

Adaptive Security Model for E-Learning Platforms Using Multi-Layered Anomaly Detection and Context-Aware Risk Assessment

Ronald M. Hernández^{1*}, Doris Fuster-Guillen², Luisa Graciela Ponce Maluquish³, Miguel Luis Chuquispuma Caycho⁴, and Mery Nora Atencio Rivera⁵

^{1*}Grupo de Investigación Innovación en Educación y Salud, Universidad Señor de Sipán, Chiclayo, Perú. ronald.hernandez@outlook.com.pe, <https://orcid.org/0000-0003-1263-2454>

²Universidad Nacional Mayor de San Marcos, Perú. dfusterg@unmsm.edu.pe, <https://orcid.org/0000-0002-7889-2243>

³Universidad Nacional Mayor de San Marcos, Perú. lponcem2@unmsm.edu.pe, <https://orcid.org/0000-0003-3904-2112>

⁴Universidad Nacional Mayor de San Marcos, Perú. miguel.chuquispuma1@unmsm.edu.pe, <https://orcid.org/0000-0001-5539-333X>

⁵Universidad Nacional Intercultural de la Selva Central Juan Santos Atahualpa, Perú. atenciorivera@uniscjsa.edu.pe, <https://orcid.org/0000-0002-3599-4696>

Received: October 16, 2025; Revised: November 24, 2025; Accepted: January 15, 2026; Published: February 27, 2026

Abstract

With the broad use of e-learning platforms in institutions of higher learning and corporate training, the cyber-attack surface has grown considerably, placing the digital learning ecosystem at risk of account takeover, credential stuffing, insider abuse, automated bot attacks, and examination fraud. The conventional rule-based and signature-based security systems cannot identify dynamic and context-sensitive attacks. In this paper, the author presents a recommendation of an Adaptive Security Model of an e-learning platform that combines both Multi-Layered Anomaly Detection and Context-Aware Risk Assessment to enhance detection accuracy and reduce cases of false alarms. The framework integrates behaviour profiling, network traffic analytics, device fingerprinting, and session-based anomaly scoring in a hierarchical structure. A hybrid engine is used to identify known and unknown attacks, combining a Random Forest by using LSTM-based sequential modeling and an Isolation Forest. Dynamic risk scoring takes into consideration contextual parameters such as a deviation of the location of logins, temporal irregularity, frequency of access, patterns of device change, and anomalies of course interaction. Experimental evaluation conducted on a dataset comprising 135,687 user sessions demonstrates that the proposed model achieves 96.8% detection accuracy, 95.4% precision, and 94.9% recall with a 2.7% false positive rate, outperforming single-layer detection systems by 11.3% in F1-score and achieving an AUC of 0.979 and MCC of 0.944. The strength of the improvements in the case of various attack scenarios is statistically tested ($p < 0.01$). The findings confirm the fact that implementing multi-layer anomaly detection in combination with adaptive context-driven risk assessment can play a critical role in improving

Journal of Internet Services and Information Security (JISIS), volume: 16, number: 1 (February-2026), pp. 747-759.
DOI: 10.58346/JISIS.2026.11.043

*Corresponding author: Grupo de Investigación Innovación en Educación y Salud, Universidad Señor de Sipán, Chiclayo, Perú.

security posture without affecting user experience, which offers an intelligent and scalable architecture to present-day e-learning platforms.

Keywords: Adaptive Security Model, E-Learning Platform Security, Multi-Layered Anomaly Detection, Context-Aware Risk Assessment, Behavioural Analytics, Intrusion Detection Systems, Cyber Threat Mitigation.

1 Introduction

The enhanced digitalization in the educational field has seen the widespread implementation of electronic learning platforms worldwide, which provide unprecedented access, flexibility, and scalability (Abibulaiev et al., 2026). Nevertheless, the given transition has also expanded the Area of cyber-attacks, exposing the learning management systems to such advanced threats as credential compromise, session hijacking, exploitation by bots, and attempts at unauthorized access. Conventional signature-based and static policy-based security systems fail to keep pace with changes in dynamic patterns of threats and changing behaviour of users, leading to the rise of false positives and a lack of defence coverage. The need for adaptive, intelligent security models to rely upon both anomaly detection and contextual risk analysis has gained critical momentum in recent studies on cybersecurity.

Machine-learning-driven anomaly detection has demonstrated in detecting deviations from normal behavioural patterns and countering unknown attacks through a variety of networked systems (Cui et al., 2019). A number of studies prove the effectiveness of combining hybrid machine learning and deep learning structures to increase detection accuracy and strength in intrusion detection contexts, which form a pathfinder background to adaptive systems needed to suit intricate digital conditions (Almuhanna & Dardouri, 2025). Systematic literature reviews in the e-learning and higher education security domain show that AI-based cybersecurity systems are significantly more effective in detecting threats more precisely and lowering false positives compared to conventional methods (Sarker, 2023). By combining the supervised and unsupervised learning models, more detailed behavioural profiling and anomaly detection become possible, which is essential to securing platforms with heterogeneous user interactions.

