APEC PUBLISHER

Cybersphere: Journal of Digital Security
ISSN *(Online)*: **3104-6819**
Volume 2, Issue 2, Apr-Jun, 2026, Page 1-16

Review Article Received: 12-04-2026| Accepted: 15-05-2026| Published: 23-05-2026

A Comparative Review of AI-Based and Traditional Intrusion Detection Systems: Challenges, Strengths, and Selection Criteria for Organizations' Security

***Saif S. Kareem*[1], Bashar I. Hameed[2], Humam Khalid Yaseen*[3]**

Abstract

The landscape of cybersecurity has undergone drastic changes in recent years, largely due to the emergence of increasingly complex cyber threats. This paper provides a comparative review of the advantages and disadvantages of AI-based and conventional Intrusion Detection Systems (IDSs), which are software applications used to monitor network or system activities and detect whether they are under attack by viruses, malware, ransomware, or other malicious threats. Traditional IDS has faced a significant challenge for many years, as unknown attacks have continued to occur, despite various approaches proposed to enhance the efficiency of IDS. Despite applying proper measures and secured configurations, many attacks, threats, and malicious activities remain undetected. AI solutions utilize Machine Learning (ML) and Deep Learning (DL) algorithms to enhance detection capabilities and adapt to evolving threats. This review indicates several intrusion detection software schemes. To assist organizations in choosing a suitable IDS. Also consider the necessary selection criteria for organizations evaluating intrusion detection, including the need for a custom approach that can be tailored to their specific requirements.

Keywords

AI-Based Intrusion Detection Systems, Traditional-Based Intrusion Detection Systems, Security Challenges, System Monitoring, Organizational Security Policy.

1Al-Nahrain University, Baghdad, Iraq
2,3Computer Science Department, Al-Imam Al-Adham University College, Baghdad, Iraq

INTRODUCTION

Nowadays, the whole world is connected to the internet. Once a person or organization connects to the network using any Wi-Fi, Ethernet cable, mobile network, or other means, they open themselves up to the world. The data privacy and protection of people only apply if proper measures for user authentication are taken to access the data. For monitoring malicious activities, an IDS was developed. IDS is a software that monitors the network, systems, and devices and alerts the person if any malicious activity is detected [1]. The concept of monitoring was developed by Jim Anderson in 1980 to monitor user activities using logs and computer records [2]. The intrusion of a system is considered a breach of someone's privacy and data, or the misuse of resources [3]. The system's authentication and authorization are compromised by an intruder exploiting flaws in the system architecture [4]. These kinds of activities require some security, which has brought a focus on the rapid growth and profound effect on the security of systems, making it a very challenging part. A perfect IDS system would identify 100% of attacks with 0% false positives, but this is difficult to achieve [5]. Every IDS has its cons, which may lead to security breaches or undetected threats/undetected malicious activities [6]. The concept of a perfect system will never be realized as long as new techniques and technologies continue to evolve on a daily basis. The more effective ways are used to handle new emerging threats and attacks, the more complex the technology becomes [7]. Traditional IDSs were mainly built on signature-based algorithms. It means that previously IDS were built using predefined and known malicious activities. While effective against documented threats, this methodology is inherently limited against novel, polymorphic, or zero-day attacks [7].

***Corresponding Author:** Saif S. Kareem

Traditional methods, such as threshold-based and signature-based detection, are insufficient for effectively detecting zero-day attacks; therefore, AI has been integrated to enhance attack detection. IDS based on AI employs methodologies that utilize algorithms capable of learning from data to detect non-linear and complex patterns associated with intrusions, thereby increasing the detection and identification of previously unknown threats. This technology can sift through massive amounts of data at very high speed, learning over time to anticipate and counter new attack tactics [8].

As technology becomes increasingly sophisticated, malware becomes more complex and undetectable. In 2017, the Australian Cyber Security Centre (ACSC) examined different levels of sophisticated attacks very critically in order to create a good IDS for protection from these kinds of complex attacks [7]. That IDS aimed to change the traditional firewall architecture and build a new architecture to protect against new, sophisticated attacks [9]. Misuse and Anomaly are the two basic types of IDS. Soft computing approaches, such as neural networks, static analysis, and data mining, are used in anomaly detection to detect attacks [5].

As shown in Figure 1, IDS types are [9]:

- Protocol-based Intrusion Detection System (PIDS).
- Application Protocol-based Intrusion Detection System (APIDS).
- Host-based Intrusion Detection System (HIDS).
- Network-based Intrusion Detection System (NIDS).
- Hybrid Intrusion Detection System.

These systems are focused on specific parts to protect that particular part of the system completely. The main focus of this paper is to review a range of intrusion detection software applications, providing a thorough analysis to assist organizations in selecting the most effective solution for safeguarding their systems against cyberattacks.

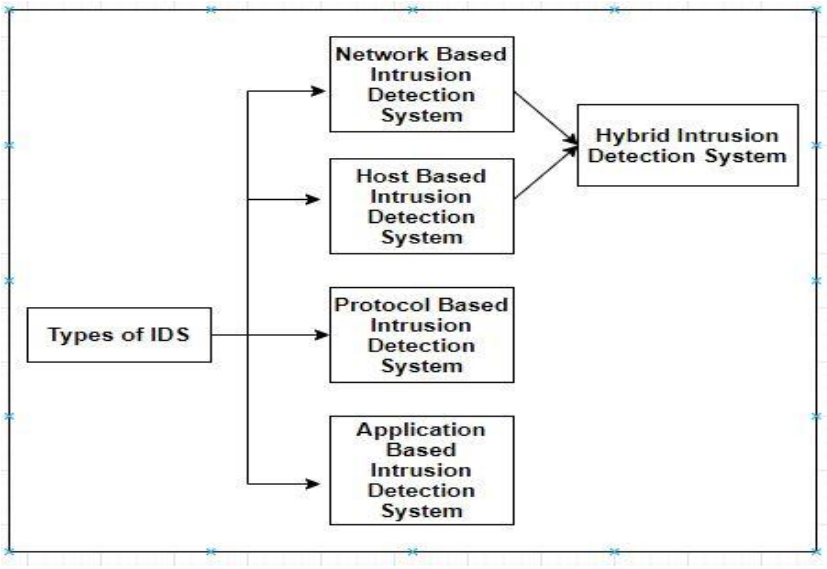

Figure 1. *Types of IDS.*

The paper includes the following sections: Section 2 describes the structure of various types of IDS. Section 3 describes the different approaches to intrusion detection. Section 4 illustrates the intrusion method. Sections 5, 6, and 7 provide a detailed comparative analysis of HIDS, NIDS, and hybrid software. Section 8 presents differences between AI-Based IDS and Traditional-Based IDS. Section 9 describes the IDS selection criteria for organizations. In Section 10, we conclude the paper.

