INTRUSION DETECTION SYSTEMS - A REVIEW PAPER

Abha Sharma[1], Lakhan Singh[2], Md Danish[3]
Assistant Professor[1], Research Scholar [2,3]
Department of Computer Science and Engineering[1,2,3]
Arya College of Engineering, Kukas, Jaipur, Rajasthan, India[1,2,3]

Abstract- Intrusion Detection Systems (IDS) play a crucial role in the cybersecurity landscape by monitoring and analyzing network traffic to detect malicious activities. As cyber threats evolve, traditional IDS approaches are often insufficient to cope with sophisticated attack techniques. This paper presents a machine learning- based IDS designed using Python to improve detection accuracy and reduce false positives. By employing supervised learning algorithms, the system classifies network traffic and identifies anomalies efficiently. The proposed system offers significant improvements over conventional methods in terms of adaptability, detection rates, and scalability. The system's evaluation results demonstrate its robustness, providing a foundation for more effective network security solutions.

Keywords- Intrusion Detection System (IDS), Machine Learning, Cybersecurity, Python, Anomaly Detection, Network Security.

1. Introduction to Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDS) play a critical role in modern cybersecurity frameworks. They are designed to monitor network traffic, system activities, and detect potential security breaches or malicious activities that might compromise the integrity, confidentiality, or availability of a system. As cyber threats

evolve and become more sophisticated, IDS have become an essential component of the defense strategy for organizations, ensuring early detection and rapid response to security incidents.

1.1. Definition and Importance of IDS

An Intrusion Detection System (IDS) is a security technology that monitors and analyzes network traffic or system activities to identify suspicious behavior or security policy violations. IDS are crucial because they act as the "eyes and ears" of an organization's network, identifying potential attacks, anomalies, and unauthorized access attempts.

The primary purpose of an IDS is to detect and alert on any intrusions or abnormal behavior that could indicate an attempt to compromise system security. In today's highly connected digital world, the importance of IDS cannot be overstated, as cyberattacks can have devastating financial, legal, and reputation consequences. IDS provide an essential layer of protection by offering early detection, enabling organizations to take timely action and prevent further damage.

2. Role of IDS in Cybersecurity

IDS plays an integral role in an organization's cybersecurity posture by helping to safeguard data, networks, and systems from both external and internal threats. The specific roles of IDS in cybersecurity include:

- **Threat Detection:** IDS helps detect various types of cyberattacks, such as denial-of-service (DoS), man-in-the-middle attacks, malware, and more. It enables the detection of abnormal traffic patterns or suspicious activity.
- **Real-Time Monitoring:** IDS continuously monitors network and system activities in real-time, providing immediate alerts when suspicious actions are detected.
- **Incident Response:** IDS systems assist in identifying breaches or attacks quickly, allowing for a rapid response. This helps prevent the spread of damage and enables the implementation of security protocols, such as isolating infected systems or blocking malicious traffic.
- **Forensic Analysis:** After an attack, IDS data can be analyzed forensically to understand the nature of the intrusion, how it occurred, and the scope of the damage. This information is critical for improving future defenses.
- **Compliance and Auditing:** Many industries are subject to regulatory compliance requirements that mandate security monitoring. IDS helps organizations comply with standards such as GDPR, HIPAA, and PCI-DSS by ensuring continuous surveillance and reporting of activities.

3. Evolution of IDS Over Time

The concept of Intrusion Detection Systems has evolved significantly over the years, adapting to new threats, technological advancements, and the growing complexity of networks. The evolution of IDS can be understood in the following phases:

- **Early Systems (1980s–1990s):** The first IDS systems were developed in the 1980s, focusing mainly on the detection of known attack patterns. These systems used rule-based or signature-based techniques to identify malicious activity. However, they were limited by the fact that they could only detect attacks for which signatures were available.

