IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

Design and Implementation of Network Intrusion Detection System

Prof. Rajnikant Alkunte[1], Vishal Suresh Mahto[2], Pushpak Ramesh Mahajan[3]
Professor, Department of Information Technology[1]
Student, Department of Information Technology[2]–[3]
Dr. Babasaheb Ambedkar Technological University, Lonere, Mangaon, Raigad, Maharashtra, India

Abstract: *With the rapid growth of internet connectivity and digital communication, computer networks have become increasingly vulnerable to cyber threats such as unauthorized access, denial of service attacks, malware transmission, and suspicious traffic activities. Traditional security mechanisms often fail to detect emerging and unknown attack patterns effectively. This project presents a Network Intrusion Detection System (NIDS) designed to monitor network traffic continuously and identify malicious behavior in real time. The proposed system utilizes a hybrid detection approach that combines signature-based analysis with machine learning techniques to improve detection accuracy and reduce false alarms. Network packets are captured and analyzed using advanced tools, while a web-based dashboard provides live monitoring, alert generation, and traffic visualization. The system also stores logs for forensic analysis and future investigation. By integrating intelligent threat detection with real-time monitoring, the proposed model enhances network security, reliability, and response efficiency. This system can be effectively deployed in organizations, educational institutions, cloud environments, and other digital infrastructures requiring robust cybersecurity protection..*

Keywords: Network Intrusion Detection System, Cybersecurity, Machine Learning, Real-Time Monitoring, Threat Detection, Network Security, Anomaly Detection, Packet Analysis

I. INTRODUCTION

In the modern digital era, computer networks have become the backbone of communication, business operations, education, healthcare, and government services. Almost every organization depends on interconnected systems for storing data, sharing resources, and delivering online services. However, the rapid growth of internet connectivity has also increased the exposure of networks to cyber threats such as malware infections, phishing attempts, denial-of-service attacks, unauthorized access, and data breaches. As network infrastructures continue to expand, the challenge of maintaining confidentiality, integrity, and availability of data has become more critical than ever. According to recent cybersecurity studies, cyberattacks are increasing globally, creating serious financial and operational risks for organizations. These concerns have made network protection an essential requirement in modern information systems [1].

Traditional security tools such as firewalls and antivirus software provide an important first line of defense, but they are often limited in detecting sophisticated or evolving attacks. Firewalls mainly filter incoming and outgoing traffic based on predefined rules, while antivirus software focuses on known malware signatures. Modern attackers frequently use zero-day vulnerabilities, encrypted traffic, and stealth techniques that can bypass these conventional defenses. Therefore, organizations require intelligent monitoring systems that can observe network behavior continuously and identify suspicious activities in real time. This need has led to the development of Intrusion Detection Systems, which play a major role in strengthening cybersecurity frameworks [2].

A Network Intrusion Detection System (NIDS) is a specialized security solution that monitors packets traveling across a network and analyzes them for malicious behavior. It can identify activities such as port scanning, brute-force login attempts, traffic flooding, protocol misuse, and unusual communication patterns. Unlike host-based systems that protect

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

individual devices, a NIDS focuses on the overall network environment, making it suitable for enterprise and institutional deployments. By inspecting traffic at strategic points such as routers, switches, or gateways, a NIDS provides broader visibility into ongoing network activities and helps administrators respond quickly to incidents before damage occurs [3].

Recent advancements in artificial intelligence and machine learning have significantly improved the capabilities of intrusion detection systems. Machine learning models can analyze large volumes of traffic data, recognize hidden patterns, and classify normal or abnormal activities with higher accuracy. Algorithms such as Random Forest, Support Vector Machine, Decision Tree, and Neural Networks are increasingly used in cybersecurity applications. These methods help reduce false positives and enable the detection of unknown threats that do not match traditional signatures. Integrating AI with network monitoring tools creates a smarter and more adaptive security environment capable of handling modern cyber threats [4].