THE STRUCTURAL DESIGN OF VARIOUS INTRUSION DETECTION SYSTEMS

The structure of a particular IDS depends on the area that the organization aims to secure [10]. The incidents that occur cannot be resolved immediately. Only some attacks with a known structure can be fixed. The more complex the structure, the more complicated the task of solving it. It is very important to recognize which type of attack has taken place, as well as to know what structure or method is used to intrude on the system. Some structures require previous data to analyze the attack pattern, and the structures of new attacks can be inferred [9]. Network behavioral analysis (NBA) is done by the Network-based NIDS, which has a specialized hardware appliance with software. The structure of IDS also includes a monitoring port, known as Switched Port Analysis (SPA), also referred to as a mirror port, which is capable of viewing all traffic [5].

The different techniques used by the IDS are Decision Tree (DT) algorithm, random forest, K-Nearest Neighbor(K-NN), clustering and Knowledge Discovery in Databases (KDD), Automatic Dependent Surveillance-Broadcast (ADS-B), Common Path Mining, Epigenetic algorithm, Artificial Neural Network (ANN), Genetic Programming, Fuzzy Inference System for Classification (GPFISClass), Hybrid Cryptography, Real-Time Discrete Event System (RTDES), Discrete Vector Factorization (DVF) in depth learning approach which is used in real time scenarios to detect the intruders as well as the malicious behavioral activities. This section presents the popular structure of different types of traditional and AI-based IDS [11].

Protocol-based Intrusion Detection System

The Protocol-based Intrusion Detection System (PIDS) is installed on a web server that analyzes the protocols in use by the computing system and checks for any deviations from these protocols. It monitors the dynamic behavior of the protocols and consists of a monitoring agent. The agent sits in the frontend in order to analyze the events connected between the devices [12].

Application Protocol-based Intrusion Detection System

This type of IDS tries to check the events and effective behaviors of the protocols. These attacks are usually divided into two categories: intentional attacks and Unintentional attacks. The intentional attacks were carried out to cause harm to the organization. The unintentional attacks are carried out to damage the company financially by deleting its important data [12].

Host-Based Intrusion Detection System

The structure of HIDS consists of the following components, as shown in Figure 2:

- ***Preprocessing Section (PS):*** This section primarily focuses on improving the efficiency of testing techniques. It performs data normalization processing and extracts the required useful information. This section utilizes logs and records from a system to preprocess the data [7].
- ***Intrusion Detection Agent (IDA):*** In the same way as network-based IDS. When problematic activity is detected, an alarm is set. It also records abnormal behavioral situations in logs, which helps with future analysis and predictions [13].
- ***Mobile Agent (MA):*** Role of this agent is to detect an event and if the IDS fails to identify the event and make proper judgements then one or more agents will be sent to the server so that if one host may not accept it but the other hosts will accept the agent and give back the required information from the original host with proper treatment [13].

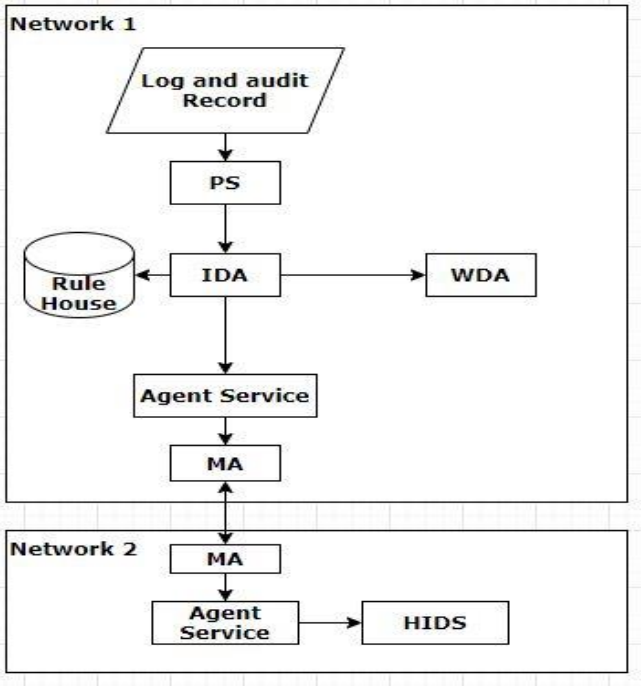

Figure 2. *The structure of HIDS is connected to separate networks.*

Warning Device Agent (WDA)

This device agent's task is to provide an instant response and set the alarm. If the TCP session is disconnected or a process is terminated, an alarm is set. The various types of alarms, for example, include ice alarms and mail alarms [13].

Network-Based Intrusion Detection System

The first and foremost step taken by the NIDS is to extract the features that are to be used for data mining analysis [12]. The structure of NIDS consists of the following components, as shown in Figure 3:

- ***Data Collection Agent (DCA*)**: Its main purpose is to filter packets in the network and analyze them to reduce network flow pressure. Data capture and data filtering are two functions that should be implemented [14].
- ***Protocol Analysis Agent (PAA):*** It is the core of IDS, which utilizes an algorithm for IP layer network intrusion analysis and directs packets to the analysis agent to achieve optimal results [14].
- ***Intrusion Detection Agent (IDA):*** Primarily responsible for system administration, intrusion detection, and data update rules, among other things. After the incursion, the Alarm Agent is recognized and reacts in several ways [14].
- ***Mobile Agent (MA):*** It is used to collect data from an IDS and to provide an interactive interface for interacting with code written for a mobile device very closely [12].

