RESEARCH PAPER

Artificial Intelligence–Driven Intrusion Detection Systems: A Systematic Review of Machine Learning, Deep Learning, and Adaptive Ensemble Approaches

Dr. Mohammed Saleh Al-Shizawi[1*], Omer Ahmed Siddig Ahmed[2], Dr. Fayez Sobhy Abdelsalam Torky[3], Dr. Adil bin Hamdan bin Zayed Al-Rudaini[4], Sheikha bint Suhail Al-Sawwafi[5], Moosa Saleh Al-Shizawi[6], Yahya Mohammed Al-Balushi[7]

[1]Assistant Professor of Grammar and Morphology, Department of Arabic Language, College of Arts and Social Sciences, Sultan Qaboos University, Muscat, Sultanate of Oman. ORCID: https://orcid.org/0009-0003-0958-652X. Email: m.alshizawi@squ.edu.om

[2]Department of Arabic Language and Literature, College of Arts and Social Sciences, Sultan Qaboos University, Al-Khoud, Muscat, Oman. ORCID: https://orcid.org/0009-0004-7422-4864. Email: almagzoob@squ.edu.om

[3]Associate Professor of Grammar, Morphology, and Prosody, College of Arts and Social Sciences, Sultan Qaboos University. ORCID: https://orcid.org/0000-0002-7615-268X. Email: f.torky@squ.edu.om

[4]Assistant Professor of Linguistics and Grammar, Sohar University, Faculty of Education and Arts, Department of Arabic Language. ORCID: https://orcid.org/0009-0005-2213-0775. Email: arudaini@su.edu.om

[5]Master's Student, Department of Arabic Language, College of Arts and Social Sciences, Sultan Qaboos University, Muscat, Sultan of Oman. ORCID: https://orcid.org/my-orcid. Email: s120877@student.squ.edu.om

[6]Master's Student, Department of Arabic Language, College of Arts, Nizwa University, Sultan of Oman. ORCID: https://orcid.org/0009-0005-5791-5599. Email: 10252334@uofn.edu.om

[7]PhD Researcher in Grammar and Morphology, Sultan Qaboos University, Muscat, Sultanate of Oman. ORCID: https://orcid.org/0009-0008-5950-789X. Email: s15656@student.squ.edu.om

***Corresponding author: Dr. Mohammed Saleh Al-Shizawi, Assistant Professor of Grammar and Morphology, Department of Arabic Language, College of Arts and Social Sciences, Sultan Qaboos University, Muscat, Sultanate of Oman.**

Abstract

This is a critical systematic review of 40 peer-reviewed articles published between 2021 and 2025 on artificial intelligence-enhanced Intrusion Detection Systems (IDS). To maintain rigour and transparency in the review, the PRISMA 2020 and Kitchenham guidelines are adhered to. The appropriate literature was also searched in six major databases, such as IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, Scopus, and Web of Science, and concentrated on the IDS methods, which used machine learning (ML), deep learning (DL), reinforcement learning (RL), and ensemble methods. The results show that there is a clear shift of traditional ML algorithms, including SVM and Random Forest, towards advanced deep learning and hybrid ensemble models that have a higher detection accuracy and flexibility in a variety of benchmark datasets, including CICIDS2017 and UNSW-NB15. The frameworks of reinforcement learning also increase the autonomy of IDS by learning on its own and adapting dynamically, but they have difficulties with the issues of computational efficiency, and the stability of the convergence. On the whole, the review demonstrates that there is ongoing methodological standardization deficit, diversity of datasets, and inter-study reproducibility absence. It finds that explainable, adaptive, and federated AI models should be the main focus of future IDS studies to attain scalable, transparent, and trustworthy cybersecurity frameworks that are able to conduct proactive and intelligent network protection.

Keywords: Artificial Intelligence; Intrusion Detection Systems; Machine Learning; Deep Learning; Reinforcement Learning; Ensemble Models; Cybersecurity

How to cite this article: Al-Shizawi MS, Ahmed OAS, Torky FSA, Al-Rudaini ABHBZ, Al-Sawwafi SBS, Al-Shizawi MS, Al-Balushi YM. Artificial Intelligence–Driven Intrusion Detection Systems: A Systematic Review of Machine Learning, Deep Learning, and Adaptive Ensemble Approaches. Int J Drug Deliv Technol. 2026;16(67s):882-896. DOI: 10.25258/ijddt.16.67s.73

Introduction

The contemporary online environment is witnessing a surge in cyber-attacks on the critical infrastructure, commercial, and personal systems as never before (Leroy et al., 2025). Attackers exploit vulnerabilities in the networks in an even more sophisticated way as the networks expand and cloud computing, IoT, and remote operations become more widespread (Pan et

al., 2025). The standard security measures like firewalls and signature-based anti-virus programs are not adequate in identifying dynamic, unknown and changing attacks. This fact explains why more sophisticated and smart systems that would detect and act against malicious actions in real time are necessary (Mohamed, 2025). Intrusion Detection Systems (IDS) have turned into an essential part of the contemporary cybersecurity structures, which may conduct continuous monitoring of the network and identify anomalies (Rehman et al., 2025). IDS solutions will improve situational awareness and reduce response time because they analyze traffic patterns, user behavior, and system activities. Nevertheless, the scale and dynamism of network data require adaptive and learning-driven IDS that can adapt to new attack vectors and guarantee its resilience to the continuously changing cybersecurity threats (Christy et al., 2025).

The idea of intrusion detection has developed greatly compared to the past rule-based methods to the present data-centric, AI-based, approaches. Initially, the IDS solutions were based on manual rules and signature databases to detect familiar patterns of attacks (Johnny & Ajao; Sowmya & Anita, 2023). Although effective when dealing with a threat that had been previously faced, these systems were not effective with zero-day attacks and new patterns of intrusion (Diana et al., 2025). The complexity in cyber threats made it necessary to have more than the simple rule-based detection. With the development of machine learning (ML) and deep learning (DL) methods, this paradigm has changed, more than ever before, as systems are trained based on large data sets and can identify abnormalities automatically (Dardouri & Almuhanna, 2025). The data-centric IDS now work on behavioral analysis, feature learning, and adaptive learning to detect slight variations of the normal activity (Kumar & Gutierrez, 2025). The models used to enhance the accuracy of intrusion detection include neural networks, decision trees, and ensemble methods, which are AI-based intrusion detection models that are beneficial in enhancing detection accuracy and minimizing false alarms. This change would be the shift towards the reactive defense to the proactive, smart, and constantly adaptive cybersecurity measures (Bibers et al., 2025).

Intrusion Detection Systems (IDS) have advanced through machine learning (ML) and deep learning (DL) to be automatable in detecting threats and increasing their accuracy (Alharthi et al., 2025). In contrast to the older methods based on fixed signatures or manual settings, ML and DL models can learn through the data and be able to detect complex attack patterns and unknown threats. Those models examine the network traffic, user behavior, and system logs to differentiate between normal and malicious actions (Ali et al., 2025). Supervised algorithms, including Support Vector Machines and Random Forests, are able to classify known attacks, whereas unsupervised and deep networks, like Autoencoders, CNNs, and LSTMs, are able to detect new or changing threats (Ataa et al., 2024). Deep learning also increases accuracy by extracting features hierarchically and learning features contextually by using large amounts of data. Because of constant changes with new data, AI-based IDS can offer adaptive defenses, reduce false positives, and offer real-time threat visibility, thereby creating a basis of proactive and self-directed cybersecurity infrastructures (Awajan, 2023).

