IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

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

ISSN: 2581-9429

Volume 5, Issue 6, November 2025

Impact Factor: 7.67

A Review on Building Cyber-Resilient Systems through Intrusion Detection and Prevention Frameworks

Hemanth Kumar K G[1] and Dr. Kamal Kumar Srivastava[2]

[1]Research Scholar, Department of Computer Application

[2]Professor, Department of Computer Application

Sunrise University, Alwar, Rajasthan

Abstract: *The rapid expansion of digital infrastructure and the proliferation of cyber threats have highlighted the critical need for cyber-resilient systems. Intrusion Detection Systems and Intrusion Prevention Systems are central to enhancing cybersecurity by identifying, mitigating, and preventing attacks on networks and information systems. This review examines recent advances in IDS and IPS technologies, frameworks, and methodologies aimed at building cyber-resilient systems. Key trends include the integration of machine learning, anomaly-based detection, hybrid frameworks, and real-time response mechanisms. The study identifies the strengths and limitations of existing frameworks and suggests directions for improving detection accuracy, reducing false positives, and enhancing system resilience*

Keywords: Cyber-resilience, Intrusion Detection System, Network Security

I. INTRODUCTION

Cyber-resilience is the ability of a system to anticipate, withstand, recover, and adapt to cyber-attacks while maintaining its essential functions. As organizations increasingly rely on interconnected systems, the complexity and frequency of cyber-attacks have surged, necessitating robust defense mechanisms (Ahmad et al., 2021). Intrusion Detection Systems monitor network traffic to detect suspicious activities, while Intrusion Prevention Systems proactively prevent malicious actions by blocking attacks in real time (Scarfone & Mell, 2007). The combination of IDS and IPS forms a critical foundation for cyber-resilient systems capable of defending against a wide range of threats. The increasing reliance on digital infrastructure has intensified the need for cyber-resilient systems capable of withstanding, detecting, and responding to cyber threats. Intrusion Detection Systems and Intrusion Prevention Systems play a critical role in achieving this resilience by monitoring network and system activities to identify malicious behavior and prevent potential attacks (Scarfone & Mell, 2007). Traditional IDS frameworks relied on signature-based detection, which effectively identifies known threats but struggles against novel or zero-day attacks (Roesch, 1999).

To address this limitation, anomaly-based detection techniques have been developed, employing machine learning and statistical methods to detect deviations from normal system behavior (Sommer & Paxson, 2010). Modern cybersecurity frameworks increasingly adopt hybrid approaches that combine signature and anomaly-based detection, enhancing both accuracy and adaptability while reducing false positives (Sharma, Singh, & Garg, 2020). Furthermore, the integration of host-based and network-based IPS provides comprehensive coverage, allowing systems to defend against both endpoint-level and network-level threats (Modi et al., 2013).

The application of machine learning, particularly supervised and unsupervised algorithms, has enabled IDS/IPS frameworks to analyze large volumes of network traffic efficiently, identifying complex attack patterns and evolving threats (Ahmed, Mahmood, & Hu, 2016; Kim, Lee, & Kim, 2018). Despite these advancements, challenges remain, including high false positive rates, computational overhead, and the complexity of integrating multiple detection techniques into a unified framework (Garcia-Teodoro et al., 2009).

DOI: 10.48175/568

Future research emphasizes the development of intelligent, adaptive systems capable of real-time threat detection and automated response, while ensuring privacy and minimizing resource consumption. Overall, IDS and IPS frameworks, particularly when enhanced with machine learning and hybrid strategies, form the backbone of cyber-resilient systems, enabling organizations to anticipate, mitigate, and recover from cyber-attacks effectively (Ahmad, Basheer, & Malik, 2021).

EVOLUTION OF INTRUSION DETECTION AND PREVENTION FRAMEWORKS

IDS and IPS frameworks have evolved significantly over the past two decades. Early systems were primarily signature-based, relying on known attack patterns to detect intrusions. While effective against known threats, signature-based systems struggled to identify zero-day attacks (Roesch, 1999). To overcome these limitations, anomaly-based detection emerged, leveraging machine learning algorithms to identify deviations from normal behavior (Sommer & Paxson, 2010). Recent frameworks adopt a hybrid approach, combining signature-based and anomaly-based methods to improve detection accuracy and reduce false positives (Sharma et al., 2020).

