Dijlah Journal of Engineering Science (DJES) Vol. 3, No. 1, March, 2026, pp.225-236
ISSN: Printed: **3078-9656, Online: 3078-9664**, paper ID: 126

A Review of AI and Dataset-Driven Approaches for Intrusion Detection Systems

Douha A. Kawam[1], Mohammed J. zaiter[2], Mohammed A. kadhim[3]
[1]Electrical Engineering Technical College, Middle Technical University, Baghdad, Iraq
[2] Electrical Engineering Technical College, Middle Technical University, Baghdad, Iraq
[3]Middle Technical University, Baghdad, Iraq

Article Info

Article history:

Received Nov., 21, 2025
Revised Dec.,7, 2025
Accepted Jan.,3, 2026

Keywords:

IDS
Machine learning
Cyber threats
Deep learning
Dataset

ABSTRACT

The increasing complexity of cyber threats has underscored the constraints of conventional Intrusion Detection Systems (IDS) and the need to have more flexible and intelligent security systems. The growth of artificial intelligence (AI) has made automated threat response, real-time analysis, and learning in the field of intrusion detection a focus. The review paper related to AI-driven IDS published between 2023 and 2025 have been examined, and efforts have focused on the hybrid metaheuristic model, machine learning, and deep learning. Well-known datasets, including CICIDS2017, CICIDS2018, UNSW-NB15, and NSL-KDD, have been tested on their appropriateness in measuring the performance of a system. It is reported that hybrid deep learning metaheuristic structures have a higher detection efficiency and flexibility than fifteen modern models, but these are reported to be highly computational. The future research direction is presented, including the explanation of AI to enhance transparency, the creation of lightweight IDS that can be implemented in the conditions of the IoT, and the enhancement of adversarial attack resistance. Overall, AI-based IDS may be deemed as a serious breakthrough in intelligent, scalable, and resilient network security.

Corresponding Author:

Douha A.Kawam
Electrical Engineering Technical College, Middle Technical University.
Almasafi street, Baghdad, Iraq
Email: BBC5015@mtu.edu.iq

1. INTRODUCTION

As the internet rapidly expands and technologies like big data and fog computing evolve, cyber-security threats are becoming more complex. The conventional defenses, such as firewalls and intrusion detection systems, cannot keep up, and artificial intelligence (AI)-based defense is needed to proactively defend against and attack more sophisticated attacks [1].Deep Learning (DL) has revolutionized AI applications in image, speech, and facial recognition and can deliver more data exploitation and performance **[**2].Another significant breakthrough in cyber-security over traditional ML is that DL helps in the detection of malware and behavioral analysis. Machine Learning (ML) promotes its potential to an enormous degree; however, its utilization based on the manual extraction of features demonstrates two significant limitations. The handcoded feature used in the case of the malware detection using the ML might jeopardize accuracy and efficiency because they take into account known features only and fail to take into account the threats that are not known [3].Therefore, the value of ML greatly depends on the correctness of the feature extraction. The aspects of deep learning enhance cyber defense by discovering hidden patterns in unstructured data, as such, enabling the detection of new threats and advanced attacks, especially in the context of growing internet connectivity throughout IoT[4].The emergence of cloud computing has intensified the demand for security platforms, and the study of malware behavior is therefore necessary to enhance conventional security solutions, particularly due to the complexity of cyber-security data [5].ML Leading automated analysis of behavior with insightful features Extraction in the face of network packets itself is the basis of the development of advanced intrusion detection. ML at its most basic level gives computers the power to learn and adapt automatically without human intervention [6].The contribution of this paper can be summarized as follows:

•Providing a comprehensive overview of machine learning and data mining techniques used in intrusion detection systems (IDS).

• Presenting an overview of the datasets employed for evaluating the performance of IDS.

2. ARTIFICIAL INTELLIGENCE OVERVIEW

The introduction of Artificial Intelligence (AI) in the information security area is gaining ever more importance because of its capacity to handle a lot of data, find patterns, and define possible threats effectively [7]. The traditional security controls also tend to be ineffective against the most recent and evolving threats, such as zero-day vulnerabilities, and AI-based security tools have the potential to adjust them based on new and unknown ones with the help of learning data. Decision making, improved intrusion detection, and containment of malicious actions are some of the advantages of AI. Its predictive mode also enables the real-time anticipation of the threats as well as its reaction and also reduces the false positives that are typical of the conventional security measures [8]. These features make AI immensely add to the resilience and adaptability of the information protection systems. The AI technologies constitute a set of diverse strategies that prove rather useful in the context of information security.

•Machine Learning (ML): It is a type of algorithm, which enables computers to acquire data and learn on their own, without a programming code, which would enable them to improve the recognition and classification of possible threats [9].

•Deep Learning (DL): Well-developed neural networks, capable of operating with huge amounts of data and learning during the course of their activity in a manner similar to that of a human brain when trying to find a complex pattern [10].

AI enhances information security through real-time monitoring and learning, while combining metaheuristics with learning models improves detection accuracy and generalization [11].Benefits of Metaheuristic Algorithms in Threat Detection [12]:

•Optimization: Metaheuristic algorithms can be used to solve complex problems that are hard to solve by the conventional methods.

•Automation: These algorithms have been able to automatically control the parameters used in the detection, and so the human factor has been eliminated, thereby increasing the speed and reliability of the detection process.

•Speed: They tend to converge faster to useful solutions, which is important in a situation where threats need to be detected and solved immediately.

2. 1 Machine Learning

(ML) is a field where computers can estimate the solution to problems and predictions even without being programmed, by utilizing past data. This section provides an overview of ML paradigms, classifications, and architectures. The variety of algorithms incorporated in ML is wide, and their complexity and aim differ, and they are generally separated by the type of task they perform or the channel by which they perform it. The algorithms within the ML discipline are commonly divided into four general categories: supervised, unsupervised, semi-supervised, and reinforcement learning (RL).There are other subcategories that have also come up in order to cover more particular or intricate learning situations [13] [14].

