International Journal of Safety and Security Engineering
Vol. 16, No. 4, April, 2026, pp. 879-888
Journal homepage: http://iieta.org/journals/ijsse

A Systematic Review of Modern Intrusion Detection Systems: Challenges, Techniques, and Future Trends for Network Security

Mojda Yahya Qader[1*], Hasan Abdulrahman[2], Mohammad Al-Azawi[3]

[1] Department of Computer Technical Engineering, Technical Engineering College for Computer and AI, Northern Technical University, Kirkuk 36001, Iraq
[2] Department of Cyber Security Technical Engineering, Technical Engineering College for Computer and AI, Northern Technical University, Kirkuk 36001, Iraq
[3] Department of Computing Science, Gulf College, Muscat 133, Oman

Corresponding Author Email: Mojda.yahya25@ntu.edu.iq

https://doi.org/10.18280/ijsse.160415

Received: 18 February 2026
Revised: 15 April 2026
Accepted: 25 April 2026
Available online: 30 April 2026

Keywords:
Intrusion Detection Systems, cybersecurity, DNA-based intrusion detection, machine learning, federated learning, hybrid detection, network security, sustainable artificial intelligence

ABSTRACT

The growing complexity and frequency of cyber threats have led to a shift in the Intrusion Detection Systems (IDS) characteristics from traditional signature-based schemes to the newer, host-adaptive, and intelligence-oriented systems. This work provides a comprehensive and systematic analysis of the state of the recent developments in IDS, with special emphasis on the integration of artificial intelligence (AI), machine learning (ML), and bio-inspired approaches. It evaluates a variety of IDS architectures, such as Host-Based, Network-Based, and Distributed architectures, as well as fundamental detection strategies such as signature-based, anomaly-based, and hybrid approaches. Key issues that have been addressed in this paper include measurement indicators, data limitations, resource optimisation and the issue of encrypted traffic. Additionally, several innovations have been analysed, with a special focus on DNA encoded IDS mechanisms, which exhibit high adaptability and low false-positive rates. This paper guides the architecture of adaptive detection frameworks, sensitive to the emergent systems of infrastructures, including Internet of Things (IoT) systems and cloud services. The key results indicate that AI-assisted and bio-inspired models of IDS, especially the DNA encoding models, exhibit high flexibility and reduced false-positive rates in comparison with the traditional methodologies. These results highlight the growing demands of hybrid, lightweight, and explainable IDS designs that are capable of effectively protecting modern networks, including cloud-centered systems, IoT systems.

1. INTRODUCTION

Cybersecurity has become one of the most significant issues in the modern digital ecosystem. The increased amount of data and the expansion of inter-system communications have significantly increased the vulnerability of computer networks to various forms of cyberattacks. The Intrusion Detection System (IDS) is one of the most significant elements of the modern cybersecurity protection arsenal, as it is designed to track the network traffic, identify abnormalities, and indicate possible security breaches. Intrusion detection can be traced back to the early 1980s when James Anderson suggested the audit of system actions to reveal misuse, and thus provided a conceptual basis for further formal solutions of implicit IDS [1]. In the early days of IDS technologies, rule-based detection was a critical element of the technologies, especially signature-based systems that compared the incoming data to a collection of known attack patterns [2]. Their effectiveness lay in recognizing threats that they had seen before, but lacked the flexibility to recognize those that were new or zero-day attacks.

The limitations of traditional IDSs were also revealed in the context of wireless sensor networks, where it was revealed as difficult to maintain privacy, scalability, and accuracy in the face of advanced and heterogeneous threats [3]. The growing sophistication of cyber threats has led to aparadigm shift to anomaly-based detection systems, which identify irregularities in the standard behavior of network traffic. These systems come with enhanced detection capability against emerging and changing threats. Examples of such attacks include zero-day attacks, which take advantage of undocumented vulnerabilities and may bypass any system that is based solely on signature databases [4].

Artificial intelligence (AI) and machine learning (ML) are other technologies that have been integrated into the developing evolution of IDS. These technologies give IDS adaptive capabilities that gain through the working environment, and hence, they respond more to threats that they are not readily aware of. Decision trees, support vector machine (SVM), and k-nearest neighbors (KNN) are classical ML algorithms that were first used to enhance the performance of IDS [5]. Nonetheless, these models are often difficult to work with in high-dimensional data and could have little dynamism in changing settings [6].

Over the last few years, Deep Learning (DL) models such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) networks have demonstrated increased performance with large amounts of network data with greater detection accuracy and lower false-alarm rates [7, 8]. Such methodologies are a major breakthrough as compared to traditional ML methods as they automatically discover levels of attributes and identify complex patterns of intrusions [9, 10].

The collaboration of IDSs with the cloud environments, the Internet of Things (IoT), and Industrial Control Systems (ICS) generates new concerns, including real-time responsiveness, information integrity, and resource management. Host and network-based IDS providers have their own advantages and limitations, so hybrid options are gaining more popularity to provide full coverage and resistance [4]. Additionally, with the interception of adversarial ML, the new attack vectors have surfaced against AI-based IDSs, whereby malicious inputs are carefully designed to avoid detection [11]. These potentials require the establishment of efficient and resilient IDS systems that have the ability to respond to the changing attack patterns without losing operational efficiency and integrity of systems. Multilayered defence strategies are further enhanced by integrating the detection systems with other security infrastructure components, such as firewalls, Security Information and Event Management (SIEM) systems, and behavioural analytics. Nevertheless, despite these improvements, various IDS models still face challenges such as reliance on labeled data, deployment complexity in decentralized settings, and maintaining low false-alarm rates. Also, application contexts, in particular, IoT and cloud platforms, have their own architecture requirements that cannot be effectively fulfilled by a one-size-fits-all solution [12].

The paper contributes to IDS in several ways. To begin with, it presents a systematic and thorough overview of the new generation IDS methods, such as classical, ML, deep learning, and new bio-inspired methods. Second, it provides a comparative analysis of various IDS techniques, their advantages and disadvantages, and the conditions of use in different settings. Third, the paper addresses the key issues like limitations of the datasets, encrypted traffic, and computational constraints, and presents a coherent view of the gaps in the current research. Lastly, the paper also points out the new developments in DNA-based and hybrid IDS models with their prospective application in the creation of adaptive and efficient intrusion detection solutions.

This paper is organized as follows. Section 1 introduces the topic and outlines the main motivations of IDS. Section 2 discusses the key challenges that affect the efficiency and reliability of modern IDS systems. Section 3 reviews recent research on IDS and presents a structured analysis of IDS approaches, commonly used datasets, and performance evaluation metrics. Finally, Section 4 concludes the paper and outlines potential future research directions.

