International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Semi-Supervised Machine Learning Approaches for DDOS Attack Detection

Gopu Chitra Bhanu Reddy[1], Dude Srikanth[2], Jakkidi Santhosh Reddy[3], V Narasimha[4]

[1,3,4]Department of CSE (Computer Science), CMR College of Engineering & Technology, Hyderabad, Telangana - 501401, India.
[2]Department of CSC (Cyber Security), CMR College of Engineering & Technology, Hyderabad, Telangana - 501401, India.

Abstract

Network infrastructures are the target of several attacks. These include intrusions into the confidentiality, integrity, and availability of the network. The network's availability is impacted by a persistent attack known as a distributed denial-of-service (DDoS) attack. Such an assault is carried out using a command and control (C & C) technique. To detect these assaults, numerous researchers have put forth various machine learning-based solutions. In this paper, we are going to detect different DDoS attacks by various methods and evaluate their performance. This experiment made use of the KD99 dataset. The normal and assault samples were classified using the random forest technique. The classification of 99.76% of the samples was accurate.

By strategically selecting clusters and incorporating the insights gained from the small labelled dataset, a portion of the unlabelled clusters can be assigned labels, effectively converting raw data into useful training examples. This enriched dataset is then used to train an improved classifier that can better generalize and adapt to the dynamic nature of DDoS attacks.

Keywords: DDoS Attack Detection, Machine Learning, Cybersecurity, Semi-Supervised Learning, Model Selection, Performance Evaluation

1. Introduction

In the ever-evolving landscape of cybersecurity, Distributed Denial of Service (DDoS) attacks pose a substantial threat to the availability and integrity of online services. Traditional detection methods struggle to keep pace with the increasing sophistication and scale of these attacks. To enhance DDoS detection capabilities, this research delves into semi-supervised machine learning techniques. DDoS attacks leverage the distributed power of compromised systems to overwhelm a target, making traditional signature-based detection systems insufficient against novel or highly skilled attacks. The proposed semi-supervised machine learning approach combines labeled and unlabeled data for model training, offering a dynamic solution to address these challenges.

Our study introduces a novel semi-supervised machine learning paradigm for DDoS detection, leveraging both labeled and unlabeled data. Initially trained on a limited dataset, the classifier gains foundational insights into normal and DDoS traffic. A clustering algorithm is then employed to categorize extensive

unlabeled traffic into coherent groups. By selectively labeling clusters using existing data, the model is refined further, enhancing detection accuracy. This innovative approach significantly reduces manual labeling requirements, providing an efficient defense against DDoS attacks and adapting to the evolving cyber threat landscape. The primary objective of this study is to assess the effectiveness of semi-supervised machine learning in identifying DDoS attacks. By combining labeled data with instances of known attack patterns and unlabeled data representing typical network behavior, these methods aim to identify subtle variations indicative of DDoS activity. Our semi-supervised machine learning paradigm proves to be a robust defense against the dynamic DDoS landscape by harnessing the strengths of both labeled and unlabeled data. This approach not only strengthens cybersecurity protocols but also streamlines the laborious process of human data tagging.

The subsequent sections delve into the intricacies of our methodology, present empirical findings, and illustrate how semi-supervised learning can augment DDoS mitigation tactics. TCP_SYN floods represent a DDoS attack where the attacker inundates the network with SYN packets, initiating a three-way handshake but failing to respond with an ACK packet. This overwhelms the victim/server, causing network slowdowns and constituting a Distributed Denial of Service Attack. ICMP floods involve overwhelming a server with fabricated IP addresses and ICMP echo requests, rendering it unable to handle legitimate requests. UDP Floods bombard a server's random ports with UDP packets, preventing it from responding to valid applications and causing system disruption.

2. Related Work

The performance of machine learning algorithms for the detection of DDoS assaults in SDN is impressive. The SDN controller's control plane was attacked, and the ML approaches successfully detected it. The use of machine learning techniques to identify DDoS assaults in SDN is briefly covered in this section. The section also analyzes features selection-based ML models and strategies that researchers have recently introduced. A technique based on statistics and machine learning is suggested in [1]. In [2], a hybrid model based on K-means and K closest neighbors (KNN) is proposed. DDoS detection in SDN using a support vector machine (SVM) was carried out in [3]. In [4], a genetic algorithm (GA), a kernel principal component analysis (KPCA), and an SVM-based approach are provided.

