INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue IV, April 2025

A Review of Intrusion Detection System: Methodology, Classification

Yousef Abuadlla[1,*]

[1] Faculty of Electrical Engineering, University of Al-Jafara, Al-Zahra, Libya.

DOI : https://doi.org/10.51583/IJLTEMAS.2025.140400039

Received: 15 April 2025; Accepted: 22 April 2025; Published: 07 May 2025

Abstract: An Intrusion Detection System is the process of monitoring events within a computer network and analyzing them for unusual behavior. Moreover, IDS detects attempts at misuse, whether by authorized users or external parties who seek to abuse privileges or exploit security vulnerabilities. Computer intruders, who can be found across the internet, pose a significant threat, making it challenging to ensure that information systems are secure and maintained in a safe state throughout their lifetime and use. Intrusion Detection Systems can be software or hardware products designed to monitor system usage and identify any signs of an insecure state. This paper aims to review the methodology of intrusion detection systems and their classifications, summarizing the advantages and disadvantages of the most used approaches.

Keywords: Intrusion detection, host-based, anomaly detection, misuse detection, network-based intrusion detection

1. Introduction

In an era dominated by unprecedented digital transformation, the ability to safeguard sensitive information has become a paramount concern for organizations worldwide. The rise of cyber threats necessitates advanced mechanisms that can detect intrusions and respond preemptively to mitigate potential damage. An Intrusion Detection System (IDS) is a critical component in the cybersecurity framework, functioning through various techniques to identify and analyze suspicious activities within a network. Computer networks have rapidly expanded over the past decade. Furthermore, the use of computers in homes and businesses has significantly increased. Consequently, security has become a crucial concern for all networks and computer systems in today's enterprise environment. The internet, like many other tools, has both advantages and disadvantages. It provides access to numerous beneficial resources, but it also exposes devices to various harmful threats. Hackers and intruders have successfully targeted the networks and systems of many companies. In light of the growing security risks we face, it's heartening to see that many thoughtful solutions have been created to safeguard our system infrastructure and ensure secure communication over the internet. These efforts reflect a collective commitment to protecting our digital lives and nurturing a safer online environment for everyone. These include firewalls and encryption [8], [17]. Intrusion detection systems are a relatively new technology in intrusion detection methods that have emerged in recent years. The growth of maliciIn light of the growing security risks we face, it's heartening to see that many thoughtful solutions have been created to safeguard our system infrastructure and ensure secure communication over the Internet. These efforts reflect a collective commitment to protecting our digital lives and nurturing a safer online environment. Our software presents a significant challenge in the design of intrusion detection systems.

In today's digital landscape, cyberattacks have evolved into highly sophisticated threats. The biggest hurdle we face is detecting unknown and cleverly concealed malware that can slip through traditional defence. Furthermore, there is a surge in security threats, particularly with the alarming rise of zero-day attacks. These insidious threats are specifically designed to exploit vulnerabilities and put internet users at serious risk [19]. This highlights the need for advanced security measures to detect and prevent sophisticated threats, ensuring users' safety in an increasingly digital world. Intrusion detection involves monitoring the events occurring within a computer system or network and analyzing them for signs of unauthorized access. The primary goal is to ensure the integrity, confidentiality, and availability of important information are effectively protected.

An Intrusion Detection System (IDS), as shown in Figure 1, collects and analyzes information from various computer or network components to identify potential attacks [18]. It plays a crucial role in an overall security strategy by complementing other security technologies and providing valuable insights for management. The primary function of an intrusion detection system is to identify attacks and notify users of new, unforeseen threats. This is achieved through continuous monitoring and analysis of events occurring within a computer system or network, regardless of whether the threats originate from internal or external sources [3].

