IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 12, December 2025

DOI: 10.17148/IARJSET.2025.121241

# Cyberflux: Intrusion Detection and Monitoring System

**Gayathri S[1], M Dheeraj[2], Mayur S[3], Sanjana P[4], Sonika N C[5]**

Assistant Professor, Department of Computer Science and Engineering, Maharaja Institute of Technolgoy, Mysore, Karnataka, India[1]

Undergraduate student, Department of Computer Science and Engineering, Maharaja Institute of Technology, Mysore, Karnataka, India[2,3,4,5]

**Abstract**: With the rapid growth of digital infrastructure and network-based services, organizations are increasingly vulnerable to cyber threats such as unauthorized access, malware injection, and denial-of-service attacks. Traditional security mechanisms often fail to provide real-time detection and continuous monitoring of network activities. This paper presents CyberFlux, a intrusion detection and monitoring system designed to identify malicious network behavior and provide timely alerts to system administrators. The proposed system analyzes network traffic patterns and system logs to detect anomalies and classify potential intrusions. CyberFlux integrates a centralized monitoring dashboard that enables real-time visualization of security events and intrusion reports. The system is implemented using a scalable backend architecture and evaluated under simulated attack scenarios to validate its effectiveness. Experimental results demonstrate improved detection accuracy and faster response times compared to conventional rule-based systems. The proposed solution is suitable for deployment in small- and medium-scale organizational environments to enhance cybersecurity resilience.

**Keywords**: Intrusion Detection, Cybersecurity, Machine Learning, Deep Learning, Network Security, Monitoring System.

## I. INTRODUCTION

### *A. Problem Statement*

With the rapid growth of digital networks, cloud platforms, and online services, organizations are increasingly exposed to cyber threats such as unauthorized access, malware, brute-force attacks, and denial-of-service attacks. Traditional intrusion detection systems are primarily signature-based and rely on predefined rules to identify known attacks. While effective against previously identified threats, these systems fail to detect zero-day attacks and evolving intrusion patterns. Furthermore, many conventional security solutions generate a high number of false positives, leading to alert fatigue and delayed responses from security administrators. The lack of real-time monitoring and intelligent analysis makes it difficult for organizations to maintain continuous situational awareness of their network security posture. These limitations highlight the need for an adaptive, intelligent, and real-time intrusion detection and monitoring system.

### *B. Proposed Solution*

To address the above challenges, this paper proposes CyberFlux, a hybrid machine learning and deep learning–based intrusion detection and monitoring system. The proposed system integrates ensemble-based machine learning algorithms with deep learning models to effectively detect both known and unknown cyber attacks.

CyberFlux employs machine learning models such as Random Forest and XGBoost for fast and efficient classification of network traffic. In parallel, deep learning models including Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, and Autoencoders are used to capture complex spatial and temporal patterns in network data. The hybrid detection strategy enhances detection accuracy while reducing false positives.

In addition to intelligent detection, CyberFlux provides a web-based monitoring dashboard that enables real-time visualization of intrusion alerts, network activity, and system logs. This integrated approach allows security administrators to quickly identify threats and take appropriate action.

DOI: 10.17148/IARJSET.2025.121241

### C. Contributions

The main contributions of this work are summarized as follows:

- Development of a hybrid intrusion detection framework combining machine learning and deep learning techniques for improved detection accuracy.
- Implementation of ensemble-based machine learning models (Random Forest and XGBoost) for efficient classification of network traffic.
- Integration of deep learning models (CNN, LSTM, and Autoencoder) to detect complex and previously unseen attack patterns.
- Design of a web-based real-time monitoring dashboard for visualization of intrusion events and alerts.
- Experimental evaluation of the proposed system using benchmark datasets along with synthetic data generator (GAN) to validate system performance.

*Paper Structure*

"The remainder of this paper is organized as follows: Section II details the Literature Survey. Section III describes the System Architecture including data collection, detection engine, backend processing, and monitoring dashboard. Section IV presents the methodology and implementation. Section V discusses the experimental results and performance analysis of the system. Section VI outlines the testing and validation procedures, and section VII concludes the paper and highlights future research directions."

