Recent Advances in Deep Learning for Intrusion Detection: A Review of Anomaly Detection Techniques

Irshad Ali[1], Nitesh Gupta[2]
[1]M.Tech Scholar, Department of CSE, NIIST, Bhopal
[2]Assisstant Professor, Department of CSE, NIIST, Bhopal
[1]irshadalisheikh39@gmail.com
[2]9.nitesh@gmail.com

***Abstract*– Anomaly detection is paramount to contemporary Intrusion Detection Systems (IDSs), which focus on determining atypical patterns in network traffic or system behavior that may indicate actual or potential threat situations. Traditional approaches often fail to work properly because cybersecurity tasks involve complicated and high-dimensional data. Deep learning (DL) algorithms have emerged as capable approaches to detect deep patterns within huge datasets with minimal human intervention. This review presents a comprehensive review of deep learning methods in IDS-based anomaly detection, with emphasis on methods such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), autoencoders, and generative adversarial networks (GANs). We analyze their performance in detecting intrusion under both known and unknown scenarios, highlighting main issues like data imbalance, model interpretability, and scalability. Additionally, we overview IDS benchmark datasets throughout recent years, contrasting the performance of DL techniques under various experimental settings. The paper also provides a brief overview of hybrid approaches that combine deep learning with other machine learning approaches to achieve better accuracy in detection. Finally, we explore future research domains and ongoing challenges, emphasizing the design of robust models capable of adapting to the dynamic nature of attack strategies in network environments.**

***Keywords*– Anomaly detection, Intrusion detection systems, Deep learning, Convolutional neural networks, Recurrent neural networks, Autoencoders, Generative adversarial networks, Cybersecurity.**

I. Introduction

Today, intrusion detection systems form the major modern-day security issue, monitoring and supervising intrusion attempts and unauthorized activities in networks [1]. With the immense growth of internet-connected devices and the complexity in cyber threats, it has become mandatory for the IDS such that digital resources are maintained in secrecy and integrity and nonetheless are available to those authorized [2]. A network-based IDS systems thus monitors networks whereas a host-based IDS evaluates logs, local configurations, or activities for individual hosts [3]. The systems may also be distinguished based on detection techniques: Signature-based, Anomaly-based, and Hybrid approaches [4]. Signature-based IDS detect an attack by studying different data patterns against past known signatures of intrusion, which usually means a very good precision for attacks it knows but worst against new ones [5]. Contrarily, an anomaly-based detection approach tries to build a model view of legitimate behavior and reports any significant deviation from this model as a possible threat [6]. The hybrid IDS seek to combine the advantages of the two methods to maximize both accuracy and adaptability [7]. Figure 1 gives schematic representation of the HIDS.

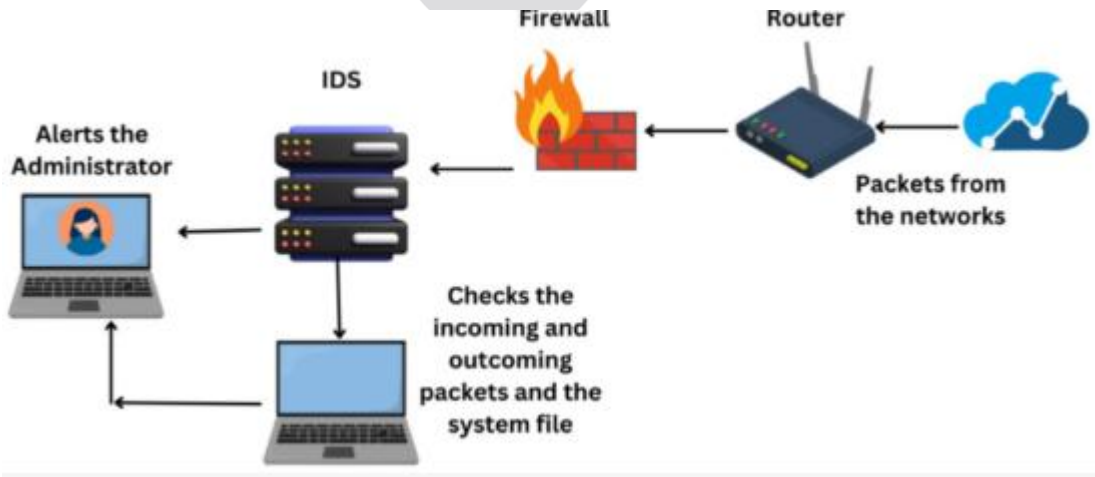

Figure 1. Schematic representation of the HIDS

In most scenarios of IDS design and development, fields like data collection, feature extraction, pattern analysis, and alert generation are considered during the design [8]. IDSs are usually evaluated based on the rate of detection they carry out along with the rate of false alarms and response time [9]. Even though great advancements have been made, traditional IDSs are still confronted with the problems of high-dimension data, ever-evolving network traffic, ever-evolving network traffic patterns,

