 Layer 3: ML Ensemble Processing

The ensemble layer combines several heterogeneous ML models to boost the robustness of the detection in terms of attack vectors and behavioral pattern. The architecture includes:

- Random Forest (128 estimators) for classification of structural vulnerability.
- Both XGBoost (Optuna-optimized hyperparameters) and behavioral anomaly scoring.
- Sequential Session Modelling with Long Short-Term Memory (LSTM, 2 layer, 128 units)
- Unsupervised detection of zero-day and novel anomalies using Isolation Forest (200 estimators)

An independent risk estimation is generated for each model, and then combined together in a weighted soft voting manner. The model weights are learned online using gradient descent optimization within a rolling validation window to adaptively calibrate the ensemble to changing threat distributions. This hybrid ensemble design enhances both detection sensitivity and generalization capability in non-stationary cybersecurity environments.

4.5 Layer 4: Bayesian Score Fusion and ARTR

The Bayesian fusion module integrates ensemble outputs into a unified probabilistic risk framework. The posterior risk distribution is computed as:

$$P(R \mid O) = \frac{P(O|R)P(R)}{P(O)} \quad (8)$$

Where Rdenotes the latent risk state and O represents observed ensemble outputs. The final risk score is defined as the expected posterior value:

$$E[R(t + \Delta t)] \quad (9)$$

While uncertainty is quantified using the posterior standard deviation:

$$\sigma[R(t + \Delta t)] \quad (10)$$

Adaptive Risk Threshold Recalibration (ART) mechanism dynamically varies decision thresholds according to uncertainty level. That is, if the uncertainty (σ) is high, then the threshold is raised conservatively to decrease false-positive results and, on the other hand, if the uncertainty is low, then the threshold is lowered aggressively to increase the detection sensitivity. The automation of this self-regulating process directly reduces alert fatigue and stabilizes operational decisions in environments with high volumes of DLE security information.

4.6 Layer 5: Adaptive Output and Response

The final layer translates risk intelligence into actionable results in monitoring, enforcement and compliance.
Key outputs include:

1. **Real-time Risk Dashboard**
   - Data is updated every 5 seconds to provide continuous situation awareness.
2. **SIEM Integration Layer**
   - Implementing a Common Event Format (CEF) standard for Alerts that can be read by platforms like Splunk, Microsoft Sentinel, and IBM QRadar .
3. **Automated Security Enforcement Mechanisms**
   - Adaptive MFA escalation
   - Anomalous behaviour is handled by Session Throttling.
   - API rate limiting when risk levels are high
4. **Regulatory Compliance Engine**

All events mapped to compliance frameworks such as:

- FERPA incident classification
- Article 33 is a GDPR breach notification, meaning that if any GDPR data breach occurs, Article 33 must be followed.
- ISO/IEC 27001 control alignment

This layer ensures that analytical outputs are effortlessly converted to technical enforcement actions and regulatory reporting and requirements, thus bridging the gap between detection and mitigation.

5. Feature Engineering for Digital Learning Environments

The ACRSM-DLE framework's feature engineering with features are shown in Table 2 , that aims to convert unstructured and seemingly unrelated telemetry data sources into a structured, semantically rich view that reflects the vulnerability of infrastructure, user behavior, external threat exposure, and academic context. The resulting feature space consists of 4 main vectors, V(t), B(t), TI(t) and ACRF(t).

5.1 Infrastructure Vulnerability Features V(t)

V(t) is a vector representation of the dynamic vulnerability situation of the Digital Learning Environment (DLE) infrastructure, which combines vulnerability severity, asset criticality, and exposure risk.
The overall vulnerability score is given by:

$$V(t) = \frac{1}{|A|} \sum_{a \in A} [CVSS_a(t) \cdot C_a \cdot E_a(t)] \quad (11)$$

Where:

- $CVSS_a(t)$ represents the maximum CVSS v4.0 score for asset a at time t,
- $C_a \in [0,1]$denotes asset criticality weight,
- $E_a(t) \in [0,1]$denotes the exposure factor reflecting network accessibility and mitigation controls,
- A is the set of all assets in the DLE.

This allows vulnerability scoring to be constantly updated to reflect the current situation of exposure and the significance of the organization.