Although there has been a great advancement in the usage of artificial intelligence in cybersecurity, study in relation to Intrusion Detection System (IDS) is very disjointed. There are so many studies suggesting machine learning and deep learning models but they vary in terms of datasets, evaluation metrics and experimental setups and therefore it is hard to compare them directly. There are those that use classical algorithms like SVM and Random Forest, and there are also those that examine deep neural networks like CNN, LSTM and Autoencoders. Nevertheless, data preprocessing, feature selection, and validation protocols commonly give inconsistent findings on model effectiveness due to inconsistencies in data preprocessing. Further, the majority of the reviews do not contain quantitative synthesis in order to determine statistically significant trends in performance. Thus the systematic review and meta-analysis is necessary to summarize the available results, measure the methodological rigor and give the collective information on model performance and gaps in the research. This will help to have a full picture of the state of AI-driven IDS and is oriented on the future research of standardized, reproducible, and scalable intrusion detection solutions. The fast growth of AI-based solutions to cybersecurity has led to a wide range of methodologies, but the common opinion on which ones is more effective than the others is still ambiguous. Since datasets, evaluation criteria and algorithm designs are inconsistent, there is an acute necessity of systematic study on existing research. The paper fills this gap by conducting a systematic review and a meta-analysis to bring together evidence on a variety of AI-based IDS frameworks. The synthesis of empirical findings in the review is aimed at determining predominant models, the performance trends, and limitations that impede the implementation of large scale. In order to direct this study, the following research questions (RQs) are developed:

- RQ1: What machine learning and deep learning models have been applied to Intrusion Detection Systems (IDS), and how do their performance metrics (accuracy,

recall, F1-score, AUC) compare across standard benchmark datasets?
- RQ2: How do hybrid and ensemble AI-driven IDS architectures improve detection accuracy and adaptability compared to traditional single-model approaches?
- RQ3: How can reinforcement learning and adaptive AI frameworks be integrated with traditional IDS models to enable self-learning and autonomous cyber defense systems?

Methodology

To guarantee the methodological rigor, transparency, and reproducibility, this systematic review adhered to the PRISMA 2020 protocol and the protocol used to conduct evidence-based software engineering reviews by Kitchenham (Kitchenham & Brereton, 2013; Page et al., 2021). The objective of the review was to identify, analyze, and synthesise the research on artificial intelligence-based Intrusion Detection Systems (IDS) with the emphasis on using machine learning (ML), deep learning (DL), reinforcement learning (RL) and ensemble-based adaptive architectures published between 2021 and 2025.

Search Strategy

The search strategy adopted was comprehensive so as to cover a large amount of the latest and topical literature. It was searched in six high-impact academic databases: IEEE Xplore, ACM Digital Library, ScienceDirect (Elsevier), SpringerLink, Scopus, and Web of Science. The data source selected these databases because they have a huge number of indexed peer-reviewed journals and conference proceedings in artificial intelligence, computer science, and cybersecurity. Search was carried out with a combination of Boolean operators and groups of key words which had a general and a specific content pertaining to AI-driven research in the field of IDS. There were added synonyms and abbreviations to enhance recall and accuracy. The timeframe of search was January 2021 to December 2025, which guaranteed the presence of more recent work representing the newest developments in the field of ML, DL, and RL methods of intrusion detection.

Table 1: Search Databases and Keyword Strings

Database	**Search Period**	**Search String / Keywords Used**
IEEE Xplore	2021–2025	(“machine learning” OR “deep learning” OR “neural network”) AND (“intrusion detection” OR “IDS” OR “cybersecurity”)
ACM Digital Library	2021–2025	(“SVM” OR “Random Forest” OR “CNN” OR “LSTM”) AND (“network security” OR “threat detection”)
ScienceDirect (Elsevier)	2021–2025	(“federated learning” OR “adversarial attack” OR “explainable AI”) AND (“intrusion detection” OR “cyber defense”)
SpringerLink	2021–2025	(“machine learning” OR “deep learning”) AND (“cybersecurity” OR “IDS”)
Scopus	2021–2025	(“hybrid model” OR “ensemble learning”) AND (“intrusion detection system” OR “AI security”)
Web of Science	2021–2025	(“intelligent IDS” OR “reinforcement learning”) AND (“network threats” OR “cyber attacks”)

The search was done on titles, abstracts, as well as key words. Manual backward and forward reference checking to the snowballing of references was also done to obtain the wider range of studies that were not directly indexed in databases. Only articles peer reviewed and written in English were retained as represented in table 1.

Inclusion and Exclusion Criteria

Inclusion and exclusion criteria were pre-screened so as to ensure the integrity, relevance, and scientific quality of the review. They were used in the abstract screening as well as full-text assessment as presented in table 2.

Table 2: Inclusion and Exclusion Criteria

Category	Criteria	Description / Rationale
Inclusion Criteria	Peer-reviewed journal or conference papers (2021–2025)	Ensures selection of high-quality, credible sources within the defined period.
	Studies applying ML, DL, RL, or ensemble algorithms for IDS	Focuses on AI-driven, empirical approaches to intrusion detection.
	Quantitative performance metrics (accuracy, precision, recall, F1, AUC)	Enables comparative analysis and meta-synthesis.
	English-language, full-text available	Guarantees accessibility and linguistic uniformity.

Exclusion Criteria	Non-peer-reviewed, theoretical, or opinion papers	Removes studies lacking empirical rigor.
	Duplicate or incomplete records	Prevents redundancy and data inconsistency.
	Papers unrelated to IDS (e.g., cryptography-only, blockchain-only)	Maintains focus strictly on IDS and network intrusion detection.

The inclusion process ensured methodological soundness and empirical grounding. Only studies that met all inclusion criteria and passed quality assessment were retained for synthesis.

Study Selection Process

In order to achieve methodological transparency and replicability, this review followed the PRISMA 2020 framework of systematic reviews strictly. The process of choosing the study was conducted in four consecutive stages, namely, identification, screening, eligibility, and inclusion. At the identification phase, six scholarly databases (IEEE Xplore, ACM Digital Library, science direct, springer link, Scopus, and web of science) were searched and 1,500 records were found. Out of them, 15 were opted out because of the missing metadata or the unavailable sources, and 420 duplicates were eliminated before the screening. During the screening phase, 1,065 records were evaluated according to the title and abstract and 805 of them were excluded due to being irrelevant to artificial intelligence-driven Intrusion Detection System or being irrelevant as an experiment. Thereafter, 260 full-text papers were obtained to be evaluated in details but five were not available in full.

In the initial step of the eligibility, 255 articles were thoroughly reviewed considering predefined inclusion and exclusion criteria. Consequently, 210 studies have been excluded based on not satisfying inclusion criteria (Reason 1 = 100; Reason 2 = 65; Reason 3 = 40) which was mainly because they were theoretical oriented, incomplete performance measurement, or no IDS in the context. Ultimately, a total of 40 studies were included in the final synthesis, which fulfilled all the inclusion criteria and met the methodological and empirically validated works regarding the AI-powered, machine learning-driven Intrusion Detection Systems as presented in figure 1.

