Sophal Vaung

DDOS DETECTION

USING MACHINE LEARNING

American University of
Phnom Penh

COSC 221 001 - Computer
Science B

Dr. Abdallah Altrad

December 2, 2024

INTRODUCTION

Distributed Denial of Service (DDoS) attacks are a major concern in cybersecurity, because they flood networks with too much traffic, causing services to stop working. To deal with this concern, I built a project uses machine learning to detect and classify these attacks. To make it easier for users, I created a user-friendly interface using Streamlit UI that allows real-time analysis of network traffic data.

OBJECTIVE

The primary objective of this project is to develop an efficient and scalable machine learning-based system for the detection and classification of DDoS attacks. By analyzing key features from network traffic, the system aims to show the difference between normal and harmful patterns with high accuracy. The project also focuses on building a simple interface that makes it easy to upload data, choose a model, and see the results. This includes preparing the data, selecting the best features, and testing the system to make sure it works well and can be used in real-life cybersecurity situations.

TECHNOLOGY USED

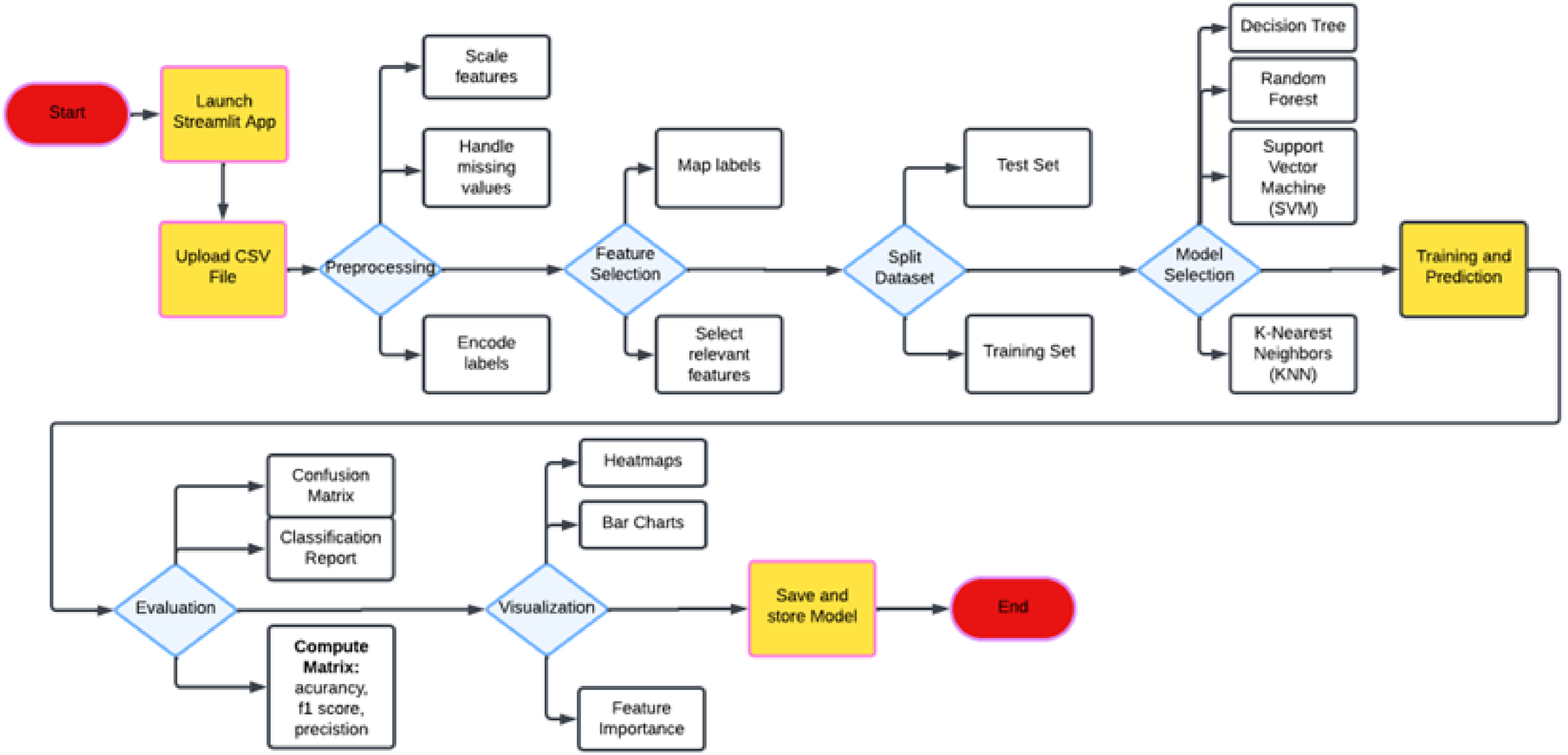
PROGTAMING LANGAUGE

-PYTHON

LIBRARIES:

- Streamlit for the user interface
- Scikit-learn for machine learning models and metrics
- Pandas and NumPy for data manipulation
- Matplotlib and Seaborn for visualization
- Joblib for model saving/loading

FLOWCHART


Start
Launch Streamlit App
Upload CSV File
Preprocessing
Scale features
Handle missing values
Encode labels
Feature Selection
Map labels
Select relevant features
Split Dataset
Test Set
Training Set
Model Selection
Decision Tree
Random Forest
Support Vector Machine (SVM)
K-Nearest Neighbors (KNN)
Training and Prediction
Evaluation
Confusion Matrix
Classification Report
Compute Matrix: acurancy, f1 score, precistion
Visualization
Heatmaps
Bar Charts
Feature Importance
Save and store Model
End

Sophal Vaung

CODE DEMO

AMERICAN UNIVERSITY OF
PHNOM PENH

REFERENCES

These references refer to the project idea, concept code, and datasets explored.

Kaggle: Your machine learning and data science community. (n.d.). Retrieved from https://www.kaggle.com/

Najafimehr, M., Zarifzadeh, S., & Mostafavi, S. (2023). DDoS attacks and machine-learning-based detection methods: A survey and taxonomy. Engineering Reports, 5(12). https://doi.org/10.1002/eng2.12697

Samruddhid. (n.d.). GitHub - DDoS Detection using Machine Learning. Retrieved from https://github.com/samruddhid5/DDoS-Detection-using-Machine-Learning

THANK YOU

Sophal Vaung

American University of Phnom Penh

COSC 221 001 - Computer Science B

Dr. Abdallah Altrad

December 2, 2024