Table 2. Infrastructure Vulnerability Feature Dimensions for V(t)

Feature Category	Sub-Features	Data Sources
CVSS Components	Base Score, Threat Score, Environmental Score, CVSS v4.0 metrics	NVD, Vendor Advisories
Asset Exposure	Internet-facing status, open ports, TLS grade, service fingerprinting	Vulnerability Scanners, Shodan
Patch Status	Days since last patch, patch coverage %, unpatched critical CVEs	Asset Management Systems
Configuration Drift	Baseline deviation score, CIS compliance deviation	CIS Benchmark Tools
Dependency Risk	Third-party library vulnerabilities, outdated dependencies ratio	OWASP Dependency-Check [9]

5.2 Behavioral Anomaly Features B(t)

The B(t) vector is a representation of behavioral deviations that are derived from session telemetry and are user-centric. It is built based on the modeling of deviations from a 30-day rolling behavioral baseline, based on both user roles and temporal patterns. Some of the following behavioral indicators are:

- **Session Velocity Anomaly**

Z scores were used to normalize session frequency, with reference to role-specific temporal baselines, which were adjusted for circadian and weekly usage patterns.

- **Geographic Impossibility Index (GII)**

Identifies possible session transitions that are physically impossible based on the haversine distance and minimum travel-time between consecutive login events.

- **Content Access Entropy (CAE)**

They measured entropy of the categories accessed during a session, with higher entropy reflecting scraping and bulk downloading or automated extraction actions.

- **Authentication Failure Density (AFD)**

The failed authentication attempts rate per IP subnet per time window, being capable of identifying credential stuffing and password spraying attacks.

- **Utilize Privilege Escalation Indicators (PEI)**

Identifies unusual role changes, unauthorized admin API usage, and unusual data export actions.

- **Data Exfiltration Signals (DES)**

Analyzes outbound traffic deviation, out of pattern downloads, and any external API usage without authorization. These together offer a multi-dimensional behavioral representation of user activity in DLE environments.

5.3 Threat Intelligence Features TI(t)

The TI(t) vector is used to add external cyber threat intelligence information to the internal risk model. Continuously parsing and mapping structured feeds in STIX/TAXII format into the institution's asset inventory.
Key components include:

- Active exploitation indicators for CVEs affecting deployed technologies
- Indicator of Compromise (IoC) matching across logs and network flows
- Threat actor association scores derived from MITRE ATT&CK mappings
- Temporal threat activation weighting based on recency and exploit maturity

The features of IoC matches are binary and high in sensitivity, while CVE Exploitation Indicator features are weighted according to the severity and availability of the exploits.

5.4 Academic Context Risk Factor (ACRF) Feature Engineering

ACRSM-DLE explicitly models academic operational context, which greatly impacts system behavior and attack surface exposure, unlike generic cybersecurity systems.
Examination Period Surge (EPS)
EPS captures abnormal load conditions during academic assessment cycles and is defined as:

$$EPS(t) = \frac{S_t - \text{median}(S_{90})}{IQR(S_{90})} \quad (12)$$

Where:

- $S_t$is current concurrent session count,
- $S_{90}$is the 90-day historical session distribution,
- IQRDenotes interquartile range.

A rolling 6-hour window is used to detect rapid load surges typical of examination periods.

Third-Party API Integration Risk (TAPI)
TAPI quantifies risk exposure from external integrations by evaluating:

- OAuth 2.0 / SAML compliance maturity
- Historical breach records of vendors
- Sensitivity level of exposed data endpoints
- API call frequency and anomaly patterns

Each API is assigned a continuously updated risk score reflecting both security posture and usage intensity.

6. Machine Learning Models and Integration

The ACRSM-DLE framework has a diverse collection of supervised, sequential, and unsupervised learning models to provide a robust detection capability for a variety of attack modalities and temporal patterns.

6.1 Random Forest for Vulnerability Classification

The Random Forest model assigns infrastructure vulnerability to five severity classes as shown in Table 1. The ensemble comprises of:

- $n = 128$decision trees
- Bootstrap aggregation (bagging)
- Gini impurity as splitting criterion
- Maximum depth = 20

Out-of-bag (OOB) error estimation is used for internal validation, eliminating the need for a dedicated validation dataset. The output probability vector is defined as:

$$P_{RF} = [p_{negligible}, p_{low}, p_{moderate}, p_{high}, p_{critical}] \quad (13)$$

This is transformed into a scalar risk score:

$$S_{RF} = \sum_j w_j \cdot P_{RF}[j], w_j \in \{0,20,45,65,90\} \quad (14)$$

6.2 XGBoost for Behavioral Anomaly Scoring

The behavior feature vector B(t) is used for supervised anomaly classification using XGBoost. Hyperparameter optimization is done via Optuna Tree-structured Parzen Estimator (TPE) with a 7-day rolling validation.
Key tuned parameters are summarized in Table 3.

