BVRIT HYDERABAD
College of Engineering for Women
Department of Information Technology
Major Project - Academic Year 2022-23

TEAM 16

REAL-TIME INTRUSION DETECTION SYSTEM USING MACHINE LEARNING ALGORITHM

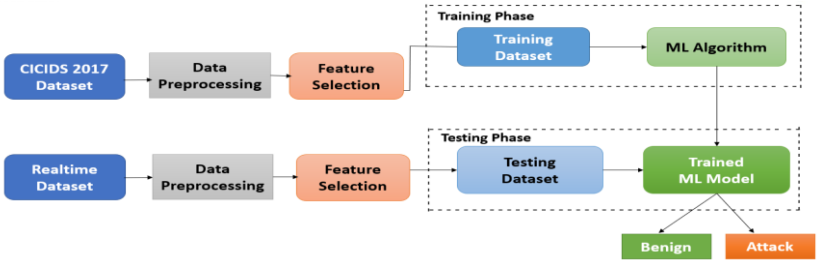
Abstract

A large rise in data traffic has been caused by recent developments in network technology and related services. But there has also been a huge rise in the negative consequences of cyberattacks. Many new types of network attacks are emerging. The intrusion detection system (IDS) is a critical tool for tracking and detecting intrusion threats. This paper attempts to analyse recent IDS research using a Machine Learning approach, with an emphasis on datasets, ML approaches, and metrics. Building an intrusion detector is the task, which entails creating a prediction model that can tell malicious connections from regular ones while also being able to discriminate between intrusions and attacks. We suggested an IDS algorithm based on supervised machine learning techniques for creating such an effective and adaptable system that can identify intrusions from the data collected in real-time.

Modules

- Generating Real-Time Dataset with attacks.
- Data Preprocessing.
- Training with Algorithms.
- Testing the model with Realtime Dataset.

Architecture



Tools and Technologies

- Virtual Box-Windows XP,Kali-Linux
- CIC Flowmeter
- Wireshark
- Python
- Google Colaboratory

Conclusion and Future Scope

In conclusion, our project focuses on developing a real-time Intrusion Detection System (IDS) using machine learning techniques. We leverage the CICIDS 2017 dataset for training our IDS model. The dataset encompasses various types of attacks, including DoS, DDoS, FTP, SSH, and benign traffic. Through extensive data preprocessing, which involves removing duplicates and handling infinity values, we ensure the dataset's quality.We have used 3 Algorithms for classification – Random Forest,Logistic Regression,Naïve Bayes. The accuracy achieved during the testing phase is an impressive 99 percent indicating the robustness of our model.In the testing phase, we utilize real-time traffic data captured through Wireshark during attacks. By preprocessing this data and ensuring feature compatibility, our trained model predicts whether each instance corresponds to an attack or benign traffic.

Guide

K.Srikar Goud
Assistant Professor of IT
srikargoud.k@bvrithyderabad.edu.in

Team

19WH1A1213 M. Shivani
19WH1A1215 B. Selvi Reddy
19WH1A1227 Ch. Shravyasree
19WH1A1234 J. ShreeyaReddy

Github links

1. github.com/it-19wh1a1213
2. github.com/19wh1a1215/III-II-ITA-Lab
3. github.com/itbvrith191227/III-IT-A-LAB
4. github.com/it-19wh1a1234