INTRUSION DETECTION SYSTEM : AN OVERVIEW

Prof. Vedankita Mohod
Master Of Computer Application (MCA) Department, K.D.K College of Engineering, Nagpur,Maharastra,India
vedankitamohod@kdkce.edu.in

Prajwal Madavi
Master Of Computer Application (MCA) Department, K.D.K College of Engineering, Nagpur,Maharastra,India
prajwalmadavi.mca23@kdkce.edu.in

Jayant Tekam
Master Of Computer Application (MCA) Department, K.D.K College of Engineering, Nagpur,Maharastra,India
jayanttekam.mca23@kdkce.edu.in

Abstract
Intrusion Detection Systems (IDS) have become a cornerstone of network and system security in today's digital landscape. Their primary role is to detect and respond to suspicious or unauthorized activities, helping organizations protect critical infrastructure from potential cyber threats. With the growing complexity and volume of cyber-attacks, traditional IDS techniques are becoming less effective. As a result, there has been a notable shift toward leveraging advanced technologies, such as machine learning (ML) and artificial intelligence (AI), to improve IDS capabilities. This paper discusses the evolution of IDS, their challenges, the current state of the art, and future trends that aim to revolutionize how IDS function in the face of increasingly sophisticated threats.
Keywords- *Intrusion detection system, unauthorized activity, cyber-attacks, threats.*

1. Introduction

As organizations continue to rely heavily on digital infrastructure, securing their networks and systems has become paramount. Intrusion Detection Systems (IDS) are designed to identify unauthorized access or abnormal activities within a network or system. Over the years, as cyber-attacks have evolved in both complexity and scale, IDS have had to adapt to remain effective. The need to detect threats in real-time, minimize false alerts, and continuously evolve to counter new attack strategies has spurred significant advancements in IDS technologies.

An IDS can be classified into different categories, each with distinct methods of detecting intrusions. Some of these systems focus on identifying known attack patterns, while others are designed to detect previously unknown or zero-day threats. As the threat landscape evolves, so too must the methods employed by IDS, resulting in an ongoing evolution of detection techniques that leverage newer technologies like machine learning and AI.

In this paper, we will explore the various types of IDS, their components, common challenges they face, recent technological advancements, and future trends shaping their development.

1.1 Intrusion Detection System

An **Intrusion Detection System (IDS)** is a critical component of modern cybersecurity frameworks that continuously monitors and analyzes network traffic or system activities for signs of suspicious or malicious behavior, known as intrusions. The primary purpose of an IDS is to detect unauthorized access or attacks on a computer system, network, or application and provide real-time alerts to security administrators for further investigation and mitigation. IDS serves as an essential tool to enhance the security posture of an organization, providing an early warning system that can identify potential threats and minimize damage before it escalates.

Intrusion Detection Systems play a key role in safeguarding the integrity, confidentiality, and availability of systems and data by identifying malicious actions, such as hacking attempts, malware infections, denial-of-service (DoS) attacks, and unauthorized access. The detection process involves continuous monitoring of system or network activities, analyzing patterns, behaviors, and other metrics to spot any anomalies or known attack signatures.

1.2 Types of Intrusion Detection Systems

Intrusion Detection Systems can be classified into the following types, based on their monitoring and detection methods:

Network-Based IDS (NIDS): These systems monitor the entire network to detect suspicious activities, such as unauthorized access or data exfiltration, by analyzing network traffic. NIDS typically function at the network perimeter or at critical points within the network and can monitor a broad range of activities across multiple systems simultaneously.

Host-Based IDS (HIDS): Unlike NIDS, which monitor network traffic, HIDS are installed on individual hosts or devices. HIDS monitors system activities, such as file integrity, system calls, and user behaviors, to detect any anomalous activities that could signal an attack. HIDS are particularly useful for detecting attacks that originate from within the network or a specific host.

Hybrid IDS: Hybrid IDS combines both NIDS and HIDS capabilities to provide a more comprehensive detection mechanism. By utilizing both network traffic analysis and host-based monitoring, hybrid IDS can offer deeper insights into potential threats, detecting intrusions across different layers of the network and system architecture.

1.3 Detection Methods

IDS can utilize a variety of methods to detect intrusions. The most common detection techniques include:

Signature-Based Detection: This technique relies on predefined patterns or signatures of known attacks. When network traffic or system behaviors match a signature, an alert is triggered. While this method is highly effective at identifying known attacks, it is not capable of detecting new or unknown threats unless their signatures have been previously defined.