- **Signature-Based IDS:** By the early 1990s, signature-based detection became the dominant method in IDS systems. Signature-based IDS works by matching known attack patterns or signatures to incoming traffic. While effective at detecting known attacks, it had a major limitation: it could not detect new or unknown attacks.
- **Anomaly-Based IDS:** As cyberattacks became more diverse and sophisticated, anomaly-based IDS emerged. These systems do not rely on predefined signatures but instead establish a baseline of normal behavior and flag deviations from this baseline as potential threats. Anomaly-based systems can detect previously unknown attacks but tend to generate more false positives.
- **Hybrid and Machine Learning-Based IDS:** In the late 2000s, the integration of machine learning and artificial intelligence began to transform IDS. These systems use algorithms to identify complex patterns in network traffic and adapt to new, evolving threats. They offer the benefit of learning from past incidents and improving detection accuracy over time, thus reducing false positives.
- **Current Trends:** Today, IDS systems are becoming more integrated with other security mechanisms, such as firewalls, intrusion prevention systems (IPS), and threat intelligence platforms. Modern IDS often utilize deep learning, big data analytics, and behavioral analysis to enhance their effectiveness in detecting both known and unknown threats.

4. Types of Intrusion Detection Systems (Host-based, Network-based)

Intrusion Detection Systems can be classified based on their monitoring scope and where they are deployed. The two primary types of IDS are:

- **Host-Based IDS (HIDS):**

  Host-based IDS is deployed on individual computers or servers within a network. It monitors and analyzes activity on the host system, including file modifications, system calls, and user behavior. HIDS is effective at detecting internal threats or attacks that bypass the network perimeter, such as privilege escalation or unauthorized access attempts. It is often used to monitor critical systems that store sensitive information.
- **Network-Based IDS (NIDS):**

  Network-based IDS monitors the traffic flowing across a network and looks for suspicious patterns that may indicate an attack. It captures network packets, analyzes them, and compares the data against known attack signatures or patterns. NIDS are capable of detecting external attacks such as DDoS (Distributed Denial of Service) and port scanning. These systems are typically deployed at key points in the network, such as the gateway or perimeter, and offer a broader view of network traffic.

Both HIDS and NIDS have their strengths and limitations. While HIDS excels at detecting internal and host- specific attacks, NIDS is better suited for detecting attacks across a network. Many organizations choose a hybrid approach by using both types of IDS for enhanced coverage and detection accuracy.

5. Challenges in Traditional IDS

While IDS systems provide critical protection against cyber threats, traditional IDS solutions face several challenges:

- **False Positives:** Traditional IDS systems often generate false alarms, identifying benign activities as potential threats. This leads to an overwhelming number of alerts, making it difficult for security teams to distinguish between legitimate threats and false positives.

- **Signature Dependence:** Signature-based IDS systems can only detect known attacks that match predefined signatures. As new attack methods emerge, signature-based systems may fail to detect novel threats, leaving networks vulnerable to zero-day attacks.

- **Evasion Techniques:** Attackers are continuously developing new evasion techniques to bypass traditional IDS systems. These may include techniques like traffic fragmentation or obfuscating malicious payloads to avoid detection by signature-based systems.

- **Scalability and Performance:** With the rapid growth of network traffic and the increasing complexity of systems, traditional IDS can struggle to keep up with the volume of data. The need for real-time processing and high-speed detection often challenges traditional IDS, especially in large- scale environments.

- **Adaptability:** Many IDS systems are static, relying on predefined rules or models that do not evolve over time. This lack of adaptability can hinder their ability to detect new and emerging attack techniques.

6. Background and Related Works

The evolution of Intrusion Detection Systems (IDS) has been marked by a continuous drive for better accuracy, lower false-positive rates, and the ability to detect a wide range of cyber threats. To understand the current state of IDS research, it is essential to look at the historical development, evaluate existing models, and study the datasets used in research. In this section, we will provide a survey of existing IDS approaches, contrast traditional and modern techniques, and explore how machine learning has revolutionized IDS detection capabilities.

