South Ural State University | National Research University

MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE RUSSIAN

FEDERATION Federal State Autonomous Educational Institution of Higher Education

“South Ural State University (National Research University)”

School of Electrical Engineering and Computer Science

Department of Computer Engineering

“MISUSE ATTACK DETECTION BASED ON DATA MINING IN NETWORK FUNCTIONS VIRTUALIZATION”

for the master graduate qualification work of

A student of the group KE-228: N . J. AL-Dulaimi

Supervisor: D.V. Topolsky, PhD, Associate Professor

Introduction

This project involves the creation of an efficient model that allows you to run data mining algorithms to detect malicious attacks on Network Functions Virtualization (NFV) .

Relevance and Novelty

Due to the growing size of internet of things IoT networks and the increased data intake that comes with it, a Network Function Virtualization (NFV) system offers the best security solution in terms of combating complexity .This project aims to proposing an early and accurate Misuse attack detection model to protect the NFV environment based on the most common and efficient data mining techniques.

Tasks necessary to achieve the goal:

1.Analyzing the Analogues of Detection Models.

2.Analyzing technological solutions to use to solve the problem.

3.Design a model architecture for Misuse Attack Detection.

4.Training the Misuse Attack Detection Model .

5. Testing the model - confusion matrix

6.Test the library and provide an example implementation of the interfaces.

7.Testing the Misuse Attack Detection model .

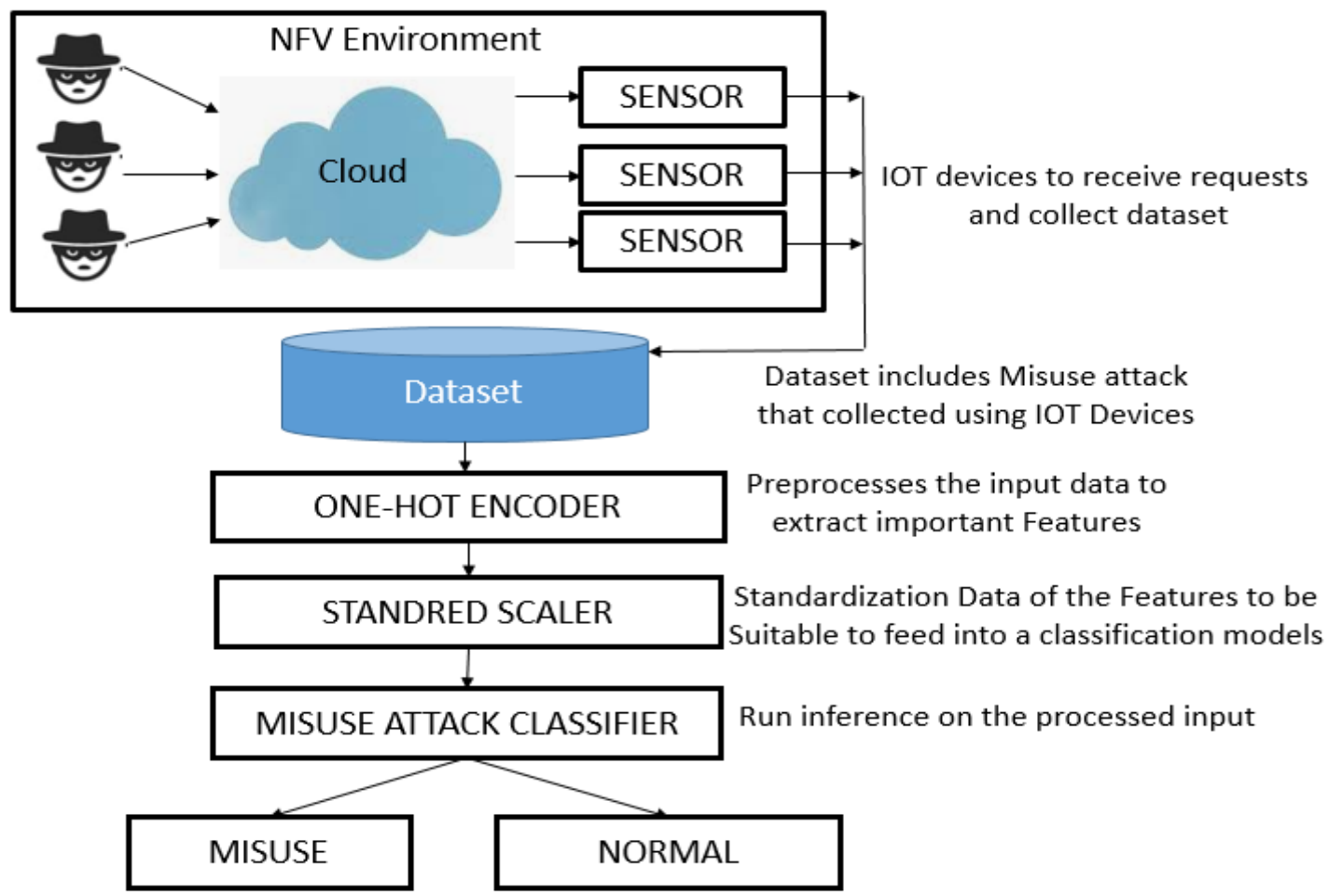
Task1:Analyzing the Analogues of Detection Model