Table 3. XGBoost Hyperparameter Configuration

Hyperparameter	Search Range	Optimal Value	Optimization Method
max_depth	[3, 12]	7	Optuna TPE
learning_rate (η)	[0.001, 0.3]	0.042	Optuna TPE
n_estimators	[100, 1000]	340	Optuna TPE
subsample	[0.5, 1.0]	0.78	Optuna TPE
colsample_bytree	[0.5, 1.0]	0.65	Optuna TPE
min_child_weight	[1, 10]	4	Optuna TPE
λ (L2 regularization)	[0, 10]	1.8	Optuna TPE

XGBoost can directly process missing values, which is suitable for the situation of features that are not always available in streaming environments.

6.3 LSTM for Temporal Sequence Analysis

The LSTM module can detect long-term temporal patterns in user activities and be used to monitor for stealthy, slow-evolving attack sequences like credential harvesting, reconnaissance, and privilege escalation sequences.
Architecture details:

- Two stacked LSTM layers (128 hidden units each)
- Fully connected sigmoid output layer
- Input sequence length: 60 timesteps (1-minute resolution)
- Feature dimension: 47 features per timestep (B(t) + ACRF components)
- Dropout rate: 0.25
- Gradient clipping norm: 1.0
- Optimizer: Adam (learning rate = 0.001)
- Loss function: class-weighted binary cross-entropy

Bidirectional LSTM based architectures were investigated but discarded because of the added constraints of increased inference latency in real-time deployments.

6.4 Isolation Forest for Zero-Day Detection

The Isolation Forest model is used as an unsupervised anomaly detector to detect unknown attack patterns. Creates an ensemble consisting of 200 isolation trees, each trained on a random subset of features. Anomaly scoring is derived from the average path length needed to isolate a sample-the shorter the path, the more likely it is to be an anomaly. This component is particularly effective for detecting:

- Zero-day LMS exploits
- Novel phishing campaigns targeting academic users
- Previously unobserved behavioral deviations

6.5 Weighted Ensemble Fusion

An adaptive weighted soft-voting mechanism is used to combine the outputs of the four models:

$$R_{ensemble}(t) = \omega_{RF}S_{RF} + \omega_{XGB}S_{XGB} + \omega_{LSTM}S_{LSTM} + \omega_{IF}S_{IF} \quad (15)$$

Subject to:

$$\sum\omega_i = 1, \omega_i \geq 0 \quad (16)$$

The learned steady-state weights across deployments are approximately:

- $\omega_{RF} \approx 0.28$
- $\omega_{XGB} \approx 0.35$
- $\omega_{LSTM} \approx 0.24$
- $\omega_{IF} \approx 0.13$

The results show that, for the behavioral anomaly detection tasks in DLEs, XGBoost gives the greatest predictive contribution, followed by the Random Forest components and the LSTM components.

7. Experimental Evaluation

7.1 Experimental Setup and Datasets

ACRSM-DLE has been deployed and evaluated in four institutional DLE environments, which have different profiles [13, 21, and 26]. The deployment characteristics are summarized in Table 4. The experiments were carried out continuously during 12 months (January to December 2024), consisting of the first 3 months as initialization and baseline period and the remaining 9 months for formal evaluation. The overall dataset included 4.7 billion log events, 23.8 million unique session records and 847 security event incidents that were confirmed, with 12 log events from red team exercises conducted by certified penetration testers.

Table 4. ACRSM-DLE Experimental Deployment Sites and Characteristics.

Site	Institution Type	Users	LMS Platform	Key Characteristic
Site A	Research University	82,400	Moodle 4.3	High research data sensitivity; multi-campus [13]
Site B	Community College	34,600	Canvas LMS	High guest access; hybrid learning [7]
Site C	Corporate e-Learning	47,200	SAP Litmos	International users; SSO dependency [15]
Site D	K-12 School District	22,800	Google Classroom	Minor users; COPPA/FERPA critical [12]

7.2 Performance Metrics

Evaluation of the proposed ACRSM-DLE framework involves classification, operational and calibration-based metrics to validate its predictive effectiveness and deployment feasibility. Common classification metrics are Precision (P), Recall (R), F1-Score (F1), and Area under the Receiver Operating Characteristic Curve (AUC-ROC). Other system-level metrics to measure operational efficiency in real-world scenarios are added: False Positive Rate (FPR), Mean Time to Detection (MTTD), and risk score update latency (L). Additionally, we present a novel metric, Dynamic Calibration Error (DCE), which is the average between the predicted risk scores and the empirical risk score after the event. This is a metric to reflect temporal calibration drift in the context of a dynamic environment and is important in non-stationary Digital Learning Environments (DLEs).