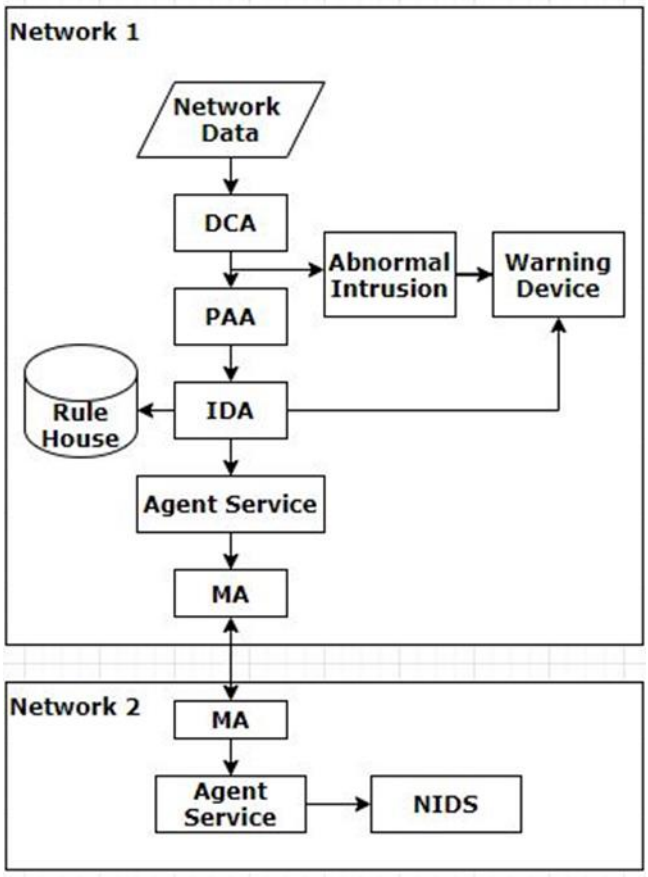

Figure 3. *The structure of NIDS is connected to separate networks.*

APPROACHES OF INTRUSION DETECTION

The approach of every intrusion is different, using various methodologies and algorithms to bypass/trespass any system or network [7]. Some of the approaches are mentioned below for better understanding:

Misuse/Signature-Based Detection

Misuse detection systems are also known as Signature-Based intrusion detection systems (SIDS) and knowledge-based detection systems. It is a type of detection in which attack patterns are learned, as well as any suspicious behavior or unauthorized access patterns, and predictions are made within the network [15].

Misuse detection technique usually gives excellent and accurate detection for previously known intrusions. The dataset is trained using machine learning methods according to its labels. This method detects the invader by automatically retaining its signature. Misuse detection techniques are generated automatically, and the process is more complex and precise than if it were done manually. These patterns can consist of data payloads, unauthorized activities, packet headers, improper File Transfer Protocol (FTP) initiation, or failed Telnet login attempts. This technique has a drawback, i.e., it is unable to detect unknown threats [15]. The traditional approach of misuse detection systems involves examining network packets and attempting to match them with previously known attacks in the database. However, there is a flaw in this system. Zero-day attacks are increasing daily. It has rendered the performance of the Signature intrusion detection systems (SIDS) as no prior signature of the attack exists. The polymorphic variants of malware reduce the accuracy and effectiveness of this system. Since different people have varying levels of design knowledge regarding cybersecurity structures, there will always be inaccurate and

incomplete IDS measures for network protection[16].

Anomaly/Statistical Detection:
Outliers are data patterns that perform abnormally, and oddities or exceptions are data patterns that function strangely. Anomaly detection is a technique for identifying unusual patterns and flagging them as potential security threats or intrusions. Static and dynamic anomaly detectors are the two types of anomaly detectors. The primary advantage of the anomaly detection system is to identify zero-day attacks and notify the organization of any abnormal activity. The system is developed in two phases: the first is the training phase, where traffic is analyzed to determine whether it exhibits normal behavior. The second phase consists of a testing phase, where a new dataset is created to establish the system's capacity to regularize previously unseen intrusions [17].

A static anomaly detector is intended to be a part of the monitored system that remains unchanged. System data and system code comprise the static section of the program. A binary bit can be used to represent the system's static components. If there is any deviation from its original form, the problem has been detected or the intruder/burglar has rearranged the system component. System behavior is incorporated in the dynamic detector. The system's behavior is defined as a series of events. IDS, for example, uses audit data generated by the OS to define specific events of interest [18].

TYPES OF INTRUSION METHODS

Every single attacker has their own methods and techniques for intrusion. Malicious activities are only detected if the IDS is aware of a particular technique. Otherwise, the IDS fails to detect and respond to unknown attacks, and an AI-based IDS provides a solution to this problem [19]. The following are some types of intrusion methods:

Asymmetric Routing
In a network, a packet travels via a single specified path. However, in asymmetric routing, the scenarios are different. The packet takes more than one path; i.e., in many cases, the packet flows from a higher security domain to a lower security domain and vice versa [20].

Buffer Overflow Attacks
In this type of attack, the primary motive of the attacker is to expose the data or information of a particular server, system, or organization. The code which has been written by a developer always has some defects. These defects are found by a hacker in order to manipulate the coding errors and to damage the execution path and expose the data. It is usually aimed for flooding the network to make it inaccessible for the organization or users [20].

Common Gateway Interface Scripts
Common Gateway Interface (CGI) scripts are mainly used to access the information which has been stored on the server. This is a type of attack in which the attacker tries to store the script on the server and when the user interacts with the server that script has been developed in such a way that the user gets a specific response. These scripts are very intelligent in order to detect the particular information as well as it verifies the authenticity of the users. Most of the servers have a directory named 'cgi-bin' which stores the cgi scripts. These scripts are used for calling other applications on the server but it could also be misused by some people [20].