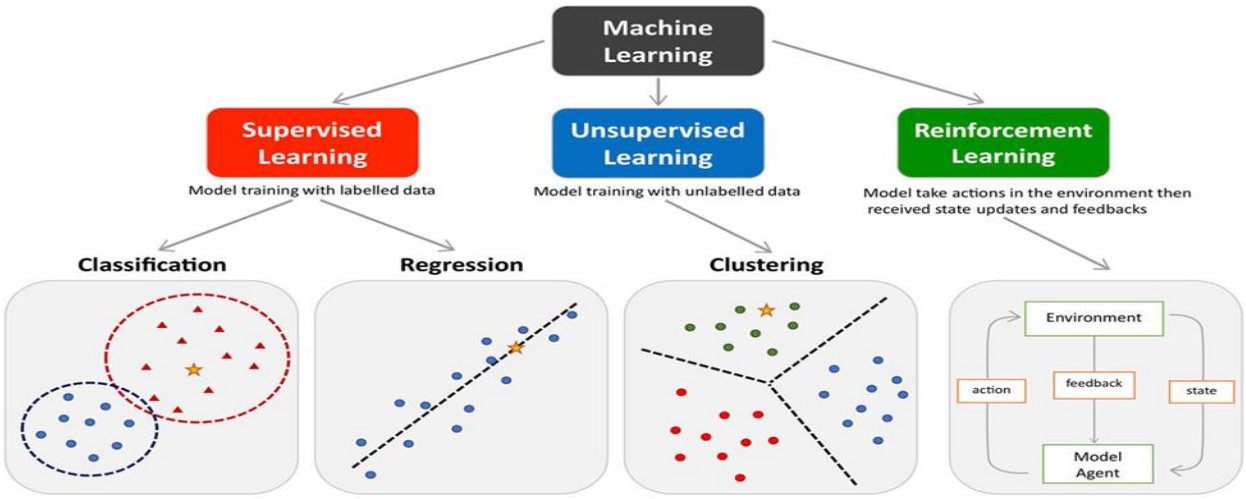

Figure 1. Main types of ML [15]

Table 1. ML techniques [9][16]

ML techniques	Description
Supervised Learning	Is a method that takes labeled data to map inputs to outputs to solve classification and regression problems.
Unsupervised Learning:	This is a type of learning that detects regularities in unlabeled data and is applied in clustering, dimensionality reduction, and association learning.
Reinforcement Learning (RL):	It learns by interacting with the environment by trial and error. Semi-Supervised Learning: It involves the use of both labeled and unlabeled data to enhance model performance.

2. 2 Deep Learning

(DL) is a specialized sub-field of Machine Learning that speculates on representation learning, consisting of multilayer transformations, enhancing accuracy in detection and prediction tasks. DL-based systems are also being employed in information security to automate the process of threat detection and improve their functionality as time progresses [17] [18]

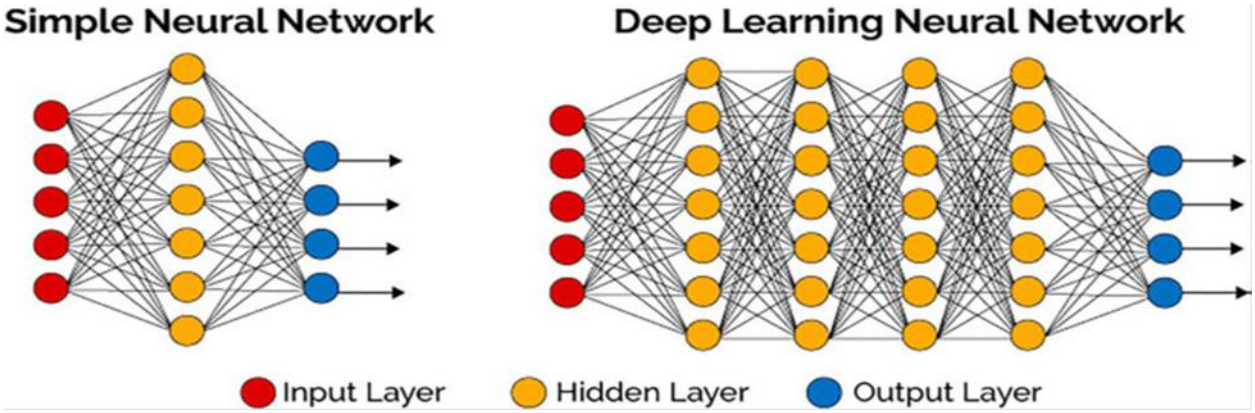

Figure 2. NN VS DNN [19]

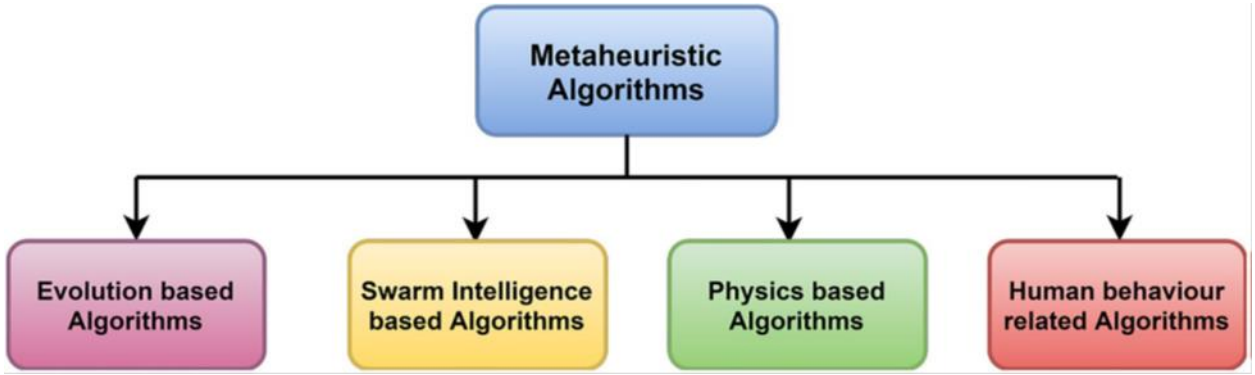

Figure 3. Metaheuristic algorithms classification [20]

Metaheuristic algorithms are advanced global optimization techniques that balance exploration (searching the solution space) and exploitation (refining promising regions), inspired by the social and collective behaviors of organisms such as birds, fish, and ants. These algorithms have demonstrated significant effectiveness in addressing complex real-world optimization problems [21]. Metaheuristics are classified into four main categories evolution-based, swarm intelligence-based, physics-based, and human-inspired algorithms according to their sources of inspiration. In the domain of cyber-security, integrating artificial intelligence, machine learning, and deep learning with metaheuristic algorithms has proven effective in enhancing cyber-attack detection [22][23] .

