© DEC 2025 | IRE Journals | Volume 9 Issue 6 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I6-1713209

AI-Powered Cybersecurity Threat Monitoring and Response System

C M SUMANA[1], AASIM RUMI SANIA[2], AISHWARYA R[3], G VAISHNAVI[4], VASANTHI G[5]
[1]*Asst Prof, Dept of CSE (Artificial Intelligence and Machine Learning), Rao Bahadur Y Mahabaleswarappa Engineering college, Ballari, Karnataka, India.*
[2,3,4,5] *Students of Dept of CSE (Artificial Intelligence and Machine Learning), Rao Bahadur Y Mahabaleswarappa Engineering college, Ballari, Karnataka, India.*

Abstract - The growing dependence on interconnected digital systems has resulted in a significant rise in complex and intelligent cyber threats that challenge the effectiveness of conventional security mechanisms. Traditional intrusion detection approaches, which rely on static rules and predefined signatures, often fail to detect newly emerging and adaptive attacks in real time. To overcome these limitations, this paper presents an artificial intelligence–based cybersecurity threat monitoring and response system capable of identifying and mitigating malicious network activities automatically. The proposed framework continuously observes network traffic and evaluates critical attributes such as protocol usage, packet behavior, and traffic flow patterns using supervised machine learning models, including Random Forest and K-Nearest Neighbors. To assess system performance under realistic conditions, an attacker simulation module is integrated to generate controlled attack scenarios. When suspicious activity is detected, the system initiates automated firewall recovery actions and immediately notifies administrators through real-time alerts. The experimental implementation demonstrates improved detection accuracy, faster response time, and enhanced network security, making the proposed system suitable for modern dynamic network environments.

Keywords: Artificial Intelligence, Cybersecurity, Intrusion Detection, Machine Learning, Network Traffic Monitoring, Automated Response

I. INTRODUCTION

The widespread adoption of digital technologies, cloud platforms, and high-speed networks has transformed the way organizations operate and exchange information. While these advancements improve efficiency and connectivity, they also introduce serious security challenges by expanding the attack surface of modern network infrastructures. Cyber threats have become increasingly sophisticated, targeting system vulnerabilities through coordinated and stealthy attack techniques that are difficult to detect using traditional security tools.

Conventional security systems such as rule-based firewalls and signature-based intrusion detection systems depend heavily on predefined attack patterns and manual updates. Although effective against known threats, these systems struggle to identify novel, zero-day, and rapidly evolving attacks. Their reactive nature often leads to delayed detection and response, increasing the risk of data breaches, service disruption, and financial loss.

This paper proposes an AI-powered cybersecurity threat monitoring and response system designed to provide real-time detection and automated mitigation of network-based attacks. The system employs supervised machine learning algorithms, specifically Random Forest and K-Nearest Neighbors, to classify network traffic as legitimate or malicious. An attacker simulation module is incorporated to evaluate system performance under realistic attack conditions. Upon detecting malicious behavior, the system automatically triggers firewall recovery mechanisms and delivers instant alerts to system administrators. The proposed approach aims to enhance network security by improving detection accuracy, minimizing response time, and strengthening overall system resilience in dynamic computing environments.

© DEC 2025 | IRE Journals | Volume 9 Issue 6 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I6-1713209

II. REVIEW OF LITERATURE

1. Axelsson S (2000) classified intrusion detection systems into signature-based and anomaly-based approaches and reported limitations in detecting unknown attacks.
2. Breiman L (2001) proposed the Random Forest algorithm, which improved classification accuracy and robustness and was later adopted for network intrusion detection
3. Tavallaee M et al. (2009) analyzed the KDD Cup 99 dataset and identified redundancy and imbalance issues affecting intrusion detection evaluation.
4. Buczak AL and Guven E (2016) reviewed machine learning techniques for cybersecurity and observed superior performance of supervised and ensemble models.
5. [Gary Bradski & Adrian Kaehler] → Offered their work "Learning OpenCV" which provides practical methods for image/video operations like frame capture, resizing, drawing, and video writing.
6. Ring M et al. (2018) demonstrated that flow-based traffic analysis enables detection of slow and stealthy network attacks.

