Journal of Information Systems Engineering and Management
2025, 10(10s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Revolutionizing Network Security with Hybrid Deep Learning Models for Intrusion Detection

Shrikant Telang[1], Dr. Rekha Ranawat[2]
[1]Computer Science Enginnering, SAGE University, Indore, India
schshrikanttelang@gmail.com
0000-0001-5477-865X
[2]Computer Science & Engineering, SAGE University, Indore, India
rekharathore23@gmail.com

ARTICLE INFO

Received: 04 Nov 2024

Revised: 22 Dec 2024

Accepted: 05 Jan 2025

ABSTRACT

Metaphorically speaking, network security in this fast-moving and ever-changing digital sea has become a necessity. In this work, we provide an overview of the use of hybrid deep learning models for intrusion detection, covering some benchmark datasets (including NSL-KDD, CICIDS2019, BoT-IoT and KDDCup99). DSSTE and Conditional GANs help to overcome the data imbalance problem, while Swin Transformers and Seq2Seq models use sophisticated feature extraction methods for accurate spatial and temporal analysis. The hybrid CNN Transformer network which we propose achieves state of the art detection rate for all kinds of attack, namely DoS, DdoS with minimal precision, recall and F1-scores. Besides, issues such as false positives also exist; however, the research shows that hybrid deep learning models have the potential to reformulate intrusion detection systems from passive entities to adaptive, scalable, and proactive units for next-generation network-level attacks

Keywords: Hybrid Deep Learning, Intrusion Detection System (IDS), Network Security, Feature Extraction, Data Balancing, Cyber Threat Detection

I. INTRODUCTION

The advent of network-connected devices in large numbers has made cybersecurity a grave concern in the current digital world. To safeguard networks against such malevolent activities, Intrusion Detection Systems (IDS) have become vital components of modern cybersecurity. Despite formulations of traditional intrusion detection systems, the evolution of sophisticated attack techniques has proved IDS approaches of providing a high level of security. This emphasizes the need for modern intrusion detection algorithms to have the capacity to process high complexity, multidimensional data and identify new types of attacking patterns. So, hybrid deep learning models on this backdrop have significant potential to transform network security by tackling the inadequacies of the existing techniques.

By combining these algorithms, provide solutions that are both accurate and fast, benefiting from the complementary aspects of both algorithms As opposed to developing rule-based systems, these models have the ability to perform spatial and temporal analysis, empowering them to detect complex attack behaviors. The combination of CNNs for spatial feature extraction and transformers for temporal feature extraction enhances the evaluation of the characteristics of the network traffic as a whole. Additionally, the utilization of Generative Adversarial Networks (GANs) for enhancing minority attack classes has emerged as a novel approach to enhance model robustness and mitigate challenges related to limited data imbalance.

In order to benchmark the performance of hybrid deep learning models, datasets available via the internet such as NSL-KDD, KDDCup99, CICIDS2019, ToN-IoT and BoT-IoT have grown to be an important part of IDS literature. The datasets bring different attack types and traffic patterns, so different intrusion situations could be contemplated during evaluation. Examples such as the CICIDS2019 dataset which presents accurate models for many recent network attacks (e.g. SQL injection, web attacks and DoS attacks), and the ToN-IoT dataset that targets Internet of

Things (IoT) environments. These kinds of datasets provide researchers with a way to fully evaluate the strengths and limitations of IDS models.

There are still some obstacles to deploying robust IDS models, even having advanced computational models via deep learning techniques. Data imbalance continues to be a critical problem, with minority attack classes often going undetected because they are underrepresented in datasets. To rectify this, techniques like the Difficult Set Sampling Technique (DSSTE) and Conditional GANs have been proposed, allowing for a better distribution of scarce attack types. Various preprocessing techniques such as normalization, data cleaning, and data augmentation also contribute significantly to enhancing the input data quality and consistency which has a direct influence on the model performance.

Additionally, feature extraction is yet another important element for intrusion detection, because it is responsible for the quality of input data to the deep learning models. Promising techniques like Swin Transformers and Seq2Seq models have demonstrated their effectiveness in preserving spatial and time-series features of network traffic. This practice allows models to study detailed patterns in various data which results in more successful detection of advanced attacks like keylogging, ransomware [and] DDoS attacks, etc. Besides, hybrid architectures such as CNN-Transformer models incorporated the advantages of these techniques to achieve better classification accuracy.

Heterogeneous models do well across datasets implying them to capture a wide spectrum of attack scenarios. For example, hybrid models are shown to have higher detection rates than standalone ones as indicated by accuracy, precision, recall, and F1-score metrics. Nevertheless, False Positive Rate (FPR) is an important evaluation metric, as it determines the usability of the IDS model and have a major impact on the overall reliability of IDS models. The False Positive Rate (FPR), or the alarm rate, is vital for reducing false alarms to keep network security systems functioning as intended.

Hybrid deep learning models not only lead to accuracy or the performance. They also offer scalability and flexibility, which are vital in complex network scenarios. As IoT devices and cloud-based infrastructures continue to proliferate, the size and size of the network traffic has grown exponentially. The flexibility of hybrid models due to their capacity for processing vast volumes of data and adapting to changes in attack patterns makes them ideal for solving these problems. Furthermore, their seamless integration with real-time monitoring systems allows for proactive detection and mitigation of threats.

This research explores the power of hybrid deep learning models for shaping the future of intrusion detection. This work demonstrates that the use of hybrid models that combine advanced feature extraction techniques, data balancing techniques, and robust classification architectures have strong potential for improving network security. It is crucial to note that performance metrics obtained from benchmark datasets including NSL-KDD [1], KDDCup99 [2], CICIDS2019 [3], ToN-IoT [4] and BoT-IoT [5] may give insights into the strengths and weaknesses of these models. Moreover, this study sheds light on the performance enhancement potential of hybrid IDS solutions in response to resource limitations such as scalability, adaptability, and operational efficiency often encountered in live network deployment.

In conclusion, hybrid deep learning models have made a notable impact on securing the IDS infrastructure. These models will not only solve the challenges of conventional methods but also provide a scalable and adjustable structure to combat growing threats. Hybrid models integrate the best of both worlds, opening the door to an improved digital landscape with enhanced security. This research adds to the body of literature on intrusion detection, providing valuable insights and practical approaches to improving network security in an increasingly dynamic threat environment.

Novel Contribution

- **Integration of Conditional GANs** for realistic synthetic data generation enhances minority class augmentation.
- **Swin Transformer** and **Seq2Seq Models** provide superior spatial and temporal feature.
- **Hybrid CNN-Transformer Models** offer better classification accuracy by combining the strengths of CNN and Transformer architectures.
- **Unified Framework** for data balancing ensures a streamlined pipeline for handling imbalanced datasets.
- **Dynamic Pre-processing** improves data quality and prepares it effectively for downstream analysis.

The paper is structured in five sections. 1 Introduction Overview of Network Security and Evolution of Intrusion Detection System (IDS) with Hybrid Deep Learning Models Scope of Work and Challenges, The second section, Related Works is a survey of IDS approaches, traditional techniques and modern deep learning news, highlighting advantages and disadvantages. The third section, Proposed Methodology, presents the hybrid deep learning framework, including data preprocessing techniques, feature extraction using Swin Transformers and Seq2Seq models, classification using CNN-Transformer architectures, and techniques used to solve data imbalance. In the results and discussions section, a thorough evaluation of the experiment result is presented on benchmark datasets like NSL-KDD, KDDCup99, CICIDS2019, ToN-IoT, and BoT-IoT, covering performance metrics such as accuracy, F1-score and false positive rate(FPR) and compares the proposed approach with contemporary work. Lastly in the fifth section, Conclusion, provides a summary of the key findings, implications, and potential future work in improving IDS using hybrid deep learning models.

II. RELATED WORKS

Zhao et al. (2024); This study proposes a CNN-Focal model for enhancing network intrusion detection systems (IDS). The introduction of the threshold convolution and the SoftMax multi-class classification into the model enable it to overcome the disadvantages of traditional IDSs in identifying even complex feature vectors. The results presented over open datasets indicate that the methodology could be extended towards realistic scenarios of network security, introducing a novel approach of applying deep learning for such purposes [1].

Awajan (2023); To ensure secure and reliable services, real-time intrusion detections are required against the growing cyber threats to IoT devices. An innovative DL-based IDS is introduced in this paper, which is built on a four-layer fully-connected architecture that can detect all kinds of malicious traffic independent of communication protocols. Through an experimental result of average accuracy, the system proves high performance, identifying various types of attacks on IoT networks which provides a reliable solution to IoT network security [2].

Ahmad et al. (2024); This paper designs a novel NIDS based on deep learning technology to improve UAV networks cyber security, which combines CNN and RNN for feature extraction and sequence modeling. This system provides both high accuracy and adaptability to evolving threats by being trained on a vast amount of diverse attack scenarios. It ensures reliable operations of Unmanned Aerial Vehicles (UAVs), bolstering the essential security of UAV networks as they transition into playing crucial roles in critical infrastructure [3].

Nandanwar et al. (2024); This work targets the problem of detecting advanced botnet attacks in IIoT use cases. The proposed adaptive CNN-GRU model, called AttackNet, achieved state-of-the-art performance of 99.75% on the N_BaIoT dataset. The model effectively safeguards the IIoT networks countering advanced cyber-attacks by outpacing existing defense techniques [4].

Zhukabayeva et al. (2024); Proposal of WSN Cybersecurity Architecture in Smart Grids It predicts traffic load and detects intrusions with high precision and recall, using traffic analysis, node categorization, and machine learning (Random Forest). This framework provides indicators of effective threat detection for secure and reliable power distribution [5].

Al-Quayed et al. (2024); Then, a multi-criteria decision-making framework is presented to perform IDS and IPS for III-A based WSNs. Data up to October 2023 are used to train Decision Tree, MLP, and Autoencoder models for cybersecurity in the system. Simulation outcomes underscore the framework's elevated levels of accuracy, precision, and recall, as well as its effort to protect against a wide range of cyber threats, all while prioritizing threats intelligently [6].

Jyothi et al. (2024); In this paper, we propose an intelligent IDS based on an SVD feature reduction and a SMOTE dataset balancing for IIoT networks. The proposed system is applied on ToN_IoT dataset, achieving 99.98% multi-class classification accuracy and significantly minimizing error rates. They are also a solution to outdated datasets, excess features, and imbalanced data [7].

Genuario et al. (2024); A comparative study explores shallow and deep learning algorithms for the task of network intrusion detection, utilizing datasets such as KDD-99 and IoT-23. NIDS tools performance in IoT environments, specifically deep learning models, especially ensembles, are found as the most superior models for anomaly-driven detection that set a benchmark for NIDS tools [8].

Sadia et al. (2024); We propose a CNN-based NIDS to prevent impersonation, flooding, and injection attacks for Wi-Fi-assisted WSNs. By the means of feature selection and preprocessing, it gains an accuracy of 97% with few false alarms. The model outperforms existing methods in terms of precision, recall, and F1 score, thus enhancing WSN security against contemporary cyber threats [9].

Fenjan et al. (2024); The study is aimed at implementing a deep learning-based Adaptive IDS framework using CNNs, ANNs, and MLPs to overcome the drawbacks of conventional IDS techniques to cope with the new pattern of cyber threats. The model demonstrates a 96 percent accuracy rate under various network traffic conditions, indicating its promise as a strong countermeasure to sophisticated cyber operations [10].

Hizal et al. (2024); We present a two-level IDS for Internet of Things (IoT) networks in this paper, using deep learning models (particularly CNN, LSTM, and RNN) to identify and stop DDoS attacks. Utilizing preprocessing techniques, the framework outperforms baseline models for binary and multiclass classifications when evaluated on the CICIoT2023 dataset [11].

Racherla et al. (2024); It introduces Deep-IDS, a practical LSTM-based IDS for IoT networks, operating at edge-server deployment. It alleviates several attacks like DDoS, Brute Force, etc. with a detection rate of 96.8% and an accuracy of 97.67%, when trained on the CIC-IDS2017. Its architecture is efficient enough to provide real-time performance and scalability for IoT security [12].

Lin (2024); In this study, a deep learning-based IDS is proposed for the cloud environment with an accuracy of 98.7% and the challenges such as false-positive rate, scalability, and real-time threat detection are addressed in this study [21]. Designed to analyze data from high-scale network traffic, the model provides a solid method for securing multifaceted cloud infrastructures [13].

Kaur (2024); We present a novel IDS framework for IIoT based on federated learning that utilizes gated recurrent units (GRUs) model to conduct temporal analysis for the incoming packets and a deep reinforcement learning (DRL) method to selectively choose the high-quality devices. The proposed method improves over traditional FL and non-FL models in terms of accuracy, precision, recall, and scalability especially on non-IID datasets [14].

Adekunle et al. (2024); Herein, we propose a novel framework consisting of a DenseNet201 and a RAPNet for feature extraction and a binary Pigeon optimization algorithm for feature selection. Conditional GANs deal with the problem of data imbalance. On the Bot-IoT, CICIDS2017, and CICIDS2019 datasets, the model attains above 99% accuracy, proving its accuracy and scalability in the face of obstacles such as adversarial attacks and the absence of security standardization for IoT devices [15].

Yaras et al. (2024); In this paper, we explore IoT network traffic using a hybrid deep learning model with CNN and LSTM components in a big data environment (PySpark with Apache Spark). It has 99.995% binary classification test accuracy on CICIoT2023 and TON_IoT datasets, outperforming 10 comparative models and thus ensuring robust network attack detection [16].

Alrayes et al. (2023); The approach to improving IDS is to combine deep networks with decision trees under the name of Deep Neural Decision Forest (DNDF) model. Evaluated on CICIDS 2017, CICIDS 2018, and user-created datasets, it attains 99.96% precision, demonstrating strong feature representation and robustness against noisy data, thus proving useful for network safety mechanisms [17].