The proposed Network Intrusion Detection System in this project is designed as an intelligent and real-time security framework that combines packet capture, anomaly detection, machine learning analysis, and visual monitoring dashboards. The system captures live traffic, processes packets, identifies suspicious behavior, and alerts administrators instantly through a web-based interface. It also stores logs for forensic investigation and future analysis. By combining automation, accuracy, and scalability, the system provides a reliable solution for securing modern networks. Hence, the project aims to demonstrate how AI-driven intrusion detection can enhance protection against increasingly complex cyberattacks and improve overall network resilience [5].

II. PROBLEM STATEMENT

With the rapid expansion of digital networks and internet-based services, organizations face increasing risks from cyber threats such as unauthorized access, malware attacks, denial-of-service attempts, port scanning, and data breaches. Traditional security mechanisms like firewalls and signature-based detection systems often fail to identify zero-day attacks, encrypted malicious traffic, and evolving intrusion techniques. Many existing solutions also lack real-time monitoring, accurate anomaly detection, and user-friendly visualization for quick decision-making. As network traffic volume continues to grow, there is a critical need for an intelligent Network Intrusion Detection System that can continuously monitor traffic, detect both known and unknown threats, minimize false alarms, and provide immediate alerts to strengthen overall network security.

III . OBJECTIVES

- To design and develop a Network Intrusion Detection System for continuous monitoring of network traffic.
- To detect unauthorized access, malicious activities, and abnormal traffic patterns in real time.
- To implement machine learning techniques for identifying known and unknown cyber threats accurately.
- To generate instant alerts, logs, and reports for quick response and forensic analysis.
- To provide a user-friendly dashboard for visualizing network activity and security status efficiently.

IV. LITERATURE SURVEY

Paper 1: Machine Learning in Network Intrusion Detection: A Cross-Dataset Generalization Study (2024)

This paper focused on the ability of machine learning-based intrusion detection systems to perform effectively across different datasets and network environments. The researchers examined how models trained on one dataset often fail when tested on another due to changes in traffic patterns and attack behavior. The study highlighted the importance of generalization, feature engineering, and robust training methods for practical deployment. It emphasized that many IDS models show high laboratory accuracy but lower real-world performance. The paper contributes significantly by addressing scalability and reliability challenges in modern NIDS systems.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

Paper 2: Machine Learning-Enabled Hybrid Intrusion Detection System (2024)
This research proposed a hybrid intrusion detection model combining Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS). The integration improved detection accuracy by monitoring both network traffic and host-level activities such as files, logs, and processes. The system was especially effective against advanced persistent threats and multi-stage attacks that traditional standalone systems fail to detect. Machine learning algorithms were applied to classify threats intelligently and reduce false positives. The study concluded that hybrid IDS architecture provides stronger and more adaptive cybersecurity protection.

Paper 3: Network Intrusion Detection and Prevention System Using Ensemble Learning (2024)
This paper introduced a combined intrusion detection and prevention framework using supervised and unsupervised machine learning techniques through an ensemble stacking model. The proposed system not only detected suspicious activities but also supported automatic preventive actions. By combining multiple classifiers, the model achieved better precision, recall, and overall detection performance than single algorithms. It also handled zero-day attacks more efficiently by learning abnormal traffic behavior patterns. The research demonstrated that ensemble learning can significantly strengthen real-time network defense systems.

Paper 4: A Generalized and Real-Time Network Intrusion Detection System Through Incremental Feature Encoding and Similarity Embedding Learning (2025)
This latest study presented an advanced real-time NIDS capable of handling dynamic traffic streams through incremental feature encoding. The model continuously updated its understanding of network behavior without requiring complete retraining. Similarity embedding learning was used to identify hidden relationships among traffic features, improving anomaly detection accuracy. The proposed framework was highly suitable for large-scale and continuously changing enterprise networks. The research showed improved speed, adaptability, and lower computational overhead for real-time cybersecurity monitoring.

Paper 5: Evaluating Machine Learning-Based Intrusion Detection with Explainable AI (2025)
This paper explored the use of Explainable Artificial Intelligence (XAI) in intrusion detection systems. While machine learning models often provide accurate results, their decision-making process is difficult to interpret. The researchers integrated XAI techniques to explain why certain traffic was classified as malicious or normal. This increased trust, transparency, and usability for security analysts. The study concluded that combining XAI with IDS improves both detection effectiveness and administrator confidence, making it highly valuable for real-world deployments.