2. METHODOLOGY OF THE REVIEW

This study is based on a systematic review of the recent research on IDS. The review process is divided into several steps that include theidentification of data sources, search strategy, study selection, and data filtering.

Data Sources: The major academic databases, including Google Scholar, IEEE Xplore, SpringerLink, and ScienceDirect, were searched.

Search Strategy: The search was restricted to the studies published in 2015-2024. These keywords were: Intrusion Detection System, IDS, and Intrusion Detection System Review.

Inclusion Criteria: The studies had to be included due to: Concentration on IDS or other processes. Appeared in peer-reviewed journals or conferences. Make relevant technical, methodological, or analytical contributions.

Exclusion Criteria: The studies were filtered out because they were not directly related to IDS. were duplicated across multiple databases.Lacked sufficient technical description or text.

Study Selection Process: The nature of the search employed led to a very large number of studies retrieved. After eliminating duplicates and sifting the titles and abstracts to eliminate irrelevant studies, a subset of studies was then selected to go through full-text review. Finally, 55 studies that fitted the inclusion criteria were identified for detailed review. To provide a system-level perspective that complements this review, a generalized architecture of IDS is illustrated in Figure 1.

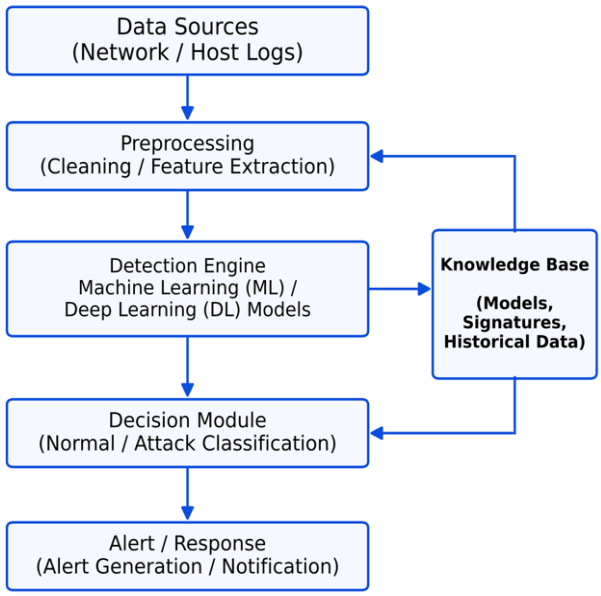

Figure 1. General Intrusion Detection System (IDS) architecture

3. KEY CHALLENGES

Although there has been an advancement in the most recent research on intrusion detection, some essential issues still persist in obstructing the design of completely autonomous and dependable IDS frameworks.

False Positive (FP) and False Negative (FN) rates: In most cases, even the sophisticated models of IDS produce false alerts because the normal behaviour and malicious behaviour resemble. This makes the work of administrators heavier and demeans automated detection systems. Nevertheless, ML-based IDSs continue to have high rates of false alarms and reduced flexibility [9].

Dataset limitations: Common datasets used in the study of IDS, like KDD Cup 99, NSL-KDD, and CICIDS2017. Nevertheless, such datasets do not capture the complexity,

heterogeneity, and dynamism of the modern network environments. Consequently, numerous models of IDS trained on such data sets are not generalized in a successful way when implemented into practice. The success of IDS algorithms strongly depends on the quality of thedatasets to be used during training and testing. The diversity of the features in representation, the characteristics of the classes, and labelling variability may greatly affect the performance of the detection and cause over-fitting or biased models. As indicated in [13], theperformance of the learning algorithm is dependent on the type of data as input. Hence, the different methods of preparing data are used as transformation, normalization, and sampling to enhance data quality. This is why data preparation is important to guarantee consistency. In addition, the situation of data imbalance persists. Most datasets contain large numbers of benign samples, greatly exceeding those of malicious samples, such that an unbiased classifier is biased towards normal behaviour. This inhibits detecting the rare or novel attacks by the system. As stated in [14], the issue of data imbalance and the creation of realistic and dynamic datasets should be among the priorities to enhance the flexibility and longevity of contemporary IDS structures.

Computational cost and consumption of resources: Deep learning-based IDS architectures are very power-consuming and thus cannot be used in edge and IoT devices with small hardware. The models are not easy to implement efficiently in resource-constrained situations because they represent a high resource consumption in terms of calculations [15].

Encrypted traffic: Packet analysis becomes inefficient due to widespread use of encryption, including VPNs, HTTPS, and obfuscation techniques**.** Current studies reveal that the encryption of communications hides important packet characteristics and makes IDS invisible and inaccurate; hence, contemporary systems should use flow-level or metadata-based detection to be effective in encrypted settings [16].

Explainability of IDS models: The more complicated the IDS models become, the more difficult it will be to learn how the decisions will be made by the AI-based system. According to recent studies, explainable AI improves transparency and trust in intelligent IDS by revealing the decision-making process of the model and helping human analysts in the decision-making process

To better understand how recent studies have addressed these challenges, the next section reviews the most influential research on modern IDS approaches.

4. RELATED WORK

The last ten years have seen advancements in the field of IDS due to developments in the areas of non-traditional machine-learning approaches and the emergence of deep learning, hybrid frameworks, bio-inspired techniques, federated systems, explainable AI, and sustainable security systems. A time review will help explain how the different waves of research dealt with various issues and how the relevance of the DNA-based signature encoding concerning modern network contexts increases. To provide a structured overview of the following developments, a chronological summary is presented in Table 1.

Table 1. Intrusion Detection System (IDS) approaches

IDS Approach	Techniques Used	Strengths	Limitations	Relevance / Notes
Signature-Based IDS	Rule matching, pattern databases	Very low false positives; efficient for known attacks	Fails to detect zero-day attacks; requires constant rule updates	Highly reliable in stable environments but limited in dynamic or evolving networks
Machine Learning IDS	Support Vector Machine, Random Forest, K-Nearest Neighbors	Learns statistical relationships; adaptable	Depends on manually engineered features; struggles with temporal patterns	Useful for moderate-scale detection where features are well-defined
Deep Learning IDS	Convolutional Neural Network, Long Short-Term Memory, Autoencoders	Strong feature extraction; effective with encrypted traffic	High computational cost; requires large datasets; low interpretability	Suitable for large networks but impractical for constrained devices
Hybrid IDS	Signature + anomaly detection	Better detection coverage; improved zero-day detection	More complex and costly to deploy	Works well in layered security architectures
Federated IDS	Distributed training across nodes	Preserves privacy; decentralized	Vulnerable to poisoning; model divergence	Effective for IoT/cloud scenarios requiring local data privacy
Bio-Inspired IDS	Amino-acid encoding, genetic algorithms	Pattern-driven, structured representations	Still emerging; limited optimization research	Promising direction for alternative feature encoding
Emerging Sequence-Based Approaches	Symbolic encoding, sequential patterns	Captures temporal/structural behavior	Requires robust mapping strategies	Increasingly relevant as attacks become sequence-based

Foundations and Large-Scale ML (2015–2018): Introduction of TensorFlow [17] allowed training of models in a distributed and scalable way, as well as provided an opportunity to integrate deep-learning methods with the work in IDS. A more recent study investigated the application of DL based IDS on the deployment of IDS in fog-to-things environments, showing that the latency, heterogeneity, and scarce computational resources continue to be strong limitations [18]. These observations further underscore the need to have lightweight, efficient IDS models.

