TRUSTY SECURITY SOLUTIONS

Securing IoT Environments

Trusty Security Solutions

Background and Purpose

The Internet of Things (IoT) paradigm has evolved into a technology for building smart environments. Widespread use of the Internet of Things (IoT) in various domains like smart city, healthcare, supply chain and transportation make IoT a target of potentially malicious attacks which affect smart environment applications. Thus, there is a crucial need for Intrusion Detection Systems (IDSs) designed for IoT environments to mitigate IoT-related security attacks that exploit some of these security vulnerabilities.

Mission Statement

Our mission is to thwart malicious attacks in IoT systems and mitigate these threats.

About our Product

IDS for IoT

An Intrusion Detection System(IDS) detects malicious attacks.

ML as it's soul

It based on a ML model which upgrades and learns as it geos along to keep up with new threats.

Why TSS?

Faster

Robust & Reliable

High Detection Rate

Low False Positive Rate

About Our IDS

Anomaly Based

Multiple Classifiers

Accurate & Precise

Methods of Intrusion Detection

Anomaly Based

- **Less Data Intensive and hence Faster**
- **Can Detect new Threats**

Our Anomaly based IDS (A-IDS) is trained using NSL-KDD dataset and it also learns the behaviour of the network to predict whether a connection is normal or a threat. Thus, our A-IDS can check for threats and can even detect new threats, for which the model was not trained.

Signature Based

- **More Data Intensive**
- **Cannot Detect new Threats**

Signature based IDS (S-IDS) compares the signature of a connection with signatures in a database to detect threats. Hence it is more data intensive and consumes more time. Also, it cannot predict a new threat unless the data set is updated and hence is not reliable for vulnerable IoT environment.

How it Works

1

KNN

Every connection is classified as normal or threat using KNN classifier and a probability is assigned to it.

2

Random Forest

Every connection is classified as normal or threat using Random Forrest classifier and a probability is assigned to it.

3

Combine Results

The results of KNN and RF are combined using a voting classifier to get a combined probability.

4

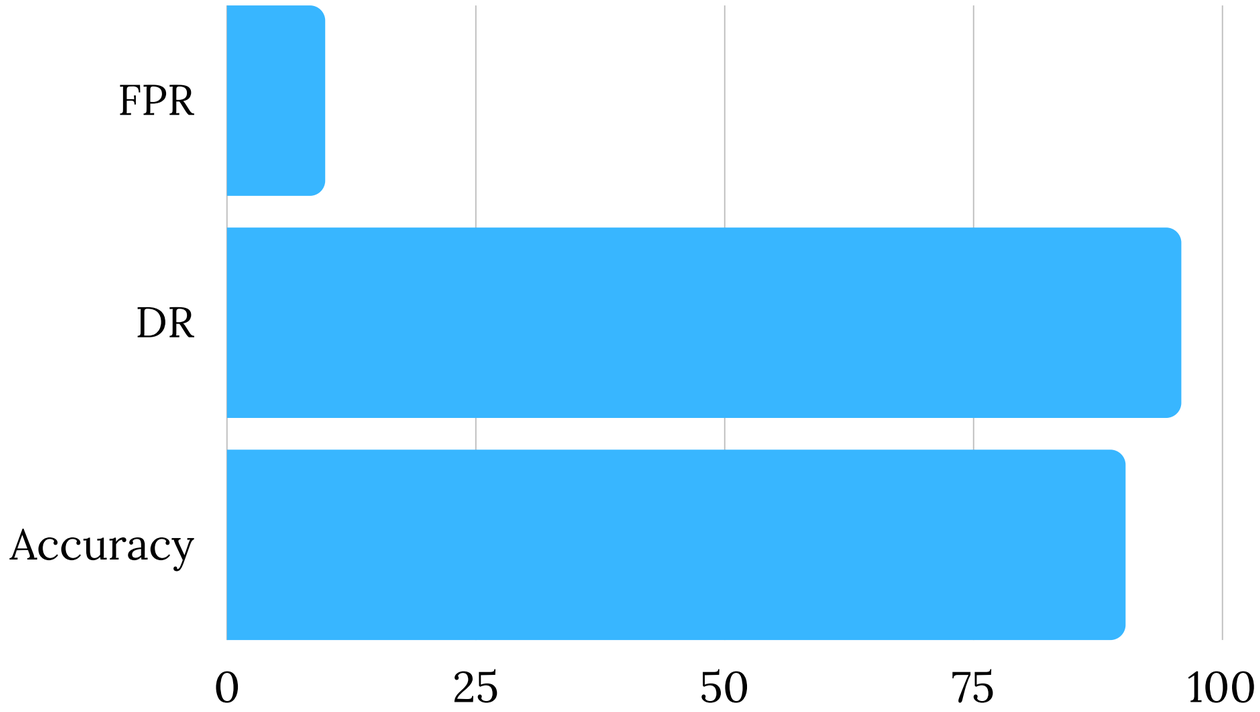
Result

Based on a certain threshold probability, the connection is classified as either normal or threat.

How our Model Performs

Using Threshold for optimizing

For different thresholds, False Positive Rate (FPR), Detection Rate (DR) and Accuracy. Our aim is to maximise DR for a significantly less FPR. We have achieved 95.8% DR which is 90.2% accurate for FPR less than 10%.



Thank you!

Feel free to approach us if you have any questions.

Contact us

Reach out if you have any questions or clarifications

Phone Number

123-456-7890

Email Address

helpdesk@tss.com

Website

www.tss.com

Address

IIT Bombay, Powai, Mumbai, Maharashtra, India 400076