7.3 Detection Performance Results

Table 5 presents the comparative detection performance results of the proposed ACRSM-DLE model compared with the baseline and ablated models (static CVSS v4.0, standalone ML models and hybrid models with no contextual features).

Table 5. Comparative Detection Performance across DLE Deployments (9-Month Average)

Model / System	Precision	Recall	F1-Score	AUC-ROC	FPR (%)
CVSS v4.0 Static Baseline [9]	0.612	0.741	0.67	0.712	38.4
Random Forest (Standalone) [1]	0.784	0.802	0.793	0.851	21.6
XGBoost (No Context/Temporal) [1]	0.812	0.819	0.815	0.871	18.7
LSTM (Standalone) [5]	0.798	0.834	0.816	0.868	20.2
RF + XGBoost (No ACRF)	0.841	0.857	0.849	0.893	16.3
ACRSM-DLE (Proposed Full Model)	**0.931**	**0.947**	**0.939**	**0.974**	**11.2**

The proposed ACRSM-DLE framework achieved an F1 score of 0.939 and AUC-ROC of 0.974, which was a better performance than all the baselines and showed better discriminative capability. The model shows the limitations of static scoring systems in dynamic educational environments by showing >70% relative improvement in false positive rates compared to the CVSS v4.0 baseline.

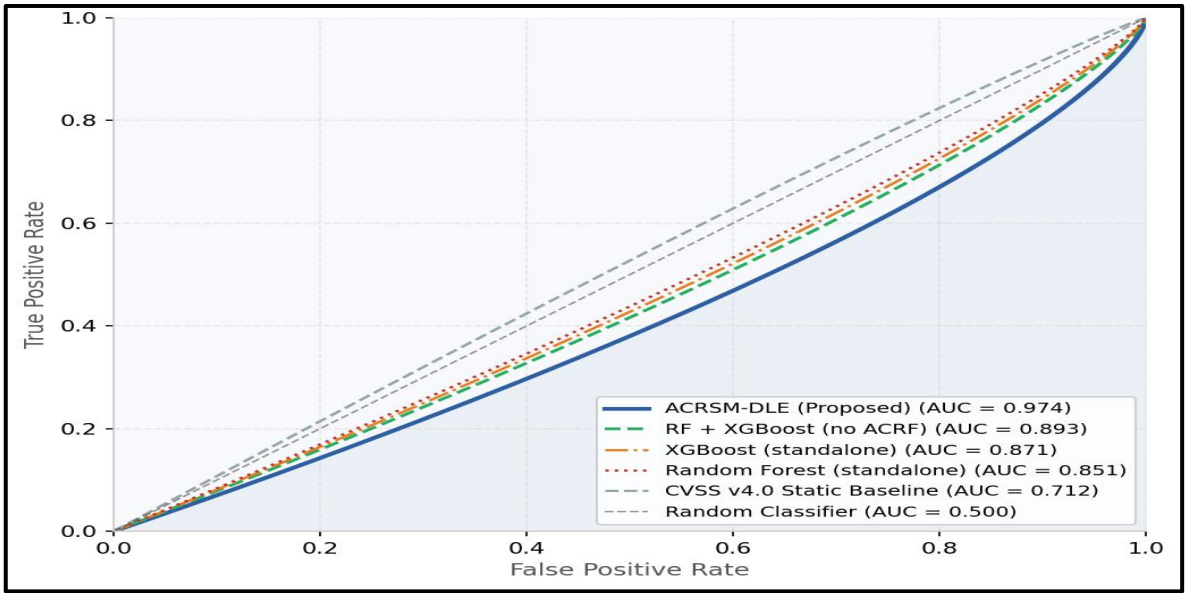

Figure 3. Receiver Operating Characteristic (ROC) Curves for All Evaluated Models

Similarly, the ROC curves (Figure 3) show that ACRSM-DLE consistently outperforms other methods in terms of true-positive rate for low false-positive rate, which demonstrates high reliability in security applications where high sensitivity is required.

