IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 5, Issue 1, January 2025

A Review on Machine Learning Framework for Detection of Intrusion

Nandan S[1], Mr. Pradeep Nayak[2], Amar B M[3], Manikanta[4], Karthik Madakari T P[5]

Students, Department of Information Science & Engineering[1,3,4,5]

Assistant Professor, Department of Information Science & Engineering[2]

Alva's Institute of Engineering and Technology, Mijar, Moodbidri, Karnataka, India

Abstract: *Intrusion Detection Systems (IDSs) are critical tools in the realm of cybersecurity, designed to detect and respond to unauthorized access, malicious activities, and potential threats within network or host environments. These systems monitor and analyze network traffic or system behavior, identifying patterns that may indicate security breaches. IDSs are classified into various types, including Network-based (NIDS), Host-based (HIDS), and Hybrid systems, each offering distinct advantages based on the nature of the monitored environment. Signature-based detection focuses on identifying known threats, while anomaly-based detection aims to detect unknown or novel attacks by analyzing deviations from normal system behavior. Despite their effectiveness, IDSs face challenges such as false positives, resource constraints, and the need for constant updates. The integration of IDSs with complementary tools, such as firewalls and Security Information and Event Management (SIEM) systems, enhances their capabilities. This abstract highlights the importance of IDSs in maintaining robust cybersecurity defenses, emphasizing the need for continuous adaptation and improvement to combat ever-evolving threats and safeguard organizational systems and data*

Keywords: Intrusion Detection Systems

I. INTRODUCTION

An Intrusion Detection System (IDS) is a critical cybersecurity tool designed to monitor and analyze network traffic or system activities to detect suspicious behavior or unauthorized access. Its primary goal is to identify potential threats, such as data breaches, malware, or other malicious activities, that may compromise the confidentiality, integrity, or availability of a system or network. IDSs can be categorized into two types: Host-Based IDS (HIDS), which monitors individual devices and their logs, and Network-Based IDS (NIDS), which analyzes network traffic for anomalies**.**Detection techniques include signature-based methods, which rely on known patterns of attacks, anomaly-based methods that flag deviations from normal behavior, and hybrid approaches that combine both for enhanced accuracy.

IDSs provide several benefits, including early threat detection, improved network visibility, and faster response to security incidents. However, they can have limitations such as false positives, false negatives, and potential performance impacts.Despite these challenges, IDSs are widely used in various sectors to protect sensitive data, secure critical infrastructure, and assist in forensic analysis. As cyber threats evolve, IDS technology continues to advance, integrating machine learning and artificial intelligence to improve detection capabilities and reduce false alerts.

Overview of Intrusion Detection Systems

An Intrusion Detection System (IDS) is a critical component of modern cybersecurity strategies, designed to monitor and analyze network or system activities to detect potential security threats, malicious behavior, or policy violations. Acting as a surveillance mechanism, IDS alerts administrators to suspicious activities, enabling timely intervention to mitigate potential damage. There are two primary types of IDS: Host-Based IDS (HIDS), which monitors activities on individual devices, such as operating system logs and file integrity, and Network-Based IDS (NIDS), which analyzes network traffic to identify anomalies, suspicious patterns, or known attack signatures.

DOI: 10.48175/IJARSCT-22908

Detection methods include signature-based detection, which relies on known attack patterns, anomaly-based detection, which identifies deviations from normal behavior using statistical models or machine learning, and hybrid approaches that combine both methods for greater accuracy. IDS provides several benefits, including early threat detection, enhanced visibility into network and system activities, and support for forensic analysis. However, challenges such as false positives, false negatives, and the need for regular updates to address evolving threats must be managed. Despite these limitations, IDS plays a vital role in safeguarding organizational assets, complementing other security measures like firewalls and intrusion prevention systems to provide a comprehensive defense against cyber threats.

Major types of IDS

Intrusion Detection Systems (IDS) are primarily classified into two major types: Host-Based Intrusion Detection Systems (HIDS) and Network-Based Intrusion Detection Systems (NIDS). HIDS operates on individual devices, monitoring system logs, configurations, and application activities for suspicious behavior or unauthorized changes, making it highly effective for identifying threats on specific hosts.

NIDS, on the other hand, monitors network traffic in real time, analyzing data packets to detect anomalies, malicious activity, or known attack patterns, thus providing comprehensive network-level protection. Other specialized types include Signature-Based IDS, which identifies threats based on predefined attack signatures, Anomaly-Based IDS, which uses behavioral analysis to detect deviations from normal patterns, and Policy-Based IDS, which relies on predefined rules and policies for threat detection. Each type serves a unique purpose, andtheir selection often depends on the specific security requirements of the environment.

