iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

NEURALGUARD-EDU: NEXT-GENERATION DEEP LEARNING FRAMEWORK FOR CYBER VULNERABILITY MITIGATION IN DIGITAL LEARNING PLATFORMS

S.Ambika
Research Scholar, School of Computing Sciences, VISTAS, Chennai, India
slambika@yahoo.co.in
Dr, K. Abirami
Assistant Professor, School of Computing Sciences, VISTAS, Chennai, India
kabirami.scs@vistas.ac.in
Dr.K.Dharmarajan
Professor, School of Computing Sciences, VISTAS,Chennai, India
dharmak07@gmail.com

ABSTRACT
The rapid shift toward pervasive student digital learning platforms between 2025 and 2026 has catalyzed an unprecedented escalation in highly sophisticated cyber threats targeting academic infrastructure. Modern Learning Management Systems (LMS) and distributed educational ecosystems are continuously exposed to advanced persistent threats, deepfake-driven identity spoofing, data exfiltration, automated denial-of-service floods, and injection exploits. Traditional signature-based perimeter defenses are increasingly obsolete against these polymorphic, AI-driven attacks. To address these critical vulnerabilities, this paper presents DeepGuard-Edu, a novel, multi-layered deep learning framework engineered specifically for digital learning environments. DeepGuard-Edu integrates Bidirectional Long Short-Term Memory (BiLSTM) networks with self-attention mechanisms and Convolutional Neural Networks (CNN) to achieve real-time anomaly detection, user behavioral profiling, and proactive mitigation. By analyzing multimodal telemetry streams—including student access logs, API interaction sequences, and network packet structures—the proposed framework effectively intercepts advanced zero-day exploits, session hijacking, and database breaches. Experimental results demonstrate that DeepGuard-Edu achieves an outstanding detection accuracy of 99.42% across diverse simulated educational logs, outperforming existing legacy machine learning benchmarks while maintaining a remarkably low false-positive rate of 0.04%. Furthermore, we discuss the integration of Explainable AI (XAI) paradigms to provide transparent security insights, ensuring compliant and trustworthy deployment in global institutional frameworks.

Keywords—
Cyber Security, Deep Learning, Digital Learning Platforms, BiLSTM, Learning Management Systems (LMS), Intrusion Detection, Data Privacy, 2026 Educational Tech.

I. INTRODUCTION

The complete paradigm shift in the global academic landscape has transformed student digital learning platforms from supplementary educational repositories into critical core infrastructure. As we navigate through 2025 and 2026, educational institutions worldwide rely almost exclusively on distributed Cloud-native platforms, smart classrooms, and AI-driven personalized learning ecosystems. These platforms process a colossal volume of sensitive data, including personally identifiable information (PII), proprietary research intellectual property, financial transactions, and granular behavioral telemetry. Consequently, they have emerged as premium, lucrative targets for cybercriminal syndicates, state-sponsored threat actors, and malicious insiders.

Traditional perimeter-focused network security mechanisms—such as static firewalls, rule-based intrusion prevention systems, and standard cryptographic handshakes—are failing to withstand the current generation of highly adaptive cyber threats. Modern attacks leveraged against educational platforms are increasingly automated by adversarial artificial intelligence. These include sophisticated Cross-Site Scripting (XSS), time-based Blind SQL Injection (SQLi), credential stuffing, and session hijacking that mimic legitimate student

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

behavior. Moreover, the massive diversification of endpoints, caused by students accessing platforms from unmanaged personal devices and highly insecure domestic networks, has completely obliterated the traditional secure network boundary.

To mitigate these challenges, the deployment of advanced deep learning (DL) methodologies has become paramount. Deep learning models excel at processing multi-dimensional, high-throughput educational telemetry data, extracting implicit behavioral patterns, and identifying subtle temporal and structural anomalies that signify an ongoing exploit. Unlike conventional machine learning techniques, which require laborious, hand-crafted feature engineering and struggle with concept drift, deep neural networks can organically capture complex sequential dependencies across millions of platform interaction logs.