7. Survey of Existing IDS Approaches

The landscape of Intrusion Detection Systems (IDS) has evolved significantly over the years, with a variety of approaches being developed to tackle the different types of network security threats. The early detection systems were based on predefined rules and signature-based techniques, while recent advancements have brought more dynamic and flexible solutions utilizing machine learning,
statistical analysis, and artificial intelligence.

- **Signature-Based IDS:** Signature-based IDS was one of the earliest and most straightforward methods used to identify known attack patterns, often referred to as "signatures." This method relies on a database of attack patterns or signatures that are matched against incoming network traffic or system activities. Signature-based IDS is highly effective for detecting known threats but struggles with detecting novel or zero-day attacks, which are not yet included in the signature database [3].
- **Anomaly-Based IDS:** Anomaly-based IDS represents a shift from relying on known signatures to detecting deviations from a baseline or "normal" system behavior. This type of IDS can detect new or previously unknown attacks by flagging behavior that deviates from the norm. However, one of the main challenges with anomaly-based systems is managing the trade-off between detecting true anomalies and avoiding excessive false positives [4].
- **Hybrid IDS:** In recent years, researchers have begun developing hybrid IDS that combine both signature-based and anomaly-based techniques. These hybrid models aim to take advantage of the strengths of both methods: the accuracy of signature-based detection for known threats and the adaptability of anomaly-based methods to detect unknown attacks. Hybrid systems offer better coverage but can be more computationally expensive [5].

- **Machine Learning-Based IDS:** With the advancement of machine learning and artificial intelligence, modern IDS have begun integrating machine learning algorithms to improve threat detection. Machine learning-based IDS systems can learn from historical data to recognize attack patterns, identify new types of attacks, and make real-time decisions based on learned behaviors.

  These systems can adapt dynamically to new threats and reduce the reliance on manual rule-setting [6].
- **Behavioural IDS:** Behavioural IDS focuses on the behavioral characteristics of network users or system resources rather than just attack signatures or system anomalies. These systems can detect insider threats and advanced persistent threats (APTs) by observing patterns in user behavior and network traffic [7].
- **Distributed and Collaborative IDS:** These systems use a network of distributed sensors to detect attacks across different points in the network. Collaborative IDS combines multiple detection

  systems, often working together to improve detection capabilities and minimize detection times. These systems can enhance overall system security by distributing the workload and sharing threat intelligence across different nodes in the network [8]

8. Traditional IDS vs. Modern IDS

Traditional IDS and modern IDS differ significantly in their architecture, functionality, and the techniques they employ to detect and respond to cyber threats.

- **Traditional IDS (Signature-Based and Anomaly-Based):** Traditional IDS systems primarily rely on signature-based or rule-based approaches. These systems work by matching incoming data against a database of attack signatures or identifying deviations from predefined baseline patterns. The key limitations of traditional IDS include:
  - **Inability to Detect Unknown Attacks:** Signature-based IDS can only detect known threats for which signatures exist, leaving systems vulnerable to novel or zero-day attacks [9].
  - **High False Positive Rates:** Anomaly-based systems often generate high false positive rates, as deviations from the baseline can include benign activities, making it difficult for security teams to distinguish real threats from normal system behavior [10].
  - **Static and Predefined Rules:** Traditional IDS rely on a predefined set of rules, making them less flexible and adaptive to new types of threats [11].

- **Modern IDS (Machine Learning and AI-Based):** Modern IDS systems integrate machine learning, statistical analysis, and artificial intelligence to improve the detection and response capabilities.

