Project Proposal

Question/needs:

Coburg Intrusion Detection Data Sets (CIDDS) is a concept to create evaluation data sets for anomaly-based network intrusion detection systems. The external server attack logs are the most interesting part. These days sophisticated systems are being built to encounter Server attacks and suspicious content. Working in building a model to predict an attack session.

Data description:

Dataset I obtained was from Kaggle https://www.kaggle.com/kartikjaspal/server-logs-suspicious. this dataset is uploaded to check what factors contribute to server anomalies.

Dataset: 172838 rows, 16 columns, Included columns: Time and duration of attack, Source and destination IP, Packets, bytes, flows, and flags, Type, ID, and label/class

I am planning to use deep learning model such KNN, RNN and Logistic Regression. I will plan to conduct this model in which differentiate between normal and suspicious attacks.

Tools:

I will be planning to use deep learning model and library. I will be using TensorFlow, Sklearn, Matplotlib, Seaborn, Pandas and NumPy library for visualization and calculation.

MVP Goal:

The goal of this project is to differentiate between normal and suspicious attacks.

A visual image below provides a better idea.