The evolution of Intrusion Detection Systems and Intrusion Prevention Systems has been driven by the increasing complexity of cyber threats and the growing dependence on digital networks and infrastructures. Initially, IDS frameworks were primarily signature-based, relying on predefined attack patterns or signatures to detect malicious activity. Signature-based IDS are highly effective at identifying known threats with low false-positive rates; however, they are inherently limited in detecting new or zero-day attacks that do not match existing signatures (Roesch, 1999; Scarfone & Mell, 2007). This limitation prompted the development of anomaly-based IDS, which detect deviations from established baseline behaviors. Anomaly-based systems can identify novel threats and adapt to evolving attack strategies, but they often suffer from higher false-positive rates and require significant amounts of training data to define “normal” behavior accurately (Sommer & Paxson, 2010; Ahmed, Mahmood, & Hu, 2016).

Over time, hybrid IDS/IPS frameworks emerged, combining signature-based and anomaly-based methods to leverage the advantages of both approaches. These hybrid frameworks improve detection accuracy, reduce false positives, and offer the flexibility to handle both known and unknown threats (Sharma, Singh, & Garg, 2020). In parallel, the distinction between network-based and host-based systems became important: network-based IDS/IPS monitor network traffic in real-time, providing immediate protection against distributed attacks, whereas host-based systems monitor individual endpoints, focusing on system-level threats and insider attacks (Modi et al., 2013). Modern frameworks integrate both approaches to provide comprehensive coverage across networks and endpoints.

The integration of machine learning and artificial intelligence represents a significant milestone in the evolution of IDS/IPS frameworks. Supervised learning algorithms such as Support Vector Machines, Random Forests, and Neural Networks are commonly used to classify network traffic and identify attack patterns (Ahmed et al., 2016). Unsupervised learning and clustering techniques enable the detection of previously unknown attacks by identifying deviations from typical system behavior (Javaid et al., 2016). More recently, deep learning approaches have enhanced the ability of IDS/IPS frameworks to analyze large-scale, high-dimensional network traffic, enabling rapid detection of complex and multi-stage attacks (Kim, Lee, & Kim, 2018).

Key points summarizing the evolution of IDS/IPS frameworks include:

Signature-Based IDS (1990s): Relied on known attack signatures; high accuracy for known threats but unable to detect zero-day attacks (Roesch, 1999).

Anomaly-Based IDS (2000s): Detected deviations from normal behavior; capable of identifying new threats but prone to false positives (Sommer & Paxson, 2010).

Hybrid IDS/IPS (2010s): Combined signature and anomaly-based methods to improve accuracy and flexibility (Sharma et al., 2020).

Host-Based vs Network-Based Systems: Addressed endpoint vs network threats; modern frameworks integrate both for comprehensive protection (Modi et al., 2013).

Machine Learning Integration: Enhanced adaptability and automated threat detection using supervised and unsupervised algorithms (Ahmed et al., 2016; Javaid et al., 2016).

Deep Learning Approaches: Enabled analysis of complex traffic patterns and multi-stage attacks with higher detection rates (Kim et al., 2018).

The evolution of IDS/IPS frameworks reflects the ongoing arms race between cybersecurity defenses and increasingly sophisticated cyber threats. While early frameworks focused on static signature detection, modern approaches emphasize adaptability, automation, and comprehensive monitoring. Current research trends include developing intelligent, self-learning systems capable of real-time threat mitigation while minimizing false positives and computational overhead. This evolution underscores the critical role of IDS and IPS in building cyber-resilient systems capable of maintaining operational continuity in the face of emerging threats (Ahmad, Basheer, & Malik, 2021).

CLASSIFICATION OF IDS AND IPS FRAMEWORKS

Intrusion Detection Systems and Intrusion Prevention Systems are fundamental components of modern cybersecurity frameworks, designed to protect digital assets from malicious activities. These systems can be classified based on their detection methodology, deployment approach, and operational strategy. The first major classification is signature-based IDS, which relies on predefined patterns of known attacks.

Signature-based systems, such as Snort, are highly effective at detecting recognized threats with low false-positive rates (Roesch, 1999; Scarfone & Mell, 2007). However, they are limited in their ability to detect novel or zero-day attacks, as their effectiveness depends on regularly updated attack databases. The second classification is anomaly-based IDS, which uses statistical models, machine learning algorithms, or behavior profiling to identify deviations from normal network or host activity (Sommer & Paxson, 2010; Ahmed, Mahmood, & Hu, 2016). Anomaly-based systems can detect previously unknown attacks and are adaptive to changing network environments, but they often suffer from higher false-positive rates and require extensive training data for accuracy.