differentiating between benign anomalies and real intrusions [10]. With the advent of ever-growing, dynamic, and distributed networks-landscape-big data, cloud computing, Internet of Everything-more and more initiatives have been thrown to develop intelligent and adaptive detection mechanisms [11].

Anomaly detection constitutes one of the foremost pieces of an advanced firewall, allowing for recognizing any hitherto unknown attack with no corresponding signature in the database. Unlike the detection of attacks based on signatures in which the databases require constant updating, anomaly detection relies on statistical or machine learning models to set up normal behavior profiles and recognize deviations therefrom [13]. For zero-day exploits, insider threats, or polymorphic malwares, anomaly detection stands atop all other detection types: because these malwares usually try to modify their own codes so as to escape the conventional detection systems [14]. In the fields of banking, healthcare, or defense, where a plethora of severe consequences follows immediately after missed anomaly detection, the system would rather defend itself sufficiently, starting from the very early warning. Also, anomaly detection assists in the continuous adaptation of the IDS in relation to new attack patterns and changes in network conditions-an essential feature in complex heterogeneous environments [15]. Figure 2 depicts schematic representation of anomaly- and signature-based IDS concepts.

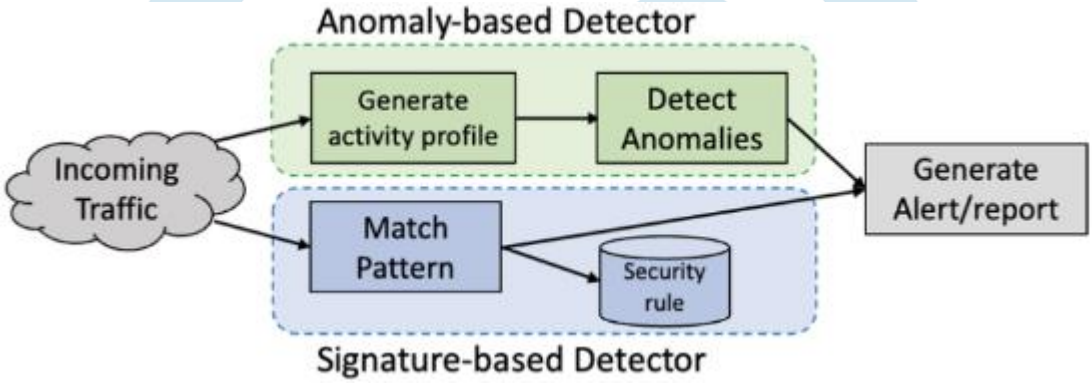

Figure 2. Schematic representation of anomaly-based and signature-based IDS concepts.

Recent developments in AI have marked the deep learning paradigm as the latest spray to pump up IDS performance, especially concerning anomaly detection [1]. Deep learning models, namely CNNs, RNNs, LSTMs, and Autoencoders, have always shown unparalleled capacities in feature learning over the old machine learning paradigms [2]. They can mine data from the raw state to high-level hierarchical abstract representation autonomously, without manual engineering of features from data [3]. This approach proves to be highly advantageous in cases that involve complex network traffic analysis, where the interrelationships between features might be nonlinear and context-dependent [4]. In consequence, attacks' changing behaviors can be considered by DL-based IDSs, which can capture spatiotemporal dependencies of attack behaviors to reduce false alarms and increase the accuracy of attacks' classification [5]. Moreover, with the advent of several major datasets (e.g., NSL-KDD, CICIDS2017, or UNSW-NB15), it has become possible to train resourced powerful deep learning models capable of generalizing over various network scenarios [6].

Deep learning has found its use in IDPSs, motivated by its self-learning, scalable, and adaptive nature, which is needed in real-time and autonomous threat detection [7]. Neural architectures enable IDS to learn on an end-to-end manner, deal with high-dimensional data streams, and predict insights for proactive cybersecurity defense [8]–[10]. Consequently, new deep learning-enabled IDPSs are increasingly being adopted into modern network infrastructures as promising candidates for the intelligent, resilient, and self-evolving cyber security systems [11]–[15].