Dataset Issues, Encrypted Traffic, and Explainability (2019–2021): Significant evaluations of IDS data sets [19] indicated that it still had problems such as outdated attack signatures, an imbalance between classes, and anunrealistic traffic model. Since later work [20] prioritized the growing complexity of identifying anomalies in encrypted traffic, where inspection of individual payloads is no longer possible and flow-based characteristics are an essential requirement.

Within environmental sustainability issues, the Green AI framework [21] emerged, emphasizing that the IDS implementation on a large scale requires and needs to be energy-efficient. Explainability issues were also extended in [22] with a call towards making the ML/DL-based IDS models more transparent to enhance security forensics and operational confidence.

Federated, Hybrid, and Representation Learning (2022): To improve privacy protection and support cooperative detection of nodes located in different locations, [23] proposed a hierarchical, blockchain-based federated IDS architecture. An inclusive survey of the methodology for federated IDS [24] identified the following key challenges: model diversification, adversarial poisoning, and communication cost. Hybrid detection frameworks based on the model of representation learning were investigated, and it was shown that combining the rule-based patterns with learned features of anomalies can be used effectively to detect zero-day attacks [25]. Encoding of the traffic flows into symbolic representations, e.g., DNA-inspired sequences, has assisted in creating structured and interpretable intrusion detection models with the use of symbolic rendering techniques [26].

Bio Inspired-Encoding, Concept Drift, and IoT Detection (2023): In 2023, techniques of bio-inspired IDS came along way. The study [27] showed that hybrid bio-inspired processes are capable of enhancing the IoT detection power. Encoding based on amino acids suggested in the study [28] did offer evidence that biologically formatted feature representations are better than traditional numeric vectors, which gives solid grounds to use DNA-based IDS models. The concept drift became an essential issue in the dynamic network environments and led to the emergence of incremental IDS frameworks, which can handle the changing data streams [29]. The lightweight IoT-oriented hybrid optimization models [30] were applied to achieve efficiency-oriented IDS design, and autoencoder-based anomaly detection of encrypted traffic was also considered [31].

Transformers, Deep IDS Surveys, and Explainable Detection (2023–2024): ransformers have also been introduced to the IDS research with TranAD [32], a system that uses attention-based sequence models to extract time-related patterns, as well as detect zero-day attacks. Through a recent survey of deep-learning IDS [33], serious limitations were identified, such as high computational cost, bias in datasets, and poor interpretability. Federated IDS developments included FetFIDS [34], which combined feature embeddings with federated learning to achieve location-independent generalization of heterogeneous devices. Modern explainable IDS surveys [35] highlight the requirement that explainable sequence-level features of DL-based IDS, a feature of which structured DNA-based encoding has natural benefits.

Although IDS have made tremendous achievements, there exist a number of limitations in the current methods. Conventional ML techniques tend to be constrained by relying on engineered features and not being able to efficiently work with high-dimensional and dynamic data. Deep learning models, although they have high detection accuracy, have high computational costs and low interpretability, which limits their usage in resource-constrained settings.

New techniques, including DNA-based and bio-inspired IDS models, have demonstrated a promising outcome in the field of adaptability and pattern representation. Such techniques are, however, in their infancy and have not been validated over large scales in the real world. Moreover, other issues like limitations in data sets, class imbalance, encrypted traffic, and so forth remain in play as far as the performance and generalization of IDS models are concerned. There is a need for lightweight, flexible, and scalable IDS solutions.

Table 1 shows that traditional IDS methods are effective for known attacks, while advanced approaches such as ML, deep learning, and hybrid models provide better adaptability to evolving threats. This highlights the importance of adopting more flexible and intelligent IDS techniques in modern network environments.

To provide a clearer understanding of IDS classifications and enable fair comparison among approaches, this section outlines the main intrusion detection methods and provide an indicative comparison of different IDS approaches presented in Table 2.

Table 2. Performance comparison of Intrusion Detection Systems (IDS) approaches

IDS Approach	Model	Dataset	Accuracy (%)
Machine Learning [36]	SVM	NSL-KDD	97.11
Machine Learning [37]	Decision Tree	CICIDS2017	98.63
Deep Learning [38]	CNN-LSTM	UNSW-NB15	93.68
Hybrid IDS [39]	CNN + LSTM	CICIDS2017	98–99
Federated IDS [40]	Federated LSTM	IoT Dataset	95–97

The results presented in Table 2 provide a comparative view of different IDS approaches using a unified evaluation metric (accuracy). It can be observed that ML and hybrid approaches achieve relatively high accuracy, indicating their effectiveness in structured environments.

However, deep learning models show variability in performance across different datasets, as reflected by the lower accuracy on UNSW-NB15, highlighting challenges related to generalization and dataset dependency. In contrast, federated IDS demonstrate comparatively lower accuracy due to its decentralized nature and communication constraints, despite offering advantages in data privacy and scalability.

These observations are consistent with the limitations discussed in the related work, emphasizing that no single approach is universally optimal, and the choice of IDS technique depends on the application context and system requirements.

4.1 Intrusion Detection System approaches

IDS are critical elements of network and system security, which serve to monitor, analyze, and report malicious activity. There exist various types of IDSs depending on their architecture, placement, and the way they operate. This part gives a specific discussion of the most notable types of IDS as reported in the literature.

(1) Architecture-based IDS

Host-based IDS (HIDS): HIDS is an IDS that tracks internal actions on each host, e.g., system calls, OS logs, and process behaviours. It is also useful to monitor insider threats and privilege escalations by giving a close look at the host-level

happenings [41, 42]. However, HIDS consumes resources of the system and cannot identify external network threats. Some are OSSEC, Tripwire, and Wazuh.

Network-Based IDS (NIDS): A NIDS monitors network traffic at strategic locations like routers and gateways to detect malicious patterns. It works well in identifying external threats like DDoS attacks and port scans, among others, and it tends to use both signatures and non-signature methods [43]. Though NIDS can provide wide visibility, it is faced with difficulties in encrypted traffic and can be affected by performance limitations in high-speed settings.