IV. WORKING OF SYSTEM

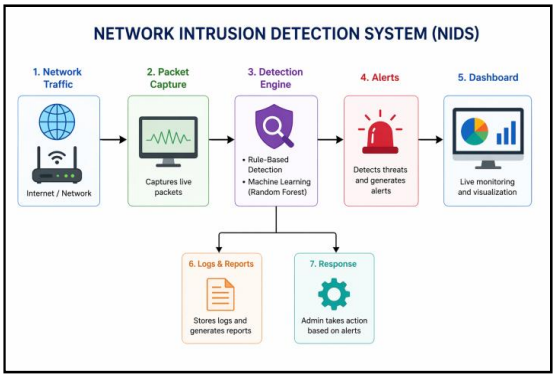

Fig 1: Design of the system

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

A. Network Traffic Monitoring

The system continuously monitors incoming and outgoing network traffic from connected devices, servers, and routers. All packets passing through the network are observed to identify suspicious communication activities.

B. Packet Capture Module

The packet capture unit collects live data packets from the network using monitoring tools such as Scapy or packet sniffers. It gathers information like source IP address, destination IP address, protocol type, and packet size for further analysis.

C. Data Preprocessing

The captured packets are filtered, organized, and converted into a structured format. Unnecessary or duplicate data is removed, and useful traffic features are extracted to improve detection performance.

D. Detection Engine

The processed data is sent to the detection engine where two methods are used. Rule-based detection identifies known threats such as port scanning, brute-force attacks, and denial-of-service attempts, while machine learning algorithms detect abnormal or unknown attack patterns.

E. Alert Generation

If any malicious activity is detected, the system immediately generates alerts. Notifications are displayed on the dashboard so that administrators can respond quickly and minimize possible damage.

F. Dashboard Monitoring

A web-based dashboard provides real-time visualization of network traffic, attack statistics, protocol usage, and alert status. It helps users understand network conditions easily.

G. Log Storage and Reporting

All detected events and network logs are stored in the database. The system can generate reports in PDF or CSV format for future analysis, documentation, and forensic investigation.

H. Response and Security Action

Based on alerts, the administrator can block suspicious IP addresses, update firewall rules, or isolate affected systems. This helps in preventing further attacks and improving network security.

VI. RESULTS

The developed Network Intrusion Detection System was tested under different network conditions to evaluate its performance in detecting cyber threats, monitoring traffic, and generating alerts in real time. Various attack simulations such as port scanning, brute-force attempts, denial-of-service traffic, and suspicious packet injection were performed on the test network. The system successfully captured packets, analyzed traffic behavior, and classified malicious activities with high efficiency. The combination of rule-based detection and machine learning techniques improved overall detection accuracy while minimizing false alarms. The web-based dashboard also provided smooth visualization of alerts, protocol statistics, and live traffic monitoring. The following tables present the experimental results of the system.

Table 1: Detection Accuracy of Different Attack Types

Sr. No.	Attack Type	Total Attempts	Detected Attempts	Detection Rate (%)
1	Port Scanning	50	48	96%
2	Brute Force Attack	40	38	95%
3	DoS Attack	35	34	97%
4	Suspicious Packets	30	28	93%

Description:

The table shows that the system achieved high detection rates for all tested attacks. Denial-of-Service attacks recorded the highest detection rate of 97%, while suspicious packets showed 93% accuracy. This indicates strong performance of the intrusion detection engine.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