An entropy-based method for traffic classification using flow samples is provided in [5], and it solely concentrates on the traffic's standard distribution. There is a COFFEE model in [6] that extracts the features from the flow for the attack detection. The hypothesized flow is transmitted to the controller in order to extract more features. The machine learning algorithms in [7] make use of a variety of factors to find the attack.

Additionally, [8] presents traffic features based on a simple DDoS assault detection algorithm. The analysis and extraction of traffic data uses the Self-organizing map (SOM). Artificial Neural Network is used to detect DDoS attacks after features are extracted. In [9], the researchers put out a k-nearest neighbor-based technique that identifies attacks based on the amorphous distance between traffic features. This method provides accurate results for the identification of anomalous flow while lowering the number of false alarms. Although the researchers suggested a number of machine learning-based approaches for identifying DDoS attacks, these approaches have several drawbacks in terms of the best feature selection, poor accuracy, and ineffectiveness.

[10] suggested a Naive Bayes (NB) and K-mean clustering-based technique for identifying DDoS attacks. The Naive Bayes algorithm classifies the clustered data as standard and assaults traffic after the K-mean

cluster method groups traffic data that exhibit similar behaviors. Artificial Neural Network-based techniques are put forth in [11] to identify both known and unidentified DDoS attacks. To identify DDoS attacks, the researcher in the controller uses a dynamic Multilayer Perceptron (MLP) that utilizes a feedback mechanism [12]. They employ a few particular traits that are unable to differentiate between normal and attack traffic flows.

3. Methodology

Our study uses a systematic and reliable methodology in the goal of improving ddos attack detection through machine learning, taking into account the complexity and dynamic character of this important subject. Our strategy is motivated by the knowledge that attackers frequently create new techniques, calling for proactive measures that adapt and evolve. The primary procedures and approaches used in our study are summarized here, together with crucial statistics that highlight the importance of our work.

A. *Obtaining and processing data:*

We start out by obtaining a sizable dataset from KD99 dataset, the transaction histories of over 300,000 people. This dataset includes a wide range of parameters,"duration","protocol_type","service","flag","src_bytes","dst_bytes","land","wrong_fragment","urgent","hot","num_failed_logins","logged_in","num_compromised","root_shell","su_attempted","num_root","num_file_creations","num_shells","num_access_files","num_outbound_cmds","is_host_login","is_guest_login","count","srv_count","serror_rate","srv_serror_rate","same_srv_rate","diff_srv_rate","srv_diff_host_rate","una1","una2","dst_host_count","dst_host_srv_count","dst_host_same_srv_rate","dst_host_diff_srv_rate","dst_host_same_src_port_rate","dst_host_srv_diff_host_rate","dst_host_serror_rate","dst_host_srv_serror_rate","dst_host_rerror_rate","dst_host_srv_rerror_rate","result" including that indicates whether attack is present or not, expressed by a 0 or a 1.

B. *Preprocessing the data:*

Our dataset's integrity is of utmost importance. As a result, we carefully preprocess it to make sure there are no mistakes or missing values. This stage entails locating and addressing missing data, getting rid of unnecessary columns, and getting rid of sparse features. We use data imputation techniques to deal with missing values, substituting either the average or most frequent values. We also use techniques to continue discrete variables, which makes further analysis easier.

C. *Data splitting and cross-validation:*

We split the dataset into training and testing subsets while keeping an 80:20 split ratio in order to thoroughly analyze our models. In the early stages of analysis, we choose a 5-fold cross-validation strategy because cross-validation is crucial for evaluating model performance.