Distributed IDS (DIDS): This is a form of IDS that involves the deployment of multiple IDS agents on both host and network layers to detect threats through coordinated analysis. This infrastructure provides a global security overview, which builds the monitoring of distributed or coordinated attacks. It also enables combining diverse detection techniques across nodes, but comes with complexity in synchronization as well as communication overhead, especially in a large environment [44].

(2) Detection technique-based IDS

Signature-based IDS: Signature-based IDS detects the presence of malicious traffic by comparing that traffic with known attacks. Snort, Suricata, and Zeek are tools that are based on constantly updated rule sets to be effective. These systems are very precise in identifying threats, though they cannot identify undetermined threats, and they also demand regular maintenance [45, 46].

Anomaly-based IDS: Anomaly-Based IDS is used to identify an aberration of normal behaviour employing learned baselines that include workload, protocols, and the duration of connections [47]. It is also better in detecting zero-day threats but has a high false positives. Labanne (2020) has stated that these systems are better with emerging threats and signature models are better with known threats [14]. Towards this end, themost common tools include ADAM, DROIDS, and Kitsune, which commonly use SVMs, Decision Trees, CNNs, and RNNs. Nonetheless, some of the lingering issues exist, such as the reliance on labelled data and the limitation to real-time performance.

AI/ML-based IDS: AI/ML-based IDS is a system that implements machine-learning or deep-learning algorithms and is used to detect more complex traffic behaviour patterns. These systems are capable of responding to new threats and decreasing false positives [48]. SVMs, Random Forests, CNNs, andLSTMs are some of the algorithms that have been used in software like Kitsune and DeepIDS. As such, these methods require the existence of labeled datasets, large computational power, and substantial model sensitivity.

(3) Environment-based IDS

Protocol-Based IDS (PIDS): PIDS is a monitoring of traffic used by application-layer protocols in HTTP, FTP, or DNS. These systems concentrate on breaches of protocol rules and are able to identify malformed packets, injection attacks or unusual behaviour within services. PIDS suits well in securing web servers, proxies as well as application gateways. However, it is restricted to what it is monitoring in the form of protocols and cannot determine the entire behaviour of the host or the network [49].

Application-Based IDS (APIDS): APIDS runs within the application, e.g., in databases, ERP systems, or email servers. It scans within commands, access patterns, or query logs to identify abuse, insider threats, or suspicious behaviour. APIDS provides profound visibility and context-based analysis, but might be unable to identify threats that may exist at the network layer or other systems. Its setting is highly related to the application that it safeguards [50].

Cloud/IoT-Based IDS: These IDSs are specific to the virtualised, cloud-based, or Internet of Things infrastructure in situations where traditional IDS deployment is not feasible. To monitor data flows in decentralised or dynamic environments, they use lightweight agents or external monitors to inspect the data flows. Despite offering scalability and interoperability with current architectures, they are subject to resource constraints, heterogeneity, and latency, limiting their maturity and functionality [51].

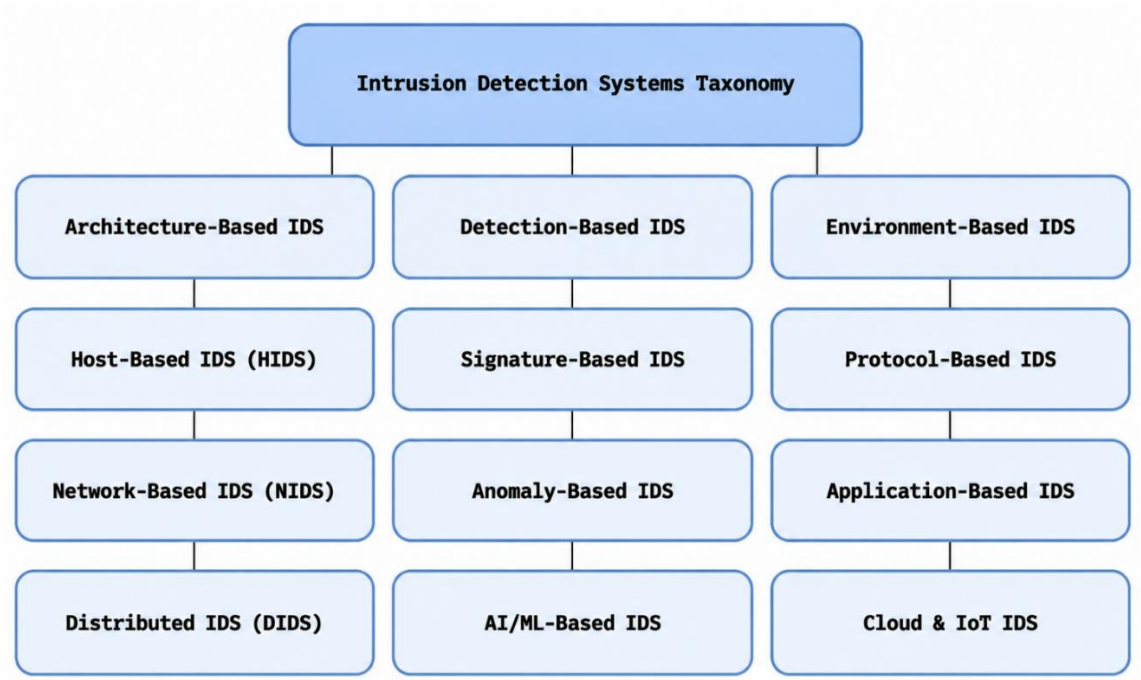

Figure 2. Taxonomy of Intrusion Detection Systems (IDS)

Table 3. Comparative summary of Intrusion Detection System (IDS) types

Types	Scope/Deployment	Strengths	Limitations
Host-Based IDS	Host-level (individual systems)	Provided with deep details on the system operational behavior	No visibility outside host
Network-Based IDS	Network-level (traffic inspection)	Monitores external threats	Has problems with encrypted traffic and inefficient performance
Distributed IDS	Distributed (host + network agents)	Provides global monitoring and coordinated threat detection	Complex deployment and high communication overhead
Signature-Based IDS	Pattern matching (predefined signatures)	Very accurate in the detection of attacks	Fails to detect new/unknown attacks
Anomaly-Based IDS	Behavioral deviation from baseline	Detection of new and zero-day attack	It's prone to false positive and it needs profiling
AI/ML-Based IDS	Learning-based (Machine learning /Deep learning models)	Adaptive to evolving attack patterns	It takes labeled data and intensive computing capacity
Protocol-Based IDS	Application-layer protocols	Factors of correct detection of protocol misuse.	Limited to specific protocols only
Application-Based IDS	Specific applications	Context-aware within specific apps	limited area of application to internal use
Cloud/IoT-Based IDS	Cloud/IoT environments	Scalable and cloud-native compatible	cannot work in resource limited environments

IDS are categorized based on multiple criteria to better understand their structure and operation. Figure 2 illustrates a hierarchical taxonomy of IDS classifications and summarizes the main IDS categories and their types. It helps in understanding and comparing different IDS approaches. Table 3 shows that different IDS types offer complementary strengths and limitations depending on deployment, detection method, and scope. Distributed and AI-driven systems provide broader coverage, while NIDS and HIDS offer more focused monitoring. IDS selection depends on system requirements and threats.

