IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 11 ISSUE : 02 Print / Issue Publication Date: 09-Jul-2026

ISSN : 2455-2143

DOI : 10.33564/IJEAST.2026.v11i02.017

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 02, ISSN No. 2455-2143, Pages 144-148
Published Online June 2026 in IJEAST (http://www.ijeast.com)

AI-DRIVEN CYBER THREAT DETECTION AND RESPONSE FRAMEWORK FOR HIGHER EDUCATIONAL INSTITUTIONS (HEIS)

Irfan Y. Belim
Research Scholar
Faculty of Computer Application
Noble University, Junagadh, Gujarat, India

Dr. Bhargav Rajyagor
Associate Professor
Faculty of Computer Application
Noble University, Junagadh, Gujarat, India

Abstract— **Higher Educational Institutions (HEIs) are increasingly exposed to complex cyber threats due to their open-access digital ecosystems, diverse user populations, and extensive research infrastructures. Conventional signature based intrusion detection systems often fail to detect zero-day and evolving attacks, creating an urgent need for intelligent and adaptive security mechanisms. This study proposes an AI-driven cyber threat detection and response framework tailored specifically for HEIs. The framework employs an unsupervised machine learning model—Isolation Forest— trained exclusively on benign network traffic to identify anomalous behaviour without prior attack signatures. Using the CSE-CIC-IDS2018 dataset, the model was evaluated within a dynamic monitoring window of 50,000 network flows. Experimental results identified 2,115 anomalous flows, corresponding to a 4.23% anomaly rate. Unlike static evaluation models, the proposed framework incorporates a dynamic risk scoring mechanism that adapts to real-time institutional traffic patterns by comparing current anomaly rates against historical baselines. The observed anomaly deviation remained within acceptable operational thresholds, indicating a low institutional threat level. The findings demonstrate that AI-driven anomaly detection can effectively support proactive cyber security strategies in HEIs. The proposed framework contributes to both theoretical and practical advancements by integrating machine learning– based anomaly detection with institutional cyber risk quantification.**

Keywords— **Artificial Intelligence, Cyber security, Anomaly Detection, Higher Education Security, Risk Scoring**

I. INTRODUCTION

Digital transformation has fundamentally reshaped Higher Educational Institutions (HEIs). Universities now operate highly interconnected infrastructures supporting academic portals, online learning platforms, research databases, cloud computing environments, IoT-enabled laboratories, and administrative systems. While this digital evolution enhances accessibility and innovation, it also significantly increases institutional exposure to cyber threats. HEIs differ from corporate organizations in one critical aspect: openness. Academic institutions prioritize collaboration and accessibility, often allowing broad network access to students, faculty, visiting researchers, and third-party partners. This openness, combined with high user turnover and Bring-Your Own-Device (BYOD) practices, creates a complex cyber security environment.

Traditional intrusion detection systems (IDS) primarily rely on signature-based detection mechanisms. While effective against known threats, these systems struggle to detect previously unseen or zero-day attacks. As cyber attacks grow more sophisticated and adaptive, HEIs require intelligent, self learning detection frameworks capable of identifying abnormal behavior rather than predefined attack patterns. This research proposes an AI-driven anomaly detection framework designed specifically for HEIs. The system leverages unsupervised machine learning to model normal network behavior and dynamically assess institutional cyber risk.

II. BACKGROUND

Recent global cyber incidents targeting universities have demonstrated vulnerabilities in academic networks. Ransomware campaigns, DDoS attacks during examination periods, and data exfiltration attempts have highlighted the need for proactive security monitoring.

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 02, ISSN No. 2455-2143, Pages 144-148
Published Online June 2026 in IJEAST (http://www.ijeast.com)

Machine learning has emerged as a promising solution in cyber security. Particularly, unsupervised anomaly detection techniques allow detection of abnormal traffic without requiring labeled attack data.

III. RESEARCH PROBLEM

HEIs currently lack:

- A dynamic AI-based anomaly detection framework.
- Institutional-level cyber risk quantification.
- Adaptive threat classification mechanisms.
- Real-time deviation analysis relative to normal baseline behavior.

IV. RESEARCH OBJECTIVES

This study aims to:
I. Develop an AI-driven anomaly detection framework for HEIs.
II. Train an Isolation Forest model on benign network traffic.
III. Detect suspicious network flows without attack signatures.
IV. Introduce a dynamic institutional cyber risk scoring mechanism.
V. Classify threat levels based on real-time anomaly deviations.