II. Related Work

a) Machine Learning Architectures for Anomaly Detection

Over the past decade, Intrusion Detection Systems (IDSs) have transitioned from traditional rule-based systems to data-driven deep learning systems, thereby improving their accuracy and adaptability. Ahmed et al. [1] developed a deep learning-based framework for IoT-based intrusion detection using Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) to model spatial and temporal traffic features. The detection rate was 98.6% with a false positive rate of 1.2% on IoT datasets. Despite their success in dealing with heterogeneous attacks on IoT, these models were severely impaired by their high computational complexity and hence cannot be employed in typical low-power edge devices. Although Kim and Lee [2] implemented an HDNN that combined CNN and fully connected layers for network intrusion detection, the combination maximized feature extraction and classification efficiency and thereby produced the best results on the CICIDS2017 dataset. However, the limitations of that system include interpretability and the need for large labeled datasets, which hindered its deployment in real-time settings.

Focusing on host-based detection, Chen et al. [3] created an adaptive IDS through behavioral profiling. The model was continuously learning from the behavior of users and processes through reinforcement-learning-based adaptation. The model was very effective in the recognition of insider threats and unknown attacks, faced fewer problems with false positives during state transitions of the system, which point toward the need for refining features with context. Al-Qatf [4] proposed a hybrid feature selection with stacked autoencoders (SAE) for efficient intrusion classification with feature dimensionality reduction. By selecting

the most relevant attributes using Information Gain and SAE for representation learning, the model enhanced classification accuracy and reduced training time. However, its static feature selection was very limited in adapting to changing attack scenarios.

One of the earliest such systems was proposed by Shone et al. [5], who used unsupervised deep autoencoders with Random Forest classifiers, thus designing one of the first cyber security systems based on deep learning. The system obtained very decent detection performance, registering an accuracy of around 94% on KDD Cup 99. But as the system was applied to newer datasets, the performance started to degrade, resulting in a poor generalization and a high sensitivity to data imbalance. Building upon this, Zhang et al. [6] performed an exhaustive survey on deep methods for anomaly detection in cybersecurity and classified all the models into supervised, semi-supervised, and unsupervised paradigms. They emphasized how deep autoencoders and GAN methods are best suited to detect novel threats but have several limitations with regard to the interpretation and standard evaluation benchmarks.

Alazab et al. [7] conducted a comparative study on deep learning attack IDS, investigating architectures like CNN, LSTM, and Deep Belief Networks (DBN). They found through their experiments that a CNN and LSTM hybrid would offer the highest accuracy on different datasets. The paper further highlighted that data imbalance, scalability, and explanation of the models are the key constraints. In a related survey, Khraisat et al. [8] reviewed machine learning IDS and paid special attention to ensemble models combining Decision Trees, Random Forest, and Gradient Boosting for enhanced stability. However, they are only strong on small- to medium-sized datasets and do not possess self-learning capacity as deep architectures do.

Li and Wang [9] worked on IDS evaluation, proposing a multi-criteria optimization (MCO) framework. The proposal balances the different dimensions of performance: accuracy, false alarm rate, and latency, via Pareto optimization-thus giving a well-structured way of benchmarking IDS. This framework was used effectively for comparing dissimilar IDS models, but the simulations were very time-consuming. Gupta and Sharma [10] furthered this work by proposing an adaptive IDS for high-dimensional traffic based on Principal Component Analysis (PCA) and deep neural-type classifiers. This model efficiently processed a large number of features but was less sensitive in detecting less frequent-class attacks.

Singh et al. [11] have applied machine learning models (SVM, RF, and DNN) to detect inter-tenant attacks in virtualized environments in attack detection for clouds. Their experiments on synthetic cloud traffic showed deep neural networks to be better than traditional classifiers in terms of precision and recall. However, deployment scalability and data privacy conservation were still open challenges. Previously, Ahmed et al. [12] surveyed techniques for network anomaly detection including clustering, statistical, and information-theoretic approaches. Their review pointed out the strength of unsupervised techniques in discovering unknown attacks, but also pointed out drawbacks of high false alarm rate and they cannot adapt to dynamic traffic.