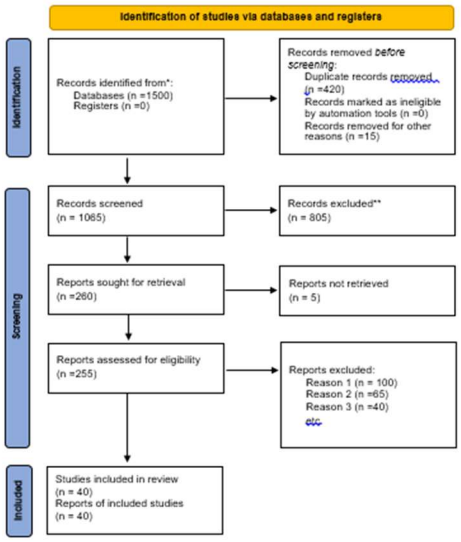

Figure 1: PRISMA 2020 Flow Diagram

Data Extraction and Quality Assessment

All 40 selected studies underwent a structured data extraction and quality evaluation process to ensure consistency and reliability. For each study, key information was recorded, including the author(s), year of publication, AI/ML approach category (classical ML, deep learning, reinforcement learning, or ensemble), the datasets used (e.g., NSL-KDD, UNSW-NB15, CICIDS2017, TON_IoT), and the performance metrics (accuracy, precision, recall, F1-score, and AUC). Extracted data were compiled into a comparative matrix to assess algorithmic performance, dataset dependencies, and methodological rigor across studies as shown in table 3. Quality assessment was conducted using four criteria: relevance to AI-driven IDS research, experimental rigor of model development and evaluation, data transparency regarding datasets and reproducibility, and scholarly impact of the publication. Only studies meeting a minimum quality threshold (≥3 out of 5) were included in the synthesis, ensuring the inclusion of methodologically sound and empirically validated research.

Table 3: Data Extraction and Quality Assessment Summary

Criterion	**Purpose**
Author(s), Year	Identify research patterns and trends
AI/ML Method, Dataset, Metrics	Enable algorithmic and dataset comparison

Findings, Limitations	Capture key results and research gaps
Relevance, Rigor, Transparency, Impact	Ensure validity, reproducibility, and credibility

Result

Classical Machine Learning in IDS

Table 4 shows a summary of the recent works that utilized classical machine learning algorithms in Intrusion Detection Systems. The evidence has always shown that the Support Vector Machines, Decision Trees, Random Forests, Naïve Bayes, and K-Nearest Neighbor models are still used to form the analytical foundation of the IDS research. Their advantage is that they are interpretable, computationally efficient, and stable in the case of structured datasets, including NSL-KDD, UNSW-NB15, and CICIDS2017. Among these, the ensemble-based models, especially the Random Forest, is often better than other models because the method has the capability to handle non-linearity and address overfitting. In spite of these strengths, the research findings in the studies indicate some significant weaknesses. Classical algorithms have limited adaptability to dynamic and zero-day attacks, only through using a static feature engineering and retraining to adapt to changing threats. Besides, the lack of consistency in preprocessing and evaluation of benchmark data sets undermines the reproducibility of published findings and makes meta-analytic comparisons more difficult. Although high accuracy scores, usually above 98 percent are commonly reported, this is mostly because of dataset homogeneity and not actual generalization ability. A combination of those findings shows that classical machine learning is still unavoidable in cases of a baseline benchmark and interpretable intrusion detection. Nonetheless, its scalability and ability to withstand more advanced and dynamic attack vectors is still low. This limitation has led to a methodology of change to hybrid and ensemble models that aim to combine the openness of classical models and the adaptive adaptability of deep learning models.

Table 4: Summary of Classical Machine Learning Approaches in Intrusion Detection Systems

Study / Year	**Algorithms Used**	**Benchmark Datasets**	**Evaluation Metrics**	**Key Findings**	**Identified Gaps / Challenges**
(Hakke, 2025)	SVM, DT, NB, RF, KNN, LR, QDA, LDA, AdaBoost, CatBoost, XGBoost	NSL-KDD, UNSW-NB15, CICIDS2017	Accuracy, Precision, Recall, F1-score	RF and XGBoost models achieved the highest detection accuracy; demonstrated performance variability across datasets.	Dataset imbalance and non-standard preprocessing affected comparability.
(Tripathy & Beheera, 2025)	SVM, KNN, DT, LR, NB, RF, XGBoost, Adaboost, ANN	KDD'99, NSL-KDD, UNSW-NB15, CICIDS2017, CSE-CIC-IDS2018	Accuracy, Detection Rate, F1-score	Comprehensive dataset-based ML review; highlighted classifier roles and dataset biases.	Lack of standardization in feature extraction and evaluation criteria.
(Azhar et al., 2024)	Random Forest (optimized sub-ensemble)	Proprietary / real-time traffic dataset	Accuracy, Testing Time	Proposed "IDRandom-Forest" model improving detection accuracy and lowering latency.	Needs validation on public datasets; limited cross-dataset comparison.
(Shakir & Mohsin, 2024)	SVM, DT, NB, RF, LR	KDD'99, NSL-KDD	Accuracy, Precision, Recall	Demonstrated that applying feature selection significantly enhances ML performance.	Overfitting due to limited dataset diversity; redundancy in selected features.

(Baidoo et al., 2023)	SVM, DT, RF, Ensemble	UNSW-NB15	Energy & Memory Consumption, Accuracy	Assessed energy/memory usage of ML models; ensemble balanced accuracy and resource efficiency.	High computational cost for SVM; lack of runtime IDS testing.
(Abbas et al., 2023)	RF, RFE, Ensemble Methods	NSL-KDD, UNSW-NB15, CSE-CIC-IDS2018	Accuracy, Precision, Recall	Hybrid ensemble achieved up to 99.9% accuracy with reduced training time.	Limited interpretability; overreliance on ensemble structures.
(Vanin et al., 2022)	SVM, DT, NB, KNN, RF	NSL-KDD, CICIDS2017	Accuracy, Detection Rate, FAR	Classified ML techniques and compared IDS performance across datasets.	Poor zero-day detection; inconsistent performance metrics.
(Maseno et al., 2022)	Hybrid (RF, SVM + DL variants)	Multiple IDS datasets (2012–2022)	Accuracy, Detection Rate, FAR	Reviewed 111 hybrid ML-based IDS papers; identified integration trends with DL.	Lack of reproducibility; inconsistent hybrid architectures.
(Musa et al., 2021)	ML, Bayesian, Swarm, Markov Models	KDD'99, NSL-KDD, UNSW-NB15	Accuracy, Recall, F1-score	Reviewed ML-based IDS methods; compared algorithms and datasets.	Dataset imbalance and lack of cross-validation across studies.
(Jaw & Wang, 2021)	K-means, One-Class SVM, DBSCAN, EM (KODE Ensemble)	CICIDS2017, NSL-KDD, UNSW-NB15	Accuracy, Detection Rate, FAR	Hybrid feature selection (HFS-KODE) achieved >99% accuracy on all datasets.	High computational complexity and limited interpretability.

Evaluation Metrics and Datasets

Table 5 introduces a summary analysis of the benchmark datasets and metrics of evaluation used in a recent AI-powered Intrusion Detection System (IDS) research. There is an apparent tendency toward using a small number of benchmark datasets - CICIDS2017, UNSW-NB15 and NSL-KDD - which collectively represent the majority of experimental assessments. Although this indicates a step towards standardized benchmarking, there is also a methodological bottleneck of the approach, since the excessive use of older datasets including KDD99 and NSL-KDD is restricting the ecological validity of the model performance in current heterogeneous network settings. More modern datasets such as CICIDS2017 and UNSW-NB15 are more realistic in their network traffic and attack patterns, resulting in increased reported accuracies (usually over 98%), especially when using hybrid or ensemble architectures that have deep and classical learning elements. Secondary observation is related to the inconsistency and incompleteness of evaluation metrics. Almost all studies use the accuracy as a major measure, and only some of them report precision, recall, and F1, and hardly any report AUC or false alarm rate (FAR). This measure difference makes the comparability of cross-studies and meta-analytic rigor invalid because different models with similar levels of accuracy can have a radically different error balance. The pre-eminence of accuracy without supporting measures of sensitivity and specificity has the danger of overstating the actual performance of detection, especially in skewed data sets where the attack classes have been underrepresented.