III. SYSTEM ARCHTECTURE

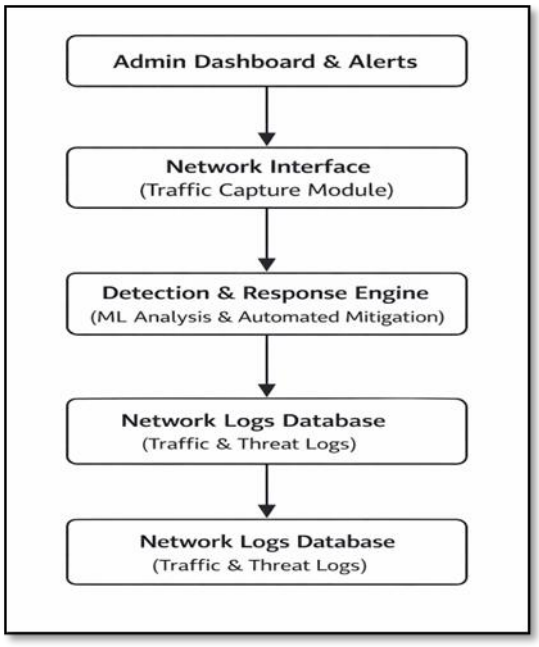


Fig 1: System Archtecture

Admin Dashboard and Alert Management:
This phase provides a centralized interface for administrators to monitor network activity and system status. Detected threats and system events are displayed in real time. Alert notifications are generated for suspicious or malicious activities. The dashboard enables visualization of traffic trends and threat statistics. Administrative actions are logged for audit and analysis purposes. At the data acquisition layer, real-time network traffic is continuously captured from the monitored environment. In parallel, an attacker simulation module generates controlled cyberattack scenarios to evaluate the system's detection and response capabilities. The collected data includes network attributes such as source and destination IP addresses, protocol types, packet sizes, and traffic frequency.

Network Interface (Traffic Capture Module):
This phase is responsible for continuous monitoring of network traffic. Incoming and outgoing packets are captured from the network interface. Traffic data is collected without interrupting normal network operations. Relevant traffic attributes are forwarded for further analysis. This module serves as the primary data acquisition layer of the system.

Detection and Response Engine:
In this phase, captured traffic is analyzed using machine learning techniques. Behavioral features are extracted and classified as benign or malicious. Supervised learning models perform real-time threat detection. Upon detection, automated mitigation actions are triggered. This phase integrates detection and response within a single processing unit. The visualization and monitoring layer provides an administrative dashboard that displays threat statistics, system logs, and alert history. This interface enables administrators to monitor system performance, review detected threats, and analyze historical data for further security assessment.

Network Logs Database:
This phase stores network traffic records and detected threat information. Logs include timestamps, traffic features, and detection outcomes. Stored data supports forensic analysis and system evaluation. The database enables historical trend analysis and

© DEC 2025 | IRE Journals | Volume 9 Issue 6 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I6-1713209

reporting. Log retention facilitates model retraining and performance assessment.

Continuous Monitoring and Feedback:
This phase ensures continuous system operation and performance improvement. Logged data is utilized for system auditing and optimization. Detection results are fed back to the monitoring dashboard. System behavior is evaluated for accuracy and reliability. This phase supports scalability and long-term deployment.

IV. IMPLEMENTATION

The project implements an AI-based cybersecurity system for real-time network monitoring and threat detection. Machine learning algorithms identify malicious activities and trigger automated responses. Alerts and dashboards support effective security management

- Layer 1: Problem and Design layer

Problem Identification: The increasing inability of traditional rule-based security systems to detect evolving cyber threats was identified as the core problem. Existing limitations such as delayed response and manual dependency were analyzed

Requirement Analysis: Functional requirements such as real-time detection, automated response, and alerting were defined. Non-functional requirements including scalability, accuracy, and reliability were also considered

System Architecture Design: A layered architecture was designed to integrate traffic monitoring, machine learning detection, automated mitigation, and administrative visualization. Proper data flow between system components was planned.

- Layer 2: Data Acquisition and Processing layer

Network Traffic Data Collection: Real-time network traffic data was collected from the monitored environment. An attacker simulation module was used to generate malicious traffic for effective training and evaluation.

Data Preprocessing and Cleaning: Collected traffic data was cleaned to remove noise and irrelevant information. Normalization and feature scaling were applied to ensure data consistency.

