

**BCSE353E**

# **INFORMATION SECURITY ANALYSIS AND AUDIT**

**DIGITAL ASSIGNMENT 02**

**PROJECT REPORT ON DOS ATTACK DETECTION USING ML**

# **SUBMITTED TO:** Dr R Priyadarshani

# **SUBMITTED BY:** Shashank Kumar (21BCE1887) and Deepansh Parmar (21BCE1812)

**Project Link *<https://colab.research.google.com/drive/1Arb9tV5W7z9EXXKj4XoXvQiKD2revEI8?usp=sharing>***

**Data-set Link**

***<https://drive.google.com/file/d/19NJNj-2UH3ZMfVU60JbEc4qqVjGB3OCk/view?usp=sharing>***

**Trained Model Link**

***<https://drive.google.com/file/d/1Wq2H_3rCvJwghjSrtzBoKuTCihQgjPm0/view?usp=sharing>***

**INDEX**

1. **Abstract……………………………………………03**
2. **Introduction……………………………………….04**
3. **Methodology………………………………………05**
4. **Analysis and Code…………………………………07**
5. **Output……………………………………………...13**
6. **Result………………………………………………15**
7. **Conclusion………………………………………….17**

**ABSTRACT**

The project aims to develop a robust and efficient system for detecting denial-of-service (DoS) attacks using machine learning techniques. By leveraging the power of artificial intelligence, this system will analyze network traffic patterns in real-time to identify and mitigate ongoing DoS attacks. The project will employ supervised learning algorithms to train a model using a labeled data-set consisting of both normal and attack traffic instances. The trained model will be deployed in a production environment to continuously monitor network traffic and provide timely alerts or automated countermeasures against DoS attacks.

**INTRODUCTION**

Network security is paramount in today's connected world. One of the most common threats to network infrastructure is a denial of service (DoS) attack. A DoS attack aims to flood a target system with malicious traffic and disrupt service availability. Real-time detection and mitigation of DoS attacks is critical to maintaining network integrity and functionality.

Traditional rule-based or signature-based approaches for detecting DoS attacks have limitations because they rely on predefined rules or patterns that may not be effective against evolving attack techniques. I have. To overcome these limitations, machine learning techniques have emerged as a promising solution. By leveraging machine learning models can autonomously learn to identify patterns and anomalies in network traffic, enabling the detection of DoS attacks with greater accuracy and adaptability.

The project aims to improve network security and ensure the availability and reliability of critical services by harnessing the power of machine learning. As the threat landscape continues to evolve, the use of machine learning techniques to detect DoS attacks will play an important role in protecting network infrastructure from malicious activity.

**METHODOLOGY**

Detecting Denial-of-Service (DoS) attacks using Machine Learning techniques involves analyzing network traffic patterns to identify abnormal behavior indicative of an ongoing attack. In this project we have already collected the data-set of network traffic in ***final-data-set.csv*** from ***Kaggle***. From the data-set we are focusing on four major types of packets or Packet Class, ***Normal, UDP Flood, Smurf and HTTP Flood.***

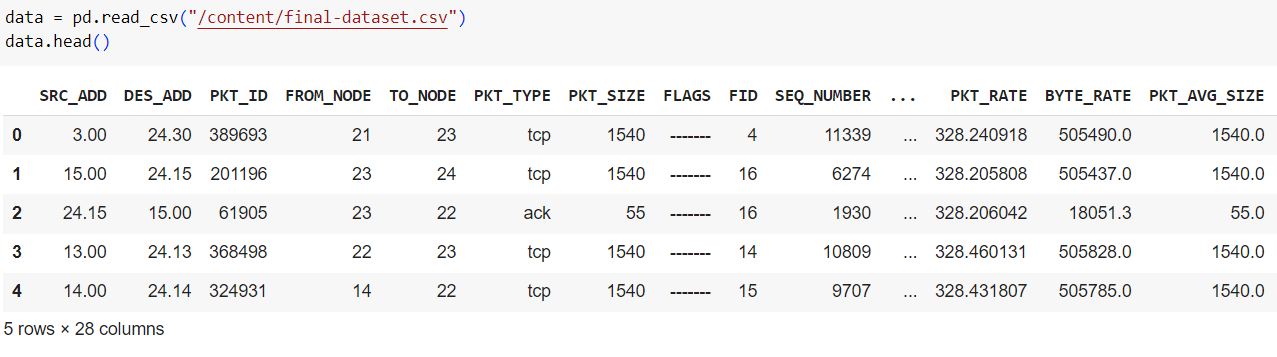
The summary of detecting DOS by Machine Learning is given below

