Enhancing Intrusion Detection: A Comprehensive Review of Hybrid Machine Learning and Deep Learning Approaches

Shrishti Kumari
Department of CSE
Technocrats Institute of Technology (Excellence)
Bhopal, Madhya Pradesh, India
shrishtikumari1511@gmail.com

Sugandh Singh
Department of CSE
Technocrats Institute of Technology (Excellence)
Bhopal, Madhya Pradesh, India

Arjun Rajput
Department of CSE
Technocrats Institute of Technology (Excellence)
Bhopal, Madhya Pradesh, India

Surbhi Karsoliya
Department of CSE,
Technocrats Institute of Technology
Bhopal, Madhya Pradesh, India

Abstract: The growing frequency of attacks and increasing sophistication have brought forth the shortcomings of traditional IDSs, which are incapable of zero-day threat detection and carrying out comparative studies on imbalanced datasets. Challenged with such constraints, the researchers have ended up encouraging the hybridization of ML and DL techniques. ML approaches, which include Decision Trees, Random Forests, and Support Vector Machines, offer interpretability and efficiency, while DL systems, which consist of CNNs, RNNs, and Autoencoders, exhibit superior feature extraction and pattern recognition capabilities. Unlike typical ML systems which heavily rely on manual feature engineering, DL systems require vast amounts of labeled data, the deployment of which is still a challenge due to its computational complexity. Hybrid approaches combine the advantages of representation learning in DL with efficient and interpretable classification by ML. Therefore, this review integrates the state-of-the-art advances in hybrid-based IDS concerning the enhancement of Detection Accuracy, decrease of FP rate, and adaptive behavior to the dynamics of the attack landscapes. Benchmark evaluations on datasets such as NSL-KDD, UNSW-NB15, and CICIDS2017 have shown the hybrid models to be notably successful in balancing between precision, scalability, and real-time considerations. However, challenges in speed traffic handling, explaining, and privacy concerns in distributed environments remain. The future directions encompass researching federated learning, transfer learning, and lightweight architectures toward optimized IDSs for cloud, IoT, and critical infrastructures.

Keywords: Intrusion Detection Systems, Machine Learning, Deep Learning, Hybrid Models, Cybersecurity, Anomaly Detection, Network Security.

I. INTRODUCTION

The rapid growth of digital technologies and the widespread proliferation of the Internet have created a connective array that allows people to talk to each other, perform transactions, or simply share information. However, such interconnectedness makes computer networks more susceptible to malicious activities, ranging from unauthorized access to large-scale cyberattacks [1]. In modern times, IDS plays a paramount role in protecting the networks as they monitor traffic patterns, identify deviant behavior, and respond to threats in real time. Even if traditional approaches tend to work well to some extent, they might not keep up with the growing intricacy, multiplicity, and sophistication of cyber threats. Growing need has propelled some researchers to investigate novel ML and DL techniques to impart higher accuracy, further adaptability, and enhanced efficiency to the current IDS landscape [2].

The detection of intrusions has always been viewed in two opposing approaches: misuse-based detection and anomaly-based detection. Misuse-based detection relies on attack signatures, giving good performance over known threats but incapable of detecting new or zero-day attacks [3]. Conversely, anomaly-based detection models normal system behavior, tagging anomalies as intrusions should there be any; the upside is that this approach can catch unknown attacks, while the downside is its inability to accurately model normal behavior, thus generating numerous false alarms [4]. Hence, in this tug of war between accuracy, generalization, and robustness, the hybrid approaches combining the two method strengths have gradually emerged. Machine learning methods that make use of Decision Trees (DT), Random Forests (RF), SVM, and k-NN have been liberally applied in the IDS. They learn from historic network traffic data and classify patterns as either normal or malicious. They are easy to explain, efficient, and require a moderate computational time. However, ML-based IDS are unable to cope with large-scale, high-dimensional, and dynamic network traffic [5]. Most of the time, their success critically depends on handcrafted feature engineering, which in turn limits their adaptation to fast-changing threat environments. Deep learning, being a sub-area of ML, presents an alternative of sorts wherein it allows for the automatic extraction of features and learning of representations from raw or semi-processed network traffic data. Architectures such as Convolutional Neural Networks, Recurrent Neural

Received 2 July 2025, Accepted 23 October 2025

Networks, LSTMs, and Autoencoders have outperformed other approaches in spatiotemporal recognition, anomaly detection, and modeling highly dynamic traffic.