Protocol-Specific Attacks
These attacks occur on targeted devices whose ports are open or whose services are not properly secured. For example, an Address Resolution Protocol (ARP) does not authenticate messages, which gives the attackers a way to perform a Man-in-the-middle attack. In these scenarios the protocols like TCP/IP, ICMP, UDP, ARP, etc. give a way of entering the applications or web servers to the attackers. So, it should be monitored continuously in order to prevent information leakage [20].

Traffic Flooding
This attack is generally known as a DDoS attack, in which the attacker tries to flood the network with useless packets, which causes the application or processor to process more things. It leads to

exhausted processing power and can result in the failure of the application or a delay in the application processes. It can also stop other processes running on the server/client PC [20].

Trojans

The Trojans are a form of malicious code whose sole purpose is to take control of the target machine and then manipulate the data on it. It usually attempts to delete or lock the data using a passkey. It can also grant remote access to the target machine to an attacker as soon as the trojans are executed on it [20].

Worms

A worm is a type of virus that self-replicates and spreads throughout an entire connected network. It utilizes a very large amount of bandwidth as well as memory. Once the worm starts spreading, it often affects individual systems, causing overloading and resulting in the systems crashing or stopping their response [20].

COMPARATIVE ANALYSIS OF HIDS SOFTWARE

The surge in cyberattacks has driven significant advancements in the field of HIDS. Several HIDS software-based solutions are designed to identify malicious activities within an organization's network infrastructure. HIDS operate by continuously monitoring system calls, network traffic patterns, and file system interactions, comparing these observations against predefined patterns and anomalies. The following are some types of HIDS software:

OSSEC

It is a log analysis/ log inspection tool, divided into two parts. The first part consists of a log collector, and the other part consists of an analyzer. The analyzer mainly decodes, classifies, and filters the data. As soon as any event occurs, it reads the data and processes it to identify threats or any malicious activity [21]. This software provides full host-based intrusion detection support for Linux, Debian, Solaris, BSD, AIX, HP-UX, Windows, Mac, and VMware ESX [21, 22].

Sagan

It is a log analysis engine that has a high performance for log analysis. The correlation engine runs on systems such as FreeBSD, OpenBSD, Linux, etc. This software is written in the C language and utilizes a multithreaded architecture, which ultimately delivers high performance. It generally maintains compatibility with rule management software, such as Pulled Pork and Oinkmaster, etc. It also correlates the log analysis with the software, such as Snort and Suricata [21, 22].

AIDE

AIDE (Advanced Intrusion Detection Environment) is an integrity checker for files and directories. It features several message digest algorithms used to verify the file's integrity. Inconsistencies can be found in all of the standard file attributes. It can read database information from both previous and current versions. For more information, consult the distribution's manual pages [21].

Fail2Ban

It is primarily used to block IP addresses associated with attackers. If any unauthenticated user tries to access the network, it detects and then blocks that user from accessing the network. It supports IPv4 and IPv6. As soon as the abusive IP is detected, it is stored in the 'hosts. deny' table of the software. This function helps to reject the IP addresses of attackers [21].

Samhain

It is both a file integrity checking tool and a log analysis tool. It also detects rootkits, rogue set-user-identifier (SUID) executables, and any hidden processes. This software also does port monitoring. This is a multiplatform open-source software. It is primarily developed for Portable Operating System Interface (POSIX) systems, such as Cygwin/Windows, Unix, and Linux [21].

ManageEngine

IDS/IPS security reports generated by the Event Log Analyzer of ManageEngine utilize previous data on network attacks, including information on the most common assaults and the sources of these attacks [22].

Cybersphere: Journal of Digital Security
ISSN *(Online)*: **3104-6819**
Volume 2, Issue 2, Apr-Jun, 2026, Page 1-16

Review Article Received: 12-04-2026| Accepted: 15-05-2026| Published: 23-05-2026

Table *1* presents a comparison of HIDS on various platforms along with their prices. Each software has a name, supported platform, type of IDS, support for authentication, authorization, auditing, data encryption, and a stable price version.

Table 1: *Comparison of HIDS on various platforms along with their prices.*

Tool Name	Platform Supported	Type of IDS	Support authenticat-ion	Support authori-zation	Support auditing	Support data encrypt-ion	Price	Stable Version
OSSEC	Unix,Linux, Mac-OS	HIDS	Yes	Yes	Yes	Yes	$50 per agent.	3.6.0
Sagan	Linux	HIDS	Yes	Yes	No	Yes	Free	2.0.1
AIDE	Unix,Linux, Mac-OS	HIDS	Yes	Yes	Yes	Yes	Free	0.17.4
Fail2Ban	Unix,Linux, Mac-OS	HIDS	Yes	Yes	Yes	Yes	Free	0.11. 2
Samhain	Linux	HIDS	Yes	Yes	Yes	Yes	Free	4.4.9
Samhain	Unix, MacOS	HIDS	Yes	Yes	No	Yes	Free	4.4.9
ManageEngine	Windows Server or Linux	HIDS	Yes	Yes	Yes	Yes	Free	12.6

Comparative Analysis of NIDS Software

IDS/IPS security reports generated by the Event Log Analyzer of ManageEngine utilize previous data on network attacks, including information on the most common attacks and their sources. Table 2 presents a comparison of HIDS on various platforms along with their prices. Each software has a name, supported platform, type of IDS, support for authentication, authorization, auditing, data encryption, and a stable price version:

Solarwinds

It is a Security Information and Event Management (SIEM) tool that provides a 24/7 view of the network. It can minimize the time required to demonstrate compliance reports. This software uses tools such as PCI-DSS, SOX, HIPAA, etc. It has various pre-built connectors for gathering logs [21].

Zeek (AKA: Bro)

Zeek is an open-source tool in the digital security world. Vern Paxson began the development of 'bro' software in the 1990s to understand the networks of the University. Later on, it was named "Zeek" in late 2018 [21, 22].Zeek is a software that unobtrusively and quietly watches the network. It is installed on a virtual storage device, cloud, or sensor, so that it is not easily recognized and can monitor everything [21].

Snort

Snort is both an IDS and an IPS. It can be deployed inline, allowing it to track packets in the network and remove them accordingly. The features of Snort include Real-time Traffic Monitoring, packet logging, protocol analysis, content matching, and operating system fingerprinting, among others. It also features various modes, including packet

***Corresponding Author:** Saif S. Kareem

sniffer and packet logger, as well as a Network Intrusion and Prevention Detection System (NIPDS) [21, 22].