V. SIGNIFICANCE OF THE STUDY

This research contributes by:

- Integrating anomaly detection with institutional risk scoring.
- Proposing a scalable AI security architecture for HEIs.
- Supporting adaptive cybersecurity governance strategies.
- Enhancing theoretical understanding of anomaly based threat quantification.

VI. LITERATURE REVIEW

The integration of artificial intelligence in intrusion detection has gained substantial academic attention. Supervised learning models such as Random Forest and Neural Networks achieve high classification accuracy but depend heavily on labeled attack datasets. These models may struggle to detect novel or evolving threats.
Unsupervised anomaly detection techniques, particularly Isolation Forest, provide a promising alternative. Isolation Forest isolates anomalies by randomly partitioning data points; anomalous instances typically require fewer splits to isolate due to their rarity. However, most prior research emphasizes detection accuracy metrics such as precision and recall, rather than institutional-level risk assessment. Limited literature explores translating anomaly detection outputs into operational cyber risk metrics tailored to HEIs. This study addresses this gap by combining anomaly detection with dynamic risk scoring.

VII. METHODOLOGY

I. Research Design

An experimental research design was adopted using unsupervised machine learning implemented in Python with Scikit-learn.

II. Flow of Framework Execution

The proposed dynamic cyber risk assessment framework operates in a sequential and modular manner to ensure accurate anomaly detection and adaptive risk scoring. The execution flow is illustrated in **Figure 1.**

Step 1: Data Acquisition
Network traffic data is collected from the CSE-CIC-IDS2018 dataset, which contains both benign and malicious traffic samples across multiple attack categories.

Step 2: Data Preprocessing
Raw traffic records undergo preprocessing, including: • Removal of missing values

- Feature selection
- Encoding of categorical variables
- Normalization of numerical attributes

This ensures model stability and improved prediction performance.

Step 3: Model Training
A Random Forest classifier is trained using labeled traffic data. The ensemble learning mechanism enhances classification robustness and reduces overfitting.

Step 4: Real-Time Traffic Classification
Incoming traffic windows are fed into the trained model. Each instance is classified as:

- Benign (0)
- Malicious (1)

Step 5: Risk Score Computation
The risk score is dynamically calculated using:

$$Risk = \frac{Number\ of\ Anomalies}{Total\ traffic\ in\ Window}\ X\ 100$$

Step 6: Baseline Comparison
The computed risk score is compared against a historical baseline to determine deviation.

Step 7: Threat Level Assignment
Based on deviation magnitude, the system categorizes threat levels into:

- Low Risk
- Medium Risk
- High Risk

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 02, ISSN No. 2455-2143, Pages 144-148
Published Online June 2026 in IJEAST (http://www.ijeast.com)

Step 8: Alert Generation

If the deviation exceeds a predefined threshold, an alert is triggered for network administrators.