Goals

The primary goals of Intrusion Detection Systems (IDS) are to enhance the security of computer systems and networks by identifying and responding to potential threats in real time. IDS aims to detect unauthorized access, misuse, or malicious activities that could compromise data integrity, confidentiality, and availability. It seeks to provide timely alerts to security teams, enabling rapid response to mitigate threats and minimize damage. Additionally, IDS facilitates the identification of vulnerabilities and weaknesses within a system, supporting proactive measures to strengthen defenses. By monitoring and analyzing user behavior, system activities, and network traffic, IDS also contributes to compliance with security policies and regulations, ensuring a robust and secure environment for critical operations.

Tools that Complement IDSs

Tools that complement Intrusion Detection Systems (IDSs) enhance the overall security framework by addressing specific aspects of threat detection, prevention, and response. Firewalls are a key complement, acting as the first line of defense by filtering incoming and outgoing traffic based on predefined rules. Security Information and Event Management (SIEM) systems integrate with IDSs to provide centralized logging, real-time monitoring, and advanced analytics for threat correlation. Antivirus and anti-malware solutions work alongside IDSs to detect and remove known malicious software. Vulnerability scanners help identify system weaknesses that attackers might exploit, while endpoint detection and response (EDR) tools monitor and analyze endpoint activities for suspicious behavior. Threat intelligence platforms offer insights into emerging threats, enabling IDSs to stay updated with evolving attack patterns. Together, these tools create a layered defense strategy, ensuring comprehensive protection against a wide range of cyber threats.

Benefits

Intrusion Detection Systems provide several significant advantages in safeguarding networks and systems against unauthorized access and malicious activities. They enable early detection of potential threats by continuously monitoring network traffic and system behavior. This proactive approach helps organizations mitigate risks before they escalate into severe security breaches. IDSs enhance overall security by providing detailed logs and alerts, which aid in forensic analysis and compliance with regulatory standards. They improve response times by identifying and isolating suspicious activities in real time, thus minimizing potential damage. Additionally, IDSs bolster the effectiveness of other security measures, such as firewalls and antivirus software, by acting as a complementary layer in a multi-faceted defense strategy. Overall, IDSs play a crucial roll in strengthening an organization's security posture and maintaining operational integrity.

Challenges

Despite their critical role in cybersecurity, Intrusion Detection Systems face several challenges that can hinder their effectiveness. One major issue is the high rate of false positives and false negatives. False positives can lead to unnecessary alerts and wasted resources, while false negatives may allow malicious activities to go undetected.

scalability is another challenge, as modern networks generate massive amounts of data, making it difficult for IDSs to process and analyze traffic efficiently.

Evolving attack techniques, such as advanced persistent threats (APTs) and polymorphic malware, also pose difficulties for traditional IDSs to adapt and identify sophisticated threats. Additionally, integrating IDSs with existing security frameworks and ensuring compatibility across diverse environments can be complex and resource intensive.

Balancing performance and accuracy while minimizing system overhead further complicates deployment. These challenges highlight the need for continuous improvement and innovation in IDS technologies.

II. METHODOLOGY

Requirement Analysis and Design

- Objective Definition: Clearly define the goals and objectives of the IDS based on the network environment. Determine whether the IDS will focus on network-based attacks (NIDS) or host-based attacks (HIDS).
- Threat Model Creation: Identify potential threats, attack vectors, and vulnerabilities within the network infrastructure or host systems.
- System Architecture Design: Design the architecture of the IDS, which includes data sources (network traffic, logs, system activities), detection methods (signature-based, anomaly-based, hybrid), and response mechanisms (alerting, blocking, or logging events).

Data Collection and Analysis:

- Data Acquisition**:** Gather relevant data for the IDS to monitor. This could include network traffic, system logs, file integrity checks, and system calls.
- Preprocessing and Filtering: Clean and preprocess data to eliminate noise and irrelevant information. Techniques like data normalization, feature extraction, and data transformation are applied to make the data suitable for detection algorithms.

Detection Mechanism Implementation:

- Signature-based Detection**:** Implement a database of known attack signatures (patterns of malicious activities) that the IDS can match against the incoming traffic or events.
- Anomaly-based Detection: Develop models based on normal behavior profiles. Any deviation from these profiles indicates potential intrusion. Machine learning and statistical techniques are often used to model normal behaviors.
- Hybrid Approach: Combine both signature and anomaly-based methods to balance the strengths and weaknesses of both. Signature-based detection is fast but limited to known attacks, while anomaly-based detection can identify unknown threats but may have higher false positive rates.

Alerting and Reporting:

- Alert Generation: When the IDS detects an intrusion or suspicious activity, it triggers alerts. Alerts can be categorized based on severity (e.g., critical, high, medium, low).
- Incident Reporting**:** A report is generated, providing detailed information about the event, including affected systems, attack type, and possible remedies.

Response Mechanism:

- Automated Response**:** Configure the IDS to automatically respond to certain threats by blocking suspicious IPs, terminating malicious sessions, or isolating affected systems.
- Manual Response**:** In some cases, alerts require manual investigation and intervention by security personnel to assess the threat and take further action.

