MANTECH Publications

Journal of Computer, Internet and Network Security
Volume 10, Issue 1, January-April, 2025
ISSN: 2457-0176 (Online)

# *Intrusion Detection Systems (IDS) for Network Security: Emerging Trends and Future Directions*

***Himanshu Verma[1], Ritu Saxena[2], Kavita Pal[3]***
*Research Scholar[1, 2], Professor[3]*
*Department of CSE*
*Gyan Bharti Institute of Technology, Muzaffarnagar, Uttar Pradesh*
***Email Id:*** *myselfhimanshu048@gmail.com[1]*

***Abstract***

*With the rapid evolution of cyber threats and increasing complexity of network architectures, Intrusion Detection Systems (IDS) have become a crucial component of modern network security. IDS monitor, analyze, and respond to malicious activities in real-time, helping organizations prevent data breaches and ensure the integrity of their systems. Traditional IDS approaches such as signature-based and anomaly-based methods have demonstrated effectiveness but face limitations in detecting zero-day attacks and sophisticated threats. Recent advancements in artificial intelligence (AI), machine learning (ML), and deep learning (DL) have revolutionized IDS capabilities, enabling more accurate and adaptive detection mechanisms. This paper explores the emerging trends in IDS, highlighting the integration of AI techniques, cloud-based IDS solutions, and Blockchain technologies. It also discusses the challenges associated with IDS implementation and presents future directions for enhancing IDS performance to safeguard networks against evolving threats.*

***Keywords:*** *Intrusion Detection Systems, Network Security, Artificial Intelligence, Anomaly Detection, Future Directions.*

## INTRODUCTION

As organizations become increasingly reliant on digital infrastructure, ensuring the security of networks has become a top priority. Intrusion Detection Systems (IDS) play a pivotal role in

detecting, analyzing, and mitigating unauthorized activities within a network. IDS are designed to identify suspicious behavior, prevent potential attacks, and maintain the confidentiality, integrity, and availability of information systems.

### Traditional IDS Techniques and Their Limitations

Traditional IDS approaches include signature-based and anomaly-based techniques. Signature-based IDS rely on a predefined database of attack signatures to identify known threats. While effective for recognizing established attack patterns, this approach is incapable of detecting zero-day exploits and novel attacks. Anomaly-based IDS, on the other hand, detect deviations from normal behavior patterns, offering the ability to identify previously unseen threats. However, anomaly-based systems often generate high false-positive rates, making them less reliable for real-time threat detection.

### Need for Advanced IDS Techniques

The growing sophistication of cyber threats, including polymorphic malware, Distributed Denial of Service (DDoS) attacks, and Advanced Persistent Threats (APTs), necessitates the use of advanced IDS techniques. Artificial intelligence, machine learning, and deep learning models have emerged as promising solutions to enhance IDS capabilities, enabling the detection of complex patterns and adapting to evolving threats.

## LITERATURE REVIEW

Extensive research has been conducted on enhancing IDS capabilities through advanced technologies and innovative approaches.

## SIGNATURE-BASED AND ANOMALY-BASED IDS

***Table no. 1 Comparison of Signature-Based and Anomaly-Based IDS***

| **Feature** | **Signature-Based IDS** | **Anomaly-Based IDS** |
|---|---|---|
| Detection Method | Matches known attack signatures | Detects deviations from normal behavior |
| Accuracy for Known Attacks | High | Moderate |
| Detection of Zero-Day | Low | High |

| | | |
|---|---|---|
| Attacks | | |
| False Positive Rate | Low | High |
| Computational Efficiency | High | Moderate |
| Adaptability | Low | High |

**Description:** This table compares the key characteristics of signature-based and anomaly-based IDS, highlighting their strengths and limitations.

Signature-based IDS compare incoming network traffic with known attack signatures stored in a database. Popular tools such as Snort and Suricata utilize signature-based detection to identify malicious patterns. However, these systems are ineffective against novel or zero-day attacks that do not match existing signatures.

