

**Department of Computer Science & Engineering**

**A Project Based Learning**

**On**

**USING MACHINE LEARNING DETECTING DENIAL OF SERVICE**

**ATTACKS**

**Internal Guide By**

**Mr. S.Kiran Kumar Jurru Prabhakar**

**Assistant Professor, (218R1A05G0)**

**Dept of CSE**

# Table Of Contents

* Abstract
* Introduction
* Literature Survey
* Existing System
* Disadvantages
* Proposed System
* Advantages
* System configuration
* Modules
* Module Description
* Data Flow Diagram
* Uml Diagrams
* Output Screenshots
* Conclusion
* References

# Abstract

u The system is used for detecting denial of service attacks on a Network Intrusion Detection System(IDS) using Machine Learning algorithms. The performance of these algorithms are analyzed and compared

u For detecting the attacks, we use KNN, CNN, RF and SVM algorithms.

# Introduction

* Cyber threats are a major concern for any organizations across the globe. One of the most common attack is DOS(Denial Of Service).DOS is a attack that shut down a machine or network, making it inaccessible to its users.
* Therefore, a reliable system with good accuracy is created which is used to detect DOS using Machine Learning Algorithms.

# Literature survey

* **DOS using machine learning approach,[2019]- Saini and Mouhammd**

The machine learning model is validated using the dataset which contains most DOS attacks. For detecting DOS attack a machine learning tool WEKA is used.

* **Machine Learning approach for detecting DOS,[2019]-Doshi Singh and Wani**

For detecting the attack, five ml algorithms are used such as KNN, LSVM, Decision Tree, Random Forest and neural networks are tested and validated using a dataset. The accuracy is above 70%.

* **Use of Block chain to mitigate DOS,[2020]- Swathi Sambangi and Laxmeshwari Gondi**

It compares and examines the existing blockchain-based techniques for defending against DOS attacks. It also used Software Defined Network(SDN) for DOS mitigation.

Existing System

* In existing system, Intrusion Detection System is used to detect DOS.
* IDS is a software that monitors suspicious activity and issues alerts when such activity is discovered.
* **Disadvantages:**
* Encrypted packets are not processed by the IDS.IDS provides information based on the network address that is associated with IP packet. But the address may be fake.

1. IDS can create a large number of false alarms.

# Proposed System

* In proposed system, we use machine learning techniques to pre-processed dataset.
* The algorithms included are SVM, CNN, KNN and RF.

**Advantages:**

1. Protection from malicious attacks on your network.
2. Gives high accuracy while detecting the attacks.
3. Securing confidential information.
4. Prevents users from unauthorized access to the network.

# Hardware Requirements

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  |  |  | | --- | --- | --- | | • | **Processor** | **:** Intel core i5 | | • | **HDD** | **:** 80 GB | | • | **RAM** | **:** 2 GB | | • | **Input Devices** | **:** Keyboard, Mouse | | • | **Output Device** | **:** Monitor | | • | **Speed** | **:** 1.2 ghz | |

# Software Requirements

* **Operating System :** Any Operating System
* **Programming Language :** Python 3.7.0 and More
* **Front End :** HTML/CSS/XHTML
* **Data-Set :** Cyber Attack Dataset

# Modules

u Data Collection u Data Pre-processing u Train and Test Modelling u Attack Detection Model

# Modules Description

* **Data Collection :**

Collect sufficient data samples and software samples.

* **Data Pre-processing :**

Data Augmented techniques will be used for better performance.

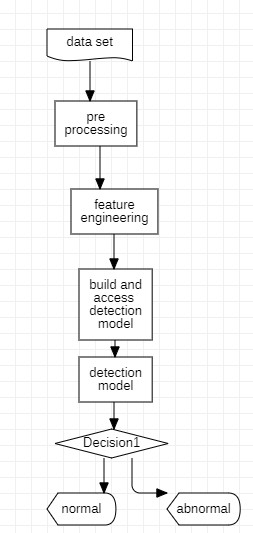
* **Train and Test Modelling :**

Split the data into train and test data Train will be used for training the model andTest data to check the performance.

