An Intelligent Software Defined Network Controller for Preventing Distributed Denial Of Service Attack

In this paper author is evaluating performance of different data mining algorithms to detect denial of service attacks, to disturb network services malicious users send hundreds of requests to server to corrupt the services and packet monitoring application like DDOS detection will check signature of request and if request contains valid data then it will allow to execute otherwise it will drop it.

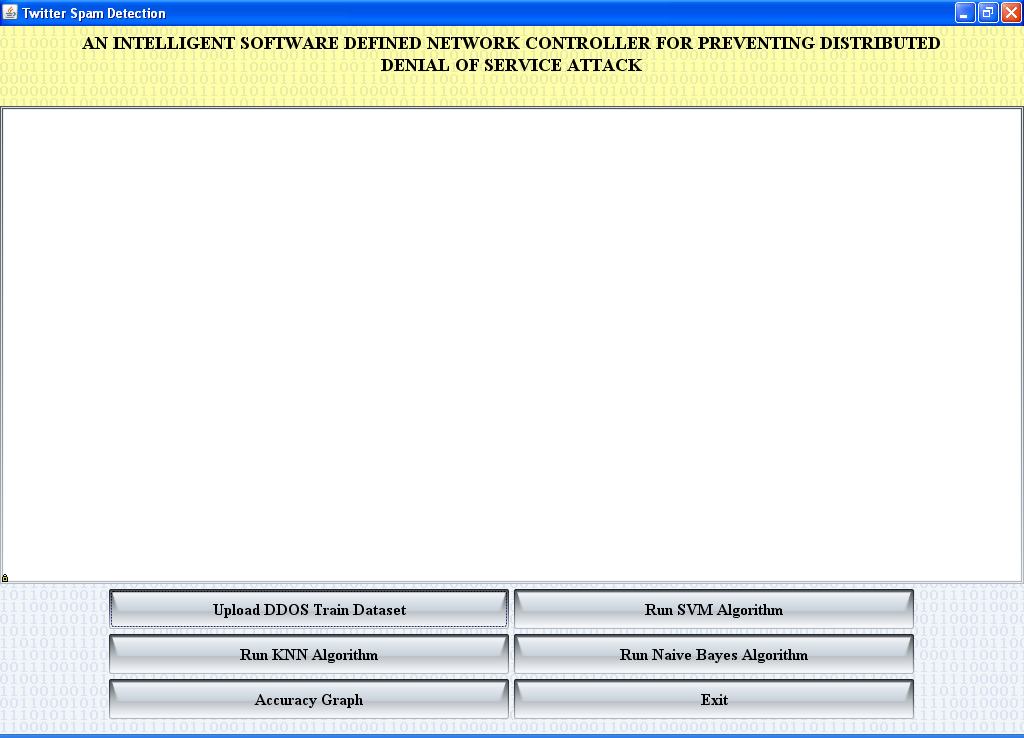
Signature checking and predicting packet contains attack or not can be done by using data mining algorithms called SVM, KNN or Naïve Bayes.

Author is using above three algorithms from weka tool to evaluate performance.

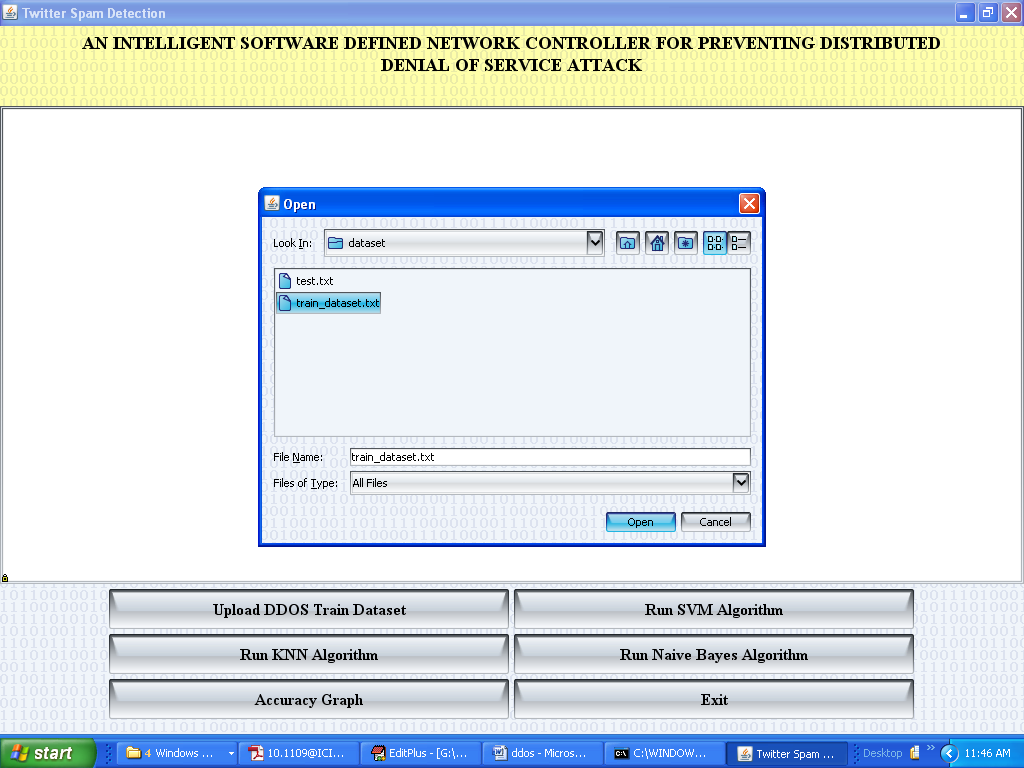
To implement above concept I have downloaded DDOS dataset from UCI machine learning website.