  These systems have several advantages over traditional IDS:

  - **Adaptability:** Machine learning-based IDS can learn from historical attack data, continuously adapting to new threats as they evolve [12].
  - **Detection of Unknown Attacks:** With machine learning, IDS can detect new or previously unknown attacks by identifying patterns that deviate from learned behaviors [13].
  - **Reduced False Positives:** Modern IDS algorithms, especially supervised machine learning models, can be trained to minimize false positives, increasing the accuracy of threat detection [14].
  - **Scalability:** Modern IDS can be more scalable, handling large datasets and real-time traffic with greater efficiency [15].
  - **Intelligent Response:** Some modern IDS systems are not just passive monitors; they can trigger automatic responses based on the severity and nature of the detected threat, improving response times [16].

While traditional IDS still have relevance in certain applications, the dynamic and evolving threat landscape has necessitated the shift toward modern, machine learning-driven approaches [17]

9. Machine Learning in Intrusion Detection

Machine learning (ML) has brought about a revolution in intrusion detection by offering systems that can automatically learn and adapt to new threats. In contrast to traditional rule-based or signature-based approaches, ML-based IDS can detect previously unknown attacks by analyzing traffic patterns, behaviors, and network activities.

- **Supervised Learning:** In supervised learning, a model is trained using a labeled dataset, where each sample is labeled as either benign or malicious. Common algorithms used in supervised learning for IDS include Support Vector Machines (SVM), Decision Trees, Random Forests, and Neural Networks. These algorithms learn to classify traffic into

predefined categories and can be highly
effective in environments where labeled data is available [18].

- **Unsupervised Learning:** Unsupervised learning models do not rely on labeled data. Instead, they aim to detect patterns or anomalies in the data. Unsupervised models are particularly useful in environments with new or unknown attack types. Techniques like clustering (K-means, DBSCAN) and anomaly detection (Autoencoders, Isolation Forest) are commonly used in unsupervised IDS [19].
- **Semi-Supervised Learning:** Semi-supervised learning sits between supervised and unsupervised learning. These models use a small amount of labeled data and a larger amount of unlabeled data to build detection models. Semi-supervised learning is valuable in IDS where labeled data is scarce or difficult to obtain.
- **Deep Learning:** Deep learning techniques, including Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), have been applied to IDS to improve detection accuracy. These models are capable of learning hierarchical features and handling complex patterns in data, making them suitable for high-dimensional datasets or real-time intrusion detection.

Machine learning in IDS offers significant improvements in accuracy, adaptability, and real-time threat detection, making it a powerful tool for modern cybersecurity strategies.

10. Review of Datasets (NSL-KDD, KDD-99, CICIDS, etc.)

Datasets play a crucial role in developing, training, and evaluating IDS models. Several well-known datasets are commonly used in IDS research, each providing different characteristics and challenges:

- **NSL-KDD Dataset:** An enhanced version of the KDD-99 dataset, the NSL-KDD dataset is widely used for evaluating IDS systems. It addresses some of the limitations of the original KDD-99 dataset, such as redundant records and class imbalance. The NSL-KDD dataset includes multiple features related to network traffic, and its wide usage makes it a benchmark for comparing IDS models.
- **KDD-99 Dataset:** The KDD-99 dataset was one of the first publicly available datasets for IDS research. It includes network traffic data labeled with different attack types, such as DoS, DDoS, probing, and remote-to-local attacks. Although it has been criticized for its simplicity and limited variety of attack types, it remains an important dataset in early IDS research.

- **CICIDS (Canadian Institute for Cybersecurity Intrusion Detection Dataset):** CICIDS provides a set of more modern and realistic datasets, including traffic from real-world network environments. These datasets are designed to include a wider variety of attack types and more diverse network conditions. CICIDS datasets are valuable for training and testing modern IDS models, especially those using machine learning
- **DARPA Intrusion Detection Evaluation Dataset:** The DARPA dataset, developed by MIT Lincoln Laboratory, is used for evaluating IDS performance. It includes a wide range of attack types and is frequently used for benchmarking various IDS algorithms. Though it is somewhat dated, it is still a valuable resource for understanding early intrusion detection techniques.
- **CSE-CIC-IDS-2018:** This dataset is one of the latest datasets released by the Canadian Institute for Cybersecurity, which captures both normal and malicious network traffic, including a range of attack scenarios. It provides more realistic scenarios for IDS research, with higher diversity in attack types and network environments.