Suricata

This platform is IDS, IPS, and network security monitoring (NSM) software, which performs in-depth packet inspection. It also does pattern matching, which is very useful for threat detection and attack detection. Packet Capture (PCAP) processing is also performed in Suricata software [23].

Open WIPS-NG

It is an open-source tool that also features wireless IPS [21]. It consists of three parts:

- **Sensor:** This captures the traffic and sends it to the server for further analysis.
- **Server:** It gets the data from the Sensor and analyzes it. It also responds to attacks and logs all events.
- **Interface:** The Graphical User Interface (GUI) displays information about threats and manages server activities.

McAfee Network Security Platform

- It is an intelligent software designed to provide unmatched protection and superior performance. It also provides a multi-tenant scale as it is an IPS. The software is deployed on site and managed by McAfee [21].
- Features are:
- Advanced malware protection: Identification of signatureless malware with advanced defenses, analysis, and data correlation.
- Performance and scale: 40 Gbps of IPS capacity.
- Cost-effective and flexible deployment.
- Industry reception: It is also recommended by NSS labs.
- Multi-tenant management: Role-based management, which is accessed through APIs, web, or console.

Palo Alto Networks

Its main products are a sophisticated firewall platform and cloud-based options that expand those firewalls to handle other security concerns. The platform features a command-line interface (CLI) for individual management. Additional REST API-based standard tools enable the platform to integrate with third-party management tools. It also features predefined reports that can be edited and exported as CSV files and PDF files [21].

BluVector

BluVector is a machine learning pioneer with over a year of experience using artificial intelligence to detect and track cyber threats. It has been utilized in the US defense sector and has addressed acute problems faced by the US government. It has data from ten years to build its learning engines, which identify threats [21].

Fidelis Network

Fidelis Network is more than just a network visibility solution. It continuously assesses the cyber risks for all assets and communications flowing into, out of, and through the network in order to prepare for the next attack [21]. All the assets on the cloud and on-premise networks should be identified and classified. Analyze risk in real-time with Fidelis Insight's tailored threat intelligence. Examine cyber risk at a high level and provide detailed information on asset classification and status [21].

Hillstone Networks

This software gives high-speed dedicated appliances for the network Intrusion Prevention System (IPS). It also features next-generation firewalls for protection [21]. It only provides security to appliances. It is an expensive software solution for the users. It has sandboxing capabilities for investigative purposes. It also provides features such as URL blocking and anti-spam [21].

Kismet

Kismet is a wireless IDS framework that includes wireless networks and device detectors, sniffers, war driving tools, and wireless IDS. It works with both Bluetooth interfaces and Wi-Fi interfaces. It also works with some Software-Defined Radio (SDR) hardware, such as the Realtek Software Defined Radio (RTLSDR) and other specific hardware components [22].

NSFOCUS
This software is Beijing-based and provides a next-generation IPS with throughput of up to 20 Gbps. Its main problem is that it does not inspect SSL. This software can integrate with threat feeds. It features a database of over 9,000 threat signatures for advanced anomaly detection. It secures webshells and protects against malicious URLs and SQL injection attacks [21].

Trellix (McAfee + FireEye)
The Trellix network security products undergo frequent advancements. The company's extended detection and response (XDR) platform is based on McAfee's Network Security Platform (NSP). There are many false positive responses for harmful site detection. It also negatively impacts network performance. FireEye's protection focuses on anomaly detection. This software also blocks harmful sites and protects against bots and DOS attacks [21].

Trend Micro
This software is available for both physical and virtual appliances. It is deployed in-line on local networks, private clouds, or public clouds. It lacks compatibility for integration with other IPS. It is way more expensive. It uses both signature and anomaly detection analysis techniques. It also scans inbound, lateral, and outbound traffic [21].

Vectra Cognito
Across the cloud platform, Software as a Service (SaaS), federated identity, and data center networks, the Vectra threat detection and response platform gathers packets and records. It connects into the security stack for providing rapid reaction and uses patent security-led AI to uncover and prioritize threats [21].

Z-Scalar Cloud IPS
This software captures all the traffic of on-site, remote or cloud SaaS resources. It only offers SaaS license. Its installation globally and app alignment is difficult [21]. It supports all types of resources like: cloud data, local data. It also decrypts SSL information. This software has unlimited capacity to store. It is supported on iOS, macOS, android, windows and some linux systems [21].

Table 2: *Comparison of NIDS on various platforms along with prices.*

Tool Name	Platform Supported	Type of IDS	Support authent-ication	Support author i-zation	Support auditing	Support data encry pt-ion	Price	Stable Version Release
Solarwinds	Windows	NIDS	NO	YES	YES	YES	Rs 85000/unit	12.4
Zeek (AKA: Bro)	Unix,Linux, Mac-OS	NIDS	NO	YES	YES	YES	$1,075. per month	3.0.0
Snort	Unix,Linux, Mac-OS	NIDS	YES	YES	audit data like log files from computer	YES	$399/sensor	2.9.11.1
Suricata	Linux, Mac-OS	NIDS	YES	YES	YES	SSL encryp tion	$625.00 once a month	Old Stable 5.0
Open WIPS-NG	Linux	NIDS	YES	YES	system logs only	NO	Free	0.1.1
McAfee Network Security Platform	Linux, windows, Mac-OS	NIDS	YES	Not mentio ned	YES	SSL encryp tion	$10,995	1.0.0