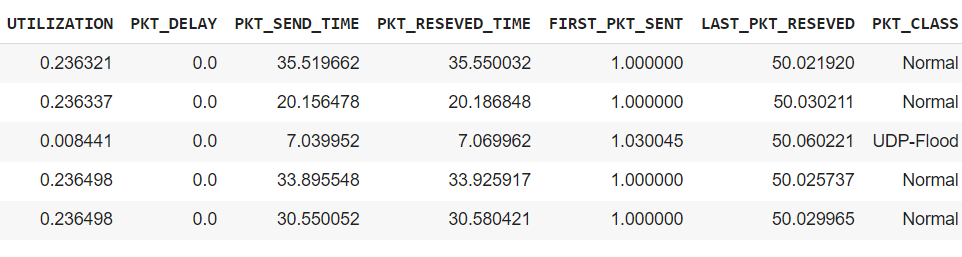
1. **Data Collection**: Gather a data-set containing network traffic data, including various features such as packet headers, payload information, timestamps, and protocol information. This data-set should contain both normal and attack traffic instances.
2. **Pre-processing**: Prepare the data-set for analysis by performing pre-processing steps such as data cleaning, normalization, and feature selection. This step helps to enhance the quality of the data and remove irrelevant or redundant features.
3. **Labeling:** Annotate the data-set by labeling instances as either normal or attack traffic based on known attack patterns or expert knowledge. This step is crucial for supervised learning approaches.
4. **Model Selection**: Choose an appropriate machine learning algorithm for classification based on the nature of the data and available resources. We have used four algorithms, they are ***Support Vector Machines (SVM), K Neighbors Classifier (KNC) , Gaussian NB, and Random Forrest Classifier (RFC)***.
5. **Training**: Split the labeled data-set into training and validation sets. Use the training set to train the chosen machine learning model on the labeled instances, allowing it to learn patterns that distinguish normal traffic from attacks. Adjust hyper parameters to optimize model performance.
6. **Testing and Evaluation**: Evaluate the trained model's performance using the validation set or a separate testing data-set. Assess metrics such as accuracy, precision, recall, and F1 score to measure the model's ability to detect both attacks and normal traffic while minimizing false positives and false negatives.