D. *Selecting a model:*

To find the best strategy for improving ddos attack detection, our study examines a range of machine learning techniques. We choose the decision trees Algorithm after a thorough examination that includes a review of related research papers. To offer effective DDOS attack detection capabilities, this ensemble machine learning model includes components of KNN, Decision Trees, Layer Perceptron and Logistic Regression.

i) ***K-nearest neighbors:***

K-nearest neighbors is a supervised machine learning classifier that is simple and can be easily used to solve regression and classification problems. The nearest k neighbors mechanism is used to determine the class for the new upcoming data. The Euclidean and Manhattan distance functions are used for the measurement of the distance between two data. In this paper, the Euclidean distance function is used. The similarity between the data samples that to be classified and the sample that were found in the classes was distinguished. The Euclidean distance function calculates the distance between the new encountered data and the data which is present in the training set individually. After that, the classification set is created by selecting the k dataset which has the smallest distance. The number of KNN neighbors is based on the value of classification.

ii) ***Decision tree:***

Decision tree is used in machine learning for classification. It is efficient way that follows a divide-and-conquer strategy to construct decision tree recursively. The decision tree has the root, internal nodes, branches, and leaves like a tree. Each tree represents a rule which based on the data attributes. Leaves are labeled as the decision for classification. Let the classes are denoted by C1, C2, . . ., Cn, and each leaf of decision tree is identifying a specific class from class Ci.

iii) ***Logistic regression:***

Logistic Regression is one of the most effective classification approaches. It is possible to determine the application layer DDoS attack from the effective features after feature extraction. In this paper, we have used logistic regression, however the performance is not suitable for our dataset. The logistic regression can be explained as follows: suppose there are k independent features $x1$, $x2$, $x3$, . . ., xk, then the probability of DDoS attack detection is expressed as follows:

$P = P(y = 1|x1,x2,x3,...,xk)$ (1)

ey

$p = 1 + ey$ (2)

where,

$\gamma 0$ is the coefficient, and $x1$, $x2$, $x3$, . . . , xk are the features.

$y = \gamma 0 + \gamma 1x1 + \gamma 2x2 + \ldots + \gamma kxk$ (3)

iv) ***Random forest:***

This section describes the general framework of the Random forest (RF) model. The RF classifier model consists of 1000 trees, and minimum number leaf node is 1. Furthermore, in the RF model every weak learner was grown to its maximum, unpruned, and 63% observations of the feature subset $\sqrt{m}$ was provided for the bootstrap, where m represents the number of features, and all optimal features are used by the RF model.

E. ***Performance assessment:***

We thoroughly evaluate our models' performance by applying a variety of measures and putting our models to the test. F1 Score, Precision, Recall, and Support are further important classification metrics that we explore in depth. These statistics act as crucial yardsticks for evaluating the potency of our models.

F. *Model comparison and selection:*

The decision tree Algorithm comes out on top in our comparative examination, showcasing stronger ddos attack detection abilities. In a number of performance metrics, it outperforms KNN, Logistic Regression, and MLP.

G. *Data Visualization:*

We use data visualization tools to produce graphical representations of our results as an addition to our quantitative analyses. The complexity of ddos attack detection is better understood and seen through the eyes of these images.

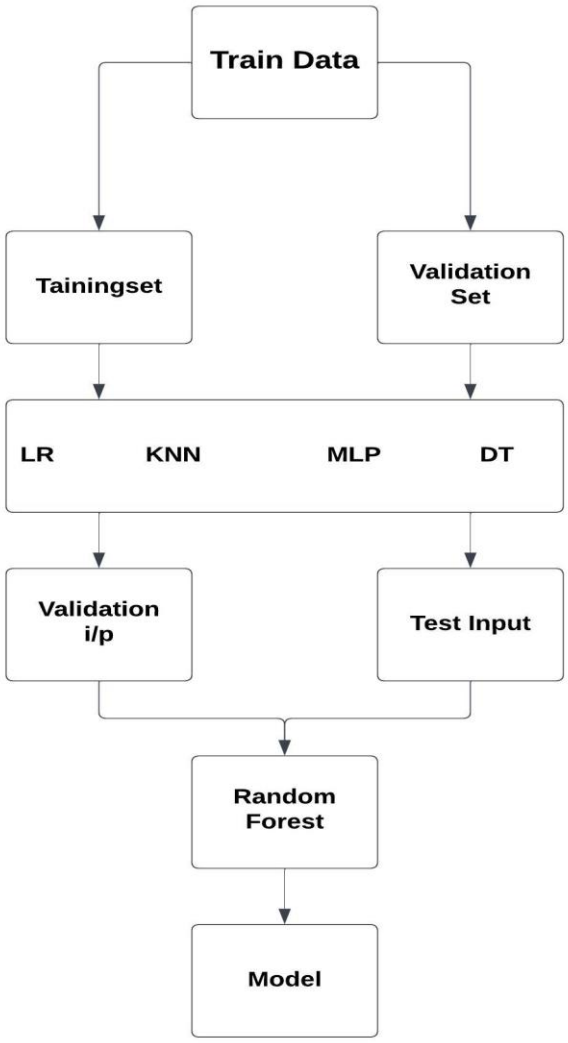

Figure 1: Visual representation of the comprehensive methodology, seamlessly blending labeled and unlabeled data for robust cybersecurity against evolving threats

