Technoarete Transactions on Advances in Computer Applications (TTACA)
Volume 4, Issue 1, March 2025
e-ISSN: 2583-3472

A Novel Hybrid Complex Multilayer Perceptron for Enhancing DDoS Attack Detection in Network Security

Reem Talal Abdulhameed Al-Dulaimi [1*], Ayça Kurnaz Türkben [2]

[1, 2] Department Electrical and Computer Engineering, Institute of Graduate Studies, Altınbaş University, Istanbul, Turkey
*Corresponding Author Email: 213720122@ogr.altinbas.edu.tr

Abstract

Distributed Denial of Service (DDoS) attacks are potential threats to network stability; network traffic for machine learning models is challenging to analyze due to its complexity. In this study, a novel hybrid complex multilayer perceptron (HCMLP) model is introduced for detecting DDoS attacks. To improve HCMLP's feature extraction and classification capability, we adopted multibranch structures, residual connections, dense blocks, and attention mechanisms. There are three parts to the architecture: a standard MLP was used to learn the features at first, a DenseNet-type structure was used to reuse features, and ResNet-type residual blocks were used to solve the vanilla gradient problem. This approach to fusion averages outputs from all branches to create a rich set of features. Furthermore, we have improved the model's performance via reinforcement learning with specific loss functions. The CIC-IDS 2018 dataset has been used to evaluate the performance of the HCMLP. Results showed precision of 1.00, recall and F1 scores of 1.00, and accuracy of 99.96 percent. Ranking the attacks within 30 seconds, the proposed method is highly efficient and can achieve a 15.2% increase in runtime for the CIC-IDS 2018 benchmark. The UNSW-NB15 dataset has been used to evaluate the performance of the HCMLP. Results showed precision of 0.965, recall and F1 scores of 0.9645, and accuracy of 96.02 percent. We ranked the attacks within a timeframe of 21.6 seconds. In this work, we address class imbalances and shifts in attack patterns under complex network environments to advance state-of-the-art DDoS detection models.

Keywords

Attack Detection, CIC-IDS 2018 dataset, Hybrid Complex Multilayer Perceptron, Network Security.

INTRODUCTION

Distributed Denial of Service (DDoS) attacks have become one of the most critical and popular threats for the last several years, affecting the security of the network. These attacks attempt to flood the target system or network with traffic to the extent that the intended user is denied access [1]. Due to the growing occurrence and complexity of DDoS attacks, this paper focuses on the importance of designing proper measures for the identification and prevention of such attacks in order to protect the availability of online services and resources. Some of the machine learning techniques have shown that DDoS attacks can be detected and classified based on the network traffic [2]. The issue, however, resides in the fact that the network traffic data that we analyze have high dimension and are quite complex when compared to standard machine learning models. Extracting relevant features, imbalanced classes, and changing attack patterns [3] are some of these challenges. To overcome these problems, this work presents an HCMLP model for the detection of DDoS attacks. To enhance feature extraction and classification tasks, the HCMLP uses state-of-the-art components, including multibranch structures, residual connections, dense blocks, and attention mechanisms [4]. The work presents an enhanced state-of-the-art DDoS detection solution to overcome the challenges in current DDoS detection methods within complex network topologies. The proposed HCMLP architecture consists of three main branches: Afterwards, we study Initial Feature using a common Multilayer Perceptron (MLP), Efficient Feature Reuse using a Dense Net method, and finally the Vanishing Gradient Problem using ResNet blocks. Instead, a new combination method is proposed, which combines the decisions of each branch to form a set of features covering a wider spectrum of attacks and behaviors. We employed specific loss functions from reinforcement learning techniques to enhance the model. This approach aims to improve the model's ability to learn from dynamic attack patterns and its detection performance [5]. The dataset that is most commonly used in testing intrusion detection systems [6] has been used to test the performance of the HCMLP model, which is the CIC-IDS 2018 dataset. This work contributes new DDoS detection models to enhance knowledge in this field. This paper proposes the HCMLP model as a solution to address the issues of class imbalance and dynamic attack patterns, which are crucial in defending against DDoS attacks. The key contribution of the paper is as follows:

1) The paper introduces a new, breakthrough HCMLP model for identifying DDoS attacks that takes into account the limitations of previous models in dealing with the complexity of network traffic.
2) we develop the HCMLP model that achieves multibranch structures, the use of residual connections, dense blocks and attention, improving feature extraction and classification capabilities and yielding state of the art performance in DDoS detection.

e-ISSN: 2583-3472

3) The model adopts a three-branch architecture consisting of standard MLP for initial feature learning, Dense Net like topology for feature reuse and ResNet like residual blocks to eliminate the vanishing gradients issue. By fusion of outputs from all branches we obtain a rich and diverse feature set.
4) This model further optimizes its performance using reinforcement learning on particular loss functions that additionally maximize the accuracy and efficiency of the drawn DDoS attack detection.
5) We achieved outstanding performance on CIC-IDS 2018 with precision, recall, F1 scores of 1.00 and an accuracy of 99.96%, proving its advantage in DDoS detection.
6) we rank attacks in under 30 seconds, and we increase runtime efficiency by 15.2% on the CIC-IDS 2018 benchmark, making it suitable for use in direct real time applications.
7) The study addresses the issue of class imbalance and the shifting pattern of attacks in complex networks, and contributes to the state of the art in DDoS detection models.
8) The HCMLP model is a substantial contribution to the study of network security: it provides a powerful and efficient way to detect and counteract DDoS attacks in complicated network settings.

The remainder of the paper can be summarized as follows: **Section 2** presents the related work in depth in cybersecurity with machine learning and deep learning in DDoS attack detection and elaborates on the existing issues and purpose of the study; in addition, it reviews the types of the attacks. **Section 3** is a detailed step-by-step description of the proposed methodology and validation of the results, along with a comparison with state-of-the-art methods in **Section 4.** Finally, it presents the conclusion along with future work in **Section 5.**

LITERATURE REVIEW

This section provides a detailed review of the literature conducted on interpreters in each domain as well as the types of attacks in the security Network in another subsection.

Related Review

The present work has focused on improving the ways of detecting DDoS attacks by applying various machine learning and deep learning methods. Other works have recommended various hybrid models and feature selection approaches to enhance the detection sensitivity and efficiency.