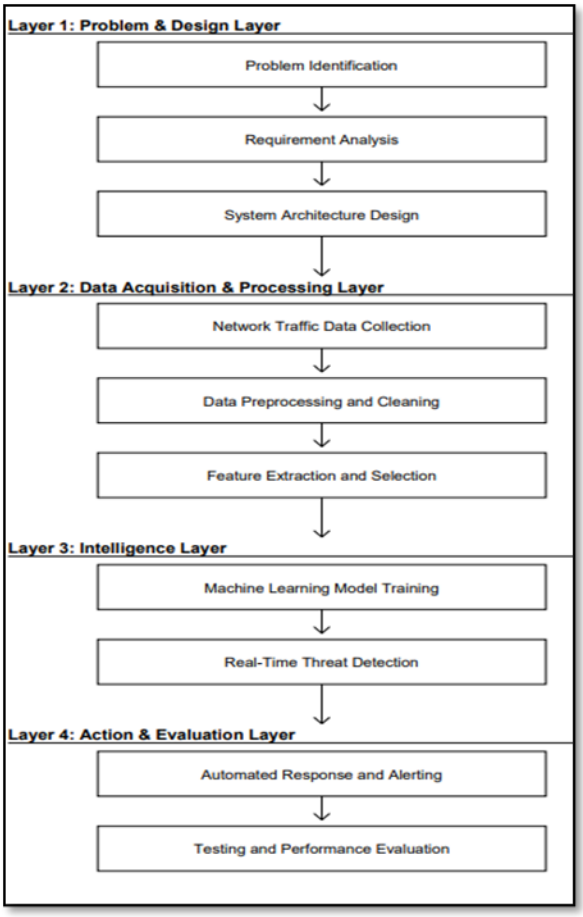


Fig 2: Layers of Implementation

Feature Extraction and Selection: Relevant network features such as packet size, protocol behavior, and traffic frequency were extracted. Feature selection was performed to improve detection efficiency.

- Layer 3: Intelligence layer

Machine Learning Model Training: Supervised learning algorithms, namely Random Forest and K-Nearest Neighbors, were trained using labeled datasets. Model parameters were optimized for better accuracy.

Real-Time Threat Detection: The trained models were deployed to analyze live network traffic. Each

© DEC 2025 | IRE Journals | Volume 9 Issue 6 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I6-1713209

traffic instance was classified as normal or malicious in real time.

- Layer 4: Action and Evaluation layer

Automated Response and Alerting: Upon detecting malicious activity, automated actions such as firewall recovery and traffic blocking were triggered. Real-time alerts were sent to administrators.

Testing and Evaluation: The system was tested under various attack scenarios. Performance metrics such as detection accuracy and response time were evaluated and optimized.

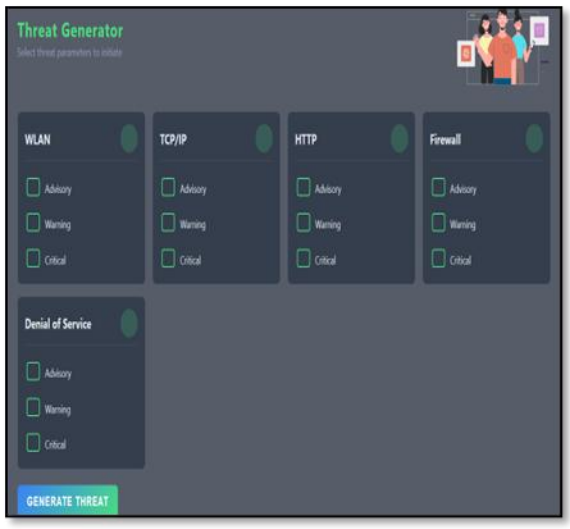
V. RESULT

This section presents representative screenshots of the implemented system to illustrate key functional components and system behavior. The figures demonstrate the interaction between users, the attacker simulation environment, the threat detection module, and the administrative monitoring interface.

