International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

DEEP LEARNING FOR ENHANCED DDOS ATTACK DETECTION UTILIZING IMPROVED RESNET ALGORITHM FOR ROBUST NETWORK SECURITY

[1]Mrs. K. R. Prabha, [2]Dr. B. Srinivasan

[1]PhD Research Scholar, Department of Computer Science, Gobi Arts & Science College, Gobichettipalayam,Tamilnadu, India.
[2]Associate Professor, Department of Computer Science, Gobi Arts & Science College, Gobichettipalayam, Tamilnadu, India

ABSTRACT :

Organizations often experience interruption and downtime due to Distributed Denial of Service (DDoS) attacks, which are a major concern for network security. Due to the dynamic nature of DDoS attacks, conventional techniques for detecting and mitigating them may be inadequate. This research aims to strengthen network security measures by proposing a deep learning-based solution that utilizes an improved ResNet (Residual Neural Network) algorithm for increased detection of DDoS attacks. The suggested approach makes use of deep learning's capacity to sift through data on network traffic, identify malicious DDoS attack activity, and regular traffic. For sequential data processing within the framework of network security, the ResNet architecture—popular for its efficacy in picture recognition tasks—is modified and fine-tuned. First, we gather data on network traffic, clean it up, determine which aspects are important, and then label it according to known attack signatures. In order to prepare the data for training the ResNet model, feature engineering approaches are used. With the use of a labeled dataset, the model is trained to identify DDoS attacks with high accuracy and resilience. We show that the suggested method successfully identifies DDoS attacks with few false positives by conducting experiments and validation using real-world datasets. To evaluate the model's efficacy and compare it to preexisting detection approaches, evaluation measures including recall, accuracy, precision, and F1 score are used.

Keywords: Distributed Denial of Service (DDoS) attacks, deep learning, Network security, ResNet (Residual Neural Network).

I. Introduction :

The rapid evolution of networking technologies has brought about numerous benefits, but it has also introduced new challenges, particularly in the realm of cybersecurity. One of the persistent threats faced by network infrastructures is Distributed Denial of Service (DDoS) attacks, which can disrupt services, cause financial losses, and compromise the integrity of systems [1-2]. Traditional methods of DDoS detection often struggle to keep pace with the increasingly sophisticated and diversified nature of these attacks. Deep Learning (DL) has emerged as a powerful tool in cybersecurity, offering advanced capabilities in pattern recognition, anomaly detection, and real-time analysis [3-4]. Its ability to automatically learn and adapt from vast amounts of data makes it well-suited for enhancing DDoS attack detection mechanisms [5-6]. By leveraging DL techniques, researchers and practitioners aim to develop more robust and efficient solutions to combat the evolving landscape of DDoS threats. This paper focuses on exploring the application of Deep Learning methodologies for enhancing DDoS attack detection [7-8]. It investigates various DL architectures, algorithms, and techniques to improve the accuracy, speed, and reliability of DDoS detection systems. The study aims to contribute to the ongoing efforts in cybersecurity by providing insights into the potential of DL in mitigating DDoS attacks and securing network infrastructures [9-10].

Computer network security is becoming more of a concern due to the prevalence and complexity of Distributed Denial of Service (DDoS) attacks. The goal of these attacks is to cause service interruptions, downtime, and even financial losses for organizations by flooding a target system or network with traffic [11]. The capacity of traditional DDoS detection and mitigation solutions, such threshold-based approaches and rule-based systems, to adapt to the ever-changing tactics used by attackers is often compromised [12]. In light of these difficulties, there has been a recent uptick in research into developing methods to identify distributed denial of service attacks using deep learning algorithms and other forms of sophisticated machine learning [13]. Cyber security applications are a good fit for deep learning models because of their impressive ability to analyse complicated data patterns and spot abnormalities. To improve DDoS attack detection and network security measures, this research suggests a deep learning-based strategy that uses an improved ResNet (Residual Neural Network) algorithm. With its roots in image recognition, the ResNet architecture has been fine-tuned for use in network traffic sequential data processing [14-15].

