International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 05 Pages: 19-30
OCLC – 1368736135

Journal Website: http://sciencebring.com/index.php/ijasr

Research Article

Intrusion Detection Systems In Modern Networks Technologies Challenges And Future Research Directions

Submission Date: March 25, 2026, **Accepted Date:** April 20, 2026,
Published Date: May 11, 2026
Crossref doi: https://doi.org/10.37547/ijasr-06-05-03

Nuriddin Safoev
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan

Suhrobjon Bozorov
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan

Sirojiddin Salimov
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan

Shakarov Muhiddin Abdug'Affor O'G'Li
Cyber university, Tashkent region, Uzbekistan

Abstract

This paper examines the main types, detection approaches, and architectural solutions of Intrusion Detection Systems (IDS). Based on early research, it analyzes host-based, network-based, and hybrid deployment models, as well as signature-based, anomaly-based, and hybrid detection methods. The paper further presents modern industry-grade platforms widely used today—such as Suricata, Zeek, Wazuh, and AI/ML-based security solutions—in place of earlier academic prototypes developed in the 2010s. In addition, it discusses current challenges, including real-time processing requirements, false positive rates, encrypted traffic analysis, scalability issues, and the integration of artificial intelligence, as well as outlines future research directions in the field.

Keywords

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 05 Pages: 19-30
OCLC – 1368736135

ISSN-2750-1396

Network security, Intrusion Detection Systems (IDS), anomaly detection, signature-based analysis, artificial intelligence, network monitoring, XDR.

INTRODUCTION

The rapid development of information and communication technologies, the expansion of corporate networks, the widespread adoption of cloud computing, and the growing number of IoT and mobile devices have significantly increased the complexity of modern network infrastructures. Alongside these developments, the increasing scale, sophistication, and automation of cyberattacks have created serious security challenges for organizations, government institutions, and individual users. In particular, threats such as malware, Distributed Denial-of-Service (DDoS) attacks, zero-day exploits, insider threats, and Advanced Persistent Threats (APT) have exposed the limitations of traditional security mechanisms. Consequently, the development of modern security systems capable of continuous network traffic monitoring, early detection of suspicious activities, and rapid response to cyberattacks has become one of the most critical issues in cybersecurity [1].

Today, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are widely recognized as essential components of network security infrastructures. IDS technologies monitor network traffic and host activities in order to detect malicious behavior, unauthorized access attempts, and various anomalies, whereas IPS solutions are capable of automatically blocking identified threats and filtering malicious traffic. These systems play a vital role in ensuring the confidentiality, integrity, and availability of information resources by detecting cyber threats during the early stages of an attack.

Early IDS/IPS solutions were primarily based on signature-based detection and statistical analysis techniques. However, modern systems increasingly incorporate Machine Learning (ML), Deep Learning (DL), behavioral analysis, and artificial intelligence technologies. These approaches significantly improve the effectiveness of identifying unknown threats, analyzing anomalies, and making decisions in real time. Furthermore, the integration of zero-trust architectures, Security Information and Event Management (SIEM) platforms, and security orchestration systems has substantially enhanced the functional capabilities of IDS/IPS solutions [1-5].

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 05 Pages: 19-30
OCLC – 1368736135

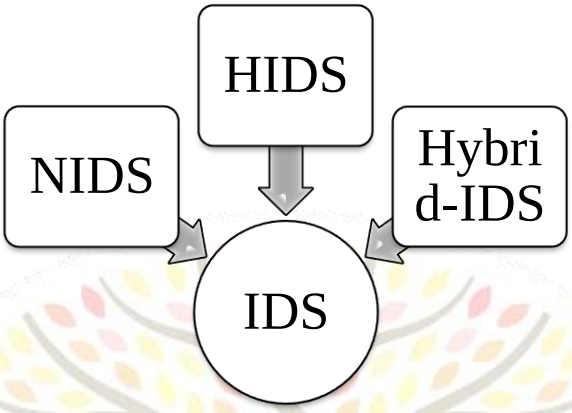

Figure 1. Main types of IDS.