Moreover, the critical analysis of Table 5 reflects the fact that lack of balance in databases, use of outdated benchmarks and non-standardized metrics reporting are some of the chronic constraints in research on IDS. Although in the recent times, the integration of IoT-specific datasets (e.g., MQTT-IoT-IDS2020) and

methods to eliminate class-imbalances (e.g., SMOTE, ADASYN) are present, they are still intermittent and do not have integrated methodological frameworks. This fragmentation does not allow the reliable cross-validation and generalization to the real-life deployments. As a result, the next round of studies in the field of IDS needs to focus on the creation and implementation of extended, updated, and publicly accessible datasets (like TON_IoT) and consistent assessment frameworks requiring the imposition of multi-metric reporting. This type of standardization would greatly promote reproducibility, comparative evaluation and statistical strength of meta-analytic inferences in AI-based cybersecurity studies.

Table 5: Summary of Benchmark Datasets, Evaluation Metrics, and Performance Results in AI-Driven Intrusion Detection Systems

Study / Year	Datasets Used	Evaluation Metrics	Performance Summary	Limitations / Gaps
(Sharma & Kumar, 2025)	CICIDS2017, UNSW-NB15, KDD CUP 99	Accuracy, Confusion Matrix	Hybrid CapsNet + BiLSTM model achieved 99% (CICIDS2017), 97% (UNSW-NB15), 98% (KDD CUP 99).	Dataset imbalance not addressed; FAR and AUC not reported.
(Lv et al., 2025)	KDD99, NSL-KDD, UNSW-NB15, CICIDS2017	Accuracy, Precision, Recall, F1	TAN model showed competitive performance and improved interpretability through DT integration.	Metric reporting inconsistent; no IoT dataset testing.
(Kamal & Mashaly, 2024)	NF-UNSW-NB15-v2, CICIDS2017	Accuracy, Precision, Recall, F1	Achieved ≈99.7% (binary) and 99.0% (multiclass) accuracy; addressed class imbalance with SMOTE/ADASYN.	Real-time validation absent; high computational cost.
(Alsaffar et al., 2024)	CICIDS2017, UNSW-NB15	Accuracy, Recall, F1	Multi-stacking ensemble outperformed baseline models on both datasets.	Dataset imbalance and computational overhead persist.
(Memon et al., 2023)	MQTT-IoT-IDS2020	Accuracy (97–99%)	PSO + LIME framework enhanced model interpretability and attack detection.	Uses non-standard IoT dataset; limited comparability with traditional benchmarks.
(Abbas et al., 2023)	NSL-KDD, UNSW-NB15, CSE-CIC-IDS2018	Accuracy, Precision, Recall	Ensemble RF-RFE achieved up to 99.9% accuracy across datasets.	Lack of interpretability; no runtime testing.
(Thirimanne et al., 2022)	NSL-KDD	Accuracy, Precision, Recall, F1	DNN pipeline achieved 81–96% across metrics with real-time feature extraction.	Single (outdated) dataset; limited generalizability.
(Khan et al., 2022)	KDD99, NSL-KDD, UNSW-NB15, CICIDS2017	Accuracy, Precision, Recall, F1, FAR	Review showed DL outperforms ML on recent datasets; highlighted dataset bias issues.	Metrics not standardized across studies; dataset variation not controlled.
(Ghurab et al., 2021)	KDD99, NSL-KDD, UNSW-NB15, CICIDS2017, CIDDS-001	Descriptive comparison	Compared 8 datasets by size, features, and attack classes; outlined dataset characteristics.	No model testing or performance analysis included.

(Mahalakshmi et al., 2021)	UNSW-NB15	Accuracy	CNN model achieved high binary classification accuracy on UNSW-NB15.	Single dataset; recall and F1 not reported.

Deep Learning Architectures in Intrusion Detection Systems

Table 6 is a synthesis of current findings on the use of deep learning (DL) models in intrusion detection systems, which shows a convincing shift towards automation and making use of data to model threats as a classical machine learning. In various papers, convolutional neural networks (CNNs), recurrent neural networks (RNNs), long short-term memory (LSTM), gated recurrent units (GRU), autoencoders, generative adversarial networks (GANs), and Transformers demonstrate higher accuracy and generalization than other types of architectures. The presence of the same benchmark datasets (CICIDS2017, UNSW-NB15, CSE-CIC-IDS2018) indicates the persistence of reproducibility and comparability of the benchmark on the use of standardized benchmarks.

Importantly, there are the hybrid types, e.g. CNN-LSTM, CNN-GRU and Cu-LSTMGRU models, which demonstrate the increased incorporation of the spatial and temporal learning into complex network traffic analysis. These configurations are more accurate and recallable and more beneficial in dealing with multi-class attack detection than single-model settings. Systems based on transformers and GAN-promised enhancements even more to allow greater adaptability, especially in real-time settings and when dealing with imbalanced data, but at a very high computational cost and stability implications. Table 6 synthesis indicates that, although the accuracy and feature abstraction are always higher when using the DL models, interpretability, scalability, and resource usage are major weaknesses. The growing scientific attention to explainable AI (XAI) and lightweight DL models is one sign of an acute shift to operational, trusted and energy-efficient IDS solutions that can operate in a wide range of environments including IoT, IIoT, and cloud infrastructures.

Table 6: Summary of Deep Learning Architectures and Hybrid Models for Intrusion Detection Systems

Study / Year	Deep Learning Architecture	Dataset(s) Used	Performance Metrics	Key Findings	Identified Challenges / Trends
(Afraji et al., 2025)	CNN + LSTM + GRU (hybrid)	TON_IoT, CICIDS2017	Accuracy = 99.49%, Precision = 0.9954, F1 = 0.9949	Parallel–sequential fusion of CNN-LSTM-GRU achieves state-of-the-art detection for IoT / IIoT traffic.	High computational cost; limited interpretability despite excellent accuracy.
(Musthafa, 2025)	CNN, RNN, Transformer	CICIDS2017, UNSW-NB15	Accuracy, FAR, F1, Inference Latency	Transformer yields best generalization and low-latency detection in live traffic.	Transformer models require large memory and complex fine-tuning.
(Sajid et al., 2024)	XGBoost + CNN + LSTM (hybrid)	CICIDS2017, UNSW-NB15, NSL-KDD, WSN-DS	Accuracy, FAR, Precision	Hybrid feature extraction (XGBoost, CNN) + LSTM classifier improves detection and reduces FAR.	Model complexity; potential overfitting on high-dimensional data.
(Wu et al., 2024)	Autoencoder, DNN, CNN, RNN, GAN, Transformer	Multiple benchmark IDS datasets	Comparative accuracy, AUC	Comprehensive review identifying BERT / GPT transformer trends in IDS.	Lack of explainability and high compute demand hinder deployment.
(Luo et al.,	CNN, RNN, LST	Automotive (IVN)	Accuracy, Detection Rate	Deep learning effectively detects IVN	Limited real-world IVN dataset