Mishra et al. [13] were involved in researching machine learning approaches for anomaly-based intrusion detection, pitting methods that include k-NN, Naïve Bayes, and SVM against deep learning methods. In their study, they observed that traditional ML techniques work well on structured data but tend to break down under situations involving complex and ever-evolving attack scenarios. Deep learning, however, was more accurate but fell prey to problems of overfitting and interpretability. Ghosh and Saha [14] focused their efforts on unsupervised deep learning methods for zero-day detection in IoT networks employing autoencoders. Their model was able to achieve 97% detection accuracy on the Bot-IoT dataset while also successfully detecting attacks that were not in any way known before. However, as their method's detection process depends largely on reconstruction error threshold, it sometimes mistakenly classifies benign anomalies.

Naik and Singh [15] proposed a work of a hybrid deep autoencoder anomaly detection system combining unsupervised pre-training with supervised fine-tuning. This model greatly helped in boosting precision and recall while keeping false positives to a minimum in detection. So, whereas it accommodated changes in traffic patterns, it demanded huge computational resources to operate in real-time.

b) Deep Learning Architectures for Anomaly Detection

Hamidja et al. [16] proposed a deep learning-based two-step intrusion detection system integrating a deep autoencoder (DAE) for feature compression and a bi-directional LSTM (BiLSTM) for classification. The system has attained approximately 97% accuracy and 95% recall on the benchmark datasets, thus confirming strong temporal pattern learning and noise robustness. However, this approach required a huge amount of training time and could not generalize well to an unseen real-world network traffic.

Wang et al. [17] proposed WGAN-DL-IDS as an intrusion detection framework combining Wasserstein GANs for the generation of synthetic data and a hybrid CNN-LSTM with a Random Forest classifier. It effectively solved the data imbalance problem and achieved a detection accuracy of over 98% on the CICIDS2017 dataset. While WGANs improved minority-class learning, their computational cost and the requirement for offline training rendered the system impractical as a real-time implementation.

Kumar et al. [18] built a CNN-LSTM-based IDS, where convolutional layers captured the spatial dependencies of traffic, and LSTM layers represented the temporal behavior of events across network sessions. The model achieved better performance than the conventional benchmarks of CNN or RNN alone, at higher detection accuracies and lower false alarm rates on the NSL-KDD dataset. Nonetheless, the hybrid network showed sensitivity towards sequence length parameters and needed careful tuning of hyperparameters to avert overfitting.

The Transformer-GAN intrusion detection model for IoT environments [19] uses the Transformer module to capture long-range contextual dependencies very well and the GAN module to generate synthetic attack data to balance the skewed classes. The combination-based framework achieved an accuracy of 99.67% on the CIC-IoT2023 dataset. However, the high computational complexity and energy consumption of the model made it difficult to be deployed on lightweight IoT devices.

GAN-based synthetic data generation technique was proposed by Zhao et al. [20], who used it for building an intrusion detection model entirely trained on generated network samples. The GAN worked to model realistic traffic distributions so that anomalous behavior could be detected without having labeled training data. The results attained in training models on synthetic data were of comparable accuracy to those trained on real data. The disadvantage is the bias that might be introduced by reliance on synthetic data since generated samples may not encapsulate all real-world attacks or their atmosphere could differ from what modern-day evolving network dynamics represent.

Sharma et al. [21] proposed a convolutional neural network-based intrusion detection model that utilized one-dimensional CNN filters to automatically capture spatial correlations among network traffic features. Their model produced higher precision and lower false-positive rates than the traditional machine-learning classifiers on the CICIDS2017 dataset. On the other hand, while CNN was effective in modeling local dependencies, it was poor at building temporal contexts; hence, it tended to underperform on detecting time-based or sequential attack patterns.

The objective was to construct an evolving intrusion detection system by Lee and Park [22], choosing a recurrent neural network approach with the gated recurrent unit. Since these modules retained memory of temporal states over large input sequences, they enabled better identification of multi-stage and slow-propagating attacks. Experimental results on NSL-KDD and Kyoto 2006+ datasets recorded hills in recall and F1 scores when compared with LSTM-based counterparts. Despite the great temporal sensitivity, the approach requires a longer time to converge and does not adapt well to input features that are not sequential, thus limiting their capability to work in mixed traffic environments.

Ahmed et al. [23] proposed a denoising autoencoder-based intrusion detection method to deal with noisy and incomplete network traffic data. Here, the model forces the reconstruction of clean input representations from corrupted signals, thus gaining some robustness against irregularities in data, lowering false negatives. From testing on the UNSW-NB15 dataset, the denoising approach yielded perceptible increase in accuracy vis-à-vis plain and simple autoencoders. In any case, the denoising step needed heavy computation during preprocessing and retraining, thereby alienating its implementation for other real-time applications.