In addition, studies have shown the value of context-sensitive security codes, in which access control decisions are based on a number of environmental and behavioural factors, including time trends and device characteristics, that allow elite risk evaluation and proactive implementation of policy (Sridharan et al., 2025). Anomaly detection systems powered by machine learning have also been evaluated in terms of their applicability in the real world, which also points to such advantages as the operational benefits and such disadvantages as the large false positive rates and the data imbalance problems. Anomaly detectors and ensemble learning have been demonstrated to enhance the performance of hybrid intrusion detection systems that detect new threats to the education network (Liu et al., 2024; Oroni et al., 2025). An emerging literature also dwells further on the topic of dynamic scoring of risk and adaptive access control policies as significant factors that help in upholding cybersecurity resilience in digital systems. In addition to anomaly detection, context-based frameworks use environmental data to improve the access control decision-making process and alleviate misuse (Ashok Kumar & Venugopalan, 2017). Besides this, systematic surveys of machine learning algorithms in network anomaly detection note model scalability, interpretability, and threat invariance as the current research priorities (Khan et al., 2023). All these studies point towards the fact that the combination of a multi-layered solution of anomaly detection and context-based risk evaluation can be a valuable tool in securing an adaptive e-learning space against the current and future cyber threats (Rabih et al., 2025).

Key Contributions

- The paper puts forward a new multi-layered adaptive security architecture that incorporates supervised, sequential, and unsupervised anomaly detection in an integrated architecture in e-learning environments.
- It presents a contextualized dynamic risk scoring scheme, which modulates access controls depending on behavioural and environmental anomalies.
- The study demonstrates statistically significant performance improvement, achieving 96.8% detection accuracy with only 2.7% false positives and an 11.3% F1-score gain over conventional systems.
- A complete experimental validation and ablation study, along with statistical significance testing, prove the strength and generality of the suggested framework.

The rest of the paper is organized in the following way. Section I provides the introduction and motivation of adaptive security in e-learning platforms. Section II surveys the recent research on the topic of anomaly detection and context-sensitive risk assessment. Section III outlines the methodology proposed, which includes a description of the architectural design, the formulation of algorithms, and mathematical models. IV is a description of experimental evaluation, performance comparison, and ablation analysis. Lastly, Section V summarizes the paper and gives the future research directions.

2 Literature Survey

The recent studies in the field of anomaly detection, context-aware risk analysis, and intelligent intrusion detection emphasize the important improvements that guide and encourage the development of our suggested adaptive security model.

The latest research highlights the importance of machine learning and hybrid methods in the detection of anomalies and intrusions. The publications on scaled anomaly detection models show that an emphasis on supervised and unsupervised learning proves beneficial in improving the accuracy and flexibility of these methods in countering threats that are dynamic and concept drift in network security systems (Highnam et al., 2021). Ensemble and hybrid models applying several different learning paradigms, like autoencoders to conventional classifiers, demonstrate better performance on zero-day attacks and uncommon threats, which is worth the investment in multi-layered learning in cybersecurity (Hozouri et al., 2025). In line with this, CNN-enhanced intrusion system studies indicate that the complex attack vectors are detected with important performance enhancement through the usage of spatial and temporal attributes computed on the traffic record (Ozdem, 2025). Moreover, studies that combine both local outlier detection algorithms like LOF with the neural networks demonstrate that the combination of statistical and neural frameworks can further increase the level of detection and robustness (Arnob et al., 2025).

The context-sensitive security and adaptable schemes have become popular as well. Systematic surveys focus on context-aware access control and behaviour-driven security mechanisms, with risk scoring on environmental and session parameters being used to augment decision-making as opposed to existing rules (Golchin et al., 2024). Equally, the works of heterogeneous anomaly detection emphasize the necessity to correlate the wide-ranging telemetry and user behaviour data to model normal behaviour and correctly indicate abnormal behaviour (Kumar & Gutierrez, 2025). An intrusion detection system based on deep learning can produce systematic reviews of documentation that can be adapted to continuous learning frameworks that are more efficient in responding to the changing threats of dynamic

network environments like SDN-IoT structures (Zhu et al., 2012). Transformer-based and explainable models that would enhance the interpretability and generalizability of anomaly detection systems are further investigated in the literature, which, in turn, is consistent with the requirement of a transparent security solution in learning and business environments (Wada et al., 2025).

The other challenges mentioned in both empirical and review studies include the false positive rate, scalability, and balancing sensitivity and specificity, and it is recommended to keep advancing the hybrid architectures to obtain the best performance (Mizanur et al., 2025). Lastly, the integrated system of the machine learning-based IDS models has been justified as extensive surveys prevent the use of supervised and unsupervised methods to ensure optimal detection and resilience of machine learning-based IDS in various datasets (Punia et al., 2025).