2023)	M, Autoencoder	datasets		attacks; LSTM and Autoencoder perform best.	s; generalization to unseen vehicles unclear.
(Shiri et al., 2023)	CNN, RNN, LSTM, GRU, GAN, DRL	Comparative (3 open datasets)	Accuracy, Precision, Recall	Benchmarks CNN and GRU as highly accurate for temporal cyber tasks.	Interpretability and dataset bias remain major issues.
(Aldallal, 2022)	Cu-LSTM + GRU (hybrid)	CICIDS2018	Accuracy ↑ 12.05% vs baseline	Cu-LSTMGRU achieves notable gain in cloud IDS accuracy and symmetry.	High training time; requires hardware optimization.
(Neto et al., 2025)	CNN, RNN, Autoencoder, Transformer (review)	Multi-domain datasets (cloud, IoT, edge)	N/A (qualitative review)	Identifies need for trustworthy and operational DL IDS solutions.	Poor explainability (XAI gap); scarcity of real-system validation.
(Khan, 2021)	CNN + RNN (hybrid)	CSE-CIC-IDS2018	Accuracy = 97.75%	CRNN captures both spatial and temporal features effectively.	Requires frequent dataset updates; computationally intensive.
(Xiaodong Liu et al., 2021)	GAN (WGAN-GP) + Feature Selector	KDD, UNSW-NB15, CICIDS2017	F1 vs baseline	oversampling mitigates data imbalance and boosts ML model accuracy.	GAN training instability and computational load.

AI-Driven Adaptive and Ensemble Intrusion Detection Systems

Table 7 is a synthesis of the modern methods of combining reinforcement learning, adaptive retraining, and ensemble intelligence with intrusion detection. The overall data confirms a sharp transition to self-optimizing and context-aware IDS systems that can autonomously modify model parameters based on the changing threats. The Proximal Policy Optimization and Deep Q-Learning reinforcement learning models show significant improvement of both detection accuracy and robustness by means of policy-guided adaptation and dynamic decision maximization. Similarly, ensemble mechanisms, such as stacking, boosting, and bagging, are always used to increase accuracy and generalization by integrating heterogeneous base learners into unified hybrid systems.

Most importantly, these architectures are significantly more accurate (usually more than 97%) and have significantly reduced false-alarm rates relative to their counterparts in the case of static ML or DL. Nevertheless, the incorporation of several adaptive elements brings with it some novel constraints: RL-based systems become converge-unstable and computationally in-efficient, whereas ensemble and incremental-learning systems become complex in architecture and energy-intensive. Moreover, although there are claims of performance under offline operation, there is limited real-world validation, even though it is claimed to perform well in large-scale, decentralized, or live operations. All in all, Table 7 points to an evident research direction towards the continuous learning federated and resource-aware IDS architecture. The existing trade-off is between adaptivity and interpretability - how to come up with scalable systems that maintain the high performance in detection without compromising explainability or operational efficiency.

Table 4: Summary of AI-Driven Adaptive and Ensemble Intrusion Detection Systems (IDS)

Study / Year	**Approach Type**	**Core Method / Architecture**	**Performance Highlights**	**Key Limitation / Trend**

(Suresh & Cyril Jose, 2025)	Reinforcement Learning (PPO)	Dynamic ensemble weighting with PPO + MLP meta-learner	Avg Acc = 97.16 %; strong novel-attack detection	RL stability and scalability issues
(Ntayagabiri et al., 2025)	Ensemble (LightGBM + XGBoost)	Bagging-based OMIC framework for IoT	99.26 % Acc on CICIoT 2023	Limited web/recon attack accuracy
(Alsaffar et al., 2024)	Adaptive Ensemble (ResNet + Stacking)	Multi-stacking with dimensionality reduction	Superior to DL baselines on CICIDS / UNSW	High complexity, costly feature processing
(Tarigan, 2024)	Hybrid Ensemble (RF + GB + Voting)	Simple hybrid ensemble on NSL-KDD	Higher accuracy, reduced FPR	Needs multi-dataset validation
(Alserhani & Aljared, 2023)	Hybrid Ensemble ML	Integrated ensemble for advanced attack prediction	> 99 % Acc, < 1 % FPR	Computational overhead
(Jemili et al., 2024)	Hybrid (Big-Data Ensemble)	RF + XGBoost fusion for big data IDS	97 % Acc on multiple datasets	Model tuning and data imbalance
(Das & Pramod, 2022)	Ensemble (Tree & Bagging)	IoT malware detection via stacked tree models	Excellent PE malware detection	Limited real-world deployment
(Alavizadeh et al., 2022)	Deep Q-Learning (RL)	DQL + DNN for autonomous IDS	Outperforms ML baselines on NSL-KDD	Convergence and training cost
(Xiaohu Liu et al., 2021)	Deep Recurrent Q-Network (RL)	DQN with stochastic game model	Effective adaptive defense	Partial observability constraints
(Wu et al., 2021)	Adaptive Incremental Ensemble (DEIL-RVM)	Dynamic ensemble for streaming data	Stable accuracy with low resource use	Limited testing on live networks

Discussion

This systematic review provided a synthesis of results of forty peer reviewed papers published between 2021 and 2025 finding a distinct shift in the traditional machine learning based intrusion detection systems (IDS) to deep learning and self-learning systems. In all the categories, the results concur that although the classical ML algorithms are still viable in detecting baselines, deep and ensemble based architectures are at the lead in accuracy, recall, and adaptability especially to real-time intrusion detection.

Other algorithms, including Support Vector Machines (SVM), Decision Trees (DT) and Random Forests (RF), still form the basis of IDS development in the classical ML research. Ensemble models (RF and XGBoost) that were studied by Hakke (2025) showed that they consistently achieve a high accuracy exceeding 98 percent even in datasets as NSL-KDD and CICIDS2017. On the same note, Tripathy and Behera (2025) gave a detailed data-driven comparison, with the consistent problem of bias in data sets and non-standardized evaluation procedures. The IDRandom-Forest model proposed by Azhar et al. (2024) offered a contribution to the field by being more accurate and with lower latency, but it also had not been tested on publicly available datasets. Taken altogether, these papers confirm that, although classical models are understandable and computationally efficient, they are not adaptable to changing and zero-day threats, which is also highlighted by Vanin et al. (2022) and Baidoo et al. (2023). Therefore, classical ML is good when it comes to stability and explainability but not enough to suit modern dynamic cyber settings.

Deep learning architectures on the other hand have transformed the research of the IDS by proposing data-driven and context-aware detection features. The Afraji et al. (2025) study with CNNLSTMGRU hybrid model reported state-of-the-art results of 99.49% accuracy in TONIoT and CICIDS2017 datasets - showing the strength of the combination of spatial and

temporal features learning. Equally, Musthafa (2025) contrasted CNN, RNN, and Transformer architectures and found that Transformer-based models are more likely to be generalized in the case of live network conditions and with a low latency. Another hybrid system proposed by Sajid et al. (2024) includes XGBoost together with CNN and LSTM and minimizes false alarms, at the cost of higher computation rate. These results are consistent with those of Wu et al. (2024) and Luo et al. (2023), who have stressed that deep architectures provide much better detection accuracy and flexibility, especially with the use of modern and complicated datasets such as UNSW-NB15 and CICIDS2017. However, the interpretability issue remains the problem in itself, as deep neural networks are frequently a black box, which makes it difficult to use them in mission-critical or resources-limited contexts like an IoT network as suggested by Shiri et al. (2023).