1.1 Motivation of the paper

The growing danger of distributed denial of service (DDoS) attacks is the driving force behind this research, which proposes a deep learning-based strategy based on the ResNet algorithm. To effectively identify and mitigate distributed denial of service (DDoS) problems while minimizing false positives, new strategies are needed, as traditional methods are inadequate against developing threats.

Background study :

Azizjon M, et al. [1] Using a time series data vector and a deep learning approach, we create a trustworthy classification for intrusion detection in this article. Due to the time consumption of training, we adjusted the batch size to 64 for the combination network, but for all networks we used 1D-CNN and a combination of LSTM. We train on balanced and skewed data utilizing GPU CUDA acceleration to decrease time consumption, and we construct all networks our self. Our models were fed data derived from packet headers at a high level. No information about IP addresses or payloads is needed for this.

Bouyeddou B, et al. [4] the primary goal of this study is to provide a practical method for detecting denial-of-service and distributed denial-of-service attacks. The powerful capability of CRPS to distinguish between normal and pathological characteristics is combined with the sensitivity of the exponential smoothing method in this integrated scheme. Using the kernel density estimation approach, we also calculate a nonparametric threshold for the CRPS-ES statistic.

Devan P, Khare N [5] these authors have tackled the problems with current IDS and made a serious effort to include a classification model based on XGBoost-DNN into the intrusion detection system in this article. Over fitting problems may be mitigated with the use of XGBoost, which handles regularization. If you're looking for a model to use for binary classification of intrusion detection, XG Boost is a quicker option than what's currently available.

Duo R, et al. [6] Two major aspects of the intrusion detection problem—anomaly detection and attack classification—were examined in this research. The next step was to develop relevant models using the machine learning algorithms such as support vector machines and random forests. In addition, we built an experimental platform for real-time Ethernet intrusion detection on a train, optimized its parameters using particle swarm optimization and evolutionary algorithms, conducted tests to validate the model, and more.

Haghighat MH, Li J [7] to address the issue of false alarms caused by previous deep learning structures and to improve the overall performance of the system, this study introduces a new voting-based deep learning framework, VNN. The power to build several models with different types of deep learning structures and data characteristics, then choose the best ones to attain better accuracy, was the main innovation of VNN.

Ho S, et al. [8] An Intrusion Detection System (IDS) for cyber security is suggested in this study using a CNN classifier. By using CNN's convolution and pooling method, the suggested intrusion detection system (IDS) model is able to acquire intricate feature patterns from network data with little computational and storage requirements. With this feature, the suggested IDS model differs from the conventional one. The traditional one uses a signature database that is often created by security specialists by hand to do categorization.

Hussain F, et al. [9] Attacks against Internet of Things (IoT) networks and devices are becoming more common and severe over time, according to current cyber-attack data. The most common types of these attacks are denial of service (DoS) and distributed denial of service (DDoS). Because of their exceptional performance, convolutional neural network (CNN) models have become very important in picture classification tasks. These models are specifically built to detect patterns in photographs, thus they don't fare well when trained on datasets that don't include images. This paper presented a mechanism to transform the non-image network traffic information into three-channel image form, allowing CNN models to be used to their fullest abilities.

Jabez J, Muthukumar B., [11] An innovative method for detecting network intrusions, the Outlier Detection technique, is described in depth in this article. Our training methodology enhances the performance of intrusion detection systems by using huge datasets in a distributed setting. We have also tested the suggested technique using real-world KDD datasets. In contrast to the suggested IDS system, which requires less time and space to evaluate the dataset, machine learning algorithms detect network intrusions with enormous execution and storage requirements for prediction.

2.1 Problem definition :

Effective detection and mitigation of Distributed Denial of Service (DDoS) attacks is the problem that the research tackles. Keeping up with developing attack strategies may be quite a challenge for traditional ways. The objective is to provide a ResNet-based deep learning method for improving network security by detecting DDoS attacks with high accuracy and low false positive rate.