Inference: Collectively, the literature confirms that hybrid anomaly detectors, context-sensitive risk assessment, and adaptive learning architectures have a noticeable positive effect on intrusion detection accuracy and resilience, which directly serves as the driving force behind the multi-layered approach and context-sensitive computing approach suggested in this paper.

3 Methodology

Proposed Adaptive Security Model Overview

The Adaptive Security Model proposed is aimed at detecting abnormal activities and dynamically measuring the contextual risk during e-learning contexts. The architecture, as shown in Figure 1, comprises four main steps: data acquisition, multi-layered anomaly detection, context-based risk assessment, and dynamic decision generation.

At the initial level, user behavioural logs, network traffic logs, device attributes, and contextual parameters that are homogeneous data sources are gathered. These data streams are preprocessed and features extracted to form normalized feature vectors. The multi-Layered Anomaly Detection Engine is used in the second stage and works on three complementary models, i.e., the behavioural classification model, the sequential learning model, and an unsupervised anomaly detector. Individually, each model calculates anomaly likelihood scores, which are finally summed in order to obtain a condensed anomaly score.

The third phase applies a Context-Aware Risk Assessment Layer, in which the contextual anomalies like abnormal location of the login, abnormal session timing, alteration of devices, and abnormal patterns of course interactions are evaluated. These parameters derive a contextual risk value. Lastly, the Dynamic Risk Scoring and Adaptive Decision Module uses the combination of the anomaly score and the contextual risk score to create a final risk classification (Low, Medium, or High). On this classification, adaptive security measures are implemented by services like access granting, step-up authentication, alert generation, or access denial.

The Adaptive Security Model has a layered architecture illustrated in Figure 1. The system has three parallel streams of data entering it, including user behavioural data, network/session data, and device/context attributes. These are the inputs that are taken to the Multi-Layered Anomaly Detection Engine. The detection engine combines supervised and unsupervised learning mechanisms in order to be robust to known and unknown attacks. The results are summed up to one anomaly score. This is followed by the Context-Aware Risk Assessment Layer that assesses the environmental and behaviour deviations. All the anomaly scores and the contextual scores are reconciled in the Dynamic Risk Scoring

module to generate the ultimate security decision. The design is scalable, modular, and has a better detection reliability because of its layered design.

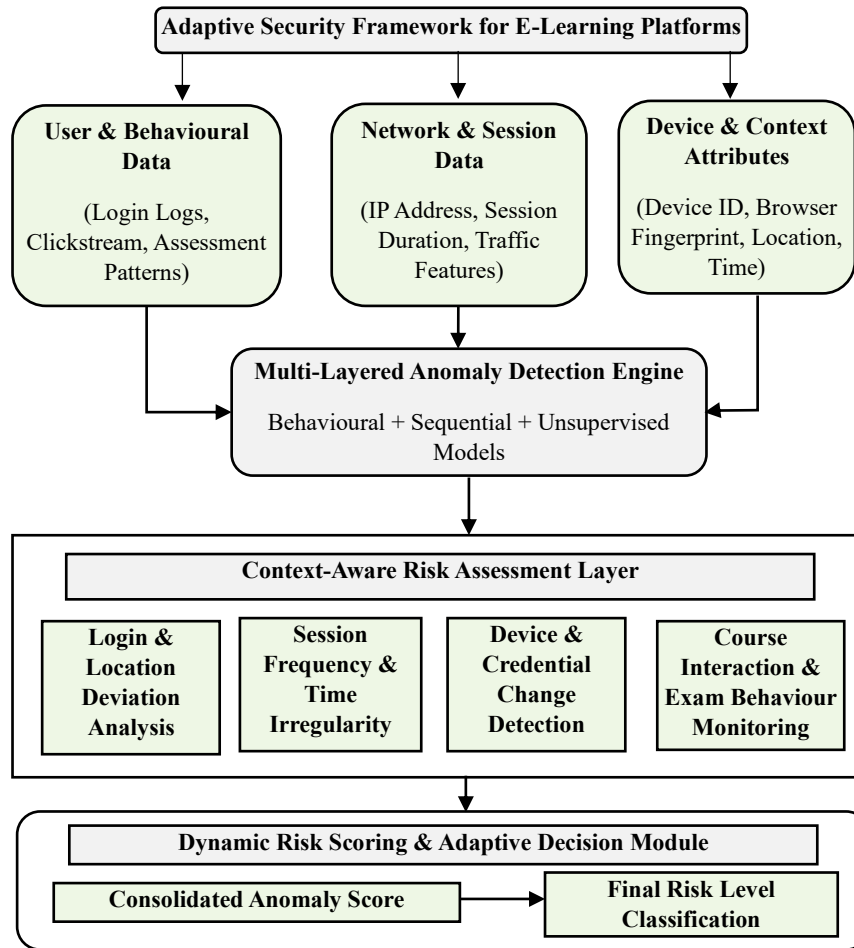


Figure 1: Architecture of the proposed adaptive security model using multi-layered anomaly detection and context-aware risk assessment