The combination of reinforcement (RL) with ensemble learning is a significant paradigm shift to self-learning and adaptive IDS models. Such a study as Suresh and Cyril Jose (2025), for example, used Proximal Policy Optimization (PPO) to weight ensemble in the case of real-time dynamic weighting, which showed an average accuracy of 97.16% and allowed real-time adjustment of the model to new threats. On the same note, Ntayagabiri et al. (2025) proposed an ensemble-like bagging-based OMIC model to achieve 99.26 percent accuracy of the large-scale IoT traffic by using LightGBM and XGBoost, demonstrating the possibility of the robustness of ensemble systems in multi-attack detection. However, Alavizadeh et al. (2022), and Liu et al. (2021) reported that although the RL-based IDS models enhance the decision-making processes and resiliency, they are associated with convergence instability and high training costs. The combination of several learners in an ensemble, including the ones suggested by Alsaffar et al. (2024) and Jemili et al. (2024), further proves the fact that stacking and boosting improve the generalization and can reduce false positives- but at the cost of higher computational complexity and overhead. Overall, these results demonstrate that adaptive and hybrid architectures, although strong, have to trade accuracy, interpretability, and efficiency so that they can be applicable to large-scale and real-time cybersecurity tasks.

The cross-model comparison shows that deep learning and hybrid ensemble systems are superior in terms of detection accuracy and recall, usually more than 98% and classical ML has moderate precision and better interpretability. Nonetheless, the common drawback of research, such as the articles by Rehman et al. (2025) and Khan et al. (2022), is the absence of reproducibility due to inconsistent preprocessing, different evaluation metrics, and the use of outdated datasets, such as NSL-KDD and KDD99. Although more recent datasets like CICIDS2017 and UNSW-NB15 are more realistic, the fact that the methodology used differs between studies complicates the ability to directly compare them. Additionally, the majority of studies, including Kamal and Mashaly (2024) and Abbas et al. (2023), do not provide several performance measures (precision, recall, F1, and AUC) to restrict the strength of meta-analysis.

Practically in deployment, the recent field highlights the potential of AI-controlled IDS in the real-time autonomous security of cyberspace. Adaptive retraining, the focus of studies by Alsaffar et al. (2024) and Jemili et al. (2024), allows models to update themselves in response to new threats, which is in line with the recent zero-trust security paradigm. But there are still operational issues such as excessive resource requirements and inability to test properly in production. Moreover, the increased application of reinforcement and autonomous learning brings about ethical and responsibility issues, especially regarding the aspect of opaque decision-making, propagation of bias, and possible exploitation of self-learning agents, which are also mentioned by Wu et al. (2024) and Neto et al. (2025). It will hence be important to ensure that explainability, transparency, and fairness in AI-driven IDS are ensured to make their adoption safe and trustful. Overall, the cumulative information presented in this review indicates that although deep and adaptive learning-based IDS have become more potent and robust than the classical ones, there is still a long way to go when it comes to reproducibility, interpretability, and ethical incorporation. The combination of reinforcement learning, explainable AI, and federated adaptive architectures will probably shape the future of intelligent IDS systems in the form of systems that are able to defend continuously and autonomously and still remain transparent and trusted in even more sophisticated cyber ecosystems.

Conclusion

This is systematic review summarized 40 peer-reviewed articles that were published between 2021 and 2025 and provided a complete analysis of AI-based Intrusion Detection Systems (IDS) based on machine learning, deep learning, reinforcement learning, and ensemble approaches. The data show that, although classical ML algorithms, including SVM and Random Forest, still stand as the foundations of their interpretability, deep learning and hybrid ensemble models have been proven to be more accurate, with higher recall and flexibility, on benchmark datasets, including CICIDS2017 and UNSW-NB15. An additional avenue that Reenforcement learning-based architectures provide to the IDS is self-learning and autonomous defense,

but with complexity and stability concerns. Irrespective of such improvements, the review reveals a severe weakness, namely, the absence of methodological standardisation and reproducibility among studies, frequently because of inconsistent preprocessing and outdated datasets. The next step of the research should focus on creating integrated benchmarking models and unified assessment criteria which allow the cross-model comparability. Moreover, explainable and federated AI implementation can help improve transparency, scalability, and ethical responsibility to use trustful, adaptive, and resource-efficient IDS in real-world, distributed systems. All of these developments will lead to the creation of smart and autonomous systems that can be used to defend the network proactively and autonomously.

Reference

Abbas, Q., Hina, S., Sajjad, H., Zaidi, K. S., & Akbar, R. (2023). Optimization of predictive performance of intrusion detection system using hybrid ensemble model for secure systems. *PeerJ Computer Science*, *9*, e1552.

Afraji, D. M. A. A., Lloret, J., & Peñalver, L. (2025). An integrated hybrid deep learning framework for intrusion detection in IoT and IIoT networks using CNN-LSTM-GRU architecture. *Computation*, *13*(9), 222.

Aldallal, A. (2022). Toward efficient intrusion detection system using hybrid deep learning approach. *Symmetry*, *14*(9), 1916.

Alsaffar, A. M., Nouri-Baygi, M., & Zolbanin, H. (2024). Enhancing intrusion detection systems with dimensionality reduction and multi-stacking ensemble techniques. *Algorithms*, *17*(12), 550.

Azhar, M., Perveen, S., Iqbal, A., & Lee, B. (2024). IDRandom-Forest: advanced random forest for real-time intrusion detection. *IEEE Access*.

Baidoo, C. Y. M., Yaokumah, W., & Owusu, E. (2023). Estimating overhead performance of supervised machine learning algorithms for intrusion detection. *International Journal of Information Technologies and Systems Approach (IJITSA)*, *16*(1), 1-19.

Ghurab, M., Gaphari, G., Alshami, F., Alshamy, R., & Othman, S. (2021). A detailed analysis of benchmark datasets for network intrusion detection system. *Asian Journal of Research in Computer Science*, *7*(4), 14-33.

Hakke, D. G. (2025). PERFORMANCE EVALUATION OF MACHINE LEARNING-BASED INTRUSION DETECTION USING NSL-KDD, UNSW-NB15 AND CICIDS2017 DATASETS. *International Journal of Applied Mathematics*, *38*(3s), 447-469.

Jaw, E., & Wang, X. (2021). Feature selection and ensemble-based intrusion detection system: an efficient and comprehensive approach. *Symmetry*, *13*(10), 1764.

Kamal, H., & Mashaly, M. (2024). Advanced hybrid transformer-CNN deep learning model for effective intrusion detection systems with class imbalance mitigation using resampling techniques. *Future Internet*, *16*(12), 481.

Khan, A. R., Kashif, M., Jhaveri, R. H., Raut, R., Saba, T., & Bahaj, S. A. (2022). Deep learning for intrusion detection and security of Internet of things (IoT): current analysis, challenges, and possible solutions. *Security and Communication Networks*, *2022*(1), 4016073.

Khan, M. A. (2021). HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system. *Processes*, *9*(5), 834.

Liu, X., Li, T., Zhang, R., Wu, D., Liu, Y., & Yang, Z. (2021). A GAN and feature selection-based oversampling technique for intrusion detection. *Security and Communication Networks*, *2021*(1), 9947059.

Luo, F., Wang, J., Zhang, X., Jiang, Y., Li, Z., & Luo, C. (2023). In-vehicle network intrusion detection systems: a systematic survey of deep learning-based approaches. *PeerJ Computer Science*, *9*, e1648.