3.DATASET

For an algorithm to learn, a dataset serves as a collection of data used to train the model, where the training data consists of pre-labeled classes. The following are the publicly available datasets commonly utilized by researchers to evaluate and experiment with their proposed intrusion detection approaches: KDD CUP 99, NSL-KDD, UNSW-NB15, CICIDS2017, CICIDS2018, and ToN_IoT (refer to Figure 4). Therefore, the following sub-section presents a report on the dataset and the attacks [24].

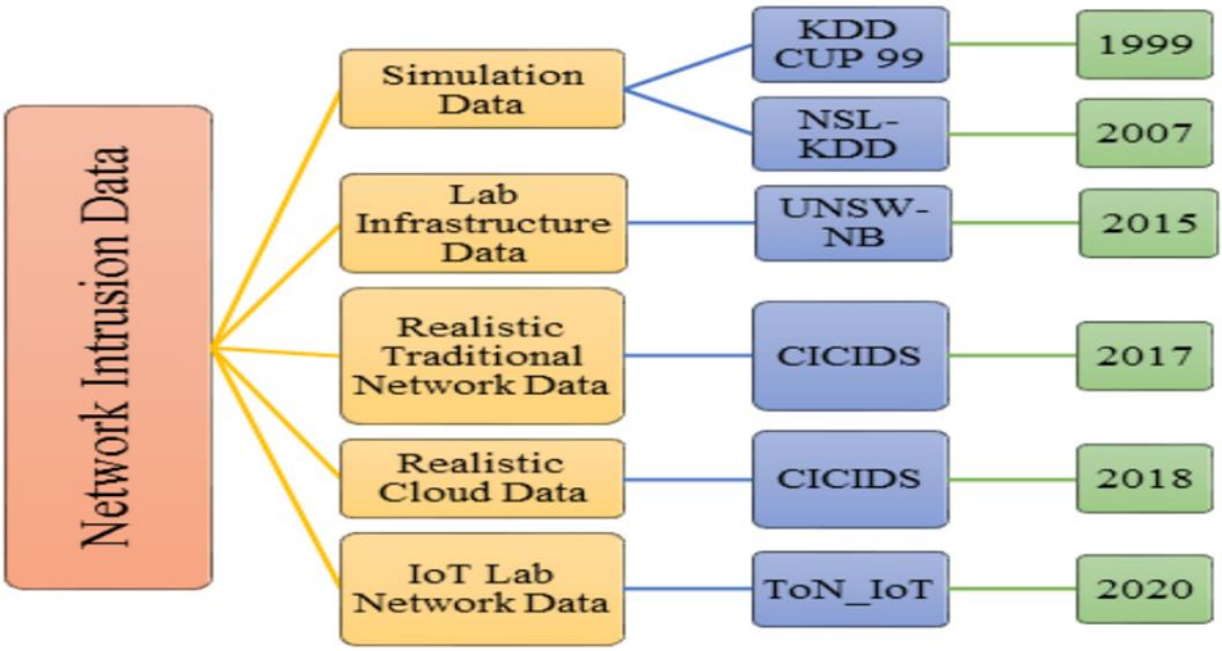

Figure 4. Data Network [24]

3. 1 The KDD CUP 99

introduced by MIT Lincoln Labs in 1998, is one of the most extensively employed benchmark datasets for the evaluation of intrusion detection systems, particularly those leveraging artificial intelligence techniques [25].It comprises nearly five million records divided into training and testing subsets, with approximately 80% of the data corresponding to malicious activities. The dataset is organized into normal traffic and four primary categories of attacks Denial of Service (DoS), User to Root (U2R), Remote to Local (R2L), and Probing encompassing 22 distinct attack types. All records are represented by 41 attributes, which characterize different aspects of network activity, such as basic attributes of connections (e.g., type of protocol, duration, and service), content-dependent aspects (e.g., failed login attempts and urgent packets), and statistic traffic characteristics (e.g., frequency of connections within a given time interval). All these aspects present a holistic description of the work of the network, thus forming a vital basis of training and testing machine learning models in the field of intrusion detection studies [26].

3. 2 The NSL-KDD

was proposed to overcome a number of drawbacks of the original KDD CUP 99 dataset, especially the problem of redundancy and imbalance. Compared to its predecessor, it does not have redundant records, and it also shrinks the data, making it easier to execute and analyze machine learning algorithms. Just like KDD CUP 99, NSL-KDD has 41 extracted features, which are basic, content-related, and traffic-related features, but it includes binary features that represent the existence or the absence of certain attributes found in network connections. These binary attributes make the dataset more representative of the various types of attacks, reducing the bias on the most frequent classes and allowing a more reliable and accurate evaluation of the intrusion detection models [27][28] .

3. 3 The UNSW-NB15

created with the IXIA Perfect Storm tool, was created to have a more modern and holistic benchmark of intrusion detection research that overcomes some of the shortcomings of previous datasets, like KDD CUP 99 and NSL-KDD. It also has modern attack scenarios and closer-to-life traffic patterns, as opposed to its predecessors, which makes it very applicable to the present use of cyber-security. The sample size is 175,341 normal records and 82,332 anomaly records; the attack types are worms, shell code, reconnaissance, generic, exploits, denial of service (DoS), backdoors, and analysis. Each record is attributed to 49 features capturing various facets of network traffic, such as basic connection information (e.g. IP addresses, port numbers, protocol type, and connection flags), information about content (e.g. number of bytes transferred, connection length, and packet counts), and characterizations of statistical flows (e.g. These characteristics allow modeling and testing machine learning models to detect intrusions in contemporary network settings in a detailed and realistic manner and understand network activity [29] [30] .