- Parallel Misuse and Anomaly Detection Model
- Self-Adaptive Misuse Detection Model
- Extract Rules Of Misuse Attack Detections Models

Task2:Technological Solutions

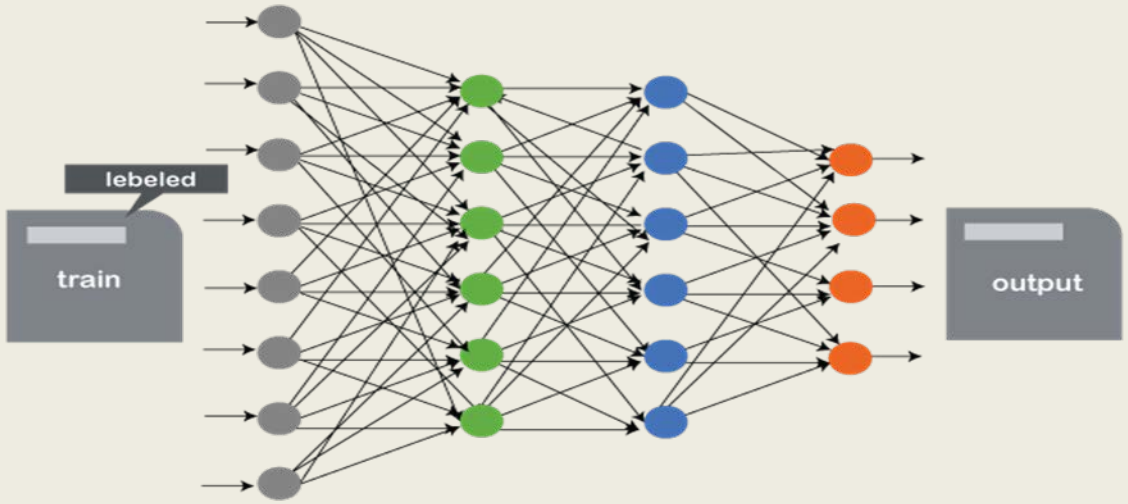
- CAID-DDoS Attack Dataset
- TansorFlow
- Pandas
- NumPy Array
- Programming Technologies