III. Sequence Diagram of Framework Execution

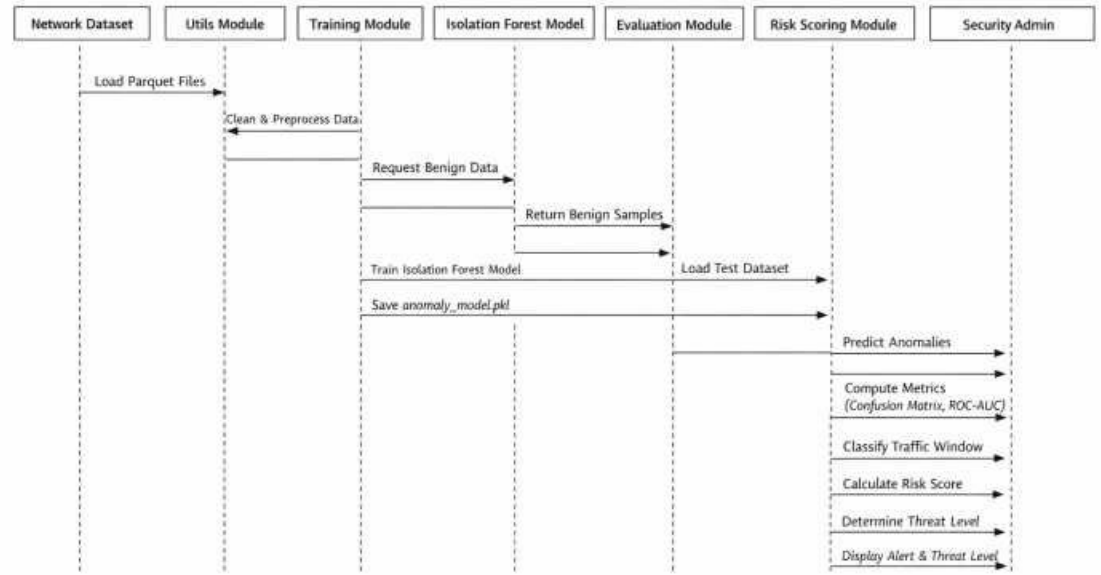

Figure 1 Sequence of Framework Execution

IV. Sample and Sampling Technique

The CSE-CIC-IDS2018 dataset was utilized. It includes diverse attack categories such as:

- DDoS attacks
- Bot attacks
- SSH brute force
- SQL injection
- Infiltration attacks

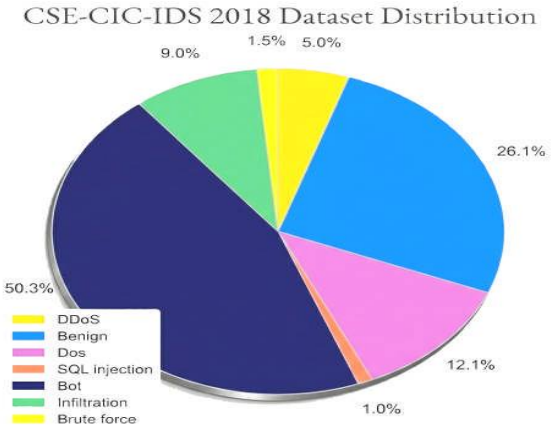

Figure 2 CSE-CIC-IDS-2018 dataset distributions

I. Sampling Strategy

To ensure balanced evaluation:

- 25,000 benign flows
- 25,000 attack flows
- Total evaluation window: 50,000 flows

II. Data Preprocessing

- Removal of null and infinite values
- Feature normalization using StandardScaler
- Binary encoding (Benign = 0, Attack = 1)

III. Model Training

Isolation Forest was trained exclusively on 5,329,008 benign flows to learn normal institutional traffic behavior.

VIII. RESULTS

I. Descriptive Statistics

Descriptive statistics summarize the dataset characteristics, including network traffic volume, user types, and types of detected activities within the sampled Higher Educational Institution network.

Variable	Frequency	Percentage
Benign Flows	25,000	50%
Attack Flows	25,000	50%
Total Flows	50,000	100%

Table 1 Class Distribution of Benign and Attack Flows in the Evaluation Dataset

II. Dynamic Risk Evaluation
Within the evaluation window:

- Total Flows: 50,000
- Anomalous Flows Detected: 2,115
- Observed Anomaly Rate: 4.23%

The dynamic risk score is calculated as:

$$\textit{Dynamic Risk Score} = \frac{\textit{Anomalous Flows}}{\textit{Total Flows}} \; X\,100$$

The framework compares the observed anomaly rate with the institutional historical baseline. Since the deviation remained within acceptable operational limits, the institutional threat level was categorized as **Low**.

IX. DISCUSSION

The observed anomaly rate of 4.23% suggests relative network stability. The system effectively identified statistically rare behaviors without relying on known attack signatures. Unlike static models, the proposed framework dynamically adjusts to institutional traffic patterns.
By incorporating baseline comparison, the model avoids overestimating risk during high-traffic academic periods.

X. LIMITATIONS

- Evaluation conducted on simulated dataset.
- Real-time streaming integration not implemented.
- Baseline thresholds predefined.
- Model performance may vary across institutions.

XI. CONCLUSION

The proposed AI-driven framework demonstrates that unsupervised anomaly detection can effectively monitor HEI network environments. By integrating dynamic risk scoring, the system provides adaptive and context-aware threat classification. The framework supports proactive cyber security management and strengthens institutional resilience against emerging threats.