3. 4 The CICIDS2017

The dataset includes attack scenarios recommended in the 2016 McAfee report namely Distributed Denial of Service (DDoS), Botnet, Infiltration, Web Attacks, Heartbleed, and Denial of Service (DoS)and employs B-Profile and Alpha-Profile systems to model user behavior and attack simulations. To ensure realism, it adheres to 11 evaluation criteria, including full traffic capture, protocol diversity, and labeled ground truth. CICIDS2017 comprises 78 extracted features that represent various aspects of network traffic, including basic connection attributes (e.g., IP addresses, ports, and protocol types), content-related properties (e.g., transmitted bytes and packet counts), statistical flow measures (e.g., packet length and inter-arrival time distributions), connection-based behavior (e.g., frequency of connections per host or service), time-related indicators, and host-based attributes . This rich feature set provides a realistic and detailed representation of network operations, making CICIDS2017 a widely adopted dataset for developing and evaluating machine learning-based intrusion detection and cyber-security solutions [31][32] [33].

3. 5 The CICIDS2018

developed through collaboration between the Canadian Institute for Communications Security Establishment (CSE), extends the scope of its predecessor, CICIDS2017, by providing a more comprehensive and diverse representation of modern network traffic. Collected over a period of ten days (February 14 to March 2, 2018) within an Amazon Web Services (AWS) environment, it incorporates multiple topologies and larger volumes of data to enhance realism. The dataset includes a wide range of attack scenarios, such as brute-force, denial of service, Hulk, , Heartbleed, web-based attacks , infiltration from internal networks, botnets, and distributed denial of service (DDoS) with port scanning. Each instance is described by 79 extracted features covering basic connection attributes, content-related properties, statistical traffic characteristics, and behavioral and time-based indicators, as well as host-based and flow-level insights. Owing to its scale, diversity, and realistic design, CICIDS2018 is regarded as one of the most complete and representative benchmark datasets for evaluating machine learning approaches in intrusion detection and cyber-security research [34][35] [36] .

3. 6 The TON_IoT

represents a next-generation benchmark for Internet of Things (IoT) and Industrial IoT (IIoT) cyber-security research, particularly for evaluating artificial intelligence-based detection and defense systems. It comprises heterogeneous data sources, including telemetry from IoT and IIoT sensors, operating system logs from Windows 7/10 and Ubuntu 14/18, and network traffic datasets. The data were collected from a large-scale, realistic testbed at the IoT Lab of UNSW Canberra Cyber, incorporating virtual machines, physical systems, cloud and fog platforms, and diverse IoT/IIoT devices to replicate the complexity and scalability of industrial networks and Industry 4.0 environments. Data collection was performed in parallel to capture both normal and malicious activities across the network. The dataset includes multiple feature types, such as sensor measurements, network communication attributes, device metadata, time-based indicators, contextual features, and derived features, providing a comprehensive representation of IoT/IIoT operations. This rich and diverse feature set makes TON_IoT particularly suitable for developing and evaluating AI-driven intrusion detection and cyber-security solutions in connected and industrial environments [37][38] .

Table 2. Characteristics for building an ideal Data [24]

Characteristic	Description
Network Configuration	It means possessing full knowledge regarding the network topology of the connection of the networking devices within the testing environment to ensure that real-life attack scenarios are simulated.
Network Traffic	It means that all the network packets exchanged between the host, destination, firewall, and web applications are captured to be analyzed into flows and generate datasets.
Labeled Dataset	The process of attaching the data instances observed in the network traffic to fully understand the network interaction is referred to as tagging.
Network Interaction	It is the possession of the full history of network communication that occurs both in and out of the network.
Capturing the Traffic	It means that the functional and non-functional network traffic is captured to measure the DR and FPR of the IDS.
Protocols	The best dataset must consist of all the communication with different protocols, both normal and malicious.
Attacks	The dataset must encompass a wide range of up-to-date attack categories.
Anonymity	The packet header information and that of the packet payload should be included in the dataset.
Heterogeneity	The data must be gathered based on divergent sources to encompass all the aspects of the process followed to identify the attacks.
Features	The dataset should include a comprehensive and clearly defined set of features to accurately classify the attack.
Metadata	The dataset must include concise, complete documentation of the testing environment, attacker and victim system architectures, and attack scenarios to ensure reproducibility and accurate evaluation.

4. Literature review

AI development has enabled real-time analysis and decision-making on large datasets, crucial for information security, reducing the time, cost, and reliance on human expertise for threat detection [8].AI has become vital in information security, enabling accurate analysis of large data, prediction and prevention of attacks, and adaptive responses to evolving threat patterns [39].Using AI in security presents challenges, as it requires large datasets and intensive processing, while false alarms and delayed responses can undermine system efficiency and user trust [39] .Asiri et al (2023) [40], The HMFS-SDLCAD model was introduced for IoT attack detection, combining metaheuristic feature selection with Stacked BiGRU, and was shown to outperform existing methods in real-time detection. An et al (2023) [41] ,V-CNN The CNN model was created to detect vulnerabilities, with a 98% accuracy rate, and it significantly surpasses RF, which is further moving AI to cyber-security. Lucky et al (2023) [42], A distributed architecture based on lightweight was suggested to identify and forestall DDoS attacks at a rate of more than 99.9%. Ok, a strong feature selection technique was used that tested both CICIDS 2017 and 2019 and only needed 7% processing and no network overhead, which shows that effective and quick DDoS response is possible. Soliman et al (2023) [43] ,A DL-based IIoT IDS was trained, where SVD was employed to reduce the number of features and SMOTE was used to tackle the imbalance issue, which resulted in 99.99% binary and 99.98% on the ToN-IoT 99.98% three-class accuracy. Psychogyios et al (2024) [44], A DL model combining CNNs, LSTMs, and attention was introduced for IDS, achieving near real-time performance and improving F1 by 8% over standalone LSTM on UNSW-NB15.Atawneh et al (2023) [45], BERT and LSTM models of DL were employed, and their results showed that they could detect phishing at 99.61%, which demonstrates their capability to improve the field of cyber-security. Asiri et al (2024) [46] ,A BiLSTM with attention was tested to improve real-time phishing detection with an accuracy of 99, and WeAS was observed to be the best choice of decision strategy. Sharmaet al(2023) [47] ,A hybrid model combining MLPs and decision trees (DTs) was proposed for real-time intrusion detection. It was found to outperform traditional methods, showing higher accuracy, fewer false positives, and strong potential as a future cyber-security solution .Butt et al (2023) [48] , Phishing was examined using cloud-based ML and DL technologies. The trio of SVM, NB, and LSTM were seen to be highly accurate, with the SVM standing at 99.62, presenting the prospect of a hybrid ML method in bolstering email security. Awajan et al (2023) [49] , A four-layer fully connected neural network was created as a DL-based intrusion detection system for IoT devices. It had an accuracy of 93.74% and was able to identify Blackhole, DDoS, Opportunistic Service, Sinkhole, and Wormhole attacks and was resource-efficient with a detection rate of 93.21.Kasongo et al (2023) **[**50] ,XGBoost-based feature selection combined with RNN models was shown to reduce feature dimensionality and improve detection performance, achieving 88.13% accuracy on NSL-KDD and 87.07% on UNSW-NB15 with minimal computational cost. Dalal et al (2025) [51] , A hybrid IDS using GWO and BPR was proposed, where GWO

