

# AI-Driven Cyber Threat Detection and Response Framework for Higher Educational Institutions (HEIs)

Irfan Belim<sup>1,\*</sup>, Bhargav Rajyagor<sup>2</sup>

## 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 research introduces an AI-based framework for detecting and responding to cyber threats, specifically designed for HEIs. The framework employs an unsupervised machine learning model—Isolation Forest—trained exclusively on benign network traffic to identify anomalous behavior 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 cybersecurity strategies in HEIs. The proposed framework offers both practical and conceptual improvements by combining machine learning-driven anomaly detection with cyber risk assessment techniques for institutions.

**Keywords:** Artificial intelligence, cyber security, anomaly detection, higher education security, risk scoring

## INTRODUCTION

Digital transformation has fundamentally reshaped higher educational institutions (HEIs). Universities now operate highly interconnected infrastructures that support academic portals, online learning platforms, research databases, cloud computing environments, IoT-enabled laboratories, and administrative systems [1]. While this digital evolution enhances accessibility and innovation, it also

### \*Author for Correspondence

Irfan Belim  
E-mail: belimirfan1989@gmail.com

<sup>1</sup>Assistant Professor, Faculty of Computer Application, Noble University, Junagadh, Bامangam, Gujarat, India

<sup>2</sup>Associate Professor, Faculty of Computer Application, Noble University, Junagadh, Bامangam, Gujarat, India

Received Date: March 14, 2026

Accepted Date: June 15, 2026

Published Date: July 20, 2026

**Citation:** Irfan Belim, Bhargav Rajyagor. AI-Driven Cyber Threat Detection and Response Framework for Higher Educational Institutions (HEIs). Journal of Network Security. 2026; 14(2): 28–34p.

significantly increases institutional exposure to cyberthreats. HEIs differ from corporate organizations in one critical aspect: their openness. Academic institutions prioritize collaboration and accessibility, often allowing broad network access to students, faculty, visiting researchers, and third-party partners [2, 3]. This openness, combined with high user turnover and bring-your-own-device (BYOD) practices, creates a complex cybersecurity environment.

Traditional intrusion detection systems (IDS) primarily rely on signature-based detection

mechanisms. Although effective against known threats, these systems struggle to detect previously unseen or zero-day attacks. As cyberattacks become more sophisticated and adaptive, HEIs require intelligent, self-learning detection frameworks capable of identifying abnormal behavior rather than predefined attack patterns [4]. This study proposes an AI-driven anomaly detection framework specifically designed for HEIs. The system leverages unsupervised machine learning to model normal network behavior and dynamically assess institutional cyber risks [5, 6].

## Background

In recent years, universities and educational institutions worldwide have become major targets for cyberattacks because of their large digital infrastructure and extensive use of online systems. Several global incidents, including ransomware attacks, distributed denial-of-service (DDoS) attacks during examination periods, and unauthorized data theft, have exposed serious weaknesses in academic network security [7]. These attacks not only disrupt teaching and administrative activities but also put sensitive student, faculty, and research data at risk of being compromised. Since universities often maintain open and collaborative environments, securing their networks has become more challenging than ever before [8].

To address these growing threats, organizations are increasingly adopting advanced cybersecurity technologies that can identify suspicious activities before significant damage occurs. Among these technologies, machine learning has gained considerable attention because of its ability to efficiently analyze large amounts of network traffic [9]. In particular, unsupervised anomaly detection techniques are highly useful because they can detect unusual or abnormal behaviors without depending on previously labeled attack data. This makes them effective for identifying new and evolving cyber threats in real time [10].

## 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 is relative to normal baseline behavior.

## Research Objectives

This study aims to:

1. Develop an AI-driven anomaly detection framework for HEIs.
2. Train an Isolation Forest model on benign network traffic.
3. Detect suspicious network flows without attack signatures.
4. Introduce a dynamic institutional cyber risk scoring mechanism.
5. Classify threat levels based on real-time anomaly deviations.