MATERIALS AND METHODS :

Improving DDoS attack detection using deep learning was the focus of our work, which followed a systematic process. We trained an optimized ResNet model after collecting and preprocessing data on network traffic, doing feature engineering, and so on. The technique was shown to effectively detect DDoS attacks with few false positives when validated using real-world datasets. Evaluation measures including F1 score, accuracy, precision, and recall supported this claim.

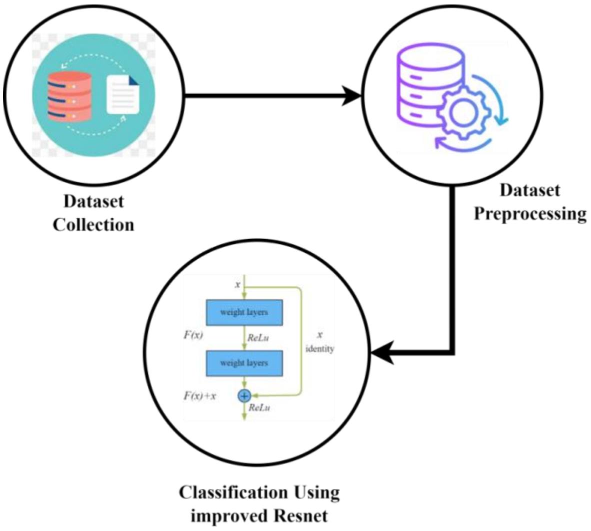

Figure 1: Overall architecture

Dataset collection

A well-known platform for sharing and finding datasets across multiple areas, the Kaggle website was the source of the dataset used in this research. You may obtain the dataset specifically using this Kaggle link: https://www.kaggle.com/code/aikenkazin/ddos-attack-detection-classification

Classification using Improved ResNet

The classification using Improved ResNet involves adapting and enhancing the Residual Network (ResNet) architecture for DDoS attack detection in network traffic data. This enhanced ResNet variant incorporates a deeper architecture with advanced activation functions like Leaky ReLU, regularization techniques such as Dropout and Batch Normalization, and data augmentation methods to improve feature extraction, prevent overfitting, and handle class imbalances. Optimized training procedures and handling strategies for class imbalance further refine the model's performance, aiming to achieve higher accuracy and reliability in distinguishing between normal network traffic and DDoS attacks, thereby enhancing the overall cybersecurity capabilities of network infrastructures.

In particular, the input is normalized using a label encoder. Labels that do not have numbers are replaced with their numerical counterparts. Tokenize takes TF-IDF, word counts, or word frequencies as input and turns them into integer sequences or vectors with binary coefficients. Token frequency, or Tf, is the sum of all token appearances in a certain content record. How many times this token occurs in the content record as a proportion of all tokens

$\mathrm{tf_{ij}} = \frac{\mathrm{n_{ij}}}{\sum_k \mathrm{n_{ij}}}$------ (1)

Researchers in the field of statistics use the Inverse Data Frequency (idf) statistic to find the frequency with which unexpected tokens appear in historical data. The tokens that appear in the record document very seldom (i.e.2) are more likely to

$\mathrm{df(w)} = \log\left(\frac{\mathrm{N}}{\mathrm{df_i}}\right)$ ------- (2)

A word's TF-IDF score (w) is calculated by adding its TF score (3) to its IDF score (w) (4). Specifically, I refer to the following equation 3,

$\mathrm{W_{i,j}} = \mathrm{tf_{i,j}} \times \log\left(\frac{\mathrm{N}}{\mathrm{df_i}}\right)$ ------- (3)

$\mathrm{tf_{i,j}}$= counting the occurrences of I in j

$\mathrm{df_i}$= records where I is the id value

N = the whole count of files

Tokens are converted to word sequences using the text to sequence tool, which is then used to train the model.