was used for feature reduction and BPR for classification, achieving up to 99.88% accuracy on NSL-KDD and UNSW-NB15, proving effective for real-time detection. Zaman et al (2025) [52] ,It has been suggested that Deep Cyber-IDS is a deep learning-based system employing CNN, GRU, and LSTM to process raw network traffic without feature engineering. Accuracies of up to 99.84 were obtained on NSL-KDD, UNSW-NB15, and SmartGrid datasets with great F1, precision, and recall, and relatively low processing times (469 ms to 53 s), which are appropriate in real-time monitoring.

Table 3: Literature review

Author(s)	**Methodology**	**Datasets Used**	**Advantage**	**Limitation**
An et al., (2023)	CNN detects vulnerabilities from preprocessed data.	Public vulnerability datasets: ~10,000 CVE instances and ~5,000 CWE instances.	High accuracy (>95%), scalable to large codebases, automates detection, adaptable to different datasets.	Performance depends on data quality, CNNs are complex to implement, limited interpretability
Lucky et al., (2023)	Lightweight decision tree for fast DDoS detection.	CICIDS 2017 and CICIDS2019 data	Accuracy >99.9%Low CPU usage No network overhead	Only DDoS Limited datasets
Soliman et al., (2023)	Features reduced by SVD, balanced with SMOTE, classified using ML/DL.	ToN_IoT	Very high accuracy, handles imbalance, reduces features	Data-dependent, computationally heavy
Atawneh et al., (2023)	Deep learning (LSTM, BERT) with NLP-based feature extraction.	Phishing & benign emails.	Very high accuracy (99.61%).	High computational cost; may overfit on small datasets.
Sharmaet al., (2023)	Hierarchical attention hybrid deep learning model for email spam detection.	Spam and legitimate email datasets (text-based).	high detection accuracy; captures contextual information via hierarchical attention.	Requires significant computational resources; may overfit on small datasets.
Kasongo et al (2023)	RNNs with XGBoost for efficient intrusion detection.	NSL-KDD UNSW-NB15.	Efficient, captures temporal patterns, good accuracy.	High training time, GRU less accurate on some datasets, may struggle with unseen attacks.
Awajan et al .,(2023)	Deep Learning-based IDS using a 4-layer fully connected network.	Simulated and real IoT intrusion data.	Real-time detection, high accuracy, reliable on multiple attack types, easy deployment.	Potential resource constraints on IoT devices; generalization to unseen attacks not discussed.

Butt et al ., (2023)	Cloud-based system using ML and deep learning (e.g., SVM/RF + CNN/LSTM) for phishing detection and scalable deployment.	Phishing & benign emails/URLs (hosted/processed in cloud).	Scalable real-time detection; centralised updates and model deployment.	Privacy and latency concerns; higher infrastructure cost; reliance on cloud availability.
Asiri et al., (2023)	Feature selection is performed using SSOPSO, while attack classification is conducted with stacked SBiGRU.	Benchmark Dataset.	Enhances IoT attack detection via DL on selected features.	Computationally intensive and dataset unspecified.
Psychogyios et al .,(2024)	Convert IDS data to time series and use CNN and LSTM and Attention for attack prediction.	Classic IDS dataset (converted to time series format).	Proactive detection, high F1 and AUC scores, ~8% improvement over LSTM.	Computationally intensive, relies on quality of time series conversion, complex architecture
Asiri et al ., (2024)	BiLSTM and attention for URL classification; browser extension & Docker for URL extraction	Phishing & benign URLs (TinyURL, BiTB, regular phishing).	High accuracy (~99%).	Complex setup; higher computational cost.
Dalal et al., (2025)	Hybrid IDS using Bayesian Probit Regression for classification and Grey Wolf Optimizer for feature selection.	NSL-KDD and UNSW-NB15	High accuracy, fast detection, efficient feature reduction, real-time capable.	Benchmark-only testing, sensitive to parameter tuning, may need high computational resources.
Zaman et al., (2025)	Deep Cyber-IDS using CNN, GRU, and LSTM to learn from raw network traffic without manual feature engineering.	NSL-KDD, UNSW-NB15, SmartGrid	High accuracy, perfect precision/recall on some datasets, real-time capable, adaptable to evolving threats.	Only benchmark-tested, processing can be up to 53s, may need high computational resources.

5. AI-DRIVEN INTRUSION DETECTION SYSTEMS (IDS)

The theoretical framework for AI-driven Intrusion Detection Systems (IDS) is grounded in principles from both machine learning and cyber-security domains [53] [54].At its core, the framework relies on the following key components:

- Machine Learning Algorithms: AI-driven IDS employ techniques such as neural networks, decision trees, support vector machines, and clustering to accurately distinguish between normal and malicious network activities.
- Feature Extraction and Selection The raw network data is converted to useful features and the most valuable ones are selected in order to create fewer dimensions and less computation cost with the least detection loss.