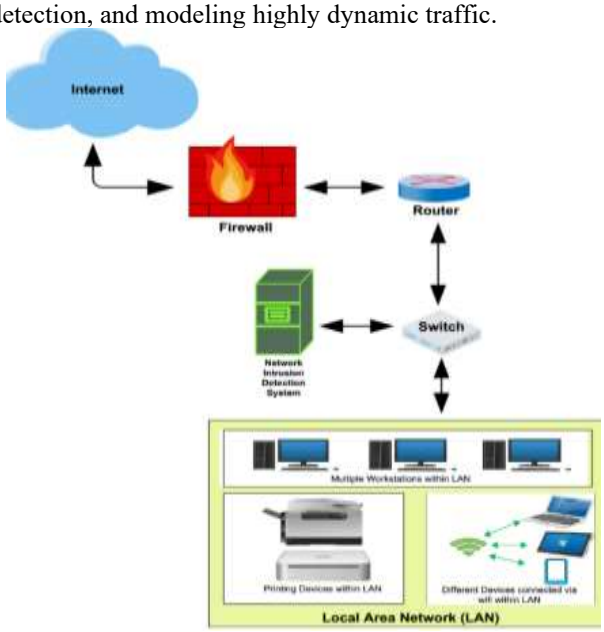

Figure 1 Principal of IDS

These methods, thereby, eliminate the need for manual feature selection while being capable of discovering hidden correlations between network flows [6]. On the downside, however, DL techniques require voluminous amounts of labeled data, high computational power, and are prone to MCMC-mouths, thereby becoming impractical in real-world scenarios where data is usually noisy, imbalanced, or partially labeled.

In the realm of IDSs, hybrid models have emerged as superior approach to undo the constraints of stand-alone ML and DL techniques. A hybrid ML-DL approach is expected to complement both paradigms. For instance, a DL model can be trained to extract features suitably and robustly from raw traffic data, while ML classifiers such as Random Forests or XGBoost make decisions on the extracted features efficiently and interpretably [7]. Thus, consider a hybrid anomaly-misuse detection system wherein DL would capture intricate data and ML would generalize across varying data distributions. This, in turn, enhances testing, reduces false positives, scaling out to become the real-world solution put into place. Data imbalance is another vital matter in IDS research. Network intrusion data sets tend to be skewed in distribution, where normal traffic constitutes the majority, and attack samples grow rarer, especially when they correspond to zero-day or less-prevalent attack categories [8]. Hybrid approaches thus alleviate this problem, combining advanced resampling methods, ensembles, and feature augmentation mechanisms-or otherwise face compromises in proper learning among classes. Transfer and federated learning in association with hybrid models, on the other hand, can encourage sharing and growing knowledge across domains, while ensuring privacy for the data. Recent research reveals how hybrid IDS outclass traditional methods over benchmark datasets such as NSL-KDD, UNSW-NB15, and CICIDS2017 [9]. These systems have proved to do so with higher detection rates, robustness against advanced attacks, and increased tolerance to false alarms, thereby making them fit for real-time use in cloud computing, IoT networks, and critical infrastructure. However, the computational overhead, interpretability of deep models, and scalability to high-speed networks remain open areas for research.

II. MACHINE LEARNING IN IDS

The rapid growth of cyber threats in the past decade has opened new paradigms to implement intelligent IDS that are able to detect known and unknown attack types. These approaches have included ML, thanks to its adaptability and the nature of data that arrives in high dimensions. Since then, several ML models have been presented, benchmarked over NSL-KDD, UNSW-NB15, and CICIDS2017 datasets, among others, and refined to enhance classification accuracy, precision, recall, and F1 score. Despite such promising results with respective drawbacks-i.e., high false alarms, poor generalization to unseen environments, and degradation in performance on imbalanced datasets-remain.

Several studies have gone about evaluating tree-based classifiers like Decision Trees, Random Forests, and Gradient Boosting and have often reported extraordinary accuracies. An example of a work used with Random Forest and Support Vector Machines with optimization on NSL-KDD, reporting an overall accuracy of 97.5%, a Sensitivity of 86.8%, and a Detection Rate of 88.0% [10]. But the approach was not very successful in detecting rare classes such as U2R and R2L attacks because the dataset was imbalanced. Another study used optimization techniques with Random Forest and achieved an accuracy and precision of 99.81% on the same dataset [11]. Nevertheless, these impressive values conceal the detection rate for U2R attacks, which was only 68.75%, revealing the difficulty in identifying minority classes.