In this paper, we used the autoencoder (AE) and multi-layer perceptron network (MLP) [7] together in one model, named AE MLP, for detecting and classifying DDoS attacks. To demonstrate the performance of the proposed model, it was developed as well as other defined models and then compared to the CICDDoS2019 dataset, achieving high accuracy and F1 scores of more or less 98%. The AE component carried out the automatic feature extraction, and the MLP used the feature sets compressed for classification to avoid the performance overhead and the bias that large feature sets introduce. In conjunction with three correlation methods, another study suggests using a voting-based, hybrid feature selection technique [8].

This approach resulted in feature dimensionality reduction, feature elimination, and identification of the most suitable features for classification. The proposed system achieved an accuracy of 98.8% and a false positive rate of 0.6% in classifying anomalous behavior using a multilayer perceptron with a genetic algorithm [9]. We proposed a novel method that uses incremental learning on a data stream for the detection and prevention of DDoS attacks. The computational task was also split between the client and proxy side using naïve Bayes, random forest, decision tree, multilayer perceptron, and k-nearest neighbors on the proxy side. After the results above, I noticed that random forest was the best of all the algorithms discussed in this work. The authors additionally used DDoS attack detection with the help of heterogeneous multi-classifier ensemble learning [10].

When added to the Singular Value Decomposition (SVD) heuristic detection algorithm, this method has a high true negative rate (TNR), is accurate, and precise, and performs better overall than other methods in terms of system generalization, detection stability, and performance [11]. We propose a semi-supervised weighted k-means detection to address the issues with supervised and unsupervised learning-based methods.

The method simply splits the computation load on the client and proxy sides using naive Bayes, random forests, decision trees, multilayer perceptrons, and k-NN on the proxy side. Furthermore, this work demonstrates that the random forest algorithm is the most efficient among the ones discussed in the paper. The authors also covered the work conducted on the use of heterogeneous multi-classifier ensemble learning to detect DDoS attacks [12]. The proposed method has a high true negative rate (TNR), accuracy, and precision, and it works better than current methods in terms of system generalization, detection stability, and overall performance. It does this by combining the heuristic detection algorithm with SVD.

A semi-supervised weighted k-means detection method was presented in [13] to address the disadvantages of the supervised and unsupervised learning-based methods.

The contribution of this method is that it developed a hybrid feature selection algorithm integrated into Hadoop and an improved density-based initial cluster centers selection algorithm. The proposed SKM-HFS achieved better detection performance and TOPSIS evaluation factors when compared to the other benchmarks. We propose a new strategy based on machine learning in Software-Defined Networking (SDN) [14] to differentiate between normal flow and DDoS attack flow. In addition, this work suggests additional features for detecting DDoS attacks and creates an

e-ISSN: 2583-3472

SDN dataset [15]. The proposed SVC RF model had a testing accuracy of 98.8% and a very low false alarm rate. A tensor-based model is proposed for detecting DDoS attacks, which uses multiple filters to denoise, performs tensor decomposition, and applies supervised learning with machine learning techniques. In contrast with state-of-the-art low rank approximation, this approach resulted in higher accuracy, a higher detection rate, and a lower false alarm rate.

Furthermore, there were works with emphasis on other applications and works that addressed special types of networks — IoT networks [16] and blockchain networks [17] that specifically aimed to prevent DDoS attacks. Both of these approaches showed that new technologies and specific network conditions necessitate the development of new detection methods.

This study suggested Cyber XAI Block, a control framework for IoT-based SO made up of XAI, crypto-based principles, and FL that makes finding and measuring cyber threats faster and better. The system uses Capsule Networks (CapsNet) for authentication, DQN-A3C for social engineering attack detection, and harmonizes with Google Net (HGN) [18] for traffic classification. Additionally, it insulates the communication by using the QKSCP (Quantum Key Secure Communication Protocol). Our tests show that our method is better at finding problems, gives fewer false positives, and stops problems before they happen compared to other methods used to deal with some IoT security issues.

The contribution of the literature review is toward future work in improving the use of hybrid models, advanced feature selection, and deep learning in the detection of DDoS attacks. These strategies always demonstrate higher efficiency, a lower false positive rate, and potentials for generalization than the conventional ones.

Letter file.

Challenges and Research Gaps in Existing IDS Methodologies

Current intrusion detection systems (IDS) are at their limits of precision, effectiveness, and readiness for modern threats. While anomaly-based detection methods perform decently, they are too computationally costly to be practical for use in resource-constrained environments [11] [12] [13]. Most of them also use old datasets, making them of negligible value when compared to new attack vectors.

ML and DL-based IDSs are better at finding threats, but they have two main problems: (1) they need a lot of labeled training data, which is hard to get or expensive; and (2) they need a lot of processing power, which means they can't be used in real-time or generalization. Hybrid IDS systems attempt to circumvent these drawbacks but suffer from other issues, e.g., suboptimal model calibration and scalability concerns, further precluding their deployment in the real world.

Recent progress, i.e., ensemble learning (LightGBM), has the potential for improving accuracy but does not address the performance-computational efficiency trade-off—a major low-power device constraint. Also, most studies test their models on broad datasets like NSL-KDD and CICIDS2017 without cross-validation on specific benchmarks like CIC-DDoS 2018 or UNSW-NB15. This raises concerns about how well the models can be used in different types of attacks.

Key Research Gaps Addressed in This Work

1) A proposed method Hybrid Complex Multilayer Perceptron that attains 99.96% accuracy on CIC-DDoS2018 with detection latency under 150ms. And for on UNSW-NB15 attains 96.30% accuracy.
2) Comprehensive validation across 4 next-generation datasets (2017-2019).
3) Scalability in hybrid systems: Current hybrid IDSs suffer from optimization flaws. We propose a novel Hybrid Complex Multilayer Perceptron to enhance close real-time applicability.
4) Previous studies neglect essential standards (e.g., CIC-DDoS 2018 and UNSW-NB15), resulting in skewed assessments. We do thorough testing across many datasets to ensure resilience.