- Anomaly Detection: These are the statistical analysis, unsupervised learning and clustering of the system which are used to detect the potential intrusion by detecting the variations of the established patterns of normal functioning in the system.
- Ensemble Learning: The methods of bagging, boosting and stacking are applied to obtain robustness, reduce overfitting, and enhance the overall detection.
- Real-Time Adaptation and Feedback Loop: The system will be online learning the system as it will be updating its model online which will make the system dynamism in the process of reacting to emerging threats and the change in attack patterns.
- Cyber Threat Intelligence Integration: External threat intelligence feeds are crucial to provide context about known threats, malware signatures, and indicators of compromise to enhance the prioritization and detection capabilities of alerts.
- Model Interpretability and Explainability: Transparency is ensured through techniques such as the feature importance analysis and model visualization that enable the security practitioners to comprehend and trust system.

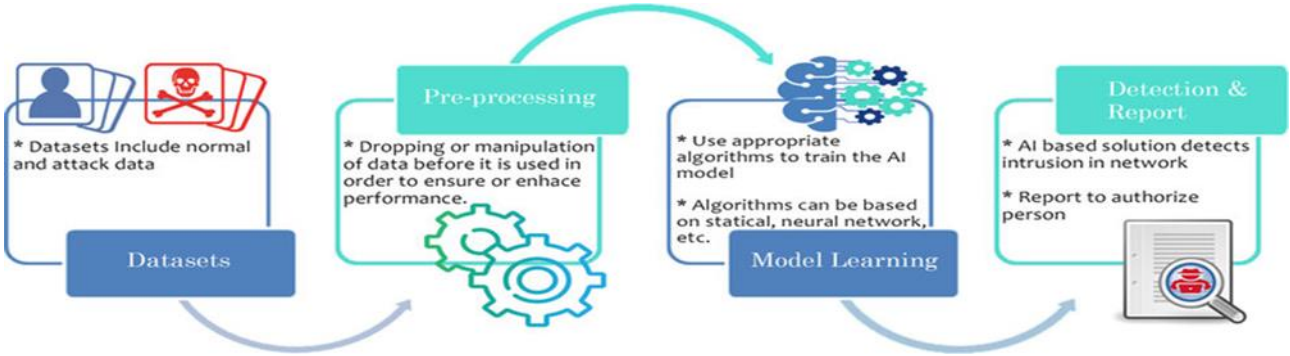

Figure 5. The architecture of AI based IDS [55]

6.COMPARATIVE ANALYSIS

AI-driven IDS are evaluated against traditional solutions based on [56] [57] :

- Detection Accuracy: Capacity to detect threats at reduced false positives and false negatives.
- Scalability: Scaling to high network traffic and distributed systems.
- Adaptability: Real-time detecting of the emergent threats and revising of strategies.
- Response Time: Rapidity of threat detection/response.
- Strong integrity: Vulnerability to evasion methodology and adversarial attacks.
- Cost-Effectiveness: Trade-off between implementation and maintenance cost and security.
- Usability: Convenience of configuration, administration, and monitoring.
- Compliance: The data privacy and regulatory standards. This assessment assists organizations in selecting the best IDS solutions that support their security and operation requirements.

7. LIMITATIONS & DRAWBACKS

Despite their advantages, AI-driven Intrusion Detection Systems (IDS) face several challenges [58] [59]

- Data Dependency: Performance relies on large, high-quality labeled datasets, which are difficult to obtain, especially for rare or novel threats.
- Overfitting: Models may memorize training data rather than generalizing, leading to reduced accuracy on unseen traffic and higher false positives.
- Adversarial Attacks: IDS are vulnerable to carefully crafted inputs designed to evade detection or trigger false alarms.
- Model Interpretability: Complex models often lack transparency, making it difficult for analysts to trust and validate decisions.
- Resource Intensiveness: Training and deployment require significant computational power, storage, and skilled personnel, challenging organizations with limited resources.
- Maintenance and Updates: Continuous retraining and tuning are necessary to adapt to evolving threats; neglect can degrade performance.
- Ethical and Legal Concerns: Data privacy, bias, and accountability issues may arise, particularly when handling sensitive information.

- Single Point of Failure: Relying solely on AI-driven IDS can leave networks vulnerable if the system fails, necessitating complementary security measures.

Addressing these limitations requires robust data management, adversarial defenses, interpretability techniques, and ongoing monitoring to ensure the IDS remains effective and reliable.

8. Conclusion

The new generation of cyber-attacks has rendered traditional Intrusion Detection Systems (IDS) obsolete, emphasizing that security solutions must be intelligent and dynamic rather than simplistic. This paper has shown that Artificial Intelligence (AI) can help the work of IDS in a great way to improve the process of progressive machine learning to monitor and respond to attacks within several seconds. The known and the unknown attacks will be recognized more effectively in the case of the AI-based IDS, the false alarms will be reduced, and the changing nature of the attacks will also be adapted successfully. However, it is not that simple, as huge data are being trusted, adversarial attacks are subject to attack, and clearer and explicatory models are demanded. To make these systems more dependable, comprehensible, and safe, it should be done with continuous research and development. However, AI-based IDS may be viewed as a desirable initiative to increase the safety of the network. The modern globalized world could also apply artificial intelligence to help establish more stable and adaptable security systems that would be able to protect sensitive information and digital backbones with the further collaboration of researchers, businesses, and governments.

ACKNOWLEDGEMENTS

Many thanks to the entire respected editorial team.

REFERENCES

[1] P. Parkar and A. Bilimoria, “A survey on cyber security IDS using ML methods,” in *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*, IEEE, 2021, pp. 352–360.

[2] N. S. Musa, N. M. Mirza, S. H. Rafique, A. M. Abdallah, and T. Murugan, “machine learning and deep learning techniques for distributed denial of service anomaly detection in software defined networks—current research solutions,” *IEEE Access*, vol. 12, pp. 17982–18011, 2024.

[3] M. Eswaran, S. Hamsanandhini, and K. I. Lakshmi, “Survey of cyber security approaches for attack detection and prevention,” *Turkish J. Comput. Math. Educ.*, vol. 12, no. 2, pp. 3436–3441, 2021.