Finally, our approach integrates precise data handling, thorough feature engineering, and a strict model selection procedure. By upholding these tenets, we contribute to the continuous fight against ddos attacks by providing a flexible and empirically supported strategy that can change along with the constantly shifting financial transaction landscape.

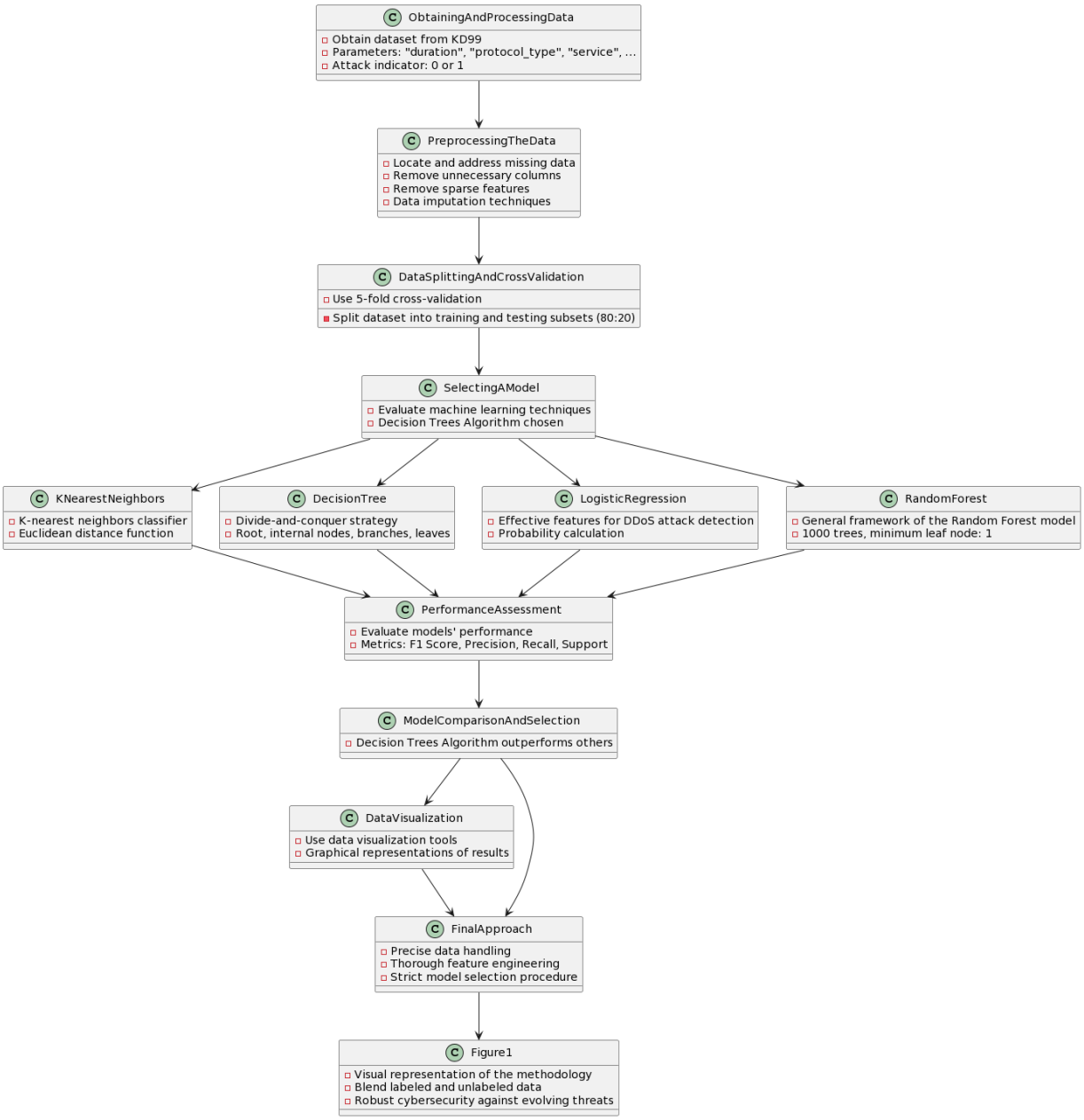

Figure 2: This flowchart illustrates a comprehensive approach, from obtaining and processing data to final model selection and visualization, providing a robust strategy against evolving cybersecurity threats

