Developing a Real - Time Intrusion Detection System

In this project we will build IDS that can detect network intrusions in real time.This involves detecting network traffic, port scans and other security breaches.

For this I have collected one popular dataset which is CIC-IDS 2017.
Dataset - https://www.kaggle.com/datasets/chethuhn/network-intrusion-dataset

Tasks to be done:

1. Requirements gathering
2. Download dataset
3. Preprocessing the data - feature scaling, convert categorical to numerical features, clean data
4. Feature engineering - handling IP addresses, feature transformation
5. Training a ML model - random forest or svm, knn
6. Evaluate the model - accuracy, precision, recall and confusion matrix
7. Real time integration - collect real time data and stream it.
8. Testing and optimization - hyper parameter tuning.