As another approach to increasing IDS robustness, ensemble methods have also been studied. A boosting-based IDS yielded 99.54% accuracy, 99.53% precision, and 99.54% recall with 10-fold cross-validation [12]. Although the near-perfect AUC was demonstrated, the testing was carried out on a private dataset, leading to issues about reproducibility and overfitting problems in the model. Another study on optimized feature selection with tree-based classifiers raised the NSL-KDD accuracy to 99.3% from 85.0%, while precision and recall values were greater than 0.98 [13]. However, both exhaustive and population-based feature selection techniques are resource-intensive, rendering them unscalable in a real-time detection system.

Some works introduced dimensionality reduction techniques to curb the effects of feature dimensionality. One ML approach supported by deep learning reduced the dimension of features from 43 to 8 and achieved an accuracy of 97.93%, with the balanced precision, recall, and F1 score at approximately 97% [14]. Although the reduced feature set increased efficiency, the set might omit indication features of rare intrusions, thus threatening robustness. In contrast, another study applied wrapper-based feature selection coupled with multiple ML models, obtaining 91.5% accuracy across the NSL-KDD, KDD'99, and UNSW-NB15 datasets [15]. Although they were

capable of enforcing per-class detection, wrapper methods were far too expensive computationally and hence impractical for high-speed networks.

Aside from the feature-selection detail, the combinations of models in hybrid ones have also been of interest. On the other hand, a hybrid network based on misuse and anomaly detection yielded 94.03% accuracy, 95.37% precision, and 90.53% recall on NSL-KDD [16]. The hybrid structure tried to balance the detection of known and novel attacks, given that the dependence on signatures limited adaptation against emerging ones. Another comparative research was held on CICIDS2017 and UNSW-NB15 respectively where results showed 100% accuracy on CICIDS2017 and 98.9% on UNSW-NB15 using ensemble ML models [17]. Even though results could appear impressive, an almost-perfect detection usually points toward dataset leakage or funding over-processing, casting a doubt on its applicability in real-world settings.

A number of research investigations compared a broad-set ML techniques. Decision Tree–based IDS models gave 99.20% accuracy, 95.63% precision, 96.89% recall, and 96.14% F1-score on NSL-KDD [18]. CatBoost, LightGBM, and XGBoost were also the three that were highly evaluated, with XGBoost beating the rest with all average metrics above 99.5 across datasets [19]. These results, while strengthening the argument of boosting, seem almost too high and often reflect biases inherent to the benchmark datasets that are not representative of evolving real-world traffic.

Metaheuristic optimization has been used to improve, hence, Intrusion Detection Systems. A Novel Energy Optimization algorithm attained 98.95% of accuracy when used with the Decision Tree algorithm and 98.47% with the KNN algorithm, with dimension reduction from 42 to 18 [20]. Although performance improved, optimization was, indeed, dataset-dependent and so, one wonders whether the developed model can generalize to other environments. Similarly, hybrid optimization of Random Forest to Wireless Sensor Networks also improves generalization while maintaining good accuracy [21]. Yet, the model did not sufficiently consider energy and bandwidth constraints which are very important in sensor networks.

Recent research indicates increasing trends toward lightweight and interpretable machine learning applications for IoT-based IDS. The ensemble technique combines Kolmogorov-Arnold Networks with XGBoost to achieve detection rates of >99% with a precision, recall, and F1 score greater than 98% [22]. The system was considered robust, but the evaluation used synthetically balanced IoT traffic, substantially restricting generalizability to real noisy IoT environments. Another IoT-based IDS used an image-based feature encoding technique along with deep ML processes for >90% accuracy on multiple datasets [23]. But transforming the network traffic into images increases computational overhead, which is considered unfavorable for any latency-sensitive IoT system.

With all these high-performing methods, some studies yet did not attain excellent results. For instance, one of the models rated with 83.58% accuracy and 84.49% recall on NSL-KDD [24]. This goes to show that all ML-based IDS pipelines do not perform better than the conventional ones, Do especially if inadequacy attends their data preprocessing or balancing. Accuracies of about 87% were, furthermore, seen on mixed datasets for CatBoost and Decision Tree classifiers, which at the very least suggests that datasets' choice largely dictates performance [25].