Lv, M., Gan, S., Xu, K., Chen, T., Zhu, T., & Chen, J. (2025). An Interpretable Network Intrusion Detection Model via Decision Tree Enhanced Deep Attention Network. *IET Information Security*, *2025*(1), 5552833.

Mahalakshmi, G., Uma, E., Aroosiya, M., & Vinitha, M. (2021). Intrusion detection system using convolutional neural network on UNSW NB15 dataset. In *Advances in Parallel Computing Technologies and Applications* (pp. 1-8). ios press.

Maseno, E. M., Wang, Z., & Xing, H. (2022). A systematic review on hybrid intrusion detection system. *Security and Communication Networks*, *2022*(1), 9663052.

Memon, S. A., Wiil, U. K., & Shaikh, M. (2023). Explainable intrusion detection for internet of medical things. 15th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management,

Musa, U. S., Chakraborty, S., Abdullahi, M. M., & Maini, T. (2021). A review on intrusion detection system using machine learning techniques. 2021 international conference on computing, communication, and intelligent systems (ICCCIS),

Musthafa, M. (2025). Real-Time Intrusion Detection Leveraging Deep Learning: A Comparative Analysis of CNN, RNN, and Transformer Architectures. *International Journal of Advanced Engineering, Management and Science*, *11*(5), 632790.

Neto, E. C. P., Iqbal, S., Buffett, S., Sultana, M., & Taylor, A. (2025). Deep learning for intrusion detection in emerging technologies: a comprehensive survey and new perspectives. *Artificial Intelligence Review*, *58*(11), 340.

Sajid, M., Malik, K. R., Almogren, A., Malik, T. S., Khan, A. H., Tanveer, J., & Rehman, A. U. (2024). Enhancing intrusion detection: a hybrid machine and deep learning approach. *Journal of Cloud Computing*, *13*(1), 123.

Shakir, V., & Mohsin, A. (2024). A comparative analysis of intrusion detection systems: leveraging classification algorithms and feature selection techniques. *Journal of Applied Science and Technology Trends*, *5*(01), 34-45.

Sharma, V., & Kumar, M. (2025). Improving intrusion detection with hybrid deep learning models: A study on CIC-IDS2017, UNSW-NB15, and KDD CUP 99. *Journal of Information Systems Engineering and Management*, *10*.

Shiri, F. M., Perumal, T., Mustapha, N., & Mohamed, R. (2023). A comprehensive overview and comparative analysis on deep learning models: CNN, RNN, LSTM, GRU. *arXiv preprint arXiv:2305.17473*.

Thirimanne, S. P., Jayawardana, L., Yasakethu, L., Liyanaarachchi, P., & Hewage, C. (2022). Deep neural network based real-time intrusion detection system. *SN Computer Science*, *3*(2), 145.

Tripathy, S. S., & Behera, B. (2025). A review of various datasets for machine learning algorithm-based intrusion detection system: Advances and challenges. *arXiv preprint arXiv:2506.02438*.

Vanin, P., Newe, T., Dhirani, L. L., O'Connell, E., O'Shea, D., Lee, B., & Rao, M. (2022). A study of network intrusion detection systems using artificial intelligence/machine learning. *Applied Sciences*, *12*(22), 11752.

Wu, Y., Zou, B., & Cao, Y. (2024). Current status and challenges and future trends of deep learning-based intrusion detection models. *Journal of Imaging*, *10*(10), 254.

Abbas, Q., Hina, S., Sajjad, H., Zaidi, K. S., & Akbar, R. (2023). Optimization of predictive performance of intrusion detection system using hybrid ensemble model for secure systems. *PeerJ Computer Science*, *9*, e1552.

Afraji, D. M. A. A., Lloret, J., & Peñalver, L. (2025). An integrated hybrid deep learning framework for intrusion detection in IoT and IIoT networks using CNN-LSTM-GRU architecture. *Computation*, *13*(9), 222.

Alavizadeh, H., Alavizadeh, H., & Jang-Jaccard, J. (2022). Deep Q-learning based reinforcement learning approach for network intrusion detection. *Computers*, *11*(3), 41.

Aldallal, A. (2022). Toward efficient intrusion detection system using hybrid deep learning approach. *Symmetry*, *14*(9), 1916.

Alharthi, A., Alaryani, M., & Kaddoura, S. (2025). A comparative study of machine learning and deep learning models in binary and multiclass classification for intrusion detection systems. *Array*, 100406.

Ali, M. L., Thakur, K., Schmeelk, S., Debello, J., & Dragos, D. (2025). Deep Learning vs. Machine Learning for Intrusion Detection in Computer Networks: A Comparative Study. *Applied Sciences*, *15*(4), 1903.

Alsaffar, A. M., Nouri-Baygi, M., & Zolbanin, H. (2024). Enhancing intrusion detection systems with dimensionality reduction and multi-stacking ensemble techniques. *Algorithms*, *17*(12), 550.

Alserhani, F., & Aljared, A. (2023). Evaluating ensemble learning mechanisms for predicting advanced cyber attacks. *Applied Sciences*, *13*(24), 13310.

Ataa, M. S., Sanad, E. E., & El-Khoribi, R. A. (2024). Intrusion detection in software defined network using deep learning approaches. *Scientific Reports*, *14*(1), 29159.

Awajan, A. (2023). A novel deep learning-based intrusion detection system for IOT networks. *Computers*, *12*(2), 34.

Azhar, M., Perveen, S., Iqbal, A., & Lee, B. (2024). IDRandom-Forest: advanced random forest for real-time intrusion detection. *IEEE Access*.

Baidoo, C. Y. M., Yaokumah, W., & Owusu, E. (2023). Estimating overhead performance of supervised machine learning algorithms for intrusion detection. *International Journal of Information Technologies and Systems Approach (IJITSA)*, *16*(1), 1-19.

Bibers, I., Arreche, O., Alayed, W., & Abdallah, M. (2025). Ensemble-IDS: An Ensemble Learning Framework for Enhancing AI-Based Network Intrusion Detection Tasks. *Applied Sciences*, *15*(19), 10579.

Christy, C., Nirmala, A., Teena, A. M. O., & Amali, A. I. (2025). Machine learning based multi-stage intrusion detection system and feature selection ensemble security in cloud assisted vehicular ad hoc networks. *Scientific Reports*, *15*(1), 27058.

Dardouri, S., & Almuhanna, R. (2025). A deep learning/machine learning approach for anomaly based network intrusion detection. *Frontiers in Artificial Intelligence*, *8*, 1625891.

Das, A., & Pramod, P. (2022). A Novel Ensemble Model Using Learning Classifiers to Enhance Malware Detection for Cyber Security Systems. *vol*, *10*, 31-43.

Diana, L., Dini, P., & Paolini, D. (2025). Overview on intrusion detection systems for computers networking security. *Computers*, *14*(3), 87.

Ghurab, M., Gaphari, G., Alshami, F., Alshamy, R., & Othman, S. (2021). A detailed analysis of benchmark datasets for network intrusion detection system. *Asian Journal of Research in Computer Science*, *7*(4), 14-33.

Hakke, D. G. (2025). PERFORMANCE EVALUATION OF MACHINE LEARNING-BASED INTRUSION DETECTION USING NSL-KDD, UNSW-NB15 AND CICIDS2017 DATASETS. *International Journal of Applied Mathematics*, *38*(3s), 447-469.

Jaw, E., & Wang, X. (2021). Feature selection and ensemble-based intrusion detection system: an efficient and comprehensive approach. *Symmetry*, *13*(10), 1764.