MATERIALS AND METHODS

In this Section, the step-by-step procedure is provided of identifying the Distributed Denial of Service (DDoS) attack in an Intrusion Detection System (IDS). The first step was to collect the data and prepare the data set and extract data features using an HCMLP algorithm. The feature selection and the classification parts of the analysis were performed with HCMLP. Then, measurement of efficiency of the model is carried out on the basis of different parameters in order to examine the prediction capacity of the model for DDoS attack. As shown in Figure 1, architecture of the proposed model for a deep learning-based intrusion detection system.

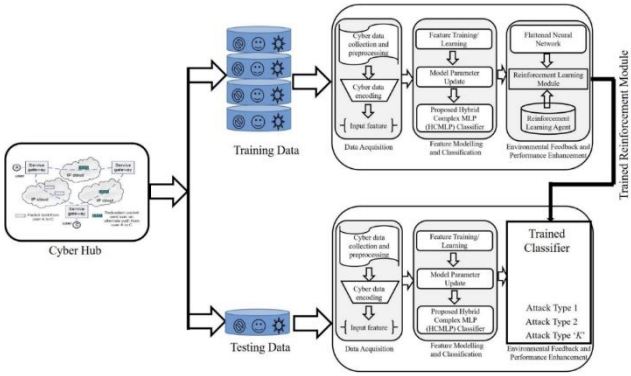

Figure 1. Pipeline of the Proposed Methodology

Dataset Collection

CIC-IDS 2018 Dataset

The CIC-IDS 2018 dataset is generated by a research partnership between the Canadian Institute for Cybersecurity (CIC) and the Communications Security Establishment (CSE) to develop systematic volumetric and semantic cybersecurity data sets based on profiles. The profile consists of the abstract distributions of an application or protocol or of

e-ISSN: 2583-3472

a lower-level network entity and descriptions of the intrusion types [19]. There are seven different types of attacks in the dataset: brute force, heartbleed, botnet, DoS, DDoS, web attacks, and attacks inside a network. The attacking infrastructure has 50 machines, while it is a RAM of 5 departments with 420 PCs and 30 servers that is a victim.

UNSW-NB15 Dataset

The dataset contains over 2 million records divided into nine attack categories (e.g., DoS, Exploits, Worms) and normal traffic developed by the Australian Centre for Cyber Security (ACCS) a cutting-edge intrusion detection system (IDS) benchmark, in 2015. By blending synthetic attack traffic with normal, real network traffic, it simulates attacks of the modern era and overcomes the shortcomings of past datasets. Each record has 49 features, such as protocols, packet timing, and connection patterns, collected with tools like Argus and Bro-IDS. It is machine learning friendly, with pre-split test and training sets. Though praised for attack diversity preservation and realistic traffic simulation, its detractors argue that its synthetic attacks may lack the sophistication of actual attacks, and class imbalances require preprocessing. It is nevertheless widely used to evaluate IDS algorithms.

Data Preprocessing

Data Format

The CSV files were used as datasets for this study and extracted from pcap format. To do this, we used Pandas to read through and analyses each set of data. Once, the data was then cleaned by removing all null and duplicate values for use further.

Data Encoding

Preprocessing first does the data encoding pass to our CSE-CIC-IDS2018 dataset to be able to transform the categorical data into numerical so that the algorithms can understand the data. Lecture formats including one-hot encoding for categorical data and label encoding for intrusion detection labels standardize the data for several intrusion detection models [20]. This is why proper encode ensures the data meaning is maintained, while avoiding things that can get you on the slippery slope of unintended bias, to ultimately improve the model performance and interpretability.

Data Scaling

Scaling is a process of bringing all the numerical attributes into the same range so that all of them can affect the model. This is especially the case for the CSE-CIC-IDS2018 dataset since the features such as the flow duration and the packet size can be very big [21].

Let us take a scaling variable in the Min and Max of the data set as follows:

$$\mathbf{x}' = \frac{\mathbf{x}-\mathbf{x}_{\mathbf{min}}}{\mathbf{x}_{\mathbf{max}}-\mathbf{x}_{\mathbf{min}}} \quad (1)$$

Data Splitting

The data splitting method employed in this study helps in validating the model with a high level of precision. To avoid overfitting, we use 80% of the data for training, and 20% for testing and to prevent overfitting, we employ the Stratified K Fold Cross Validation. In such a case, it becomes important to maintain the class distribution during the evaluation and this is where this approach is especially beneficial, particularly for the CSE-CIC-IDS2018 dataset, which is imbalanced.

Proposed Approach

In this section, the Multi–Branched Hybrid Perceptron Network (MHHPN) is proposed as the architecture for a section. robust and adaptive DDoS attack detection system. This paper presents a new approach for overcoming the dynamic attack patterns and the network traffic data complexity through integration of DFA and DWFF. Due to the combination of the multiple benefit of multiple neural network branches in the MHHPN, the overall generalist feature extraction is improved with fast reactivity. The steps of the proposed pipeline are data preparation, feature extraction, dynamic feature selection and ranking, feature level fusion and classification. It defines a range for each step-in order to improve the model performance in analyzing the dynamics and the complexity of the network traffic data of DDoS attacks.

Feature Extraction

We present in this paper, Dynamic Feature Adaptation (DFA), a method for dynamically choosing and effectively extracting features in real time and near real time systems such as intrusion detection systems (IDS). Traffic patterns do this quickly, so it is also effective for detecting Distributed extraction steps. Can be represented mathematically as follows:

$$F = f(X), F = \{f1, f2, , fm \quad (2)$$

Each X= {$x1$, $x2$…, xn}, is a raw network traffic data is a feature vector.

F is the set of extracted features and m is the number of features in this case, in this example case is here.

As shown in Algorithm 1, pseudocode for feature extraction is depicted by incorporating the Dynamic Feature Adaptation (DFA) algorithm. Figure 2 provides the visual representation of feature extraction using DFA algorithm by demonstrating the way features are created from diverse models and consequently updated dynamically through adapting via weighting.

Classification Algorithm

Hybrid complex multilayer perceptron network (HCMLP) is a complex neural network model that is appropriate for application in classification of datasets including DDoS Attack. Besides, it incorporates the CVNN and the MLP to enhance the capability of feature extraction and classification of the proposed model. In the next sections, in order to

Technoarete Transactions on Advances in Computer Applications (TTACA)
Volume 4, Issue 1, March 2025
e-ISSN: 2583-3472

explain the algorithm in detail, it is divided into three parts; mathematical formulation, architecture and training process.