* **Attack Detection Model :**

Based on the model trained algorithm will detect whether the given transaction isanomalous or not.

# Data Flow Diagram

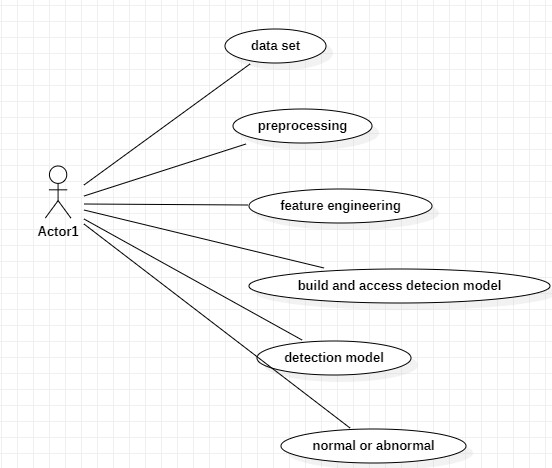


# UML Diagrams

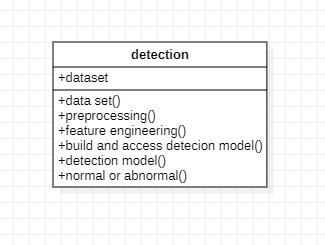
• UML stands for Unified Modeling Language. The goal is for UML to become a common language for creating models of object-oriented computer software.