Jemili, F., Meddeb, R., & Korbaa, O. (2024). Intrusion detection based on ensemble learning for big data classification. *Cluster Computing*, *27*(3), 3771-3798.

Johnny, R., & Ajao, F. The Evolution of Intrusion Detection Systems: From Signature-Based to AI-Driven Models.

Kamal, H., & Mashaly, M. (2024). Advanced hybrid transformer-CNN deep learning model for effective intrusion detection systems with class imbalance mitigation using resampling techniques. *Future Internet*, *16*(12), 481.

Khan, A. R., Kashif, M., Jhaveri, R. H., Raut, R., Saba, T., & Bahaj, S. A. (2022). Deep learning for intrusion detection and security of Internet of things (IoT): current analysis, challenges, and possible solutions. *Security and Communication Networks*, *2022*(1), 4016073.

Khan, M. A. (2021). HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system. *Processes*, *9*(5), 834.

Kitchenham, B., & Brereton, P. (2013). A systematic review of systematic review process research in software engineering. *Information and software technology*, *55*(12), 2049-2075.

Kumar, A., & Gutierrez, J. A. (2025). Impact of machine learning on intrusion detection systems for the protection of critical infrastructure. *Information*, *16*(7), 515.

Leroy, I., Zolotaryova, I., & Semenov, S. (2025). Impact of Critical Infrastructure Cyber Security on the Sustainable Development of Smart Cities: Insights from Internal Specialists and External Information Security Auditors. *Sustainability*, *17*(3), 1188.

Liu, X., Li, T., Zhang, R., Wu, D., Liu, Y., & Yang, Z. (2021). A GAN and feature selection-based oversampling technique for intrusion detection. *Security and Communication Networks*, *2021*(1), 9947059.

Liu, X., Zhang, H., Dong, S., & Zhang, Y. (2021). Network defense decision-making based on a stochastic game system and a deep recurrent Q-network. *Computers & security*, *111*, 102480.

Luo, F., Wang, J., Zhang, X., Jiang, Y., Li, Z., & Luo, C. (2023). In-vehicle network intrusion detection systems: a systematic survey of deep learning-based approaches. *PeerJ Computer Science*, *9*, e1648.

Lv, M., Gan, S., Xu, K., Chen, T., Zhu, T., & Chen, J. (2025). An Interpretable Network Intrusion Detection Model via Decision Tree Enhanced Deep Attention Network. *IET Information Security*, *2025*(1), 5552833.

Mahalakshmi, G., Uma, E., Aroosiya, M., & Vinitha, M. (2021). Intrusion detection system using convolutional neural network on UNSW NB15 dataset. In *Advances in Parallel Computing Technologies and Applications* (pp. 1-8). ios press.

Maseno, E. M., Wang, Z., & Xing, H. (2022). A systematic review on hybrid intrusion detection system. *Security and Communication Networks*, *2022*(1), 9663052.

Memon, S. A., Wiil, U. K., & Shaikh, M. (2023). Explainable intrusion detection for internet of medical things. 15th International Joint Conference on Knowledge Discovery,

Knowledge Engineering and Knowledge Management,

Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems*, 1-87.

Musa, U. S., Chakraborty, S., Abdullahi, M. M., & Maini, T. (2021). A review on intrusion detection system using machine learning techniques. 2021 international conference on computing, communication, and intelligent systems (ICCCIS),

Musthafa, M. (2025). Real-Time Intrusion Detection Leveraging Deep Learning: A Comparative Analysis of CNN, RNN, and Transformer Architectures. *International Journal of Advanced Engineering, Management and Science*, *11*(5), 632790.

Neto, E. C. P., Iqbal, S., Buffett, S., Sultana, M., & Taylor, A. (2025). Deep learning for intrusion detection in emerging technologies: a comprehensive survey and new perspectives. *Artificial Intelligence Review*, *58*(11), 340.

Ntayagabiri, J. P., Bentaleb, Y., Ndikumagenge, J., & El Makhtoum, H. (2025). OMIC: A Bagging-Based Ensemble Learning Framework for Large-Scale IoT Intrusion Detection. *Journal of Future Artificial Intelligence and Technologies*, *1*(4), 401-416.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., & Brennan, S. E. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *bmj*, *372*.

Pan, Y., Ling, Z., Zhang, Y., Wang, H., Liu, G., Luo, J., & Fu, X. (2025). TORCHLIGHT: Shedding LIGHT on Real-World Attacks on Cloudless IoT Devices Concealed within the Tor Network. *arXiv preprint arXiv:2501.16784*.

Rehman, H. M. R. U., Liaquat, S., Gul, M. J., Jhandir, M. Z., Gavilanes, D., Vergara, M. M., & Ashraf, I. (2025). A systematic literature study of machine learning techniques based intrusion detection: datasets, models, challenges, and future directions. *Journal of Big Data*, *12*(1), 264.

Sajid, M., Malik, K. R., Almogren, A., Malik, T. S., Khan, A. H., Tanveer, J., & Rehman, A. U. (2024). Enhancing intrusion detection: a hybrid machine and deep learning approach. *Journal of Cloud Computing*, *13*(1), 123.

Shakir, V., & Mohsin, A. (2024). A comparative analysis of intrusion detection systems: leveraging classification algorithms and feature selection techniques. *Journal of Applied Science and Technology Trends*, *5*(01), 34-45.

Sharma, V., & Kumar, M. (2025). Improving intrusion detection with hybrid deep learning models: A study on CIC-IDS2017, UNSW-NB15, and KDD CUP 99. *Journal of Information Systems Engineering and Management*, *10*.

Shiri, F. M., Perumal, T., Mustapha, N., & Mohamed, R. (2023). A comprehensive overview and comparative analysis on deep learning models: CNN, RNN, LSTM, GRU. *arXiv preprint arXiv:2305.17473*.

Sowmya, T., & Anita, E. M. (2023). A comprehensive review of AI based intrusion detection system. *Measurement: Sensors*, *28*, 100827.

Suresh, A., & Cyril Jose, A. (2025). Adaptive network intrusion detection using reinforcement learning with proximal policy optimization. *ACM Transactions on Privacy and Security*, *28*(4), 1-24.

Tarigan, H. P. (2024). Hybrid Learning Approach For Intrusion Detection In Network Security Using Ensemble Methods. *Jurnal Komputer*, *2*(2), 71–74-71–74.

Thirimanne, S. P., Jayawardana, L., Yasakethu, L., Liyanaarachchi, P., & Hewage, C. (2022). Deep neural network based real-time intrusion detection system. *SN Computer Science*, *3*(2), 145.

Tripathy, S. S., & Behera, B. (2025). A review of various datasets for machine learning algorithm-based intrusion detection system: Advances and challenges. *arXiv preprint arXiv:2506.02438*.

Vanin, P., Newe, T., Dhirani, L. L., O'Connell, E., O'Shea, D., Lee, B., & Rao, M. (2022). A study of network intrusion detection systems using artificial intelligence/machine learning. *Applied Sciences*, *12*(22), 11752.

Wu, Y., Zou, B., & Cao, Y. (2024). Current status and challenges and future trends of deep learning-based intrusion detection models. *Journal of Imaging*, *10*(10), 254.

Wu, Z., Gao, P., Cui, L., & Chen, J. (2021). An incremental learning method based on dynamic ensemble RVM for intrusion detection. *IEEE Transactions on Network and Service Management*, *19*(1), 671-685.