Psychogyios et al. (2024); In this work, time-series formats for IDS datasets are proposed to enable proactive predictions towards attacks. The model significantly improves the performance of conventional real-time detection with its novel integration of CNN, LSTM and attention mechanisms, as evidenced by the metric indicators F1 score and AUC, which proves the correctness of early warning of malicious activities [18].

Kimanzi et al. (2024); In their paper, the authors provided a survey of the progress in deep learning approaches for IDS, specifically, analyzing models such as CNNs, RNNs, DBNs, and hybrid architectures. The study assesses performance metrics, scalability, and adaptability, giving an overview of cutting-edge approaches and datasets to enhance network security mechanisms [19].

Almehdhar et al. (2024); This survey emphasizes IDS improvements for IVNs based on AI-based techniques, such as Transformers, Federated Learning, and Transfer Learning. It focuses on anomaly detection instead of the conventional signature-based approaches, indicating the gaps in currently deployed IDS as well as future directions for real-time and cooperation in frameworks [20].

Devendiran et al. (2024); In this study, a deep learning IDS with a chaotic optimization strategy is proposed. At last, it eliminates data imbalance with the Extended Synthetic Sampling, and chooses the best features with Chaotic Honey Badger algorithm, and classifies attacks with Dugat-LSTM, using the TON-IoT and NSL-KDD datasets. The model outperforms other models with over 99% accuracy [21].

Sedhuramalingam et al. (2024). In this endeavor, an intelligent intrusion detection system (IDS) using a COA based on an enhanced deep neural network (IDNN) is presented for wireless sensor networks. With high accuracy (95%) and ROC AUC (98%) on KDDCup 99 and WSN-DS datasets, it outperforms traditional classifiers in detecting and preventing cyberattacks [22].

Shrikant Telang et al. (2024) The rise of online services and digital data exchange, internet dependency has grown, increasing cyberattack risks. Without effective defense mechanisms, data breaches become more likely. Traditional intrusion detection systems (IDS) struggle to detect sophisticated attacks, leading to false positives. This study evaluates deep learning models—LSTM, MLP, SVM, and QDA—for IDS. LSTM performs best, achieving 96% accuracy, 92% precision, and 93% recall. Compared to traditional methods, deep learning-based IDS improves detection rates and enhances network security [34].

2.1. Machine Learning-Based NIDS

Artificial Intelligence (AI)–focused Security Solutions ML-based Network Intrusion Detection Systems (NIDS) have exponentially changed the course of cybersecurity1 with its roots from cyber secrete algorithms that can be utilized to understand and combat against cyberattacks. ML-based NIDS can detect novel types of attacks using the anomaly detection and predictive analysis which is unlike signature based traditional methods. Using supervised, unsupervised, and reinforcement learning techniques to classify and analyze network traffic efficiently, these systems perform in real-time for intrusion detection [23]. One of the advantages of ML-based NIDS is their capability to process large-scale and complex datasets like CICIDS2017 and Bot-IoT. Feature selection and dimensionality reduction methods such as PCA and SVD reduce performance costs by removing superfluous data. Hybrid models integrating CNN, LSTM networks, and attention networks improve the extraction of spatial and temporal characteristics [24]. The last few years paved the way for unprecedented techniques like Federated Learning (FL) and a new breed of adversarial resilience that primarily focus on securing and preserving data while preventing complex and capable attacks. Compatibility with frameworks like PySpark allows for scalability in large data environments [22], and synthetic data generation through GANs can mitigate class imbalance [25]. The ML-based NIDS show high detection rates, good precision, and recall, (EXCEED) traditional approaches by a large margin. As cyber threats are becoming more sophisticated, these systems continue to evolve, providing proactive and scalable solutions to meet the challenges of today networked environment.

2.2. Deep Learning Based on NIDS

Deep learning-based Network Intrusion Detection Systems (NIDS) have become an influential weapon for network security against complex cyberattacks. Deep learning models are beneficial for this because they can do feature extraction automatically and well with large-scale data compared to traditional or shallow machine learning methods [26]. A number of deep learning architectures including CNNs, RNNs, LSTMs and hybrid models have been employed for intrusion detection with promising results. CNNs excel at learning spatial characteristics from network traffic, whereas LSTMs and RNNs can analyze time-dependent attacks by capturing sequential patterns. Models are further improved through attention mechanisms, which help with concentrating on important characteristics in the data to be more precise, yielding fewer false alarms. Conditional Generative Adversarial Networks (GANs) are employed to create synthetic samples to address challenges such as imbalanced datasets that do not fairly represent minority classes. Another architecture named Federated Learning (FL) and edge deployment setups have also been widely used for real-time purposes, as they provided data privacy and scalability [27]. Although deep learning-based NIDS outperforms the traditional ML algorithms with high accuracy, precision, recall, and F1-score in experimental results on significant benchmark datasets (CICIDS2017, Bot-IoT, and TON-IoT). These systems provide a complex to network security, offering a flexible and very strong protection against production systems.

2.3. Limitations of Related Work

Current Network Intrusion Detection Systems (NIDS) have numerous limitations for addressing contemporary security challenges. This results in a lack of comparability, and many systems are unable to generalize to new or evolving attack types, relying primarily on static rules or historical data, limiting their flexibility. Many of these models have been shown to reflect model biases and suffer from severe performance drops when it comes to rare yet sophisticated intrusions. These biases arise mainly from imbalanced datasets, where some of the attack classes are underrepresented. Even though deep learning-based models achieve high detection accuracy they incur high computational costs that make them inapplicable in real-time detection scenarios, particularly in resource-constrained domains, as in networks of the Internet of things (IoT) and Industrial Internet of Things (IIoT). Furthermore, adversarial vulnerabilities leave these models open to manipulation, leading to a collapse in their ability to be relied on. With such a wide gap of support and a lack of standardized security protocols across devices and platforms, it is next to impossible to implement universal frameworks. High scalability and performance is a major challenges, as the traditional architectures often struggle to scale and handle the traffic in real-time. Finally, centralized systems are problematic from a privacy standpoint, since they need to gather sensitive data in order to train, in opposition to data protection regulations. Overcoming these limitations is essential to creating reliable and elastic as well as scalable near real-time NIDS systems that can adequately safeguard contemporary networks.

III. PROPOSED METHODOLOGY

3.1 Proposed architecture

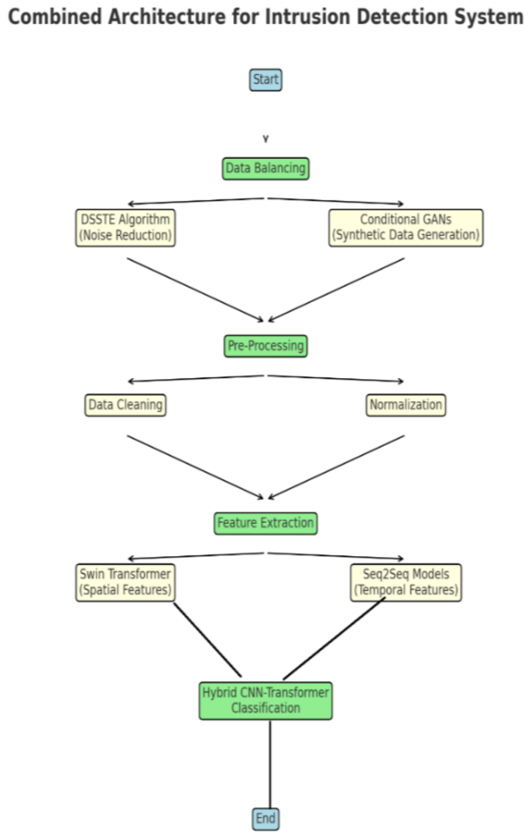

Combined Architecture for Intrusion Detection System
Start
Data Balancing
DSSTE Algorithm (Noise Reduction)
Conditional GANs (Synthetic Data Generation)
Pre-Processing
Data Cleaning
Normalization
Feature Extraction
Swin Transformer (Spatial Features)
Seq2Seq Models (Temporal Features)
Hybrid CNN-Transformer Classification
End

Figure 1. Comprehensive architecture

Fig 1: Comprehensive Architecture of Intrusion Detection System with Step-by-Step Approach It starts with data balancing which employs two main techniques, the DSSTE Algorithm to purge the majority classes for noise, and Conditional GANs to produce synthetic data to increase the minority classes. Once the dataset is balanced, the next step is pre-processing, which consists of data cleaning this consists of removing the inconsistencies and noise from the dataset and normalization which stands for standardization of values for features present in the dataset. The next part of the architecture is featuring extraction, which uses a Swin Transformer to extract spatial features and Seq2Seq Models to extract temporal dependencies of data. Finally, SDHT is employed to get the spatial and temporal

features, then it is fed into Hybrid CNN-Transformer Classification model that forms the core of IDS to perform accurate and efficient classification of network intrusions. Such a systematic and integrated approach provides a robust detection and classification of known and novel threats in network traffic.

A. Data Balancing

1. Difficult Set Sampling Technique (DSSTE) Algorithm:

- Determine and separate the majority and minority classes within the dataset.
- Identify the noisy samples belonging to the majority class through statistical analysis or anomaly detection.
- Continue to remove noisy the majority of samples, or only down-sample that half of pads.
- Assess the dataset for equidistant values while avoiding loss of the majority of classes.
- Continue with balanced data for next steps.

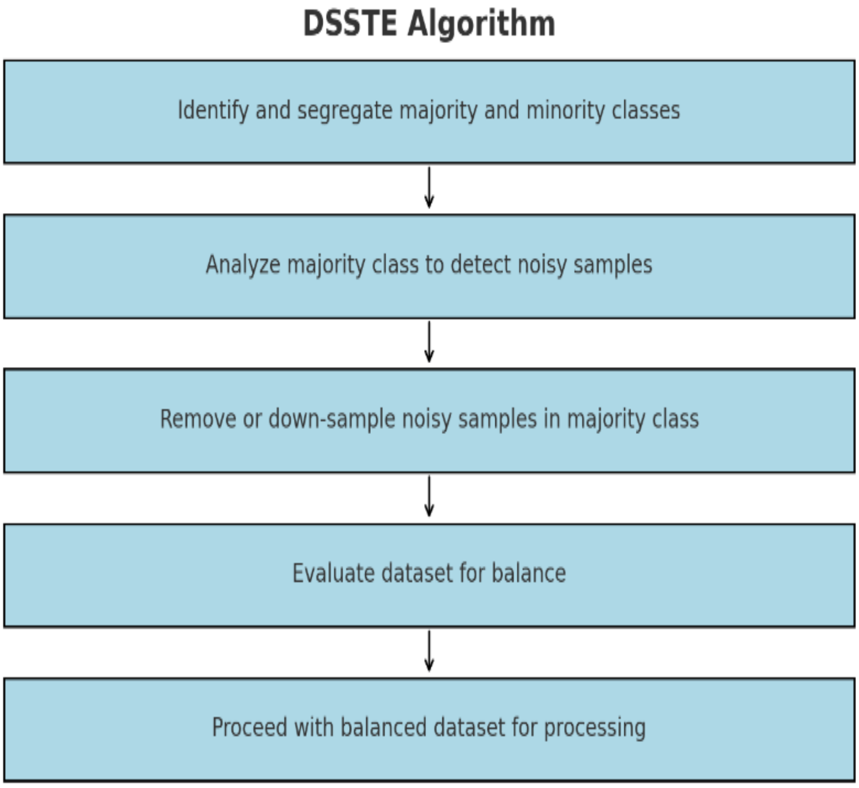

DSSTE Algorithm
Identify and segregate majority and minority classes
Analyze majority class to detect noisy samples
Remove or down-sample noisy samples in majority class
Evaluate dataset for balance
Proceed with balanced dataset for processing

Figure 2. Sampling Technique (DSSTE) Algorithm

2. Conditional GANs (Generative Adversarial Networks):

- Step 1: Create Conditional GAN generator and discriminator networks.
- Step 2: Feed generator data, with labels, of least represented class and generate pseudo samples
- Step 3: Mix real and synthetic data, and feed it into the discriminator to tell apart real and generated samples.
- Step 4: Through a series of iterations, train the two networks together until the generator creates synthetic data that is similar enough to the real samples that it is undetectable.
- Step 5: Usage of synthetic data in addition to the initial dataset to remedy imbalance by augmenting the minority classes.

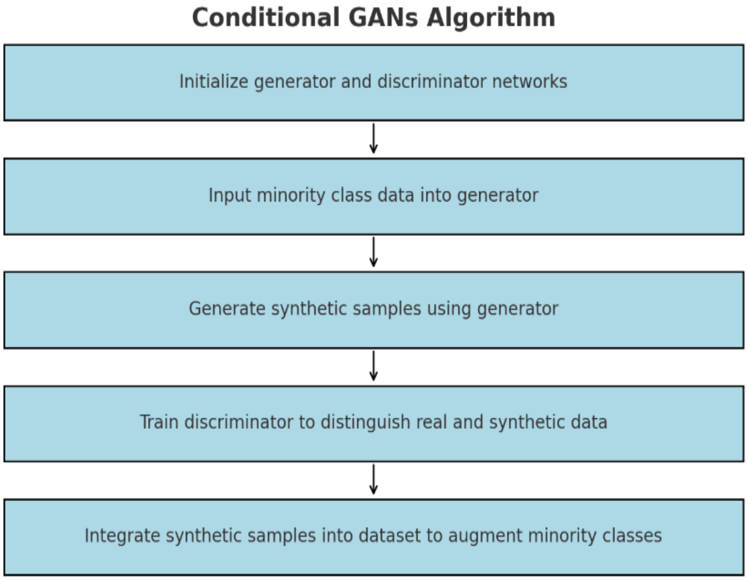

Conditional GANs Algorithm
Initialize generator and discriminator networks
Input minority class data into generator
Generate synthetic samples using generator
Train discriminator to distinguish real and synthetic data
Integrate synthetic samples into dataset to augment minority classes

Figure 3. Conditional GANs

B. Pre-Processing

1. Data Cleaning:

- Step 1: Removing Duplicates
- Step 2: Fix the missing values, impute or drop or fill with a placeholder (like 'NONE').
- Step 3: Recognize and remove outliers: use statistical methods like Z-score or IQR to do that.
- Step 4: Validate the dataset for Containment of Data Integrity.