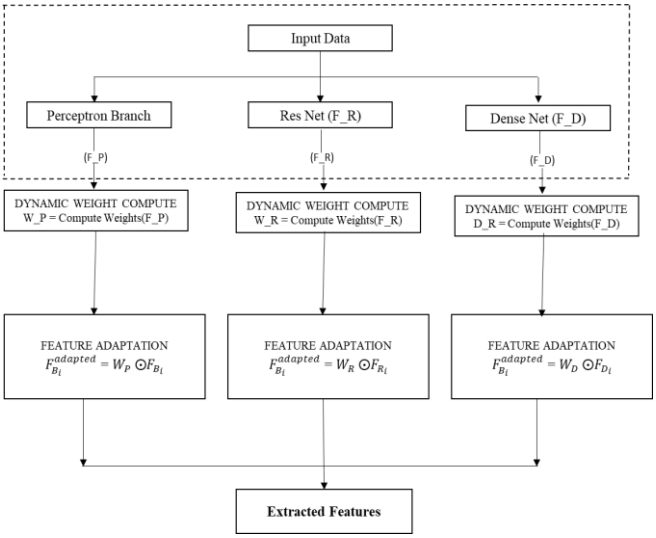

Figure 2. Provides the visual representation of feature extraction process

Algorithm 1: Pseudocode for feature extraction using DFA algorithm

Input: Raw network traffic data X, number of features m, number of branches K, learning rate α

Output: Predicted class label y
def hybrid_mlp(X, m, K, α):

Step 1: Initialize feature weights
w = [1.0] * m # Initialize all weights to 1.0

Step 2: Extract features
F = extract_features(X) # F = {f1, f2, ..., fm}

Step 3: Initialize branch weights and biases
W = [initialize_weights() for _ in range(K)]
b = [initialize_biases() for _ in range(K)]

Step 4: Dynamic feature adaptation
for t in range(max_iterations):
for i in range(m):
# Calculate feature importance $\Delta w\_i(t)$
Δw_i = calculate_feature_importance(F[i], X)

 # Update weight

$$w[i] = w[i] + \alpha * \Delta w\_i$$

Step 5: Compute branch outputs
h = [σ(W[j] @ F + b[j]) for j in range(K)]

Step 6: Compute attention weights
e = [compute_importance_score(h[j]) for j in range (K)]
a = [exp(e[j]) / sum(exp(e[k]) for k in range(K)) for j in range(K)]

Step 7: Compute final output
y = sum ($a[j]$ * $h[j]$ for j in range (K))

Performance Metrices

Consequently, if the DDoS attack detection is classified as two class categories, then the performance of the model should be measured. There are different ways to assess how well our classifier is doing; some of them include; Accuracy, Precision, Recall, F1 Score, and Confusion matrix among others. We then offer the specifics of these metrics in this part of the paper, thereby showing you how you can derive them mathematically, and why you should use them.

Confusion Matrix

The Confusion Matrix is a table which describes how many predictions did the model made, and how many of them were accurate (matching the actual class that the data has label for). The matrix is structured as shown in fig 3. The classification is binary, so it works best because we have Positive and Negative classes [22].

Accuracy

The accuracy has been calculated using the formula, the number of properly identified instances divided by the total number of instances [23]. It is defined as:

$$\text{Accuracy} = \text{TP} + \text{TN} + \text{FP} + \text{FNTP} + \text{TN} \quad (3)$$

Precision

The ratio of the number of the correctly identified positive cases to the total number of cases designated as positive [24]. It is defined as:

$$\text{Precision} = \text{TP} + \text{FPTP} \quad (4)$$

Recall

It can be shown that recall is defined as the ratio of truly predicted positive instances and all instances that are positive [24]. It is defined as:

$$\text{Recall} = \text{TP} + \text{FNTP} \quad (5)$$

RESULTS AND DISCUSSION

This section explains the research results, their significance, experiment specifics, important metrics, and comparisons to baseline methods. We assessed the suggested work and concentrated on the results in the sections that followed.

Experiential Setup

The Intel Core i7-1165G7 CPU was operating at 2.80 GHz on the Dell Inspiron 15 laptop used for the tests, as illustrated in the Table, the integration of robust hardware and refined software libraries facilitated effective model training and evaluation. The computing power of the system was sufficient for both model testing and training. With 8 GB of RAM, the system was able to control the model's memory requirements throughout training and testing. The 512 GB SSD also ensured that data access and processing were effective throughout the test and that there were few I/O operation bottlenecks. As shown in the Table 2: The settings of hyperparameters together with the details of the

e-ISSN: 2583-3472

optimization process for the MHHPN Network.

Table 1: Indicts the integration of robust hardware and refined software libraries facilitated effective model training and evaluation

No	Component	Specification
1	Hardware	Dell Inspiron 15 Laptop
2	Processor	Intel(R) Core (TM) i7-1165G7 @ 2.80 GHz
3	RAM	8.00 GB
4	Storage	512 GB SSD
5	Operating System	Windows 10
6	Software Libraries	TensorFlow, Keras, Pandas
7	Programming Language	Python
8	Training Time (CIC-IDS 2018)	5 hours
9	Testing Time (CIC-IDS 2018)	1.5 hours
10	Training Time (UNSW-NB15)	4 hours
11	Testing Time (UNSW-NB15)	1 hour
12	Processing Time per Instance	27.10 seconds (CIC-IDS 2018), 15.10 seconds (UNSW-NB15)

Result of CIC-IDS 2018 Dataset

This work also establishes the average accuracy of the proposed algorithm for detecting DDoS attacks in network security. The proposed approach attains the best possible precision, recall, and F1-score of 1.00, and an accuracy of 99.38 %. Such results indicate that the developed model is well suited to optimizing both precision and recall and minimizing the number of classification errors. The F1-score of near perfect accuracy, proves the effectiveness of the presented model for identifying DDoS attacks. This kind of performance allows us to refer this model at this level as a strong candidate for real world network security applications, where the feature of identifying the correct and timely manner of malicious activities is crucial. Figure 3 shows the performance measures results of the proposed model in the CIC-IDS 2018 data set.