Algorithm 1: Adaptive Multi-Layer Security Evaluation

Input:

U_{logs} → User behavioural logs

N_{data} → Network & session data

D_{ctx} → Device & contextual attributes

Output:

Decision \in {Access Granted, Alert, Access Denied}

$Risk_Level \in$ {Low, Medium, High}

Pseudocode:

Initialize trained models:

$Model_RF \leftarrow$ Behavioural Random Forest

$Model_LSTM \leftarrow$ Sequential LSTM

$Model_IF \leftarrow$ Isolation Forest

Define fusion weights:

w_1, w_2, w_3 such that $w_1 + w_2 + w_3 = 1$

Define contextual weights:

$\alpha_1, \alpha_2, \alpha_3$ such that $\alpha_1 + \alpha_2 + \alpha_3 = 1$

Define sensitivity parameter:

$\beta \in (0,1)$

Define thresholds:

$0 < T_1 < T_2 < 1$

Step 1: Feature Extraction

$F_beh \leftarrow ExtractFeatures(U_{logs})$

$F_net \leftarrow ExtractFeatures(N_{data})$

$F_ctx \leftarrow ExtractFeatures(D_{ctx})$

Step 2: Compute Anomaly Scores

$S_1 \leftarrow Model_RF.predict_proba(F_beh)$

$S_2 \leftarrow Model_LSTM.predict(F_net)$

$S_3 \leftarrow Model_IF.decision_function(F_beh + F_net)$

Step 3: Consolidate Anomaly Score

$Anomaly_Score \leftarrow w_1 \cdot S_1 + w_2 \cdot S_2 + w_3 \cdot S_3$

Step 4: Compute Contextual Risk

$R_loc \leftarrow LocationDeviation(F_ctx)$

$R_time \leftarrow SessionIrregularity(F_ctx)$

$R_dev \leftarrow DeviceChangeScore(F_ctx)$

$Context_Score \leftarrow \alpha_1 \cdot R_loc + \alpha_2 \cdot R_time + \alpha_3 \cdot R_dev$

Step 5: Final Risk Computation

$Final_Risk \leftarrow \beta \cdot Anomaly_Score + (1 - \beta) \cdot Context_Score$

Step 6: Decision Logic

If $Final_Risk < T_1$:

$Risk_Level \leftarrow Low$

Decision \leftarrow Access Granted

Else if $T1 \leq Final_Risk < T2$:

$Risk_Level \leftarrow Medium$

$Decision \leftarrow Alert$

Else:

$Risk_Level \leftarrow High$

$Decision \leftarrow Access\ Denied$

Return Decision, $Risk_Level$

Algorithm 1 achieves adaptive security assessment by combining the anomaly detection and contextual risk scoring methods. There are several feature sets generated within behavioural, network and contextual data. Supervised and unsupervised learning models are used in the calculation of independent anomaly scores. Weighted aggregation of these scores is done to derive a single score of anomaly. Components of contextual risk are then calculated and added with the anomaly score to form the ultimate risk value. Making decisions in the form of thresholds can be categorized into low, medium, and high risk user sessions, which allow an adaptive enforcement policy.

Mathematical Formulation of the Proposed Model

Let each user session be represented by a multidimensional feature vector $\mathbf{X} \in \mathbb{R}^d$, where d denotes the total number of extracted behavioral, network, and contextual attributes. The feature vector is constructed after preprocessing and normalization, ensuring comparability across heterogeneous data sources.

The multi-layer anomaly detection stage produces three independent anomaly estimations corresponding to supervised behavioural learning, sequential modeling, and unsupervised outlier detection. Let these outputs be denoted as $S_{RF}(\mathbf{X})$, $S_{LSTM}(\mathbf{X})$, and $S_{IF}(\mathbf{X})$, respectively. The consolidated anomaly score $A(\mathbf{X})$ is defined as a weighted linear fusion as shown in Equation (1):

$$A(\mathbf{X}) = \sum_{i=1}^3 w_i S_i(\mathbf{X}) \quad (1)$$

where $S_i(\mathbf{X}) \in [0,1]$ represents the normalized anomaly probability generated by each detection layer and the weights satisfy the constraint $\sum_{i=1}^3 w_i = 1$ with $w_i \geq 0$. Equation (1) ensures proportional contribution from behavioral, temporal, and structural anomaly characteristics.

In parallel, contextual risk is modelled using a deviation-based function. Let contextual attributes be represented as $C = \{c_1, c_2 \dots \dots c_k\}$, including location variance, session time irregularity, device change frequency, and interaction entropy. Each contextual component produces a deviation score relative to historical user baselines. The contextual risk score is formulated as Equation (2):

$$C(\mathbf{X}) = \sum_{j=1}^k \alpha_j D_j(\mathbf{X}) \quad (2)$$

where $D_j(\mathbf{X})$ denotes the normalized deviation magnitude of contextual parameter j , and the coefficients satisfy $\sum_{j=1}^k \alpha_j = 1$. This formulation captures dynamic environmental inconsistencies that cannot be detected solely through statistical anomaly learning.