## II. Literature Survey

Intrusion detection has been a major research focus in cybersecurity due to the increasing sophistication of cyber attacks. Traditional signature-based intrusion detection systems are limited in their ability to detect novel and zero-day attacks. As a result, researchers have explored machine learning and deep learning techniques to improve detection accuracy and adaptability.

[1] Yin et al. (2017): Proposed an intrusion detection framework based on Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) models to analyze network traffic sequences. The study demonstrated that LSTM models are effective in capturing temporal dependencies in traffic flows, which is crucial for identifying attacks such as Denial of Service (DoS) and brute-force intrusions. Although the system achieved higher detection accuracy than traditional machine learning approaches, it relied on a single deep learning model, which limited its generalization capability. The work also lacked real-time deployment, explainability, and user interaction features. [2] Kim et al. (2018): Explored the application of Convolutional Neural Networks (CNNs) for intrusion detection by transforming network traffic features into matrix-like representations. The CNN model successfully learned spatial correlations between traffic features and achieved promising classification accuracy. However, the proposed system focused mainly on supervised learning and struggled with detecting zero-day attacks. Additionally, the model lacked interpretability and real-time visualization support. [3] Mirsky et al. (2018): Presented an anomaly-based intrusion detection system using Autoencoders trained on normal network traffic. The system detected intrusions based on reconstruction error, making it suitable for identifying previously unseen attacks. Despite its effectiveness in anomaly detection, the system suffered from high false positive rates and did not classify attack types. It also lacked visualization and real-time alerting mechanisms. [4] Zhou et al. (2019): Proposed an ensemble-based IDS combining multiple machine learning classifiers to improve detection accuracy and stability. The study showed that ensemble methods outperform individual classifiers across different datasets. However, the approach did not integrate deep learning models, explainability mechanisms, or real-time system deployment. [5] Lin et al. (2020): Investigated the use of Generative Adversarial Networks (GANs) to generate synthetic network traffic for improving intrusion detection model training. The study addressed dataset imbalance and enhanced model robustness.The work focused mainly on data generation and did not implement a complete IDS pipeline or real-time detection system. [6] Josef Koumar, Timotej Smole, Kamil Jeřábek, Tomáš Čejka (2025): Conducted a comparative analysis of various deep learning models, including LSTM and CNN, on real-world network traffic data. The study focused on forecasting traffic behavior and demonstrated that deep learning models can effectively learn complex traffic patterns under realistic conditions. Although the work does not directly address intrusion detection, it provides strong evidence that deep learning models are capable of modeling real-world network traffic dynamics. [7] Ravi Sekhar, Pritesh Shah, B. S. Veena (2024): Proposed a machine learning-based approach for network traffic classification, using

DOI: 10.17148/IARJSET.2025.121241

supervised learning algorithms to categorize network flows. The system achieved improved classification accuracy and demonstrated the effectiveness of ML techniques in traffic analysis. However, the study relied on limited ML models and did not include anomaly detection, explainability, ensemble learning, or real-time visualization. [8] Ons Aouedi, Van An Le, Kandaraj Piamrat (2025): This survey paper presents a comprehensive overview of deep learning techniques applied to network traffic analysis, including LSTM, CNN, Autoencoders, and hybrid approaches. It highlights open challenges such as scalability, interpretability, real-time deployment, and robustness. The paper emphasizes the need for explainable and adaptive IDS systems in modern networks. [9] Breiman et al (2001): Breiman introduced the Random Forest algorithm, which has since been extensively applied in network intrusion detection due to its robustness, low overfitting, and ability to handle high-dimensional tabular data. In IDS research, Random Forest models have shown strong performance in classifying network traffic into normal and attack categories. Random Forest classifiers are particularly effective in handling noisy network data and providing stable predictions with low inference latency. However, when used alone, they may fail to capture complex temporal patterns present in advanced cyberattacks. [10] Tianqi Chen and Carlos Guestrin. (2016): Proposed XGBoost, a highly efficient and scalable gradient boosting framework. XGBoost has been widely adopted in intrusion detection systems due to its high classification accuracy, regularization support, and efficient handling of large-scale tabular datasets. In IDS applications, XGBoost performs well in detecting known attack patterns and provides strong generalization across different datasets. However, similar to other supervised models, it requires labeled data and may struggle with zero-day attacks when used independently.