[4] J. Alsamiri and K. Alsubhi, “Internet of things cyber attacks detection using machine learning,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 12, 2019.

[5] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, “Cyber security in iot-based cloud computing: A comprehensive survey,” *Electronics*, vol. 11, no. 1, p. 16, 2021.

[6] K. Morovat and B. Panda, “A survey of artificial intelligence in cybersecurity,” in *2020 International conference on computational science and computational intelligence (CSCI)*, IEEE, 2020, pp. 109–115.

[7] J. Li, “Cyber security meets artificial intelligence: a survey,” *Front. Inf. Technol. Electron. Eng.*, vol. 19, no. 12, pp. 1462–1474, 2018.

[8] N. B. Dokur, “Artificial Intelligence (AI) applications in cyber security,” *Comput. Eng. MEF Univ. Istanbul, Turkey. URL https//www. Res. net/publication/367253331*, 2023.

[9] T. Thomas, A. P. Vijayaraghavan, and S. Emmanuel, *Machine learning approaches in cyber security analytics*. Springer, 2019.

[10] K. Barik, S. Misra, K. Konar, L. Fernandez-Sanz, and M. Koyuncu, “Cybersecurity deep: approaches, attacks dataset, and comparative study,” *Appl. Artif. Intell.*, vol. 36, no. 1, p. 2055399, 2022.

[11] “A comparative analysis of metaheuristic algorithms in fuzzy modelling for phishing attack detection,” *Indones. J. Electr. Eng. Comput. Sci*, vol. 23, no. 2, pp. 1146–1158, 2021.

[12] H. Zhang, X. Yu, P. Ren, C. Luo, and G. Min, “Deep adversarial learning in intrusion detection: A data augmentation enhanced framework,” *arXiv Prepr. arXiv1901.07949*, 2019.

[13] G. S. Kuntla, X. Tian, and Z. Li, “Security and privacy in machine learning: A survey.,” *Issues Inf. Syst.*, vol. 22, no. 3, 2021.

[14] J. G. Carbonell, R. S. Michalski, and T. M. Mitchell, “An overview of machine learning,” *Mach. Learn.*, pp. 3–23, 1983.

[15] J. Peng, E. C. Jury, P. Dönnes, and C. Ciurtin, “Machine learning techniques for personalised medicine approaches in immune-mediated chronic inflammatory diseases: applications and challenges,” *Front. Pharmacol.*, vol. 12, p. 720694, 2021.

[16] R. Muhamedyev, “Machine learning methods: An overview,” *Comput. Model. new Technol.*, vol. 19, no. 6, pp. 14–29, 2015.

[17] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, “Cybersecurity data

science: an overview from machine learning perspective," *J. Big data*, vol. 7, no. 1, p. 41, 2020.

[18] A. Shrestha and A. Mahmood, "Review of deep learning algorithms and architectures," *IEEE access*, vol. 7, pp. 53040–53065, 2019.

[19] F. Pourafshin, "Big data mining in internet of things using fusion of deep features," *Int J Sci Res Eng Trends*, vol. 7, no. 2, pp. 1089–1093, 2021.

[20] A. H. Salem, S. M. Azzam, O. E. Emam, and A. A. Abohany, "Advancing cybersecurity: a comprehensive review of AI-driven detection techniques," *J. Big Data*, vol. 11, no. 1, p. 105, 2024.

[21] M. Abdel-Basset, L. Abdel-Fatah, and A. K. Sangaiah, "Metaheuristic algorithms: A comprehensive review," *Comput. Intell. Multimed. big data cloud with Eng. Appl.*, pp. 185–231, 2018.

[22] A. H. Gandomi, X.-S. Yang, S. Talatahari, and A. H. Alavi, "Metaheuristic algorithms," *Metaheuristic Appl. Struct. infrastructures*, pp. 1–24, 2013.

[23] I. H. Hassan, A. Mohammed, and M. A. Masama, "Metaheuristic algorithms in network intrusion detection," *Compr. metaheuristics*, pp. 95–129, 2023.

[24] A. Gharib, I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "An evaluation framework for intrusion detection dataset," in *2016 International conference on information science and security (ICISS)*, IEEE, 2016, pp. 1–6.

[25] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *2009 IEEE symposium on computational intelligence for security and defense applications*, Ieee, 2009, pp. 1–6.

[26] T. Eldos, M. K. Siddiqui, and A. Kanan, "On the KDD'99 dataset: Statistical analysis for feature selection," *J. Data Min. Knowl. Discov.*, vol. 3, no. 3, p. 88, 2012.

[27] L. Dhanabal and S. P. Shantharajah, "A study on NSL-KDD dataset for intrusion detection system based on classification algorithms," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 4, no. 6, pp. 446–452, 2015.

[28] M. Jiang *et al.*, "Text classification based on deep belief network and softmax regression," *Neural Comput. Appl.*, vol. 29, no. 1, pp. 61–70, 2018.

[29] S. Meftah, T. Rachidi, and N. Assem, "Network based intrusion detection using the UNSW-NB15 dataset," *Int. J. Comput. Digit. Syst.*, vol. 8, no. 5, pp. 478–487, 2019.

[30] L. P. Dias, J. de J. F. Cerqueira, K. D. R. Assis, and R. C. Almeida, "Using artificial neural network in intrusion detection systems to computer networks," in *2017 9th Computer Science and Electronic Engineering (CEEC)*, IEEE, 2017, pp. 145–150.

[31] D. Stiawan, M. Y. Bin Idris, A. M. Bamhdi, and R. Budiarto, "CICIDS-2017 dataset feature analysis with information gain for anomaly detection," *IEEE Access*, vol. 8, pp. 132911–132921, 2020.

[32] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, "A detailed analysis of the cicids2017 data set," in *International conference on information systems security and privacy*, Springer, 2018, pp. 172–188.

[33] A. Boukhamla and J. C. Gaviro, "CICIDS2017 dataset: performance improvements and validation as a robust intrusion detection system testbed," *Int. J. Inf. Comput. Secur.*, vol. 16, no. 1–2, pp. 20–32, 2021.