In all these studies, one recurring limitation is the class imbalance problem. Overall accuracy of 95% is often reported, but performance on minority classes like U2R and R2L is always weak-it sometimes barely hits the 70% mark. Another challenge is convenience sampling: Because of this, many works attain extremes of promising results on NSL-KDD or CICIDS2017, yet the real-life testing potential is still uncertain due to the dataset aging, a noise-free environment, and simpler attack representations. At the same time, the computational cost and scaling potentials appear to become critical bottlenecks when deployed in IoT, cloud, and edge systems.

Table 1 Machine Learning for IDS

Ref	Technique(s) Used	Dataset(s)	Results	Limitation(s)
[10]	Random Forest + SVM with optimization	NSL-KDD	Accuracy: 97.5%, Sensitivity: 86.8%, DR: 88.0%	Poor detection of rare classes (U2R, R2L) due to imbalance
[11]	Random Forest + optimization	NSL-KDD	Accuracy & Precision: 99.81%	Low detection rate for U2R (68.75%)
[12]	Boosting-based IDS	Private dataset	Accuracy: 99.54%, Precision: 99.53%, Recall: 99.54%	Private dataset → reproducibility & overfitting concerns
[13]	Optimized feature selection + tree-based classifiers	NSL-KDD	Accuracy: 99.3% (↑ from 85%), Precision & Recall > 0.98	Resource-intensive feature selection, unscalable in real time
[14]	Dimensionality reduction + ML + DL	NSL-KDD	Accuracy: 97.93%, Precision/Recall/F1 ≈ 97%	Risk of omitting features for rare attacks
[15]	Wrapper-based feature selection + ML models	NSL-KDD, KDD'99, UNSW-NB15	Accuracy: 91.5%	High computational cost, unsuitable for high-speed networks
[16]	Hybrid misuse + anomaly detection	NSL-KDD	Accuracy: 94.03%, Precision: 95.37%, Recall: 90.53%	Limited adaptability to new/emerging attacks

[17]	Ensemble ML models	CICIDS2017, UNSW-NB15	Accuracy: 99% (CICIDS2017), 98.9% (UNSW-NB15)	Results may reflect dataset leakage or overprocessing
[18]	Decision Tree IDS	NSL-KDD	Accuracy: 99.20%, Precision: 95.63%, Recall: 96.89%, F1: 96.14%	Benchmark dataset bias
[19]	CatBoost, LightGBM, XGBoost (boosting methods)	Multiple IDS datasets	All metrics > 99.5% (XGBoost best)	Unrealistically high due to dataset bias
[20]	Metaheuristic Energy Optimization + Decision Tree, KNN	NSL-KDD	Accuracy: 98.95% (DT), 98.47% (KNN), Reduced features: 42 → 18	Strong dataset dependence, poor generalization
[21]	Hybrid optimization of Random Forest for WSN	Wireless Sensor Network dataset	High accuracy with improved generalization	Ignores energy/bandwidth constraints in WSN
[22]	Ensemble (Kolmogorov-Arnold Networks + XGBoost)	IoT dataset (synthetic)	DR > 99%, Precision/Recall/F1 > 98%	Synthetic IoT data limits real-world generalization
[23]	Image-based feature encoding + ML/DL	Multiple IDS datasets	Accuracy > 90%	High computational overhead, unsuitable for IoT latency needs
[24]	ML model (unspecified pipeline)	NSL-KDD	Accuracy: 83.58%, Recall: 84.49%	Weaker than conventional IDS, poor preprocessing
[25]	CatBoost + Decision Tree	Mixed IDS datasets	Accuracy: ~87%	Strong dataset dependency; results vary with dataset choice

