MACHINE LEARNING PROJECT

Vasisht Duddu::2015137
Shubham Khanna::2015179
Anubhav Jain::2015129

CYBERSECURITY TOOLKIT USING MACHINE LEANRING

PROBLEM STATEMENT

With the advancement of technology, security of systems and detection of attacks are of prime importance. As part of the semester course project, we would like to use machine learning techniques to implement a cybersecurity toolkit. The toolkit will comprise of the following:

->Virus and Malware Detection (Classification)
->Intrusion Detection (Classification)
->Network Log Analysis (Classification)

LEARNING ALGORTIHMS

->K-Nearest Neighbours
->Naive Bayes
->Decision Trees
(We will choose the most optimal algorithm among the above mentioned)
->Random Forrests (Will use ensemble approaches)

TRAINING APPROACHES

We would like to try both Stochastic Gradient Descent and Batch Gradient Descent.

MODEL SELECTION AND PARAMTER TUNING

We would try various models(linear, nonlinear and Gaussian) and use cross validation to choose the optimal values.

DATASETS

All the code and Datsets will be available at:
->Datasets: https://github.com/vduddu/MachineLearningScripts/tree/master/MLCyberSec/Data
->Code: https://github.com/vduddu/MachineLearningScripts