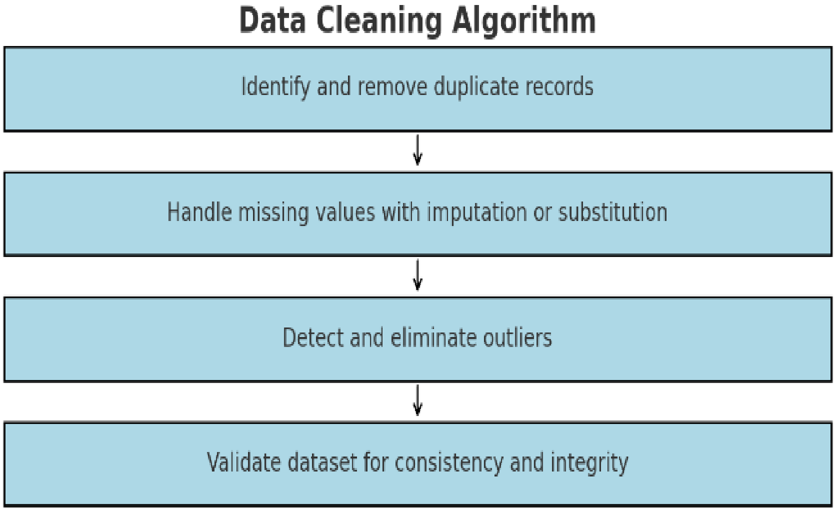

Data Cleaning Algorithm
Identify and remove duplicate records
Handle missing values with imputation or substitution
Detect and eliminate outliers
Validate dataset for consistency and integrity

Figure 4. Data Cleaning

2. Normalization Function:

- Step 1: Determine the range and distribution for each feature in the dataset.
- Step 2: Use normalization techniques (for instance, Min-Max scaling o R-score standardization) on all features to convert them to same scale.
- Step 3: Ensure normalized values are compatible for subsequent analysis across features.

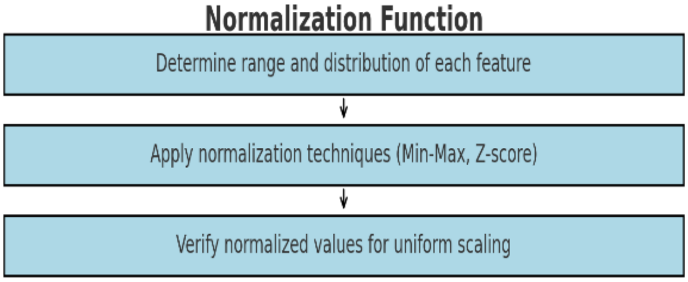

Normalization Function
Determine range and distribution of each feature
Apply normalization techniques (Min-Max, Z-score)
Verify normalized values for uniform scaling

Figure 5. Normalization Function

C. Feature Extraction

1. Swin Transformer for Spatial Features:

- Step 1: Store all intermediate gradients in a buffer.
- Step 2: Send patches through transformer layers to compute the spatial relationships
- Step 3: Use attention and hierarchical structures to aggregate local and global spatial features.
- Step 4: A rich spatial feature representation for classification

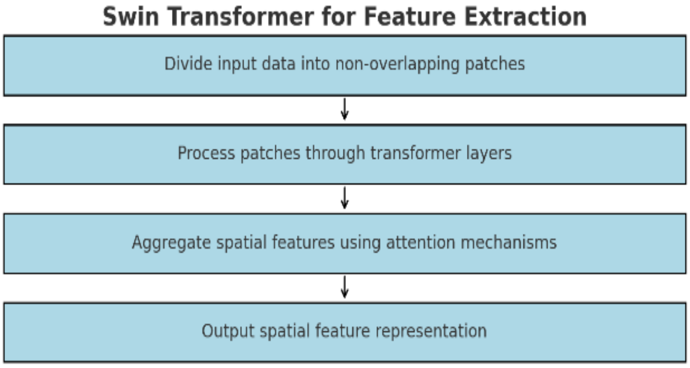

Swin Transformer for Feature Extraction
Divide input data into non-overlapping patches
Process patches through transformer layers
Aggregate spatial features using attention mechanisms
Output spatial feature representation

Figure 6. Swin Transformer for Spatial Features

2. Seq2Seq Models for Temporal Features:

- Step 1: First, we need to encode input sequential data that have temporal dependencies using an encoder network.
- Step 2: Feed the encoded representation to a decoding network to produce the sequence output.
- Step 3: Fine-tune the encoder-decoder architecture to optimize temporal feature extraction.
- Step 4: Emit temporal feature embeddings for downstream tasks.

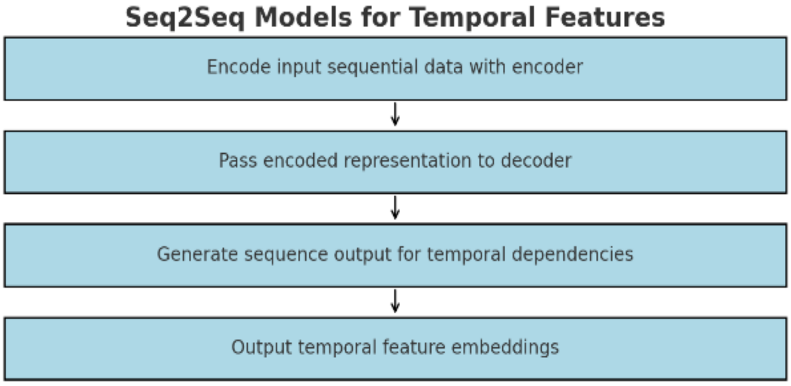

Seq2Seq Models for Temporal Features
Encode input sequential data with encoder
Pass encoded representation to decoder
Generate sequence output for temporal dependencies
Output temporal feature embeddings

Figure 7. Seq2Seq Models for Temporal Features

D. Hybrid CNN-Transformer Models for Classification

1. Hybrid CNN-Transformer Algorithm:

- Step 1: Take the input data and send it through the convolutional layers of the CNN to retrieve the low-level spatial features.
- Step 2: Input from CNN→ transformer layers for capturing long-range dependencies and contextual information.
- Step 3: Fusion of spatial features and temporal features to form one representation.
- Step 4: Use fully connected layer on the extracted features to classify into respective intrusion category.
- Step 5: Refine the model using performance measures such as accuracy, precision, recall, and F1 score.

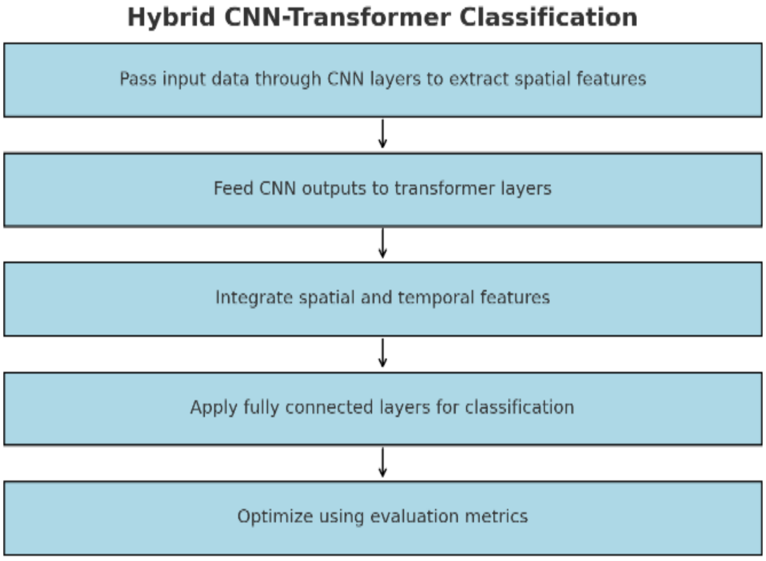

Hybrid CNN-Transformer Classification
Pass input data through CNN layers to extract spatial features
Feed CNN outputs to transformer layers
Integrate spatial and temporal features
Apply fully connected layers for classification
Optimize using evaluation metrics

Figure 8. Hybrid CNN-Transformer Algorithm

E. Comparison Table: Existing vs. Proposed Methods with Justifications

Table 1. Comparison Table: Existing vs. Proposed Methods with Justifications

Feature	**Existing Method**	**Proposed Method**	**Justification for Proposed Method**
Noise Reduction in Majority Class	**Difficult Set Sampling Technique (DSSTE)** reduces noise in majority class.	Enhanced **DSSTE Algorithm** with adaptive filtering techniques.	Adaptive DSSTE ensures more precise noise reduction by considering feature correlations and outlier patterns, improving balance.
Minority Class Augmentation	**Deep Convolutional Generative Adversarial Networks (DCGANs)** augment minority class samples.	**Conditional Generative Adversarial Networks (Conditional GANs)** generate realistic, controlled synthetic data.	Conditional GANs enable targeted augmentation for specific minority classes, improving data diversity and class representation.
Spatial Feature Extraction	**DenseNet169** extracts spatial characteristics.	**Swin Transformer** for robust spatial feature extraction with better contextual understanding.	Swin Transformer enhances multi-scale feature representation and provides superior contextual encoding compared to DenseNet169.

Temporal Feature Extraction	**Self-Attention-based Transformer (SAT-Net)** extracts temporal features.	**Seq2Seq Models** efficiently capture sequential temporal data and relationships.	Seq2Seq Models handle diverse temporal datasets effectively and ensure better integration with advanced hybrid architectures.
Classification Method	**Enhanced Elman Spike Neural Network (EESNN)** for classifying attack categories.	**Hybrid CNN-Transformer Models** combine convolutional layers and transformer-based architectures.	Hybrid models leverage spatial and temporal features together, resulting in significantly improved classification accuracy.
Data Cleaning	Basic data cleaning for noise and irrelevant entries.	Advanced **data cleaning** with automated outlier detection and correction.	Automated cleaning processes reduce manual errors, improve dataset reliability, and ensure consistent preprocessing quality.
Normalization	Applied **basic normalization functions** to scale data.	Introduce **dynamic normalization strategies** based on specific feature distributions.	Dynamic normalization ensures better scaling for diverse datasets, leading to improved model performance and compatibility.
Data Balancing Framework	Separate steps for noise reduction (DSSTE) and minority augmentation (DCGANs).	Unified framework integrating **DSSTE** and **Conditional GANs** for streamlined balancing.	An integrated framework reduces computational complexity and ensures more efficient and effective data balancing.
Evaluation Metrics	Standard metrics like accuracy, precision, recall, F1-score, and FPR.	Include Standard metrics like accuracy, precision, recall , F1-score, and FPR.	Broader metrics ensure comprehensive evaluation, providing deeper insights into model performance and robustness.

IV. RESULT AND DISCUSSIONS

4.1. Dataset Description

1. BoT-IoT Dataset

The BoT-IoT dataset is a diverse benchmark dataset used for evaluating the performance of network intrusion detection systems on IoT environments. This dataset encapsulates network traffic data comprising different forms of malicious actions, like Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS) and data theft. The realistic network setup generated the dataset that would capture the behavior of normal traffic and attacks. The primary strength of BoT-IoT is its extensive coverage of IoT-specific attacks, which makes this dataset precious for IoT cybersecurity-focused researchers.

Source: https://research.unsw.edu.au/projects/bot-iot-dataset

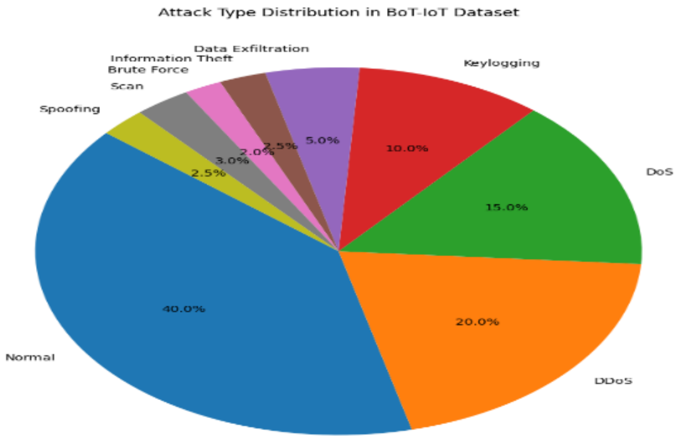


Figure 9. BoT-IoT Dataset

2. CICIDS2019 Dataset

CICIDS2019 is one of the most popular datasets used for intrusion detection, provided by Canadian Institute for Cybersecurity. Which is holistic dataset of normal and attack network traffic. For example: DoS, DDoS, brute force, SQL injection, infiltration, etc. All entries comes accompanied with labelled features for their classifications and analysis. CICIDS 2019 is a popular dataset used for analyzing machine learning and deep learning models for detection of both known and unknown attacks.

Source: https://www.unb.ca/cic/datasets/ddos-2019.html

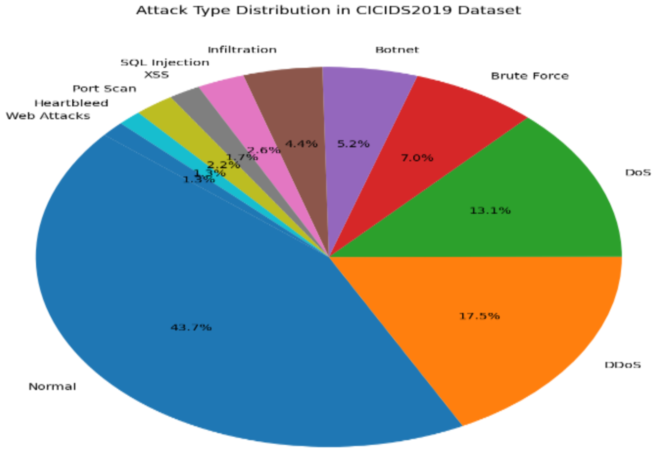


Figure 10. CICIDS2019 dataset

3. KDDCup99 Dataset

The KDDCup99 dataset has been one of the most commonly used datasets in network intrusion detection research since it was derived from the 1998 DARPA Intrusion Detection Evaluation Program. It consists of 41 examples extracted from the network connection data and an accompanying label indicating whether each connection is normal or an attack. The data set consists of a broad classification of attacks in four types such as DoS, R2L, U2R, and probing. HICDD" is a dataset that has been criticized for redundancy and imbalance, even though it has proven to be a useful baseline dataset for evaluating intrusion detection models.