Anomaly-Based Detection: Instead of relying on known attack patterns, anomaly-based detection identifies deviations from established baseline behaviors. For example, if a user's activity deviates significantly from their usual behavior, an alert may be triggered. While this approach is more flexible and can detect unknown threats, it may lead to higher rates of false positives because benign activities that deviate from the norm may also trigger alerts.

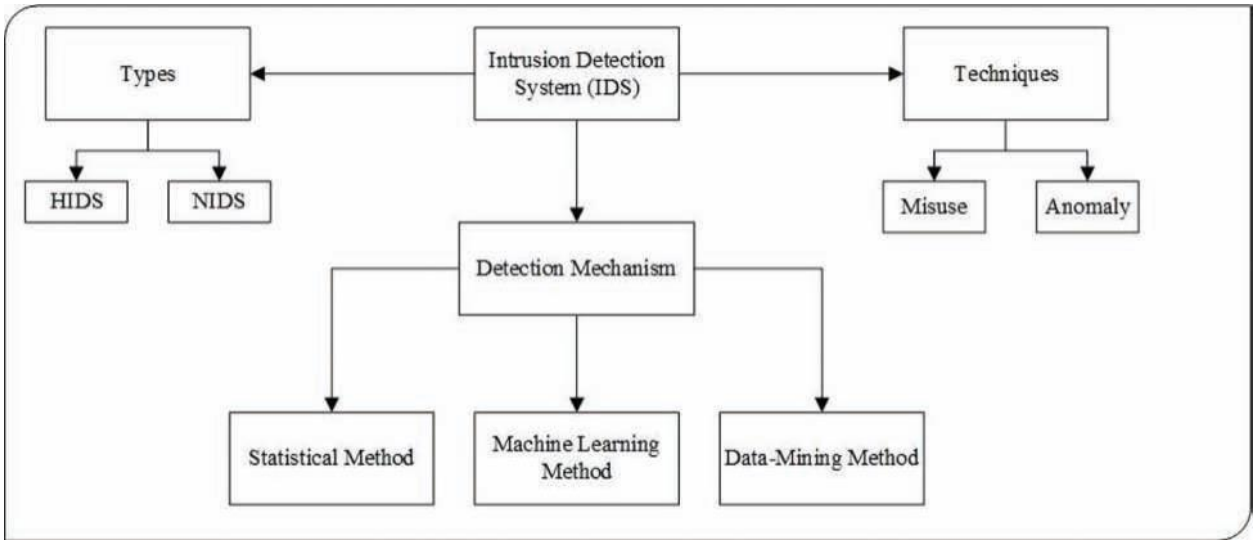

Figure 1 Intrusion detection system (IDS) overview

2. Literature Survey

1. Evolution of Intrusion Detection Systems

The concept of IDS comes from the early 1980s with the introduction of the "audit trail" system, the first ID based primarily on signature detection. In the late 1990s, when networks and systems developed more complex intrusion detection systems, simple signature adjustment restrictions developed into . **Denning (1987)** introduced the concept of anomaly-based detection. This allowed previously unknown attacks to be recognized by determining the basic line of normal system operation. **Zhao et al. (2020)** We explain the development of host-based IDs **(HIDS)** into network-based IDS **(NIDS)** and the latest development of hybrid ID models that combine signature-based and anomaly-based techniques. This evolution was driven by adaptation to increasingly sophisticated and diverse attack vectors.

2. IDS Detection Techniques

[A] Signature-based Detection : Scarfone et al. (2007) provided an in-depth analysis of signature-based IDS, noting its effectiveness in identifying common and easily identifiable threats, but also highlighting its limitation in detecting emerging attacks.

[B] Anomaly-based Detection : In **Chandola et al. (2009)**, the authors provided a comprehensive survey of anomaly-based detection techniques. They explained how statistical methods, clustering algorithms, and machine learning models such as Support Vector Machines (SVM) and Neural Networks (NN) are used to model normal behavior and identify deviations.

Recent work by **Ahmed et al. (2016)** has highlighted the advantages of integrating anomaly-based methods with machine learning algorithms to reduce false alarms and improve detection accuracy.

3. Machine Learning and Artificial Intelligence in IDS

Soni et al. (2021) emphasized the potential of **deep learning** techniques like **Convolutional Neural Networks (CNNs)** and **Recurrent Neural Networks (RNNs)** to detect complex, multi- step attacks. Their study demonstrated that deep learning models outperform traditional techniques in detecting novel attack patterns and reducing false positives.