The third classification is hybrid IDS/IPS frameworks, which integrate both signature and anomaly-based techniques. Hybrid systems leverage the strengths of both approaches, detecting known attacks efficiently while also identifying novel threats (Sharma, Singh, & Garg, 2020). By combining multiple detection mechanisms, hybrid systems can reduce false positives and provide a more comprehensive security posture, although they can be computationally intensive and complex to configure. Beyond detection methodology, IDS and IPS frameworks can also be classified by deployment type**.**

Network-based IDS/IPS monitor traffic at strategic points in the network, analyzing packets to detect malicious activity in real-time (Modi et al., 2013). NIDS/NIPS are effective for monitoring multiple hosts simultaneously and detecting attacks such as Denial of Service or network scans, but they may miss attacks targeting specific endpoints or encrypted traffic. Host-based IDS/IPS on the other hand, are deployed on individual systems and monitor internal activities such as file modifications, system calls, and user behavior (Garcia-Teodoro et al., 2009). HIDS/HIPS provide granular security and can detect insider threats but are resource-intensive and require deployment across all endpoints.

Another dimension of classification includes passive versus active systems. IDS are generally passive systems, generating alerts when suspicious activities are detected but not directly preventing attacks, whereas IPS are active, capable of taking real-time action, such as blocking IP addresses, terminating sessions, or isolating compromised systems (Scarfone & Mell, 2007). The combination of passive and active strategies enables organizations to detect attacks early and mitigate potential damage efficiently. Emerging frameworks also incorporate machine learning and artificial intelligence, allowing for predictive detection, adaptive response, and automated threat mitigation. Algorithms such as Random Forests, Support Vector Machines and neural networks enhance both anomaly detection and hybrid IDS/IPS performance by identifying complex attack patterns in large-scale network data (Kim, Lee, & Kim, 2018; Javaid et al., 2016).

IDS and IPS frameworks can be classified according to detection methodology deployment type operational strategy and technological enhancement. Each classification has unique advantages and limitations, and selecting an appropriate framework depends on organizational needs, network complexity, and threat landscape. Effective cyber-resilient systems often employ a combination of these frameworks, integrating multiple layers of detection and prevention to protect against known and emerging cyber threats (Ahmad, Basheer, & Malik, 2021).

Table 1: Classification of IDS and IPS Frameworks

Framework Type	Key Features	Advantages	Limitations	References
Signature-Based IDS	Detects attacks using known signatures	High accuracy for known attacks, low false positives	Cannot detect unknown/zero-day attacks	Roesch, 1999; Scarfone & Mell, 2007
Anomaly-Based IDS	Uses behavior models and ML algorithms	Detects novel attacks, adaptive	High false positive rate, requires training data	Sommer & Paxson, 2010; Ahmed et al., 2016
Hybrid IDS/IPS	Combines signature and anomaly detection	Balanced accuracy, detects known and unknown attacks	Computationally intensive, complex configuration	Sharma et al., 2020; Ahmad et al., 2021
Network-Based IPS	Monitors network traffic in real-time	Immediate attack prevention	Limited to network-level threats, may miss host-level attacks	Modi et al., 2013
Host-Based IPS	Monitors individual system activity	Protects endpoints, detects insider threats	Resource-intensive, requires endpoint deployment	Modi et al., 2013; Garcia-Teodoro et al., 2009

MACHINE LEARNING IN CYBER-RESILIENCE

Machine learning has become integral to modern IDS and IPS frameworks. Supervised learning algorithms such as Random Forest, Support Vector Machines and Neural Networks have been applied to classify network traffic as malicious or benign (Ahmed et al., 2016). Unsupervised methods, including clustering and anomaly detection algorithms, identify previously unknown attacks without labeled data (Javaid et al., 2016). The integration of deep learning enables the analysis of large-scale, complex network traffic patterns, providing higher detection rates and adaptability to evolving threats (Kim et al., 2018).

Machine learning has become a cornerstone in developing cyber-resilient systems, particularly in enhancing the capabilities of Intrusion Detection Systems and Intrusion Prevention Systems. Traditional IDS and IPS frameworks rely on static rules or signature-based detection, which are effective only against known threats. However, the rapid evolution of cyber-attacks, including zero-day exploits, ransomware, and advanced persistent threats has necessitated the adoption of intelligent and adaptive approaches for real-time threat detection (Sommer & Paxson, 2010). Machine learning algorithms provide these systems with the ability to learn from historical data, identify patterns, and predict anomalies that signify potential attacks, thereby significantly improving system resilience (Ahmed, Mahmood, & Hu, 2016).

KEY CONTRIBUTIONS OF MACHINE LEARNING IN CYBER-RESILIENCE

Enhanced Threat Detection:

Supervised learning algorithms such as Support Vector Machines Random Forest, and Neural Networks can classify network traffic as malicious or benign with high accuracy. These models are trained on labeled datasets containing examples of normal and attack traffic, allowing the system to detect both known and slightly modified attack patterns (Kim, Lee, & Kim, 2018).