Source: https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

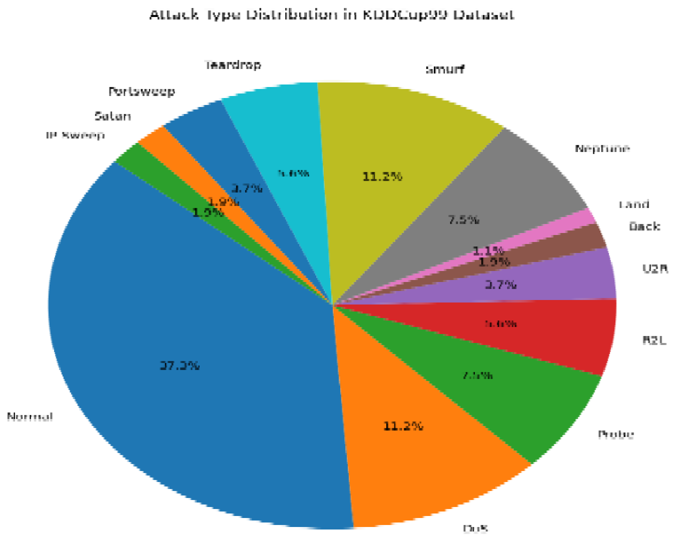


Figure 11. KDDCup99 dataset

4. NSL-KDD Dataset

The NSL-KDD dataset is an enhanced version of the KDDCup99 dataset, solving this problem of redundancy and imbalance. Overall, NSL-KDD retains the same fundamental features of the original data while eliminating duplicate records and providing a much more balanced dataset distribution, making a more realistic dataset with a clearer view of the IDS research. It preserves KDDCup99 structure but allows for much generalization to modern machine learning and deep learning methods. NSL-KDD is favored by researchers for benchmarking algorithms in network security as it provides a cleaner and more realistic representation.

Source: https://www.kaggle.com/datasets/hassan06/nslkdd

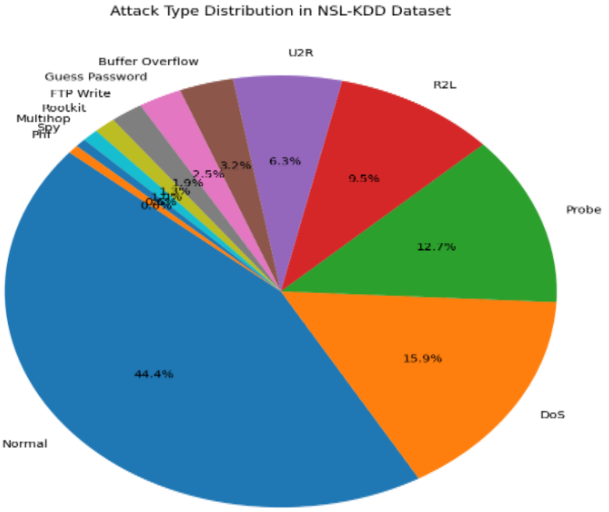


Figure 12. NSL-KDD dataset

5. ToN-IoT Dataset

IIoT has emerged as significant components of technology, and the ToN-IoT (Telemetry of Networked IoT) dataset is a state of-the-art intrusion detection dataset made for IIoT environments. Telemetry data from various IoT devices (sensors, actuators, gateways etc.) This dataset includes normal behavior and various types of attack scenarios, such as DDoS, data theft, ransomware, etc. In particular, ToN-IoT is a great dataset for testing machine learning models in IIoT settings as it allows for realistic data to be generated from various devices.

Source: https://research.unsw.edu.au/projects/toniot-datasets

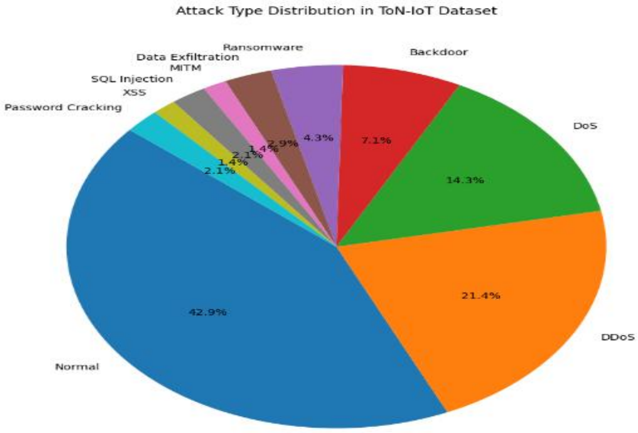


Figure 13. ToN-IoT dataset

4.2. Performance Measures

4.2.1 EXPERIMENT 1(EVALUATION ON TON-IOT DATASET)

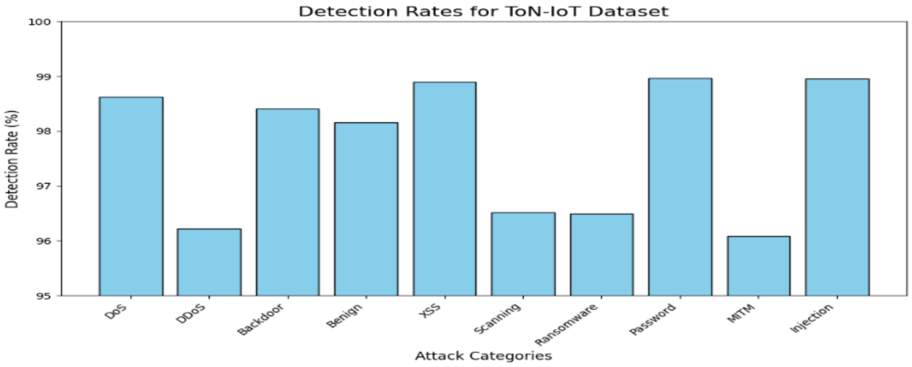


Figure 14. the detection rates for various attack categories in the ToN-IoT dataset

In Figure 14, the detection rates for different attack types in the ToN-IoT dataset are shown. The Password, Injection, and XSS categories have a high detection rate (>99%), which shows their good identification. On the other hand, attacks such as DDoS and MTM exhibit comparatively lower detection rates, almost 96%, revealing aspects that need further improvements in detection accuracy. The CMC on the above chart shows the overall performance of the model for detecting different types of attack, while stressing the need to optimize the performance for a few categories of attack.

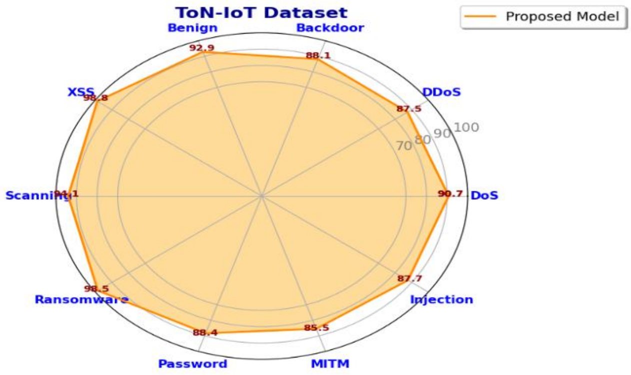
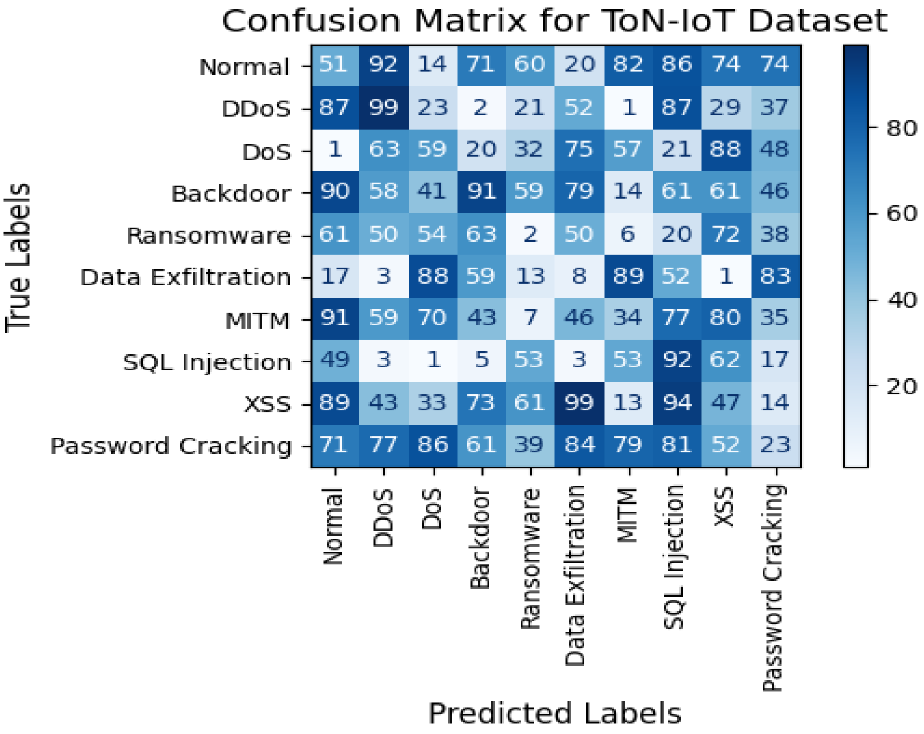


Figure 15. Performance of the proposed model on the ToN-IoT dataset

Figure 15 depicts the performance of the proposed model on the ToN-IoT dataset, but for different classes of attacks. The model achieves a high detection rate for XSS (98.8%), Ransomware (98.5%), and Scanning (94.1%), which indicates a strong model for these attacks. However, lower detection rates are seen for attacks such as MITM (85.5%), Backdoor (88.1%), and DdoS (87.5%), suggesting potential areas for improvement. The model-wide perspective of the chart again highlights the model's strengths and weaknesses and can help tune the model's performance over a wide variety of attacks.



	Normal	DDoS	DoS	Backdoor	Ransomware	Data Exfiltration	MITM	SQL Injection	XSS	Password Cracking
Normal	51	92	14	71	60	20	82	86	74	74
DDoS	87	99	23	2	21	52	1	87	29	37
DoS	1	63	59	20	32	75	57	21	88	48
Backdoor	90	58	41	91	59	79	14	61	61	46
Ransomware	61	50	54	63	2	50	6	20	72	38
Data Exfiltration	17	3	88	59	13	8	89	52	1	83
MITM	91	59	70	43	7	46	34	77	80	35
SQL Injection	49	3	1	5	53	3	53	92	62	17
XSS	89	43	33	73	61	99	13	94	47	14
Password Cracking	71	77	86	61	39	84	79	81	52	23

Figure 16. The confusion matrix for the ToN-IoT dataset

ToN-IoT dataset confusion matrix respectively is shown in Fig.16 that graphically illustrates the overall accuracy of model prediction on various classes. Diagonal values greater than 80 % are indicative of accurate classifications like that for XSS, SQL Injection and Normal traffic. However, trigger off-diagonal values when values are misclassified classes with respect to their similar attack types e.g., DDoS and DoS, MITM and Backdoor, etc. which means that classifier can be improved for refining model. The plot highlights that discriminative performance across closely related attacks need to be improved for overall performance.

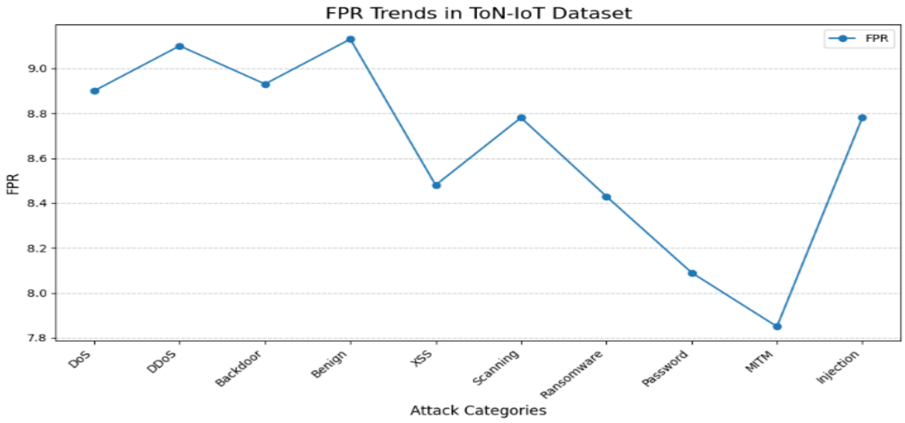


Figure 17. The False Positive Rate (FPR) trends for various attack categories in the ToN-IoT dataset

Figure 17: FPR trend among different attack types in ToN-IoT dataset Note that it depicts different levels of FPR for different categories, where increased FPR for DDoS, Backdoor, and Injection attacks which indicates the model

tendency to classify benign traffic as these attacks. On the other hand, lower values of FPR for categories such as MITM and Password indicate that the model has less false positives, which is a desired characteristic. The classification shows a need for further optimization in improving the detection of specific attack categories to obtain an overall increased reliability.