Palo Alto Networks	Linux, windows, Mac-OS	NIDS	External(YES)	YES	YES	YES	$9,509.50	10.2
BluVector	Not specified	NIDS	MFA(YES)	YES	YES	YES	Not available	Not mentioned
Fidelis Network	Not specified	NIDS	YES	YES	YES	YES	$78,000+ / year based on GB bandwidth and days of storage	9.4.x
Hillstone Networks	Appliance	NIDS	YES	YES	YES	YES	Perpetual license based on users and functionality	5.5R8F1
Kismet	Linux, OSX, Windows 10 (limited)	NIDS	NO	YES	YES	NO	Free	2021-08-R1
NSFOCUS	Not specified	NIDS	YES	YES	Log audit	YES	Not available	2.16.0
Trellix (McAfee + FireEye)	Appliance or software	NIDS	YES	YES	YES	Full disk encryption	$10,995+	10.7.x
Trend Micro	Appliance or software	NIDS	YES	Not mentioned	YES	YES	Not available	12
Vectra Cognito	Appliance or software	NIDS	YES	YES	Log audit	YES	$10,000+, based on IP addresses	6 . 0
ZScalar Cloud IPS	Windows, MacOS, some Linux, Android, iOS	NIDS	YES	YES	YES	YES	Offers different levels: Business, Transformation, ELA	Not available

Comparative Analysis of Hybrid IDS Software

As the Hybrid IDS is a combination of NIDS and HIDS, it compensates for the limitations of either approach when applied alone. Pattern recognition and response are combined in IDS for HIDS and NIDS, making it stronger in responding to and stopping attacks.

Security Onion

Doug Burks had started this software as an open-source project. It was first developed and deployed in 2008, which was based on Ubuntu/Linux. The major version of this software was based on Ubuntu 16.04. It is limited to Ubuntu systems only. It has its own tools, which are used for the monitoring of systems. It has been downloaded by security teams worldwide more than 2 million times, which helps defend their enterprise systems [21, 22].

CrowdStrike Falcon

Threat intelligence is the cornerstone of any excellent security product, according to CrowdStrike. It is impossible to create a security solution that can identify, detect, and stop the enemy without the capacity to identify an adversary and understand their tools, strategies, and procedures. CrowdStrike has established a world-class intelligence group that feeds information into the product based on this understanding. Falcon Intelligence is now employed by some of the world's most security-

conscious enterprises, which rely on the most up-to-date intelligence to help them defend against attacks ranging from simple malware to sophisticated, nation-state-sponsored, targeted attacks [23].

ManageEngine Log360

ManageEngine Log360 is a Security Information and Event management (SIEM) software for monitoring and managing network security, auditing Active Directory changes, logging devices, and gaining visibility into cloud infrastructures. Log360 is indeed a fully featured log management platform that integrates the functionality of ManageEngine's EventLog Analyzer, Audit Plus, Cloud Security Plus, and Exchange Reporter Plus applications [24].

Table 3: *Comparison of HIDS on various platforms along with prices.*

Tool Name	Platform Supported	Type of IDS	Price	Support authen t-ication ?	Support authori -zatio	Support auditing	Support data encrypt-ion	Stable Release
Security Onion	Linux, Mac-OS	NIDS, HIDS	Free	Yes	Yes	Yes	Yes	16.04
CrowdS-trike Falcon	Windows	HIDS, NIDS	$99.99	Yes	Yes	Yes	Yes	5.21
Manage Engine Log360	Windows Server	HIDS, NIDS	Free	Yes	Yes	Yes	Yes	Not available

Differences Between AI-Based IDS and Traditional IDS

IDSs play a vital role in defending the networks of organizations against cyber threats. Traditional IDS uses pre-defined rules for detection and a signature-based approach to discover threats; they are efficient only against known attacks, but they are incapable of identifying unknown and advanced attacks. In contrast, the AI-driven IDS relies on ML and DL algorithms to process network traffic patterns, which help in identifying the anomalies and unknown attack vectors more efficiently [25]. The key differences between these two approaches are outlined below:

Detection Capabilities:

- Traditional-based IDS often relies on signature-based approaches that match input data against a library of attack signatures. This method is only capable of detecting known threats and may not be able to distinguish zero-day attacks [5].
- AI-based IDS incorporates advanced algorithms such as ML, DL, and ensemble learning to identify a range of known and unknown threats. These systems are efficient in detecting deviations from the normal and predicting pattern attack vectors with greater accuracy [25].

False Positive and Negative Rates:

- Traditional-based IDS commonly have high false alarm rates because they are based on static rules that can misdiagnose legitimate actions as abnormal [7].
- AI-based IDS reduces false positives and negatives by learning from historical data and adapting to new attack methodologies [7].

Scalability and Adaptability:

- Traditional-based IDS is weak when it comes to scaling and coping with changes in its environment, which are common in cloud computing and IoT networks, as it is fixed-based [26].
- AI-based IDS is very flexible and scalable, which makes it an efficient choice for

challenging environments such as industrial cyber-physical systems [26].

Real-Time Detection:

- Traditional-based IDSs tend not to have real-time detection capabilities that can quickly follow a threat [27].
- AI-based IDS monitors (real-time checks and detection) and response processes enable organizations to detect and respond in real-time to incoming threats by utilizing AI-based IDS [7].

The key differences between the application types of AI-based IDS and conventional IDS are summarized in Table 4:

Table 4: *AI-based IDS versus conventional IDS applications.*

Application Type	Traditional IDS	AI-Based IDS
Known Threat Detection	Effective	Highly Effective
Unknown Threat Detection	Ineffective	Highly Effective
False Positive Reduction	Limited	Significant
Scalability	Limited	High
Real-Time Monitoring	Limited	Advanced
IoT and Cloud Environments	Struggles	Highly Adaptable

IDS Selection Criteria for Organizations

Selecting an appropriate Intrusion Detection System (IDS) represents a critical cybersecurity decision that requires careful evaluation of multiple organizational, technical, and financial factors. Due to the diversity of modern threat landscapes and the rapid evolution of signature-based and AI-driven detection engines, there is a need for a comprehensive approach to IDS selection that satisfies the security goals of the organization, utilizes limited resources, and addresses operational constraints. The following are the key criteria for selecting an appropriate IDS.

Technical Infrastructure and Environmental Considerations

Before selecting an IDS, companies must assess their technical infrastructure, network architecture, security environment, and other relevant factors. The proposed generic framework should consider integrating the proposed features with the existing tools, data quality for AI-based systems, scalability, and compatibility of the system. The organizational structure is also relevant: a structured environment is a good target for rule-based IDS, whereas a dynamic environment may require a solution based on adaptive AI [28].