This paper analyzes the operational principles, classification, technical foundations, and modern implementations of IDS and IPS technologies. In addition, it examines signature-based and anomaly-based detection methods, AI-driven approaches, real-time monitoring mechanisms, and threat prevention strategies, along with their advantages and limitations. The study also evaluates practical challenges associated with IDS/IPS deployment, including False Positive and False Negative detections, as well as performance issues in high-speed network environments. The findings of this research provide a scientific and practical foundation for improving modern network security infrastructures, increasing the efficiency of early threat detection, and developing next-generation intelligent protection systems.

MAIN TYPES OF INTRUSION DETECTION SYSTEMS

Intrusion Detection Systems (IDS) are among the most important security mechanisms designed to detect malicious activities and monitor security events within network infrastructures. IDS technologies can be classified into several categories depending on the monitored environment, deployment method, and analysis mechanisms. In practice, the most widely used IDS architectures include Network-based Intrusion Detection Systems (NIDS), Host-based Intrusion Detection Systems (HIDS), and hybrid IDS solutions, as shown in Figure 1. Each type possesses specific technical capabilities, advantages, and limitations, and their selection depends on the organization's infrastructure and security requirements [1].

Network-based Intrusion Detection Systems (NIDS). Network-based Intrusion Detection Systems are designed to monitor and analyze traffic transmitted across network segments. These systems are typically deployed near routers, switches, or network gateways, where they collect network packets through dedicated sensors. NIDS platforms analyze packet headers and payloads to identify signs of malicious activity, suspicious traffic patterns, and known exploit signatures. One of the primary advantages of NIDS is the ability to centrally monitor an entire network segment. Consequently, NIDS solutions can detect various threats in real time, including Distributed Denial-of-Service (DDoS) attacks, port scanning, spoofing, brute-force attempts, and protocol-based attacks.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 05 Pages: 19-30
OCLC – 1368736135

In addition, a single sensor can monitor multiple devices simultaneously, simplifying security management in large-scale corporate networks.

However, NIDS technologies also have several limitations. In particular, the widespread adoption of modern encryption protocols such as TLS/SSL complicates packet payload inspection. Furthermore, processing large volumes of traffic in high-speed networks requires substantial computational resources and may lead to packet loss. Therefore, modern NIDS solutions increasingly utilize hardware accelerators, parallel processing architectures, and artificial intelligence-based optimization techniques to improve performance and scalability.

Host-based Intrusion Detection Systems (HIDS). Host-based Intrusion Detection Systems are deployed on individual servers, workstations, or endpoint devices and monitor activities occurring within the host itself. HIDS platforms analyze operating system log files, file system modifications, user activities, registry keys, system processes, and local network connections. These systems are particularly effective in detecting insider threats, unauthorized configuration changes, and malicious software activities. The major advantage of HIDS lies in its ability to provide deep host-level monitoring and detect malicious actions even when network traffic is encrypted. For example, HIDS solutions can effectively identify rootkits, privilege escalation attempts, unauthorized process execution, and modifications of critical system files. In addition, by analyzing user behavior, HIDS systems can successfully detect insider threats and abnormal user activities [3-6].

Despite these advantages, deploying and managing HIDS across numerous hosts introduces additional complexity. Each endpoint requires an agent process that consumes system resources, and the absence of centralized management can make monitoring more difficult. Moreover, in cases where a host is compromised, attackers may manipulate or delete log records, potentially reducing the effectiveness of the monitoring process.

Hybrid IDS Systems. In modern enterprise infrastructures, relying solely on either NIDS or HIDS is often insufficient. As a result, hybrid IDS architectures have become increasingly popular. Hybrid systems integrate the capabilities of both NIDS and HIDS into a unified platform, enabling centralized analysis of both network-level and host-level monitoring data. Within such architectures, security data is typically forwarded to Security Information and Event Management (SIEM) or Extended Detection and Response (XDR) platforms. These systems correlate logs and events collected from multiple sources, assess threat severity, and initiate automated response mechanisms. As a result, detection accuracy improves, false positives decrease, and incident response times are significantly reduced.

Hybrid IDS solutions are particularly effective in cloud infrastructures, virtualized environments, and large-scale enterprise networks. Nevertheless, deploying such systems may require considerable technical expertise and substantial financial investment. Despite these challenges, the increasing complexity of modern cyber threats makes hybrid IDS/IPS architectures one of the most promising approaches for advanced cybersecurity protection.