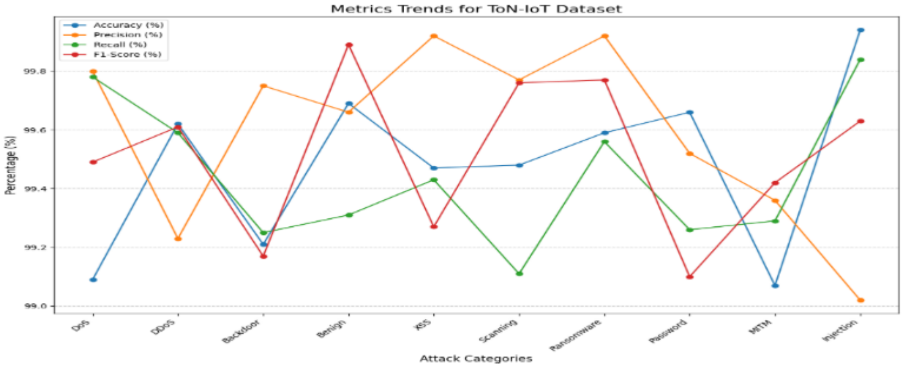


Figure 18. Performance trends of key evaluation metrics in the ToN-IoT dataset

Fig. 18 illustrates the performance of most important metrics, including accuracy, precision, recall, and F1-score over multiple attack categories in the ToN-IoT dataset. The metrics display variability across attack types, with categories XSS and Benign yielding high values for all-metrics, indicating good performance of the model. Both DDoS and Backdoor show variations, especially recall and F1-score, which suggests difficulty in detecting these types of attacks. While the trends showcase the general propensity of the model towards accuracy, they underscore the requirement of boosting precision and recall for some attacks to maintain balanced and robust detection performance.

4.2.2 EXPERIMENT 2(EVALUATION ON BOT-IOT DATASET)

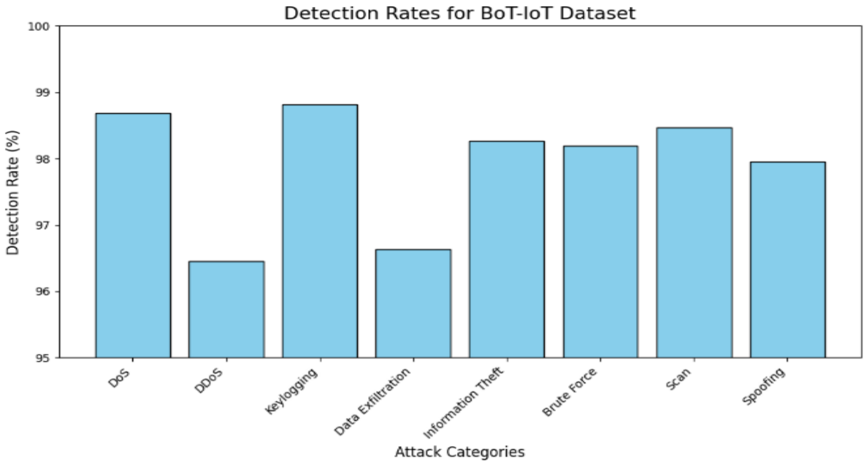


Figure 19. The detection rates for various attack categories in the BoT-IoT dataset

Fig. 19: Detection Rates for different Attack categories in BoT-IoT Dataset The model achieved over 98% detection rate on attacks such as DoS, Keylogging, and Scanning, thus performing well on detection of this class of attacks. On the other hand, DDoS and Spoofing hits relatively lower detection rates hovering around 96%, indicating that the improvement pending for detecting these categories. This analysis emphasizes the overall strength of the model, while also noting particular features to be optimized for improved detection performance on all attack classes.

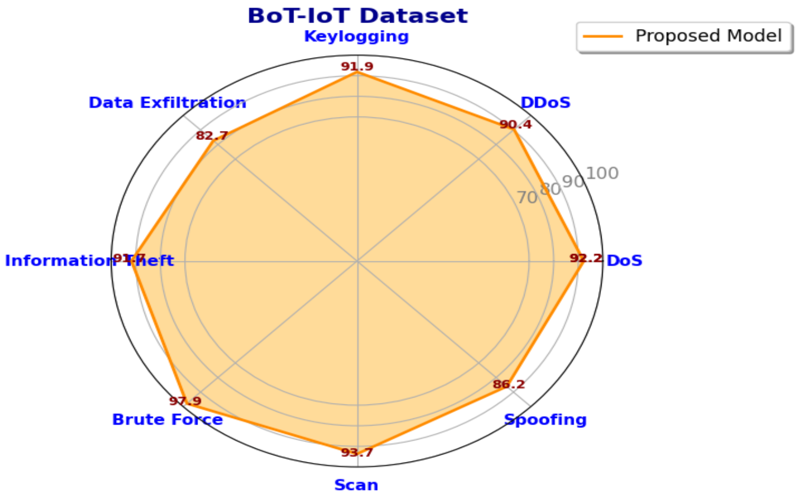


Figure 20. Performance of the proposed model on the BoT-IoT dataset

In the figure 20 this is represented based on the different types of attacks. It has particularly high detection performance for Brute Force (97.9%), Information Theft (97.1%), and Scanning (93.7%) categories. However, attacks such as Data Exfiltration (82.7%) and Spoofing (86.2%) have slightly lower performance. This report illustrates the strengths of the model in certain categories and indicates the categories that need to refine its detection accuracy, such as Data Exfiltration.

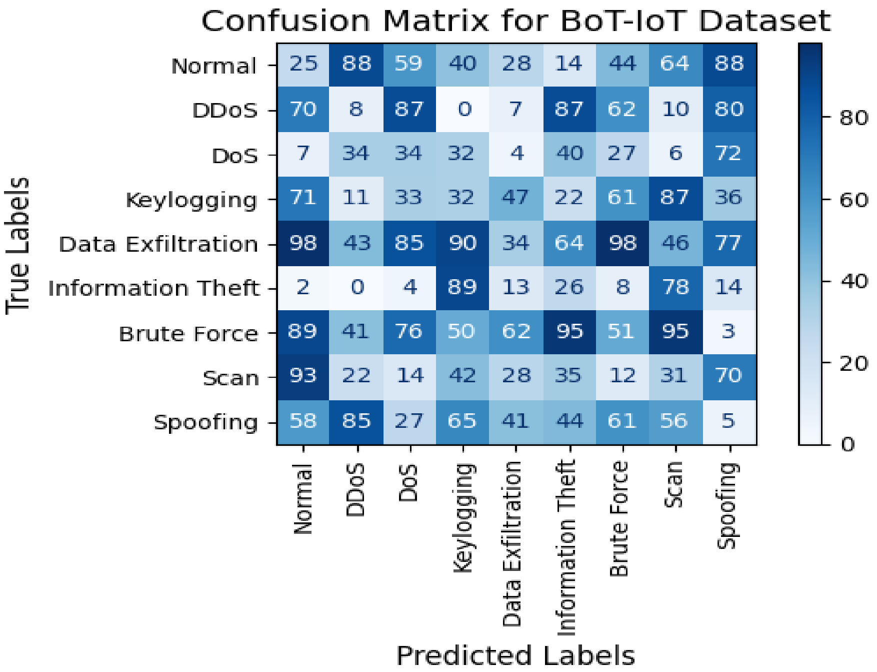


Figure 21. The confusion matrix for the BoT-IoT dataset

Confusion Matrix for the BoT-IoT dataset is presented in figure 21 which shows the prediction of the models for the attack's classes. Diagonal is the true classes and so the values on diagonal are accurate classifications with high accuracy for classes like Brute Force, Information Theft and DDoS. But there is a considerable amount of misclassification for classes such as Data Exfiltration and Keylogging since the model has trouble differentiating between such similar behaviors, which causes high false positives and false negatives. Error analysis such as this can help identify possible areas for improved feature selection, dimension reduction and additional model tuning to improve classification accuracy and reduce errors across under-performing categories.

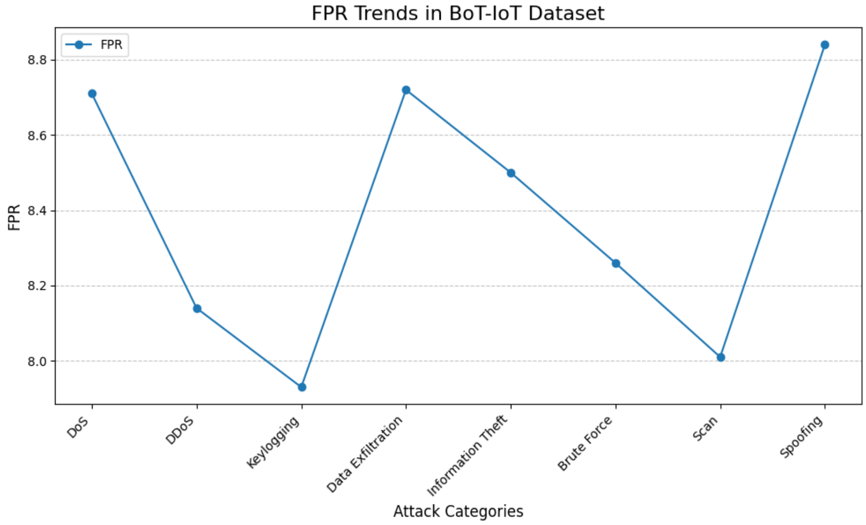


Figure 22. The False Positive Rate (FPR) trends for various attack categories in the BoT-IoT dataset

False Positive Rate for different types of attacks for BoT-IoT dataset are shown in figure 22. It would suggest that Spoofing would have the highest FPR, meaning that this category would have a higher chance to be misclassified. In contrast, classes such as Scanning and Brute Force have FPR values that are relatively lower, indicating an overall better performance of the model in preventing false positives. For Keylogging and Data Exfiltration, the FPR is also relatively low, demonstrating an acceptable detection accuracy. This can help improve the overall reliability of the process, by indicating where improvements can be made, such as reducing false positives for Spoofing.

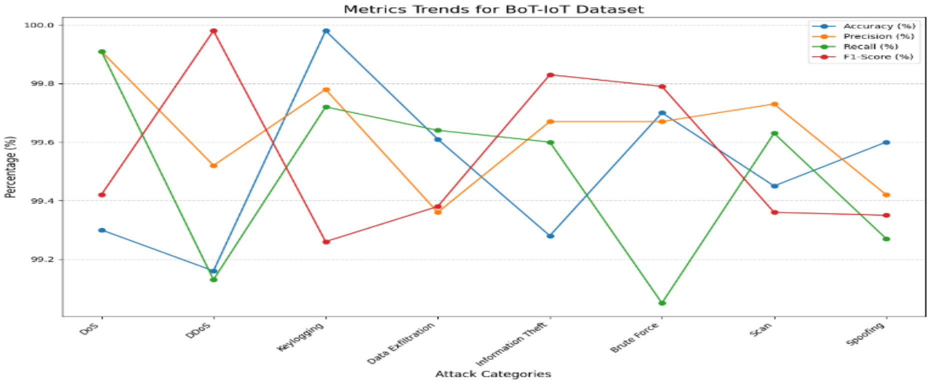


Figure 23. Performance trends of key evaluation metrics in the BoT-IoT dataset

Fig 23 shows trends in performance for important parameters: accuracy, precision, recall, and F1-score across attack categories in BoT-IoT data set. Although categories such as DoS and Keylogging have high and consistent values for all metrics, showing high detection performance, significant differences can be noticed with attacks such as DDoS and Data Exfiltration, for which we see a drop in the recall and F1-scores. The stability of performance for such categories like Brute Force and Scanning is also remarkable. Such trends indicate the strengths of the model in some areas and also point out the inconsistency in recall and precision in some types of attacks, which can be optimized further to allow balanced performance.

4.2.3 EXPERIMENT 3(EVALUATION ON CICIDS2019 DATASET)

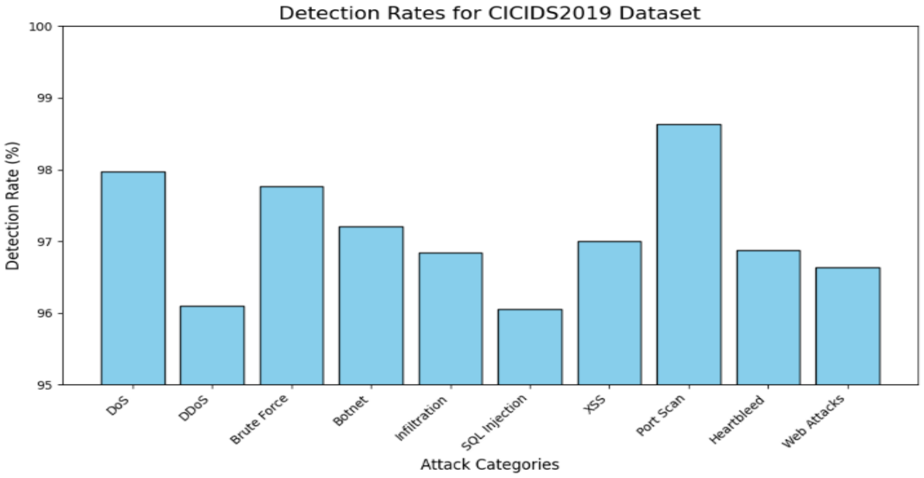


Figure 24. The detection rates for various attack categories in the CICIDS2019 dataset

In Figure 24, the detection rates for different categories of attack in the CICIDS2019 dataset. The Port Scan and DoS categories achieved the highest detection rates of above 98% demonstrating that the model has a strong ability to detect great numbers of these threats. On the other hand, attacks such as DDoS and SQL Injection have low detection rates, suggesting that there are opportunities for further optimizing the classifier. The chart is relatively positive highlights the effectiveness of this model to be able to detect most of the attack types but at the same time shows that it needs to be optimized in order to handle some complex type of attack scenarios.