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue IV, April 2025

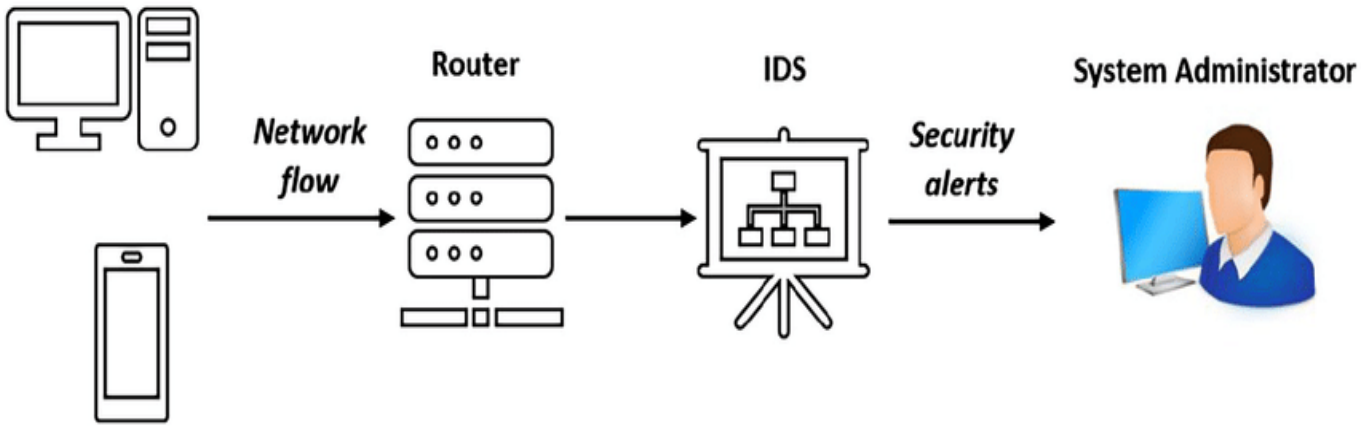

Figure 1. An intrusion detection system

The primary goal of an Intrusion Detection System is to identify various types of malwares as early as possible, a task that traditional firewalls cannot accomplish. As the prevalence of computer malware continues to surge, the necessity for an advanced intrusion detection system has become more crucial than ever. These sophisticated systems are essential for identifying, monitoring, and responding to potential security threats in an increasingly complex digital landscape. In recent periods, machine learning techniques have been utilized to enhance intrusion detection effectively. Therefore, there is a significant need for an updated and thorough classification and overview of recent developments in this field. Many researchers prominently rely on the KDD-99 [10] or the DARPA data set [5] to confidently assess and affirm the use of an intrusion detection system. However, there is no definitive answer regarding which data mining techniques pack the most punch when it comes to effectiveness. Additionally, the time required to build an IDS is often overlooked in evaluating various intrusion detection system techniques, even though this factor is crucial for the effectiveness of online IDSs. In recent years, numerous studies have been published, highlighting the growing importance of this field. The frequently cited survey by Debar [8] examined many approaches to detection techniques that rely on the behavior of attacks. In survey conducted by Axelsson, various intrusion detection systems were categorized by their unique detection methods [20]. Liao classified intrusion detection systems into five subclasses according to their characteristics: Pattern-based, Rule-based, and static-based. Heuristic-based and State-based [13]. Ahmed, on the other hand, focuses on techniques for network anomaly detection systems [14]. The evolution of cybersecurity has necessitated robust solutions that can effectively monitor and defend against many threats targeting network infrastructures. Intrusion Detection Systems (IDS) are pivotal in this landscape, functioning to detect unauthorized access or anomalous behavior within systems. These systems analyze network traffic and system logs to identify suspicious activities, thereby acting as a critical line of defense against cyber threats such as advanced persistent threats, which have been increasingly prevalent in recent years. As highlighted in the existing literature, effective deployment of IDS can significantly enhance an organization's situational awareness and provide actionable insights necessary for timely responses to incidents. Furthermore, the integration of IDS with emerging technologies, particularly in cloud and fog computing environments, underscores their adaptability and importance in maintaining security across diverse platforms. Organizations must prioritize IDS within their cybersecurity frameworks to mitigate risks effectively and safeguard their digital assets [22]. This survey aims to provide comprehensive insights into the evolution, methodologies, and practical implementations of IDS, exploring their effectiveness across diverse environments. By surveying contemporary approaches—ranging from signature-based detection to anomaly detection—this research will underscore the importance of staying ahead in the ever-changing threat landscape. Consequently, understanding the nuances of IDS deployment and functionality is integral to enhancing an organization’s cybersecurity posture and ensuring data integrity in a connected world.

This paper addresses the following topics: Methodologies of intrusion detection systems, classification of intrusion detection systems, available intrusion detection datasets, and finally, the conclusion.

Methodologies of Intrusion Detection Systems

Intrusion Detection System technologies employ various methodologies to detect incidents. The most common types are Signature-based and Anomaly-based detection, which can be used individually or in combination to achieve broader and more accurate detection.