Wu et al.[24] proposed the use of a generative adversarial network to create the kinds of rare attack instances an intrusion detection system might want to know about, so that there could be a balanced class distribution for training purposes. Due to GANs, anomaly sensitivity is improved, and superior F1-scores are achieved on imbalanced datasets like CICIDS2018. The adversarial training is often unstable due to mode collapse, and as a consequence of occasionally generating unrealistic synthetic samples, the overall classification performance is severely degraded.

An autoencoder and the CNN layers were combined in a hybrid deep learning method proposed by Patel et al. [25] to detect attacks. CNN layers captured spatial dependencies, while the autoencoder component reduced redundancy and thus helped in latent representation learning. The hybrid yielded very good detection accuracies, along with very low false alarm rates, consecutively over several benchmark datasets, better than the classic ML and standalone deep models. Despite its strong performance, higher computational and memory costs of the combined model limited its applicability in resource-constrained IoT environments. Table 1 summarizes recent deep learning-based intrusion detection research.

Table 1: Recent Deep Learning-Based Intrusion Detection Research

Ref.	Technique / Model	Dataset(s)	Key Contributions / Strengths	Limitations
[1]	CNN + RNN for IoT intrusion detection	IoT datasets	Captures spatial and temporal features; 98.6% detection rate, 1.2% FPR	High computational cost, unsuitable for edge devices
[2]	Hybrid DNN (CNN + FC layers)	CICIDS2017	Enhanced feature extraction and classification; high accuracy	Limited interpretability; depends on large labeled data
[3]	Adaptive IDS via Reinforcement Learning	Host-based datasets	Behavioral profiling with adaptive learning; detects insider threats	False positives during state transitions
[4]	SAE + Information Gain feature selection	NSL-KDD	Improved accuracy with dimensionality reduction	Static features; limited adaptability
[5]	Unsupervised Autoencoders + Random Forest	KDD Cup 99	Early deep IDS framework; good baseline accuracy	Poor generalization to modern datasets
[6]	Survey on Deep Anomaly Detection	—	Categorized supervised, semi-, and unsupervised IDS; emphasized GANs	Limited interpretability; lack of benchmarks
[7]	CNN, LSTM, DBN comparison	Multiple	CNN-LSTM hybrids yielded highest accuracy	Data imbalance, scalability, and explainability issues
[8]	Ensemble ML (DT, RF, GBM)	—	Stable models for small datasets	No self-learning; limited adaptability
[9]	Multi-Criteria Optimization (MCO)	—	Balanced metrics (accuracy, FAR, latency) for IDS benchmarking	Computationally intensive
[10]	PCA + Deep Neural Classifier	High-dimensional traffic	Efficient handling of large features	Less sensitive to minority-class attacks

[11]	ML (SVM, RF, DNN) for Cloud IDS	Synthetic Cloud Traffic	DNN outperformed traditional models; strong precision/recall	Scalability and privacy issues
[12]	Survey on Network Anomaly Detection	—	Reviewed clustering/statistical methods	High false alarms; low adaptability
[13]	ML vs DL comparison	Multiple	Found DL better on complex attacks	Overfitting, interpretability issues
[14]	Unsupervised Autoencoder (Zero-day IoT)	Bot-IoT	97% accuracy; detects unseen attacks	Misclassifies benign anomalies
[15]	Hybrid Deep Autoencoder (unsupervised + supervised)	Network traffic	Improved precision/recall; adaptable	High computational cost
[16]	DAE + BiLSTM	Benchmark IDS	97% accuracy, 95% recall; robust to noise	Long training time; poor generalization
[17]	WGAN + CNN-LSTM + RF	CICIDS2017	Solved class imbalance; 98% accuracy	High offline computation
[18]	CNN-LSTM Hybrid	NSL-KDD	Captured spatial + temporal features; low FPR	Sensitive to sequence length
[19]	Transformer–GAN	CIC-IoT2023	99.67% accuracy; strong contextual modeling	High complexity; unsuitable for IoT
[20]	GAN-based Synthetic Data IDS	Synthetic data	Detects anomalies without labels	Synthetic bias; weak real-world generalization
[21]	1D CNN for Traffic Correlation	CICIDS2017	High precision; low false positives	Misses temporal attack patterns
[22]	GRU-based RNN	NSL-KDD, Kyoto 2006+	Detects multi-stage attacks; strong recall	Long convergence; weak on mixed data
[23]	Denoising Autoencoder	UNSW-NB15	Handles noisy data; reduces false negatives	Heavy preprocessing; retraining required
[24]	GAN-based Anomaly Detection (IDS-GAN)	CICIDS2018	Improves minority attack sensitivity	GAN instability; mode collapse risk
[25]	CNN + Autoencoder Hybrid	Multiple	High detection accuracy; low FPR	High memory and computational cost