Anomaly-based IDS, in contrast, establish a baseline of normal network behavior and detect deviations from that baseline. Machine learning techniques such as Support Vector Machines (SVM), Decision Trees (DT), and k-Nearest Neighbors (k-NN) have been widely employed to enhance anomaly detection accuracy. However, anomaly-based IDS are prone to false positives, which can lead to alert fatigue and reduced operational efficiency.

## AI AND MACHINE LEARNING IN IDS

Artificial Intelligence (AI) and Machine Learning (ML) have significantly improved the performance of IDS by enabling systems to learn from historical data and adapt to evolving threats. Deep learning techniques such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) have been used to detect complex attack patterns and reduce false positives. Researchers have demonstrated that AI-powered IDS outperform traditional methods by providing higher accuracy and better adaptability.

## CLOUD-BASED IDS SOLUTIONS

Cloud-based IDS solutions offer scalable, real-time threat detection by leveraging the computational power and flexibility of cloud environments. These systems provide centralized monitoring and enhanced threat intelligence by aggregating data from multiple sources.

Cloud-based IDS can dynamically scale to handle high-volume traffic and improve threat detection accuracy.

## BLOCKCHAIN TECHNOLOGY IN IDS

Blockchain technology has been explored as a means to enhance IDS security and reliability. Blockchain-based IDS solutions provide immutable records of network activity, ensuring data integrity and preventing tampering. Decentralized consensus mechanisms in blockchain technology enhance trust and transparency in IDS operations.

## TYPES OF INTRUSION DETECTION SYSTEMS

### Network-Based Intrusion Detection Systems (NIDS)

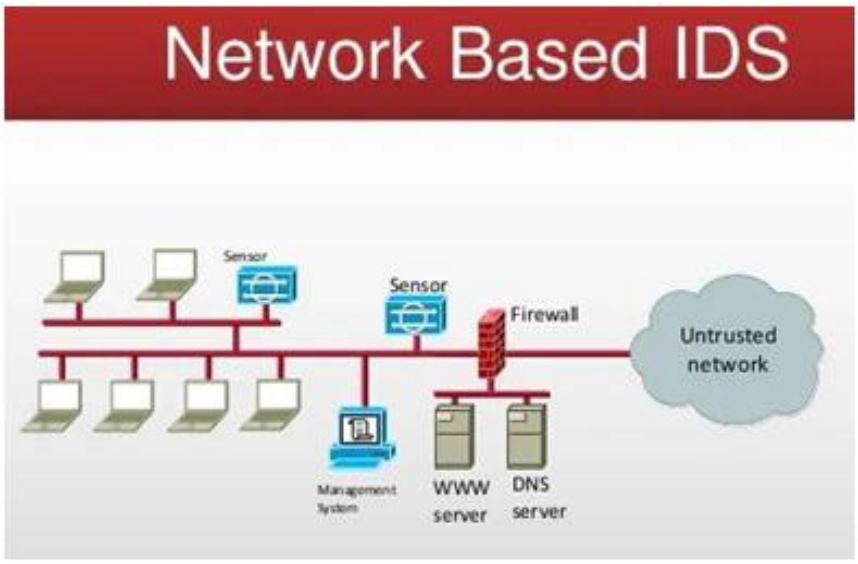


***Figure no. 1: Architecture of a Network-Based Intrusion Detection System (NIDS)***

**Description:** The image illustrates the architecture of a Network-Based Intrusion Detection System (NIDS),

Showcasing the key components such as packet analyzers, signature databases, and alert generation modules. It highlights the process of monitoring network traffic and identifying malicious activity. NIDS monitor incoming and outgoing traffic across a network, analyzing packets for malicious activity. These systems provide real-time threat detection and alert administrators to potential security breaches.

## HOST-BASED INTRUSION DETECTION SYSTEMS (HIDS)

HIDS operate at the individual host level, monitoring system files, logs, and processes for suspicious behavior. They provide detailed visibility into host activity and are particularly useful for detecting insider threats.