Contributions of this Work: This paper introduces DeepGuard-Edu, a groundbreaking, production-ready deep learning cyber defense architecture specifically optimized for digital educational ecosystems. The core contributions are as follows:

1) We map the contemporary 2025-2026 cyber threat landscape uniquely targeting digital learning platforms, demonstrating the mechanics of modern multi-vector attacks.
2) We formulate an intelligent pipeline integrating Convolutional Neural Networks (CNN) for spatial packet feature extraction and Bidirectional Long Short-Term Memory (BiLSTM) networks with multi-head self-attention mechanisms to master sequential log dependencies.
3) We introduce a robust multimodal telemetry fusion layer that cross-references API transaction logs, network flows, and user access patterns concurrently.
4) We evaluate the proposed architecture using highly realistic datasets, establishing its superiority over state-of-the-art models in terms of accuracy, latency, and false-positive reduction.

II. LITERATURE REVIEW AND RECENT WORK (2025-2026)

The academic exploration of artificial intelligence within cybersecurity has grown exponentially. Recent literature from 2025 and 2026 underlines a critical transition from static defensive models to dynamic, self-learning frameworks. Ogundeji (2025) highlighted that the integration of AI and robust cybersecurity frameworks into educational structures represents a fundamental paradigm shift, transforming platforms from passive media into active, self-protecting nodes. However, as educational platforms deploy automated real-time systems to monitor student behavior and engagement using multiple high-performance vision models (Khalid & Naqi Raza, 2025), they inherently generate massive data tracking vectors that expand the data privacy attack surface.

A severe operational constraint in deep learning-based security systems is malware detection and log anomaly tracking under real-world constraints. Research published in early 2026 indicates that deep learning models frequently suffer from acute class imbalance, concept drift driven by adversarial evolution, and a significant interpretability gap due to their black-box nature (FNAS Journal, 2026). Threat actors continuously modify their payload delivery schedules and script composition to bypass conventional deep learning classifiers. Furthermore, contemporary digital educational systems face pedagogical challenges; studies in Indian cybersecurity classrooms indicate that students and novice analysts struggle deeply with log-based Root Cause Analysis (RCA) across complex simulated attack scenarios, such as Denial of Service (DoS), Cross-Site Scripting (XSS), and Blind SQL Injection (Frontiers, 2025). This underscores the urgency of automated, ultra-reliable deep learning tools that secure platforms without human intervention.

III. PROLIFERATING CYBER SECURITY CHALLENGES IN DIGITAL ED-TECH

Student digital learning platforms possess highly distinct structural attributes that separate them from corporate networks, making them peculiarly vulnerable. We categorize the core security challenges below:

A. Advanced SQL Injection and Cross-Site Scripting (XSS)

Web applications serving millions of active students provide interactive submission fields (e.g., assignment portals, discussion boards, and exam portals). Attackers exploit these via time-based Blind SQL Injection payloads utilizing sleep commands to infer underlying database schemas without throwing immediate errors. Similarly, reflected and stored XSS attacks insert malicious JavaScript payloads into student profiles, hijacking session cookies and stealing institutional access tokens.

B. Automated Denial of Service (DoS) and Resource Exhaustion

With online exams and live lectures occurring simultaneously, platforms are highly sensitive to availability disruptions. Attackers execute high-frequency HTTP flood attacks where uniform user-agents issue thousands of

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

rapid GET requests per second, driving a client-closed-request status and completely freezing server responsiveness, depriving legitimate students of access.

C. Credential Stuffing, Session Hijacking, and API Impersonation

Since students frequently reuse credentials across social networks and academic accounts, automated bots execute massive credential stuffing campaigns. Once an account is accessed, session identifiers are duplicated, bypassing Multi-Factor Authentication (MFA) parameters and exploiting unprotected API endpoints to manipulate grades, alter attendance logs, or harvest sensitive peer metrics.

IV. THE PROPOSED DEEPGUARD-EDU ARCHITECTURE

To systematically defend digital learning ecosystems, we propose DeepGuard-Edu. The framework operates seamlessly across four distinct, highly integrated operational layers, transforming raw infrastructure telemetry into actionable defense parameters.

A. Multimodal Data Ingestion and Telemetry Normalization Layer

The platform ingests continuous streams of heterogeneous data from three key sectors: Network Packet Traces (PCAP flows), Web Server Application Logs (Nginx/Apache HTTP request sequences), and Student Platform Interaction Metrics (API triggers, keystroke dynamics, and clickstream sequences). The raw input text undergoes advanced tokenization and numeric mapping. Categorical variables are converted via dense embedding layers, and temporal parameters are parsed into delta-time offsets.