Since the performance of these IDS techniques depends heavily on the datasets used for training and evaluation, the following section presents the most widely adopted IDS datasets. Since the performance of IDS models depends heavily on data quality, the following section reviews the most commonly used datasets.

4.2 Common datasets

Benchmark datasets are considered to be the fundamental training and comparison tools in the creative process and the testing of IDS developments. Despite the wide adoption of many public datasets in the IDS research, all of them have certain inherent limitations that restrict the applicability of the model in practice and generalizability.

KDD99 is one of the first benchmarks in the study of IDS, which is based on records of the traffic in DARPA 1998, which were simulated in a military setting. It consists of several types of attacks, such as DoS, Probe, U2R, and R2L. However, it has been widely condemned as being synthetic, redundant to a large extent, and heavily skewed in the class actions. The dataset does not reflect the current tendency of attacks, coded protocols, and user traffic, and maybe it is not appropriate to implement modern IDS applications [52].

To reduce the issues of redundancy and imbalance in KDD-99, NSL-KDD was introduced. It provides train-test splits and is more class-balanced. Nonetheless, it continues to suffer the structural shortcomings of its predecessor, i.e., archaic traffic patterns and a lack of encrypted communications or cloud-driven activity. As such, it cannot be as useful in assessing modern IDS models [53].

CICIDS2017 is one of the most comprehensive and realistic datasets offering benchmarking of the IDS developed by the Canadian Institute of Cybersecurity. It records benign and attack traffic in many scenarios, such as DDoS, brute-force, botnet, and infiltration, and it also makes full packet captures (PCAP) and flow-based and labeled feature sets. However, the data set was produced in a controlled setting, and this reduces the uncertainty and heterogeneity of the traffic. In addition, it does not have encrypted flows and has imbalanced classes-problems that cripple its use with contemporary encrypted networks [54].

The UNSW-NB15, which was generated using the IXIA PerfectStorm tool, uses modern protocols and maintains a wide range of various types of attacks in contrast to the earlier datasets. It comprises rich labeled features and an environment simulation of contemporary threats. Nonetheless, similarly to CICIDS2017, it was also created in a laboratory, and surveys have found issues with label noise, class imbalance, and little applicability to real-time operation conditions [55].

The CSE-CIC-IDS2018 data, as a continuation of CICIDS2017, expands the scope to that of multi-day attacks, user profiles, and cloud-native activities, which are simulated. Even though it covers a wider range of attacks and diversity of traffic, it is still limited by the same factors- namely, lack of encryption, the artificial laboratory setup, and complexity of data. Liu and Lang [56] recorded that the use of irrelevant or redundant features in this data set can hamper the use of IDS as well as make the deployment of IDS complex in real-time. A comparative summary of the commonly used intrusion detection datasets, along with their strengths and limitations, is presented in Table 4.

Table 4 highlights that while commonly used datasets provide valuable benchmarks, they still suffer from limitations such as data imbalance, lack of realism, and limited representation of modern network environments.

The features of IDS datasets are crucial for figuring out how well a model works and how well it can be used in other situations. For example, class imbalance in datasets like KDD Cup 99 and CICIDS2017 can cause models to be biased toward the majority class, which makes it harder to find rare attacks. Also, the fact there aren't any realistic or varied traffic patterns makes it harder for trained models to work in real-world situations. These limitations show how essential it is to use balanced and representative datasets to make sure that IDS works well and is reliable.

To assess objectively the performance of IDS on these

datasets objectively, a number of evaluation metrics are normally used as discussed in the following section.

Table 4. Summary of intrusion detection datasets

Dataset	Year	Strengths	Limitations
KDD Cup 99	1999	Large, well labeled collection of network traffic	Large amount of redundancy and class imbalance.
NSL-KDD	2009	Fewer duplicated records, and Improvement of sample distribution	Still outdated, limited realism
CICIDS2017	2017	Modern and realistic data and includes a substantial range of existing assaults	No encrypted traffic, imbalance
UNSW-NB15	2015	Mixture of real and artificially created traffic hence covering a combination of nine contemporary attack modalities	Noise Labeling, reduced real-time capability
CSE-CIC-IDS2018	2018	The dataset is large, all-encompassing, as it is able to capture everyday attacks	Lab generated

4.3 Performance evaluation metrics

IDS evaluation is important to determine its accuracy and reliability. Quantitative measures are applied by researchers in determining the effectiveness of an IDS in identifying normal and malicious activity. Popular measures are Accuracy, Precision, Recall, F1-Score, False Positive Rate (FPR), and Receiver Operating Characteristic-Area Under the Curve (ROC-AUC). As noted in [57], these metrics are common in ML, and they are True Positive (TP), False Positive (FP), False Negative (FN), and True Negative (TN), which are usually assessed through a confusion matrix. Equally important is the fact that balanced and up-to-date datasets, including NSL-KDD and CICIDS2017, were highlighted in the study [14] as datasets that, despite their diversities, are still characterized by data imbalance and outdated traffic patterns, which still affect the generalizability of IDS models.

(1) Accuracy

As defined in [42], Accuracy represents the number of right responses (attacks and normal traffic) of the predictions of an IDS. It is calculated as in Eq. (1).

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \quad (1)$$

Although high accuracy is preferable, it is misleading when used with skewed data sets. On most related datasets, one of the classes predominates, and it may skew the results and misrepresent the normative findings.

(2) Precision

As defined [14], precision is the fraction of attacks that were correctly detected among all instances signaled as attacks by the IDS. It is calculated as in Eq. (2).

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \quad (2)$$

It shows the percentage of alerts in the system that are valid. High precision means that there will be fewer false positives, which is critical in decreasing fatigue with alerts and guaranteeing confidence in alerting with IDS.

(3) Recall (Detection Rate)

As described in [8], Recall refers to the capability of an IDS to detect the true attacks. out of all the attack instances present It is calculated as in Eq. (3).

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \quad (3)$$

A high recall implies that the system is effective in identifying majority of malicious activities. Yet, it can be at the expense of an increase in false positives and is particularly true of anomaly-based systems.

(4) F1-Score

As explained in [19] The F1-Score is the harmonic mean of precision and recall which is a balanced measure that considers the false positives and false negative. It is calculated as in Eq. (4).

$$\text{F1} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (4)$$

It is also useful especially when the data set used is skewed or when both forms of error are equally essential.