## HYBRID IDS

Hybrid IDS combine the strengths of NIDS and HIDS, offering a comprehensive security solution that monitors both network traffic and host activities. Hybrid IDS provide higher accuracy and coverage by correlating data from multiple sources.

## EMERGING TRENDS IN IDS

### AI and Deep Learning Integration

AI-powered IDS utilize deep learning models such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Generative Adversarial Networks (GAN) to enhance detection accuracy and reduce false positives. These models can identify complex attack patterns and adapt to evolving threats.

***Table no. 2: AI Models Used In Intrusion Detection Systems***

| AI Model | Application in IDS | Key Advantage |
|---|---|---|
| Convolutional Neural Networks (CNN) | Detects spatial patterns in network traffic | High accuracy in identifying complex attack patterns |
| Recurrent Neural Networks (RNN) | Analyzes sequential data for anomaly detection | Suitable for real-time anomaly detection |
| Support Vector Machines (SVM) | Classifies network traffic based on learned patterns | Effective in binary classification tasks |
| k-Nearest Neighbors (k-NN) | Identifies anomalies by comparing with nearest neighbors | Simplicity and efficiency |
| Generative Adversarial Networks (GAN) | Generates synthetic attack data to train IDS models | Improves resilience against evolving threats |

**Description:** This table highlights the various AI models used in IDS and their respective applications in improving intrusion detection efficiency.

### Behavioral Analysis and User Entity Behavior Analytics (UEBA)

Behavioral analysis techniques, including User and Entity Behavior Analytics (UEBA), analyze user behavior patterns to detect anomalies indicative of malicious activities. UEBA enhances IDS effectiveness by identifying insider threats and abnormal user behavior that traditional techniques may miss.

### Autonomous and Self-Learning IDS

Self-learning IDS leverage unsupervised machine learning techniques to autonomously identify and adapt to emerging threats. These systems continuously refine their models based on new attack patterns, reducing the need for manual intervention.

### Cloud-Based IDS with Real-Time Threat Intelligence

Cloud-based IDS solutions integrate real-time threat intelligence feeds to provide up-to-date protection against new and emerging threats. These systems dynamically scale to handle high-volume traffic and enhance threat visibility across distributed environments.

## CHALLENGES IN IMPLEMENTING IDS

### High False Positive Rates

One of the most critical challenges faced by Intrusion Detection Systems (IDS), particularly anomaly-based IDS, is the high rate of false positives. False positives occur when legitimate or benign network activities are incorrectly flagged as malicious threats. Since anomaly-based IDS relies on identifying deviations from predefined normal behavior, it often misclassifies uncommon but legitimate network events as potential intrusions. This misclassification leads to an influx of unnecessary alerts, a phenomenon known as alert fatigue.

### Resource and Computational Overhead

Advanced IDS techniques, particularly those powered by Artificial Intelligence (AI) and Deep Learning (DL), require significant computational resources to analyze and process vast amounts of network data. These systems rely on complex algorithms and models that consume substantial processing power, memory, and storage capacity. As networks continue to grow in size and complexity, the computational demands of IDS increase, posing scalability and performance challenges.

### Evasion Techniques and Advanced Threats

As intrusion detection technologies advance, sophisticated attackers continually develop evasion techniques to bypass IDS detection mechanisms. Evasion techniques involve modifying attack patterns or disguising malicious activities to appear as normal traffic, thereby avoiding detection. These tactics exploit weaknesses in IDS algorithms, allowing attackers to infiltrate systems undetected.

## SCOPE OF IDS IN FUTURE NETWORK SECURITY

### Integration of AI-Driven Threat Detection

Future IDS systems will integrate AI and ML models capable of detecting sophisticated attack patterns with minimal human intervention. AI-driven IDS will leverage predictive analytics and threat intelligence to identify and mitigate threats in real time.