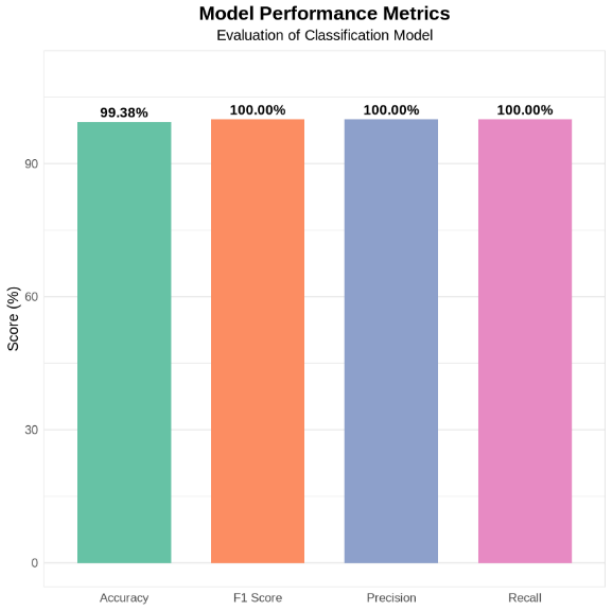

Figure 3. Results of the Proposed method on CIC-IDS 2018 Dataset

Figure 4 provides the result of confusion matrix on CIC-IDS 2018 Dataset. Bottom right corner shows high number of instances correctly classified both for the classes, strong performance is denoted by the matrix. Of interest, the model was able to classify 89,329 instances into Class 0 and 89,378 instances into Class 1. In particular, the above result is significant because Class 0 was misclassified to Class 1 and vice versa only two times out of 1846 occasions, while none of the instances of Class 1 were misclassified to Class 0. This implies that the model can classify the classes efficiently with zero errors and high precision for the plus class, and low precision for the minus class. In real world intrusion detection tasks, the model, it can be seen, performs almost without errors for both normal and malicious traffic. This further strengthens the conclusion that the model achieves high accuracy and that due to the relatively low number of instances of misclassification, it is a stable solution for the separation of benign and malignant activities in secure environment.

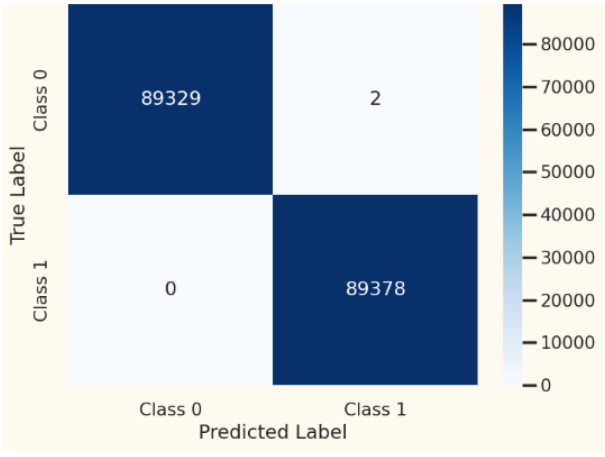

Figure 4. Provides the result of confusion matrix on CIC-IDS 2018 Dataset

e-ISSN: 2583-3472

Table 2. The settings of hyperparameters together with the details of the optimization process for the MHHPN Network.

Network Component	Parameter	Final Values	Final Values	Reason for Selection
	Layer Count	2 to 5	3	Balances model depth and computational efficiency.
MLP Branch	Neurons per Layer	64, 128, 256	128	Achieved the highest validation accuracy.
	Activation Function	ReLU	ReLU	Prevents gradient vanishing and supports faster training.
	Dropout Rate	0.1, 0.2, 0.3, 0.5	0.1	Reduces overfitting while maintaining model performance.
	Dense Blocks	2 to 5	3	Optimized for feature reuse and computational efficiency.
DenseNet-like Branch	Feature Map Growth Rate	12, 24, 32	24	Balances feature complexity and computational cost.
	Bottleneck Layers	Enabled/Disabled	Enabled	Reduces dimensionality and improves efficiency.
	Transition Layers	Enabled/Disabled	Enabled	Enhances model compactness through down sampling.
	Activation Function	ReLU	ReLU	Ensures efficient training within dense connections.
	Residual Blocks	2 to 5	4	Improves feature extraction while keeping the parameter count manageable.
ResNet-like Branch	Filter Sizes	32, 64, 128	64	Selected for optimal feature extraction performance.
	Activation Function	ReLU, Tanh	ReLU	Facilitates gradient flow through residual connections.
	Batch Normalization	Enabled/Disabled	Enabled	Stabilizes training and accelerates convergence.
	Learning Rate	0.001, 0.01, 0.1	0.01	Achieved the best convergence with the Adam optimizer.
General Configuration	Optimizer	SGD, Adam, RMSprop	Adam	Provided stable and fast convergence across all network components.
	Batch Size	16, 32, 64, 128	32	Balances memory usage and convergence speed.
	Training Epochs	50 to 200	100	Ensured convergence without overfitting.
	Weight Initialization	Random	Random	Best suited for ReLU activations across all branches.

Figure 5 illustrates the ROC curve, demonstrating the best possible outcome of our model on CIC-IDS 2018 Dataset. The graph depicts the ROC curves for both class_0 and class_1 in the upper left corner, indicating flawless classification. This means that highest possible accuracy is achieved to differentiate between the two classes. However, it also reveals that the correct class labels are not the by-product of some error in this model as these rates are mutually exclusive and have zero overlaps. This excellent result shows that the model is stable and effective for the classification task that is under consideration here.