(5) FPR

According to reference [57], the rate called a FPR is used to describe the percentage of real events that are not malicious, which is incorrectly recognized as a malicious event by the IDS. It is calculated as in Eq. (5).

$$\text{FPR} = \frac{\text{FP}}{\text{FP} + \text{TN}} \quad (5)$$

When the FPR is lower, it means a more reliable and effective IDS. On the other hand, high FPR may overwhelm the security team with irrelevant notifications and increase alert fatigue and loss of trust in the warning.

(6) ROC and AUC

The ROC curve shows the relationship between the true positive rate (TPR) and FPR of both prediction thresholds. The AUC measures the total capability of an IDS to discriminate between attack and normal traffic:

If AUC close to 1.0 is an excellent rejection performance.

If AUC close to 0.5 implies no or random discrimination.

The AUC could be considered as the probability that the IDS will rate higher an attack that was randomly selected in comparison to a standard instance [53]. Figure 3 illustrates a curve of individual ROC, demonstrating how a high-performance IDS model can maintain a high TPR while keeping a low FPR across various threshold configurations.

The blue curve is an IDS performance curve, that is, in terms of TPR against FPR, given a different threshold. The AUC measures the detection capability, and a larger number represents a stronger model. The AUC of 0.5 indicates a case of random guessing, and there is no discriminative power.

(7) Additional Metrics

In addition to accuracy indicators, it is impossible to assess the work of IDS without a number of operational measures, such as:

- Detection Time: This is the time that the IDS takes to detect an intrusion.
- Throughput: The number of data packets that have been analysed each second.

- Resource Utilization: The common measurements are memory usage, bandwidth consumption, and CPU load.

To provide a consolidated overview of the standard evaluation metrics and their significance, a summary is presented in Table 5.

These are important metrics when evaluating the deployment of an IDS in real-time or massive situations. Table 4 summarizes the key evaluation metrics used in IDS analysis, highlighting that no single metric is sufficient on its own, and a combination of measures is necessary for a comprehensive performance assessment.

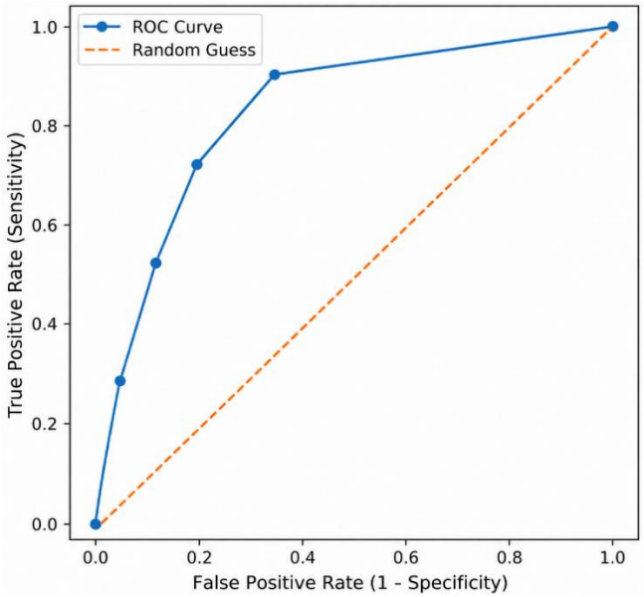

Figure 3. Receiver Operating Characteristic (ROC) curve illustrating Intrusion Detection Systems (IDS) performance evaluation [58]

Table 5. Summary of standard metrics for Intrusion Detection Systems (IDS) performance analysis

Metric	Definition	Importance
Accuracy	Ratio of correct predictions (both attack and normal) over total instances	Misleading in imbalanced data
Precision	How many predicted attacks were actually attacks	Penalizes false alarms
Recall (Sensitivity)	How many actual attacks were correctly detected	Crucial for reducing undetected threats
F1-Score	Harmonic mean of precision and recall	Balanced view of performance
AUC-ROC	Area under the ROC curve	An effective measure of comparing models with different thresholds

Note: Receiver Operating Characteristic-Area Under the Curve (ROC-AUC)

5. CONCLUSION

This paper provides a comprehensive review of IDS, covering their evolution, architectures, and advancements in detection techniques, particularly the transition toward intelligent, hybrid, and bio-inspired approaches. The analysis highlights the growing need to move from traditional signature-based and anomaly-based models toward AI-driven and hybrid IDS solutions that offer improved scalability, adaptability, and resilience in modern network environments. However, existing IDS systems still face challenges in effectively addressing dynamic and sophisticated cyber threats.

The integration of AI, ML, and biologically inspired computing presents promising opportunities for developing adaptive and self-evolving IDS models. In particular, DNA-based IDS encode network traffic behavior into sequence-based representations, enabling mutation-based signature generation that can reduce false positives and improve interpretability. Additionally, the increasing adoption of AI models raises concerns regarding computational cost and energy consumption, emphasizing the importance of Green AI approaches that aim to design efficient and sustainable IDS solutions. For example, biologically inspired encoding methods, such as amino-acid sequence representations, have demonstrated high detection rates and reduced false alarms on datasets like UNSW-NB15.

To further advance these emerging directions, future research should focus on developing practical frameworks for DNA-based IDS, including efficient encoding strategies and real-time detection mechanisms. Moreover, the design of lightweight and energy-efficient IDS models should be prioritized to support deployment in resource-constrained environments such as IoT systems. Integrating explainable AI (XAI) techniques can also enhance transparency and trust in IDS decision-making processes. Furthermore, future studies should emphasize the use of realistic, diverse, and up-to-date datasets to improve generalization and real-world applicability.

These approaches are particularly relevant in scenarios involving encrypted traffic, resource-constrained systems, and rapidly evolving attack patterns. To further strengthen security in such environments, robust cryptographic mechanisms should also be considered as part of an integrated defense strategy.

Despite these advancements, this study has certain limitations, including the limited number of reviewed studies, variations in evaluation methodologies, and the exclusion of non-English publications.

REFERENCES

[1] Anderson, J.P. (1980). Computer Security Threat Monitoring and Surveillance. Technical Report, James P. Anderson Company. https://cir.nii.ac.jp/crid/1573950399661362176.

[2] Quintero-Bonilla, S., Martín del Rey, A. (2020). A new proposal on the advanced persistent threat: A survey. Applied Sciences, 10(11): 3874. https://doi.org/10.3390/app10113874

[3] Roesch M. (1999). Snort—Lightweight intrusion detection for networks. In Proc. 13th USENIX Conf. System Administration (LISA '99), Seattle, WA. pp. 229-238. https://www.usenix.org/legacy/event/lisa99/full_papers/roesch/roesch.pdf?utm_source=chatgpt.com.