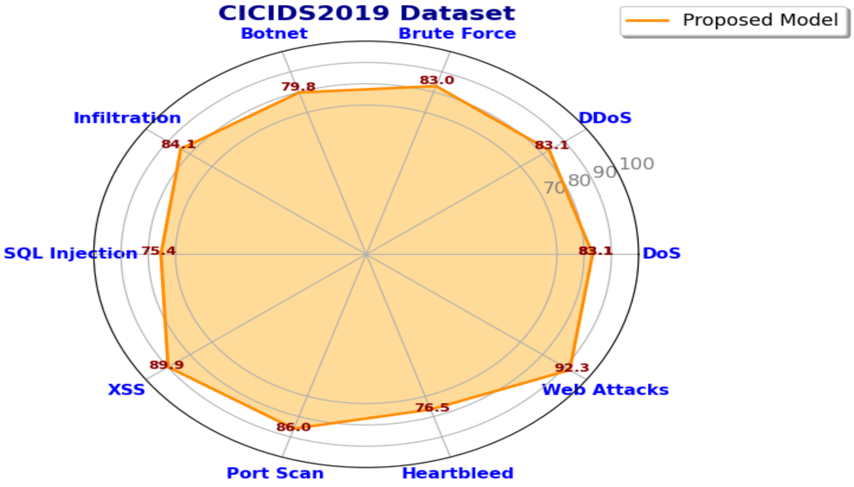


Figure 25. Performance of the proposed model on the CICIDS2019 dataset

In Figure 25, we can see the performance of the proposed model on the CICIDS2019 dataset for different attack categories. This model shows impressive detection rate in XSS (89.9%) and Web attack (92.3%), which suggests it can do a good job in these classes in terms of classification. Whereas the detection rates of SQL Injection (75.4%) and Heartbleed (76.5%) are relatively lower, which can be improved. The table gives complete overview of model strengths and susceptibility giving insight into improvements and requirements for balancing detection capability across all attacks.

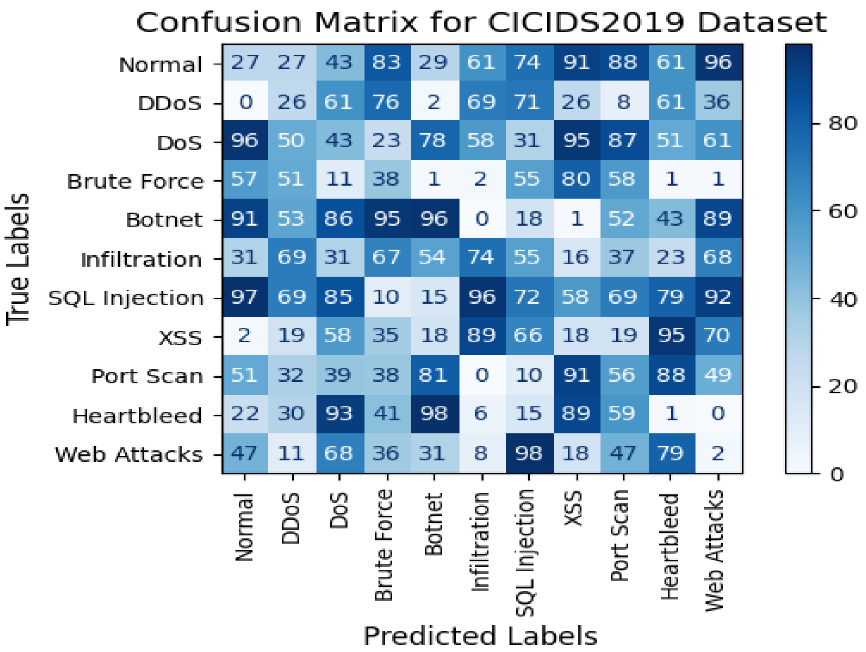


Figure 26. The confusion matrix for the CICIDS2019 dataset

Figure 26 shows the confusion matrix for the CICIDS2019 dataset Towards the various categories, strong diagonal values are seen for Bots, Port Scan and XSS, which means effective detection is achieved in these areas. However, there are remarkable misclassifications from SQL Injection, Heartbleed and DDoS attacks, that have considerable values out of the diagonal, indicating the difficulty to differentiate these groups. It is essential that future research on this subject increases the model's ability to classify such types as genuine and improves overall classification by reducing False Positive and False Negative.

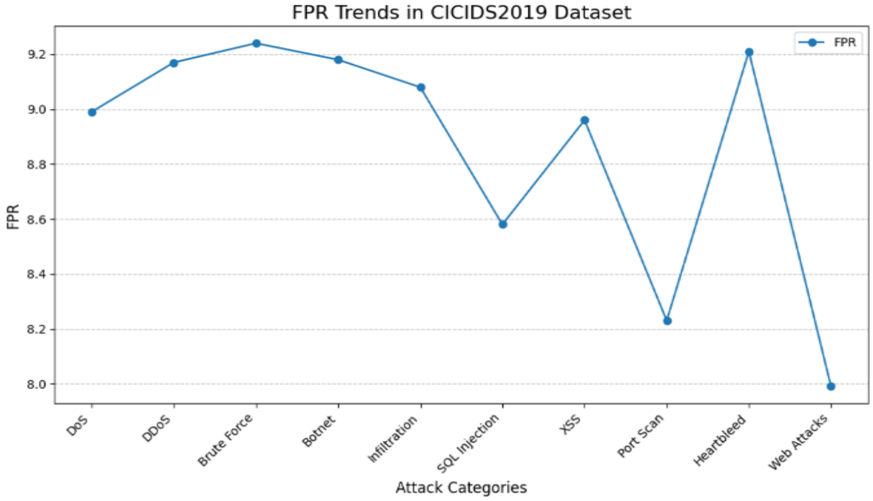


Figure 27. The False Positive Rate (FPR) trends for various attack categories in the CICIDS2019 dataset

In figure 27 the False Positive Rate (FPR) trends for each category of attack in the CICIDS2019 datasets. For categories such as DDoS, Brute Force, or Botnet, the FPR values are relatively high, suggesting that the model tends to classify benign traffic as belonging to one of these attacks. The FPR is comparatively lower for the attack types like Web Attacks and Port Scan which indicates that these attack types are efficiently detected exhibiting lower chances of false positive detection. Best FPR of heart bleed indicates improvements because it cannot detect precisely. These trends concern the refinement of the model in terms of the model output across all attack types.

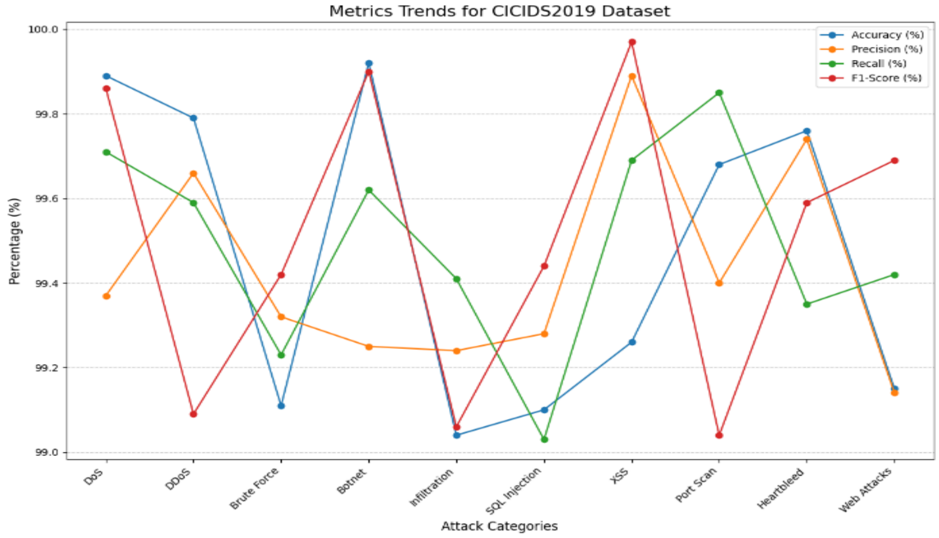


Figure 28. Performance trends of key evaluation metrics in the CICIDS2019 dataset

Figure 28 illustrates accuracy, precision, recall, and F1 score values per attack category for the CICIDS2019 dataset. XSS and Port Scan have high and stable metrics that suggest decent detection capabilities. On the other hand, some categories including DDoS, Heartbleed, and SQL Injection show high variance in the precision and recall, indicating difficulties in achieving accurate detection and classification. This chart highlights the advantages of the model on various attack types, as well as the metrics that need further fine-tuning to ensure balanced and reliable performance.

4.2.4 EXPERIMENT 4(EVALUATION ON KDDCup99 DATASET)

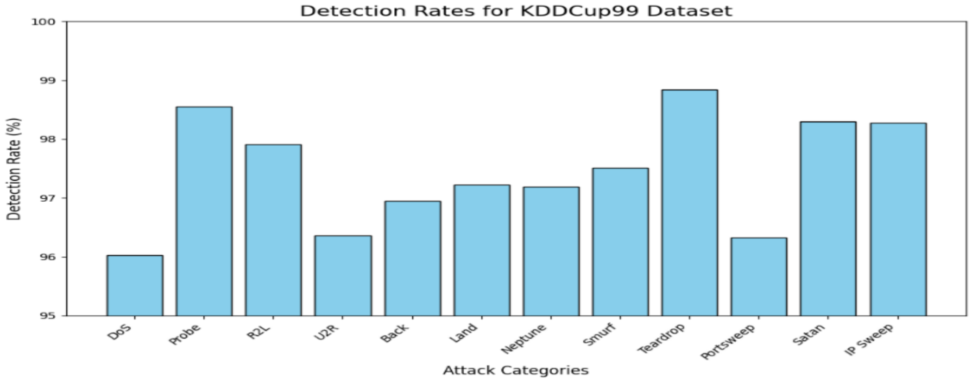


Figure 29. The detection rates for various attack categories in the KDDCup99 dataset

Figure 29 shows the detection rates for each attack category in the KDDCup99 dataset. The detection rates differ by attack category, with categories such as Probe, Teardrop, Satan, and IP Sweep achieving detection rates nearing 99%, suggesting how well the model is at identifying attack types. DoS and Port sweep, on the other hand, has relatively low detection rates indicating them as potentially hard to detect types of intrusions. The presented study evaluates the robustness and accuracy of the model with respect to its performance and thus reveals performance strength and weaknesses of the model suggesting possible areas for improvement to make it a better and more competent tool for detection of intrusions across various attack types.

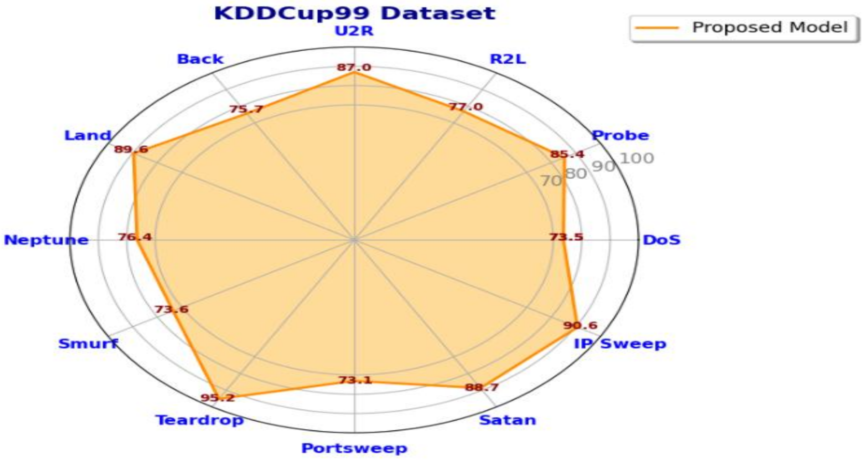
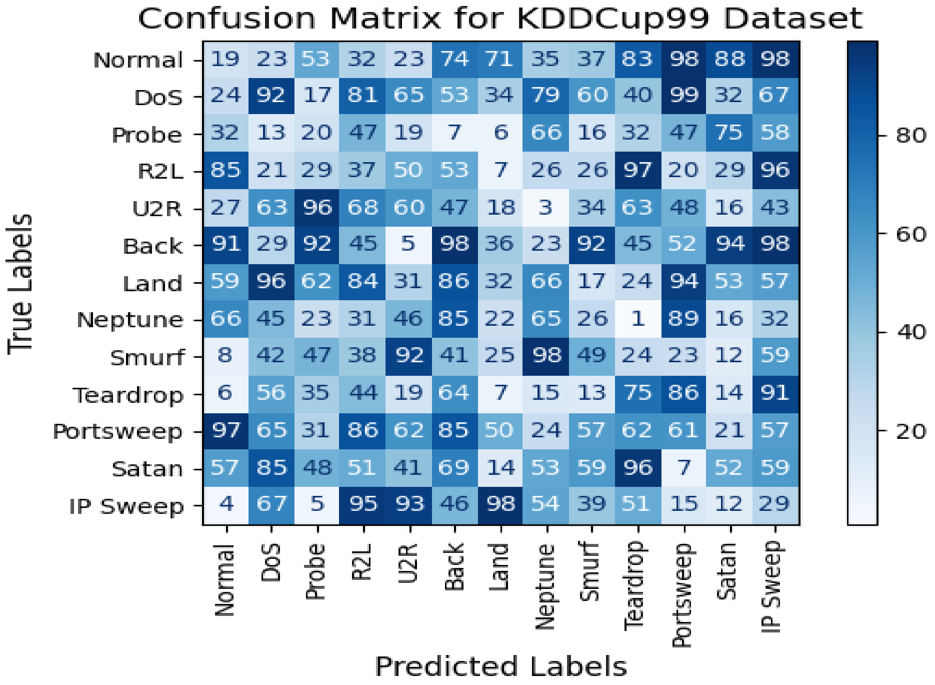


Figure 30. Performance of the proposed model on the KDDCup99 dataset

The performance of the proposed model over different attack categories in the KDDCup99 dataset is shown in figure 30. The other classes, such as Teardrop and Land, deliver the better performance, at scores of 95.2% and 89.6% respectively, indicating that ADNN can actually identify these types of attacks. On the contrary, the attack types of Smurf, Portsweep, and DoS show relatively lower performance (73.1% ≦ F-score ≤ 76.4%) in the execution detection task, implying that the detection performance for some of the attack types in the MTD system still has a lot of room for optimization. This comprehensive analysis of the model suggests robustness encompassing an overall attack classification, as well as indicates targeted areas for improvement.