Task3:Architecture Design



Task 4: Training the detection model

a) One Hot Encoding

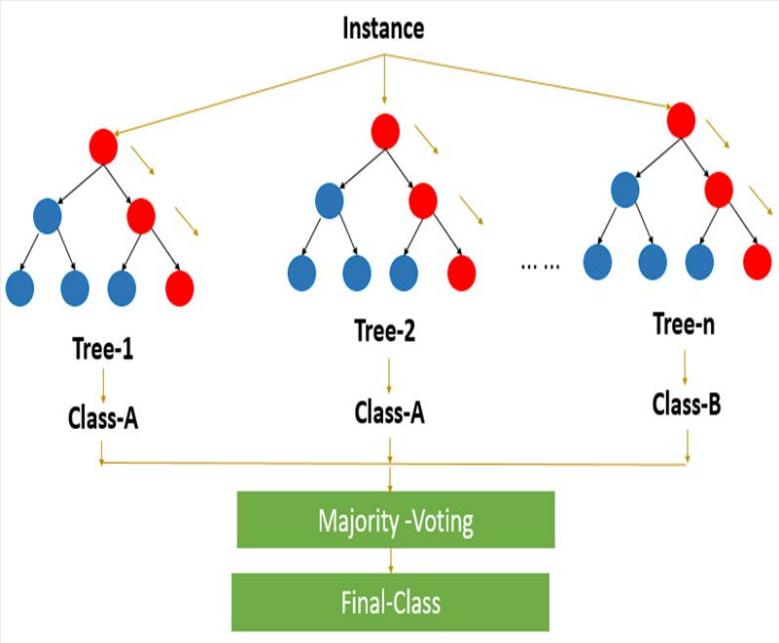


b) Stander Scaler Data

Task 4: Training the detection model

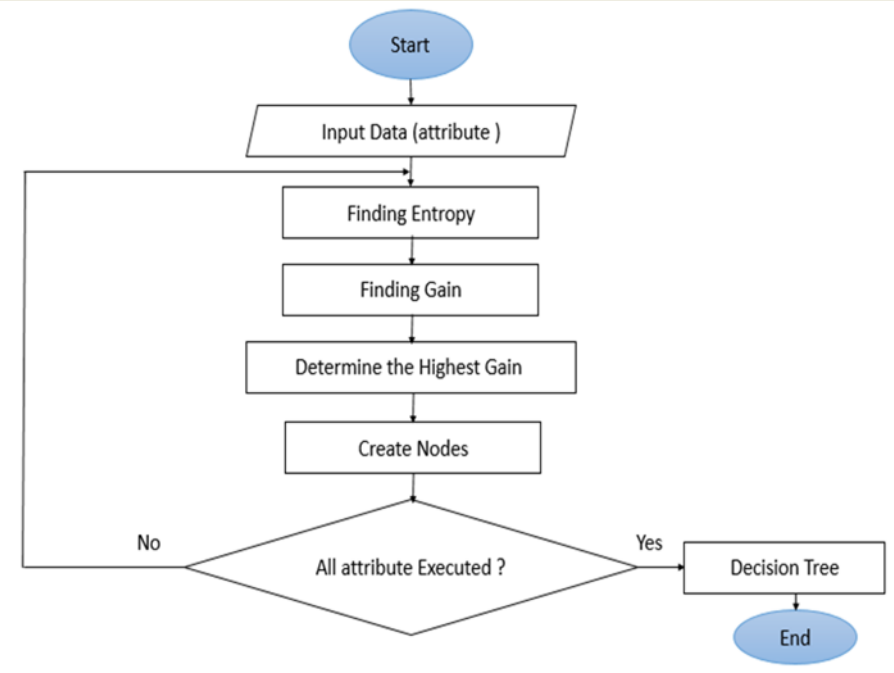