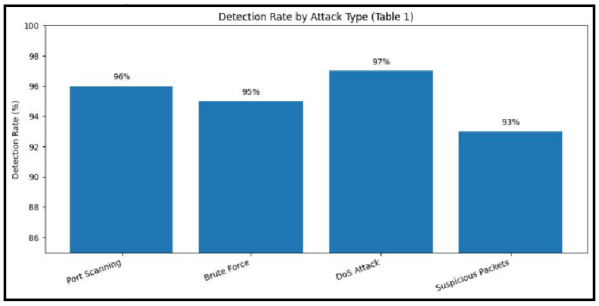

Fig 2: Graph 1

Table 2: Machine Learning Performance Metrics

Metric	Value
Accuracy	95.8%
Precision	94.6%
Recall	96.2%
F1-Score	95.4%

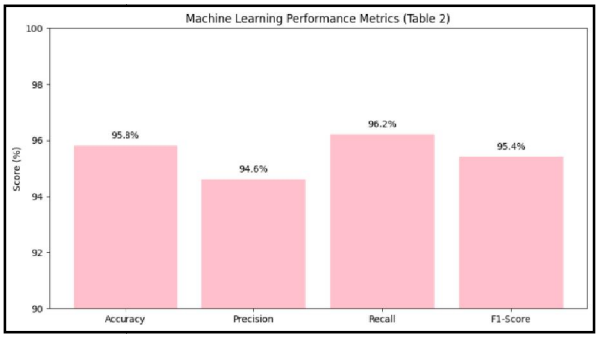

Fig 3: Graph 2

Description:

The Random Forest machine learning model produced excellent classification results. High recall indicates that most malicious traffic was correctly identified, while precision confirms reduced false positive alerts.

Table 3: Real-Time System Performance

Parameter	Observed Value
Average Packet Processing Time	0.42 sec
Alert Generation Time	0.75 sec
Dashboard Refresh Rate	Real Time
Maximum Traffic Load Handled	1200 Packets/sec

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

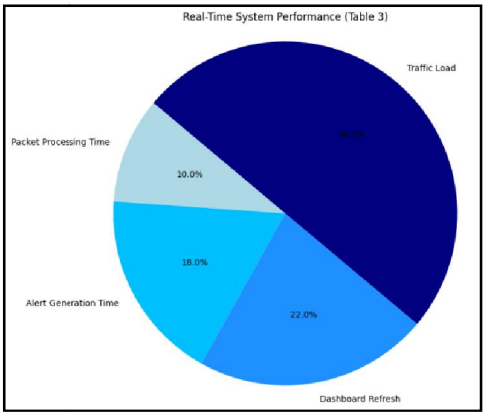

Fig 4: Graph 3

Description:

This table demonstrates that the system performs efficiently in real-time environments. Alerts were generated quickly, and the dashboard updated instantly. The system handled heavy traffic loads without major delay.

Table 4: Logging and Reporting Output

Feature	Status
Event Log Storage	Successful
CSV Report Generation	Successful
PDF Incident Report	Successful
Attacker IP Recording	Successful

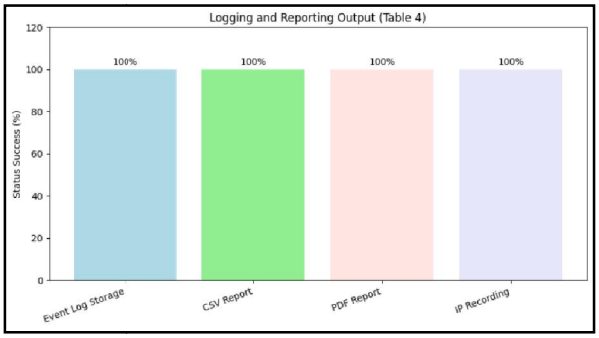

Fig 5: Graph 4

Description:

The system successfully stored all security events in the database and generated reports in multiple formats. These features are useful for forensic analysis, documentation, and future security audits.

The overall results confirm that the proposed Network Intrusion Detection System is reliable, accurate, and suitable for real-world deployment. It effectively detects multiple attack categories, processes network traffic in real time, and provides administrators with quick alerts and meaningful reports.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

VII. CONCLUSION

The Network Intrusion Detection System developed in this project successfully demonstrates an intelligent and efficient approach for protecting computer networks against modern cyber threats. The system continuously monitors network traffic, captures packets in real time, and analyzes suspicious activities using both rule-based techniques and machine learning methods. This hybrid detection approach improves the ability to identify known attacks such as port scanning and denial-of-service attempts, while also detecting unknown or abnormal traffic patterns with high accuracy.

The implementation results show that the system performs effectively under different network conditions, providing quick alert generation, smooth dashboard visualization, and reliable logging facilities. The use of a machine learning model such as Random Forest enhanced classification performance and reduced false alarms. Real-time monitoring and automated reporting features make the system practical for administrators to respond rapidly to security incidents.