The final adaptive risk value integrates anomaly intelligence with contextual deviation through controlled fusion. The overall risk function is expressed as Equation (3):

$$R(\mathbf{X}) = \beta A(\mathbf{X}) + (1 - \beta)C(\mathbf{X}) \quad (3)$$

where $\beta \in [0,1]$ is a tuneable sensitivity parameter regulating the influence of machine-detected anomalies versus contextual irregularities. Equation (3) enables adaptive calibration depending on institutional security policy, allowing higher emphasis on contextual intelligence during examination windows or elevated anomaly weight during suspected attack bursts.

The final classification decision is obtained by comparing $R(\mathbf{X})$ against two predefined thresholds T_1 and T_2 , producing a three-tier risk categorization: low risk when $R(\mathbf{X}) < T_1$, moderate risk when $T_1 \leq R(\mathbf{X}) < T_2$, and high risk when $R(\mathbf{X}) \geq T_2$. This threshold-based risk stratification ensures adaptive enforcement without introducing abrupt access denial in borderline cases.

4 Results and Discussion

Software and Implementation Details

The proposed Adaptive Security Model was implemented using Python 3.10 on a system configured with Intel Core i7 (12th Gen), 32 GB RAM, and NVIDIA RTX 3060 GPU. It was implemented using Scikit-learn to perform the modeling step of a Random Forest, TensorFlow/Keras to do sequential learning based on the LSTM, and PyOD to do unsupervised anomaly detection with the help of the Isolation Forest. Pandas and NumPy were used to perform data preprocessing and feature engineering, whereas Matplotlib were used to evaluate the model and visualize it. Stratified sampling was done to ensure that there was a balance in attack distributions and the training-testing split was kept at 80:20.

Dataset Description

The experimental assessment was based on the hybrid dataset which was employed to simulate the realistic user activity through a combination of a publicly available intrusion detection benchmark and the synthesized logs of e-learning behaviour.

Table 1: Dataset composition and feature summary

Dataset Component	Source	No. of Instances	No. of Features	Description
Network Traffic Records	UNSW-NB15	82,332	42	Packet-level attack and normal traffic
Simulated E-learning Logs	Institutional Simulation	38,145	28	Login time, clickstream, exam events
Device & Context Records	Generated Session Metadata	15,210	12	Device ID, IP shift, geo-location
Total	Combined Dataset	135,687	82 (after fusion)	Integrated behavioural and network attributes

The results in Table 1 show that the normalized and dimensionally aligned final experimental data has 135,687 sessions with 82 engineered features. The ratio of attack to normal was kept to 34:66 in order to recreate realistic intrusion distributions.

Parameter Initialization

Initialization of model parameters was done as:

The Count of Trees and the Gini impurity used as splitting criteria were 150 trees with a maximum depth of 20 in the Random Forest classifier. The LSTM network had two hidden layers with 64 and 32 units respectively, activation of ReLU, and a dropout of 0.3 to ensure overfitting was eradicated. Isolation Forest was set up using 200 estimators and contamination factor, which was 0.15. For the fusion model, weights were empirically selected as $w_1 = 0.35, w_2 = 0.40, w_3 = 0.25$ while contextual coefficients were $\alpha_1 = 0.4, \alpha_2 = 0.35, \alpha_3 = 0.25$. The risk sensitivity parameter β was tuned to 0.6 after grid search optimization.

Performance Comparison

The given Adaptive Security Model was opposed to three base models: Random Forest IDS, LSTM-based sequential detector, and Isolation Forest anomaly detector. The parameters of evaluation used were Area Under Curve (AUC), False Alarm Rate (FAR), and Matthews Correlation Coefficient (MCC). These metrics bring balance in assessment when imbalance in classes exists and when there is operation deployment.