[4] Satılmış, H., Akleylek, S., Tok, Z.Y. (2024). A systematic literature review on host-based intrusion detection systems. IEEE Access, 12: 27237-27266. https://doi.org/10.1109/ACCESS.2024.3367004

[5] Guo, Y., Zhao, L., Sun, J. (2023). A survey of machine-learning-based zero-day attack detection: Challenges and

future directions. Computer Communications, 198: 175-185. https://doi.org/10.1016/j.comcom.2022.11.001
[6] Liu, M., Xue, Z., Xu, X., Zhong, C., Chen, J. (2018). Host-based intrusion detection system with system calls: Review and future trends. ACM Computing Surveys (CSUR), 51(1): 1-36. https://doi.org/10.1145/3214304
[7] Salem, H., Darwich, M., El-Ghamry, A. (2024). Advancing cybersecurity: A comprehensive review of AI-driven detection techniques. Journal of Big Data, 11(1): 58. https://doi.org/10.1186/s40537-024-00957-y
[8] Diana, L., Dini, P., Paolini, D. (2025). Overview on intrusion detection systems for computer networking security. Computers, 14(3): 87. https://doi.org/10.3390/computers14030087
[9] Sultana, N., Chilamkurti, N., Peng, W. (2019). Survey on SDN-based network intrusion detection system using machine learning approaches. Peer-to-Peer Networking and Applications, 12(2): 493-501. https://doi.org/10.1007/s12083-017-0630-0
[10] Ahmad, Z., Khan, A.S., Shiang, C.W., Abdullah, J., Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1): e4150. https://doi.org/10.1002/ett.4150
[11] Samrin, R., Vasumathi, D. (2017). Review on anomaly-based network intrusion detection system. In 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT), Mysuru, India, pp. 141-147. https://doi.org/10.1109/ICEECCOT.2017.8284655
[12] Kumar, S., Gupta, S., Arora, S. (2022). Research trends in network-based intrusion detection systems: A review. IEEE Access, 10: 127855-127878. https://doi.org/10.1109/ACCESS.2021.3129775
[13] Sharafaldin, I., Lashkari, A.H., Ghorbani, A.A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Proceedings of the 4th International Conference on Information Systems Security and Privacy ICISSP - Volume 1, pp. 108-116. https://doi.org/10.5220/0006639801080116
[14] Labonne, M. (2020). Anomaly-based network intrusion detection using machine learning. Doctoral dissertation, Institut polytechnique de Paris.
[15] Umar, H.G.A., Yasmeen, I., Aoun, M., Mazhar, T., Khan, M.A., Jaghdam, I.H., Hamam, H. (2025). Energy-efficient deep learning-based intrusion detection system for edge computing: A novel DNN-KDQ model. Journal of Cloud Computing, 14(1): 32. https://doi.org/10.1186/s13677-025-00762-9
[16] Alwhbi, I.A., Zou, C.C., Alharbi, R.N. (2024). Encrypted network traffic analysis and classification utilizing machine learning. Sensors, 24(11): 3509. https://doi.org/10.3390/s24113509
[17] lom, M.Z., Taha, T.M., Yakopcic, C., Westberg, S., Sidike, P., Nasrin, M.S., Hasan, M., Van Essen, B.C., Awwal, A.A.S., Asari, V.K. (2019). A state-of-the-art survey on deep learning theory and architectures. Electronics, 8(3): 292. https://doi.org/10.3390/electronics8030292
[18] Abeshu, A., Chilamkurti, N. (2018). Deep learning: The frontier for distributed attack detection in fog-to-things computing. IEEE Communications Magazine, 56(2): 169-175. https://doi.org/10.1109/MCOM.2018.1700332
[19] Ring, M., Wunderlich, S., Scheuring, D., Landes, D., Hotho, A. (2019). A survey of network-based intrusion detection data sets. Computers & Security, 86: 147-167. https://doi.org/10.1016/j.cose.2019.06.005
[20] Albulayhi, K., Smadi, A.A., Sheldon, F.T., Abercrombie, R.K. (2021). IoT intrusion detection taxonomy, reference architecture, and analyses. Sensors, 21(19): 6432. https://doi.org/10.3390/s21196432
[21] Schwartz, R., Dodge, J., Smith, N.A., Etzioni, O. (2020). Green AI. Communications of the ACM, 63(12): 54-63. https://doi.org/10.1145/3381831
[22] Tjoa, E., Guan, C. (2021). A survey on explainable artificial intelligence (XAI): Toward medical XAI. IEEE Transactions on Neural Networks and Learning Systems, 32(11): 4793-4813. https://doi.org/10.1109/TNNLS.2020.3027314
[23] Yang, Q., Liu, Y., Chen, T., Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST), 10(2): 1-19. https://doi.org/10.1145/3298981
[24] Latif, N., Ma, W., Ahmad, H.B. (2025). Advancements in securing federated learning with intrusion detection systems: A comprehensive review. Artificial Intelligence Review, 58: 91. https://doi.org/10.1007/s10462-024-11082-w
[25] Khan, M.A., Karim, M.R., Kim, Y. (2019). A scalable and hybrid intrusion detection system based on the convolutional-LSTM network. Symmetry, 11(4): 583. https://doi.org/10.3390/sym11040583
[26] Sun, P., Liu, P., Li, Q., Liu, C., Lu, X., Hao, R. (2020). DL-IDS: Extracting features using CNN-LSTM hybrid network for intrusion detection system. Security and Communication Networks, 2020(1): 8890306. https://doi.org/10.1155/2020/8890306
[27] Singh, R., Ujjwal, R.L. (2023). Hybridized bio-inspired intrusion detection system for Internet of Things. Frontiers Big Data, 6: 1-12. https://doi.org/10.3389/fdata.2023.1081466
[28] Ibaisi, A., Ali, I., Yusuf, M. (2023). Bio-inspired intrusion detection using amino acid encoding. Electronics, 12(20): 4294. https://doi.org/10.3390/electronics12204294
[29] Shyaa, M.A., Zainol, Z., Abdullah, R., Anbar, M., Alzubaidi, L., Santamaría, J. (2023). Enhanced intrusion detection with data stream classification and concept drift guided by incremental learning genetic programming combiner. Sensors, 23(7): 3736. https://doi.org/10.3390/s23073736
[30] Hosseini, F., Gharehchopogh, F.S., Masdari, M. (2022). A botnet detection in IoT using a hybrid multi-objective optimization algorithm. New Generation Computing, 40(3-4): 693-727. https://doi.org/10.1007/s00354-022-00188-w
[31] Shone, N., Ngoc, T.N., Phai, V.D., Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1): 41-50. https://doi.org/10.1109/TETCI.2017.2772792
[32] Zhou, C., Paffenroth, R.C. (2017). Anomaly detection with robust deep autoencoders. In KDD '17: Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 665-674. https://doi.org/10.1145/3097983.3098052
[33] Guidotti, R., Monreale, A., Ruggieri, S., Turini, F.,