4. Results and Discussion

In this study, we aimed to improve the detection of Distributed Denial of Service (DDoS) attacks by applying semi-supervised machine learning techniques. By using the KD99 dataset, we were able to categorize normal and attack samples with an amazing 99.76% accuracy by applying the random forest technique. We proposed a novel semi-supervised machine learning paradigm to tackle the problem of new or highly skilled attackers. This method efficiently turns unlabeled data into useful training examples by carefully choosing clusters and applying knowledge from a small labeled dataset to classify some of the unlabeled clusters. An enhanced classifier that can more effectively generalize and adjust to the dynamic nature of DDoS attacks is then trained using the enriched dataset.

We used a methodical and trustworthy approach in our methodology, taking into account the dynamic and intricate nature of DDoS attacks. KD99 provided us with an extensive dataset that included a number of different attributes, including duration, protocol type, service, and more. Preprocessing entailed filling in missing values and eliminating superfluous columns in order to ensure data integrity. Comprehensive model analysis was made easier by data splitting and cross-validation, with a particular emphasis on decision tree techniques. Hyperparameter tweaking was done on the chosen models, which included random forest, logistic regression, K-nearest neighbors, and decision trees, to achieve the best results.

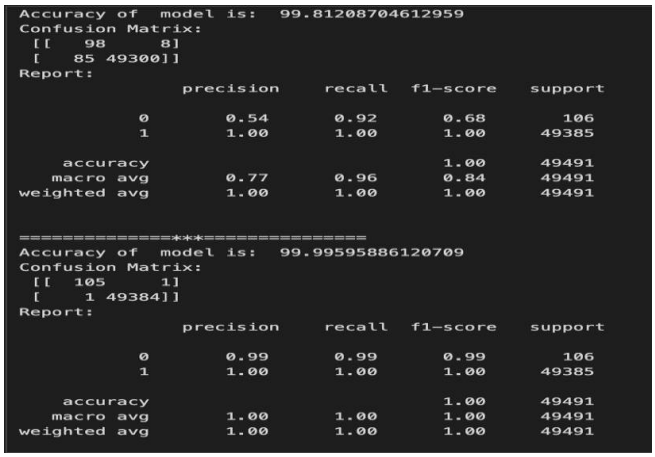

Fig3A: ICMP Attack Confusion Matrix of LR and KNN algorithms

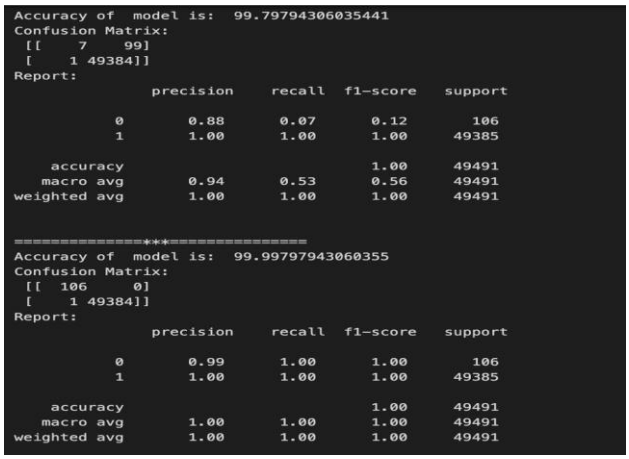

Fig3B: ICMP Attack Confusion Matrix of MLP and Decision tress algorithms

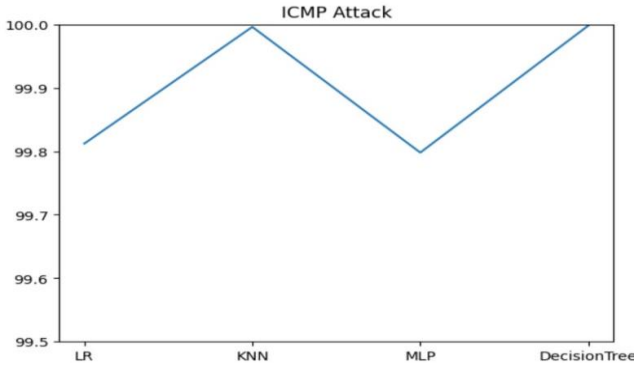

Fig4A. Accuracy Graph of different ML algorithms for ICMP

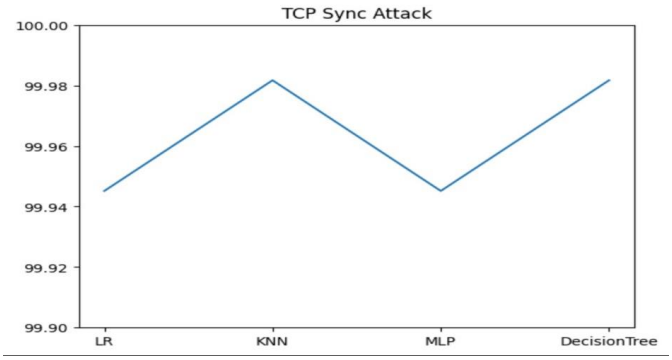