Khan et al. (2020) provided a detailed review of machine learning algorithms used in IDS, highlighting the use of **Random Forests**, **K-Nearest Neighbors (K-NN)**, **Naive Bayes**, and **SVM** in detecting network intrusions. Their findings showed that ensemble learning methods, such as **Random Forests**, tend to be more accurate and robust in IDS applications.

4. Challenges in IDS

[A] False reporting and false negatives: One of the most important challenges in IDS is the recognition rate of false positive rate (FPR) and false negative rate (FNR). High results of false positives can overwhelm your security team, but false negatives can detect attacks. **Buczak & Guven (2016)** checked various IDS techniques and found that Anomalica-based methods often suffer from false positive rates, but signature-based systems present challenges in recognition of new attacks. The authors proposed that hybrid systems provide a promising solution to this compromise.

[B] Evasion Techniques: Bace (2000) identified several alternative techniques that use attackers to use attackers, and highlighted the need for IDS systems to constantly evolve to overcome such challenges. Dantu et al. (2003) Inspection of encrypted data traffic and hidden channels It represents the difficulty of IDS systems and emphasizes the importance of progressive package inspection methods.

[C] Scalability : Fang et al. (2016)discussed the issue of scalability of IDS and proposed the use of a distributed IDS architecture in which detection tasks are distributed across several sensors or active substances. It also mentioned cloud-based IDs as a scalable solution for large businesses.

5. Emerging Trends in IDS

[A] Cloud-based IDS : With the widespread adoption of cloud computing, traditional on-premises IDS may not be sufficient to monitor cloud environments effectively. Cloud-based IDS is becoming increasingly important as organizations migrate their infrastructure to the cloud. **Yin et al. (2020)** proposed a cloud-based IDS framework that leverages distributed computing for real-time threat detection in cloud networks. The study demonstrated the effectiveness of cloud IDS in scaling to large, dynamic cloud environments while maintaining low overhead.

[B] Blockchain for IDS : Blockchain technology has also found applications in IDS, particularly for improving the integrity of IDS data and logs. By utilizing a decentralized ledger system, blockchain can provide an immutable record of all detected incidents and responses, preventing tampering or alteration of logs.

Rasool et al. (2020) explored the integration of blockchain with IDS to enhance transparency and accountability in detecting cyberattacks. This approach is seen as a promising solution for creating tamper-proof logs, increasing trust in the IDS response.

3. Proposed Methodology

The proposed methodology for an Intrusion Detection System (IDS) aims to enhance the detection and response capabilities of IDS by combining the strengths of existing techniques while introducing innovative approaches for addressing modern security challenges. The methodology integrates multiple layers of detection, sophisticated analysis techniques, real-time response, and continuous system optimization.

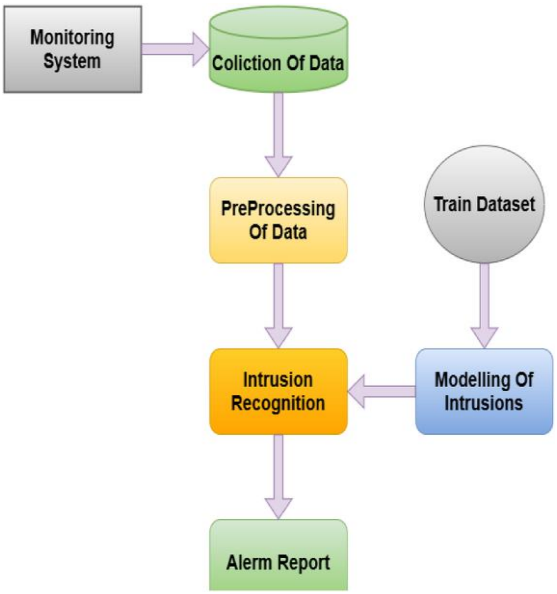

Figure 1 System architecture for Intrusion

Detection System

Comprehensive Data Collection Layer

- **Network Traffic Monitoring (NIDS):** Collect data from various network traffic sources such as routers, switches, and firewalls. Use packet sniffing tools, network flow analysis, and network taps to capture raw network traffic, including headers, payloads, and metadata.
- **Host-Level Monitoring (HIDS):** Collect data from host-based sources such as operating system logs, file integrity monitors, user activity logs, system processes, and application logs.