### Deployment of Blockchain-Based IDS

Blockchain technology holds the potential to revolutionize IDS by providing immutable records of network activity and enhancing data integrity. Blockchain-based IDS can prevent data tampering and ensure secure communication between network entities.

### Securing IoT Networks with Lightweight IDS

With the proliferation of IoT devices, securing IoT networks has become a critical priority. Lightweight IDS solutions designed specifically for IoT environments will provide enhanced security while maintaining minimal computational overhead.

### Advanced Threat Hunting and Incident Response

Future IDS will incorporate advanced threat hunting capabilities to proactively identify and neutralize potential threats before they escalate. Automated incident response mechanisms will enable real-time mitigation of security breaches.

## CONCLUSION

Intrusion Detection Systems (IDS) have become an essential part of modern network security, protecting organizations against malicious activities and ensuring the confidentiality, integrity, and availability of sensitive information. Traditional IDS techniques, including signature-based and anomaly-based approaches, have proven effective in identifying known threats and

detecting deviations from normal behavior. However, these systems face challenges in terms of high false positive rates, computational overhead, and susceptibility to sophisticated evasion techniques.

To address these limitations, the integration of Artificial Intelligence (AI) and Machine Learning (ML) has revolutionized IDS capabilities. AI-powered IDS models leverage deep learning techniques such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) to analyze complex attack patterns and minimize false positives. Additionally, cloud-based IDS solutions provide scalable and real-time threat detection, while blockchain technology enhances the integrity and transparency of intrusion detection mechanisms.

Despite these advancements, IDS face ongoing challenges, including the need for continuous refinement to counter advanced persistent threats (APTs) and polymorphic malware. Resource and computational constraints, particularly in IoT and edge environments, further complicate IDS deployment. To overcome these hurdles, future IDS systems will need to incorporate federated learning, edge AI, and adaptive threat detection mechanisms capable of autonomously learning and adapting to emerging threats.

The future of IDS lies in the seamless integration of cutting-edge technologies that can proactively detect and mitigate threats in real time. As cyber threats evolve, IDS systems must advance in parallel to ensure robust network security, minimizing false positives, reducing computational overhead, and enhancing resilience against sophisticated evasion tactics. By embracing these innovations, organizations can strengthen their defense posture and safeguard their critical assets from ever-evolving cyber threats.

**REFERENCES**

1. Bose, S., & Kumar, R. (2022). Enhancing anomaly detection using machine learning for IoT networks.Journal of Emerging Trends in Computer Science and Information Security, 19(2), 87-95.
2. Chen, Y., & Nakamura, H. (2021). Blockchain-based intrusion detection system for network security.Journal of Cryptography and Secure Communication Technologies, 16(4), 78-92.

3. Deshmukh, A., & Mehta, P. (2023). Challenges in deploying AI-powered IDS in IoT environments.Indian Journal of Cyber Security and Data Protection, 12(1), 34-47.
4. Evans, T., & Williams, J. (2023). A comparative study of signature-based and anomaly-based intrusion detection systems.Cybersecurity Journal of Advanced Network Defense, 22(3), 101-114.
5. Fang, X., & Liu, J. (2021). Deep learning models for improving false positive reduction in IDS. International Journal of Artificial Intelligence and Cybersecurity, 18(2), 45-58.
6. Gupta, R., & Sharma, A. (2024). Role of blockchain technology in securing internet communications.Journal of Computer Science Innovations in India, 15(3), 112-125.
7. Harrison, M., & Zhang, W. (2022). Mitigating computational overhead in AI-powered IDS using edge computing.International Journal of Distributed Network Security, 11(4), 67-78.
8. Iyer, V., & Prasad, K. (2023). Analyzing evasion techniques and challenges in modern IDS. Journal of Cybersecurity and Threat Mitigation in India, 9(2), 51-63.
9. Johnson, D., & Lewis, P. (2023). Exploring the effectiveness of hybrid intrusion detection systems.Journal of Emerging Technologies in Network Security, 20(1), 87-99.