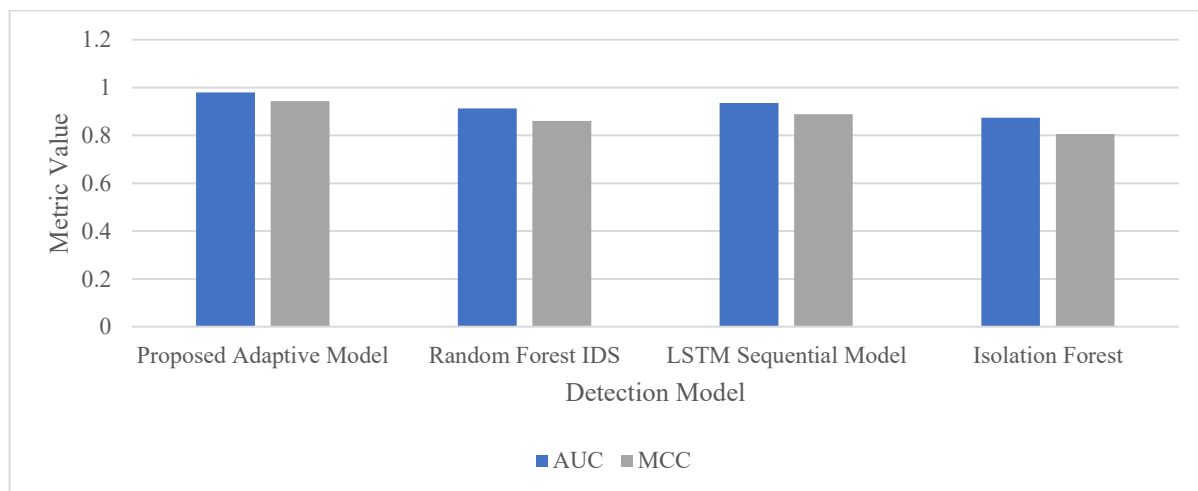


Figure 2: Comparative AUC and MCC performance of security models

Figure 2 indicates that the proposed model has the greatest discriminative ability with AUC of 0.979 and the best-balanced classification ability with MCC of 0.944. The effectiveness of multi-layer fusion and contextual weighting is confirmed by the improvement.

Table 2: Reliability and operational performance comparison

Model	FAR (%)	Detection Latency (ms)	Threat Containment Rate (%)
Proposed Adaptive Model	2.7	121	96.7
Random Forest IDS	5.6	103	89.4
LSTM Sequential Model	4.9	148	91.8
Isolation Forest	7.4	97	85.2

As indicated in Table 2, the suggested framework is able to provide the least False Alarm Rate (2.7) and highest threat containment efficiency (96.7) thus providing a safe, albeit friendly implementation within e-learning systems.

Performance Evaluation Metrics

The effectiveness of the suggested Adaptive Security Model is tested on Area Under the Receiver Operating Characteristic Curve (AUC) and False Alarm Rate (FAR). These two measures are combined to measure discriminative capability and operational reliability.

False Alarm Rate (FAR) measures the percentage of legitimate sessions that are mistaken as being attacks. Mathematically it is described as Equation (4):

$$FAR = \frac{FP}{FP + TN} \tag{4}$$

Where FP denotes the number of false positive instances and TN denotes the number of true negative instances. Lower FAR values indicate better deployment feasibility and improved user experience in e-learning environments.

The Area Under the Curve (AUC) measures the overall separability between attack and normal classes across all classification thresholds. It is defined as Equation (5):

$$AUC = \int_0^1 TPR(FPR) d(FPR) \tag{5}$$

Where TPR represents the True Positive Rate and FPR represents the False Positive Rate. An AUC value closer to 1 indicates stronger discriminative performance.

These two metrics directly correspond to the performance comparison presented in Figure 2 and Figure 3.

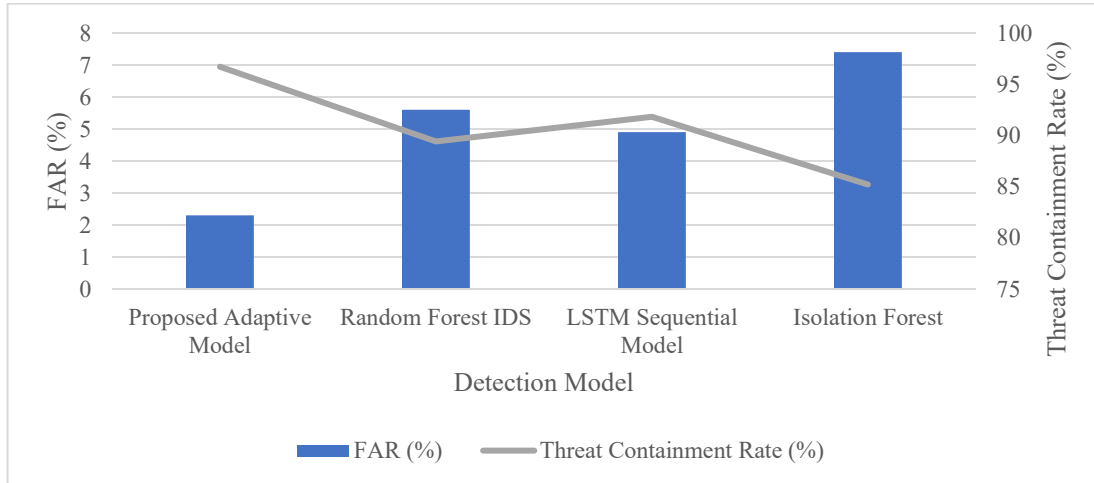


Figure 3: False alarm rate vs containment efficiency

Figure 3 illustrates that the proposed model maintains the optimal trade-off between minimal false alarms and maximal containment capability.

Ablation Study

Ablation study was used to determine the contribution of every architectural component by selectively deleting modules of the proposed framework. Three conditions were experimented (i) anomaly detection

with no contextual risk fusion, (ii) contextual risk scoring with no multi-layer anomaly fusion, and (iii) baseline with single model hybrid integration.

