Defense Mechanism For Proactive Detection Of Compromised Systems

AMRITA VISHWA VIDYAPEETHAM
DEEMED TO BE UNIVERSITY UNDER SECTION 3 OF UGC ACT, 1956
SCHOOL OF COMPUTING CHENNAI

Department of Computer Science and Engineering (Cybersecurity)

Panchadarla Shiva Poojitha, Podile Sruthi

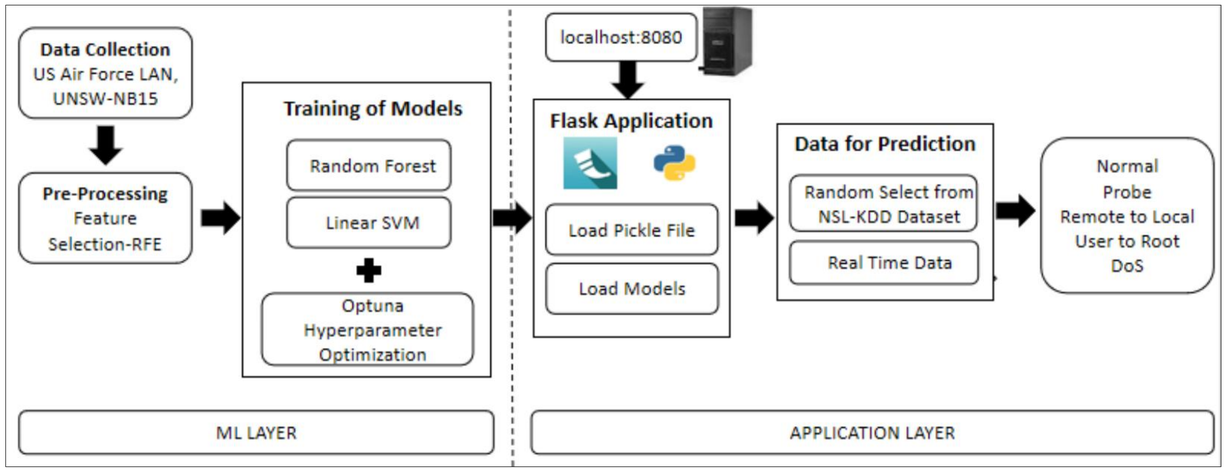
Abstract

- This study aims to enhance NIDS reliability using modern ML techniques, focusing on RF and Linear SVM models optimized with RFE and hyperparameter tuning.
- Achieving exceptional accuracy rates on benchmark datasets, the optimized models demonstrate robust performance in detecting diverse network intrusions, bolstering NIDS effectiveness in real-world scenarios.

Introduction

- Network Intrusion Detection Systems (NIDS) are crucial for modern cybersecurity, detecting evolving threats by monitoring network traffic.
- The objective is to enhance compromise detection capabilities using advanced AI/ML models, addressing limitations of traditional methods and bolstering resilience against dynamic cyber threats.

System Architecture and Design



Methodology

- Training Datasets: US Air Force LAN, UNSW_NB15
- Feature Selection: Recursive Feature Elimination
- ML Models: RF, Linear SVM
- Hyperparameter Optimization: Optuna
- Testing Dataset: NSL-KDD
- Flask Application that detects attcaks in real time

Results

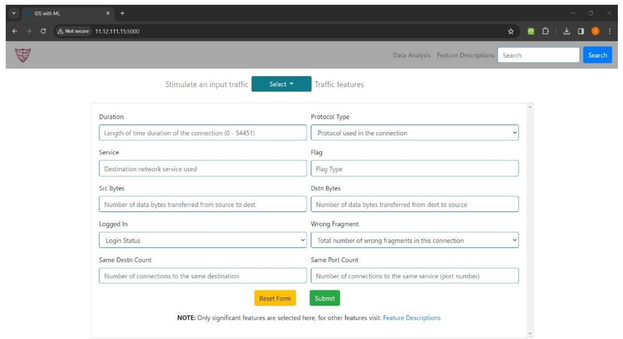
Classification Report:

	precision	recall	f1-score	support
0	1.00	1.00	1.00	3498
1	1.00	1.00	1.00	4060
accuracy			1.00	7558
macro avg	1.00	1.00	1.00	7558
weighted avg	1.00	1.00	1.00	7558

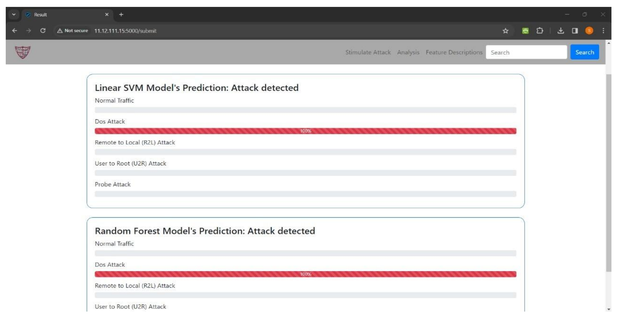
Classification Report:

	precision	recall	f1-score	support
0	0.96	0.94	0.95	3498
1	0.95	0.97	0.96	4060
accuracy			0.95	7558
macro avg	0.95	0.95	0.95	7558
weighted avg	0.95	0.95	0.95	7558

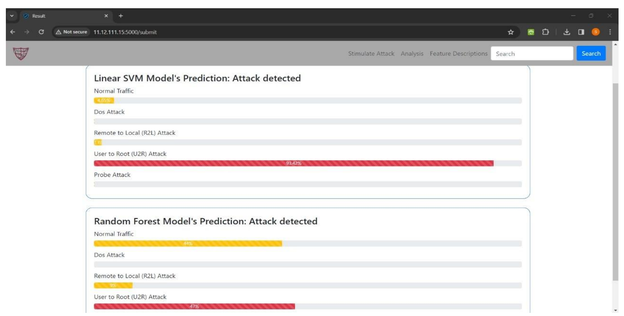
Detecting Attacks



Network Traffic input



DOS Attack



U2R Attack