Signature-based Intrusion Detection System

As shown in Figure 2, signature intrusion detection systems use pattern-matching techniques to identify known attacks, also called misuse intrusion detection. [11]. The pattern-matching technique is employed to detect known previous intrusions. Signature-based detection is a well-established method for identifying malicious activities. It examines network traffic, compares it to known signatures, and generates an alert when a match is found. Our primary goal is to create a robust and comprehensive data set of intrusion signatures. This dataset will be used to compare current activities against established signatures to potential threats. If a

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue IV, April 2025

match is identified, an alarm will be triggered to alert the relevant parties. A signature intrusion detection system typically provides high detection accuracy for known intrusions. However, the signature intrusion detection system struggles to identify zero-day attacks because there is no matching signature in the database until a signature of the new attack is extracted and stored in the signature database [12]. Unlike anomaly-based methodologies, signature-based systems are easier to deploy because they do not require learning about the environment. This approach works by searching,

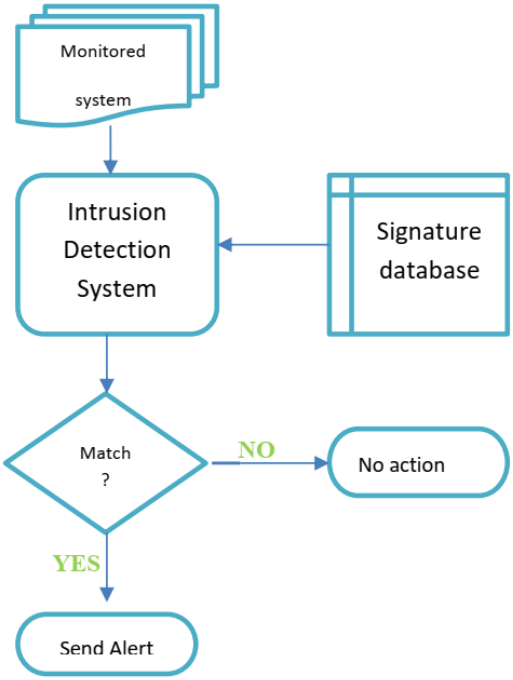

Figure 2. Signature Intrusion System

Inspecting and comparing the contents of captured network packets against known threat signatures. It also compares behavioral signatures with allowed behavior signatures [6]. Signature technique, while effective in identifying known threats, can be easily circumvented by attackers who simply modify recognized attack patterns or exploit vulnerabilities in systems that lack updated signatures to recognize these alterations. This evasion tactic poses a significant challenge, as it demands considerable resources and efforts to keep up with the seemingly endless array of variations that known threats can present. However, one notable advantage of signature-based systems is their relative simplicity when it comes to modification and enhancement; their functionality is primarily dependent on the signatures that are deployed, allowing for straightforward updates and improvements as new threats are identified [9].

Anomaly-based Intrusion Detection System

The anomaly intrusion detection technique, illustrated in Figure 3, is designed to identify traffic anomalies by assessing the extent to which monitored traffic deviates from a predefined normal profile. This baseline profile encapsulates the typical behaviour of the monitored system and is established during the learning period. During this phase, the intrusion detection system acquires knowledge of the environment and formulates a profile that delineates what is regarded as normal traffic for the monitored system. This environment may encompass networks, users, and systems.