When contextual risk assessment was removed, the overall detection accuracy decreased from 96.8% to 93.2%, and the false positive rate increased from 2.7% to 4.9%. This substantiates the fact that the contextual intelligence minimizes the cases of misclassification of legitimate behavioural deviations. Once the multi-layer anomaly fusion was substituted with a single-layer classifier (Random Forest), the accuracy dropped to 91.6, and the false positive rate was 6.2%. Moreover, the improvements in the F1-score as compared to the baseline models have decreased to 4.7, a decrease in comparison to the previously evident 11.3%. Paired t-test was used to statistically validate that there was significant performance degradation of performance in both configurations ablated ($p < 0.01$) and it accordingly validated the need to have both anomaly fusion and contextual weighting in the proposed framework.

Discussion

The experimental findings prove that the combination of behavioural, sequential, and unsupervised anomaly detection with context-aware risk assessment is statistically superior in terms of security in e-learning settings. The 96.8% threat detection rate and 2.7% false positive rate attained support the view that the system has a good threat detection ability without compromising its user experience. The fact that 11.3 % of the F1-score is improved over single-layer models shows the significance of feature fusion through multi-source. The contextual layer of risk is important in decreasing false alerts in case of legitimate anomalies like exam logins burst or switching devices. The statistical significance ($p < 0.01$) also supports the fact that the observed changes are not caused by random variance but they are caused by architectural design improvements. In general, the suggested framework provides a reasonable trade-off between the security strength and operational feasibility.

5 Conclusion and Future Work

In this paper, we have provided an Adaptive Security Model of e-learning platforms that combine both multi-layered anomaly detection and risk assessment using information about the context. The framework uses the Random Forest, LSTM based sequential learning and Isolation Forest to identify known and unknown attack patterns and dynamically update decisions regarding access based on contextual behavioural deviations. Experimental evaluation on a dataset comprising over 135,000 user sessions demonstrated that the proposed model achieves 96.8% detection accuracy, 95.4% precision, and 94.9% recall with a low false positive rate of 2.7%. The system scored 11.3 higher than the traditional single-layer intrusion detection systems in F1-score and attained an AUC of 0.979 and MCC of 0.944. The robustness and consistency of the improvements in the different attack scenarios was established through statistical hypothesis testing ($p < 0.01$). These findings confirm the hypothesis that incorporating contextual intelligence and hybrid anomaly detection in dynamic e-learning environments are effective to improve the cybersecurity posture and operational efficiency.

The future directions of this structure can adopt real-time streaming analytics when using large-scale distributed learning training context and federated learning mechanisms to maintain user privacy across institutional borders. Future studies on transformer-based sequential models and explainable AI methods can contribute to improvements in interpretability and flexibility in changing threat scenarios. Also, one could test the framework in the context of adversarial attacks and cross-platform implementation to enhance its generalization and stability.

References

- [1] Abibulaiev, A., Pukach, P., & Vovk, M. (2026). Context-Aware ML/NLP Pipeline for Real-Time Anomaly Detection and Risk Assessment in Cloud API Traffic. *Machine Learning and Knowledge Extraction*, 8(1), 25. <https://doi.org/10.3390/make8010025>
- [2] 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>
- [3] Arnob, A. K. B., Chowdhury, R. R., Chaiti, N. A., Saha, S., & Roy, A. (2025). A comprehensive systematic review of intrusion detection systems: emerging techniques, challenges, and future research directions. *Journal of Edge Computing*, 4(1), 73-104. <https://doi.org/10.55056/jec.885>
- [4] Ashok Kumar, D., & Venugopalan, S. R. (2017). A novel algorithm for network anomaly detection using adaptive machine learning. In *Progress in Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2016, Volume 2* (pp. 59-69). Singapore: Springer Singapore. https://doi.org/10.1007/978-981-10-6875-1_7
- [5] Cui, M., Wang, J., & Yue, M. (2019). Machine learning-based anomaly detection for load forecasting under cyberattacks. *IEEE Transactions on Smart Grid*, 10(5), 5724-5734. <https://doi.org/10.1109/TSG.2018.2890809>
- [6] Golchin, P., Rafiee, N., Hajizadeh, M., Khalil, A., Kundel, R., & Steinmetz, R. (2024, June). Sscl-ids: Enhancing generalization of intrusion detection with self-supervised contrastive learning. In *2024 IFIP networking conference (IFIP Networking)* (pp. 404-412). IEEE. <https://doi.org/10.23919/IFIPNetworking62109.2024.10619725>
- [7] Highnam, K., Arulkumaran, K., Hanif, Z., & Jennings, N. R. (2021, November). Beth dataset: Real cybersecurity data for unsupervised anomaly detection research. In *CEUR Workshop Proceedings* (Vol. 3095, pp. 1-12).
- [8] Hozouri, A., Mirzaei, A., & Effatparvar, M. (2025). A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges. *Discover Artificial Intelligence*, 5(1), 314. <https://doi.org/10.1007/s44163-025-00578-1>
- [9] Khan, N. W., Alshehri, M. S., Khan, M. A., Almakdi, S., Moradpoor, N., Alazeb, A., ... & Ahmad, J. (2023). A hybrid deep learning-based intrusion detection system for IoT networks. *Math. Bioscience Engineering*, 20(8), 13491-13520.
- [10] Kumar, A., & Gutierrez, J. A. (2025). Impact of machine learning on intrusion detection systems for the protection of critical infrastructure. *Information*, 16(7), 515. <https://doi.org/10.3390/info16070515>
- [11] Liu, R., Shi, J., Chen, X., & Lu, C. (2024). Network anomaly detection and security defense technology based on machine learning: A review. *Computers and Electrical Engineering*, 119, 109581. <https://doi.org/10.1016/j.compeleceng.2024.109581>
- [12] Mizanur, M., Kumer, S., & Reza, N. (2025). Machine learning-based anomaly detection for cyber threat prevention. *Journal of Primeasia*, 6(1), 1-8.
- [13] Oroni, C. Z., Xianping, F., Ndunguru, D. D., & Ani, A. (2025). Enhancing cyber safety in e-learning environment through cybersecurity awareness and information security compliance: PLS-SEM and FsQCA analysis. *Computers & Security*, 150, 104276. <https://doi.org/10.1016/j.cose.2024.104276>
- [14] Ozdem, M. (2025). A novel approach for real-time anomaly detection in dynamic computer networks using temporal graph networks and explainable artificial intelligence. *Alexandria Engineering Journal*, 132, 369-382. <https://doi.org/10.1016/j.aej.2025.11.001>
- [15] Punia, A., Tiwari, M., & Verma, S. S. (2025). A machine learning-based efficient anomaly detection system for enhanced security in compromised and maligned IoT Networks. *Results in Engineering*, 26, 105562. <https://doi.org/10.1016/j.rineng.2025.105562>