Detection Approaches And Technical Foundations

Intrusion Detection Systems (IDS) can be classified into several major categories based on their attack

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 05 Pages: 19-30
OCLC – 1368736135

detection mechanisms. These approaches differ according to the principles of malicious activity detection, the algorithms employed, and the analytical methods applied. In practice, the most widely used approaches include signature-based detection, anomaly-based detection, and hybrid detection methods, as shown in Figure 2.

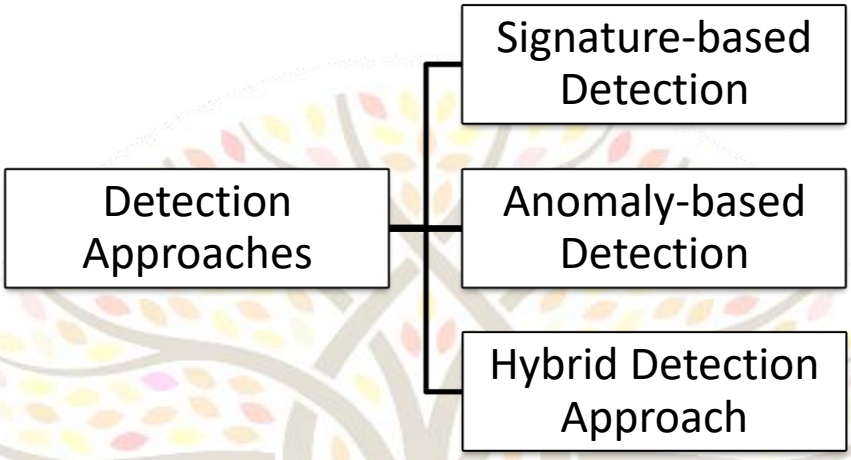

Figure 2. IDS detection aproaches.

Signature-based Detection. Signature-based detection relies on databases containing known attack patterns, exploit descriptions, and malicious traffic signatures. In this approach, the IDS compares network traffic or system activities against predefined rule sets and generates alerts whenever a match is identified. This method is particularly effective in detecting classical attacks such as malware infections, port scanning, SQL injection, buffer overflow exploits, and other well-known threats. The primary advantage of this approach lies in its high detection accuracy and relatively low False Positive rate. Since the system only identifies activities that match predefined signatures, the number of incorrect alerts is significantly reduced. Today, widely used IDS/IPS platforms such as Suricata and Snort heavily depend on signature-based rule databases for threat detection.

However, the major limitation of this method is its inability to effectively detect unknown or modified attacks. Zero-day exploits, polymorphic malware, and newly emerging attack techniques may remain undetected because their signatures are not yet included in the rule database. Therefore, continuous updating and maintenance of signature repositories are essential for maintaining the effectiveness of signature-based IDS systems [4-9].

Anomaly-based Detection. Anomaly-based detection is based on creating a model of normal network or system behavior and identifying deviations from this model as potential threats. In this approach, parameters such as traffic volume, packet transmission frequency, user activities, session duration, and other behavioral metrics are analyzed using statistical methods or machine learning algorithms. One of the most significant advantages of anomaly-based systems is their ability to detect unknown and previously unseen

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 05 Pages: 19-30
OCLC – 1368736135

attacks. Unlike signature-based methods, anomaly detection focuses on deviations from normal behavior rather than predefined attack patterns. This capability increases the effectiveness of detecting Advanced Persistent Threats (APT), insider threats, and sophisticated multi-stage attacks.

Algorithms such as Isolation Forest, Autoencoder models, and One-Class Support Vector Machines are widely used in anomaly detection systems. These techniques establish models of normal traffic behavior and classify substantial deviations as suspicious or malicious activities. Nevertheless, anomaly-based systems often suffer from relatively high False Positive rates, particularly during the initial deployment stage. In many cases, natural variations in network behavior or unusual but legitimate traffic may be incorrectly classified as attacks.

Hybrid Detection Approaches. Modern IDS/IPS systems frequently employ hybrid detection mechanisms that combine the advantages of both signature-based and anomaly-based approaches. In hybrid systems, known attacks are identified using signature databases, while unknown or suspicious behaviors are analyzed through anomaly detection models. Hybrid architectures provide more accurate evaluation of security events. For instance, a signature-detected event may be further analyzed together with user behavior patterns and traffic context information. As a result, both False Positive and False Negative rates can be reduced, significantly improving overall detection efficiency. Today, hybrid approaches are extensively implemented within SIEM and XDR platforms, where they are integrated with artificial intelligence, behavioral analytics, and real-time monitoring technologies. This integration enables the development of multi-layered and adaptive defense mechanisms against modern cyber threats [4-9].