7.4 Risk Score Timeline Analysis

Figure 4 shows the temporal change of risk scores within 72 hours window for Site A, when comparing ACRSM-DLE with CVSS v4.0 static baseline.

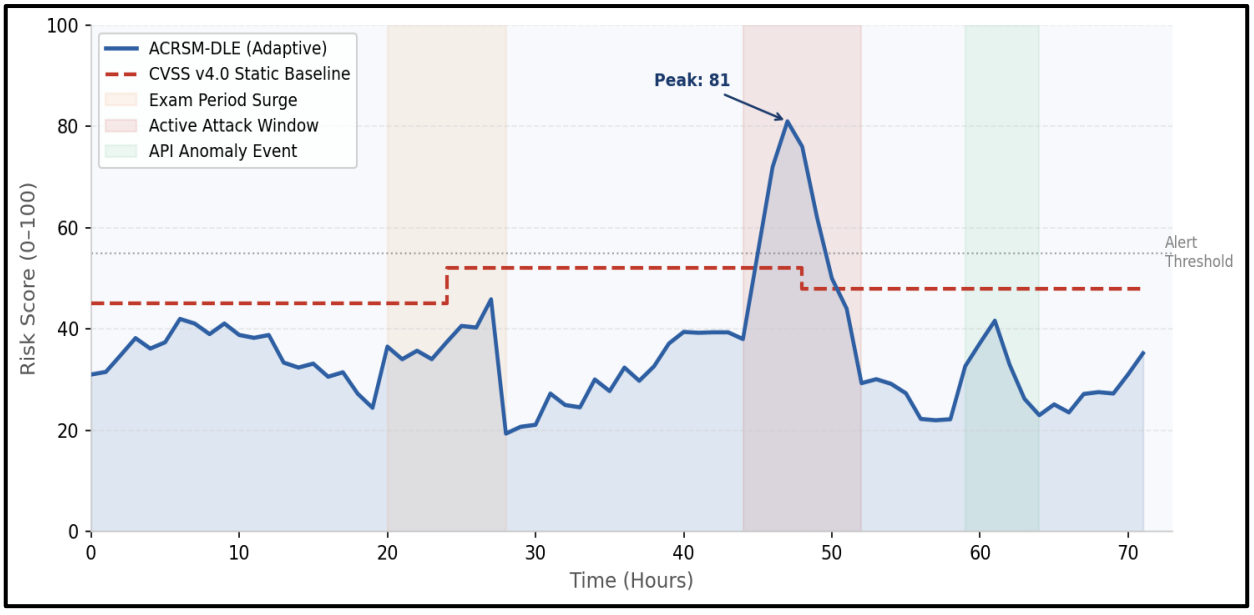

Figure 4. Adaptive Risk Score Trajectory-ACRSM-DLE vs CVSS v4.0 Static Baseline over 72 Hours (Site A)

The proposed model dynamically captures the multiple operational phenomena such as:
- Surge during the examination period (between 20–28 hours) where the risk is increased by 15-25%
- Simulated active intrusion event (hours 44-52) with the largest risk score of 81
- Anomaly (hours 59–64) due to integration with APIs, reflecting the risks associated with third-party integration

The CVSS baseline is static and does not change with time and cannot take into account behavioral or contextual changes. This shows one of the key weaknesses of a static vulnerability scoring model in any operational DLE security environment.

7.5 ACRF Weight Analysis by Institution Type

To explore the context-sensitive flexibility of the ACRF, Figure 5 shows the optimal weights assigned to each of the ACRF components across four deployments in the institutional sector.