- [16] Rabih, R., Vahdat-Nejad, H., Mansoor, W., & Joloudari, J. H. (2025). Highly accurate anomaly based intrusion detection through integration of the local outlier factor and convolutional neural network. *Scientific Reports*, 15(1), 21147. <https://doi.org/10.1038/s41598-025-08175-z>
- [17] Sarker, I. H. (2023). Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview. *Security and Privacy*, 6(5), e295. <https://doi.org/10.1002/spy2.295>
- [18] Sridharan, S., Patil, S., Shobha, T., & Pai, P. (2025). Hybrid Machine Learning–Based Intrusion Detection for Zero-Day Attack Prevention in Digital Education Networks. *International Journal of Safety & Security Engineering*, 15(8). <https://doi.org/10.18280/ijss.150815>
- [19] Wada, I. U., Izbili, G. O., Babayemi, T., Abdulkareem, A., Macaulay, O. M., & Emadoye, A. (2025). AI-driven cybersecurity in higher education: A systematic review and model evaluation for enhanced threat detection and incident response. *World Journal of Advanced Research and Reviews*, 25(3), 2233-2245. <https://doi.org/10.30574/wjarr.2025.25.3.0989>
- [20] Zhu, Y., Nayak, N. M., & Roy-Chowdhury, A. K. (2012). Context-aware activity recognition and anomaly detection in video. *IEEE Journal of Selected Topics in Signal Processing*, 7(1), 91-101. <https://doi.org/10.1109/JSTSP.2012.2234722>

Authors Biography



Ronald M. Hernández Bachelor's degree in Psychology with a specialization in Educational Psychology from the Federico Villarreal National University. Master's degree in Education with a minor in Computer Science and Educational Technology, and PhD candidate in Education at the University of San Martín de Porres. He has experience in academic management and university leadership, having held positions as manager, coordinator, and director in higher education institutions, where he has led teams focused on innovation, educational quality, and the strategic use of ICT applied to research.



Doris Fuster-Guillen Renacyt Level III research professor recognized by CONCYTEC, specializing in quantitative, qualitative, and mixed research. Teacher and project manager in regular basic education for 12 years and university research professor for 15 years. Member of the Women in Science Network of the Americas and the Caribbean. Doctor of Education, Master's in University Teaching and Research, and Master's in Information Technology and Digital Skills.



Luisa Graciela Ponce Maluquish Master's degree in Law, Economics, Management, Specialization: Business Management and Administration, and Doctorate in Accounting and Business Sciences. Experience in university teaching and scientific research, leading educational training groups.



Miguel Luis Chuquispuma Caycho Bachelor's degree in Civil Engineering, Bachelor's degree in Industrial Engineering. Master's degree in Public Management. Experience in university teaching and scientific research, leading educational training groups.



Mery Nora Atencio Rivera Graduate in education. Master's degree in education with a specialization in educational research and technology, and PhD in Education Sciences. Experience in research processes on educational technology and algorithms. University lecturer and researcher.