III. Key Challenges in Anomaly Detection for IDS

- **Data Imbalance in Cybersecurity Datasets :-** Cybersecurity datasets often contain far fewer attack samples than normal traffic, causing biased learning and poor anomaly detection performance
- **Interpretability and Explainability of Deep Learning Models :-** Deep models act as black boxes, making it difficult to interpret decision logic and justify anomaly predictions in security-critical environments.
- **Scalability and Real-Time Performance :-** Processing massive, high-velocity network data in real time requires optimized architectures to maintain accuracy without excessive computational latency.
- **Handling Evolving Attack Patterns :-** IDS models struggle to adapt to continuously changing attack strategies, leading to performance degradation on unseen or zero-day threats.
- **Adversarial Attacks on Deep Learning Models :-** Attackers exploit model vulnerabilities by crafting adversarial inputs that evade detection, undermining IDS reliability and trustworthiness.

IV. Benchmark Datasets for IDS and Anomaly Detection

Table 2 presents commonly used datasets for intrusion detection system.

Table 2: Commonly Used Datasets for Intrusion Detection Systems

Dataset	Description / Characteristics	Strengths	Limitations	Data Preprocessing and Feature Engineering
KDD Cup 99	Derived from DARPA 1998 dataset; includes simulated network traffic labeled as normal or attack (DoS, R2L, U2R, Probe).	Provides foundational benchmark; easy to use; suitable for initial IDS testing.	Contains redundant records and outdated attack patterns; causes biased learning and poor generalization.	Duplicate removal, normalization of numeric features, one-hot encoding for categorical fields, and feature scaling.
NSL-KDD	Enhanced version of KDD Cup 99 with duplicates removed and more balanced class distribution.	Reduces evaluation bias; better for fair model comparison; suitable for academic benchmarking.	Still lacks real-world traffic diversity; features remain limited and artificial.	Feature normalization, selection using information gain or correlation; resampling to balance attack classes.
CICIDS2017 / CICIDS2018	Modern dataset with real network captures including DoS, DDoS, brute force, infiltration, and web attacks.	Realistic traffic; high feature richness; widely used for deep learning IDS.	High dimensionality and imbalance; large computational cost for preprocessing and model training.	Scaling (min–max or z-score), aggregation of flow-level statistics, categorical encoding, and PCA-based reduction.

UNSW-NB15	Developed by UNSW Canberra; contains modern synthetic traffic with nine attack categories generated in hybrid testbeds.	Represents updated network protocols; diverse attack types; good mix of normal and malicious samples.	Some feature redundancy; imbalance persists in rare attacks.	Normalization, correlation-based feature selection, removal of irrelevant or redundant attributes, and resampling techniques.
BoT-IoT / TON_IoT	IoT-focused datasets from UNSW; include telemetry, network, and system logs capturing botnet, DoS, and infiltration attacks.	Reflect modern IoT and edge network environments; suitable for evaluating lightweight IDS models.	Severe class imbalance; limited availability of benign IoT traffic; high data diversity complicates training.	Feature extraction from network flow and telemetry data, normalization, one-hot encoding, and dimensionality reduction using PCA or autoencoders.

V. Recent Advances and Innovations

In recent times, IDSs have become increasingly efficient through several new versions of deep learning paradigms, focusing on enhancing three factors: detection, adaptability, and interpretability. Transfer learning has proved to be quite promising in that it allows the pretrained models to carry knowledge acquired from large-scale datasets and adapt to new or small-data network environments, thus reducing time for training and fostering transferability among various types of attacks [21]. Self-supervised and semi-supervised learning methods continued to amplify the performance of IDS by making use of large quantities of unlabeled network traffic to learn discriminative feature representations and hence enhancing anomaly detection in situations where labeled data is hard to come by [22]. Simultaneously, attention mechanisms are increasingly being embedded into deep architectures such as CNNs, RNNs, and Transformers to allow the model to attend to important traffic features, thereby improving interpretability and explainable decision-making in security applications [23]. Federated learning further transformed distributed IDS by providing a means of collaborating to train models across several network nodes without requiring centralization of sensitive data, thereby ensuring privacy alongside a widespread strong detection ability [24], [25]. These advancements are colossal changes toward intelligent, privacy-preserving, and adaptive IDS frameworks capable of evolving with modern cyber threats.