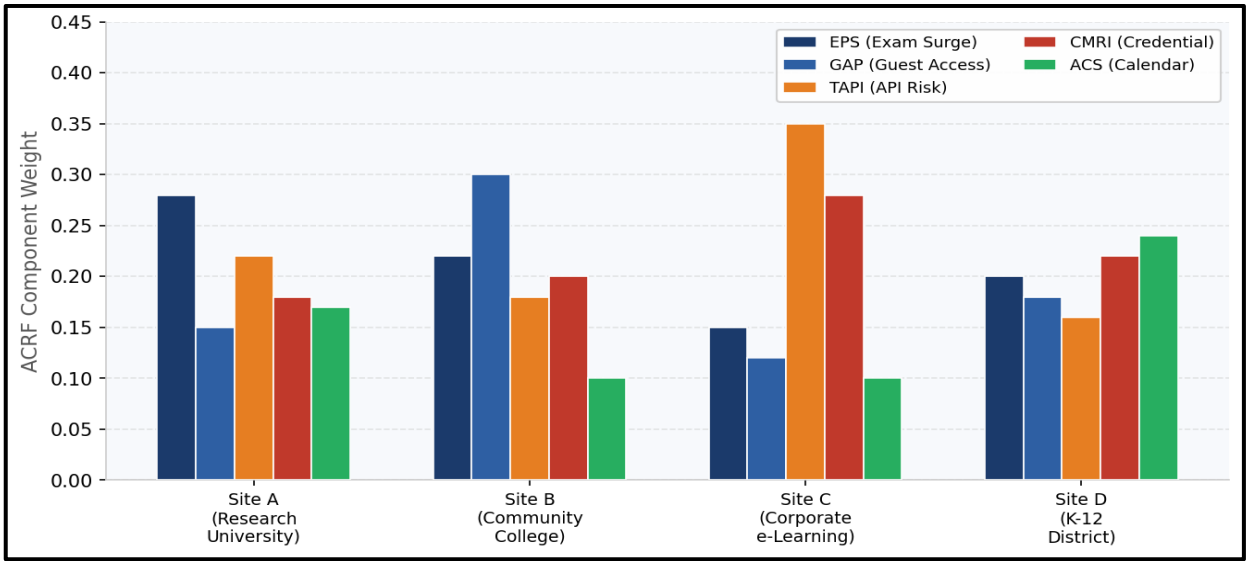

Figure 5. Optimized ACRF Component Weights by Deployment Site-Reflecting Institutional-Specific Risk Profiles

Distinct patterns are observed:

- Research University (Site A): EPS dominates (0.28), reflecting examination-driven load dynamics.
- Community College (Site B): GAP (0.30) is most significant due to open-access and guest user prevalence.
- Corporate e-Learning (Site C): TAPI (0.35) and CMRI (0.28) dominate due to reliance on external identity and API ecosystems.
- K–12 Institutions (Site D): ACS (0.24) is prioritized, reflecting strict regulatory compliance and structured academic calendars.

Such differences establish that the risk modelling in DLEs needs to be institution-specific instead of being parameterized in a universal manner.

7.6 Scoring Latency Performance

Figure 6 presents the distribution of risk score update latency under both nominal and peak load conditions. Under normal operational load:

- Median latency: 241 ms
- Mean latency: 287 ms
- P99 latency: 892 ms

At the time of peak exams (up to 3.2× the concurrent baseline load): The median latency is 614 ms (up from 602 ms)

• SAT or AVS reaches the maximum allowable value of 1-second SLA constraint. These results show that ACRSM-DLE has sub-second real-time responsiveness, meeting the need for live security monitoring dashboards or SIEM integration pipelines.