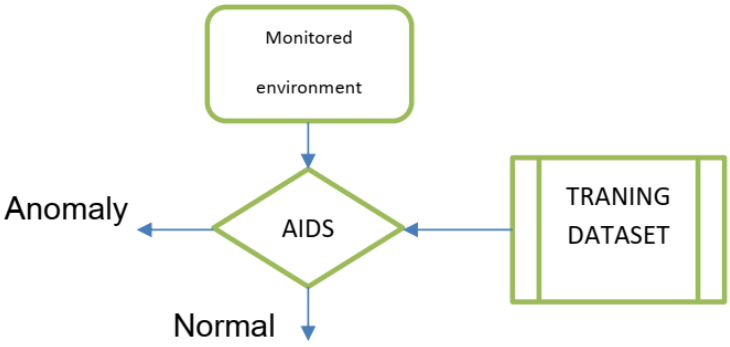

Figure 3. Anomaly Intrusion System

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue IV, April 2025

Anomaly intrusion detection systems have garnered significant interest from researchers because they address the limitations of signature-based systems. An anomaly-based system builds a detailed model that defines the expected behavior of a computer system by employing advanced learning techniques to learn patterns and typical usage over time. It employs precise statistical analysis to identify deviations from the normal, flagging irregularities that may indicate potential threats, by integrating and establishing a knowledge-based methodology. This model serves as a crucial benchmark for normal operations. When the system continuously monitors activities, any significant deviation from the established standard is unequivocally identified as an anomaly that demands immediate attention and action. The development of an anomaly-based intrusion system involves two key stages: training and testing. In the training phase, a detailed profile of normal network traffic is created, analyzing attributes like frequency and packet types to establish a model of typical behavior. In the following testing phase, the system is exposed to a new dataset to evaluate its ability to identify intrusions that were not encountered during training. This critical assessment ensures the system can differentiate between normal traffic and potential threats, thereby strengthening network security. Anomaly intrusion detection systems can be categorized based on the training method, such as statistical, knowledge-based, and machine-learning approaches [1]. The rise of anomaly-based intrusion detection systems offers a promising solution, as these systems aim to model normal behavior in systems or networks and identify deviations as potential threats [11]. Anomaly-based intrusion detection systems face a lot of technological challenges, as highlighted by [16]. These include high false alarm rates, difficulties in scaling to high-speed networks, and the need for frequent updates to maintain effectiveness. Recent advancements in machine learning and deep learning techniques have greatly enhanced the performance and scalability of these systems, leading to significant improvements in their overall effectiveness [21]. Researchers have investigated different methods to improve the robustness and reliability of anomaly intrusion detection systems. A notable strategy involves the development of hybrid systems that integrate the benefits of both signature-based and anomaly-based detection methods. This approach provides a more comprehensive security solution, effectively enhancing overall protection. Table 1 delineates the distinctions between signature-based detection and anomaly-based detection methodologies. Signature-based detection is limited to identifying known attacks, whereas anomaly-based detection possesses the capability to identify zero-day attacks. Nevertheless, it is important to note that anomaly intrusion detection systems may result in a significantly elevated rate of false positives.

Table 1. Comparisons of Intrusion Detection Methodologies

Detection method	Advantage	Disadvantage
Signature intrusion detection system	Effective in detecting intrusions with minimum false alarms Superior detection of known attacks Identifies breakthroughs instantly	It is crucial to update it regularly with a fresh signature. Unable to identify zero-day threats. Can not detect new deviation of a similar attack.
Anomaly intrusion detection system	It can be used to detect new attacks. Can be used to create an intrusion signature	Encrypted packets cannot be handled High false positive alarms. Needs training

Classification of Intrusion Detection System

When classifying intrusion detection methods, several factors can be considered. The key criteria include the nature of the techniques employed, the specific area within the computer network structure, whether the detection focuses on misuse or anomalies, and the model used for detecting intrusions. Intrusion Detection Systems are clearly categorized into two main types: Host intrusion detection or Network intrusion detection system. Host-based IDS monitors activities on individual computers, while network-based IDS oversees activities within networking environments. Some studies focused on attack detection techniques and categorized them into systems that can identify hybrid attacks, a combination of misuse and anomaly detection models [2]. Additionally, the detection of abnormality attacks can be broken down into several methods, including statistical anomaly tests, artificial neural networks, and data mining techniques aimed at detecting anomalies. Other approaches include immune-based systems for detecting abnormalities [24].

The purpose of classification is to establish a clear and concise statistical framework for comparing intrusion detection systems (IDS) and representing specific technologies within that framework. The ultimate goal of this classification standard is to provide guidance for selecting and deploying IDS technologies that meet the security requirements of individual computer systems or infrastructure components. The intended audience for this classification standard includes multiple sectors, such as critical infrastructure, medical, financial, and military systems, as well as standalone networks in both business and home environments. Sections 3.1 and 3.2 will provide detailed descriptions of host-based and network-based intrusion detection systems.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue IV, April 2025

Host-Based Intrusion Detection System

Host-based intrusion detection was widely utilized in the early 1980s, primarily relying on audit logs to track potentially harmful network activities. While this system is still in use today, audit logs have evolved into more sophisticated tools that enable automated detection and response in real time. A modern package is employed to analyse logs within the host-based system. Host intrusion detection systems can provide real-time logging and react accordingly. Certain host-based systems can monitor port activities and block access to specific private ports, thereby bolstering network security. These systems are specifically designed to monitor the traffic flowing through the server where they are deployed. They meticulously document files and transactions, drawing upon a specialized attack or signature database tailored specifically for that server, allowing them to detect and respond to potential attacks by alerting the system administrator when an unusual attack is detected [3]. Host-based intrusion detection systems (HIDS), as shown in Figure 4, are installed on specialized servers to detect attacks targeting those servers. Their main functions include managing configuration files, monitoring the log files created by the system, examining any deviation that could affect the system's integrity, and preventing malicious activity.