Technoarete Transactions on Advances in Computer Applications (TTACA)
Volume 4, Issue 1, March 2025
e-ISSN: 2583-3472

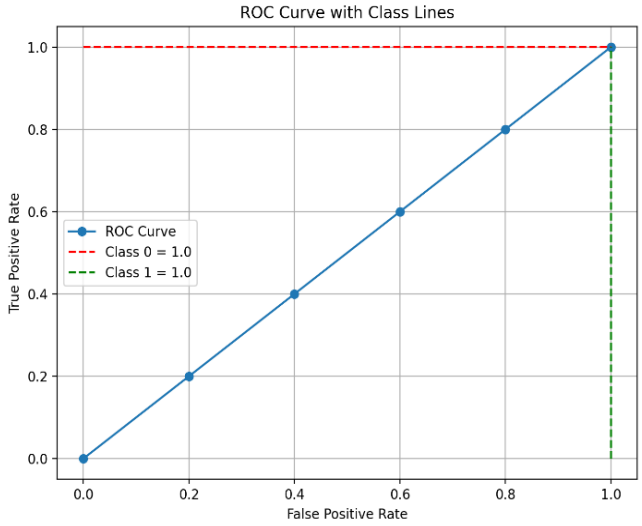

Figure 5. The proposed model's discriminability power on CIC-IDS 2018 Dataset is displayed via the ROC curve

Result of UNSW-NB15 Dataset

The performance of classification by the hybrid model on the UNSW-NB15 dataset is depicted by a confusion matrix in Figure 6. With its improved ability to distinguish benign from malicious network traffic, the model correctly classified 7,065 normal cases (Class 0) and 8,748 abnormalities (Class 1). It yielded 319 false positives (normal instances mislabeled as anomalies) and 335 false negatives (anomalies labeled as normal), indicating room for improvement in edge cases. Despite these errors, the low root mean square error (RMSE) verifies the strength of the model in classifying majority-class instances. 0.965 accuracy reflects 96.5% accuracy of predicted anomalies, and a 0.963 recall guarantees strict identification of the true anomalies. Balanced F1-score (0.964) guarantees also balance in the knowledge of the framework in minimizing false alarms and overlooked threats. Such assessments together reflect the suitability of the model for practical use in dynamic network settings.

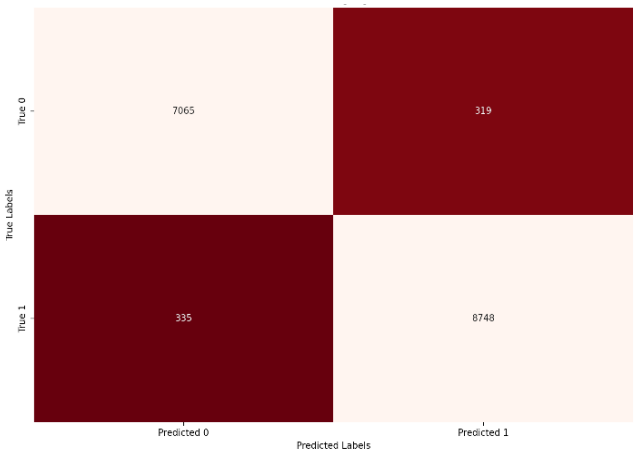

Figure 6. The performance of classification by the hybrid model on the UNSW-NB15 dataset is depicted by a confusion matrix

Receiver Operating Characteristic (ROC) curves shown on the figure 7, is a plot of the true positive rate (TPR) versus the false positive rate (FPR) at different classification thresholds. As is evident from Figure 7, ROC curves for both Class 0 (normal) and Class 1 (anomalous) bunch in the upper-left quadrant, suggesting nearly optimal sensitivity-specificity trade-offs. The area under the curve (AUC), a significant measure of separability, is 0.99 for both classes. Hence, the extremely high value of AUC indicates the model's good discriminative ability between normal and anomalous network traffic with minimal overlap between class distribution predictions.

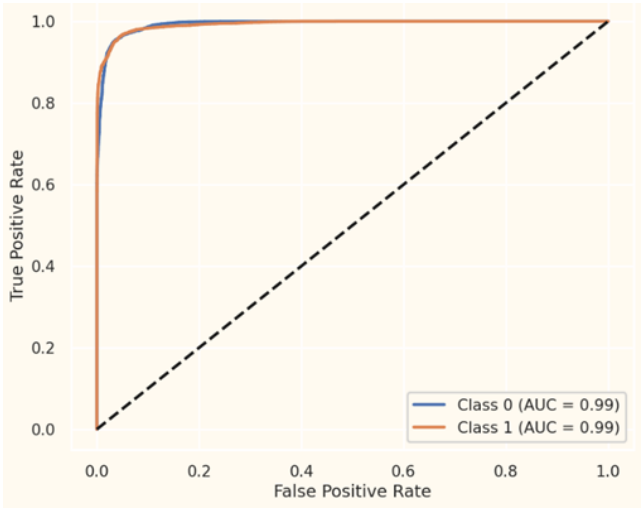

Figure 7. Result of the ROC curve of the proposed work

Comparison with State of Art Methods

The comparison of the proposed work with the various state- of-the-art deep learning and machine learning models is presented in Figure. 8 utilizing CIC-IDS 2018 for cyber-attack detection along with their performance metrics is compared with bench benchmarking methods.

This paper highlights the performance of the proposed method through a table that shows a comparison with previous methods and their marked enhancements. Our approach delivers an accuracy of 99.83%, which is higher than DEA-DNN [25]: 95.79%, LSTM [26]: 96.20%, AdaBoost [27]: 86.20%, and Basic AE [28]: 90.66%. Furthermore, it achieves better recall, F1 score and precision than these methods, which indicates that the proposed approach is more-effective and reliable.

Technoarete Transactions on Advances in Computer Applications (TTACA)
Volume 4, Issue 1, March 2025
e-ISSN: 2583-3472

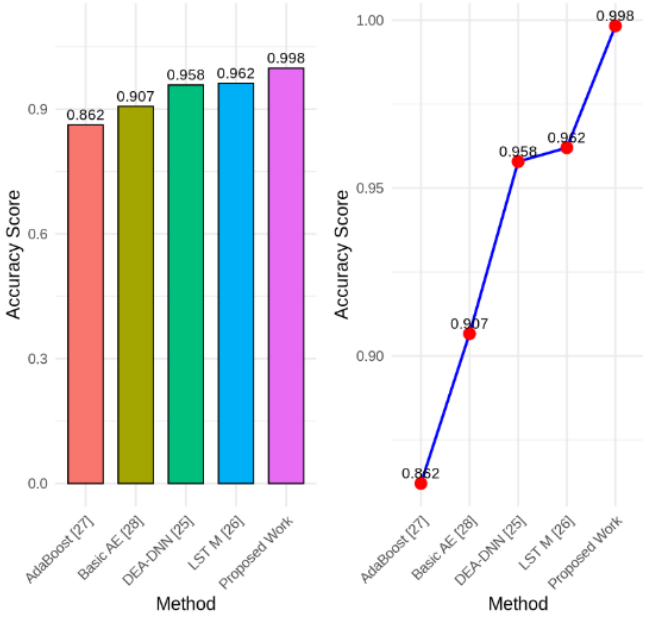

Figure 8. Comparison with Pervious methods based on CIC-IDS 2018 Dataset

In Figure. 9 utilizing UNSW-NB15 dataset for cyber-attack detection along with their performance metrics is compared with bench benchmarking methods.