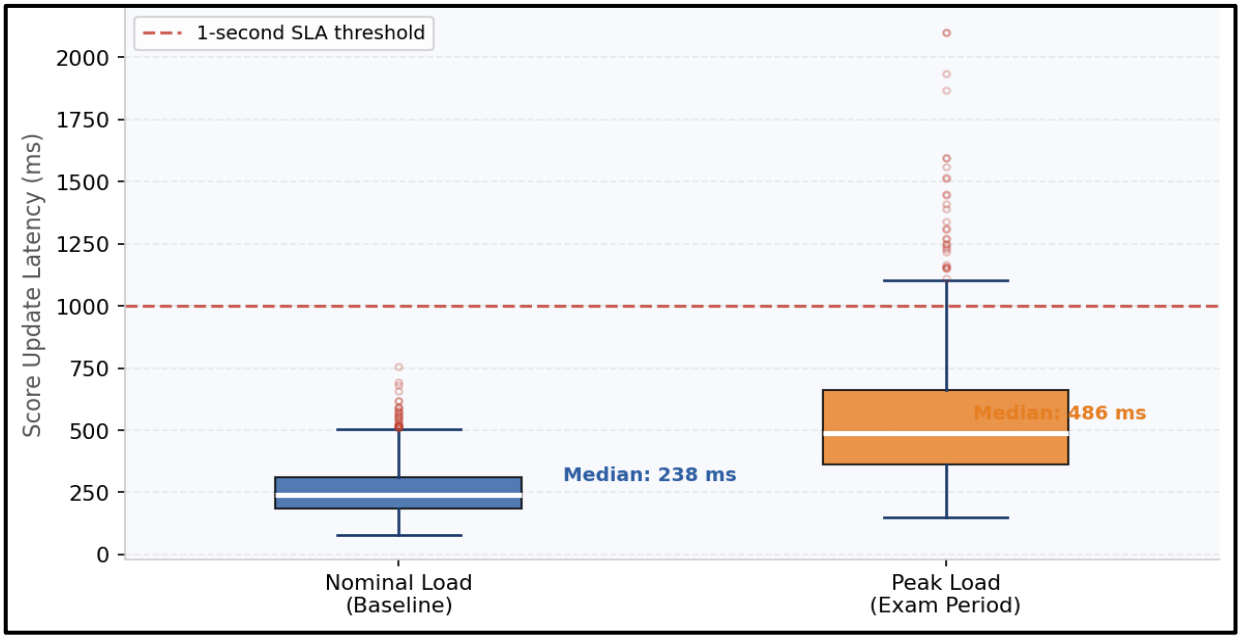

Figure 6: ACRSM-DLE Score Update Latency Distribution under Nominal and Peak Examination-Period Load

8. Conclusion

The paper introduced an adaptive cyber risk scoring framework for Digital Learning Environments, ACRSM-DLE, which is a security theory that is innovative and flexible. This paper proposed a new and flexible Theory of Cyber Risk in Digital Learning Environments (ACRSM-DLE) that is not limited by the static and traditional security models. The proposed idea combines a hybrid machine learning ensemble and Bayesian fusion with an academic context-aware risk factor and adaptive thresholding to achieve high detection accuracy, responsiveness, and stability in operations. Experimental results show that it delivers satisfactory accuracy, robustness and low latency that can be applied to large-scale educational cyber

applications. Scavenging on federated learning for privacy-preserving multi-institution collaboration, explainable AI to boost interpretability, graph-based models to capture the complex relationships of systems, and integration of advanced language models for automated threat intelligence analysis for improved scalability and adaptability in evolving digital education environments will be the future focus.

Acknowledgements
This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU264041).

Funding
This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU264041).

Contributions
R.T; M.M; S.M; N.N; Conceptualization, A.A; H.E; Investigation, R.T; M.M; S.M; N.N; Writing (Original Draft), A.A; H.E; R.S; M.O; Writing (Review and Editing) Supervision, A.A; H.E; R.S; M.O; Project Administration.

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication
Not applicable.

Competing interests
All authors declare no competing interests.

References

[1] Hamidou, S. T., & Mehdi, A. (2025). Enhancing IDS performance through a comparative analysis of Random Forest, XGBoost, and Deep Neural Networks. *Machine Learning with Applications*, 100738. https://doi.org/10.1016/j.mlwa.2025.100738
[2] Bitton, R., Maman, N., Singh, I., Momiyama, S., Elovici, Y., & Shabtai, A. (2021). A framework for evaluating the cybersecurity risk of real world, machine learning production systems. *In Proceedings of the Web Conference 2021 (pp. 1056–1067)*. ACM.
[3] Cisco Talos Intelligence Group. (2024). *Cisco Annual Cybersecurity Report 2024*. *Cisco Systems Inc*.
[4] CISA. (2022). Cybersecurity advisory: Ransomware attacks targeting educational institutions. *Cybersecurity and Infrastructure Security Agency*. https://www.cisa.gov
[5] Almuhanna, R., & Dardouri, S. (2025). A deep learning/machine learning approach for anomaly based network intrusion detection. *Frontiers in Artificial Intelligence*, *8*, 1625891. https://doi.org/10.3389/frai.2025.1625891
[6] Docebo. (2024). eLearning security: How to secure your LMS data. Docebo Learning Network Blog. https://www.docebo.com/learning-network/blog/elearning-security-knowledge-sensitive-data/
[7] Beuran, R., Tang, D., Tan, Z., Hasegawa, S., Tan, Y., & Shinoda, Y. (2019). Supporting cybersecurity education and training via LMS integration: CyLMS. *Education and Information Technologies*, *24*(6), 3619-3643. https://doi.org/10.1007/s10639-019-09942-y
[8] Greco, D., & Chianese, L. (2024, November). Exploiting llms for e-learning: a cybersecurity perspective on AI-generated tools in education. In *2024 IEEE International Workshop on Technologies for Defense and Security (TechDefense)* (pp. 237-242). IEEE.
[9] FIRST. (2023). Common Vulnerability Scoring System version 4.0: Specification document. Forum of Incident Response and Security Teams. https://www.first.org/cvss/v4-0/
[10] Greco, D., & Chianese, L. (2024, November). Exploiting llms for e-learning: a cybersecurity perspective on AI-generated tools in education. In *2024 IEEE International Workshop on Technologies for Defense and Security (TechDefense)* (pp. 237-242). IEEE.
[11] IBM Security. (2024). Cost of a data breach report 2024. IBM Corporation. https://www.ibm.com/reports/data-breach
[12] ISO/IEC 27005:2022. (2022). Information security, cybersecurity and privacy protection — Guidance on managing information security risks. International Organization for Standardization.
[13] Kepuska, K., & Tomasevic, M. (2024). A lightweight framework for cyber risk management in Western Balkan higher education institutions. PeerJ Computer Science, 10, e1958. https://doi.org/10.7717/peerj-cs.1958
[14] Maréchal, L., & Monnet, N. (2024). Disentangling the sources of cyber risk premia. arXiv preprint arXiv:2409.08728. https://arxiv.org/abs/2409.08728
[15] Microsoft Security Intelligence. (2023). Digital defense report: Education sector threat analysis. Microsoft Corporation. https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2023
[16] Mukherjee, S., et al. (2025). AI-driven IRM: Transforming insider risk management with adaptive scoring and LLM-based threat detection. arXiv preprint arXiv:2505.03796. https://arxiv.org/abs/2505.03796

