Intrusion Detection System

University of Tabuk

Abstract

IDS is a research project using an LSTM model to detect DoS attacks in networks, achieving a 99.98% accuracy. The project involves preprocessing and analyzing network traffic data to identify anomalies, enhancing cybersecurity efficiently.

Problem Overview

Vulnerabilities in programs and systems can be exploited by attackers to launch DoS attacks. These attacks may arise due to various motives:

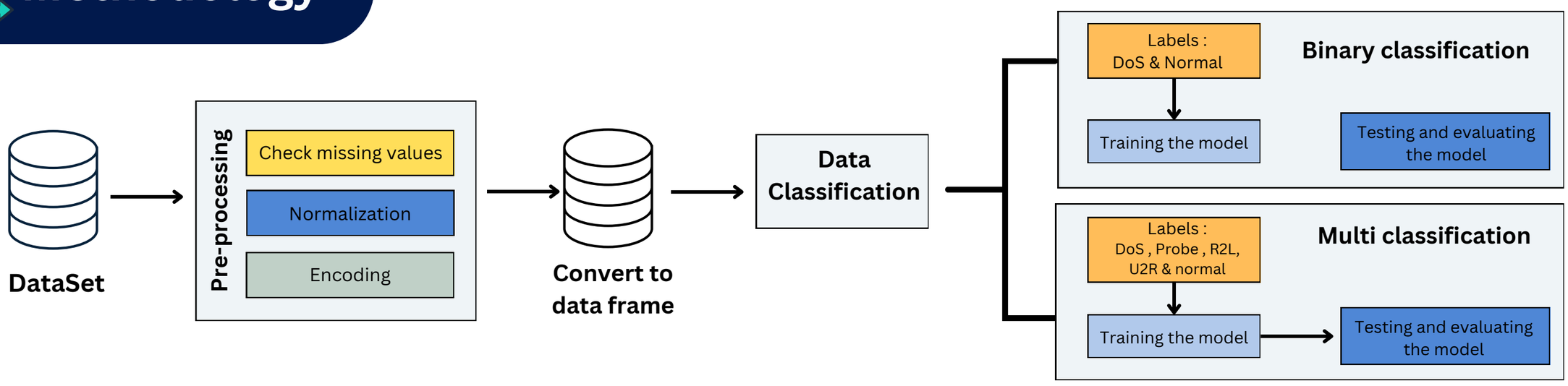
- Not all are driven by financial gains.
- Technological advancements increase attack opportunities.
- As internet usage grows, so does the frequency of attacks.

Aims and Objectives

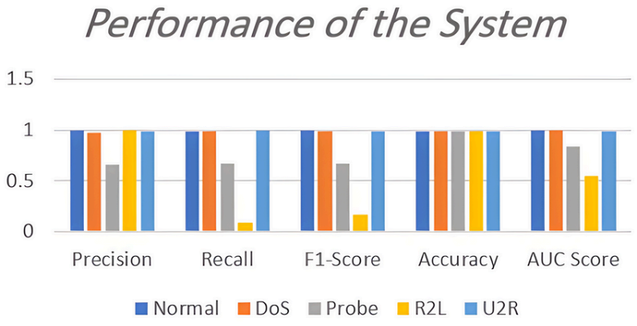
Intrusion detection system, aims to:

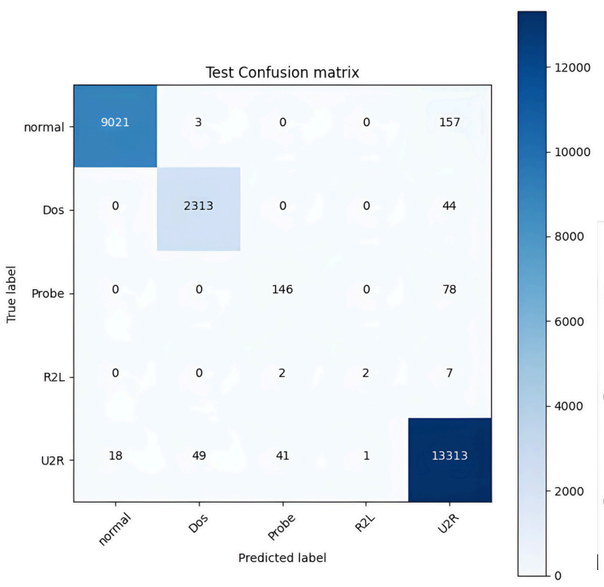
1. Define and understand key terms related to network intrusion detection.
2. Develop a NIDS to detect DoS attacks.
3. Analyze DoS patterns and build a model that sends alerts during attacks.
4. Implement the model with high accuracy and efficiency.

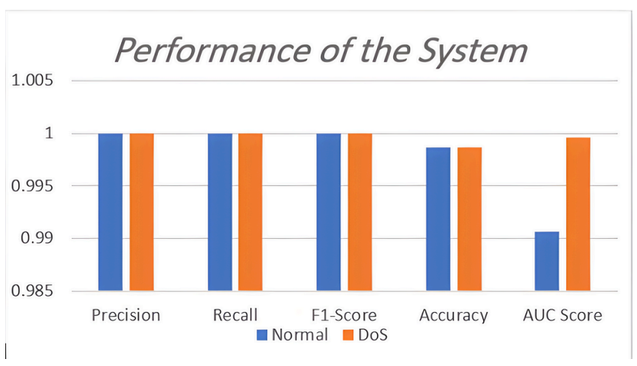
Methodology

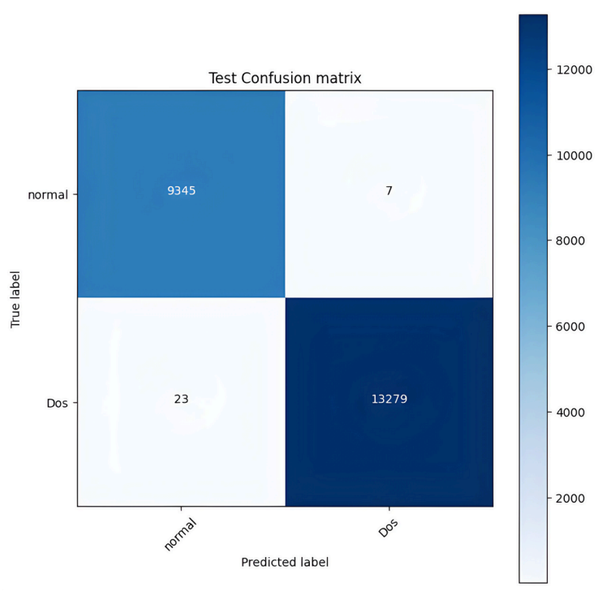


Results









Tools

colab

TensorFlow

python™

STUDENTS NAMES:

- MAWADDAH ALBALAWI
- ROLA AlSHEHRI
- RAGHAD ALQAHTANI
- HANAN ALANAZY
- SHAHAD ALBALAWI

SUPERVISED BY :

Dr. ONYTRA ABBASS

Section: 1001