c) Misuse Attack Classification

1. Random Forest Model



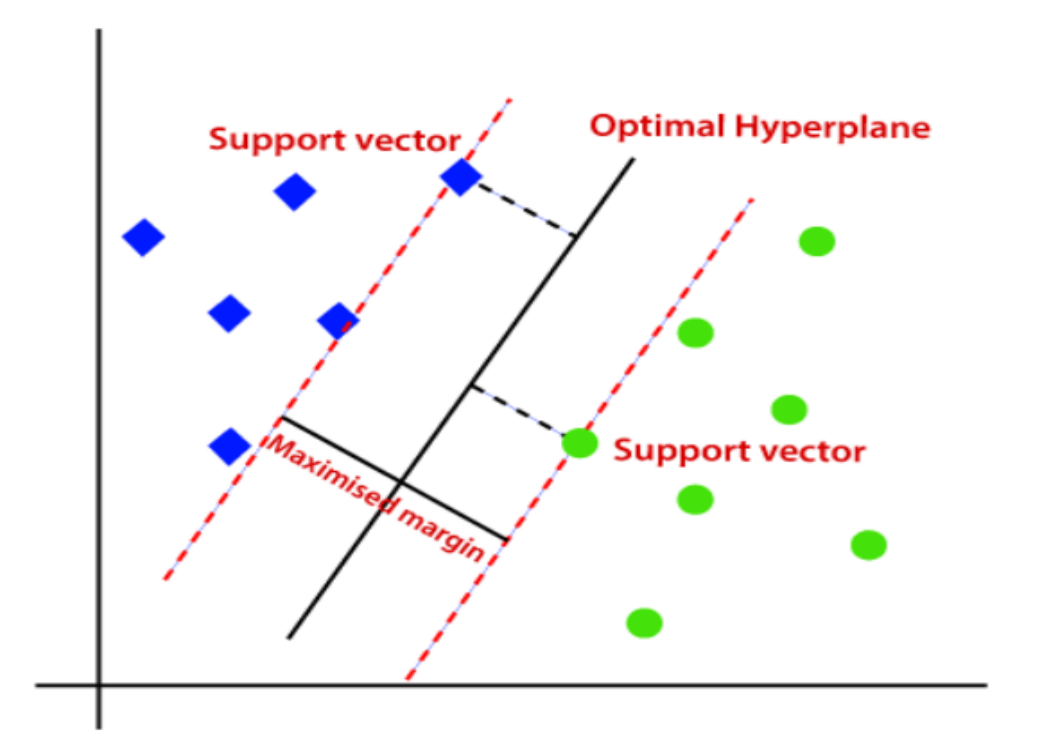
Task 4: Training the detection model

2. C4.5 Decision Tree Model



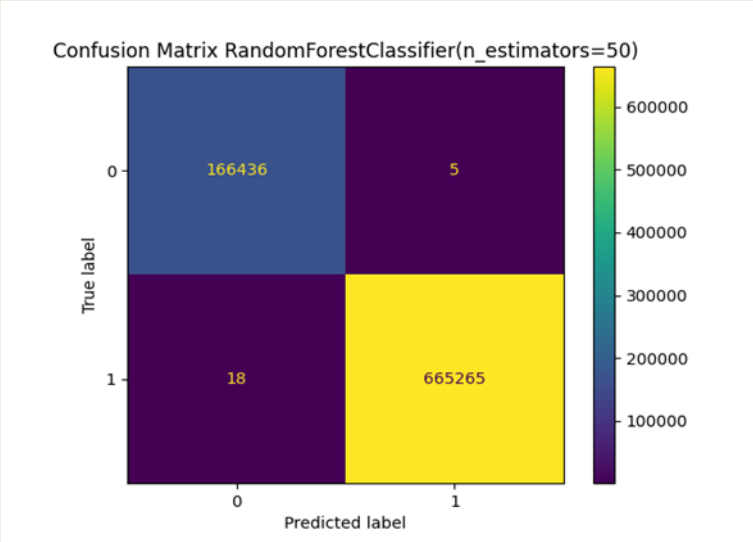
Task 4: Training the detection model

