IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Intrusion Detection in Network Security

Harpreet Kaur Gill , Komalpreet Kaur

Student, Global Group of Institutes, Amritsar, Punjab, India

Assistant Professor, Department of Computer Application, Global Group of Institutes, Amritsar, Punjab, India

Abstract

Intrusion Detection Systems (IDS) are essential elements in detecting and responding to security threats within computer systems and networks. [1].With the increasing complexity of cyber-attacks, traditional detection systems are no longer sufficient, leading to the adoption of machine learning and hybrid detection techniques [2].This paper presents an in-depth study of IDS, including detection methods, architecture, datasets, tools, experimental analysis, and future advancements [3].

Keywords

Network Security , IDS , Cyber Attacks , Machine Learning , Deep Learning , Anomaly Detection .

1. Introduction

The expansion of digital communication systems and cloud computing has significantly increased the attack surface for cybercriminals [1].Organizations face threats such as Distributed Denial of Service (DDoS), ransomware, phishing, and insider attacks [2].IDS provide a mechanism to monitor traffic and identify suspicious patterns in real time [3].Modern IDS systems incorporate artificial intelligence to enhance detection accuracy and reduce manual intervention [4].The importance of IDS has grown due to increasing reliance on online systems and sensitive data storage [5].

2. Literature Review

Earlier IDS models were based on rule-based systems that relied heavily on known attack signatures [1].Anomaly detection models introduced statistical methods to identify deviations from normal network behavior [2].Research indicates that machine learning models such as Decision Trees and Support Vector Machines significantly improve detection performance [3].
Deep learning approaches, including Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNNs) are capable of processing sequential data and identifying patterns over time extracting complex

features automatically [4].Recent literature emphasizes hybrid IDS models that combine multiple techniques for improved efficiency and reduced error rates [5].

3. Intrusion Detection Systems (IDS) Overview

IDS are designed to detect unauthorized access, misuse, or anomalies within a network system [1].They act as a second line of defense after firewalls and preventive systems [2].

Types of IDS

Network-Based IDS (NIDS):
Monitors packets across the entire network and identifies suspicious traffic patterns [3].

Host-Based IDS (HIDS):
Examines system logs, monitors file modifications, and observes operating system activities. [4].

Protocol-Based IDS (PIDS):
Monitors and analyzes communication protocols for anomalies [5].

Hybrid IDS:
Combines multiple IDS types to improve detection efficiency [6].

4. Detection Techniques

Signature-Based Detection

This method uses a database of known attack signatures to detect threats [1].
It is fast and accurate for known attacks but ineffective for unknown threats [2].

Anomaly-Based Detection

It builds a model of normal behavior and flags deviations as potential threats [3].
It can detect zero-day attacks but often generates false positives [4].

Specification-Based Detection

Defines normal system behavior manually and flags deviations [5].
It provides better accuracy than anomaly detection but requires expert knowledge [6].

Machine Learning-Based Detection

Uses supervised and unsupervised algorithms to classify network traffic [7].
Supervised learning depends on labeled data, whereas unsupervised learning works with unlabeled datasets hidden patterns [8].

Deep Learning-Based Detection

Applies neural networks to process large-scale network data efficiently [9].
These models can automatically learn features without manual intervention [10].

5. System Architecture / Methodology

The IDS architecture consists of multiple layers working together to detect intrusions [1].

Step 1: Data Collection
Network traffic is captured using packet sniffing tools such as Wireshark [2].

Step 2: Data Preprocessing
Noise removal, normalization, and handling missing values are performed [3].

Step 3: Feature Extraction & Selection
Important features such as IP address, protocol type, and packet size are selected [4].

Step 4: Model Training
Machine learning algorithms are trained using labeled datasets [5].

Step 5: Detection Engine
The trained model classifies traffic into normal or malicious categories [6].

Step 6: Alert Generation
Alerts are generated and sent to administrators for further action [7].

Step 7: Response Mechanism
The system may block IPs, terminate sessions, or log incidents [8].

6. Dataset and Tools Used

Datasets

- **KDD Cup 99** – Benchmark dataset widely used in IDS research [1].
- **NSL-KDD** – Improved version addressing KDD99 limitations [2].
- **CICIDS 2017** – Contains modern real-world attack scenarios [3].
- **UNSW-NB15** – Provides diverse attack categories with updated features [4].
- **BoT-IoT Dataset** – Designed for IoT-based intrusion detection [5].

Tools

- **Snort** – Signature-based IDS for real-time traffic analysis [6].
- **Suricata** – Multi-threaded IDS/IPS with high performance [7].
- **Wireshark** – Packet capture and analysis tool [8].
- **Bro (Zeek)** – Network analysis framework [9].
- **Python Libraries** – Scikit-learn, TensorFlow, Keras for ML models [10].

7. Experimental Results / Analysis

Experimental evaluation shows that Random Forest achieves accuracy above 95% on NSL-KDD datasets [1].Support Vector Machines perform well in binary classification tasks [2].Deep learning models such as LSTM show strong performance in time-series network data analysis [3].Hybrid IDS models outperform standalone models in both accuracy and detection rate [4]. False-positive rates remain a concern, especially in anomaly-based systems [5].

8. Comparison with Existing Systems

Traditional IDS are limited due to reliance on static rules and signatures [1].

Machine learning-based IDS provide adaptability and better detection of unknown threats [2].

Deep learning-based IDS improve performance but require high computational power [3].

Hybrid IDS systems offer the best balance between accuracy and efficiency [4].

9. Challenges and Limitations

Handling large volumes of network data in real time is a major challenge [1].False positives reduce the reliability of IDS systems [2].Lack of updated and realistic datasets affects model performance [3].High computational requirements limit deployment in resource-constrained environments [4].Attackers continuously evolve techniques to evade IDS detection [5].

10. Future Work

Future IDS systems will focus on real-time and adaptive detection mechanisms [1].Integration with cloud computing and IoT security will be essential [2].Artificial intelligence will play a major role in improving IDS efficiency [3].Blockchain technology may be used for secure logging and data integrity [4].Lightweight IDS models will be developed for edge devices and mobile systems [5].

11. Conclusion

Intrusion Detection Systems are essential for protecting network infrastructures from cyber threats [1].Traditional methods are no longer sufficient in detecting sophisticated attacks [2]. Machine learning and hybrid approaches significantly enhance detection accuracy and adaptability [3].Despite challenges, IDS continue to evolve with advancements in AI and data analytics [4].Future developments will focus on intelligent, automated, and real-time detection systems [5].

✓ References

1. https://indjst.org/articles/intrusion-detection-systems-tools-and-techniques-an-overview
2. https://www.ijraset.com/research-paper/intrusion-detection-system-comparative-analysis-of-supervised-and-unsupervised-techniques
3. https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0038-7
4. https://arxiv.org/abs/2506.02438
5. https://www.sciencedirect.com/science/article/pii/S0045790624006529
6. https://www.mdpi.com/2073-431X/14/3/87
7. https://link.springer.com/article/10.1007/s10489-021-02367-0
8. https://www.sciencedirect.com/science/article/pii/S1877050920316828
9. https://www.zeek.org/
10. https://scikit-learn.org/stable/