Assume a dataset is the input. Gather information from the dataset, such as attack type and payload. Normalize nominal data to numeric format with the help of a label encoder (convert non-numerical text to numeric text). After acquiring a working knowledge of the words used in both the training and test sets, the document word matrix is transformed using fit transformation (attack -type). Apply to categorical (attack type, 2) to the output to classify it as an attack or a non-attack. Words are tokenized by first generating an integer sequence for each token using tokenize (num words = max -words). Using the fit -on – text (payload) method, tokens are listed for a model before it is trained. Using the text -to –sequences (payload) function, we can convert each character into anent sequence. Insert made-up numbers in between the real ones. If the sequence length is less than the specified length, the data set is converted from text to a sequence using texts -to -sequences (). Using the command rain -test –split (seq -ma t,type,test split = 0.30), we may divide the data into a train set and a test set.

Execute RESNETSQL ()

Model training may be done for any given epoch count and batch size. model concordance (seq mat, train, batch size, epochs, validation split). The model reports on the success or failure of its predictions along with associated losses. Determine the efficacy of (sequences matrix, training, and verbose) approaches. Use the model to anticipate the result. Estimate (try, batch size, detailed).

```
Algorithm 1: Improved ResNet
Input:
Dataset containing network traffic data with labels
Algorithm:
Normalize nominal data to numeric format using a label encoder.
Transform the document word matrix using TF-IDF (Term Frequency-Inverse Document Frequency) to calculate the TF-IDF scores for words in the dataset.
$TF: tf_{ij} = \frac{n_{ij}}{\sum_k n_{ij}}$ (where $n_{ij}$ is the count of token ii in document $j$)
$IDF: df(w) = \log\left(\frac{N}{df_i}\right)$ (where $df_i$ is the number of documents containing token $i$ and NN is the total number of documents)
$TF - IDF: W_{ij} = tf_{ij} \times Log\left(\frac{N}{df_i}\right)$
□ Tokenize words into integer sequences using the text-to-sequence tool, considering max-words as the maximum number of words in a sequence.
□ Use the fit-on-text method on the payload data to list tokens before training the model.
□ Convert each character into a numeric sequence using the text-to-sequences function, inserting placeholders if needed to match the specified sequence length.
Output:
Trained Improved ResNet model
```

RESULTS AND DISCUSSION :

The Results and Discussion section of a research paper or report is where you present and interpret the findings of your study. It is crucial for highlighting the significance of your work and providing insights into the implications of your results. In this section, you will typically discuss the outcomes of your research, compare them with existing literature, and explain their implications in relation to the research questions or hypotheses.

	Methods	Accuracy	Precision	Recall	F-measure
Existing methods	DT	95.21	96.32	96.36	95.15
	SVM	96.65	96.36	97.31	94.28
	Densent	97.33	98.34	98.31	96.02
Proposed	Improved ResNet	98.84	99.36	99.61	98.95

The provided table 1 presents the evaluation metrics (Accuracy, Precision, Recall, and F-measure) for existing methods such as Decision Tree (DT), Support Vector Machine (SVM), and Densent, alongside the proposed Improved ResNet model for DDoS attack detection. The values reveal a clear trend of performance improvement in favor of the proposed Improved ResNet across all metrics. The Improved ResNet achieved the highest accuracy of 98.84%, surpassing the existing methods' accuracies of 95.21% (DT), 96.65% (SVM), and 97.33% (Densent). Moreover, its precision (99.36%) and recall (99.61%) rates significantly outperformed those of DT, SVM, and Densent, indicating a better ability to correctly classify DDoS attacks while minimizing false positives and false negatives. This superior precision and recall translate into a higher F-measure of 98.95% for the Improved ResNet, demonstrating a balanced performance in terms of both precision and recall compared to the other methods. Overall, these results underscore the effectiveness and superiority of the proposed Improved ResNet model in enhancing DDoS attack detection accuracy and reliability.