Performance Evaluation Metrics and Quality Assurance:

Effective IDS selection requires clear performance metrics, including accuracy, sensitivity, specificity, and precision, as well as an evaluation of packet processing, resource utilization, and alert handling. Multi-platform testing ensures reliability. One important requirement is to accurately detect intrusion with minimal false positives. AI-based IDSs have achieved high detection rates and been immune to new attack techniques when combined with ML and DL techniques, in contrast to traditional signature-based methods. Nevertheless, their efficiency relies deeply on the quality and diversity of training data [29].

Organizational Requirements and Resource Constraints:

Selection of an IDS has to take into consideration, regulations and audit standards and industry-specific imperatives, moreover, internal constraints of available resources such as budget, infrastructure and personnel knowledge. Total cost of ownership, training requirements, and integration with the current security operations are central. Effectiveness and value of IDS are influenced by organizational structure and decision processes [30].

Strategic Alignment and Future-Proofing Considerations:
The selection of IDSs must be consistent with the security goals of the organization (Threat Detection, Compliance, Usage). Factor in system flexibility, advancement routes, AI and complexity. Evaluate vendor R&D, update frequency, and integration potential to ensure the IDS remains effective against evolving threats and supports future security needs [30].

Adaptability and Scalability:
Contemporary organizations require IDSs that can adapt to dynamic network environments and evolve with the organization. IDS AI-based systems are excellent at learning new things and adapting to new threats, which makes them more well-suited in a dynamic infrastructure. Traditional IDSs, on the other hand, may have the drawback of requiring manual updates and may struggle to cope with new attack paths [31].

Resource and Maintenance Requirements:
AI-driven IDSs typically require more resources in terms of computation and maintenance due to their complexity and frequent updates. If the organization does not have a very strong IT resource base, it may not want to make the move if there are a couple of traditional IDS-type solutions available, which might be less taxing on resources (yet more limited in terms of protection against newer, more sophisticated attacks) [30].

Cost Considerations and Stakeholder Feedback:
Cost is one factor that includes the cost of initial deployment, maintenance, as well as possible operational savings. OSSEC and Snort offer free, open-source intrusion detection, but they do require resources to operate them. PyTupleueny1. With AI-based IDSs, there is usually an upfront cost; however, in the long run, operating costs can be minimized since detection and response are automated. Engage key stakeholders early in the selection process to gather insights on their needs and experiences with previous systems. Their input can help identify priorities and potential challenges [29].

CONCLUSION

IDSs remain a cornerstone of an organization's security posture, and they have evolved from rule-based systems to complex, AI-based solutions. This comparative analysis has illustrated the differences and challenges as well as the potential strengths of AI-based and traditional IDS processes. Traditional-based IDS solutions have a legacy of well-known methods and interpretability, but struggle to cope with new types of attack vectors, as well as high alert volumes. On the other hand, AI-based IDSs are more flexible and capable of detecting threats more effectively, especially against zero-day ones; however, they are still more complex in terms of transparency, data handling, and potential biases introduced with them.

Companies will want to obtain quotations from different vendors, and each vendor will present its IDS as the best option. The performance, response time after every single attack, detection rate, and the number of false positive alerts all matter greatly for the quality checks of an IDS. This paper presents a detailed investigation of intrusion detection systems and their different types. Furthermore, it includes a comparative study of IDS according to the strengths and weaknesses of particular IDS software, which assists organizations in choosing the best security system for their specific needs.

REFERENCES

1. Abdulganiyu, O. H., Tchakoucht, T. A., & Saheed, Y. K. (2024). RETRACTED ARTICLE: Towards an efficient model for network intrusion detection system (IDS): Systematic literature review. *Wireless Networks*, *30*(1), 453–482. https://doi.org/10.1007/s11276-023-03495-2
2. Mohamed, A. B., Idris, N. B., & Shanmugum, B. (2012). A brief introduction to intrusion detection system. In *International Conference on Intelligent Robotics, Automation, and Manufacturing* (pp. 263–271). Springer. https://doi.org/10.1007/978-3-642-35197-6_29
3. Jayaprakash, R., & Uma, V. (2011). Intrusion detection by pipelined approach using conditional random fields and optimization using

SVM. In *International Conference on Advances in Computing and Communications* (pp. 656–665). Springer. https://doi.org/10.1007/978-3-642-22714-1_68