XII. REFERENCES

[1]. Almuhanna R., and Dardouri S. (2025). A Deep Learning/Machine Learning Approach for Anomaly Based Network Intrusion Detection, Frontiers in Artificial Intelligence, Vol. 8, Article 1625891.
[2]. Neto E.C.P., Iqbal S., and Buffett S. (2025). Deep Learning for Intrusion Detection in Emerging Technologies: A Comprehensive Survey and New Perspectives, Artificial Intelligence Review, Vol. 58, Article 340.
[3]. Alabdulatif A. (2025). A Novel Ensemble of Deep Learning Approach for Cybersecurity Intrusion Detection with Explainable Artificial Intelligence, Applied Sciences, Vol. 15(14), Article 7984.
[4]. Wu Y., Zou B., and Cao Y. (2024). Current Status, Challenges and Future Trends of Deep Learning Based Intrusion Detection Models, Journal of Imaging, Vol. 10(10), p.254.
[5]. Sajid M., Malik K.R., and Almogren A. (2024). Enhancing Intrusion Detection: A Hybrid Machine and Deep Learning Approach, Journal of Cloud Computing, Vol. 13, Article 123.
[6]. Tian J. (2025). Integrating Artificial Intelligence into the Cybersecurity Curriculum in Higher Education: A Systematic Literature Review, Education Sciences, Vol. 15(11), Article 1540.
[7]. Adewusi M.A. (2025). A Design-Science Conceptual Framework Proposing a Zero-Trust Security Architecture and Implementation Roadmap for AI Enabled Cybersecurity in University-Industry Digital Ecosystems within the Industry 5.0 Era, SSRN Electronic Journal, Paper No. 5837705.
[8]. Afolalu O., and Tsoeu M.S. (2025). Cybersecurity in Higher Education Institutions: A Systematic Review of Emerging Trends, Challenges and Solutions, Future Internet, Vol. 17, pp.1–26.
[9]. Bosiu Y. (2017). Cybersecurity Risks and Initiatives at Higher Education Institutions, Master's Dissertation, University of Johannesburg.
[10]. Bwiino K., Mayoka G.K., Nkamwesiga L., and Nyamadi M. (2026). A Systematic Literature Review of Information Security Practices in Higher Education Contexts, IET Information Security, Vol. 2026, pp.1–19.
[11]. Dairo T.S., Shittu T.O., Beyioku J.B., and Odekunle Q.B. (2025). Transforming University Education through Usage of Artificial Intelligence (AI) in Lagos State Owned Universities: Panacea for Data-Driven Approach to Curb Menace of Cyber Security, ISA Journal of Arts, Humanities and Social Sciences, Vol. 2(6), pp.33–41.
[12]. Ibrahim N., and Rajalakshmi N.R. (2025). Examining the Influence of Advanced Persistent Threats on Higher Education Institutions and Investigating Appropriate Cybersecurity Strategies, U.Porto Journal of Engineering, Vol. 11(2), pp.96–119.
[13]. Liu F.T., Ting K.M., and Zhou Z.H. (2008). Isolation Forest, in Proceedings of the 8th IEEE International Conference on Data Mining (ICDM 2008), (pp.413–422).
[14]. Sharafaldin I., Lashkari A.H., and Ghorbani A.A. (2018). Toward a Reliable Dataset for Intrusion Detection, in Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018), (pp.177–188).
[15]. Wada I.U., Izibili G.O., Babayemi T., Abdulkareem A., Macaulay O.M., and 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, Vol. 25(03), pp.2233–2245.

[16]. Wambui B., Mwinji M., and Nyambura H. (2025). AI-Driven Cybersecurity Framework for Safeguarding University Networks from Emerging Threats, Journal of Cyber Security, Vol. 2025, pp.1– 20.

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE AND TECHNOLOGY

AUTHORS

Irfan Y. Belim

Dr. Bhargav Rajyagor

ABOUT IJEAST

International journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high - quality research paper in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

JOURNAL METRICS

H-INDEX	i10-INDEX	IJEAST CITATIONS	PEER-REVIEWED & OPEN ACCESS
33	154	9,647 (IJEAST CITATIONS)	PUBLISHED MONTHLY

PEER REVIEWED

All submission are rigorously peer reviewed to ensure quality.

AUTHORS ARE OUR PRIORITY

We value our authors and recognize their contribution to the advancement of research and knowledge.

OPEN ACCESS

Free and unrestricted access to research for all.

GLOBAL REACH

Connecting researchers and professionals worldwide.

TIMELY PUBLICATION

We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

editor@ijeast.com

www.ijeast.com

India

2455-2143