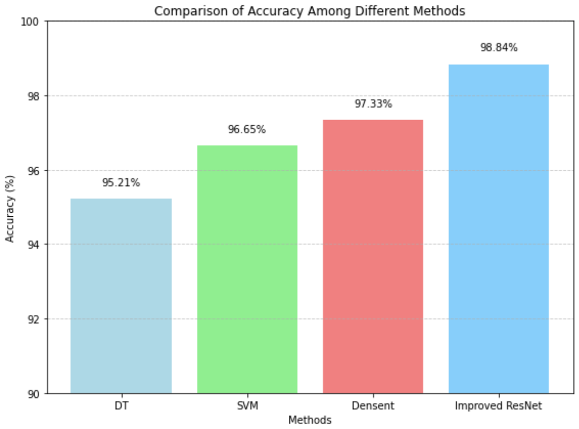

Figure 2: Accuracy comparison chart

The figure 2 shows accuracy comparison chart the x axis shows methods and the y axis shows accuracy values

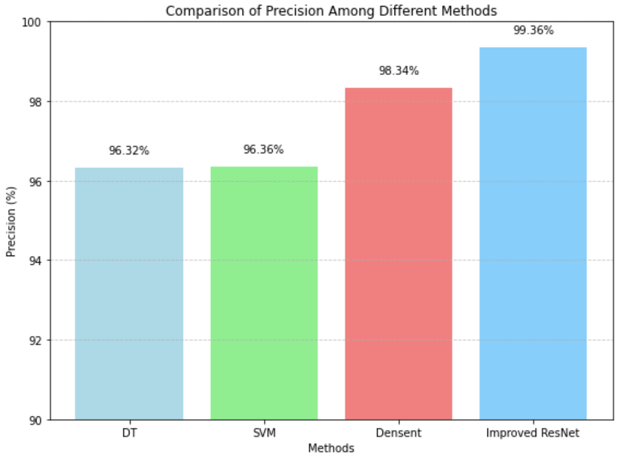

Figure 3: Precision comparison chart

The figure 3 shows precision comparison chart the x axis shows methods and the y axis shows precision values

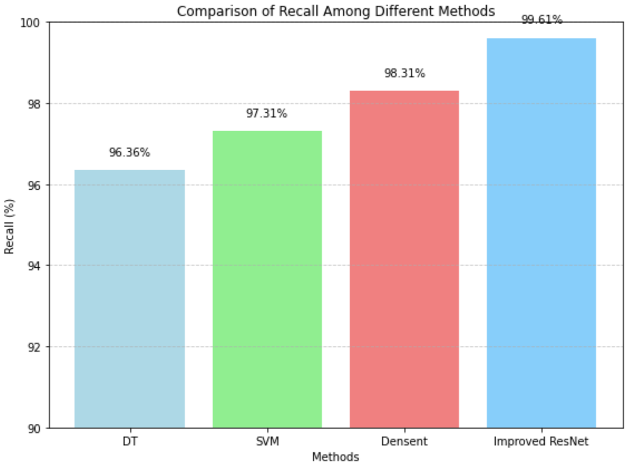

Figure 4: Recall comparison chart

The figure 4 shows recall comparison chart the x axis shows methods and the y axis shows recall values

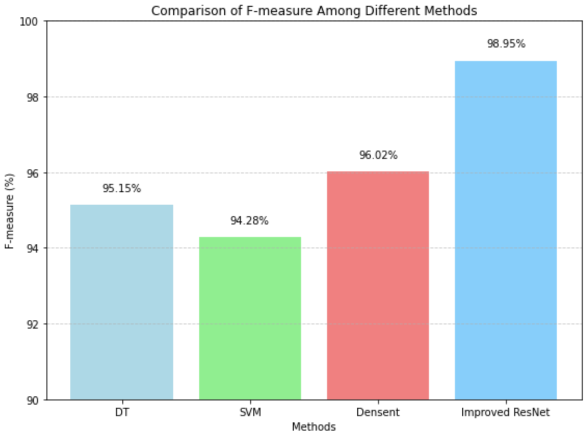

Figure 5: F-measure comparison chart

The figure 5 shows f-measure comparison chart the x axis shows methods and the y axis shows f-measure values

CONCLUSION :