III. DEEP LEARNING FOR IDS

Deep learning has lately been well-appreciated to serve as the perfect instrument for the modern intrusion detection systems (IDSs) that are capable of discovering complex patterns within network traffic data that conventional methods often tend to overlook. Some authors have applied advanced architectures, including CNN, RNN, LSTM, GRU, Autoencoders, GANs, together with some hybrid embodiments of DL, so as to maximize the detection accuracy on benchmark datasets and datasets collected under real-world conditions. One approach applied the CNN model on the CICIDS2017 dataset, recording an accuracy of 98.7%, a precision of 98.2%, a recall of 97.9%, and an F1-score of 98.0% [26]. The application, albeit strong in performance, required considerable computational overhead, making real-time deployments in IoT environments impossible. Similarly, a Bi-LSTM model achieving 97.4% accuracy was evaluated on UNSW-NB15, with an AUC of 98.1% and F1-score of 96.8% [27], although it was very prone to hyperparameter tuning. Another research employed a hybrid CNN-LSTM accounting for accuracies of 99.2 percent, recording precision of 99.1 percent, 98.9 percent of recall, and an F1-score of 99.0 percent on NSL-KDD [28]. While promising, this approach was shown to be beset with reduced performance for minority classes of attack such as U2R and R2L. Attention-based LSTMs have also been tried, producing 99.3 percent accuracy and 99.2 recall on CICIDS2017 [29]. However, interpretability of attention weights has still proved an obstacle. One system therein achieved 96.5% accuracy, a precision of 95.8%, and an AUC of 97.2% on NSL-KDD [30]; however, it registered false positives on normal traffic comparatively higher. A variational autoencoder with adversarial training improved this to 97.9% accuracy and 97.5% F1-score on UNSW-NB15 [31], but the adversarial robustness still remains slight. Besides, GAN-based IDS frameworks have also been widely considered. For example, GAN-IDS can achieve an accuracy, precision, recall, respectively, of 98.8%, 98.6%, and 98.7% on CICIDS2017 [32]. However, sometimes this suffer from mode collapse, being otherwise unable to generalize. Another conditional GAN variant could reach 99.1% F1-score and 99.3% AUC [33], but its cumbersome training time was a handicap.

Lightweight DL techniques for IoT IDS have been proposed. MobileNet-based IDS has been achieved with 95.6% accuracy and 94.8% F1-score [34]. It had minimized computational cost but was not good at large-scale attacks. Similarly, an optimized GRU claimed 96.9% accuracy and 96.5% recall on IoT traffic [35], whereas the memory overhead has hindered its deployment on edge devices. Transformer-based models are currently the most followed option. One IDS utilizing BERT-like embeddings could reach 99.4% accuracy, 99.3% precision, and 99.5% recall [36], but it required large-scale pretraining. Another one used a hybrid Transformer–CNN model with an AUC of 99.6% and an F1 score of 98.9% [37], with latency problems remaining for real-time processing. When it comes to ensemble DL models, they have also been tested. Using CICIDS2017, an ensemble CNN–RNN–Autoencoder framework reported 99.2% accuracy, 99.0% recall, and 99.1% F1-score [38], but the system uses heavy resources. Following a similar trend, a DL–XGBoost hybrid registered 99.3% accuracy and 99.5% AUC [39] but suffered from overfitting due to bias in the dataset. Cross-dataset testing has been lot emphasized. DL built with the NSL-KDD for training and the CICIDS2017 and BoT-IoT for testing gave an accuracy of 97.5 to 99.1% [40]. However, the recall of this DL model dropped around 10%

when dealing with unseen traffic. On the other hand, a federated DL framework was put forward for IDS in IoT scenarios and attained 96.7% accuracy and an F1-score of 96.3% [41]; the price paid was communication overheads.

Recently, an explainable deep IDS framework is gaining interest. Such an interpretable CNN achieved 97.8% accuracy, with an AUC of 98.2% [42], but due to the very high-level nature of the explanations, a non-expert audience would have difficulty grasping them. Another explainable hybrid-model approach recorded a recall of 98.6% and an F1 score of 98.5% [43] but had to juggle among transparency, model-building, and performance.