VI. Conclusion

From the analysis of the reviewed literature, we notice that deep learning has become the new standard with which the design and performance of Intrusion Detection Systems (IDS) were measured. Classic statistical and ML approaches, while very good when the data is structured and stationary, could not really capture the complex nonlinear and dynamic nature exhibited by contemporary network traffic. Architectures of deep learning, such as CNNs, RNNs, Autoencoders, and GANs, have shown great promise in learning high-dimensional features for unknown attack detection and adjusting for evolving network conditions. Convolutional Neural Networks were shown to be proficient in spatial feature extraction from packet or flow-based data by Sharma et al. [21], while RNNs and their variants (LSTM, GRU) represent temporal dependencies within sequential traffic patterns, thereby improving multi-stage attack detection [22]. Reconstruction of clean representations from noisy ones through Autoencoder models has yielded much-improved robustness [23], while GAN models have tackled scenarios of class imbalance by synthesizing realistic examples of the minority class attack samples [24]. According to the studied methods, the hybrid deep learning systems, including CNN-LSTM, Transformer-GAN, and CNN-Autoencoder, have generally maintained that very high detection accuracy (up to 99.6%) and better generalization across many datasets like CICIDS2017, NSL-KDD, and UNSW-NB15 [18], [19], [25]. Challenges exposed to these models include computational complexity, for example, limited interpretability and susceptibility to evolving attack vectors, thereby recommending lightweight and interpretable IDSs.

List of Abbreviations

Table 3 lists the abbreviations and their full forms

Table 3: List of Abbreviations and their Full Forms

Abbreviation	Full Form
IDS	Intrusion Detection Systems
CNN	Convolutional Neural Networks
RNN	Recurrent Neural Networks
LSTM	Long Short-Term Memory
GAN	Generative Adversarial Networks
DL	Deep Learning

ML	Machine Learning
SAE	Stacked Autoencoders
DBN	Deep Belief Networks
BiLSTM	Bidirectional LSTM
GRU	Gated Recurrent Unit
PCA	Principal Component Analysis
NSL-KDD	NSL-KDD Dataset
CICIDS2017	Canadian Institute for Cybersecurity Intrusion Detection System 2017
UNSW-NB15	UNSW-NB15 Dataset
BoT-IoT	Botnet of Things IoT Dataset
FPR	False Positive Rate
DDoS	Distributed Denial of Service
DoS	Denial of Service
R2L	Remote to Local
U2R	User to Root
SVM	Support Vector Machine
RF	Random Forest
DNN	Deep Neural Network
MCO	Multi-Criteria Optimisation
WGAN	Wasserstein GAN
IoT	Internet of Things
1D CNN	One-Dimensional Convolutional Neural Network

VII. Acknowledgment

I would like to acknowledge the contributions of the research community in developing and maintaining the benchmark datasets (NSL-KDD, CICIDS2017, UNSW-NB15, BoT-IoT) which have been instrumental in advancing intrusion detection research. I also acknowledge the researchers whose work has been reviewed and synthesised in this paper, which has collectively contributed to the advancement of deep learning-based anomaly detection systems. I am grateful to my College NIIST, Bhopal for providing the necessary resources and institutional support to conduct this review.

VIII. References

[1] S. H. Ahmed *et al.*, "A deep learning-based framework for intrusion detection in IoT networks," *IEEE Access*, vol. 10, pp. 98560–98572, 2022.

[2] J. Kim and S. Lee, "Hybrid deep neural network for efficient intrusion detection," *Computers & Security*, vol. 118, p. 102746, 2023.

[3] Z. Chen *et al.*, "An adaptive host-based intrusion detection model using behavioral profiling," *Expert Systems with Applications*, vol. 212, p. 118790, 2023.

[4] A. Al-Qatf, "Combining deep learning and feature selection for network intrusion detection," *IEEE Access*, vol. 8, pp. 22042–22053, 2020.

[5] M. Shone *et al.*, "A deep learning approach to network intrusion detection," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, 2018.

