# Project Title: Network Intrusion Detection using Deep Learning

Objective : Cyber Security: Development of Network Intrusion Detection System (NIDS), with Machine Learning and Deep Learning (RNN) models, MERN web I/O System.

## Description:


Large numbers of businesses were affected by data infringes and Cyber -attacks due to dependency on internet. To prevent such malicious activity, the network requires a system that detects anomaly and inform the user and alerts the user.

This project detects Network Intrusion anomalies by using NSL - KDD data-set. The deep learning model Long Short Term Memory (LSTM), superior version of RNN (Recurrent Neural Network) and KNN K - Nearest Neighbour Algorithm) method are used for binary and multi class classification.
The user enters the hacking parameters in the front end which is designed by using ReactJS. The model predicts the type of attack and gives information about the type of attack to the user. MongoDB is used for storing the data and NodeJS is served as back end framework.