[34] M. Cantone, C. Marocco, and A. Bria, "Generalization Challenges in Network Intrusion Detection: A Study on CIC-IDS2017 and CSE-CIC-IDS2018 Datasets," in *1st INTERNATIONAL PhD SYMPOSIUM ON ENGINEERING AND SPORT SCIENCE*, 2024, p. 185.

[35] M. Gopalsamy, "Predictive cyber attack detection in cloud environments with machine learning from the CICIDS 2018 dataset," in *IJSART*, 2024, pp. 36–46.

[36] B. I. Farhan and A. D. Jasim, "Performance analysis of intrusion detection for deep learning model based on CSE-CIC-IDS2018 dataset," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 26, no. 2, pp. 1165–1172, 2022.

[37] G. Guo, X. Pan, H. Liu, F. Li, L. Pei, and K. Hu, "An IoT intrusion detection system based on TON IoT network dataset," in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, 2023, pp. 333–338.

[38] N. Moustafa, M. Keshky, E. Debiez, and H. Janicke, "Federated TON_IoT Windows datasets for evaluating AI-based security applications," in *2020 IEEE 19th international conference on trust, security and privacy in computing and communications (TrustCom)*, IEEE, 2020, pp. 848–855.

[39] D. Aggarwal, D. Sharma, and A. B. Saxena, "Role of AI in cyber security through Anomaly detection and Predictive analysis," *J. Informatics Educ. Res.*, vol. 3, no. 2, pp. 1846–1849, 2023.

[40] M. M. Asiri *et al.*, "Hybrid Metaheuristics Feature Selection with Stacked Deep Learning-Enabled Cyber-Attack Detection Model.," *Comput. Syst. Sci. Eng.*, vol. 45, no. 2, pp. 1679–1694, 2023.

[41] J. H. An, Z. Wang, and I. Joe, "A CNN-based automatic vulnerability detection," *EURASIP J. Wirel. Commun. Netw.*, vol. 2023, no. 1, p. 41, 2023.

[42] G. Lucky, F. Jjunju, and A. Marshall, "A lightweight decision-tree algorithm for detecting DDoS flooding attacks," in *2020 IEEE 20th international conference on software quality, reliability and security companion (QRS-C)*, IEEE, 2020, pp. 382–389.

[43] S. Soliman, W. Oudah, and A. Aljuhani, "Deep learning-based intrusion detection approach for securing

industrial Internet of Things," *Alexandria Eng. J.*, vol. 81, pp. 371–383, 2023.
[44] K. Psychogyios, A. Papadakis, S. Bourou, N. Nikolaou, A. Maniatis, and T. Zahariadis, "Deep learning for intrusion detection systems (IDSs) in time series data," *Futur. Internet*, vol. 16, no. 3, p. 73, 2024.
[45] S. Atawneh and H. Aljehani, "Phishing email detection model using deep learning," *Electronics*, vol. 12, no. 20, p. 4261, 2023.
[46] S. Asiri, Y. Xiao, S. Alzahrani, and T. Li, "PhishingRTDS: A real-time detection system for phishing attacks using a Deep Learning model," *Comput. Secur.*, vol. 141, p. 103843, 2024.
[47] S. Zavrak and S. Yilmaz, "Email spam detection using hierarchical attention hybrid deep learning method," *Expert Syst. Appl.*, vol. 233, p. 120977, 2023.
[48] U. A. Butt, R. Amin, H. Aldabbas, S. Mohan, B. Alouffi, and A. Ahmadian, "Cloud-based email phishing attack using machine and deep learning algorithm," *Complex Intell. Syst.*, vol. 9, no. 3, pp. 3043–3070, 2023.
[49] A. Awajan, "A novel deep learning-based intrusion detection system for IOT networks," *Computers*, vol. 12, no. 2, p. 34, 2023.
[50] S. M. Kasongo, "A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework," *Comput. Commun.*, vol. 199, pp. 113–125, 2023.
[51] D. A. Hammood, L. H. M. Alzayadi, M. S. Mahmoud, and M. M. Abd Zaid, "Efficient Hybrid Intrusion Detection Approach based on BPR-GWO for Network Traffic Classification and Improved Network Security.," *Int. J. Intell. Eng. Syst.*, vol. 18, no. 8, 2025.
[52] Z. N. Hussein, D. A. Hammood, and Z. Q. Al-Abbasi, "DeepCyber-IDS: A Deep Learning Based Intrusion Detection System," in *2025 VI International Conference on Neural Networks and Neurotechnologies (NeuroNT)*, IEEE, 2025, pp. 62–65.
[53] M.-H. Yang, "AI-Driven Cybersecurity: Intrusion Detection Using Deep Learning," *Multidiscip. Innov. Res. Anal.*, vol. 3, no. 4, pp. 1–14, 2022.
[54] M. Goswami, "Enhancing Network Security with AI-Driven Intrusion Detection Systems," *Volume*.
[55] A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," *Knowledge-Based Syst.*, vol. 189, p. 105124, 2020.
[56] M. Markevych and M. Dawson, "A review of enhancing intrusion detection systems for cybersecurity using artificial intelligence (ai)," in *International conference knowledge-based organization*, 2023, pp. 30–37.
[57] A. Raza, A. K. S. Ali, and A. A. Hussain, "AI-DRIVEN APPROACHES TO CYBER AND INFORMATION SECURITY: MACHINE LEARNING ALGORITHMS FOR THREAT PREDICTION AND ANOMALY DETECTION," *Spectr. Eng. Sci.*, vol. 2, no. 4, pp. 565–573, 2024.
[58] J. P. Kushwaha, S. Bhadauria, and S. Tapaswi, "Unveiling IoT ecosystem security: A review of intelligent IDS, trends, challenges, and future directions," *Comput. Electr. Eng.*, vol. 128, p. 110626, 2025.
[59] M. S. R. S. Raja, "The Rise of AI-Driven Network Intrusion Detection Systems: Innovations, Challenges, and Future Directions," *Int. J. AI, BigData, Comput. Manag. Stud.*, vol. 1, no. 1, pp. 1–10, 2025.