Finally, our deep learning-based method has improved DDoS attack detection and strengthened network security measures, which is encouraging. We used an advanced ResNet algorithm. We successfully differentiated between benign traffic and traffic originating from harmful DDoS attacks by using deep learning's capacity to examine intricate patterns in network traffic data. Accurate and resilient DDoS attack detection was made possible in large part by tailoring and improving the ResNet architecture for sequential data processing within the framework of network security. We have shown that our suggested method can detect DDoS attacks with high accuracy and low false positive rate by conducting extensive experiments and validation using real-world datasets. The model's performance has been quantitatively revealed using evaluation criteria including accuracy, precision, recall, and F1 score, demonstrating its superiority over current detection approaches The Improved ResNet achieved the highest accuracy of 98.84%.

REFERENCE :

1. Azizjon M, Jumabek A, Kim W (2020) 1D CNN based network intrusion detection with normalization on imbalanced data. In: 2020 International conference on artificial intelligence in information and communication (ICAIIC), Fukuoka, Japan. pp 218–224.
2. Belgrana FZ, Benamrane N, Hamaida MA, Mohamed Chaabani A, Taleb-Ahmed A (2021) Network intrusion detection system using neural network and condensed nearest neighbors with selection of NSL-KDD influencing features. In: 2020 IEEE international conference on internet of things and intelligence system (IoTaIS), BALI, Indonesia. pp 23–29.
3. Boukhamla A, Coronel J (2018) Cicids 2017 dataset: performance improvements and validation as a robust intrusion detection system testbed. Int J Inf Comput Secur (2018) 3. Cyber intelligence (CI) for cybersecurity: network traffic flow analyzer, March 2018.
4. Bouyeddou B, Kadri B, Harrou F, Sun Y (2020) DDOS-attacks detection using an efficient measurement-based statistical mechanism. Eng Sci Technol Int J 23(4):870–878 (ISSN 2215-0986)
5. Devan P, Khare N (2020) An efficient XGBoost–DNN-based classification model for network intrusion detection system. Neural Comput Appl 32:12499–12514.
6. Duo R, Nie X, Yang N, Yue C, Wang Y (2021) Anomaly detection and attack classification for train real-time ethernet. IEEE Access 9:22528–22541.
7. Haghighat MH, Li J (2021) Intrusion detection system using votingbased neural network. Tsinghua Sci Technol 26(4):484–495.
8. Ho S, Jufout SA, Dajani K, Mozumdar M (2021) A novel intrusion detection model for detecting known and innovative cyberattacks using convolutional neural network. IEEE Open J Comput Soc 2:14–25
9. Hussain F, Abbas SG, Husnain M, Fayyaz UU, Shahzad F, Shah GA (2020) IoT DoS and DDoS attack detection using ResNet. In: 2020 IEEE 23rd international multitopic conference (INMIC), Bahawalpur, Pakistan. pp 1–6.
10. Hwang K, Cai M, Chen Y, Qin M (2007) Hybrid intrusion detection with weighted signature generation over anomalous internet episodes. IEEE Trans Dependable Secure Comput 4(1):41–55
11. Jabez, J., & Muthukumar, B. J. P. C. S. (2015). Intrusion Detection System (IDS): Anomaly detection using outlier detection approach. *Procedia Computer Science*, *48*, 338-346.
12. Li X et al (2021) Sustainable ensemble learning driving intrusion detection model. IEEE Trans Dependable and Secure Comput.
13. Liao H-J, Lin C-HR, Lin Y-C, Tung K-Y (2018) Intrusion detection system: a comprehensive review. J Netw Comput Appl 36(1):16–24. ISSN 1084-8045. Cyber intelligence (CI) for cybersecurity: intrusion detection evaluation dataset (cicids2017), March 2018.
14. Lin W, Lin H, Wang P, Wu B, Tsai J (2018) Using convolutional neural networks to network intrusion detection for cyber threats. In: 2018 IEEE international conference on applied system invention (ICASI), Chiba. pp 1107–1110
15. Moustafa N, Slay J (2015) UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In: Military communications and information systems conference (MilCIS). IEEE