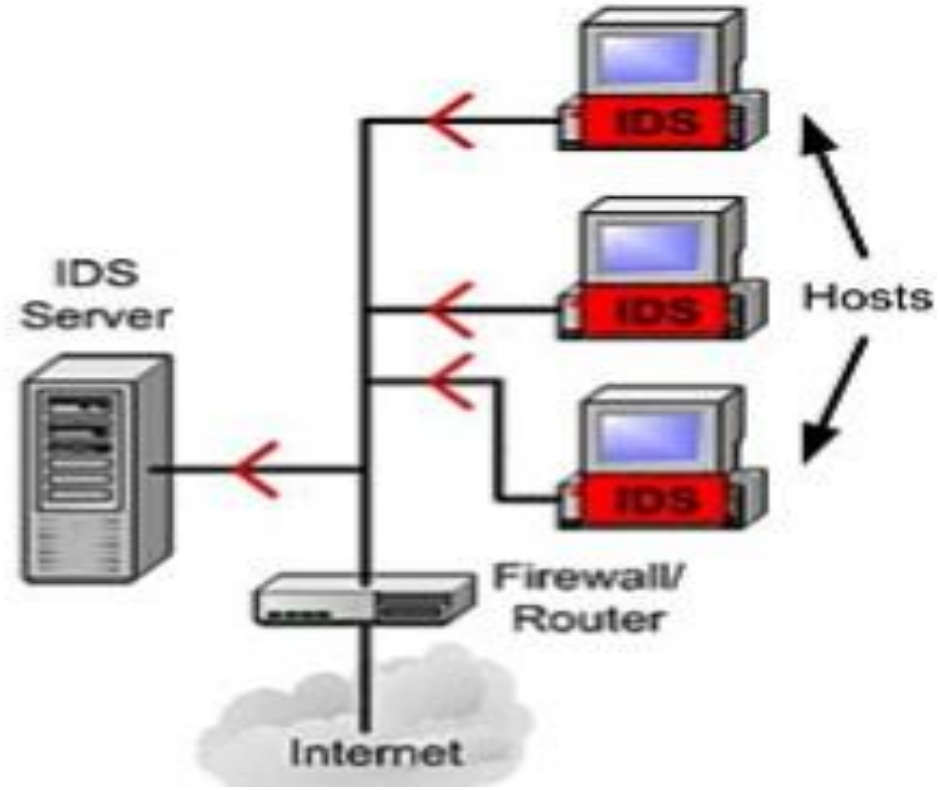

Figure 4. Host-based intrusion detection system

Network-Based Intrusion Detection System

A Network-Based Intrusion Detection System (NIDS) analyzes packets over network connections, focusing on the data portion that may indicate an attack. A network intrusion detection system detects attacks by identifying abnormal patterns or signatures. It generates an alarm to alert users in real time about potential attacks and maintains detailed logs of information related to these incidents after they occur. NIDS provide a comprehensive view of the network traffic passing through a specific segment, serving as a valuable data source for monitoring and analysis. This is typically achieved by enabling the network card's promiscuous mode, allowing it to capture all traffic that passes through it. Traffic originating from other segments of the network, as well as from various types of communication, including telephone lines, cannot be captured or displayed. As shown in Figure 5, the network-based intrusion detection system monitors packets that pass through the network using a sensor. Each packet that arrives at the detector is checked against existing signatures or knowledge [23] to determine the appropriate action. The primary filter is responsible for determining which packets are permitted for processing and which should be either discarded or redirected to the attack recognition module. If an attack is identified, the response module activates an alarm to address the potential threats. For knowledgeable and experienced attackers, the information exchanged, such as alerts, status logs, and the packets between the sensors and monitoring tools, is crucial for carrying out their intrusions. To enhance protection against denial-of-service attacks, it is beneficial to position sensors and viewers on distinct networks. An additional benefit of this configuration is that the network detecting the attack is isolated from the network under surveillance. According to Symantec, intrusion detection systems may produce false alarms that can vary from 10% to 90% based on how well they are tuned and customized.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue IV, April 2025