3. Linear Support Vector Classification Model

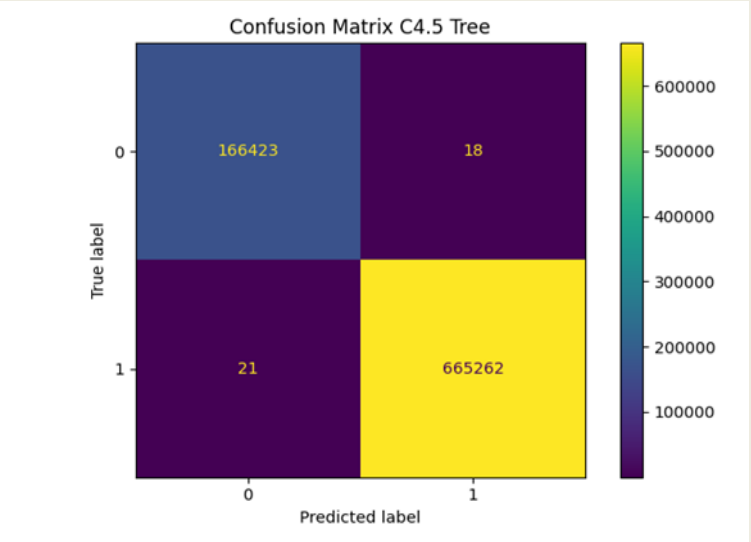


Task 5: Testing the model - confusion matrix

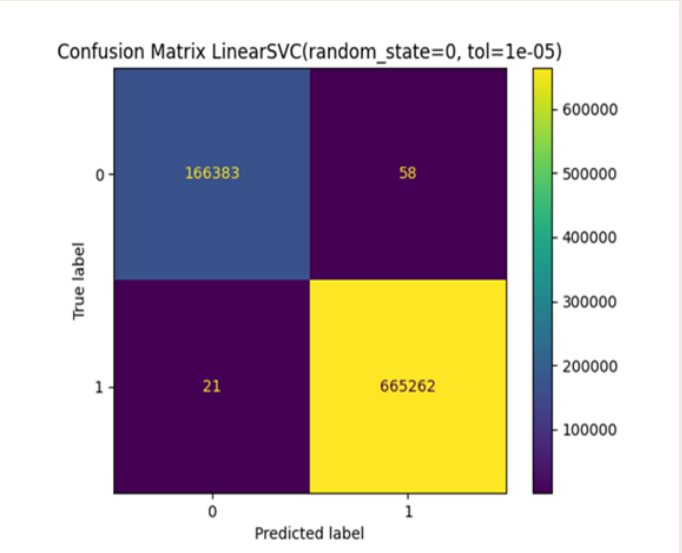
a) Random Forest Algorithm



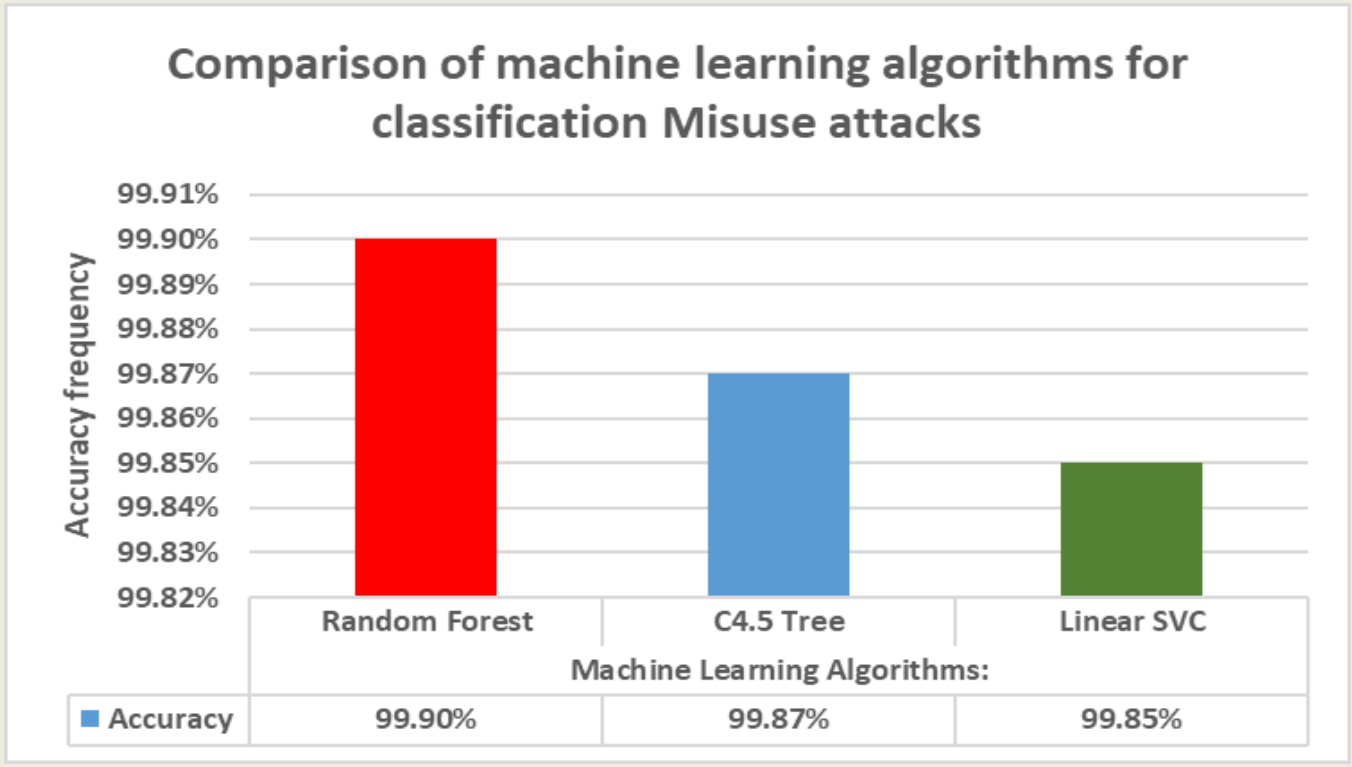
b) C 4.5 Tree Algorithm