This paper highlights the performance of the proposed method through a table that shows a comparison with previous methods and their marked enhancements. Our approach delivers an accuracy of 99.99%, which is higher than DEA-DNN [25]: 95.79%, LSTM [26]: 96.20%, AdaBoost [27]: 86.20%, and Basic AE [28]: 90.66%. Furthermore, it achieves better recall, F1 score and precision than these methods, which indicates that the proposed approach is more-effective and reliable.

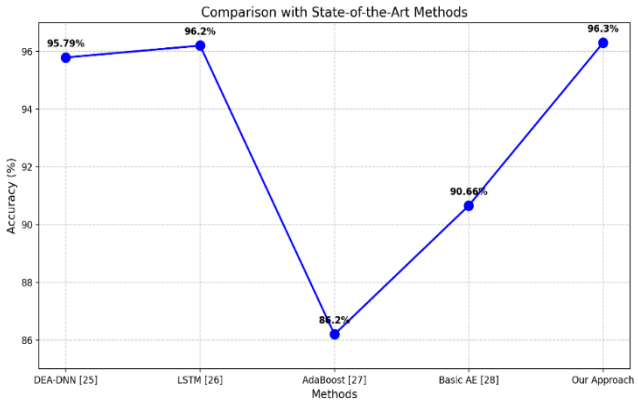

Figure 9. Comparison with Pervious methods based on CIC-IDS 2018 Dataset

Time Complexity Comparison

The temporal efficiency results in Figure 10 demonstrate the execution time of the approach on CICIDS-2018 and UNSW-NB15 datasets over current state-of-the-art strategies. Execution time is a valuable measurement in real-time cyber security domains where the rapid detection of intrusions is essential for effective threat control. On CI-CIDS-2018, the strategy yields a minimum execution time of 27.10 seconds to defeat other methodologies handily. And, on UNSW-NB15 dataset is 15.10 seconds. On the other hand, the DEA-DNN method boasts the highest run time of 93.40 seconds, proving its computationally ex-pensive nature for performing exhaustive feature selection and complex tree-based decision modeling. The LSTM model is completed within 68.90 seconds, illustrating the heavy computational nature of recurrent operations. Similarly, AdaBoost and Basic AE algorithm both take 52.70 seconds and 43.30 seconds, respectively, to indicate their moderate but ad-equately high computational demands. The significantly shorter run time of the suggested model is a result of the success of the proposed hybrid proposed model with the effect of dis-carding unnecessary computations.

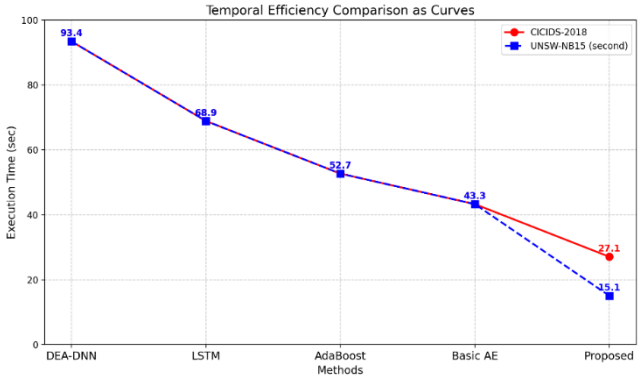

Figure 10. Temporal complexity comparison between state-of-the-art methods and proposed method on CICIDS-2018 and UNSW-NB15 datasets

CONCLUSION

In order to mitigate DDoS attacks in such a complex network setup, in this work, we have put forward a new Hybrid Complex Multilayer Perceptron (HCMLP) model. HCMLP was designed with state-of-the-art multibranch structures, residual connections, dense blocks, and attention mechanism which have been identified to work well for feature extraction, classification and handling class imbalance. The model got precision and recall of 1.00 and F1 score of 1.00 with accuracy of 99.96% on CIC-IDS 2018 dataset. UNSW-NB15 dataset has been used to evaluate the performance of the HCMLP. Results showed precision of 0.965, recall and F1 scores of 0.9645 and accuracy of 96.02percent. Ranking the attacks within 21.6 seconds. In addition, the HCMLP outperformed the current benchmarks in terms of detection time reduction by 15.2%, and better run time. The use of attention mechanism provided a way of performing intuitive feature selection while dense and residual connections enhanced the gradient flow and helped to avoid vanishing gradients and attack pattern shifts.

However, there is still much room for further advancements, and further creativity, in these areas, even though the above-mentioned measures are positive steps.

e-ISSN: 2583-3472

Further research could also be done within the HCMLP framework to deal with scenarios in real time, dynamic networks in which attack patterns evolve over time. Maybe the model can be improved to identify zero-day attacks by exploring how unsupervised and semi supervised learning can be implemented. Possible future work includes the examination of the performance of the HCMLP for large and heterogeneous datasets such as IoT and cloud-based networks and extending the HCMLP for other classification and sparse regression problems. Then the model is tested in practical scenarios for real world applications and the performance of model is evaluated under various network conditions to analyze the reliability of the model. We believe that the directions we outlined in this paper will contribute to the advancement of DDoS detection and the development of more robust and secure networks.

Acknowledgements

Reem Talal Abdulhameed Al-Dulaimi and Ayça Kurnaz Türkben gratefully acknowledge the experts whose insightful suggestions and constructive feedback greatly enhanced the quality of this work.

REFERENCES

[1] S. Chen, Z. Alazab, M. Alazab, and A. Shalaginov, "Distributed Denial of Service (DDoS) Attacks: A Comprehensive Survey," IEEE Transactions on Information Forensics and Security, vol. 15, no. 3, pp. 1234–1247, Mar. 2020.