Modern IDS/IPS technologies utilize various advanced technical foundations to ensure high detection accuracy and real-time traffic analysis. Unlike traditional rule-based systems, current-generation platforms incorporate statistical modeling, artificial intelligence, behavioral analytics, and adaptive decision-making mechanisms. These technologies considerably enhance the capability to identify sophisticated and previously unknown cyber threats.

Statistical and Probabilistic Models. One of the earliest and most fundamental techniques used in IDS systems involves statistical and probabilistic modeling. This approach analyzes parameters such as traffic volume, session duration, packet transmission frequency, byte distribution, protocol usage ratios, and connection counts. The system creates a statistical profile of normal network behavior and identifies significant deviations from this profile as anomalies. For example, an unusually large volume of packets transmitted within a short time interval may indicate a Distributed Denial-of-Service (DDoS) attack. Similarly, abnormal session durations or excessive access attempts to specific ports may suggest scanning or brute-force activities. Probabilistic models employ Bayesian theory, Markov chains, and statistical distributions to estimate the risk level of security events. Since these methods require relatively low computational resources, they are widely applied in real-time monitoring environments [10-12].

Machine Learning and Deep Learning Technologies. In recent years, Machine Learning (ML) and Deep Learning (DL) technologies have become essential components of IDS/IPS systems. These technologies enable automatic analysis of

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 05 Pages: 19-30
OCLC – 1368736135

large-scale traffic datasets, identification of complex patterns, and prediction of unknown threats. Long Short-Term Memory (LSTM) neural networks are commonly used for analyzing time-dependent traffic characteristics. Due to their effectiveness in processing sequential data, these models can identify temporal dependencies within network sessions. Convolutional Neural Networks (CNN) are applied for deep packet inspection and malicious pattern recognition. In addition, modern research increasingly employs Graph Neural Networks (GNN) to analyze relationships and interactions between devices and network nodes. The major advantage of machine learning technologies is their ability to detect previously unknown threats without relying solely on predefined signature databases. However, these approaches require large training datasets and substantial computational resources, which remain important limitations of ML-based IDS systems.

Behavioral Analysis (UEBA – User and Entity Behavior Analytics). Behavioral analysis systems identify threats by monitoring the long-term activities of users and network entities. This technology, known as User and Entity Behavior Analytics (UEBA), is based on establishing behavioral profiles of normal user activities. For example, logging into a system outside regular working hours, connecting from unusual geographic locations, or transferring large amounts of data may be classified as suspicious behavior. UEBA systems are particularly effective in detecting insider threats, credential theft, and unauthorized activities performed by privileged users. Integrated with artificial intelligence and machine learning algorithms, UEBA technologies provide contextual analysis of user and device activities. As a result, these systems can identify not only isolated incidents but also long-term threat tendencies and behavioral anomalies.

Fuzzy Logic and Dynamic Rules. Modern IDS/IPS systems also apply fuzzy logic approaches to process incomplete and uncertain information. Unlike traditional threshold-based systems, fuzzy logic evaluates traffic behavior using flexible categories such as “safe,” “partially risky,” or “highly dangerous.” This approach enables dynamic adaptation of system parameters in real time. For instance, threshold values can be automatically adjusted under high network load conditions, thereby reducing False Positive rates. Similarly, dynamic rules are automatically generated based on current traffic conditions, user behavior patterns, and historical data. Fuzzy logic-based systems are particularly effective in complex and uncertain traffic environments. Therefore, together with artificial intelligence and behavioral analytics technologies, they are considered an essential component of next-generation IDS/IPS solutions.