c) Linear SVC Algorithm

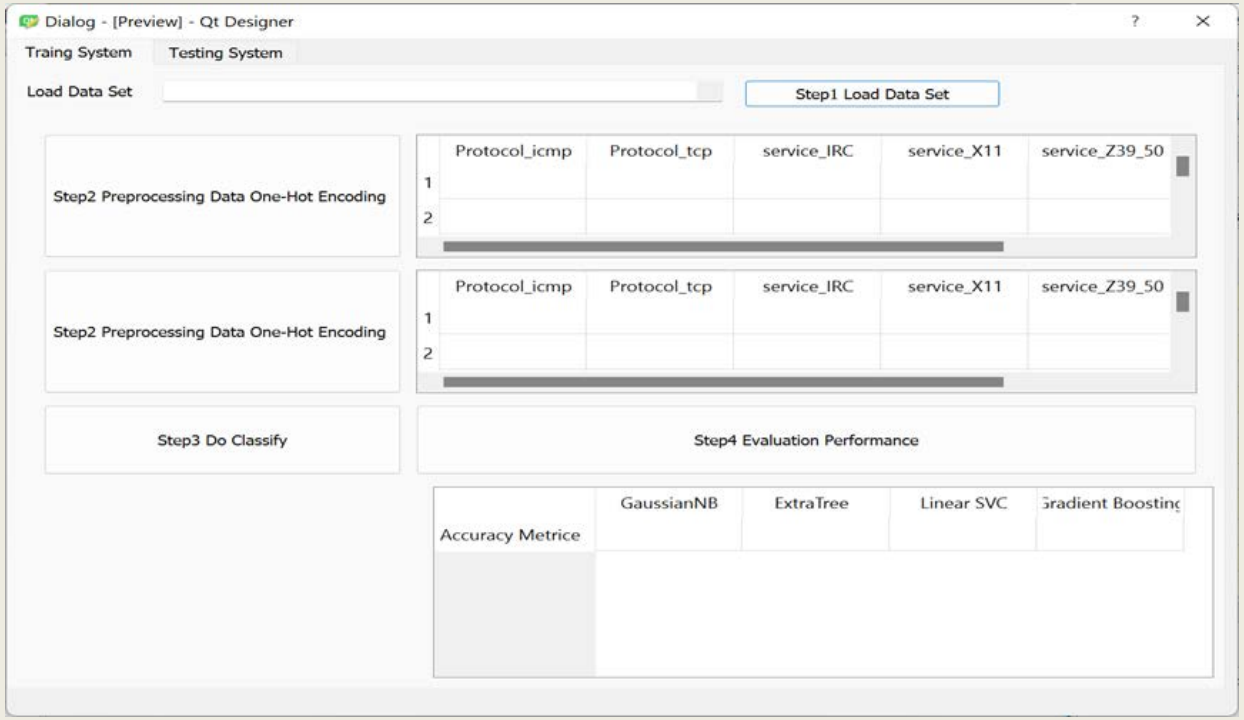


Task 5: Testing the model - confusion matrix



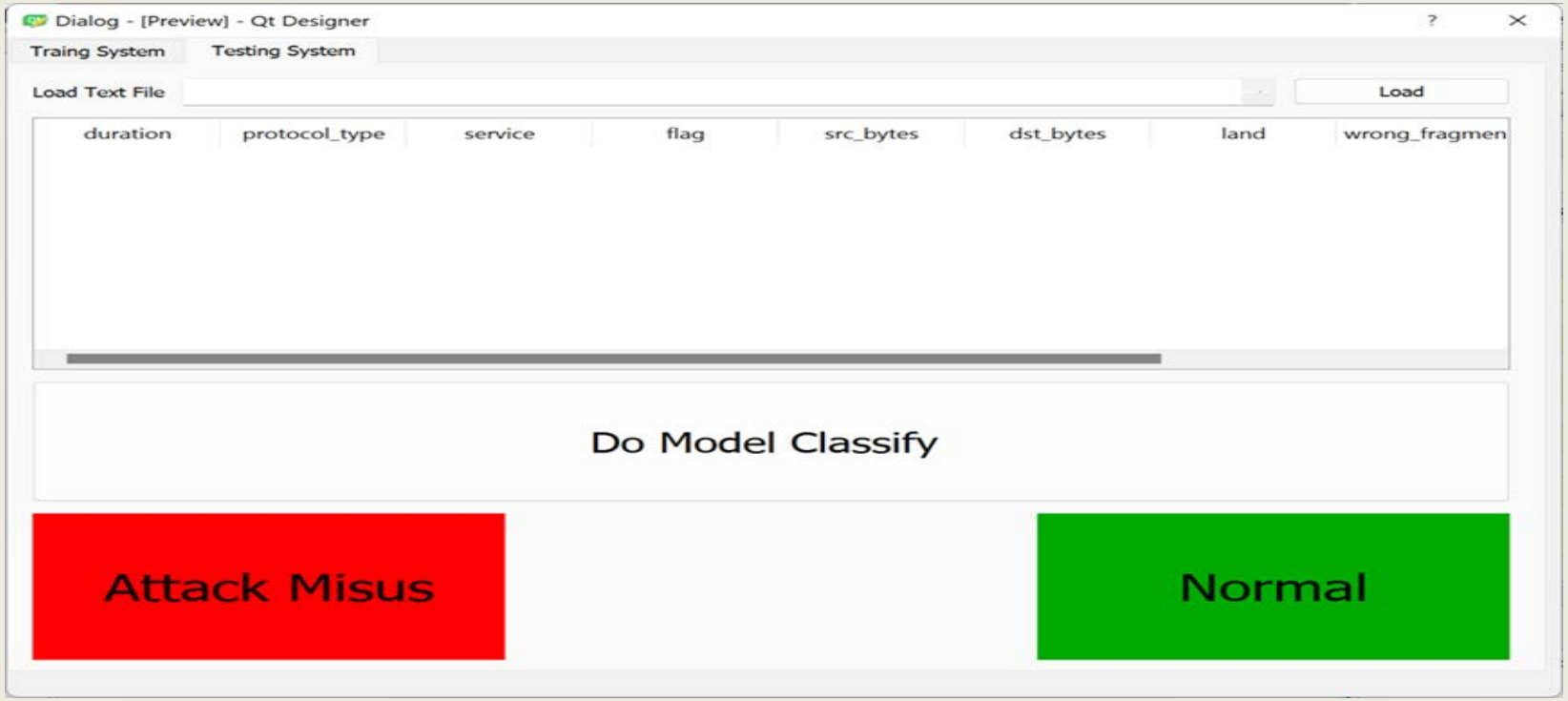
Task 6:Test the library and provide an example implementation of the interfaces