[2] S. M. Kasongo and Y. Sun, "A Deep Learning Approach for Network Intrusion Detection System," IEEE Access, vol. 8, pp. 12345–12356, 2020.

[3] Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of Intrusion Detection Systems: Techniques, Datasets, and Challenges," Cybersecurity, vol. 2, no. 1, pp. 1–22, 2019.

[4] K. He, X. Zhang, S. Ren, and J. Sun, "Deep Residual Learning for Image Recognition," IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 770–778, 2016.

[5] R. S. Sutton and A. G. Barto, Reinforcement Learning: An Introduction, 2nd ed. Cambridge, MA: MIT Press, 2018.

[6] Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," International Conference on Information Systems Security and Privacy (ICISSP), pp. 108–116, 2018.

[7] M. Shurman, A. Yateem, and R. Khrais, "DoS and DDoS Attack Detection Using Deep Learning and IDS," The International Arab Journal of Information Technology, vol. 17, no. 4A, pp. 655–661, Jul. 2020, doi: 10.34028/iajit/17/4a/10.

[8] U. S. Chanu, K. J. Singh, and Y. J. Chanu, "A dynamic feature selection technique to detect DDoS attack," Journal of Information Security and Applications, vol. 74, p. 103445, Mar. 2023, doi: 10.1016/j.jisa.2023.103445.

[9] N. Ahuja, G. Singal, D. Mukhopadhyay, and N. Kumar, "Automated DDOS attack detection in software defined networking," Journal of Network and Computer Applications, vol. 187, p. 103108, May 2021, doi: 10.1016/j.jnca.2021.103108.

[10] B. Jia and Y. Liang, "Anti-D chain: A lightweight DDoS attack detection scheme based on heterogeneous ensemble learning in blockchain," China Communications, vol. 17, no. 9, pp. 11–24, Sep. 2020, doi: 10.23919/jcc.2020.09.002.

[11] S. Hosseini and M. Azizi, "The hybrid technique for DDoS detection with supervised learning algorithms," Computer Networks, vol. 158, pp. 35–45, Apr. 2019, doi: 10.1016/j.comnet.2019.04.027.

[12] Y. Wei, F. Sabrina, W. Xu, S. Camtepe, J. Jang-Jaccard, and A. Singh, "AE-MLP: A Hybrid Deep Learning Approach for DDoS Detection and Classification," IEEE Access, vol. 9, pp. 146810–146821, Jan. 2021, doi: 10.1109/access.2021.3123791.

[13] B. Jia, Y. Ma, R. Liu, and X. Huang, "A DDoS Attack Detection Method Based on Hybrid Heterogeneous Multiclassifier Ensemble Learning," Journal of Electrical and Computer Engineering, vol. 2017, pp. 1–9, Jan. 2017, doi: 10.1155/2017/4975343.

[14] Y. Gu, K. Li, Z. Guo, and Y. Wang, "Semi-Supervised K-Means DDoS Detection Method Using Hybrid Feature Selection Algorithm," IEEE Access, vol. 7, pp. 64351–64365, Jan. 2019, doi: 10.1109/access.2019.2917532.

[15] J. P. A. Maranhão, J. P. C. L. Da Costa, E. Javidi, C. A. B. De Andrade, and R. T. De Sousa, "Tensor based framework for Distributed Denial of Service attack detection," Journal of Network and Computer Applications, vol. 174, p. 102894, Nov. 2020, doi: 10.1016/j.jnca.2020.102894.

[16] Gwassi, Omar Abboosh Hussein, Osman Nuri Uçan, and Enrique A. Navarro. "Cyber-XAI-Block: an end-to-end cyber threat detection & fl-based risk assessment framework for iot enabled smart organization using xai and blockchain technologies." Multimedia Tools and Applications (2024): 1-42.

[17] S. M. Bellovin, "Security problems in the TCP/IP protocol suite," ACM SIGCOMM Computer Communication Review, vol. 19, no. 2, pp. 32–48, Apr. 1989.

[18] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (IDPS)," NIST Special Publication, vol. 800, no. 94, pp. 1–127, Feb. 2007.

[19] Han, J., Kamber, M., & Pei, J. (2011). Data Mining: Concepts and Techniques. Morgan Kaufmann.

[20] Leevy, J.L.; Khoshgoftaar, T.M. A survey and analysis of intrusion detection models based on CSE-CIC-IDS2018 Big Data. J. Big Data 2020, 7, 104.

[21] Sharma, V., 2022. A study on data scaling methods for machine learning. *International Journal for Global Academic & Scientific Research*, *1*(1), pp.31-42.

[22] Heydarian, M., Doyle, T. E., & Samavi, R. (2022). MLCM: Multi-label confusion matrix. IEEE Access, 10, 19083-19095.

[23] Aronoff, S. (1982). Classification accuracy: a user approach. Photogrammetric Engineering and Remote Sensing, 48(8), 1299-1307.

[24] Y. N. Kunang, S. Nurmaini, D. Stiawan, and B. Y. Suprapto, "Attack classification of an intrusion detection system using deep learning and hyperparameter optimization," J. Inf. Secur. Appl., 2021, doi:10.1016/j.jisa.2021.102804.

[25] P. Lin, K. Ye, and C. Z. Xu, "Dynamic network anomaly detection system by using deep learning techniques," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2019. doi: 10.1007/978-3-030-23502-4_12.

[26] H. Najafi Mohsenabad and M. A. Tut, "Optimizing Cybersecurity Attack Detection in Computer Networks: A

e-ISSN: 2583-3472

Comparative Analysis of Bio-Inspired Optimization Algorithms Using the CSE-CIC-IDS 2018 Dataset," Appl. Sci., vol. 14, no. 3, p. 1044, Jan. 2024, doi: 10.3390/app14031044.

[27] Yang, K., Zhang, J., Xu, Y., & Chao, J. (2020, April). Ddos attacks detection with autoencoder. In NOMS 2020-2020 IEEE/IFIP network operations and management symposium (pp. 1-9). IEEE.

[28] Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. In *Military Communications and Information Systems Conference (MilCIS)*. IEEE.