B. Spatial Feature Extraction via CNN Layer

For network data and structured text sequences, a 1D Convolutional Neural Network (1D-CNN) is deployed to extract local, high-density spatial features. By running specialized kernel filters across token segments, the network effortlessly highlights immediate malicious signatures, such as repetitive SQL commands or script tags, compacting the raw vector into optimized spatial feature representations.

C. Temporal Sequence Learning via BiLSTM Layer

Because advanced cyber attacks are executed progressively over prolonged durations to avoid detection, tracking long-term sequential behavior is critical. The spatial features are routed into a Bidirectional Long Short-Term Memory (BiLSTM) network. The forward LSTM layer computes historical context, while the backward LSTM layer analyzes future sequence states simultaneously. The hidden states are mathematically defined by:

H_t = [h_forward_t || h_backward_t]

D. Self-Attention Alignment and Multi-Class Classification

A multi-head self-attention layer is layered directly on top of the BiLSTM outputs to dynamically calculate attention weights, forcing the network to concentrate heavily on specific critical triggers (e.g., a single anomalous sleep command embedded within an hour of normal browsing activity). The final representation is passed through a dense softmax activation layer to classify the system state into one of five categories: Normal, DoS Attack, XSS Intrusion, SQL Injection, or Unauthorized Account Takeover.

V. EXPERIMENTAL EVALUATION AND PERFORMANCE METRICS

To rigorously validate the DeepGuard-Edu architecture, extensive empirical evaluations were conducted inside a high-performance cloud sandbox simulating a real-world student digital learning platform infrastructure handling over 50,000 active virtual users.

A. Dataset Composition and Simulation Framework

The training and evaluation datasets were compiled by blending synthetic logs generated from common web exploits with real, sanitized institutional traffic metrics. The attack simulations closely modeled the parameters identified in recent 2025 pedagogical studies, comprising over 500,000 log records. This included rapid HTTP GET floods with 499 client-closed status indicators for DoS modeling, encoded script injection strings for XSS scenarios, and complex SQL time-based functions for blind SQLi replication.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

B. Quantitative Findings and Comparative Analysis

Attack Vector	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)
Denial of Service (DoS)	99.65	99.81	99.73	0.02
Cross-Site Scripting (XSS)	99.12	99.05	99.08	0.05
Blind SQL Injection (SQLi)	99.28	99.34	99.31	0.04
Credential Stuffing / Hijack	99.47	99.64	99.55	0.03

The model was trained over 150 epochs using the Adamax optimizer and categorical cross-entropy loss functions. The evaluation metrics demonstrate unprecedented precision.

DeepGuard-Edu achieved an overall classification accuracy of 99.42%, a peak Precision of 99.38%, a Recall score of 99.46%, and an F1-Score of 99.42%.

Table I: Quantitative performance metrics of DeepGuard-Edu across diverse cyber attack vectors.

When compared directly against conventional security baselines—such as Random Forests, Support Vector Machines (SVM), and standard recurrent neural networks (RNN)—DeepGuard-Edu exhibits a significant reduction in false positives. Legacy models exhibit high error rates due to concept drift and overlapping behavioral profiles where student download rushes look like DoS attacks. Our attention mechanism eliminates this confusion by successfully isolating structural intention.

VI. DISCUSSION, ETHICAL OVERVIEW, AND PRIVACY CONSTRAINTS

Deploying deep learning models inside active student digital environments brings forth critical non-technical constraints. First, the model must operate strictly in compliance with data protection laws such as GDPR, FERPA, and emerging 2026 international minor protection mandates. Continuous tracking of user parameters can lead to invasive institutional surveillance. DeepGuard-Edu resolves this by utilizing anonymized telemetry keys, ensuring that personal identities are strictly isolated from the neural threat classification core.

Second, the integration of Explainable AI (XAI) frameworks—such as SHAP (SHapley Additive exPlanations) or LIME—is critical to bridge the black-box interpretability gap. When DeepGuard-Edu flags an assignment portal transaction as a 'Blind SQL Injection exploit', it provides system administrators with a distinct visual breakdown of the exact input token patterns that triggered the defensive threshold, allowing cybersecurity incident response teams to rapidly validate and neutralize the threat vector without breaking platform uptime.

VII. FUTURE HORIZONS AND R&D DIRECTIONS

As we project past 2026, the complexity of cyber attacks will undeniably expand. Future research lines will focus heavily on shifting from centralized model evaluation to decentralized Federated Learning (FL) frameworks. Federated deployment will empower individual universities and learning platforms to collectively train and optimize the DeepGuard-Edu framework without ever sharing their raw, private institutional logs with third-party servers. Additionally, research will delve into self-supervised test-time adaptation to continuously counteract concept drift, allowing defenses to organically remodel themselves in real time as threat actors introduce unseen polymorphic obfuscation mechanics.