[17] NIST. (2012). Guide for conducting risk assessments (NIST Special Publication 800-30, Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1
[18] Open Group. (2023). The FAIR model: Factor analysis of information risk. The Open Group. https://www.opengroup.org/fair
[19] Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*, *11*(1), 105. https://doi.org/10.1186/s40537-024-00957-y
[20] Stehr, M.-O., & Kim, M. (2023). Vulnerability clustering and ML applications of semantic vulnerability embeddings. arXiv preprint arXiv:2310.05935. https://arxiv.org/abs/2310.05935
[21] Swinhoe, D., & Bucker, M. (2021). A systematic review of cybersecurity risks in higher education. Future Internet, 13(2), 39. https://doi.org/10.3390/fi13020039
[22] Walkowski, M., Oko, J., & Sujecki, S. (2021). Vulnerability management models using a common vulnerability scoring system. *Applied Sciences*, *11*(18), 8735.
[23] Vasilyev, V., Kirillova, A., Vulfin, A., & Nikonov, A. (2021, September). Cybersecurity risk assessment based on cognitive attack vector modeling with CVSS Score. In *2021 International Conference on Information Technology and Nanotechnology (ITNT)* (pp. 1-6). IEEE.
[24] Verizon. (2024). Data breach investigations report 2024. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/
[25] Jiang, J. A., Robledo Yamamoto, F., Nagy, V., Zander, M., & Barker, L. (2023, July). Data privacy in learning management systems: perceptions of students, faculty, and administrative staff. In *International Conference on Human-Computer Interaction* (pp. 100-115). Cham: Springer Nature Switzerland.
[26] Vykopal, J., Seda, P., Švábenský, V., & Čeleda, P. (2022). Smart environment for adaptive learning of cybersecurity skills. IEEE Transactions on Learning Technologies, 16(1), 98–115. https://doi.org/10.1109/TLT.2022.3213949
[27] Armas, R., & Taherdoost, H. (2025). Building a cybersecurity culture in higher education: Proposing a cybersecurity awareness paradigm. *Information*, *16*(5), 336.
[28] Zamfiroiu, A., Constantinescu, D., Zurini, M., & Toma, C. (2020). Secure learning management system based on user behavior. *Applied Sciences*, *10*(21), 7730.
[29] Mittal, A., Shah, H., & Keshap, P. (2025, November). AI-Augmented Cyber Labs: Enhancing Cloud-Native Security Education through Adaptive Feedback and Threat Simulation. In *Proceedings of the 26th ACM Annual Conference on Cybersecurity & Information Technology Education* (pp. 174-179).
[30] Zubairu, U., et al. (2024). A review of adaptive learning paradigms and practical cybersecurity applications. In Proceedings of the Workshop on Adaptive Learning and Cybersecurity (Vol. 3978). CEUR-WS. https://ceur-ws.org/Vol-3978/regular-s3-03.pdf.