Modern Systems and Architectural Models

Intrusion Detection Systems were initially developed as academic and experimental projects. Early research platforms such as ADAM, MINDS, HIDE, and DNIDS played an important role in establishing the theoretical and practical foundations of network threat detection. These systems primarily relied on statistical analysis, expert rule sets, and early anomaly detection algorithms. However, due to the increasing complexity of modern network infrastructures, the rapid growth of traffic volume, and the demand for real-time processing, these academic solutions have largely been replaced by industry-grade open-source and commercial IDS/IPS platforms.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 05 Pages: 19-30
OCLC – 1368736135

ISSN-2750-1396

Modern IDS/IPS technologies are based on architectures that provide high performance, scalability, automated threat analysis, and integration with artificial intelligence technologies as provided in Table 1. The following section discusses widely used contemporary platforms and their key characteristics.

Table 1. Modern IDS/IPS Platforms

System	Type	Key Features	Application Areas
Suricata	NIDS / IPS	Multi-threading architecture, real-time packet analysis, TLS/QUIC metadata extraction, Deep Packet Inspection (DPI), integration with Emerging Threats rule sets	Large enterprise networks, data centers, ISP infrastructures
Zeek (Bro)	NIDS / NSM	Protocol-level semantic analysis, high-level event generation, extensible scripting language, traffic baselining, and forensic capabilities	Threat hunting, network forensics, Security Operations Centers (SOC)
Wazuh / OSSEC	Hybrid HIDS / NIDS	File Integrity Monitoring (FIM), log analysis, rootkit detection, vulnerability scanning, and compliance monitoring	Small and medium-sized enterprises (SME), government organizations, compliance-oriented environments
Darktrace / CrowdStrike Falcon	Hybrid / Cloud-native	Self-learning AI algorithms, zero-day threat detection, lateral movement analysis, UEBA, XDR, and SOAR integration	Enterprise infrastructures, cloud-native environments, zero-trust architectures

Suricata. Suricata is one of the most widely used modern open-source NIDS/IPS platforms and is distinguished by its high-performance multi-threading architecture. Since the system can utilize multiple processor cores in parallel, it is capable of analyzing large volumes of network traffic in real time. Suricata supports Deep Packet Inspection (DPI), TLS and QUIC metadata extraction, protocol decoding, and signature-based threat detection. The platform operates in integration with the Emerging Threats rule database and supports continuously updated threat signatures. Suricata is especially suitable for large enterprise networks, Internet Service Providers (ISPs), and high-speed data center environments [9].

Zeek (Bro). Formerly known as Bro, Zeek is considered more of a Network Security Monitoring (NSM) platform than a traditional IDS solution. Unlike classical signature-based systems, Zeek performs semantic analysis at the protocol level. It generates high-level events for protocols such as HTTP, DNS, TLS, SSH, and others, while also providing an extensible scripting language for customized analysis. This platform is highly effective for threat hunting, network forensics, traffic baselining, and correlation of complex security events. Zeek's flexible scripting framework enables users to create custom security policies and monitoring mechanisms tailored to organizational requirements [8].

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 05 Pages: 19-30
OCLC – 1368736135

Wazuh / OSSEC. Wazuh and OSSEC are host-based security monitoring platforms that combine HIDS functionalities with certain NIDS capabilities. These systems support File Integrity Monitoring (FIM), log analysis, vulnerability detection, rootkit identification, and compliance management. Wazuh is particularly effective when integrated with SIEM platforms for centralized security monitoring. These solutions are commonly deployed in small and medium-sized businesses, government institutions, and environments requiring regulatory compliance [10].

AI/ML-Based Platforms. Next-generation IDS/IPS platforms based on artificial intelligence and machine learning technologies are becoming increasingly important in cybersecurity. Platforms such as Darktrace and CrowdStrike Falcon automatically learn user and network behavior patterns through self-learning algorithms and are capable of identifying previously unknown threats. These systems support zero-day attack detection, lateral movement analysis, insider threat monitoring, and automated incident response. In addition, they integrate with SOAR (Security Orchestration, Automation, and Response) platforms to provide automated reactions to security incidents. AI/ML-based solutions are particularly popular in cloud-native infrastructures and zero-trust environments.