Based on these observations, there is a clear need for an intrusion detection system that not only achieves high detection performance but also supports real-time monitoring and practical deployment. The proposed CyberFlux system addresses this gap by integrating hybrid ML-DL detection models with a centralized monitoring dashboard and alerting framework.

## III. SYSTEM ARCHITECTURE

The CyberFlux intrusion detection system is designed as a modular and scalable architecture that integrates data collection, intelligent detection, and real-time monitoring. The system follows a layered approach to ensure flexibility, maintainability, and efficient processing of large volumes of network traffic data.

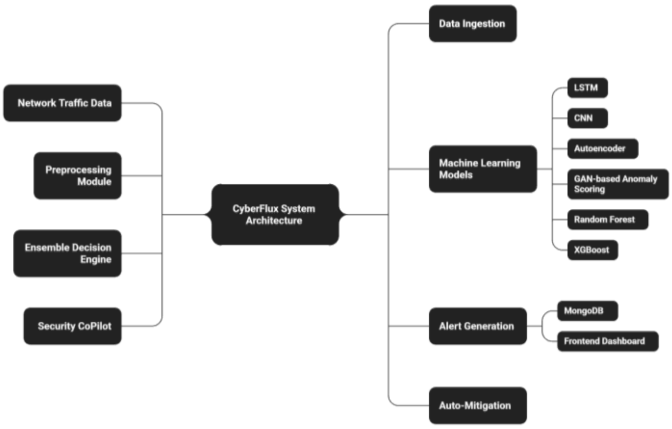


Figure 1: System Architecture

### A. *Data Collection Layer*

The data collection layer is responsible for acquiring network traffic and system activity data. For experimental evaluation, benchmark intrusion detection datasets such as NSL-KDD and KDDcup99 are used. These datasets provide labeled records representing both normal and malicious network behavior.

In a real-world deployment scenario, this layer can be extended to collect live network traffic, system logs, and packet-level information from routers, firewalls, or servers. The collected data is preprocessed to remove noise, handle missing values, and normalize features before being passed to the detection engine.

### B. *Detection Engine: Hybrid ML and DL Models*

The core intelligence of CyberFlux lies in its hybrid detection engine, which combines machine learning and deep

DOI: 10.17148/IARJSET.2025.121241

learning techniques. Machine learning models are used for fast and efficient classification of known attack patterns, while deep learning models are employed to capture complex and non-linear relationships within network traffic data.

The hybrid approach improves detection accuracy and robustness by leveraging the strengths of both methods. Feature extraction and selection techniques are applied to reduce dimensionality and improve model performance. The detection engine outputs classification results indicating normal activity or specific intrusion categories.