1. Use case Diagram
2. Class Diagram
3. Sequence Diagram
4. Activity Diagram

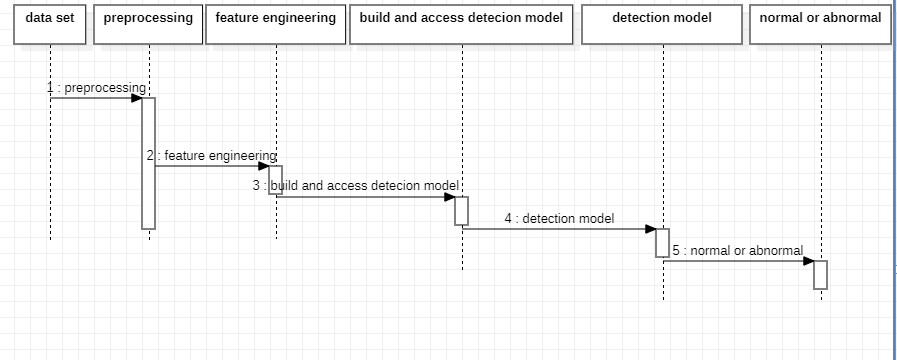
# Use Case Diagram



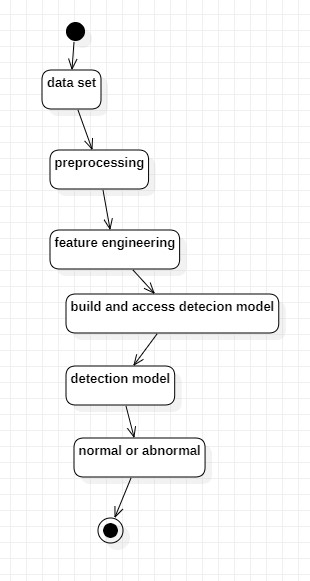
# Class Diagram



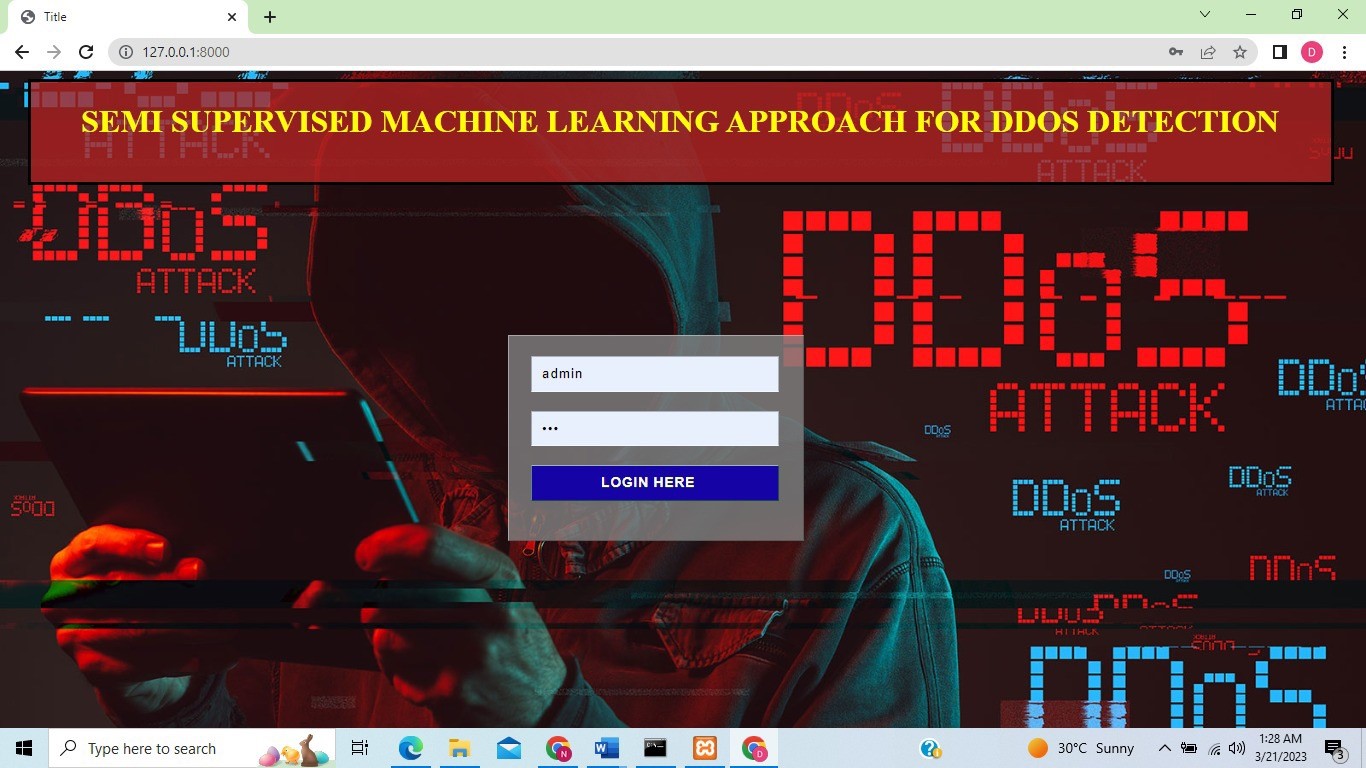