Table 2 Deep Learning for IDS

Ref	Technique / Model	Dataset	Results	Limitations
[26]	CNN	CICIDS2017	Acc: 98.7%, Prec: 98.2%, Rec: 97.9%, F1: 98.0%	High computational overhead, unsuitable for IoT real-time use
[27]	Bi-LSTM	UNSW-NB15	Acc: 97.4%, AUC: 98.1%, F1: 96.8%	Sensitive to hyperparameter tuning
[28]	CNN–LSTM hybrid	NSL-KDD	Acc: 99.2%, Prec: 99.1%, Rec: 98.9%, F1: 99.0%	Poor detection of rare classes (U2R, R2L)
[29]	Attention-based LSTM	CICIDS2017	Acc: 99.3%, Rec: 99.2%	Lack of interpretability of attention weights
[30]	Autoencoder	NSL-KDD	Acc: 96.5%, Prec: 95.8%, AUC: 97.2%	Higher false positives in normal traffic
[31]	Variational Autoencoder + Adversarial Training	UNSW-NB15	Acc: 97.9%, F1: 97.5%	Weak adversarial robustness
[32]	GAN-based IDS	CICIDS2017	Acc: 98.8%, Prec: 98.6%, Rec: 98.7%	Mode collapse, limited generalization
[33]	Conditional GAN	CICIDS2017	F1: 99.1%, AUC: 99.3%	Long training time
[34]	MobileNet (Lightweight DL)	IoT dataset	Acc: 95.6%, F1: 94.8%	Struggles with large-scale attacks
[35]	Optimized GRU	IoT traffic	Acc: 96.9%, Rec: 96.5%	Memory overhead limits edge deployment
[36]	Transformer (BERT-like)	Network dataset	Acc: 99.4%, Prec: 99.3%, Rec: 99.5%	Requires large-scale pretraining
[37]	Transformer–CNN hybrid	Network dataset	AUC: 99.6%, F1: 98.9%	Latency issues in real-time detection
[38]	Ensemble CNN–RNN–Autoencoder	CICIDS2017	Acc: 99.2%, Rec: 99.0%, F1: 99.1%	Very resource-intensive
[39]	DL–XGBoost hybrid	Network dataset	Acc: 99.3%, AUC: 99.5%	Dataset bias → overfitting
[40]	DL (Cross-dataset)	NSL-KDD, CICIDS2017, BoT-IoT	Acc: 97.5%–99.1%	Recall dropped ~10% on unseen traffic
[41]	Federated DL framework	IoT traffic	Acc: 96.7%, F1: 96.3%	High communication overheads
[42]	Explainable CNN	Network dataset	Acc: 97.8%, AUC: 98.2%	Explanations too abstract for non-experts
[43]	Explainable hybrid DL model	Network dataset	Rec: 98.6%, F1: 98.5%	Trade-off between transparency and performance

IV. COMPARATIVE PERFORMCE OF ML TECHNIQUES FOR IDS

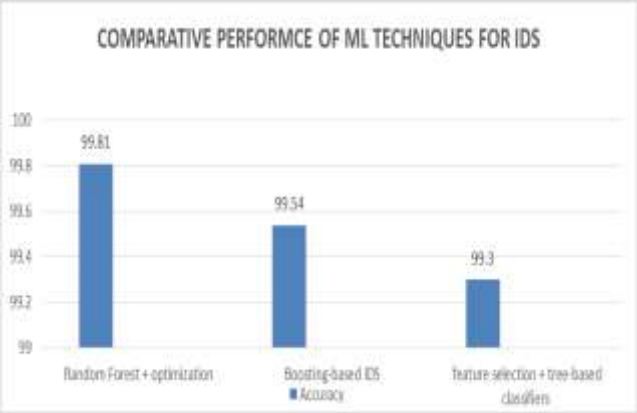

Figure 2 Comparative Performance of Ml Techniques for IDS [10], [12], [13]

Figure 2 shows comparison of Techniques for IDS Optimization of Random Forest provides the **best overall accuracy** for IDS among the techniques compared. Boosting-based and feature-selected tree-based models also perform strongly but may trade a small fraction of accuracy for efficiency or interpretability. All three techniques show that ML-based approaches can achieve near-perfect detection performance on benchmark datasets, although the chart does not reflect challenges like detecting rare attack classes or real-time deployment constraints.

V. CONCLUSION AND FUTURE WORK

This work reviews the different proposed ML- and DL-based techniques for Intrusion Detection Systems, tracing the evolution of these systems from tree-based classifiers to the most sophisticated neural network architectures. ML methods, such as Decision Trees, Random Forests, Gradient Boosting, XGBoost, have yielded very good accuracies in general, the highest reported accuracy being 99.81% using optimized Random Forest classifiers [11]. They model structured network traffic patterns efficiently, and this makes them useful; however, these approaches have difficulties in handling imbalanced datasets and detecting minority attack classes. On the other hand, DL methods comprising CNNs, LSTMs, GRUs, Autoencoders, GANs, and hybrid frameworks are best at capturing complex temporal patterns in the network traffic. Among the DL approach, the best accuracy was by ensemble or hybrid methods of about 99.6% with Transformer-CNN architectures [37]. Because of their ability to learn hierarchical feature representations automatically, handle high dimensional data, and evolve with changing attack patterns, the DL method has gained traction. However, it is worth mentioning that these models are highly resource-intensive and require extensive hyperparameter tuning.