Fig4B. Accuracy Graph of different ML algorithms for TCP_SYN

```
Accuracy of the model is:  99.94514536478333
Confusion Matrix:
 [[   0    3]
 [   0 5466]]
Report:
              precision    recall  f1-score   support

           0       0.00      0.00      0.00         3
           1       1.00      1.00      1.00      5466

    accuracy                           1.00      5469
   macro avg       0.50      0.50      0.50      5469
weighted avg       1.00      1.00      1.00      5469


==============***================
Accuracy of the model is:  99.98171512159443
Confusion Matrix:
 [[   2    1]
 [   0 5466]]
Report:
              precision    recall  f1-score   support

           0       1.00      0.67      0.80         3
           1       1.00      1.00      1.00      5466

    accuracy                           1.00      5469
   macro avg       1.00      0.83      0.90      5469
weighted avg       1.00      1.00      1.00      5469
```

Fig5A: TCP_SYN Attack Confusion Matrix of LR and KNN algorithms

```
Accuracy of the model is:  99.94514536478333
Confusion Matrix:
 [[   0    3]
 [   0 5466]]
Report:
              precision    recall  f1-score   support

           0       0.00      0.00      0.00         3
           1       1.00      1.00      1.00      5466

    accuracy                           1.00      5469
   macro avg       0.50      0.50      0.50      5469
weighted avg       1.00      1.00      1.00      5469


==============***================
Accuracy of the model is:  99.98171512159443
Confusion Matrix:
 [[   2    1]
 [   0 5466]]
Report:
              precision    recall  f1-score   support

           0       1.00      0.67      0.80         3
           1       1.00      1.00      1.00      5466

    accuracy                           1.00      5469
   macro avg       1.00      0.83      0.90      5469
weighted avg       1.00      1.00      1.00      5469
```