Modern IDS/IPS Architectures. Traditional IDS systems were primarily based on centralized architectures. However, modern infrastructures increasingly adopt distributed and microservice-based approaches. In such architectures, monitoring components are distributed across multiple nodes and managed through containerized services. As a result, system scalability and fault-tolerance capabilities are significantly improved. With the rapid development of cloud infrastructures, IDS/IPS technologies are also being adapted to cloud-native environments. For example, platforms such as AWS GuardDuty and Microsoft Defender for Cloud provide capabilities for monitoring cloud resources, detecting suspicious API calls, and ensuring container security. In containerized infrastructures, IDS modules integrated with Kubernetes Container Network Interface (CNI) technologies are being actively developed. These modules enable monitoring of traffic between microservices and detection of lateral movement activities within container ecosystems. Furthermore, to prevent packet loss in high-speed networks, technologies such as DPDK (Data Plane Development Kit) and FPGA (Field Programmable Gate Array) are increasingly utilized. These technologies make it possible to analyze traffic at speeds exceeding 100 Gbps with minimal latency. Consequently, modern IDS/IPS systems are becoming capable of processing massive volumes of data streams in real time [11-14].

practical challenges and future research directions

Although modern IDS/IPS systems have become essential components of cybersecurity infrastructures, their practical deployment and efficient operation still involve numerous technical and organizational challenges. The rapid growth of network traffic volume, the widespread adoption of encrypted communications, the emergence of sophisticated multi-stage attacks, and the evolution of artificial intelligence-driven threats have introduced new requirements for intrusion detection technologies. Consequently, contemporary research is focused not only on improving detection accuracy but also on enhancing system adaptability, scalability, and automated response capabilities.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 05 Pages: 19-30
OCLC – 1368736135

False Positives and Detection Accuracy Balance. One of the major challenges of IDS systems is maintaining an appropriate balance between False Positive rates and detection accuracy. Highly sensitive systems may successfully identify a large number of threats; however, this often increases the probability of legitimate traffic being incorrectly classified as malicious. Conversely, excessively strict threshold values may cause certain real attacks to remain undetected.

This challenge becomes even more complex in high-speed real-time network environments. Therefore, modern IDS/IPS platforms increasingly utilize dynamic thresholding, contextual correlation, and risk-based prioritization mechanisms. These approaches reduce false positives by considering the contextual characteristics of security events rather than relying solely on static detection rules.

Challenges of Encrypted Traffic Analysis. A significant portion of today's Internet traffic is transmitted through encrypted protocols such as TLS 1.3 and QUIC. This significantly reduces the effectiveness of traditional IDS systems based on Deep Packet Inspection (DPI) and payload analysis. In particular, the widespread adoption of HTTPS has made it increasingly important to detect malicious activities without directly accessing packet contents. To address this issue, modern IDS platforms employ techniques such as JA3/JA4 fingerprinting, flow-based traffic analysis, and SNI/ALPN metadata inspection. In addition, endpoint agents are increasingly used to strengthen host-level monitoring and enable the detection of malicious activities occurring within encrypted sessions.

Adversarial Machine Learning Threats. With the growing use of artificial intelligence and machine learning technologies in IDS systems, adversarial machine learning threats have also become a major concern. Attackers may intentionally manipulate network traffic by injecting noise, fragmenting packets, or modifying traffic patterns in order to deceive AI models and force incorrect classification decisions.

As a result, malicious traffic may be incorrectly interpreted as legitimate activity. Therefore, the development of robust AI models, Explainable Artificial Intelligence (XAI), and model monitoring technologies has become one of the key priorities in current cybersecurity research. In particular, XAI systems provide interpretability for AI decision-making processes, enabling security analysts to better understand and investigate detected threats.

Scalability and Real-Time Processing. In high-speed enterprise and service provider networks, the enormous volume of traffic makes real-time packet analysis without packet loss a highly challenging task. Traditional software-based IDS systems often fail to provide sufficient performance in environments operating at 40 Gbps, 100 Gbps, or higher network speeds. To address these limitations, hardware-accelerated architectures, DPDK (Data Plane Development Kit), FPGA technologies, and stream-processing frameworks are increasingly utilized. These approaches enable parallel packet processing, ensuring high throughput and minimal latency. Furthermore, microservice-based and distributed architectures are expanding the possibilities for horizontal scalability in modern IDS deployments.

XDR and Automated Response Systems. Traditional IDS systems were mainly limited to threat detection and alert generation. In contrast, modern Extended Detection and Response (XDR) platforms integrate detection, analysis, and automated response mechanisms into a unified

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 05 Pages: 19-30
OCLC – 1368736135

ecosystem. These platforms operate in conjunction with SOAR (Security Orchestration, Automation, and Response) technologies. As a result, once a threat is detected, the system can automatically isolate compromised hosts, update firewall rules, block endpoints, or collect forensic evidence. Such automation significantly reduces incident response time and minimizes errors associated with human intervention.