Giannotti, F., Pedreschi D. (2018). A survey of methods for explaining black box models. ACM Computing Surveys (CSUR), 51(5): 1-42. https://doi.org/10.1145/3236009

[34] Song, X., Ma, Q. (023). Intrusion detection using federated attention neural network for edge-enabled Internet of Things. Journal of Grid Computing, 22: 15. https://doi.org/10.1007/s10723-023-09725-3

[35] Alsoufi, M.A., Razak, S., Siraj, M.M., Nafea, I., Ghaleb, F.A. (2021). Anomaly-based intrusion detection systems in IoT using deep learning: A systematic literature review. Applied Sciences, 11(18): 8383. https://doi.org/10.3390/app11188383

[36] Suleiman, M.F., Issac, B. (2018). Performance comparison of intrusion detection machine learning classifiers. In 2018 28th International Conference on Computer Theory and Applications (ICCTA), Alexandria, Egypt, pp. 19-23. https://doi.org/10.1109/ICCTA45985.2018.9499140

[37] Maseer, Z.K., Yusof, R., Bahaman, N., Mostafa, S.A., Foozy, C.F.M. (2021). Benchmarking of machine learning for anomaly-based intrusion detection systems using CICIDS2017. IEEE Access, 9: 22351-22370. https://doi.org/10.1109/ACCESS.2021.3056614

[38] Halbouni, A., Gunawan, T.S., Habaebi, M.H., Halbouni, M., Kartiwi, M., Ahmad, R. (2022). CNN-LSTM: Hybrid deep neural network for network intrusion detection system. IEEE Access, 10: 99837-99849. https://doi.org/10.1109/ACCESS.2022.3206425

[39] Jyothi, D., Vijay, P.J., Kumar, M.K., Lakshmi, R.V. (2025). Design of an improved method for intrusion detection using CNN, LSTM, and blockchain. Journal of Theoretical and Applied Information Technology, 103(1): 1-22. https://jatit.org/volumes/Vol103No1/1Vol103No1.pdf

[40] Lazzarini, R., Tianfield, H., Charissis, V. (2023). Federated learning for IoT intrusion detection. AI. 4(3): 28. https://www.mdpi.com/2673-2688/4/3/28

[41] Scarfone, K., Mell, P. (2007). Guide to intrusion detection and prevention systems (IDPS). NIST Special Publication, 800-94. https://doi.org/10.6028/NIST.SP.800-94

[42] Buczak, A.L., Guven, E. (2016). A survey of data mining and machine learning methods for cybersecurity intrusion detection. IEEE Communications Surveys & Tutorials, 18(2): 1153-1176. https://doi.org/10.1109/COMST.2015.2494502

[43] Nwakanma, C.I., Ahakonye, L.A.C., Njoku, J.N. (2023). Explainable artificial intelligence (XAI) for intrusion detection and mitigation in intelligent connected vehicles: A review. Applied Sciences, 13(3): 1252. https://doi.org/10.3390/app13031252

[44] Chowdhury, A.P., Hossain, S.K., Nur, F.N. (2025). Distributed intrusion detection system for edge of things to enhance security. In 2025 2nd International Conference on Next-Generation Computing, IoT and Machine Learning (NCIM), Gazipur, Bangladesh, pp. 1-6. https://doi.org/10.1109/NCIM65934.2025.11160191

[45] Latah, M., Toker, L. (2019). A survey of intrusion detection systems: Techniques, datasets and evaluation methods. Cybersecurity, 2(1): 20. https://doi.org/10.1186/s42400-019-0038-7

[46] Otoum, Y., Nayak, A. (2021). AS-IDS: Anomaly and signature-based intrusion detection system for the Internet of Things. Journal of Network and Systems Management, 29: 23. https://doi.org/10.1007/s10922-021-09589-6

[47] Depren, O., Topallar, M., Anarim, E., Ciliz, M.K. (2005). An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks. Expert Systems with Applications, 29(4): 713-722. https://doi.org/10.1016/j.eswa.2005.05.002

[48] Altamimi, S., Abu Al-Haija, Q. (2024). Maximizing intrusion detection efficiency for IoT networks using extreme learning machine. Discover Internet Things, 4: 5. https://doi.org/10.1007/s43926-024-00060-x

[49] Dutta, N., Jadav, N., Tanwar, S., Sarma, H.K.D., Pricop, E. (2022). Intrusion detection systems fundamentals. In Cyber Security: Issues and Current Trends, Springer, Singapore, pp. 101-127. https://doi.org/10.1007/978-981-16-6597-4_6

[50] Razzaq, A., Latif, K., Ahmad, H.F., Hur, A., Anwar, Z., Bloodsworth, P.C. (2013). Semantic security against web application attacks. Information Sciences, 254: 19-38. https://doi.org/10.1016/j.ins.2013.08.007

[51] Ajith, V., Cyriac, T., Chavda, C., Kiyani, A.T., Chennareddy, V. (2024). Analyzing Docker vulnerabilities through static and dynamic methods and enhancing IoT security with AWS IoT Core, CloudWatch, and GuardDuty. IoT, 5(3): 26. https://doi.org/10.3390/iot5030026

[52] Liu, W. (2025). Dynamic network intrusion detection model based on transformer and adversarial autoencoder. International Journal of Intelligent Networks. https://doi.org/10.1016/j.ijin.2025.11.002

[53] Tavallaee, M., Bagheri, E., Lu, W., Ghorbani, A.A. (2009). A detailed analysis of the KDD CUP 99 data set. In 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, pp. 1-6. https://doi.org/10.1109/CISDA.2009.5356528

[54] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I.A. (2020). A survey on machine learning techniques for cybersecurity in the last decade. IEEE Access, 8: 222310-222354. https://doi.org/10.1109/ACCESS.2020.3041951

[55] Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W. (2020). A review of intrusion detection systems using machine and deep learning in Internet of Things. Electronics, 9(7): 1177. https://doi.org/10.3390/electronics9071177

[56] Liu, H., Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. Applied Sciences, 9(20): 4396. https://doi.org/10.3390/app9204396

[57] Bukhari, S.M.S., Zafar, M.H., Abou Houran, M., Moosavi, S.K.R., Mansoor, M., Muaaz, M., Sanfilippo, F. (2024). Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability. Ad Hoc Networks, 155: 103407. https://doi.org/10.1016/j.adhoc.2024.103407

[58] Fawcett, T. (2006). An introduction to ROC analysis. Pattern Recognition Letters, 27(8): 861-873. https://doi.org/10.1016/j.patrec.2005.10.010