Anomaly Detection:

Unsupervised learning methods, including clustering and autoencoders, can identify deviations from normal behavior without requiring labeled data. This capability is particularly useful for detecting novel attacks and insider threats that traditional signature-based systems may miss (Javaid et al., 2016).

DOI: 10.48175/568

Real-Time Threat Response:
ML-enabled IDS/IPS frameworks can provide near real-time detection and response, allowing for automated isolation or blocking of suspicious activity. Reinforcement learning approaches can further optimize the decision-making process, enabling systems to dynamically adapt to evolving attack strategies (Ahmad, Basheer, & Malik, 2021).

Reduction of False Positives:
One major challenge in anomaly-based systems is the high rate of false positives, which can overwhelm administrators and reduce operational efficiency. Machine learning models, particularly ensemble methods combining multiple algorithms, help reduce false alarms by cross-validating detection signals (Sharma, Singh, & Garg, 2020).

Scalability and Adaptability:
ML models can scale to large and complex network environments, analyzing high volumes of traffic data without manual intervention. Deep learning techniques, such as Convolutional Neural Networks and Recurrent Neural Networks are capable of processing sequential and temporal data, which is essential for monitoring continuous network activity and predicting attack patterns over time (Kim et al., 2018).

Predictive Threat Intelligence:
Beyond detection, machine learning can be integrated with threat intelligence platforms to predict potential attack vectors, enabling organizations to proactively strengthen vulnerable systems and mitigate risks before they are exploited (Ahmed et al., 2016).

Despite the numerous advantages, challenges remain in implementing ML for cyber-resilience. These include the need for large and high-quality datasets for training, computational resource demands for real-time analysis, and ensuring data privacy during monitoring (Garcia-Teodoro et al., 2009). Additionally, attackers are increasingly leveraging adversarial machine learning techniques to deceive ML-based defenses, highlighting the need for continuous adaptation and model validation (Sommer & Paxson, 2010).

Machine learning has transformed the field of cyber-resilience by enabling intelligent, adaptive, and proactive security mechanisms. By enhancing detection accuracy, reducing false positives, and providing predictive insights, ML-based IDS and IPS frameworks form the backbone of modern cyber-resilient systems, equipping organizations to respond effectively to an ever-evolving threat landscape (Ahmad et al., 2021; Kim et al., 2018).

CHALLENGES IN BUILDING CYBER-RESILIENT SYSTEMS

Despite technological advancements, several challenges persist in designing robust IDS and IPS frameworks:

High False Positives: Anomaly-based systems often misclassify benign activities as attacks.

Evolving Threat Landscape: Rapid emergence of new malware, ransomware, and zero-day exploits.

Resource Constraints: Real-time analysis and prevention require substantial computational resources.

Integration Complexity: Combining multiple detection methods increases system complexity.

Data Privacy: Monitoring network and host activities may involve sensitive information.

II. CONCLUSION

Building cyber-resilient systems requires a comprehensive approach, integrating IDS and IPS frameworks with modern machine learning techniques and real-time response mechanisms. While traditional signature-based methods are limited, hybrid and anomaly-based frameworks offer enhanced adaptability against emerging threats. Effective implementation must balance detection accuracy, computational efficiency, and privacy concerns. By addressing current limitations and incorporating advanced analytics, organizations can strengthen their cybersecurity posture and ensure continuity of operations in the face of evolving cyber threats.

REFERENCES

[1]. Ahmad, I., Basheer, A., & Malik, S. (2021). Cyber-resilient systems: Strategies and frameworks. *Journal of Information Security*, 12(3), 112–126.

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

[3]. Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, 28(1-2), 18–28.

[4]. Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. *Evolving Systems*, 8, 1–13.

[5]. Kim, G., Lee, S., & Kim, S. (2018). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications*, 41(4), 1690–1700.

[6]. Modi, C., Patel, D., Borisaniya, B., Patel, H., & Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. *Journal of Network and Computer Applications*, 36(1), 42–57.

[7]. Roesch, M. (1999). Snort - Lightweight intrusion detection for networks. *Proceedings of the 13th USENIX Conference on System Administration*, 229–238.

[8]. Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (IDPS). *NIST Special Publication 800-94*.

[9]. Sharma, S., Singh, M., & Garg, S. (2020). A hybrid intrusion detection system using machine learning techniques. *Journal of Information Security and Applications*, 55, 102611.

[10]. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *IEEE Symposium on Security and Privacy*, 305–316.