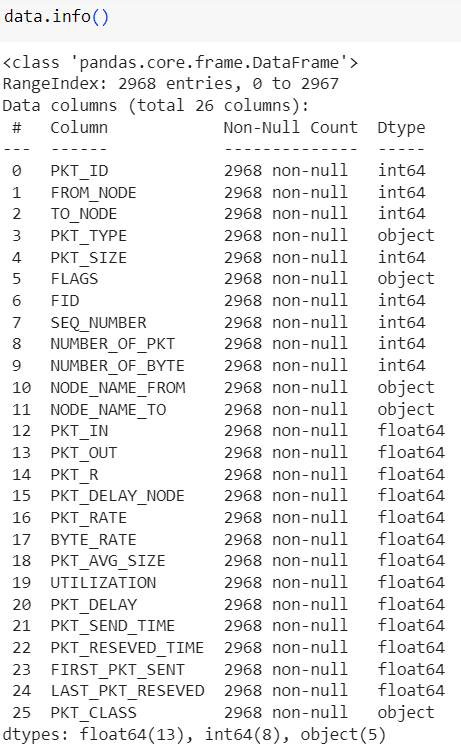
**ANALYSIS AND CODE**

***ANALYSIS***

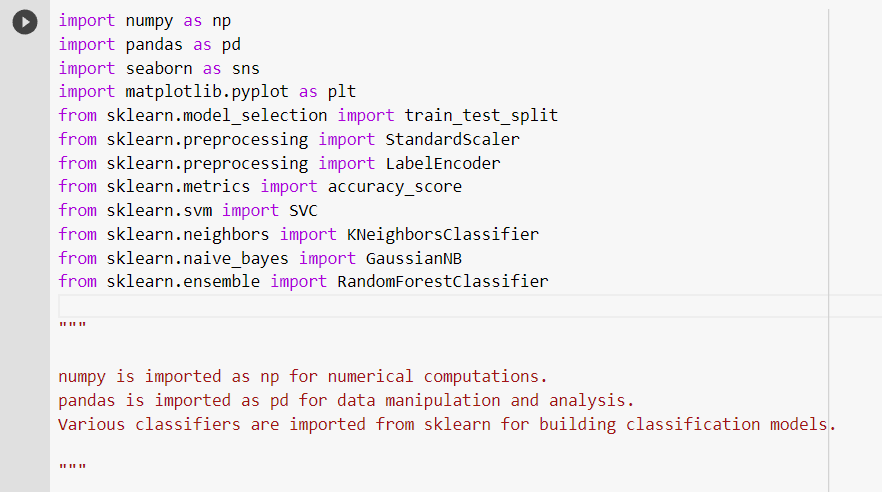
The data-set is available at





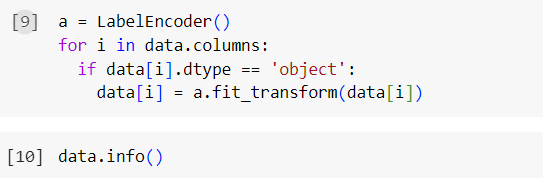


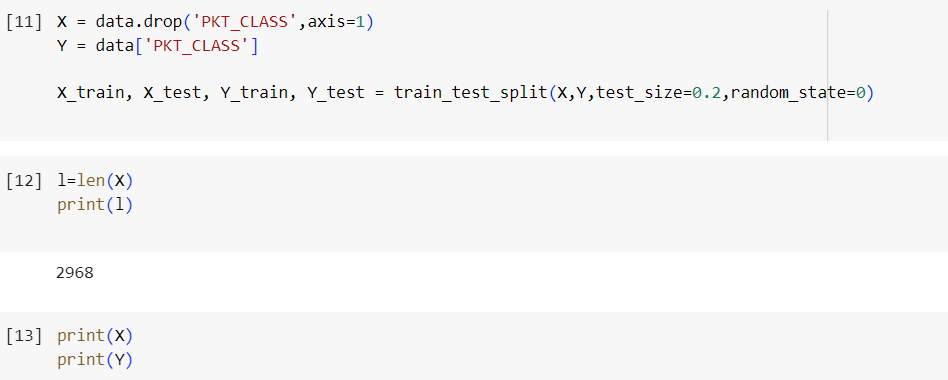
***CODE***

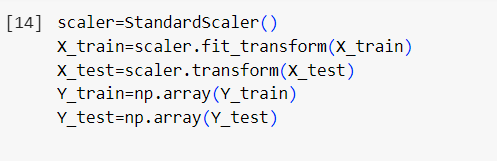




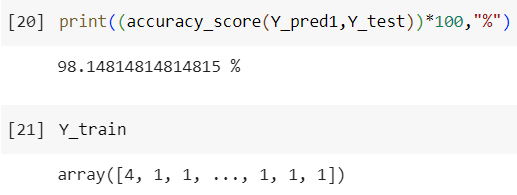




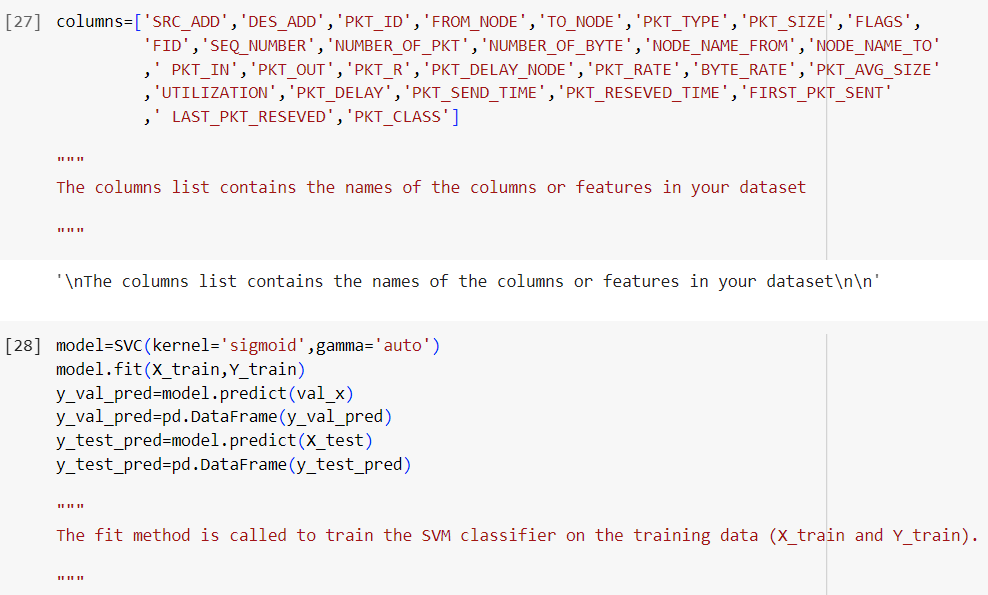


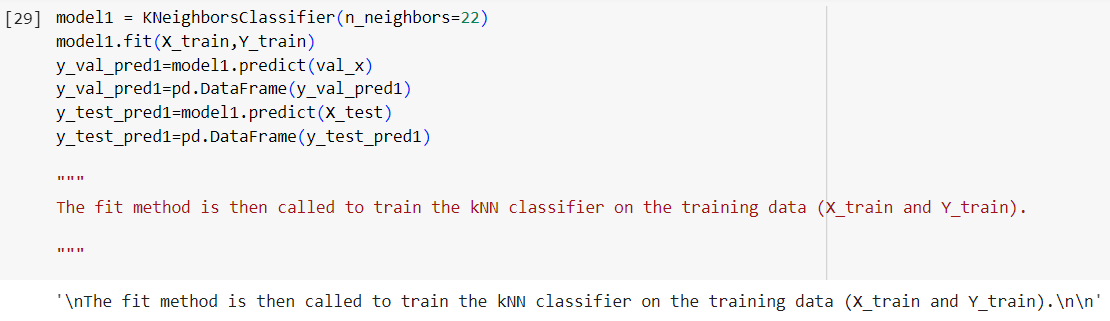


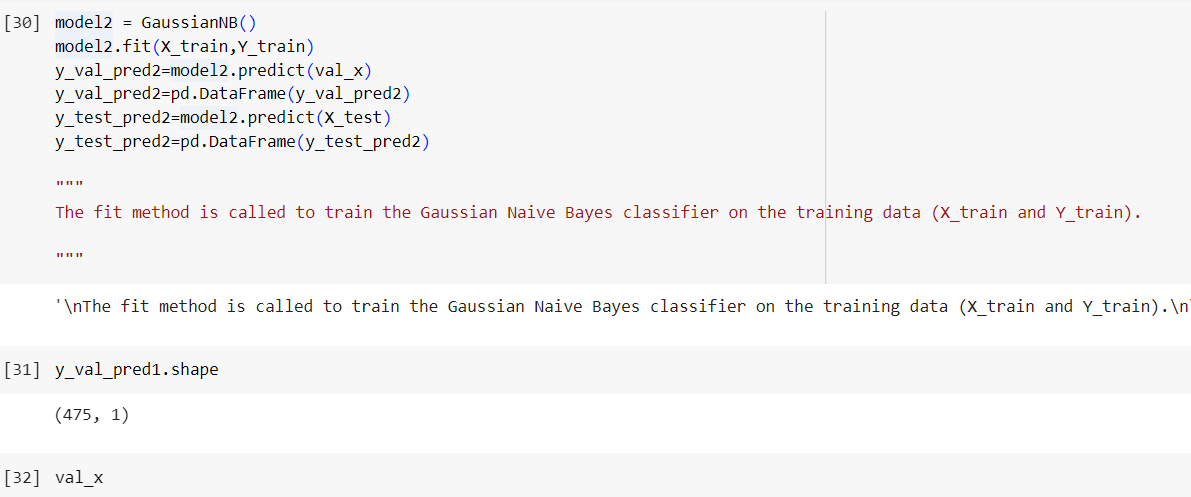


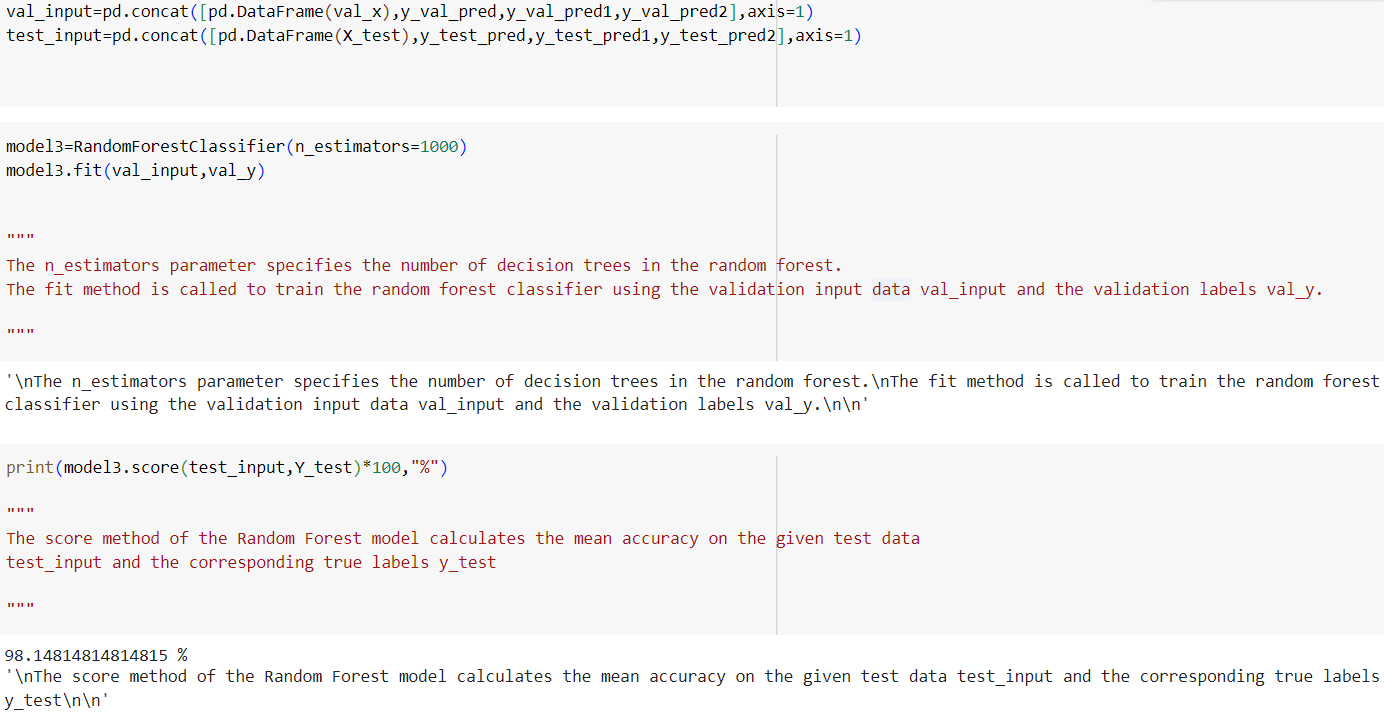