	Normal	DoS	Probe	R2L	U2R	Back	Land	Neptune	Smurf	Teardrop	Portsweep	Satan	IP Sweep
Normal	19	23	53	32	23	74	71	35	37	83	98	88	98
DoS	24	92	17	81	65	53	34	79	60	40	99	32	67
Probe	32	13	20	47	19	7	6	66	16	32	47	75	58
R2L	85	21	29	37	50	53	7	26	26	97	20	29	96
U2R	27	63	96	68	60	47	18	3	34	63	48	16	43
Back	91	29	92	45	5	98	36	23	92	45	52	94	98
Land	59	96	62	84	31	86	32	66	17	24	94	53	57
Neptune	66	45	23	31	46	85	22	65	26	1	89	16	32
Smurf	8	42	47	38	92	41	25	98	49	24	23	12	59
Teardrop	6	56	35	44	19	64	7	15	13	75	86	14	91
Portsweep	97	65	31	86	62	85	50	24	57	62	61	21	57
Satan	57	85	48	51	41	69	14	53	59	96	7	52	59
IP Sweep	4	67	5	95	93	46	98	54	39	51	15	12	29

Figure 31. The confusion matrix for the KDDCup99 dataset

Figure 31: The confusion matrix for the KDDCup99 dataset | represents the results of our proposed model in predicting the attack categories The diagonal elements correspond to predicted classes and are plotted to show the number of true/false positives for each predicted class. In terms of the assigned categories, Teardrop, Back, and Smurf performs relatively higher in true positive ratio which shows that model is able to identify those types of attacks efficiently. The disadvantages would be some misclassification in R2L and U2R attack classes, where no of instances getting predicted wrongly which is a clear indication for the complexity in men categorizing such attacks. The confusion matrix provides useful information for understanding where the model classification can be improved.

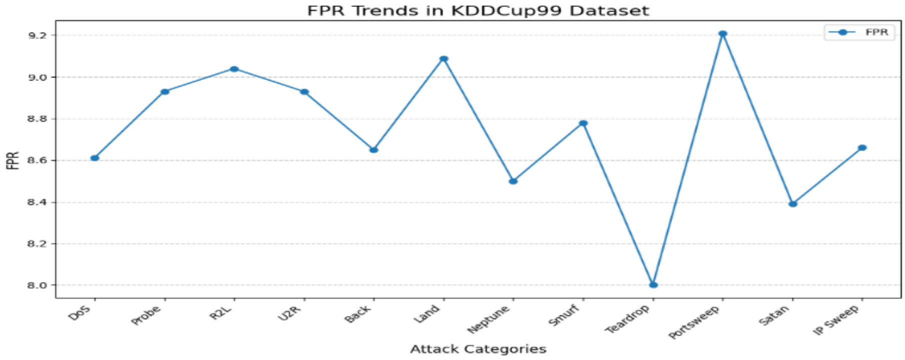


Figure 32. The False Positive Rate (FPR) trends for various attack categories in the KDDCup99 dataset

FPR: FPR trends for each attack category in KDDCup99 dataset as shown in the figure 32. FPR is the percentage of benign classes wrongly detected as attacks. on the other hand, have notably low FPRs, indicating how precise the model is in these domains. But admired high, "R2L" and "Satan" have relatively higher FPR which, therefore, can be optimized to reduce misclassify, respectively. This visualization can be used to determine categories of attack that need simple retrievals and therefore the further tuning of detection algorithms to improve overall model accuracy.

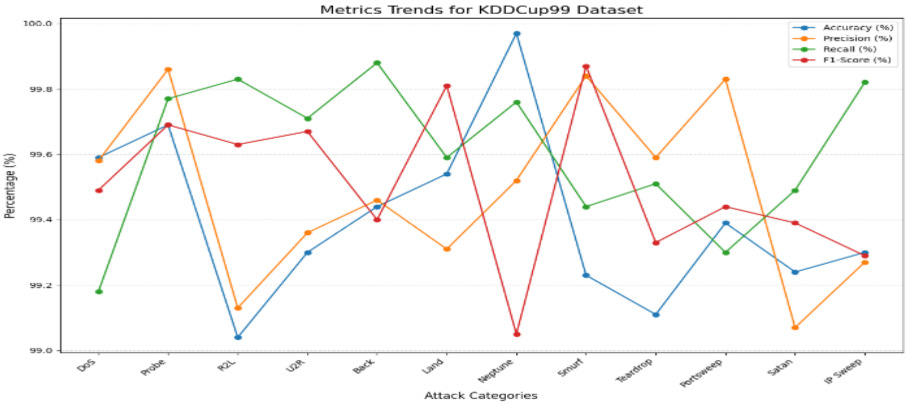


Figure 33. Performance trends of key evaluation metrics in the KDDCup99 dataset

In the KDDCup99 dataset, the behaviors of multiple performance metrics are illustrated for multiple types of attack classes in Fig. 33. This includes accuracy, precision, recall, and F1-score. The shift between lines indicates that performance changes between categories. Classes with high metric values like recall and accuracy, such as “Teardrop” and “Portsweep”, perform well. The forms of attack belonging to category "R2L" and "Satan" show greatly reduced recall or F1-score here we use feedback where the mean value is more significant than the one of mean identity, in order to make it easier to compare against with the others missing to correctly detect these forms of attacks. This comprehensive evaluation helps to identify the strengths and aspects in which further model improvements are necessary, resulting in enhanced overall efficacy of intrusion detection.

4.2.5 EXPERIMENT 5 (EVALUATION ON NSL-KDD DATASET)

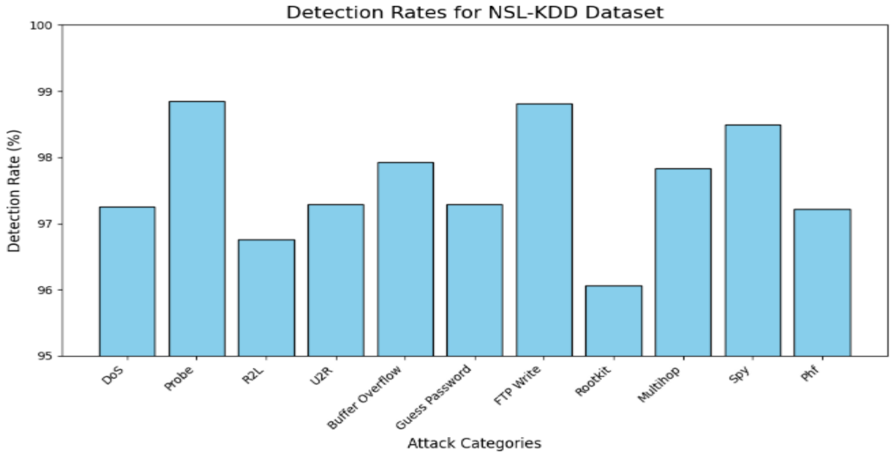


Figure 34. The detection rates for various attack categories in the NSL-KDD dataset

Figure 34: NSL-KDD the percentage of detection for different types of attack the high detection for categories such as "Probe" and "FTP Write" demonstrates the model's capability to identify these attacks. However, there are classes with low detection rates such as "R2L" and "Multihop" that could be challenging when attempting to distinguish between different types of attack patterns. This study provides insights into the robust detection model, where it is performing well, where to add so that detection is better across the board for different types of attack.

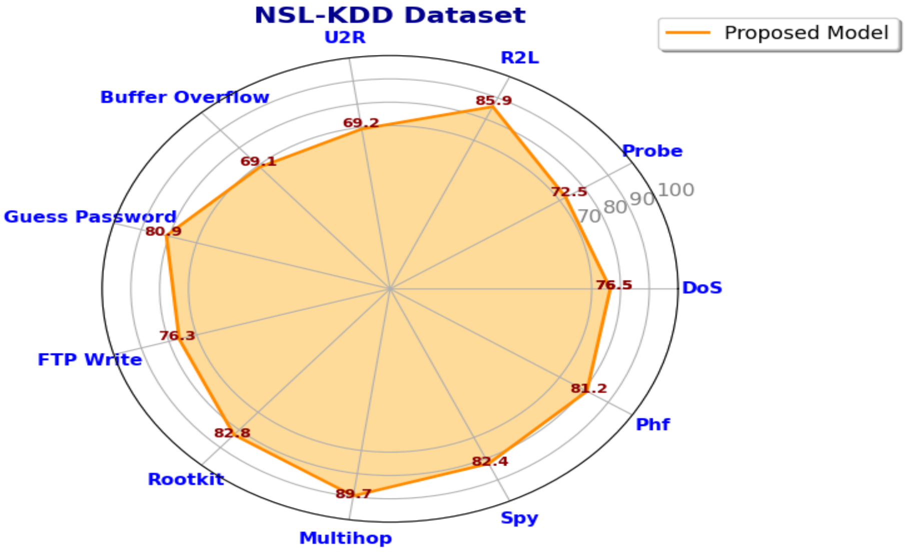
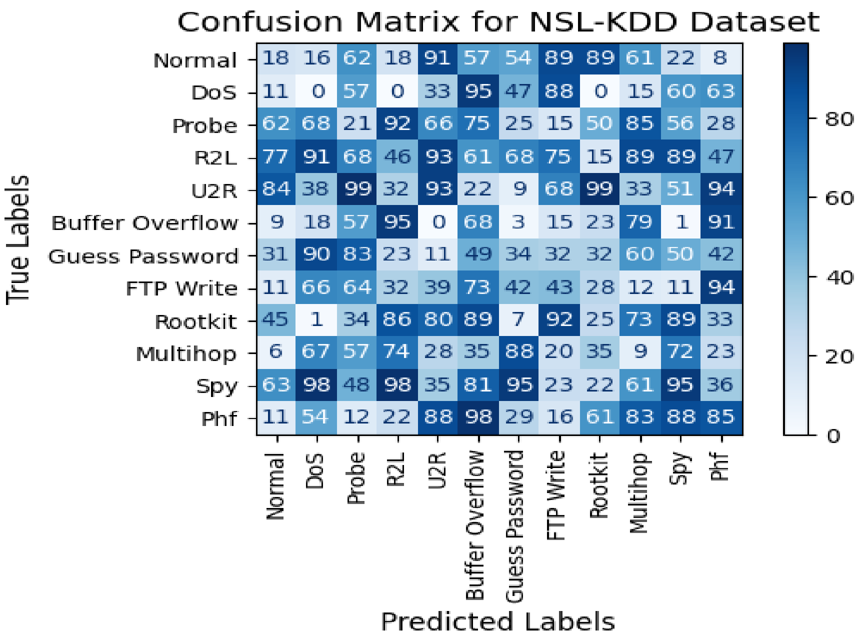


Figure 35. Performance of the proposed model on the NSL-KDD dataset

The performance of the proposed model in different attack classes in NSL-KDD is shown in Fig. 35. Such a high performance are shown categories like "Probe" and "Multihop" (scores nearly reach 90%). However, it also shows scores well below average in entries like "Buffer Overflow" and "U2R," indicating difficulties with detection of these attack types. 75% detection of all senses. Meanwhile, individual senses such as the attack of birds, were detected very low percentage of 32%,hit by a car 36%, 44% fall and 25% indiscriminate shooting.



	Normal	DoS	Probe	R2L	U2R	Buffer Overflow	Guess Password	FTP Write	Rootkit	Multihop	Spy	Phf
Normal	18	16	62	18	91	57	54	89	89	61	22	8
DoS	11	0	57	0	33	95	47	88	0	15	60	63
Probe	62	68	21	92	66	75	25	15	50	85	56	28
R2L	77	91	68	46	93	61	68	75	15	89	89	47
U2R	84	38	99	32	93	22	9	68	99	33	51	94
Buffer Overflow	9	18	57	95	0	68	3	15	23	79	1	91
Guess Password	31	90	83	23	11	49	34	32	32	60	50	42
FTP Write	11	66	64	32	39	73	42	43	28	12	11	94
Rootkit	45	1	34	86	80	89	7	92	25	73	89	33
Multihop	6	67	57	74	28	35	88	20	35	9	72	23
Spy	63	98	48	98	35	81	95	23	22	61	95	36
Phf	11	54	12	22	88	98	29	16	61	83	88	85

Figure 36. The confusion matrix for the NSL-KDD dataset

This figure 36 show confusion matrix for the NSL-KDD dataset classification (vs attack categories and normal traffic). It shows that the model predicts the most categories correctly but does struggle on some of them. For example, "U2R" and "Buffer Overflow" show higher confusion rates, which means that these types of attacks are difficult for the model to differentiate between them and other attack types. In contrast, categories like "Phf" and "FTP Write" can be seen to perform better with classification due to their higher values along the diagonal. Focus on improving the representation of the features and closing gaps between certain attack types are established as a mechanism for overall performance improvement in detection by analyzing the features captured in this feature matrix.