## Significance of 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.

## Literature Review

The application of artificial intelligence in cybersecurity and IDS has become an important area of academic and industrial research in the last decade [2]. Traditional supervised machine learning techniques, including Random Forest, Support Vector Machines, and Neural Networks, have demonstrated strong performance in identifying known cyberattacks with high levels of accuracy,

---

precision, and recall [9, 11, 12]. These approaches rely heavily on large volumes of labeled training data, allowing the models to learn attack signatures and classify malicious activities effectively. However, their dependence on predefined datasets creates a major limitation, as modern cyber threats continuously evolve and often appear in forms that are not represented in the historical training data [5, 13]. Consequently, supervised methods may fail to recognize zero-day attacks or previously unseen malicious behaviors.

To overcome these challenges, researchers have increasingly explored unsupervised anomaly detection methods [12]. Among these, the Isolation Forest has gained significant attention because of its efficiency and ability to identify unusual patterns without requiring labeled data [14]. The algorithm works by randomly partitioning observations within a dataset, where anomalous data points are isolated more quickly because of their rarity and distinct characteristics. This makes the Isolation Forest highly suitable for dynamic and complex network environments [1]. Despite these advantages, much of the existing literature focuses primarily on technical detection performance and benchmarking metrics [15, 16]. Fewer studies have examined how anomaly detection outcomes can be transformed into practical cyber risk indicators for institutional decision-making. In the context of HEIs, there is limited research on integrating anomaly detection with adaptive risk assessment frameworks [17]. Therefore, this study attempts to bridge this gap by combining anomaly detection techniques with dynamic cyber risk scoring to support more effective and proactive cybersecurity management.

## **METHODOLOGY**

### **Research Design**

This study adopted an experimental research design to examine patterns and relationships within the collected dataset using unsupervised machine learning techniques. This research primarily focused on identifying hidden structures in data without using predefined labels or target outcomes. The Python programming language was selected as the main development environment because of its flexibility, reliability, and strong support for data analysis and machine learning applications [6]. The implementation process was performed using the Scikit-learn library, which provides efficient tools for clustering, dimensionality reduction, and data preprocessing. Different experimental procedures were followed to ensure accurate model performance and consistency in the results. The design also allowed for repeated testing and comparison of the outputs generated by the algorithms. This approach helped improve the reliability of the findings while supporting the systematic analysis and interpretation of complex data patterns in an effective and organized manner [10, 11].

### **Flow of Framework Execution**

The proposed dynamic cyber risk assessment framework operates sequentially and modularly to ensure accurate anomaly detection and adaptive risk scoring [16]. The execution flow is shown in Figure 1.

#### ***Step 1: Data Acquisition***

Network traffic data were 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 was trained using labeled traffic data. The ensemble learning mechanism enhances the robustness of the classification and reduces overfitting.

**Step 4: Real-Time Traffic Classification**

The incoming traffic windows were fed into the trained model. Each instance is classified as follows:

- Benign (0)
- Malicious (1)

**Step 5: Risk Score Computation**

The risk score is dynamically calculated using:

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

**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

**Step 8: Alert Generation**

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

**SEQUENCE DIAGRAM OF FRAMEWORK EXECUTION****Sample and Sampling Technique**

The CSE-CIC-IDS2018 dataset was used, as shown in Figure 2. It includes diverse attack categories, such as:

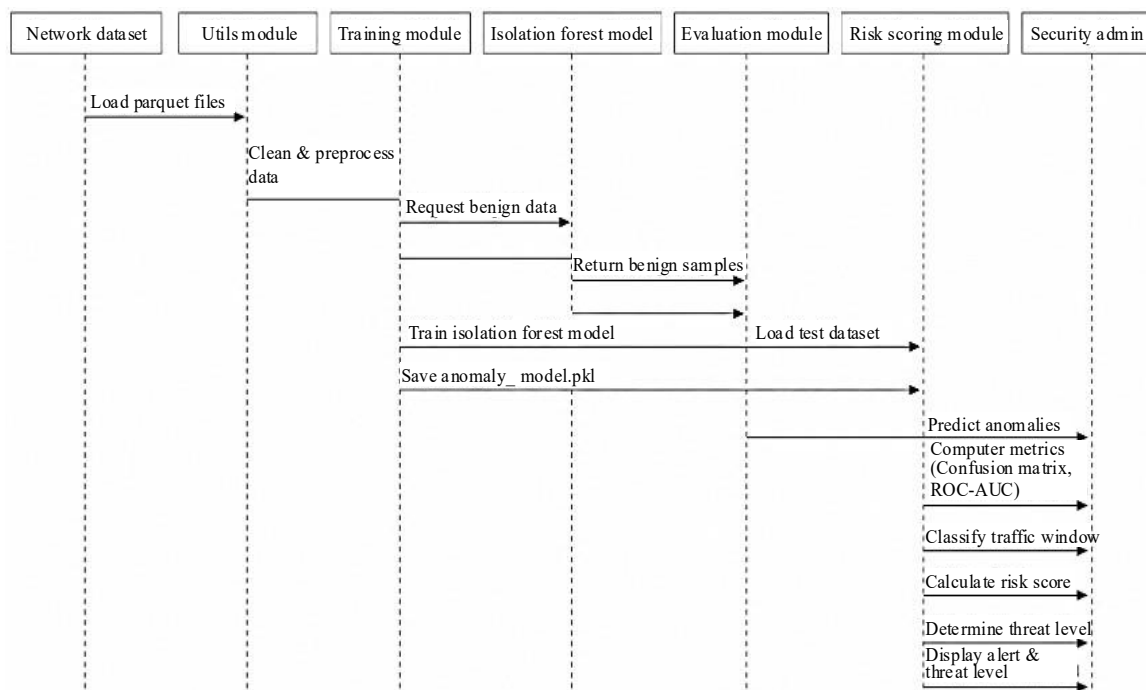


**Figure 1.** Sequence of framework execution.

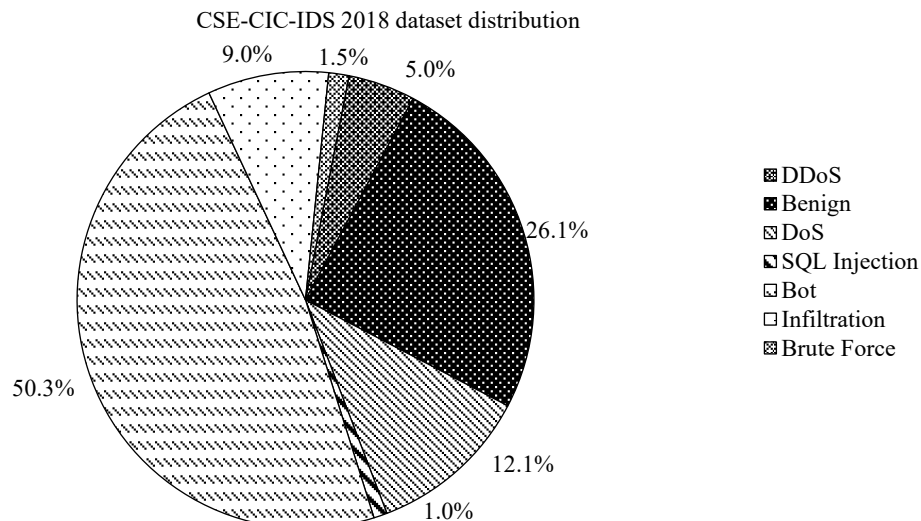


**Figure 2.** CSE-CIC-IDS-2018 dataset distributions.

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

### Sampling Strategy

To ensure balanced evaluation:

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

### Data Preprocessing

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

### Model Training

The isolation forest was trained exclusively on 5,329,008 benign flows to learn the normal institutional traffic behavior.

## RESULTS

### 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 (Table 1).

**Table 1.** Class distribution of benign and attack flows in the evaluation dataset.

| Variable     | Frequency | Percentage |
|--------------|-----------|------------|
| Benign flows | 25,000    | 50%        |
| Attack flows | 25,000    | 50%        |
| Total flows  | 50,000    | 100%       |

### 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:

$$\text{Dynamic risk score} = \frac{\text{Anomalous flows}}{\text{Total flows}} \times 100$$

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

### DISCUSSION

The observed anomaly rate of 4.23% suggests a relatively stable network. The system effectively identifies statistically rare behaviors without relying on known attack signatures. Unlike static models, the proposed framework dynamically adjusts to the institutional traffic patterns.