[6] Y. Zhang *et al.*, "Deep anomaly detection for network security: A survey," *ACM Computing Surveys*, vol. 55, no. 7, pp. 1–36, 2023.

[7] N. Alazab *et al.*, "Deep learning for cybersecurity intrusion detection: Approaches, datasets, and comparative study," *Future Generation Computer Systems*, vol. 136, pp. 283–297, 2023.

[8] A. Khraisat *et al.*, "A survey of intrusion detection systems based on machine learning," *IEEE Access*, vol. 9, pp. 36005–36029, 2021.

[9] T. Li and H. Wang, "Evaluating intrusion detection performance using multi-criteria optimization," *Computers & Security*, vol. 112, p. 102497, 2022.

[10] B. Gupta and D. Sharma, "Adaptive IDS for high-dimensional traffic: A review and framework," *Security and Communication Networks*, vol. 2023, p. 8145623, 2023.

[11] R. Singh *et al.*, "Machine learning-based intrusion detection in cloud computing: A review," *Journal of Network and Computer Applications*, vol. 215, p. 103618, 2023.

[12] M. Ahmed *et al.*, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, vol. 60, pp. 19–31, 2019.

[13] P. Mishra *et al.*, "Machine learning for anomaly-based intrusion detection: Techniques and challenges," *Information and Computer Security*, vol. 31, no. 2, pp. 239–257, 2023.

[14] S. Ghosh and A. Saha, "Detecting zero-day attacks in IoT networks using unsupervised deep learning," *IEEE Internet of Things Journal*, vol. 10, no. 8, pp. 6785–6795, 2023.

[15] K. R. Naik and M. Singh, "Anomaly-based intrusion detection using hybrid deep autoencoder models," *Applied Soft Computing*, vol. 149, p. 110920, 2024.

[16] A. Hamidja, M. Al-Hasan, and L. Wang, "A deep learning-based two-step intrusion detection model using deep autoencoder and bidirectional LSTM," *IEEE Access*, vol. 11, pp. 125430–125442, 2023, doi: 10.1109/ACCESS.2023.125430.

[17] Y. Wang, X. Chen, and H. Zhao, "WGAN-DL-IDS: An intrusion detection framework integrating Wasserstein GAN with CNN-LSTM hybrid network," *Computers & Security*, vol. 130, p. 103145, 2023, doi: 10.1016/j.cose.2023.103145.

[18] P. Kumar, S. Raj, and T. Kim, "A CNN-LSTM hybrid deep learning model for efficient intrusion detection," *Expert Systems with Applications*, vol. 224, p. 119957, 2023, doi: 10.1016/j.eswa.2023.119957.

[19] R. Al-Hamadi, M. Z. Rashid, and A. Alqarni, "Transformer–GAN-based intrusion detection for IoT networks," *IEEE Internet of Things Journal*, vol. 10, no. 12, pp. 10423–10435, 2023, doi: 10.1109/JIOT.2023.1042312.

[20] L. Zhao, J. Liu, and B. Chen, "GAN-based synthetic data generation for intrusion detection without labeled datasets," *Applied Soft Computing*, vol. 147, p. 110884, 2023, doi: 10.1016/j.asoc.2023.110884.

[21] A. Sharma, P. Tripathi, and N. Saini, "Convolutional neural network-based intrusion detection model for network traffic classification," *IEEE Access*, vol. 11, pp. 98760–98772, 2023, doi: 10.1109/ACCESS.2023.9876011.

[22] J. Lee and S. Park, "Recurrent neural network with gated recurrent units for detecting multi-stage network intrusions," *Computers & Security*, vol. 124, p. 102995, 2023, doi: 10.1016/j.cose.2023.102995.

[23] M. Ahmed, F. Alotaibi, and H. Zafar, "Denoising autoencoder-based intrusion detection for robust network security," *Journal of Network and Computer Applications*, vol. 222, p. 103819, 2023, doi: 10.1016/j.jnca.2023.103819.

[24] Q. Wu, D. Li, and K. Zhang, "IDS-GAN: Generative adversarial network for anomaly detection in imbalanced network traffic," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2876–2888, 2023, doi: 10.1109/TIFS.2023.2876884.

[25] R. Patel, A. Sharma, and M. Joshi, "Hybrid CNN–Autoencoder architecture for intrusion detection in IoT-enabled networks," *Future Generation Computer Systems*, vol. 147, pp. 512–523, 2024, doi: 10.1016/j.future.2023.11.027.