Evaluation and Testing:

- False Positive and False Negative Rate Analysis: Evaluate the effectiveness of the IDS by testing it against known attack patterns and real-world traffic. Measure the false positive and false negative rates to assess the system's accuracy.
- Performance Testing: Assess how well the IDS performs in a live network environment, ensuring that it does not cause significant overhead or degrade network performance.

Deployment and Maintenance:

- Deployment**:** Deploy the IDS on the production network or host environment, ensuring it is monitoring key points such as entry points, critical assets, and vulnerable areas.
- Continuous Monitoring and Updates: Continuously monitor the performance of the IDS. Regularly update signature databases, anomaly models, and response rules to adapt to evolving threats.
- System Tuning and Optimization**:** Fine-tune the IDS by adjusting detection thresholds and response settings based on performance metrics and changing threat landscapes.

III. CONCLUSION

Intrusion Detection Systems (IDSs) are essential components of modern cybersecurity frameworks, designed to detect and respond to potential security threats within a network or host environment. Through constant monitoring of system activities and network traffic, IDSs serve as an early warning mechanism that helps prevent unauthorized access, data breaches, and various malicious activities.

The main types of IDSs—Network-based (NIDS), Host-based (HIDS), and Hybrid IDSs—each offer unique advantages, allowing organizations to choose the appropriate system based on their specific needs. While signature-based detection excels in identifying known threats, anomaly-based systems are valuable in recognizing novel or unknown attacks by learning the usual behavior of systems and networks. Combining these detection approaches in a hybrid model can provide a balanced defense against both known and unknown threats.

Despite their benefits, IDSs face challenges such as high false positive rates, resource limitations, and the need for continuous updating and tuning to keep pace with evolving threats. The effectiveness of an IDS depends not only on the detection techniques but also on its integration with other security tools, response mechanisms, and regular updates to its databases.

Ultimately, IDSs play a vital role in enhancing an organization's cybersecurity posture by detecting, analyzing, and responding to intrusions in real time. With proper implementation, maintenance, and integration into the broader security infrastructure, IDSs can significantly contribute to reducing the risk of cyberattacks and safeguarding sensitive data and critical systems.

REFERENCES

[1]. Khraisat, Ansam, Iqbal Gondal, Peter Vamplew, and Joarder Kamruzzaman. "Survey of intrusion detection systems: techniques, datasets and challenges." *Cybersecurity* 2, no. 1 (2019): 1-22.

[2]. Liao, Hung-Jen, Chun-Hung Richard Lin, Ying-Chih Lin, and Kuang-Yuan Tung. "Intrusion detection system: A comprehensive review." *Journal of Network and Computer Applications* 36, no. 1 (2013): 16-24.

[3]. Di Pietro, Roberto, and Luigi V. Mancini, eds. *Intrusion detection systems*. Vol. 38. Springer Science & Business Media, 2008.

DOI: 10.48175/IJARSCT-22908

[4]. Abdulganiyu, Oluwadamilare Harazeem, Taha Ait Tchakoucht, and Yakub Kayode Saheed. "A systematic literature review for network intrusion detection system (IDS)." *International journal of information security* 22, no. 5 (2023): 1125-1162.

[5]. Abdulganiyu, O.H., Tchakoucht, T.A. and Saheed, Y.K., 2024. Towards an efficient model for network intrusion detection system (IDS): systematic literature review. *Wireless Networks*, *30*(1), pp.453-482.

[6]. Wang, Xiao, Lie Dai, and Guang Yang. "A network intrusion detection system based on deep learning in the IoT." *The Journal of Supercomputing* 80, no. 16 (2024): 24520-2455

[7]. Sowmya, T. and Anita, E.M., 2023. A comprehensive review of AI based intrusion detection system. *Measurement:Sensors*, *28*, p.100827.

[8]. Issa, Melad Mohammed, Mohammad Aljanabi, and Hassan M. Muhialdeen. "Systematic literature review on intrusion detection systems: Research trends, algorithms, methods, datasets, and limitations." *Journal of Intelligent Systems* 33, no. 1 (2024): 20230248.

[9]. Azam, Zahedi, Md Motaharul Islam, and Mohammad Nurul Huda. "Comparative analysis of intrusion detection systems and machine learning based model analysis through decision tree." *IEEE Access* (2023).

[10]. Azam, Zahedi, Md Motaharul Islam, and Mohammad Nurul Huda. "Comparative analysis of intrusion detection systems and machine learning based model analysis through decision tree." *IEEE Access* (2023).

[11]. Vishwakarma, Monika, and Nishtha Kesswani. "A new two-phase intrusion detection system with Naïve Bayes machine learning for data classification and elliptic envelop method for anomaly detection." *Decision Analytics Journal* 7 (2023): 100233.

[12]. Bakro, Mhamad, Rakesh Ranjan Kumar, Amerah Alabrah, Zubair Ashraf, Md Nadeem Ahmed, Mohammad Shameem, and Ahmed Abdelsalam. "An improved design for a cloud intrusion detection system using hybrid features selection approach with ML classifier." *IEEE Access* 11 (2023): 64228-64247.