iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: XII Month of publication: December 2025

DOI: https://doi.org/10.22214/ijraset.2025.76543

AI-Powered Intrusion Detection System

Dr. Radha B. K.[1], Rahul[2], Revanasiddappa[3], Rohit[4]
Department of Computer Science and Engineering, PDA College of Engineering, Kalaburagi, Karnataka, India

Abstract: With the rapid expansion of computer networks and internet-based services, ensuring network security has become a critical challenge. Commonly adopted network security measures, such as firewalls and signature-oriented intrusion detection systems, play a key role in defending against known threats, making them ineffective against evolving and previously unseen attacks. This paper presents an AI-powered Network Intrusion Detection System designed to enhance real-time threat detection in modern network environments.

The proposed system integrates live packet monitoring using Scapy, detection of SYN flood attacks, and anomaly detection through the Kitsune ensemble autoencoder framework. The system is evaluated in a simulated environment using SYN flood and ICMP flood attacks. Experimental observations demonstrate improved detection accuracy, reduced false alerts, and efficient real-time performance. The results indicate that the proposed approach provides a practical and adaptive solution for securing contemporary networks.

Keywords: Network Intrusion Detection System, Cybersecurity, Machine Learning, Autoencoders, Anomaly Detection, SYN Flood, ICMP Flood

I. INTRODUCTION

The widespread adoption of internet-connected devices, cloud computing, and online services has significantly increased the complexity of modern network infrastructures. While these advancements improve accessibility and efficiency, they also introduce new security vulnerabilities. Cyberattacks such as denial-of-service, packet flooding, and unauthorized access attempts have become more frequent and sophisticated. Traditional network security solutions mainly rely on firewalls and signature-based intrusion detection systems. Firewalls enforce access control policies but are unable to detect malicious behaviour hidden within legitimate traffic. Signature-based intrusion detection systems compare traffic against known attack patterns, which limits their ability to detect zero-day attacks and novel threat variations. To overcome these limitations, artificial intelligence and machine learning techniques are increasingly being integrated into intrusion detection systems. These techniques focus on learning normal network behaviour and identifying deviations that may indicate malicious activity. This paper proposes an AI-based intrusion detection system that combines real-time packet analysis with ensemble autoencoder-based anomaly detection to provide accurate and adaptive network security.

II. PROBLEM STATEMENT

Existing intrusion detection systems face significant challenges in detecting modern cyber threats. Signature-based approaches fail to identify unknown attacks, while traditional anomaly-based systems often generate a large number of false-positive alerts. Additionally, many solutions lack real-time adaptability and struggle to perform efficiently in dynamic network environments. Therefore, there is a need for an intelligent intrusion detection system that can accurately detect both known and unknown attacks while maintaining low false-positive rates and real-time performance.

III. OBJECTIVES

The main objectives of this project are:

1) To design an AI-based network intrusion detection system for real-time monitoring.
2) To capture and analyze live network traffic efficiently.
3) To detect SYN flood attacks using threshold-based techniques.
4) To identify ICMP flood attacks through behavioral anomaly detection.
5) To apply the Kitsune ensemble autoencoder for unsupervised anomaly detection.
6) To evaluate system effectiveness in a simulated attack environment.

IV. RELATED WORK

Intrusion detection systems are generally categorized into signature-based and anomaly-based approaches. Signature-based systems are effective for detecting known attacks but are unable to recognize new or modified attack patterns. Anomaly-based systems attempt to detect deviations from normal behaviour, but they often suffer from high false-positive rates.

V. METHODOLOGY

The proposed system captures live network packets using the Scapy library, enabling detailed inspection of packet headers and traffic patterns. Network features are extracted using the Afterimage framework, which performs incremental statistical analysis over multiple time windows to capture both short-term and long-term traffic behaviour.

SYN flood attacks are detected using threshold-based analysis of TCP connection requests. ICMP flood attacks are identified by monitoring abnormal ICMP packet rates and deviations from baseline behaviour. For anomaly detection, the Kitsune ensemble autoencoder framework is employed. This framework consists of multiple small autoencoders, each trained on correlated subsets of traffic features. Reconstruction errors from these autoencoders are combined to produce an overall anomaly score used for intrusion detection.