# Sequence Diagram

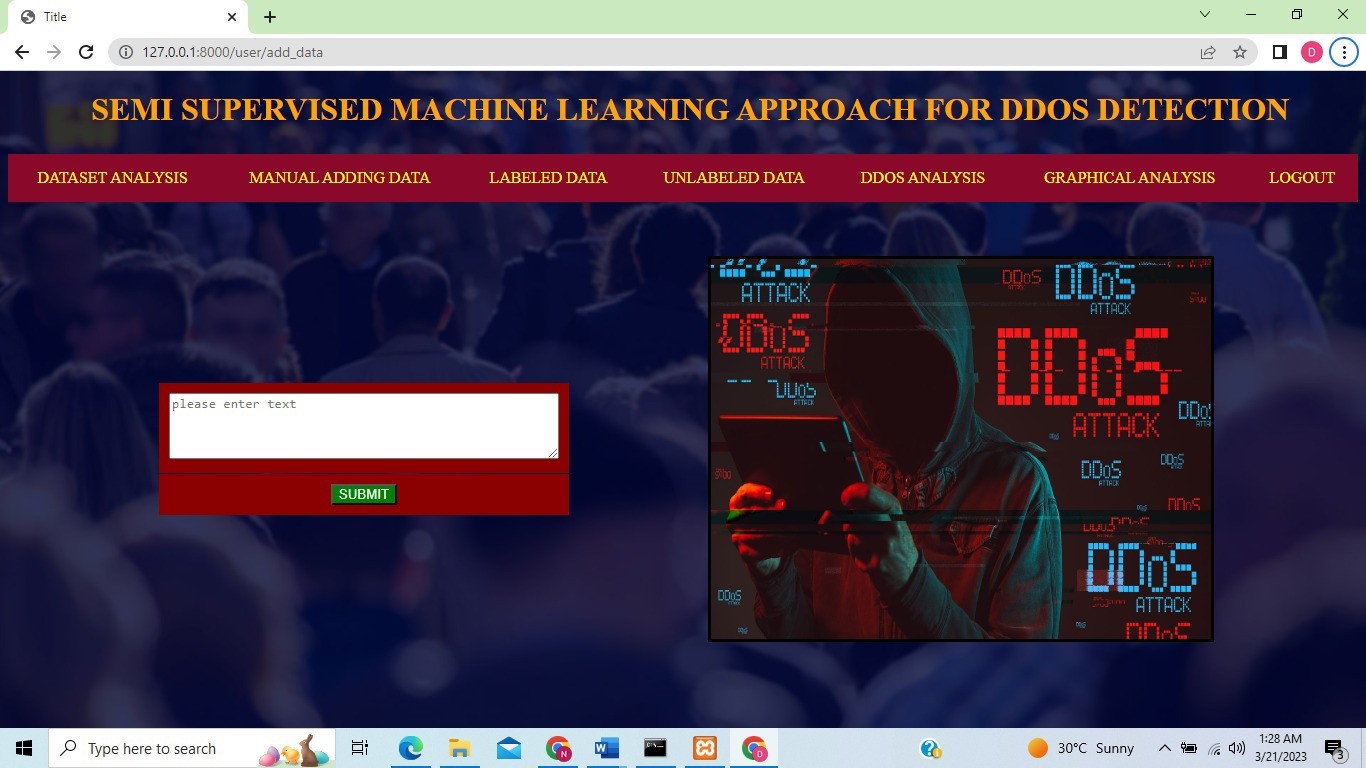


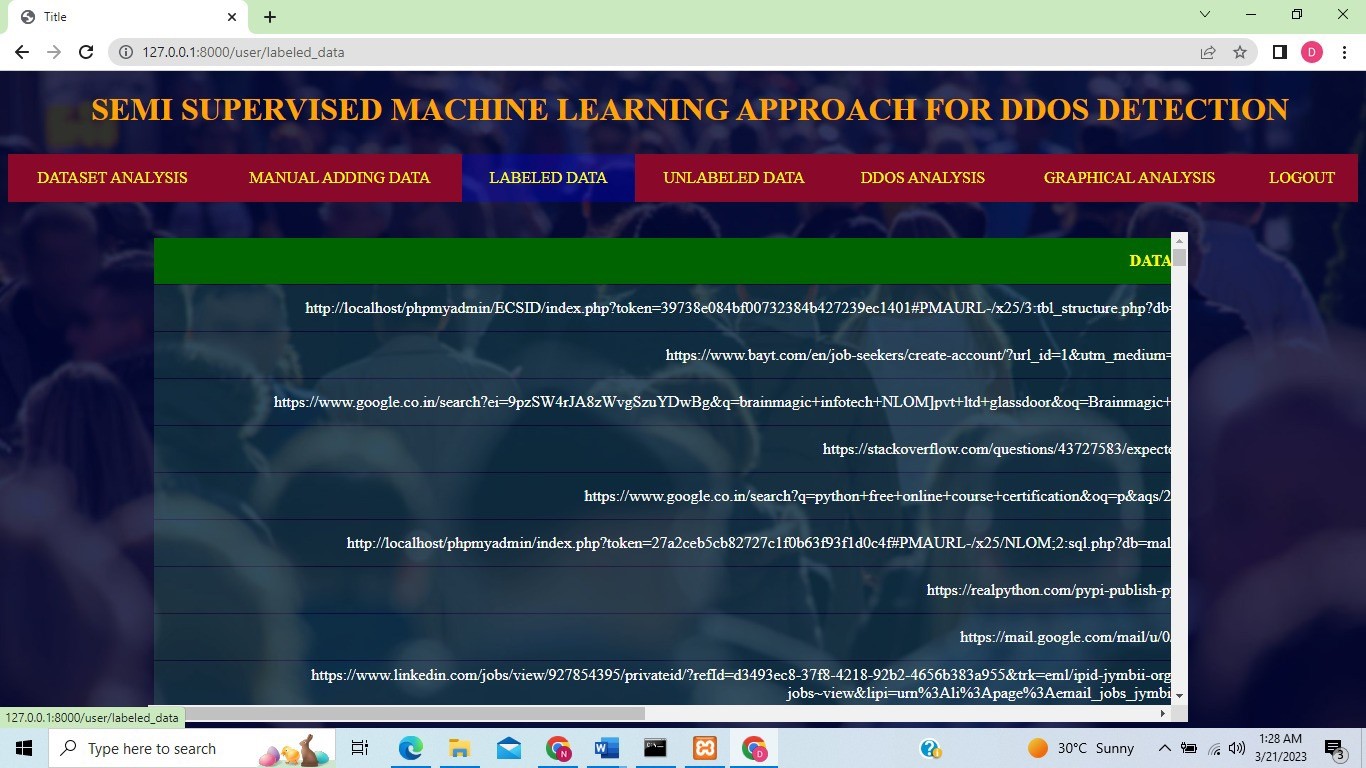
# Activity Diagram

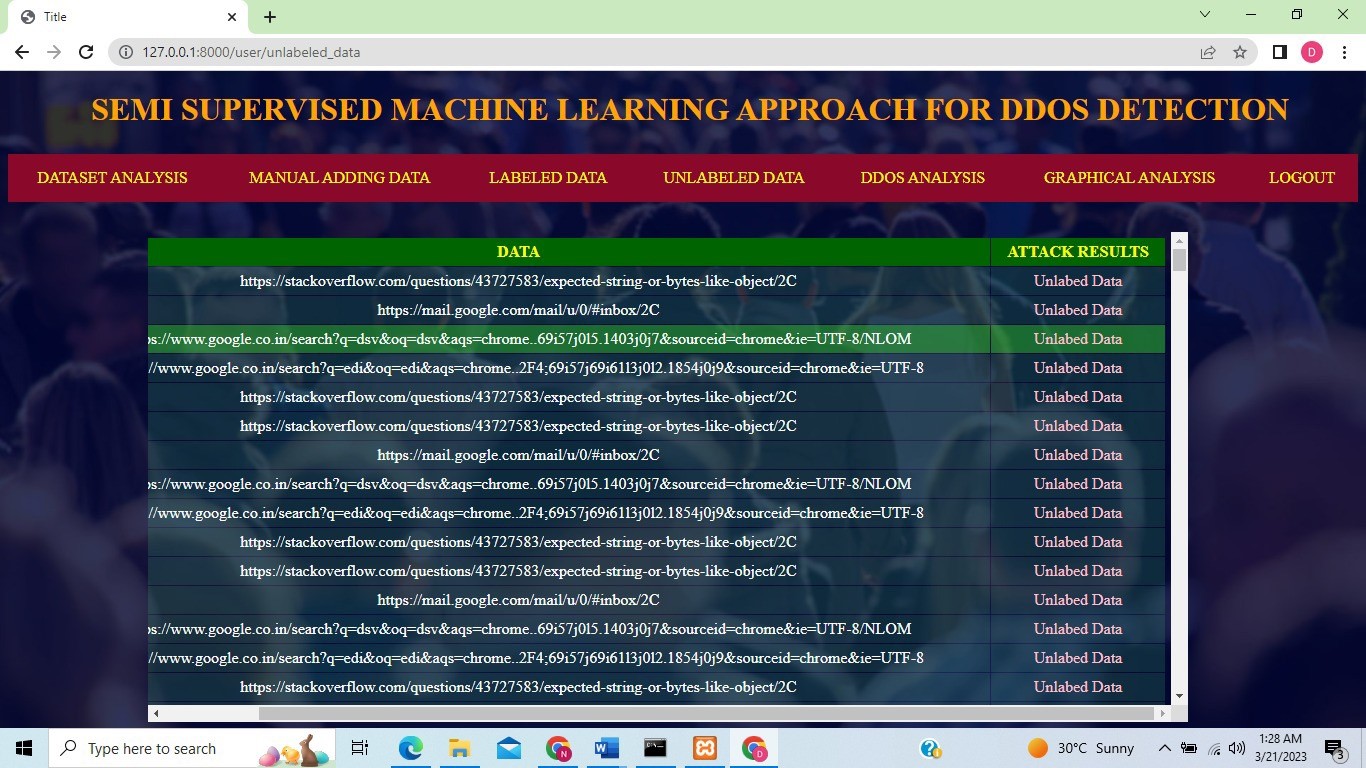


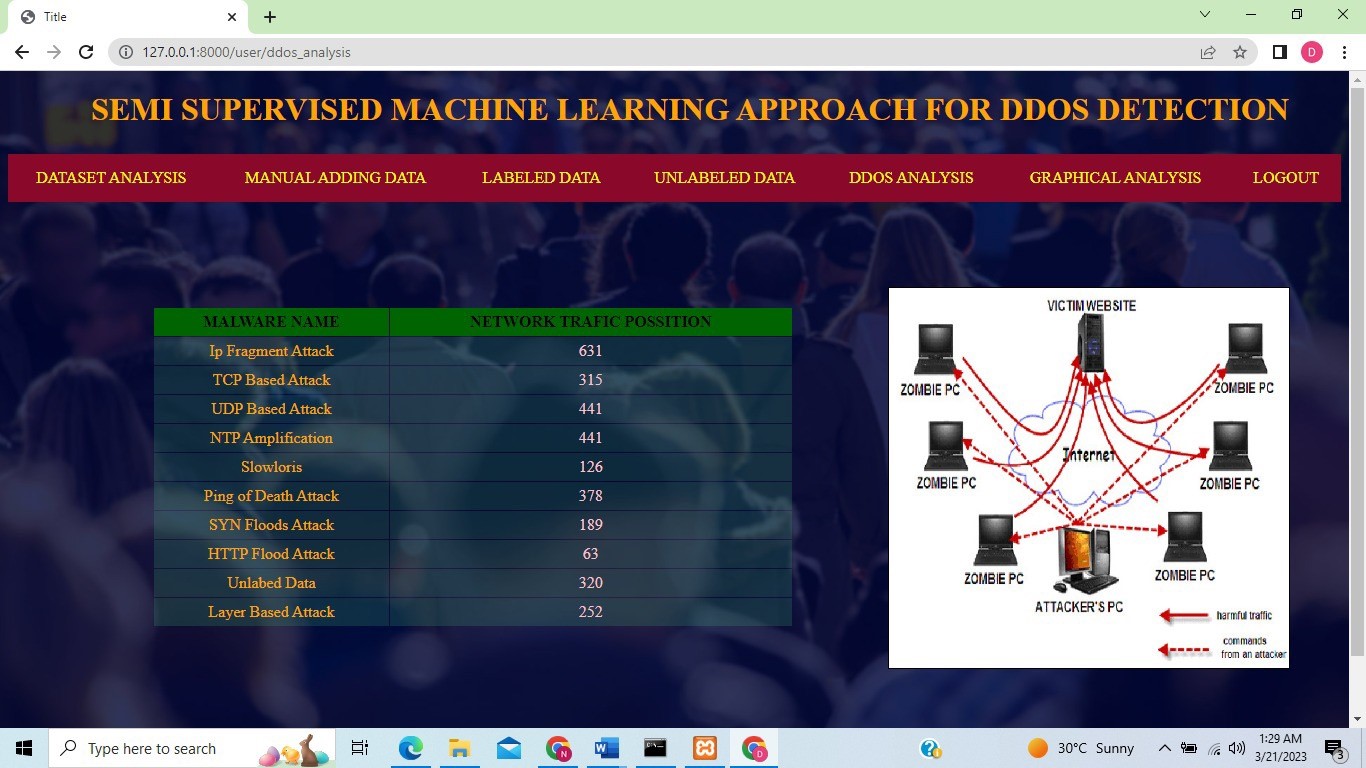