- Implementation of the Training Interface

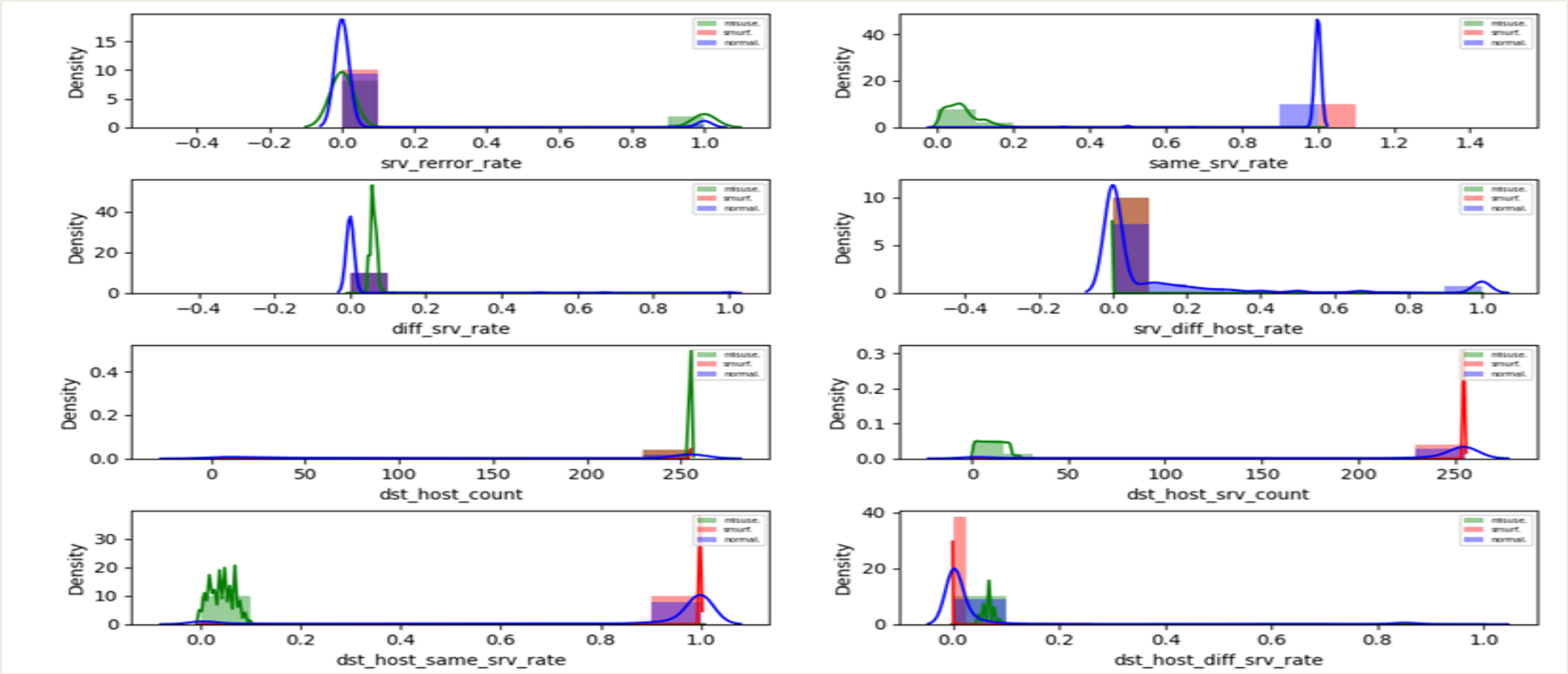


Task 6:Test the library and provide an example implementation of the interfaces

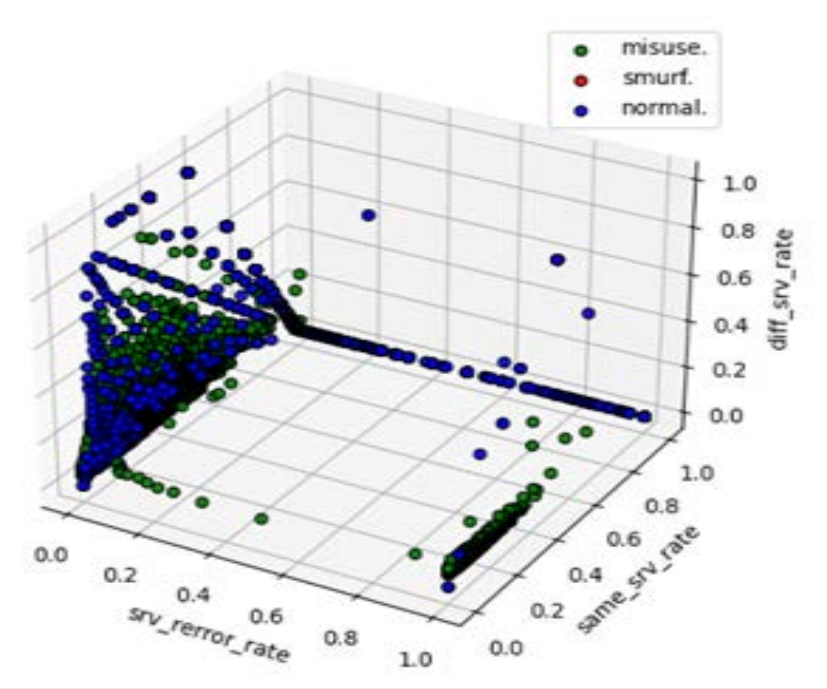
- Implementation of the Testing Interface

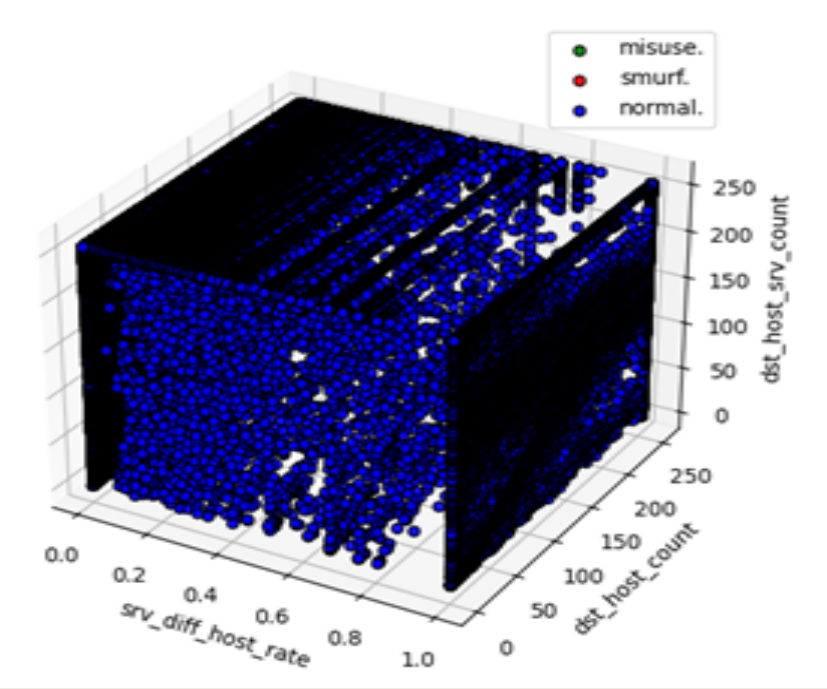


Task7:Testing the Misuse Attack Detection Model



Task7:Testing the Misuse Attack Detection Model





Conclusion

This project able to maintain the security of IoT data in NFV networks by identifying and diagnosing with high accuracy the most dangerous type of attack, which is the misuse attack in cloud services.

Future considerations

1. Improving Latency
2. Improving Power Usage
3. Improving Model and Binary size

Thank you for your attention