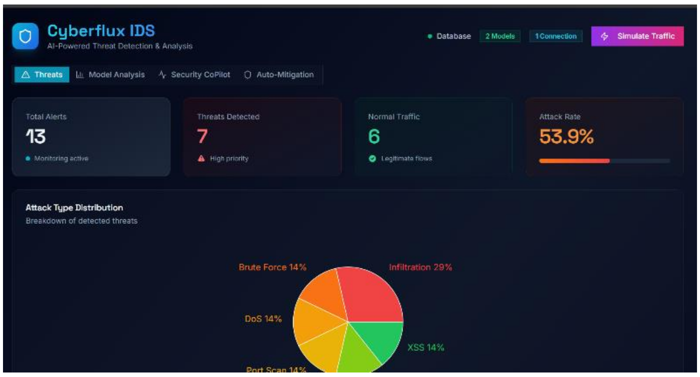
### *C. Backend Processing Layer*

The backend processing layer acts as the central coordinator of the system. It receives detection results from the ML–DL models, stores them in a structured database, and triggers alert mechanisms when suspicious activity is detected. This layer is responsible for handling user authentication, data management, and communication between the detection engine and the monitoring dashboard. The backend is designed to be scalable and capable of handling multiple data streams simultaneously. It also maintains historical records of detected intrusions, enabling trend analysis and forensic investigation

### *D. Monitoring Dashboard*

CyberFlux includes a web-based monitoring dashboard that provides real-time visualization of network activity and intrusion alerts. The dashboard displays key security metrics such as detected attack types, timestamps, severity levels, and system status. This enables security administrators to quickly identify threats and take appropriate action.

The dashboard enhances situational awareness by presenting intrusion data in an intuitive and user-friendly manner. It also supports log viewing and report generation, making the system suitable for practical deployment in organizational environments.



Total Alerts 13
Monitoring active

Threats Detected 7
High priority

Normal Traffic 6
Legitimate flows

Attack Rate 53.9%

Figure 2: Dashboard Overview

## IV. METHODOLOGY AND IMPLEMENTATION

The CyberFlux system employs a hybrid intrusion detection methodology that integrates classical machine learning models with advanced deep learning techniques. This hybrid design improves detection accuracy while maintaining computational efficiency.

### *A. Machine Learning Models*

To achieve fast and reliable classification, CyberFlux incorporates Random Forest and XGBoost models. These ensemble-based algorithms are effective in handling high-dimensional intrusion detection data and reducing overfitting.

- Random Forest is used to classify network traffic by aggregating multiple decision trees, improving robustness and generalization.
- XGBoost is employed for its gradient-boosting capability, which enhances detection accuracy and minimizes classification errors.

These models provide rapid initial classification of network activity.

### *B. Deep Learning Models*

To capture complex temporal and spatial patterns in network traffic, deep learning models are integrated into the detection engine:

DOI: 10.17148/IARJSET.2025.121241

- Convolutional Neural Networks (CNN) are used to extract spatial features from network traffic data.
- Long Short-Term Memory (LSTM) networks analyze sequential dependencies and temporal attack patterns.
- Autoencoders are utilized for anomaly detection by learning normal traffic behavior and identifying deviations.
- Generative Adversarial Network (GAN) for generating high-quality synthetic data.

The deep learning models enhance the system's ability to detect unknown and zero-day attacks.

### *C. Hybrid Detection Strategy*

The outputs of the machine learning and deep learning models are combined using a decision fusion strategy. This hybrid approach balances speed and accuracy by leveraging ML models for quick detection and DL models for deep analysis. Detected intrusions are categorized and forwarded to the backend system for logging and alert generation.

## V. RESULT AND ANALYSIS

The performance of CyberFlux is evaluated using standard metrics such as accuracy, precision, recall, and F1-score. Experimental results demonstrate that the hybrid ML–DL approach outperforms individual models in intrusion detection accuracy.

The system successfully identifies various attack types present in the NSL-KDD and KDDcup99 datasets along with synthetic data generator, including denial-of-service, probing, and brute-force attacks. The integration of deep learning models significantly reduces false positives, while ensemble-based machine learning models ensure faster classification. The web dashboard provides real-time visualization of detected intrusions, enabling effective monitoring and analysis.