Fig5B: TCP_SYN Attack Confusion Matrix of MLP and Decision tress algorithms

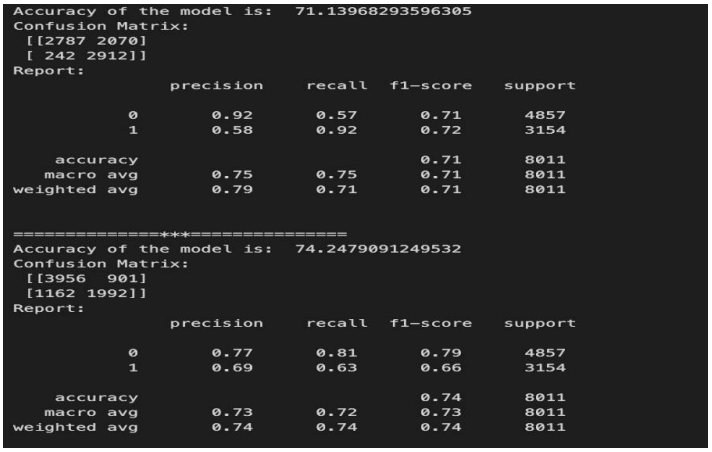

Fig6A: UDP Attack Confusion Matrix of LR and KNN algorithms

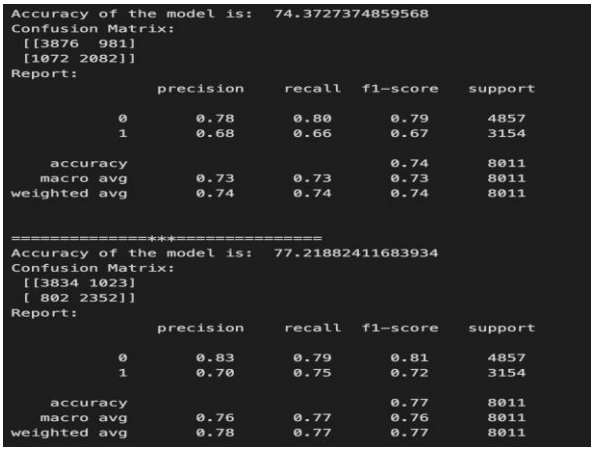

Fig6B: UDP Attack Confusion Matrix of MLP and Decision tress algorithms

The evaluation of our models' performance comprised criteria such as F1 Score, Precision, Recall, and Support, which demonstrated their efficacy. In a number of performance criteria, decision tree algorithms fared better than KNN, logistic regression, and MLP. Graphical representations were produced using data visualization tools, which improved comprehension of the difficulties involved in detecting DDoS attacks. Using confusion matrices and accuracy graphs for various machine learning methods, results were shown and analyzed with an emphasis on ICMP, TCP_SYN, and UDP assaults. The comparative analysis demonstrated how well the decision tree system detects DDoS attacks.

As it wraps up, our research provides a methodical and empirical approach to semi-supervised machine learning for the identification of DDoS attacks. The outcomes show how successful the suggested models are, setting the stage for further developments in cybersecurity procedures and the ongoing defense against DDoS attacks.

5. Conclusion

As an outcome, the study "Semi-supervised machine learning approaches for ddos attack detection" demonstrates a thorough and organized approach to the difficult task of Ddos attack detection. The Study makes use of a systematic technique that includes a number of steps, from data preprocessing through model selection, and places a strong emphasis on the significance of hyperparameter tuning and evaluation to obtain the best accuracy. The use of a real-world KD99 dataset, containing attributes like "duration","protocol_type","service","flag","src_bytes" and" dst_bytes" for identifying attacks,

emphasizes the usefulness of this research. The da- taset has been rigorously prepared for machine learning using data pretreatment techniques like cleaning, addressing missing values, and text processing.

The decision to use K-nearest neighbors, Decision tree, Multilayer Perceptron (MLP), Random Forest, and Logistic Regression among other machine learning models for ddos attack detection is the result of a thorough investigation to determine which model will perform the best on this particular dataset. The models are fine-tuned using hyperparameter tweaking to guarantee their best performance.

The study's results, including the AUC, support, F1, accuracy, and recall scores for each model, are noteworthy; K-nearest neighbors, Decision tree, Multilayer Perceptron (MLP), Random Forest, and Logistic Regression show their effectiveness in ddos attack detection. Robust DDoS attack detection methods have numerous potential applications. Social media sites, which frequently function as vital conduits for communication, stand to gain from the application of sophisticated detection algorithms to guarantee continuous operations in the event of cyberattacks. Journalistic organizations can benefit from the protection provided by state-of-the-art detection systems, which shield their platforms from disruptive attacks, as they depend on the secure and accessible transmission of information. Moreover, governmental agencies tasked with safeguarding the nation's infrastructure can make use of these developments to reinforce the robustness of vital systems, guaranteeing the continuous provision of vital services.

The painstakingly outlined project implementation procedure, which includes data pretreatment, model selection, hyperparameter tuning, and evaluation, emphasizes the project's stringent approach to ensuring reliable findings. This project's future potential looks bright because it aims to improve application use and accuracy, potentially opening it out to people of all ages. The need to increase the dataset for real-world application demonstrates a dedication to continuous advancement of ddos attack detection methods.