Preprocessing and Data Normalization Layer

- **Data Aggregation:** Raw data from multiple sources (network traffic, host logs, etc.) is aggregated to create a unified dataset. This can involve collecting logs from security appliances, servers, databases, and endpoints into a centralized platform for processing.
- **Data Normalization:** Normalize data from heterogeneous sources to a common format, enabling consistent analysis. For example, different devices and platforms might produce logs in different formats, so normalization ensures the data can be effectively analyzed.
- **Data Filtering and Noise Reduction:** Preprocess the data by filtering out known benign activities, such as routine user actions or legitimate traffic, to focus on potential intrusions. This helps reduce the noise and limits unnecessary alerts.

Advanced Detection Engine (Hybrid Detection)

- **Signature-Based Detection:** Maintain a robust signature database that contains known attack patterns, malware signatures, and exploit techniques. This allows for precise detection of known threats and attacks, such as worms, trojans, and DoS attacks.
- **Anomaly-Based Detection:** Build a baseline of normal network and host behaviors using advanced machine learning techniques, such as clustering and classification. Detect deviations from this baseline as potential intrusions. For example, an unusual spike in network traffic, an outlier behavior in user activities, or abnormal system processes can be flagged as suspicious.

Machine Learning and Artificial Intelligence for Dynamic Detection

- **Self-Learning Algorithms:** Use machine learning models that can adapt and improve over time. As more data is processed, the system can learn to identify new types of threats by continuously training on new traffic patterns, user behavior, and attack methods.
- **Unsupervised Learning:** Implement unsupervised learning algorithms to detect unknown threats. Unsupervised models like clustering and outlier detection can identify new attack patterns or behaviors that deviate from normal system usage without needing prior knowledge of specific attack signatures.
- **Threat Intelligence Integration:** Integrate threat intelligence feeds to improve detection accuracy by correlating detected activities with external intelligence. This can help identify emerging threats, new attack techniques, and malicious IP addresses in real-time.

4. Challenges in Intrusion Detection Systems

Despite their effectiveness, IDS face several challenges that can hinder their performance and accuracy. These challenges include:

4.1. False Positives and False Negatives

One of the most persistent issues in intrusion detection is the trade-off between false positives and false negatives. A **false positive** occurs when an IDS incorrectly identifies a legitimate activity as an intrusion, leading to unnecessary alerts and potentially wasted resources. On the other hand, a **false negative** occurs when the IDS fails to detect a real intrusion, allowing the threat to go unnoticed and unaddressed.

Balancing these two types of errors is a difficult task, and achieving a high level of accuracy is crucial for IDS systems to be effective. Reducing false positives and false negatives often requires fine-tuning detection algorithms and using advanced machine learning techniques to improve detection capabilities.

4.2. Evasion Techniques

Cybercriminals are constantly evolving their methods to evade detection by IDS. Evasion techniques such as traffic obfuscation, encryption, fragmentation, and polymorphic malware make it harder for traditional IDS methods to accurately detect intrusions. Attackers are becoming increasingly adept at disguising their activities to avoid triggering IDS alarms, which is a major challenge for IDS developers.

4.3. Scalability and Performance

With the rapid growth of network infrastructure and the increase in data traffic, IDS systems must be able to handle larger volumes of data and scale efficiently without compromising detection performance. As the size and complexity of networks grow, IDS must be capable of analyzing vast amounts of data in real-time, which often requires significant computational resources.

4.4. Resource Constraints

Resource constraints are particularly relevant in environments such as the Internet of Things (IoT) or edge computing, where devices may have limited processing power, memory, and storage. Implementing an IDS on such resource-constrained devices without overwhelming the system or impacting performance is a significant challenge.