## VI. TESTING AND VALIDATION

Table 1: Testing and Validation

| Test Case | Objective | Result |
|---|---|---|
| Data Preprocessing Test | Validate encoding and normalization | Successful |
| ML Model Testing | Evaluate Random Forest & XGBoost accuracy | High accuracy achieved |
| DL Model Testing | Validate CNN, LSTM, Autoencoder performance | Stable and reliable |
| Hybrid Model Test | Verify fusion-based detection | Improved accuracy |
| Dashboard Test | Validate real-time alert display | Alerts displayed correctly |
| End-to-End Test | Validate complete workflow | System operates as expected |

## VII. FUTURE IMPLEMENTATIONS

Future work will focus on integrating real-time packet capture, deploying the system in cloud environments, and enhancing detection performance using transformer-based deep learning models. Additionally, automated incident response mechanisms can be incorporated to further reduce reaction time to cyber threats.

## VIII. CONCLUSION

This paper presented CyberFlux, a hybrid machine learning and deep learning–based intrusion detection and monitoring system designed to enhance cybersecurity resilience. By combining ensemble-based machine learning models with deep learning techniques, the system achieves high detection accuracy while supporting real-time monitoring through a web-based dashboard.

CyberFlux effectively addresses the limitations of traditional rule-based intrusion detection systems by detecting both known and unknown attacks. The modular architecture ensures scalability and practical deployment in small- and medium-sized organizational environments.

DOI: 10.17148/IARJSET.2025.121241

## ACKNOWLEDGMENT

The authors express sincere gratitude to **Dr. Shivamurthy R C** – Professor and Head, **Prof. Gayathri S**, Assistant Professor, Department Computer Science and Engineering, Maharaja Institute of Technology, Mysore, for in valuable guidance in system architecture design and project mentorship. We acknowledge the support of the institution in providing resources and infrastructure for development and testing.

## REFERENCES

[1] Y. Yin, W. Zhu, J. Wang, and J. Gu, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.

[2] G. Kim, S. Lee, and S. Kim, "Convolutional Neural Network-Based Network Intrusion Detection," *Expert Systems with Applications*, vol. 95, pp. 1–13, 2018.

[3] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection," *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2018.

[4] Z. Zhou, M. Dong, K. Ota, and A. Liu, "Ensemble Learning Techniques for Network Intrusion Detection Systems," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3936–3965, 2019.

[5] E. Lin, Q. Chen, and Z. Liu, "Using Generative Adversarial Networks to Generate Synthetic Network Traffic for Intrusion Detection," *IEEE Access*, vol. 8, pp. 215743–215755, 2020.

[6] J. Koumar, T. Smole, K. Jeřábek, and T. Čejka, "Comparative Analysis of Deep Learning Models for Real-World Network Traffic Forecasting," *arXiv preprint arXiv:2503.17410*, 2025.

[7] R. Sekhar, P. Shah, and B. S. Veena, "Enhanced Network Traffic Classification with Machine Learning Algorithms," *Proceedings of the ACM Conference on Computer and Communications Security*, 2024.

[8] O. Aouedi, V. A. Le, and K. Piamrat, "Deep Learning on Network Traffic Prediction: Recent Advances, Analysis, and Future Directions," *ACM Computing Surveys*, vol. 57, no. 1, pp. 1–36, 2025.

[9] L. Breiman, "Random Forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.

[10] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 785–794, 2016.

## BIOGRAPHY

**Gayathri S** is an Assistant Professor in the Department of Computer Science and Engineering at Maharaja Institute of Technology, Mysore, Karnataka, India. Her academic and research interests include Information Technology.

**M Dheeraj** is an undergraduate student in Computer Science and Engineering at Maharaja Institute of Technology, Mysore, Karnataka, India. His areas of interest include, Artificial Intelligence, and Full stack development.

**Mayur S** is an undergraduate student in Computer Science and Engineering at Maharaja Institute of Technology, Mysore, Karnataka, India. His interests include Cybersecurity, Software development and Mern stack development.

**Sanjana P** is an undergraduate student in Computer Science and Engineering at Maharaja Institute of Technology, Mysore, Karnataka, India. His academic interests include Artificial intelligence, and Full Stack development.

**Sonika N C** is an undergraduate student in Computer Science and Engineering at Maharaja Institute of Technology, Mysore, Karnataka, India. His interests include Full Stack development, and AI/ML.