# Output Screenshots

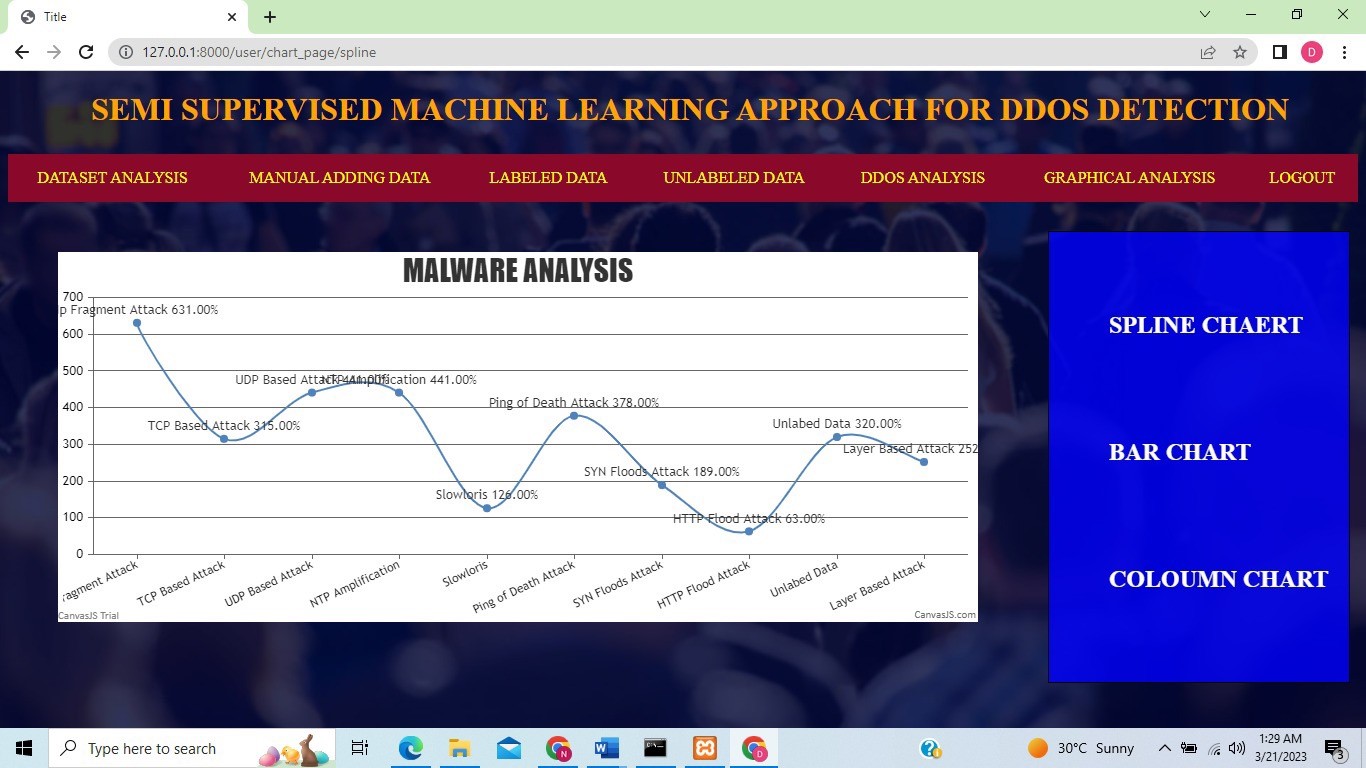












# Conclusion

u So finally we conclude by saying that, this project is used to detect denial of service attacks by using some machine learning techniques so that it protects the system from malicious attacks.

# References

* K. Ibrahim and M. Ouaddane, “Management of intrusion detection systems Analysis” in Wireless Networks and Mobile Communications (WINCOM), 2017 International Conference on. IEEE, 2017.
* M. Almansob and S. Lomte, “Addressing challenges for intrusion detection system using naive bayes algorithm,” in 2nd International Conference for. IEEE, 2017.

# THANK YOU