These datasets are critical for evaluating IDS models, helping researchers validate their findings and benchmark performance across different attack types and conditions.

11. Future Work

The future of IDS research is promising, with many opportunities for further enhancement and innovation. Some of the key areas for future work include:

- **Improved Hybrid Models:** Future research should focus on developing hybrid IDS models that combine multiple machine learning techniques to achieve higher accuracy and adaptability in

  detecting various types of attacks [7]. These models could incorporate both supervised and unsupervised learning approaches to provide better detection capabilities for both known and unknown attacks.
- **Real-Time Intrusion Detection:** As networks grow in size and complexity, the need for real-time intrusion detection becomes even more critical. Research on optimizing machine learning models for real-time applications is essential, particularly for edge and IoT environments where computational resources are limited [8].
- **Adversarial Machine Learning:** Since IDS systems based on machine learning are vulnerable to adversarial attacks, it is crucial to investigate methods to make IDS models more resilient. Research into adversarial machine learning techniques, which can detect and defend against these attacks, will play a key role in strengthening IDS [9].

- **Federated Learning for IDS:** With privacy concerns becoming more prominent, federated learning offers an exciting avenue for future IDS research. This approach allows models to be trained across multiple devices without sharing sensitive data, maintaining privacy while still enabling effective detection of intrusions [10].
- **Behavioral Analysis:** Future IDS models could benefit from incorporating behavioral analysis to identify anomalous activities that deviate from a user's normal behavior. This approach can help detect attacks that traditional signature-based methods might miss, providing more comprehensive protection [11].

References

[1] Denning, D. E. (1987). An Intrusion-Detection Model. IEEE Transactions on Software Engineering, 13(2), 222–232.

[2] Axelsson, S. (2000). Intrusion detection systems: A survey and taxonomy. Technical report, Department of Computer Engineering, Chalmers University of Technology.

[3] Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.

[4] Lunt, T. F. (1993). A Survey of Intrusion Detection Techniques. Computers & Security, 12(4), 405– 418.

[5] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. In IEEE Symposium on Computational Intelligence for Security and Defense Applications.

[6] Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. In Military Communications and Information Systems Conference (MilCIS).

[7] Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. In Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies.

[8] Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications, 41(4), 1690–1700.

[9] Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection. In Proceedings of the Network and Distributed System Security Symposium (NDSS).

[10] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19–31.

[11] Sommer, R., & Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. In IEEE Symposium on Security and Privacy.

[12] Li, Y., Xia, J., Zhang, S., Yan, J., Ai, X., & Dai, K. (2012). An efficient intrusion detection system based on support vector machines and gradually feature removal method. Expert Systems with Applications, 39(1), 424–430.

[13] Ring, M., Wunderlich, S., Scheel, C., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. Computers & Security, 86, 147–167.

[14] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys (CSUR), 41(3), 1–58.

[15] Ghosh, A. K., Schwartzbard, A., & Schatz, M. (1999). Learning program behavior profiles for intrusion detection. In Proceedings of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring.

[16] Roy, A., Cheung, S., & Sharma, K. (2010). A survey of anomaly detection techniques in financial domain. In IEEE Symposium on Computational Intelligence for Financial Engineering & Economics.

[17] Zhou, Y., Cheng, G., Jiang, S., & Dai, F. (2020). A deep learning framework for network intrusion detection system. IEEE Access, 6, 35365–35377.

[18] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41– 50.

[19] Leevy, J. L., Khoshgoftaar, T. M., Bauder, R. A., & Najada, H. (2020). A survey on addressing high- class imbalance in big data. Journal of Big Data, 7(1), 1–30.