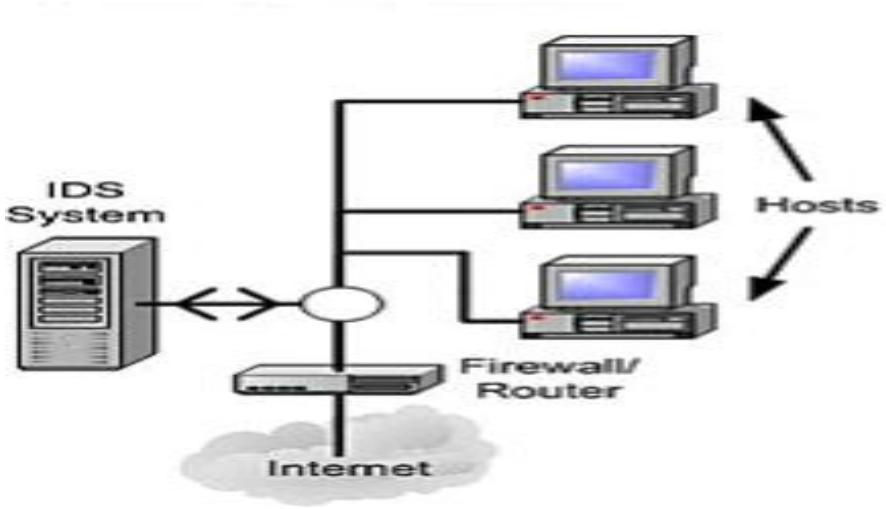

Figure 5. Network-based intrusion system

Comparison of HIDS and NIDS

Host-based Intrusion Detection Systems (HIDS) and Network-based Intrusion Detection Systems (NIDS) are two essential types of intrusion detection systems, each offering unique benefits and challenges. Table 2 provides a comprehensive comparison that highlights their respective strengths and weaknesses, helping to inform better decisions in cybersecurity strategies.

Table 2. Comparison of HIDS and NIDS

	Host-based intrusion detection	Network-based intrusion detection
Scope	Monitors, analyzes the internals of a computing system Focuses on the activities and state of a single host or endpoint	Monitors and analyzes network traffic. Focuses on the data flowing between devices on a network.
Data Sources	Log files. File integrity checks. Configuration changes. User activities.	Network packets and traffic patterns. Protocol analysis. Flow data (e.g., NetFlow, sFlow).
Detection Capabilities	Detects unauthorized changes to system files and configurations. Identifies malicious activities from within the host. Can detect insider threats and compromised user accounts.	Detects suspicious network activities (e.g., port scans, DoS attacks). Identifies malicious traffic patterns and anomalies. Can detect attacks targeting multiple hosts or network services.
Advantages	Provides detailed information about the host's state and activities. Effective at detecting attacks that do not generate network traffic. It can be tailored to the host's specific security policies.	Provides broad visibility into network traffic and activities. Can detect attacks in real-time as they traverse the network. Does not require installation on individual hosts, reducing overhead.
Disadvantages	Limited to the host it is installed on; it does not provide visibility into network-wide activities.	Limited visibility into encrypted traffic unless it is decrypted.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue IV, April 2025

	It can be resource-intensive, potentially affecting host performance. Requires installation and maintenance on each host.	May generate a high volume of alerts, leading to potential alert fatigue. Less effective at detecting attacks that do not generate network traffic (e.g., insider threats).

As presented in Table 2, a Host-based intrusion detection system is best suited for detailed monitoring and protection of individual hosts, particularly for detecting insider threats and host-specific attacks. On the other hand, a Network-based Intrusion Detection System is ideal for monitoring network-wide traffic and detecting external threats that manifest as suspicious network activities. In practice, a comprehensive security strategy often involves deploying both HIDS and NIDS to leverage the strengths of each and provide a layered defense.

II. Conclusion

This paper has presented a comprehensive overview of the key methodologies used in intrusion detection. The two predominant approaches—signature-based and anomaly-based detection—can be deployed independently or in combination to improve detection efficiency. While anomaly-based systems are proficient at identifying novel or zero-day attacks, they often suffer from a high false positive rate. In contrast, signature-based systems are more precise in detecting known threats, with fewer false alarms, but lack the ability to identify new attack patterns. Intrusion Detection Systems (IDS) can also be classified based on their deployment environment as either network-based or host-based. Contemporary IDS often integrate data from both network and host sources to enhance detection capabilities. An effective IDS aims to strike a balance between high detection accuracy and a low false positive rate.