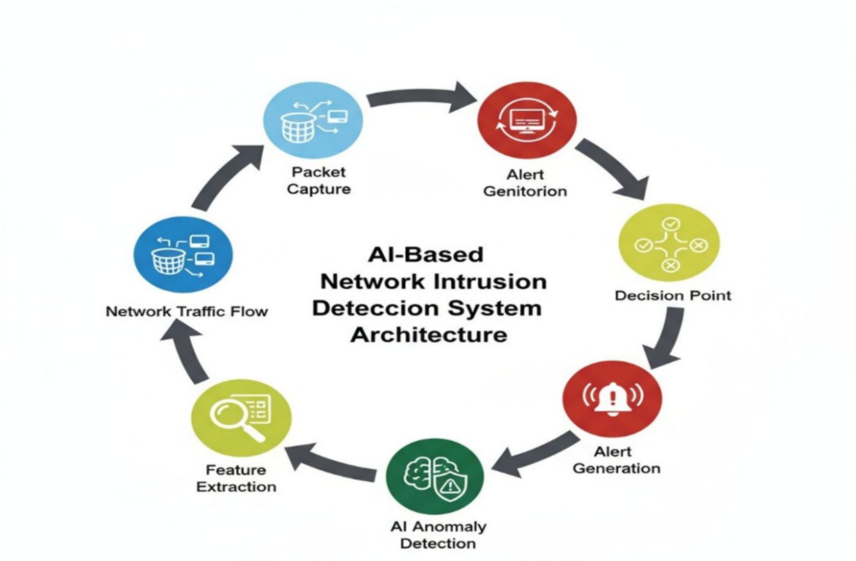

Fig. 1 System Architecture of IDS

VI. EXPERIMENTAL SETUP

The system is implemented using Python in a Linux-based environment. Live traffic is captured from the network interface, and attack scenarios are simulated using SYN flood and ICMP flood traffic generation tools. Normal traffic is generated to establish baseline behaviour for anomaly detection.

The system operates in real time, continuously monitoring traffic and generating alerts when suspicious behaviour is detected. Performance is evaluated based on detection accuracy, alert reliability, processing latency, and system responsiveness.

VII. RESULT AND ANALYSIS

Experimental observations show that the proposed intrusion detection system effectively identifies both SYN flood and ICMP flood attacks with high accuracy. The ensemble autoencoder-based anomaly detection significantly reduces false-positive alerts compared to traditional anomaly detection approaches.

The system demonstrates efficient real-time performance with low processing latency, making it suitable for deployment in practical network environments. The detection results confirm that combining rule-based detection with unsupervised learning improves overall system reliability and adaptability.

Table 1. Network Throughput Performance Under Different Traffic Scenarios

Attack Scenario	Packets/sec	Throughput without NIDS (Mbps)	Throughput with NIDS (Mbps)	Overhead (%)	Efficiency
Port Scan	500	85.2	83.8	1.64	High
SYN Flood	2000	78.5	62.3	20.63	Medium
ICMP Flood	2500	79.8	65.4	18.05	Medium
Normal Traffic	1000	86.0	85.5	0.58	High

The above table presents the network throughput analysis under normal traffic and various attack conditions. It can be observed that the throughput slightly decreases when the NIDS is enabled due to real-time packet inspection. However, the system maintains acceptable throughput levels even during high-rate attacks such as SYN flood and ICMP flood, indicating efficient packet processing with manageable overhead.

Table 2. Packet Delivery Ratio (PDR) and Detection Accuracy Analysis

Attack Scenario	Total Packets	Packets Delivered	PDR(%)	Lost Packets	Detection Accuracy
Port Scan	5000	4925	98.50	75	97.8%
SYN Flood	10000	9920	99.20	80	99.1%
ICMP Flood	12000	11868	98.90	132	99.0%
Normal Traffic	8000	7992	99.90	8	N/A

The above table shows the packet delivery ratio and detection accuracy for different attack scenarios. The results indicate a high packet delivery ratio for both normal and attack traffic, demonstrating that the proposed NIDS does not significantly disrupt legitimate communication. High detection accuracy for SYN flood and ICMP flood attacks confirms the effectiveness of the anomaly detection mechanism.