4. Musa, U. S., Chhabra, M., Ali, A., & Kaur, M. (2020). Intrusion detection system using machine learning techniques: A review. In *2020 International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 149–155). IEEE. https://doi.org/10.1109/ICOSEC49089.2020.9215333
5. Hameed, B., AlHabshy, A. A., & ElDahshan, K. A. (2021). Distributed intrusion detection systems in big data: A survey. *Al-Azhar Bulletin of Science, 32*(1-B), 27–44. https://doi.org/10.21608/absb.2021.63810.1100
6. Kareem, S. S., Hameed, B. I., & Yaseen, H. K. (2026). Enhanced mutual authentication scheme for fog computing using blockchain technology. *Journal of Advanced Research Design, 141*(1), 163–188. https://doi.org/10.37934/ard.141.1.163188
7. Alhabshy, A. A., Hameed, B. I., & Eldahshan, K. A. (2022). An ameliorated multiattack network anomaly detection in distributed big data system-based enhanced stacking multiple binary classifiers. *IEEE Access, 10*, 52724–52743. https://doi.org/10.1109/ACCESS.2022.3174482
8. ElDahshan, K. A., AlHabshy, A. A., & Hameed, B. I. (2022). Meta-heuristic optimization algorithm-based hierarchical intrusion detection system. *Computers, 11*(12), Article 170. https://doi.org/10.3390/computers11120170
9. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity, 2*(1), 1–22. https://doi.org/10.1186/s42400-019-0038-7
10. Artail, H., Safa, H., Sraj, M., Kuwatly, I., & Al-Masri, Z. (2006). A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks. *Computers & Security, 25*(4), 274–288. https://doi.org/10.1016/j.cose.2006.02.009
11. Borkar, A., Donode, A., & Kumari, A. (2017). A survey on intrusion detection system (IDS) and internal intrusion detection and protection system (IIDPS). In *2017 International Conference on Inventive Computing and Informatics (ICICI)* (pp. 949–953). IEEE. https://doi.org/10.1109/ICICI.2017.8365277
12. Mandal, S., Sai Sabitha, A., & Mehrotra, D. (2021). Analysis on protocol-based intrusion detection system using artificial intelligence. In *Machine Intelligence and Smart Systems: Proceedings of MISS 2020* (pp. 131–143). Springer.
13. Saxena, A. K., Sinha, S., & Shukla, P. (2017). General study of intrusion detection system and survey of agent based intrusion detection system. In *2017 International Conference on Computing, Communication and Automation (ICCCA)* (pp. 471–421). IEEE. https://doi.org/10.1109/CCAA.2017.8229866
14. Bernardes. (2000). Implementation of an intrusion detection system based on mobile agents. In *2000 Proceedings International Symposium on Software Engineering for Parallel and Distributed Systems* (pp. 158–164). IEEE. https://doi.org/10.1109/RoEduNet.2013.6714184
15. Thankappan, M., Rifà-Pous, H., & Garrigues, C. (2024). A distributed and cooperative signature-based intrusion detection system framework for multi-channel man-in-the-middle attacks against protected Wi-Fi networks. *International Journal of Information Security*, 1–20. https://doi.org/10.1007/s10207-024-00899-9
16. Thankappan, M., Rifà-Pous, H., & Garrigues, C. (2024). A signature-based wireless intrusion detection system framework for multi-channel man-in-the-middle attacks against protected Wi-Fi networks. *IEEE Access, 12*, 23096–23121. https://doi.org/10.1109/ACCESS.2024.3362803
17. Saba, T., Rehman, A., Sadad, T., Kolivand, H., & Bahaj, S. A. (2022). Anomaly-based intrusion detection system for IoT networks through deep learning model. *Computers and Electrical Engineering, 99*, Article 107810. https://doi.org/10.1016/j.compeleceng.2022.107810
18. Zachos, G., Essop, I., Mantas, G., Porfyrakis, K., Ribeiro, J. C., & Rodriguez, J. (2021). An anomaly-based intrusion detection system for internet of medical things networks. *Electronics, 10*(21), Article 2562. https://doi.org/10.3390/electronics10212562
19. Khraisat, A., & Alazab, A. (2021). A critical review of intrusion detection systems in the internet of things: Techniques, deployment

strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity, 4*(1), Article 18. https://doi.org/10.1186/s42400-021-00077-7

20. Moskowitz, R. (n.d.). *Network intrusion: Methods of attack*. Retrieved August 19, 2025, from https://www.rsaconference.com/library/blog/network-intrusion-methods-of-attack
21. Samson, R. (n.d.). *Top 10 intrusion detection and prevention systems*. Retrieved August 29, 2025, from https://www.clearnetwork.com/top-intrusion-detection-and-prevention-systems/
22. Cooper, S. (n.d.). *Intrusion detection systems explained: 12 best IDS software tools reviewed*. Retrieved August 29, 2025, from https://www.comparitech.com/net-admin/network-intrusion-detection-tools/
23. CrowdStrike. (n.d.). *CrowdStrike Falcon*. Retrieved August 29, 2025, from https://www.crowdstrike.com/en-us/products/trials/try-falcon/
24. Log360, M. (n.d.). *ManageEngine Log360, a unified SIEM solution for your SOCs*. Retrieved August 29, 2025, from https://www.manageengine.com/log-management/?camid=18630845953&adgid=145459895929&kwd=manageengine%20log360&matchtype=e&adid=629593428631&network=g&adposition=&loc=1007949&placement=&target=&device=c&gad_source=1&gad_campaignid=18630845953&gbraid=0AAAAAChAr7YEIfzQj6OHSaPG6VczSlQ_h&gclid=Cj0KCQjwn8XFBhCxARIsAMyH8BuZQxMa98l24OFUV-iqd6_FQuwT9iHyHNjiFq9x0D292Pwc5AKR7PwaAj_IEALw_wcB
25. Sowmya, T., & Anita, E. M. (2023). A comprehensive review of AI based intrusion detection system. *Measurement: Sensors, 28*, Article 100827. https://doi.org/10.1016/j.measen.2023.100827
26. Marks, D. G., Mell, P., & Stinson, M. (2004). Optimizing the scalability of network intrusion detection systems using mobile agents. *Journal of Network and Systems Management, 12*(1), 95–110. https://doi.org/10.1023/B:JONS.0000015700.02134.1c
27. Yu, K., Nguyen, K., & Park, Y. (2022). Flexible and robust real-time intrusion detection systems to network dynamics. *IEEE Access, 10*, 98959–98969. https://doi.org/10.1109/ACCESS.2022.3199375
28. Dini, P., Elhanashi, A., Begni, A., Saponara, S., Zheng, Q., & Gasmi, K. (2023). Overview on intrusion detection systems design exploiting machine learning for networking cybersecurity. *Applied Sciences, 13*(13), Article 7507. https://doi.org/10.3390/app13137507
29. Aleksandrova, V., Tasev, I., & Vasileva, V. (n.d.). *Challenges in choosing the type of intrusion detection and prevention system to increase the level of cybersecurity in the organization*. https://doi.org/10.6028/NIST.SP.800-31
30. Mell, R. (2001). Intrusion detection systems. *National Institute of Standards and Technology (NIST), Special Publication, 51*. https://doi.org/10.6028/NIST.SP.800-31
31. Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. In *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)* (pp. 21–26). https://doi.org/10.4108/eai.3-12-2015.2262516

Conflict of Interest: No Conflict of Interest
Source of Funding: Author(s) Funded the Research
How to Cite: Kareem, S.S., Hameed, B. I., & Yaseen, H. Y. (2025). A Comparative Review of AI-Based and Traditional Intrusion Detection Systems: Challenges, Strengths, and Selection Criteria for Organizations' Security. *Cybersphere: Journal of Digital Security, 2*(2), 1-16.