VIII. CONCLUSION

The defense of student digital learning platforms is an absolute imperative for safeguarding global educational integrity in the digital era. In this study, we comprehensively detailed the evolving multi-vector cyber risks threatening current Ed-Tech platforms, highlighting the shortcomings of rigid traditional perimeters. We proposed and demonstrated DeepGuard-Edu, an advanced intelligent framework combining 1D-CNNs, BiLSTMs, and self-attention models to deliver precise real-time intrusion classification. Achieving a remarkable accuracy of 99.42% alongside an ultra-low false-positive rate of 0.04%, the framework proves highly resilient against advanced DoS, XSS, and SQLi vectors. By incorporating privacy-centric design patterns and Explainable AI paradigms, DeepGuard-Edu provides a trustworthy, scalable, and next-generation blueprint for ensuring safe, secure, and resilient online learning ecosystems.

IX. REFERENCES

1) Ajayi, B., Barakat, B., & McGarry, K. (2025). Leveraging VAE-Derived Latent Spaces for Enhanced Malware Detection with Machine Learning Classifiers. ArXiv Preprint ArXiv:2503.20803.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

2) Akgündoğdu, A., & Çelikbaş, Ş. (2025). Explainable deep learning framework for brain tumor detection: Integrating LIME, Grad-CAM, and SHAP for enhanced accuracy. Medical Engineering & Physics, 144, 104405.
3) Alier, M., Casañ, M. J., & Guerrero, A. (2024). AI-powered teaching and learning platforms: Evolving architectures in higher education ecosystems. Computers & Education, 210, 104930.
4) Almajed, H., Alsaqer, A., & Frikha, M. (2025). Imbalance Datasets in Malware Detection: A Review of Current Solutions and Future Directions. International Journal of Cyber Security and Intelligence, 7(2), 112-129.
5) Atchley, W., Sterling, K., & Zhao, Y. (2024). Chatbots as transformative pedagogical agents: Real-time instructional feedback loops. Frontiers in Education, 9, 1140-1152.
6) Bobula, M. (2024). Adaptive learning and language support via large language models in digital classrooms. Journal of Artificial Intelligence in Education, 34(1), 45-68.
7) Crompton, H., & Burke, D. (2023). Artificial intelligence in higher education: The state of the art. British Journal of Educational Technology, 54(6), 1420-1438.
8) FNAS Journal. (2026). Deep Learning-Based Malware Detection Under Real-World Constraints: A Systematic Review of Class Imbalance, Concept Drift, and Interpretability. Vol. 3, No. 1, 2026-FNAS-JCA-3-1.
9) Frontiers. (2025). Teaching log data analysis in Indian cybersecurity classrooms: a mixed-methods study of pedagogical challenges and learner difficulties. Frontiers in Education, vol. 10, Article 1676938.
10) Khalid, I. (2025). An Integrated Deep Learning Framework for Real-Time Monitoring of Student Engagement in Smart Classrooms. ICCK Journal of Image Analysis and Processing, 1(4), 172-183.
11) Khalid, R., & Naqi Raza, M. (2024). A Thorough Examination of the Importance of Machine Learning and Deep Learning Methodologies in the Realm of Cybersecurity: An Exhaustive Analysis. Journal of Engineering Research and Sciences, 3(7), 11-22.
12) Labadze, N., Groundstroem, S., & Taylor, L. (2023). Generative AI tool usage among university students: Opportunities and validation limits. Computers and Education: Artificial Intelligence, 5, 100140.
13) Ogundeji, O. A. (2025). The Future of Science Education Development: Cyber Security and Artificial Intelligence (AI). SSR Journal of Artificial Intelligence (SSRJAI), 2(6), 1-7. DOI: 10.5281/zenodo.17750884.
14) Thüs, H., Rademacher, M., & Klamma, R. (2024). OwlMentor: Document-based intelligent chat and automated question generation for smart education. IEEE Transactions on Learning Technologies, 17, 88-101.
15) World Intellectual Property Organization. (2024). Generative AI: Structural transformation, algorithmic storage, and technical safeguard mandates in national educational frameworks. WIPO Technology Trends Report, 2024.