Table 3. End-to-End Delay Performance for Various Attack Types

Attack Scenario	Min Delay (ms)	Max Delay (ms)	Avg Delay (ms)	Std Dev (ms)	Jitter (ms)
Port Scan	0.42	2.15	1.08	0.31	1.73
SYN Flood	2.10	16.50	9.15	3.45	14.40
ICMP Flood	1.95	14.80	7.65	2.95	12.85
Normal Traffic	0.28	1.25	0.62	0.18	0.97

The above table tells us that the end-to-end delay characteristics observed during various attack scenarios. Compared to normal traffic, attack conditions introduce higher delays due to increased packet processing and congestion. Despite this, the average delay remains within acceptable limits, making the proposed system suitable for real-time network monitoring.

Table 4. Attack Detection Capability and Severity Classification

Attack Scenario	Layer	Network Impact	Severity	Detected By IDS
Port Scan	Reconnaissance (TCP)	Identifies open ports	Medium	Yes
SYN Flood	DoS (TCP)	Exhausts connection table	High	Yes
ICMP Flood	DoS (ICMP)	Network congestion	High	Yes
Normal Traffic	Benign	Legitimate communication	None	Not Flagged

The above table summarizes the types of network attacks, their impact, severity levels, and detection status by the proposed IDS. The system successfully detects reconnaissance, denial-of-service, and man-in-the-middle attacks while correctly ignoring benign traffic. This demonstrates the system's ability to distinguish between malicious and legitimate network behaviour.

VIII. CONCLUSION

This paper presents an AI-powered network intrusion detection system that enhances security through intelligent anomaly detection and real-time traffic monitoring. By integrating SYN flood detection with ensemble autoencoder-based learning and ICMP flood analysis, the proposed system effectively addresses the limitations of traditional intrusion detection methods. The experimental results demonstrate improved detection accuracy, reduced false alerts, and efficient real-time performance. The proposed approach offers a scalable and practical solution for securing modern network infrastructures.

REFERENCES

[1] 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), pp. 1–15, 2018.

[2] M. Roesch, "Snort: Lightweight Intrusion Detection for Networks," Proceedings of the 13th USENIX Conference on System Administration, pp. 229–238, 1999.

[3] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection," IEEE Symposium on Security and Privacy, pp. 305–316, 2010.

[4] A. Lazarevic, L. Ertoz, V. Kumar, A. Ozgur, and J. Srivastava, "A Comparative Study of Anomaly Detection Schemes in Network Intrusion Detection," Proceedings of the SIAM International Conference on Data Mining, pp. 25–36, 2003.

[5] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning, MIT Press, Cambridge, MA, USA, 2016.

[6] Y. Bengio, A. Courville, and P. Vincent, "Representation Learning: A Review and New Perspectives," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 35, no. 8, pp. 1798–1828, 2013.

[7] F. Chollet, Deep Learning with Python, Manning Publications, New York, USA, 2017.

[8] Scapy Development Team, "Scapy: Interactive Packet Manipulation Tool," Official Scapy Documentation, 2023. [Online]. Available: https://scapy.net

[9] R. Doshi, N. Apthorpe, and N. Feamster, "Machine Learning DDoS Detection for Consumer Internet of Things Devices," IEEE Security and Privacy Workshops, pp. 29–35, 2018.

[10] H. Hindy, E. Bayne, M. Bures, R. Atkinson, C. Tachtatzis, and X. Bellekens, "A Taxonomy of Network Threats and the Effect of Dataset Characteristics on Intrusion Detection Systems," IEEE Access, vol. 8, pp. 104650–104675, 2020.

[11] A. 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.

[12] L. Dhanabal and S. P. Shantharajah, "A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms," International Journal of Advanced Research in Computer and Communication Engineering, vol. 4, no. 6, pp. 446–452, 2015.

[13] Y. Liu, Y. Li, and X. Chen, "Adversarial Machine Learning: Security Threats and Defense Mechanisms," Journal of Information Security and Applications, vol. 58, pp. 102–115, 2021.

[14] R. Shokri and V. Shmatikov, "Privacy-Preserving Deep Learning," Proceedings of the ACM Conference on Computer and Communications Security (CCS), pp. 1310–1321, 2015.