For future research, we intend to conduct experimental studies focusing on the selection of appropriate datasets and applying well-defined evaluation criteria to assess the performance of different IDS approaches.

References

1. Butun I, Morgera SD, Sankar R (2014) A survey of intrusion detection systems in wireless sensor networks. IEEE Commun Survey Tutorial 16(1):266–282.
2. Bai Y. and Kobayashi H., "Intrusion Detection Systems: Technology and Development", 17th International Conference on Advanced Information Networking Applications.
3. Creech G, Hu J, A semantic approach to host-based intrusion detection systems using Contiguous and Discontinuous system call patterns, 2014a, IEEE Trans Compute.
4. D. Herrmann, "A practical guide to security engineering and information assurance", 2002, www.auerbach publications.com.
5. DARPA1998 http://www.ll.mit.edu/IST/ideval/docs/1998.
6. Dorothy, Denning. “An intrusion-detection model,” IEEE Transactions on Software Engineering, Vol. SE-13, No.2. February, 1987.
7. Heberlein, L. etal. "A Network Security Monitor." Proceedings of the IEEE Computer Society Symposium, Research in Security and Privacy, May 1990, pp. 296-303.
8. H. Debar, M. Dacier, and A. Wespi, "A revised taxonomy for intrusion detection systems," in Annales des télécommunications, 2000, vol. 55, no. 7–8, pp. 361–378
9. Justin Lee, Stuart Moskovics, Lucas Silacci, “A Survey of Intrusion Detection Analysis Methods,” CSE 221, University of California, San Diego, Spring 1999.
10. KDDCup1999: http://kdd.ics.uci.edu/databases.
11. Khraisat A, Gondal I, Vamplew P. ‘An anomaly intrusion detection system using C5 decision tree classifier’, 2018, Springer International Publishing, Cham, pp 149–155
12. Kreibich C, Crowcroft J, ‘creating intrusion detection signatures using honeypots’,2004, SIGCOMM Comput Commun Rev 34(1):51–56.
13. Liao H-J , Lin C-HR, Lin Y-C, Tung K-Y,‘Intrusion detection system: a comprehensive review’.2013b, J Netw Comput Appl 36(1):16–24

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue IV, April 2025

14. M. Ahmed , A. Naser Mahmood, and J. Hu, "A survey of network anomaly detection techniques," J Netw Comput Appl, vol. 60, pp. 19–31, 1// 2016
15. Muhammad Nouman [Nafees], Neetesh Saxena, Álvaro A. Cárdenas, Santiago Grijalva, Pete Burnap. "Smart Grid Cyber-Physical Situational Awareness of Complex Operational Technology Attacks: A Review". ACM Computing Surveys, 2022.
16. Patcha, A., & Park, J. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks, 51(12),2007.
17. S. Kiran, "Exploring a novel approach for providing software security using soft computing systems", International Journal of Security and Its Applications, Vol. 2, 2008.
18. S. Alexander, "An anomaly intrusion detection system based on intelligent user recognition", Ph.D. Thesis, Faculty of Information Technology, University of Jyväskylä, Finland, 2002.
19. Symantec, "Internet security threat report 2017," April, 7017 2017, vol. 22 Available: https://www.symantec.com/content/dam/symantec/docs/reports/ istr-22-2017-en.pdf
20. S. Axelsson, "Intrusion detection systems: a survey and taxonomy," technical report 2000
21. S. -i. Kim, N. Nwanze, W. Edmonds, B. Johnson and P. Field, "On network intrusion detection for deployment in the wild," 2012 IEEE Network Operations and Management Symposium, Maui, HI, USA, 2012, pp. 253-260.
22. Victor Chang, Lewis Golightly, Paolo Modesti, Qianwen Xu, Le Minh Thao Doan, Karl Hall, Sreeja Boddu, Anna Kobusińska. "A Survey on Intrusion Detection Systems for Fog and Cloud Computing". Future Internet, 2022, https://doi.org/10.3390/fi14030089
23. Young S. and Aitel D., The hacker's handbook: the strategy behind breaking into and defending networks. CRC Press, 2003.
24. Yang W., Wan W., Guo L. and Zhang L.J., "An Efficient Intrusion Detection Model Based on Fast Inductive Learning", Internation Conference on Machine Learning and Cybernetics.