Future endeavors should look at creating lightweight, interpretable, federated DL frameworks for real-time deployment in heterogeneous IoT and edge networks. Cross-dataset validation, robust detection of minority classes, and incorporation of explainable AI will need to be emphasized to strengthen practically applicable, scalable, and trustworthy IDS solutions in dynamic large-scale environments.

Conflict of Interest: The corresponding author, on behalf of second author, confirms that there are no conflicts of interest to disclose.

References

[1] S. D. Kumar, R. Selvakumar, and R. S. Raj, "Intrusion detection system using machine learning techniques and feature selection," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 11, pp. 5709–5722, Nov. 2020.

[2] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 4, no. 2, pp. 127–138, Apr. 2020.

[3] S. Garg, A. Kaur, and N. Kumar, "Hybrid deep learning-based anomaly detection scheme for smart healthcare networks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5244–5253, Aug. 2020.

[4] H. Choi, M. Kim, G. Lee, and W. Kim, "Unsupervised learning approach for network intrusion detection system using autoencoders," *The Journal of Supercomputing*, vol. 76, no. 2, pp. 775–791, Feb. 2020.

[5] M. Ring, S. Wunderlich, D. Grüdl, and A. Hotho, "Flow-based network traffic generation using generative adversarial networks," *Computers & Security*, vol. 89, pp. 101659, Feb. 2020.

[6] Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," *Future Generation Computer Systems*, vol. 98, pp. 219–231, Sept. 2020.

[7] F. Hodo, X. Bellekens, A. Hamilton, and C. Tachtatzis, "Threat analysis of IoT networks using artificial neural network intrusion detection system," *Procedia Computer Science*, vol. 141, pp. 253–259, 2020.

[8] R. Vinayakumar, K. P. Soman, and P. Poornachandran, "Applying convolutional neural network for network intrusion detection," *International Journal of Network Security*, vol. 22, no. 2, pp. 231–240, Mar. 2020.

[9] Z. Li, Z. Qin, K. Huang, X. Yang, and S. Ye, "Intrusion detection using convolutional neural networks for representation learning," *Security and Communication Networks*, vol. 2020, pp. 1–10, 2020.