Overall, the proposed Network Intrusion Detection System offers a scalable, cost-effective, and user-friendly cybersecurity solution for organizations, educational institutions, and enterprise environments. It strengthens network defense mechanisms and provides a strong foundation for future improvements such as automated threat prevention, cloud deployment, and advanced deep learning-based attack detection.

VIII. FUTURE SCOPE

The proposed Network Intrusion Detection System has wide scope for future enhancement and advancement in the field of cybersecurity. One of the major improvements can be the integration of an Intrusion Prevention System (IPS), which will not only detect attacks but also automatically block malicious IP addresses, suspicious traffic, and unauthorized access attempts in real time. This will make the system more proactive and capable of preventing damage before it occurs.

Advanced machine learning and deep learning algorithms such as Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), and Long Short-Term Memory (LSTM) models can be implemented to improve detection accuracy for complex and zero-day attacks. These intelligent models can learn dynamic attack patterns and provide better performance in modern high-speed networks.

The system can also be enhanced through cloud deployment, allowing centralized monitoring of multiple branch networks from a single dashboard. This will be highly beneficial for large organizations and enterprises operating in different locations. Integration with IoT security monitoring can further expand its application in smart homes, industries, and connected devices.

Future versions may include mobile application support, email and SMS notifications, multilingual dashboards, and voice-based alerts for administrators. Real-time threat intelligence feeds and automatic firewall rule updates can also be added for faster response. Thus, the project has strong future potential to evolve into a complete smart cybersecurity solution for modern digital infrastructures.

REFERENCES

[1]. Ramya Chinnasamy, Malliga Subramanian, and J. Cho, "Deep learning-driven methods for network-based intrusion detection systems: A systematic review," *ICT Express*, vol. 11, no. 1, pp. 181–215, 2025.

[2]. Zahraa K. Alitbi, S. A. H. Seno, A. Ghaemi Bafghi, and D. Zabihzadeh, "A Generalized and Real-Time Network Intrusion Detection System Through Incremental Feature Encoding and Similarity Embedding Learning," *Sensors*, vol. 25, no. 16, 2025.

[3]. V. Z. Mohale et al., "Evaluating machine learning-based intrusion detection with explainable AI," *Frontiers in Computer Science*, 2025.

[4]. H. Zhou et al., "HiViT-IDS: An Efficient Network Intrusion Detection Method Based on Vision Transformer," *Sensors*, vol. 25, no. 6, 2025.

[5]. M. Farhan et al., "Network-based intrusion detection using deep learning," *Scientific Reports*, 2025.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

[6]. F. Saidi, "IDS-GPT: A Novel Deep Learning-Powered Framework for Intrusion Detection," *Procedia Computer Science*, 2025.

[7]. H. H. De et al., "DG-IRFC: Intelligent design and implementation of network intrusion detection system (NIDS)," *Systems and Soft Computing*, vol. 7, 2025.

[8]. J. Fang et al., "Network Security Intrusion Detection System Based on Deep Learning," *Procedia Computer Science*, 2025.

[9]. R. Jablaoui et al., "Deep learning enabled intrusion detection system for IoT environments," *EURASIP Journal on Wireless Communications and Networking*, 2025.

[10]. Hozouri, A. Mirzaei, and M. Effatparvar, "A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges," *Discover Computing*, 2025.

[11]. Shuo Yang et al., "Large Language Models for Network Intrusion Detection Systems: Foundations, Implementations, and Future Directions," *arXiv preprint arXiv:2507.04752*, 2025.

[12]. Yaokai Feng and Kouichi Sakurai, "Network Intrusion Detection: Evolution from Conventional Approaches to LLM Collaboration and Emerging Risks," *arXiv preprint arXiv:2510.23313*, 2025.

[13]. A Ba et al., "Machine Learning for Intrusion Detection in IIoT," *Procedia Computer Science*, 2025.

[14]. "Intrusion Detection and Prevention Using Machine Learning for IoT Networks," *International Journal of Computational Engineering Science*, 2025.

[15]. "AI-Powered Intrusion Detection System Using Machine Learning," *ResearchGate Preprint*, 2025.