Future Research Directions

Future research in the field of IDS/IPS systems is expected to focus primarily on artificial intelligence, distributed security architectures, and next-generation networking technologies. In particular, federated learning-based decentralized security models allow multiple organizations to collaboratively train threat detection models while preserving data privacy.

In addition, anomaly detection within encrypted traffic using non-cryptographic metadata and flow-sequence analysis is considered one of the most promising research directions. Developing adaptive and dynamic risk-based IDS systems aligned with the Zero Trust security model is also becoming an important requirement in modern cybersecurity.

Looking ahead, the advancement of quantum computing technologies will further increase the importance of network monitoring in the context of post-quantum cryptography and quantum security. This development will require IDS/IPS systems to adapt to new cryptographic protocols and quantum-resistant security mechanisms.

Conclusion

Intrusion Detection Systems have become an integral component of modern cybersecurity infrastructures. Early statistical and rule-based approaches have evolved significantly and are now enhanced with artificial intelligence, behavioral analytics, and distributed architectures. Modern IDS/IPS technologies are designed not only to detect attacks, but also to automatically mitigate threats, predict malicious activities, and improve overall network resilience. In the future, IDS systems are expected to become more autonomous, transparent through Explainable Artificial Intelligence (XAI), and tightly integrated with Zero Trust security principles. For both researchers and practitioners, combining open-source security solutions with AI-driven modules, improving encrypted traffic analysis techniques, and developing federated security models remain highly relevant and promising research directions.

Acknowledgment. This article was prepared within the framework of the practical research project entitled “Development of Network Attack Detection and Protection Mechanisms in Information and Communication Systems Based on Intelligent Methods” under project number AL-9224104800.

References

1. Hoque N., Bhuyan M.H., Baishya R.C., Bhattacharyya D.K., Kalita J.K. Network attacks: Taxonomy, tools and systems. Journal of Network and Computer Applications, 2014, Vol. 40, pp. 307–324.
2. Al-Sada, B., Sadighian, A., & Oligeri, G. (2024). MITRE ATT&CK: State of the art and way forward. ACM Computing Surveys, 57(1), 1-37.
3. Syafril, W. I., Arifwidodo, B., & Pranindito, D. (2024, November). Analysis Of Intrusion Prevention System (IPS) On Software Defined Network (SDN) In Preventing Distributed Denial of Service (DDoS) Attacks. In 2024 IEEE

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 05 Pages: 19-30
OCLC – 1368736135

International Conference on Communication, Networks and Satellite (COMNETSAT) (pp. 759-765). IEEE.

4. Vierino, F. T., Wahanani, H. E., & Junaidi, A. (2026). Evaluating Web Application Security Using OWASP Top 10 and NIST SP 800-115. bit-Tech, 8(3), 3754-3764.
5. Sharma, N., & Arora, B. (2025). Machine Learning and Deep Learning Models for Anomaly Intrusion Detection in Networks: A Systematic Review. SN Computer Science, 6(7), 832.
6. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, 2(1), 20.
7. Somasundaram, S., & Abraham, S. (2021). Machine learning based intrusion detection systems: A review. Computers & Security, 103, 102187.
8. The Zeek Project. (2024). Zeek Network Security Monitor Documentation. https://docs.zeek.org/
9. Open Information Security Foundation (OISF). (2024). Suricata User Guide. https://docs.suricata.io/
10. Wazuh, Inc. (2024). Wazuh: Open Source XDR. Open Source SIEM. https://wazuh.com/
11. National Institute of Standards and Technology. (2012). Guide to Intrusion Detection and Prevention Systems (IDPS) (SP 800-94).
12. MITRE. (2024). ATT&CK Framework. https://attack.mitre.org/
13. Wang, Y., et al. (2022). Adversarial attacks on network intrusion detection systems: A survey. IEEE Transactions on Information Forensics and Security, 17, 3451–3466.
14. 14. European Union Agency for Cybersecurity (ENISA). (2023). ENISA Threat Landscape 2023.