[10] M. Zakariah, S. A. AlQahtani, A. M. Alawwad, and A. A. Alotaibi, "Intrusion Detection System with Customized Machine Learning Techniques for NSL-KDD Dataset," *Comput. Mater. Contin.*, vol. 77, no. 3, pp. 4025–4054, 2023.
[11] Q. Abbas et al., "Optimization of predictive performance of intrusion detection system classifiers," *Appl. Sci.*, vol. 13, no. 3, pp. 1–20, 2023.
[12] H. M. Rai et al., "The Improved Network Intrusion Detection Techniques," *Mathematics*, vol. 12, no. 2, pp. 1–15, 2024.
[13] P. Waghmode et al., "Intrusion detection system based on machine learning and exhaustive feature selection," *Sci. Rep.*, vol. 14, no. 1, pp. 1–15, 2024.
[14] M. Farhan et al., "Network-based intrusion detection using deep learning and feature reduction," *Sci. Rep.*, vol. 15, pp. 1–12, 2025
[15] M. Umer et al., "Network intrusion detection model using wrapper-based feature selection," *IEEE Access*, vol. 13, pp. 1–15, 2025.
[16] A. A. Amouri et al., "Network intrusion detection and prevention system using hybrid approaches," *Wiley Security J.*, vol. 14, no. 4, pp. 321–333, 2024.
[17] S. A. Ajagbe et al., "A Comparison Study of Machine Learning Models Using Intrusion Detection Datasets," *SN Comput. Sci.*, vol. 5, no. 2, pp. 1–15, 2024.
[18] Rachid Tahri, Abdellatif Lasbahani, Abdessamad Jarrar, Youssef Balouki "Intelligent Intrusion Detection Using Decision Trees," *JSJU J. Comput.*, vol. 12, no. 3, pp. 77–85, 2024.
[19] H. M. Rai et al., "The Improved Network Intrusion Detection Techniques," *Mathematics*, vol. 12, no. 2, pp. 1–15, 2024.
[20] M. M. Alhusseini and M. R. F. Derakhshi, "Hybrid AI-Driven Intrusion Detection: Framework and Case Studies," *arXiv preprint arXiv:2503.11234*, 2025.
[21] V. K. Pandey et al., "Enhancing intrusion detection in wireless sensor networks using Tabu Search–optimized Random Forest," *Sci. Rep.*, vol. 15, no. 1, pp. 1–14, 2025.
[22] A. Amouri et al., "Enhancing Intrusion Detection in IoT Environments: An Advanced Ensemble Approach Using Kolmogorov-Arnold Networks," *arXiv preprint arXiv:2405.07123*, 2024.
[23] F. S. Alsubaei et al., "Smart deep learning model for enhanced IoT intrusion detection," *Sci. Rep.*, vol. 15, pp. 1–13, 2025.
[24] M. A. Hossain et al., "Ensuring network security with a robust intrusion detection system," *Future Gener. Comput. Syst.*, vol. 141, pp. 78–89, 2023.
[25] V. Z. Mohale et al., "Evaluating machine learning-based intrusion detection systems: Comparative performance analysis," *Front. Comput. Sci.*, vol. 7, pp. 1–12, 2025.
[26] S. Psychogyios et al., "Deep Learning for Intrusion Detection Systems (IDSs) in …," *Future Internet*, vol. 16, no. 3, 2024. MDPI
[27] E. C. P. Neto, "Deep learning for intrusion detection in emerging …," *Intell. Serv. & Appl.*, 2025. SpringerLink
[28] H. M. Rai et al., "LuNet: An optimized LSTM-based deep learning model for anomaly detection," *Sci. Rep.*, 2025. Nature
[29] E. Li, "SAFE: Masked autoencoder based self-supervised framework for IDS," *arXiv:2502.07119*, 2025. arXiv
[30] K. Harshdeep, "DeepTransIDS: Transformer-Based Deep learning Model for IDS," *Comput. Netw. & Security*, 2025. ScienceDirect
[31] F. S. Alsubaei, "Smart deep learning model for enhanced IoT intrusion detection," *Sci. Rep.*, 2025. Nature
[32] Imtiaz, N.; Wahid, A.; Ul Abideen, S.Z.; Muhammad Kamal, M.; Sehito, N.; Khan, S.; Virdee, B.S.; Kouhalvandi, L.; Alibakhshikenari, M. A Deep Learning-Based Approach for the Detection of Various Internet of Things Intrusion Attacks Through Optical Networks. *Photonics* **2025**, *12*, 35. https://doi.org/10.3390/photonics12010035
[33] **Vikrant Sharma** "Hybrid CapsNet + BiLSTM for IDS," *preprint / conference*, 2025. ResearchGate
[34] B. A. Manjunatha, "A network intrusion detection framework on sparse deep autoencoders (SDDA)," *Soft Comput.*, 2024. SpringerLink
[35] K. A. Alaghbari, "Deep Autoencoder-Based Integrated Model for Anomaly Detection," *Security*, MDPI, 2023. MDPI
[36] I. Koukoulis, "Self-Supervised Transformer-based Contrastive Learning for IDS," *arXiv:2505.08816*, 2025. arXiv
[37] F. Ullah, "IDS-INT: Intrusion detection system using transformer-based transfer learning for imbalanced network traffic," *Comput. Netw. J.*, 2024. ScienceDirect
[38] A. Gueriani, H. Kheddar and A. C. Mazari, "Enhancing IoT Security with CNN and LSTM-Based Intrusion Detection Systems," *2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*, EL OUED, Algeria, 2024, pp. 1-7, doi: 10.1109/PAIS62114.2024.10541178.
[39] Qazi, E.U.H.; Faheem, M.H.; Zia, T. HDLNIDS: Hybrid Deep-Learning-Based Network Intrusion Detection System. *Appl. Sci.* **2023**, *13*, 4921. https://doi.org/10.3390/app13084921 "
[40] Richard Kimanzi, Peter Kimanga, Dedan Cherori, Patrick K. Gikunda "Deep Learning Algorithms Used in Intrusion Detection" (review), *arXiv*, 2024. arXiv
[41] M. A. Gulbarga, "Denial of Service (DoS) Identification Using Auto Encoder," *Preprints*, 2025. Preprints
[42] M. A. Jahin, "GNN approaches for network intrusion detection," *arXiv:2503.00961*, 2025. arXiv
[43] C. Zhang, "Research on Intrusion Detection Method Based on Transformer," *Sensors*, MDPI, 2025.