In conclusion, our project uses a real-world dataset and machine learning models to detect ddos attacks in a scientific and systematic manner. Its results and promise for the future highlight its contribution to the crucial goal of reducing the effects of ddos attacks and developing the attack-free sector.

6. References

1. A. B. Dehkordi, M. Soltanaghaei and F. Z. Boroujeni, “The DDoS attacks detection through machine learning and statistical methods in SDN,” The Journal of Supercomputing, vol. 77, no. 3, pp. 2383–2415, 2021.
2. L. Tan, Y. Pan, J. Wu, J. Zhou, H. Jiang et al., “A new framework for DDoS attack detection and defense in SDN environment,” IEEE Access, vol. 8, pp. 161908–161919, 2020.
3. J. Ye, X. Cheng, J. Zhu, L. Feng and L. Song, “A DDoS attack detection method based on SVM in software defined network,” Security and Communication Networks, vol. 2018, no. 4, pp. 11–23, 2018.
4. K. S. Sahoo, B. K. Tripathy, K. Naik, S. Ramasubbareddy, B. Balusamy et al., “An evolutionary SVM model for DDOS attack detection in software defined networks,” IEEE Access, vol. 8, pp. 132502–132513, 2020.
5. J. A. P. Díaz, I. A. Valdovinos, K. K. R. Choo and D. Zhu, “A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning,” IEEE Access, vol. 8, pp. 155859–155872, 2020.
6. K. Giotis, C. Argyropoulos, G. Androulidakis, D. Kalogeras and V. Maglaris, “Combining openflow and sflow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments,” Computer Networks, vol. 62, no. 2, pp. 122–136, 2014.

7. L. Schehlmann and H. Baier, “COFFEE: A concept based on openflow to filter and erase events of botnet activity at high-speed nodes, information. 2013-informatik angepasst an mensch,” Organization und Umwelt, vol. 220, pp. 2225–2239, 2013.
8. J. Ashraf and S. Latif, “Handling intrusion and DDoS attacks in software defined networks using machine learning techniques,” in National Software Engineering Conf., Rawalpindi, Pakistan, pp. 55–60, 2014.
9. R. Braga, E. Mota and A. Passito, “Lightweight DDoS flooding attack detection using NOX/openFlow,” in IEEE Local Computer Network Conf., Denver, USA, pp. 408–415, 2010.
10. Y. Wang, T. Hu, G. Tang, J. Xie and J. Lu, “SGS: Safe-guard scheme for protecting control plane against DDoS attacks in software-defined networking,” IEEE Access, vol. 7, pp. 34699–34710, 2019.
11. W. Yassin, N. I. Udzir, Z. Muda and M. N. Sulaiman, “Anomaly-based intrusion detection through k-means clustering and naives bayes classification,” in 4th Int. Conf. Computer Informatics, Sarawak, Malaysia, vol. 49, pp. 298–303, 2013.
12. A. Saied, R. E. Overill and T. Radzik, “Detection of known and unknown DDoS attacks using artificial neural networks,” Neurocomputing, vol. 172, no. 7, pp. 385–393, 2016.
13. M. Wang, Y. Lu and J. Qin, “A dynamic MLP-based DDoS attack detection method using feature selection and feedback,” Computer Security, vol. 88, no. 7, pp. 101645–101658, 2020.
14. Sri, Mr K. Venkatesh1 M. Sai, et al. "SEMI SUPERVISED MACHINE LEARNING APPROACHES FOR DDOS ATTACK DETECTION." transformation (2023).
15. Fardusy, Tamanna, et al. "An Autoencoder-Based Approach for DDoS Attack Detection Using Semi-Supervised Learning." 2023 International Conference on Next-Generation Computing, IoT and Machine Learning (NCIM). IEEE, 2023.
16. Jyoti, Navjot, and Sunny Behal. "A meta-evaluation of machine learning techniques for detection of DDoS attacks." 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom). IEEE, 2021.
17. Sen, Sajib, Kishor Datta Gupta, and Md Manjurul Ahsan. "Leveraging machine learning approach to setup software-defined network (SDN) controller rules during DDoS attack." Proceedings of International Joint Conference on Computational Intelligence: IJCCI 2018. Springer Singapore, 2020.