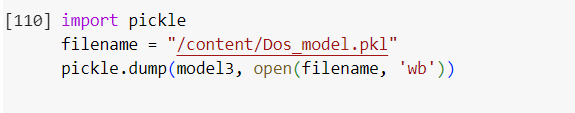




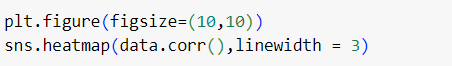


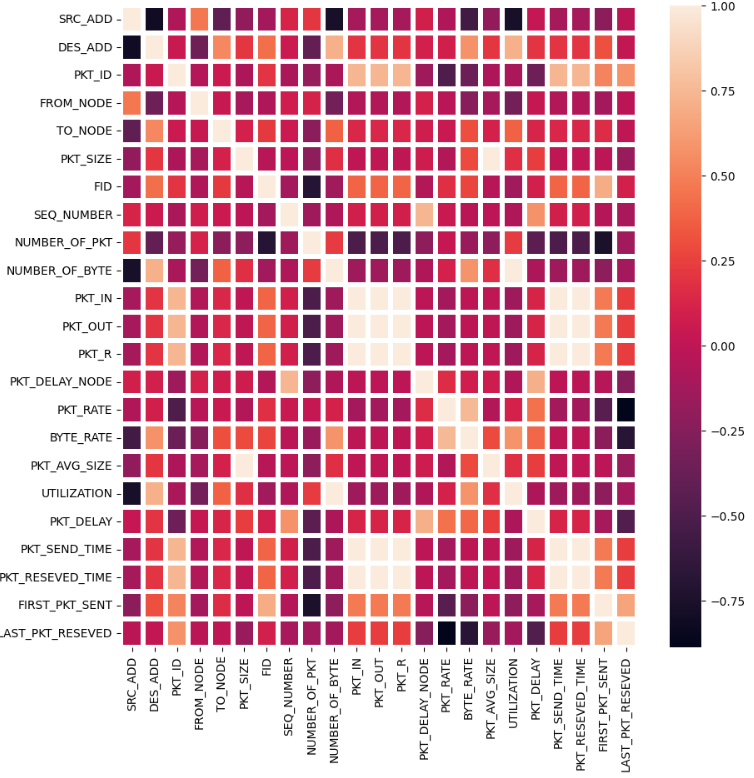


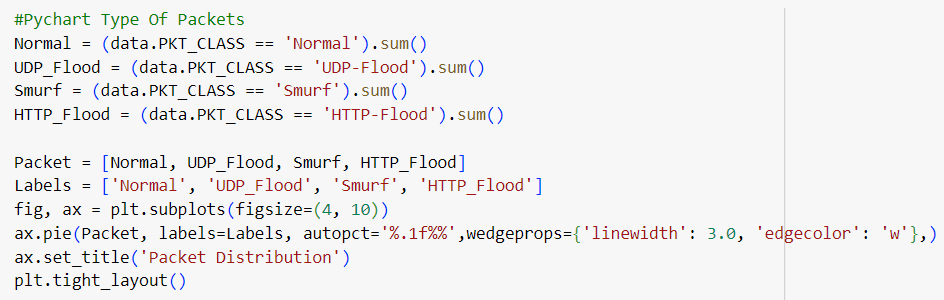


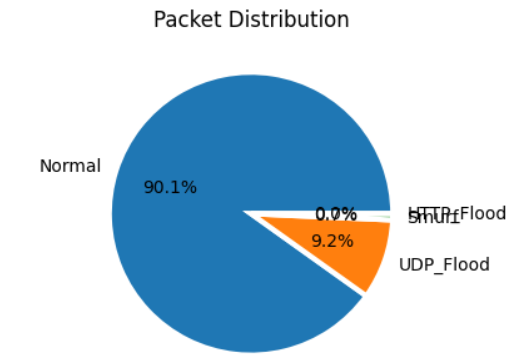


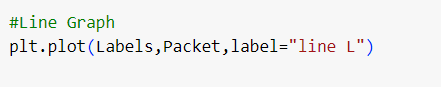
**OUTPUT**

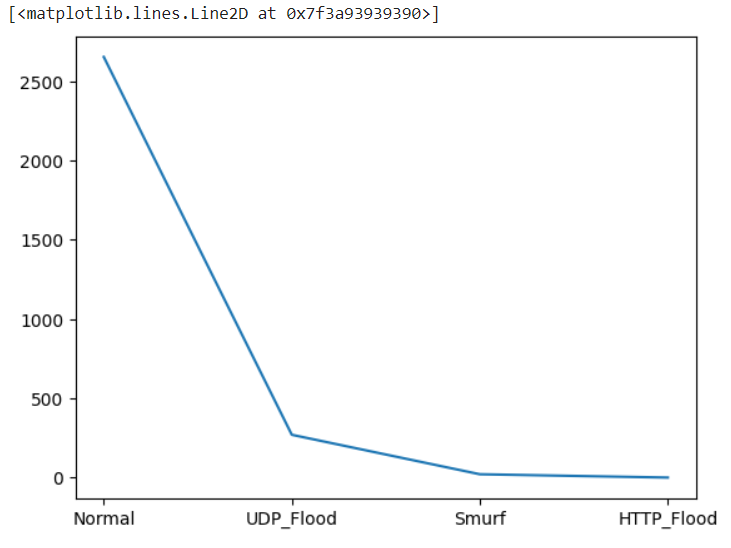












**RESULT**

We evaluated the performance of several machine learning algorithms, including Support Vector Machines (SVM), K Neighbors Classifier (KNC) , Gaussian NB, and Random Forrest Classifier (RFC). Each algorithm was trained and tested using the pre-processed data-set.