By incorporating a baseline comparison, the model avoids overestimating the risk during high-traffic academic periods.

### Limitations

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

### CONCLUSION

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

### REFERENCES

1. Almuhanha R, Dardouri S. A deep learning/machine learning approach for anomaly based network intrusion detection. *Front Artif Intell*. 2025;8:1625891. doi:10.3389/frai.2025.1625891. PMID:40995028.
2. Neto ECP, Iqbal S, Buffett S, Sultana M, Taylor A. Deep learning for intrusion detection in emerging technologies: a comprehensive survey and new perspectives. *Artif Intell Rev*. 2025;58:340. doi:10.1007/s10462-025-11346-z.
3. Alabdulatif A. A novel ensemble of deep learning approach for cybersecurity intrusion detection with explainable artificial intelligence. *Appl Sci (Basel)*. 2025;15:7984. doi:10.3390/app15147984.
4. Wu Y, Zou B, Cao Y. Current status and challenges and future trends of deep learning-based intrusion detection models. *J Imaging*. 2024;10:254. doi:10.3390/jimaging10100254. PMID:39452417.
5. Sajid M, Malik KR, Almogren A, Malik TS, Khan AH, Tanveer J, et al. Enhancing intrusion detection: a hybrid machine and deep learning approach. *J Cloud Comput*. 2024;13:123. doi:10.1186/s13677-024-00685-x.
6. Tian J. Integrating artificial intelligence into the cybersecurity curriculum in higher education: a systematic literature review. *Educ Sci (Basel)*. 2025;15:1540. doi:10.3390/educsci15111540.

7. Adewusi MA. A design-science, conceptual framework paper proposing a zero-trust security architecture and implementation roadmap for AI-enabled cybersecurity in university-industry digital ecosystems within the Industry 5.0 era [Preprint]. 2025. doi:10.2139/ssrn.5837705.
8. Afolalu O, Tsoeu MS. Cybersecurity in higher education institutions: a systematic review of emerging trends, challenges and solutions. *Future Internet*. 2025;17(12):575. doi:10.3390/fi17120575.
9. Bwiino K, Mayoka GK, Nkamwesiga L, Nyamadi M, Shirani P. A systematic literature review of information security practices in higher education contexts. *IET Inf Secur*. 2026;2026(1):1-19. doi:10.1049/ise2/6324508.
10. Mahuta GA, Abubakar H. Artificial intelligence in higher education in Nigeria: challenges and way forward. *J Contemp Res Educ Adm Manag*. 2025;2:62-71.
11. Ibrahim N, Rajalakshmi NR. Examining the influence of advanced persistent threats on higher education institutions and investigating appropriate cybersecurity strategies. *U.Porto J Eng*. 2025;11:96-119. doi:10.24840/2183-6493\_0011-002\_002671.
12. Liu FT, Ting KM, Zhou ZH. Isolation forest. In: *Proceedings of the Eighth IEEE International Conference on Data Mining*; 2008 Dec 15-19; Pisa, Italy. p.413-22. doi:10.1109/ICDM.2008.17.
13. Sharafaldin I, Gharib A, Lashkari AH, Ghorbani AA. Towards a reliable intrusion detection benchmark dataset. *Softw Netw*. 2018:177-200.
14. Wada IU, Izibili GO, Babayemi T, Abdulkareem A, Macaulay OM, Emadoye A. AI-driven cybersecurity in higher education: a systematic review and model evaluation for enhanced threat detection and incident response. *World J Adv Res Rev*. 2025;25:2233-45.
15. Singh NK, Panday A, Shrivastava V. AI in cybersecurity: detecting and preventing cyber threats using machine learning. *Clareus Sci Sci Eng*. 2025;2(8):19-25.
16. Reddy Y. Artificial intelligence in intrusion detection systems: trends, frameworks, and future directions for cybersecurity. *Int J Intell Syst Appl Eng*. 2023;12:949-59.
17. D'Hooge L. CSE-CIC-IDS2018 [dataset]. Kaggle; 2018. Available from: <https://www.kaggle.com/datasets/dhoogla/csecicids2018>