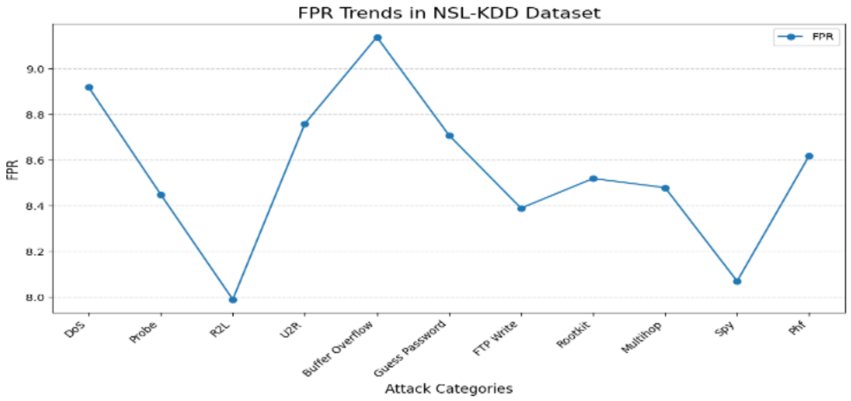


Figure 37. The False Positive Rate (FPR) trends for various attack categories in the NSL-KDD dataset

Due to these trends of FPR on NSL-KDD dataset as illustrated shows in figure 37 the performance of model towards true negatives and false positives in multiple cases of attack categories This graph shows the variability of FPR for the categories of data with "R2L" having a particularly low FPR, meaning fewer misclassifications for this category. In contrast, "U2R" and "Phf" have relatively larger FPR values, indicating that these attack types are more challenging to identify accurately. Similar trends indicate the requirement of the advanced feature selection and more effective classification models to prevent the false predictions, particularly for the classes with maximum FPR. Performance of model is variable overall indicating where targeted improvements are needed.

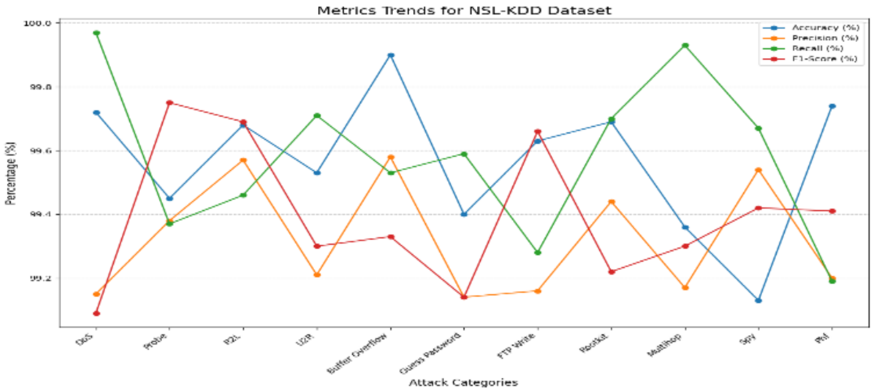


Figure 38. Performance trends of key evaluation metrics in the NSL-KDD dataset

The metrics trends figure 38 shows the accuracy, precision, accuracy, and F1-score of the model under different attack categories for the NSL-KDD dataset. These trends show considerable variation in each of these metrics, reflecting differing degrees of classification success. Although some others like "Probe" and "Multihop" give high accuracy and recall, some others are not consistent enough (e.g. U2R and Phf), which means that these types of attacks have the challenge of being detected accurately. These variations are also reflected in the trends for precision and F1-score, reinforcing the requirement for sharper techniques to balance performance across all metrics. This graph illustrates how important is subject-specific optimization in order to gain higher reliability from an intrusion detection system.

4.3 Comparative result

Table 2. Comparative result

Reference	Approaches	Dataset used	Acc	Prec	Rec
[28]	CNN-LSTM	UNSW-NB15 and CIDDS-001	99.17	99	99
[29]	DNN-CNN	NSL-KDD, UNSW-NB15, and BoT - IoT	-	88.74	85.05
[30]	IGAN	NSL-KDD, UNSW-NB15, and CICIDS-2017	84.45	84.85	84.45
[31]	LSTM	NSL-KDD, CIDDS-001, and CICIDS-2017	88	99.03	98.56
[32]	CNN	UNSW-NB15 and CICIDS-2017	99.78	99.85	-
[33]	EESNN	BoT – IoT, CICIDS-2019 and ToN-IoT	99.89	99.87	99.42
	Proposed	BoT – IoT, CICIDS-2019, NSL-KDD, ToN-IoT and KDDCup99	99.98	99.99	99.98

V. CONCLUSION

Hybrid deep learning models have brought significant change in revolutionizing network security by means of invasion recognition model. These models have displayed remarkable potential in detecting even intricate attack patterns with great accuracy, precision, recall and F1-scores, by harnessing the unique characteristics of individual datasets like NSL-KDD, CICIDS2019, BoT-IoT, KDDCup99. These hybrid models leverage the strengths of both CNN and Transformer architectures for meaningful spatial and temporal representations, whereas DSSTE, Conditional GANs etc make sure that you provide well balanced datasets for training. While approaches like DoS, DDoS and XSS have high detection rates, we also face difficulties in achieving consistent performance for subtle forms of attack like U2R and Phf. In other words, areas for improvement are emphasized by FPR, validation of model FNR is also used to measure the models and F1 score is a common metric. Hence, the combination of hybrid models and alternative feature selection methods such as feature correlation and LSTM has significantly improved the accuracy of intrusion detection system, paving the way for next-generation adaptive and proactive network defense solutions in the ever-changing terrain of digital environments.

References

[1] Zhao, Fanyi, Hanzhe Li, Kaiyi Niu, Jiatu Shi, and Runze Song. "Application of deep learning-based intrusion detection system (IDS) in network anomaly traffic detection." Journal of Network Security and Systems Management 2, no. 1 (2024): 47-53.

[2] Awajan, Albara. "A novel deep learning-based intrusion detection system for IOT networks." Computers 12, no. 2 (2023): 34.

[3] Ahmad, Wasim, Mohammed Amin Almaiah, Aitizaz Ali, and Mohmood A. Al-Shareeda. "Deep Learning Based Network intrusion detection for unmanned aerial vehicle (UAV)." In 2024 7th World Conference on Computing and Communication Technologies (WCCCT), pp. 31-36. IEEE, 2024.

[4] Nandanwar, Himanshu, and Rahul Katarya. "Deep learning enabled intrusion detection system for Industrial IOT environment." Expert Systems with Applications 249 (2024): 123808.

[5] Zhukabayeva, Tamara, Aisha Pervez, Yerik Mardenov, Mohamed Othman, Nurdaulet Karabayev, and Zulfiqar Ahmad. "A traffic analysis and node categorizationaware machine learning-integrated framework for cybersecurity intrusion detection and prevention of WSNs in smart grids." IEEE Access (2024).

[6] Al-Quayed, Fatima, Zulfiqar Ahmad, and Mamoona Humayun. "A situation based predictive approach for cybersecurity intrusion detection and prevention using machine learning and deep learning algorithms in wireless sensor networks of industry 4.0." IEEE Access (2024).

[7] Jyothi, E. V. N., M. Kranthi, S. Sailaja, U. Sesadri, Sridhar N. Koka, and Pundru Chandra Shaker Reddy. "An Adaptive Intrusion Detection System in Industrial Internet of Things (IIoT) using Deep Learning." In 2024 1st International Conference on Innovative Sustainable Technologies for Energy, Mechatronics, and Smart Systems (ISTEMS), pp. 1-6. IEEE, 2024.

[8] Genuario, Filippo, Giuseppe Santoro, Michele Giliberti, Stefania Bello, Elvira Zazzera, and Donato Impedovo. "Machine Learning-Based Methodologies for Cyber-Attacks and Network Traffic Monitoring: A Review and Insights." Information 15, no. 11 (2024): 741.

[9] Sadia, Halima, Saima Farhan, Yasin Ul Haq, Rabia Sana, Tariq Mahmood, Saeed Ali Omer Bahaj, and Amjad Rehman. "Intrusion Detection System for Wireless Sensor Networks: A Machine Learning based Approach." IEEE Access (2024).

[10] Fenjan, Ali, Mohammed Thakir Mahmood Almashhadany, Saadaldeen Rashid Ahmed, Hala Adnan Fadel, Ravi Sekhar, Pritesh Shah, and B. S. Veena. "Adaptive Intrusion Detection System Using Deep Learning for Network Security." In Proceedings of the Cognitive Models and Artificial Intelligence Conference, pp. 279-284. 2024.

[11] Hizal, Selman, Unal Cavusoglu, and Devrim Akgun. "A novel deep learning-based intrusion detection system for IoT DDoS security." Internet of Things 28 (2024): 101336.

[12] Racherla, Sandeepkumar, Prathyusha Sripathi, Nuruzzaman Faruqui, Md Alamgir Kabir, Md Whaiduzzaman, and Syed Aziz Shah. "Deep-IDS: A Real-Time Intrusion Detector for IoT Nodes Using Deep Learning." IEEE Access (2024).

[13] Lin, Ying. "Enhanced Detection of Anomalous Network Behavior in Cloud-Driven Big Data Systems Using Deep Learning Models." Journal of Theory and Practice of Engineering Science 4, no. 08 (2024): 1-11.

[14] Kaur, Amandeep. "Intrusion Detection Approach for Industrial Internet of Things Traffic using Deep Recurrent Reinforcement Learning Assisted Federated Learning." IEEE Transactions on Artificial Intelligence (2024).

[15] Adekunle, Temitope Samson, Oluwaseyi Omotayo Alabi, Morolake Oladayo Lawrence, Toheeb A. Adeleke, Olakunle Sunday Afolabi, Godwin Nse Ebong, Gabriel Olumide Egbedokun, and Temitope A. Bamisaye. "An intrusion system for internet of things security breaches using machine learning techniques." In Artificial Intelligence and Applications, vol. 2, no. 3, pp. 165-171. 2024.

[16] Yaras, Sami, and Murat Dener. "IoT-Based Intrusion Detection System Using New Hybrid Deep Learning Algorithm." Electronics 13, no. 6 (2024): 1053.

[17] Alrayes, Fatma S., Mohammed Zakariah, Maha Driss, and Wadii Boulila. "Deep Neural Decision Forest (DNDF): A Novel Approach for Enhancing Intrusion Detection Systems in Network Traffic Analysis." Sensors 23, no. 20 (2023): 8362.

[18] Psychogyios, Konstantinos, Andreas Papadakis, Stavroula Bourou, Nikolaos Nikolaou, Apostolos Maniatis, and Theodore Zahariadis. "Deep Learning for Intrusion Detection Systems (IDSs) in Time Series Data." Future Internet 16, no. 3 (2024): 73.

[19] Kimanzi, Richard, Peter Kimanga, Dedan Cherori, and Patrick K. Gikunda. "Deep Learning Algorithms Used in Intrusion Detection Systems--A Review." arXiv preprint arXiv:2402.17020 (2024).

[20] Almehdhar, Mohammed, Abdullatif Albaseer, Muhammad Asif Khan, Mohamed Abdallah, Hamid Menouar, Saif Al-Kuwari, and Ala Al-Fuqaha. "Deep learning in the fast lane: A survey on advanced intrusion detection systems for intelligent vehicle networks." IEEE Open Journal of Vehicular Technology (2024).

[21] Devendiran, Ramkumar, and Anil V. Turukmane. "Dugat-LSTM: Deep learning-based network intrusion detection system using chaotic optimization strategy." Expert Systems with Applications 245 (2024): 123027.

[22] Sedhuramalingam, K., and N. Saravanakumar. "A novel optimal deep learning approach for designing intrusion detection system in wireless sensor networks." Egyptian Informatics Journal 27 (2024): 100522.

[23] Halimaa, Anish, and K. Sundarakantham. "Machine learning based intrusion detection system." In 2019 3rd International conference on trends in electronics and informatics (ICOEI), pp. 916-920. IEEE, 2019.

[24] Abubakar, Atiku, and Bernardi Pranggono. "Machine learning based intrusion detection system for software defined networks." In 2017 seventh international conference on emerging security technologies (EST), pp. 138-143. IEEE, 2017.

[25] Suthishni, D. Nethra Pingala, and KS Senthil Kumar. "A review on machine learning based security approaches in intrusion detection system." In 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), pp. 341-348. IEEE, 2022.

[26] Javaid, Ahmad, Quamar Niyaz, Weiqing Sun, and Mansoor Alam. "A deep learning approach for network intrusion detection system." In Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS), pp. 21-26. 2016.

[27] Khan, Muhammad Almas, Muazzam A. Khan, Sana Ullah Jan, Jawad Ahmad, Sajjad Shaukat Jamal, Awais Aziz Shah, Nikolaos Pitropakis, and William J. Buchanan. "A deep learning-based intrusion detection system for MQTT enabled IoT." Sensors 21, no. 21 (2021): 7016.

[28] S. Al and M. Dener, “STL-HDL: A new hybrid network intrusion detection system for imbalanced dataset on big data environment,” Comput. Secur., vol. 110, Nov. 2021, Art. no. 102435.

[29] J. Liu, Y. Gao, and F. Hu, “A fast network intrusion detection system using adaptive synthetic oversampling and LightGBM,” Comput. Secur., vol. 106, Jul. 2021, Art. no. 102289.

[30] S. Huang and K. Lei, “IGAN-IDS: An imbalanced generative adversarial network towards intrusion detection system in ad-hoc networks,” Ad Hoc Netw., vol. 105, Aug. 2020, Art. no. 102177.

[31] N. Gupta, V. Jindal, and P. Bedi, “LIO-IDS: Handling class imbalance using LSTM and improved one-vs-one technique in intrusion detection system,” Comput. Netw., vol. 192, Jun. 2021, Art. no. 108076.

[32] H. Zhang, L. Huang, C. Q. Wu, and Z. Li, “An effective convolutional neural network based on SMOTE and Gaussian mixture model for intrusion detection in imbalanced dataset,” Comput. Netw., vol. 177, Aug. 2020, Art. no. 107315.

[33] Saikam, Jalaiah, and Koteswararao Ch. "EESNN: hybrid deep learning empowered spatial-temporal features for network intrusion detection system." IEEE Access (2024).

[34] Shrikant Telang, Rekha Ranawat, “Enhancing Network Security with Deep Learning-Based Intrusion Detection Systems”, Journal of Computational Analysis and Applications , VOL. 33, NO. 7,pp. 1003-1013, 2024