A. User Authentication Interface

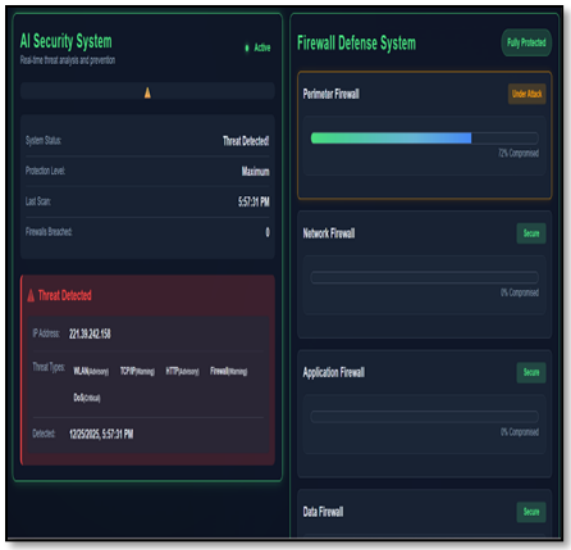
This figure illustrates the secure login interface used for system access. Authentication ensures that only authorized users and administrators can interact with the monitoring and response modules.

B. Attacker Simulation Module



This screenshot shows the attacker simulation interface, which is used to generate controlled cyberattack scenarios. The module enables testing of the system's detection capability under realistic attack conditions.

C. Real-Time Network Traffic Monitoring Dashboard



This figure displays the administrative dashboard that visualizes real-time network traffic statistics. It provides insights into traffic behavior, detected anomalies, and system status.

© DEC 2025 | IRE Journals | Volume 9 Issue 6 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I6-1713209

D. Machine Learning–Based Threat Detection Output

This screenshot presents the classification results generated by the machine learning detection engine. Network traffic is labeled as normal or malicious based on learned behavioral patterns.

E. Alert Notification Interface

This figure shows the alert notification generated when malicious activity is detected. Real-time alerts are sent to administrators to ensure immediate awareness and timely response.

VI. CONCLUSION

This research presented an AI-powered cybersecurity threat monitoring and response system designed to address the limitations of traditional rule-based security mechanisms. By integrating supervised machine learning techniques with real-time network monitoring, the proposed system enables accurate detection of malicious activities while reducing dependency on manual intervention. The use of Random Forest and K-Nearest Neighbors algorithms allows the system to effectively analyze network behavior and identify both known and evolving cyber threats.

The incorporation of an attacker simulation module enhances system evaluation by generating realistic attack scenarios, while the automated response mechanism ensures rapid mitigation through firewall recovery and traffic blocking. Real-time alerting and administrative visualization further improve situational awareness and support effective security management. Experimental observations indicate that the proposed approach improves detection accuracy, reduces response time, and enhances overall network resilience

REFERENCES

[1] S. Axelsson, “Intrusion detection systems: A survey and taxonomy,” Technical Report 99-15, Chalmers University of Technology, 2000.

[2] L. Breiman, “Random forests,” Machine Learning, vol. 45, no. 1, pp. 5–32, 2001.

[3] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, “A detailed analysis of the KDD CUP 99 data set,” in Proc. IEEE Symposium on Computational Intelligence for Security and Defense Applications, 2009, pp. 1–6.

[4] W. Lee and S. J. Stolfo, “A framework for constructing features and models for intrusion detection systems,” ACM Transactions on Information and System Security, vol. 3, no. 4, pp. 227–261, 2000

[5] J. Zhang, M. Zulkernine, and A. Haque, “Random-forest-based network intrusion detection systems,” IEEE Transactions on Systems, Man, and Cybernetics, Part C, vol. 38, no. 5, pp. 649– 659, 2008

[6] I. H. Witten, E. Frank, and M. A. Hall, Data Mining: Practical Machine Learning Tools and Techniques, 3rd ed., Morgan Kaufmann, 2011.

[7] A. L. Buczak and E. Guven, “A survey of data mining and machine learning methods for cyber security intrusion detection,” IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.

[8] M. Ring, D. Landes, and A. Hotho, “Detection of slow port scans in flow-based network traffic,” PLoS ONE, vol. 13, no. 9, 2018.

[9] N. Moustafa and J. Slay, “UNSW-NB15: A comprehensive data set for network intrusion detection systems,” in Proc. Military Communications and Information Systems Conference, 2015.

[10] S. Garcia, M. Grill, J. Stiborek, and A. Zunino, “An empirical comparison of botnet detection methods,” Computers & Security, vol. 45, pp. 100–123, 2014.