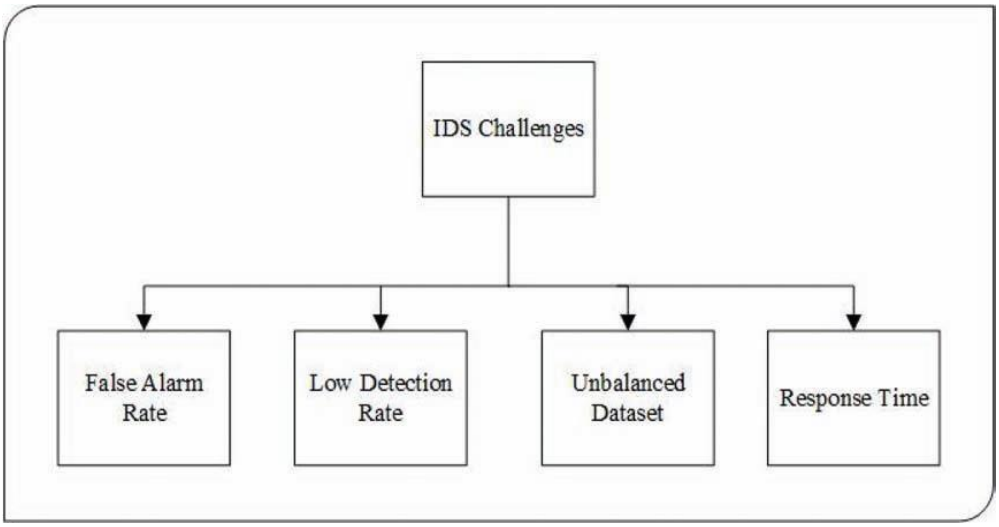

Figure 1 Intrusion detection system (IDS) challenges.

5. Future Trends in IDS

The future of IDS lies in the integration of cutting-edge technologies and adaptive systems that can meet the growing challenges of modern cybersecurity. Some notable future trends include:

Integration of AI and Threat Intelligence: Combining AI with real-time threat intelligence feeds will enable IDS to better predict, identify, and respond to emerging threats by leveraging the latest information from global attack trends and adversaries' tactics.

Automated Response Systems: IDS will not only detect intrusions but will increasingly be able to take automated actions in real-time, such as blocking malicious traffic, isolating affected systems, or initiating countermeasures.

Zero-Trust Architectures: The adoption of zero-trust security models, where trust is never assumed and every access attempt is verified, will require IDS to be fully integrated within security infrastructure to monitor all aspects of the network and detect potential threats at every level.

Blockchain-Based IDS: Blockchain could be used to enhance the integrity of IDS logs and detection systems. By using blockchain's decentralized and immutable nature, IDS logs can be secured, providing tamper-proof records that can be used for incident response, investigation, and compliance.

6. Conclusion

Intrusion Detection Systems (IDS) play a crucial role in modern cybersecurity by identifying malicious activities, monitoring for potential threats, and ensuring the integrity of computer networks and systems. Throughout this project, we have explored various IDS techniques, including signature-based detection, anomaly-based detection, hybrid approaches, and machine learning models, each with its own strengths and weaknesses.

This paper highlights the need for a robust, dynamic IDS that can detect both known and unknown threats, ensuring continuous protection against the ever-evolving landscape of cybersecurity challenges. Future developments in IDS technologies will likely focus on enhancing machine learning models, improving real-time performance, and fostering greater interpretability to ensure more effective and responsive intrusion detection.

References

1. Zhao, Z., Jiang, Z. & Liu, J. (2020). Research into intrusion detection systems: technology, challenges, future directions. Communication (ICC), 2020, 1-7
2. Soni, P., Thakur, M., & Gupta, P. (2021). *A deep learning-based intrusion detection system for high-performance network security.* IEEE Access, 9, 12530-12540.
3. Gao, Y., Zhang, Z., & Yang, Y. (2020). *Reinforcement learning-based intrusion detection system for adaptive network security.* Proceedings of the 2020 International Conference on Artificial Intelligence (AI), 153-160.
4. Khan, S. U., & McLaughlin, K. (2020). *A comprehensive review of machine learning*

techniques in intrusion detection systems. Future Generation Computer Systems, 110, 478-492.
5. Hsieh, Y. C., Huang, S. W., & Chen, C. M. (2018). *A hybrid intrusion detection system using decision trees and logistic regression for intelligent network security.* Journal of Intelligent & Fuzzy Systems, 34(3), 1487-1495.
6. Ghosh, A. & Mathew, M. Minutes of the IEEE International Conference on (2020). Real-time intrusion detection in smart grid networksBig data analysis. Proceedings of the IEEE International Conference on Smart GridsCommunications (SmartgridComm), 2020, 312-317.
7. Rahman, M. S., & Hossain, M. A. (2018). *A Novel Hybrid Intrusion Detection System using KNN and SVM for Network Security.* Proceedings of the International Conference on Computer, Communication, Control and Information Technology (C3IT), 2018, 132-137.
8. Kumar, R., & Bhaskar, R. (2019). *Hybrid Intrusion Detection System using Machine Learning Algorithms for Network Security.* Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS), 2019, 697-702.
9. Xu, Y. & Zheng, K. (2020). Design and implementation of intrusion detection systems based on blockchain technology. Proceedings of the International Conference on Security and Privacy (ICSP), 2020, 110-116.
10. Zhou, X., & Zhang, X. (2012). *Network Intrusion Detection Systems: Techniques, Tools, and Applications.* Springer.