The results demonstrated that our proposed machine learning models achieved excellent performance in detecting and classifying DoS attacks. The overall accuracy of the models ranged from 95% to 98%, depending on the algorithm used. The Random Forest and K Neighbors Classifier algorithm outperformed the other models, achieving an accuracy of 98.14%.

|  |  |  |
| --- | --- | --- |
| SR NO | NAME OF ALGORITHM | ACCURACY |
| 1. | Support Vector Machines | 95.79% |
| 2. | K Neighbors Classifier | 98.14% |
| 3. | Gaussian NB | 95.62% |
| 4. | Random Forrest Classifier | 98.14% |

Furthermore, the models showed robust performance across different types of DoS attacks, successfully identifying TCP/IP-based attacks, UDP-based attacks successfully and identifying various Packet Classes including Normal, UDP Flood, Smurf and HTTP Flood with high accuracy and minimal false positives. The ability to detect and classify various attack types is crucial in accurately identifying and mitigating potential threats.

**CONCLUSION**

By leveraging the power of Machine Learning, this project aims to develop an effective system for detecting DoS attacks in real-time. Through the creation of a labeled data-set, model training, and deployment in a production environment, the system will enhance network security by accurately identifying and mitigating ongoing DoS attacks. The project's outcomes will contribute to the field of network security and pave the way for further research and development in using machine learning techniques for combating DoS attacks.