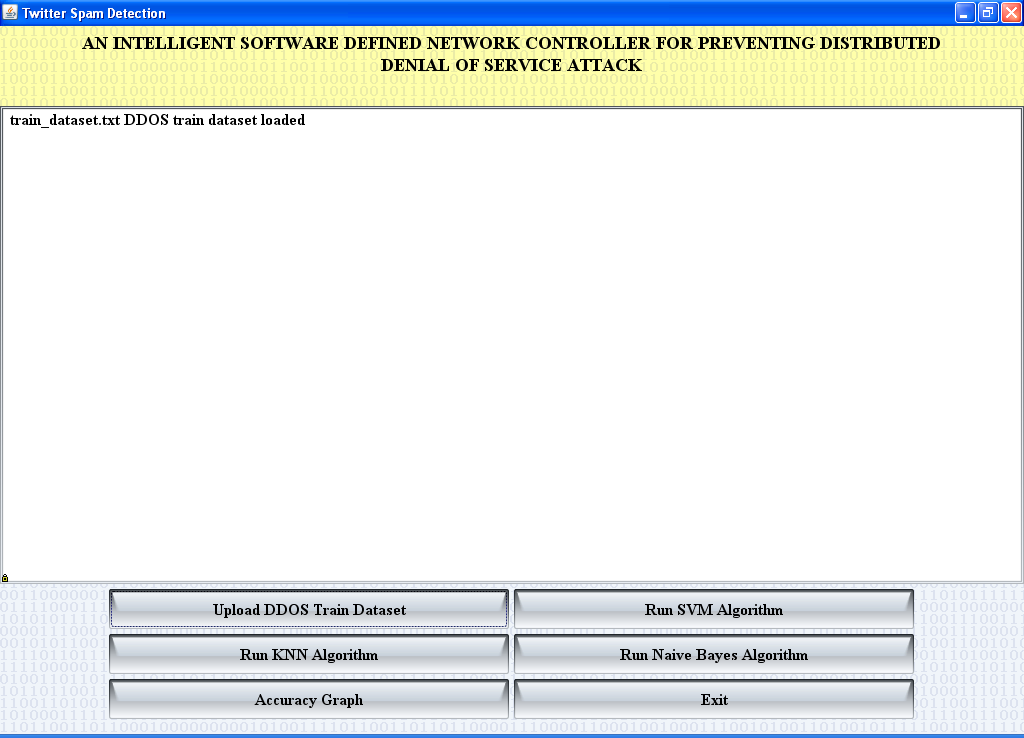
Train dataset is saved inside dataset folder and test dataset is also saved inside dataset folder

Screen shots

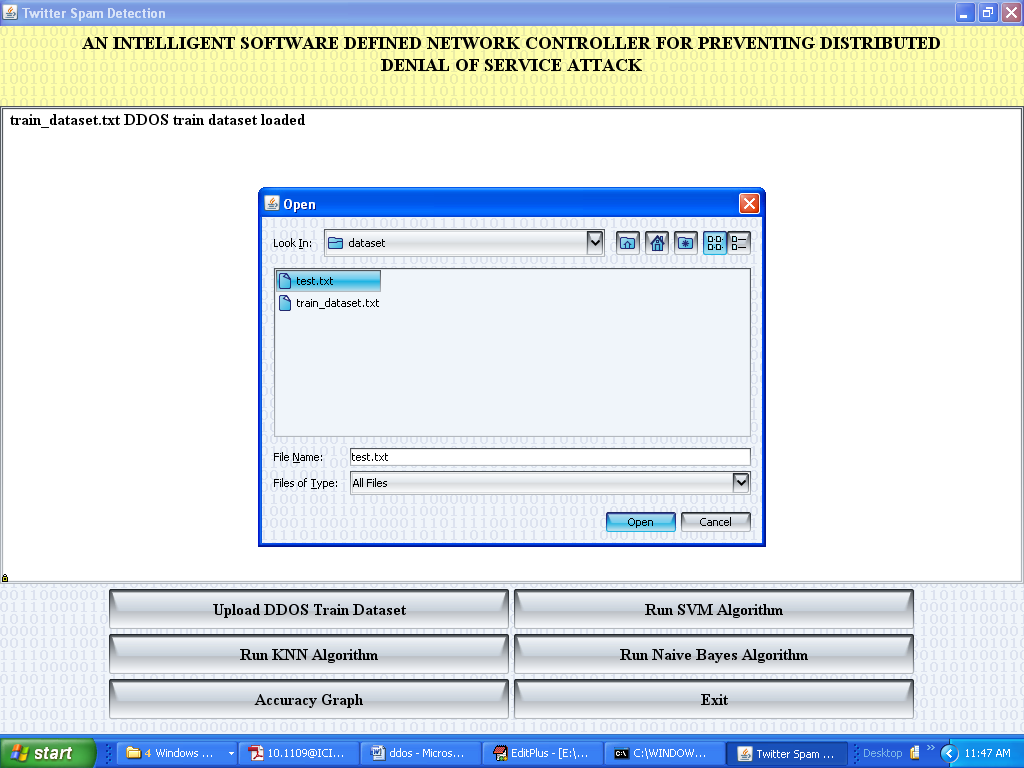


Click on ‘Upload DDOS Train Dataset’ button and upload train dataset

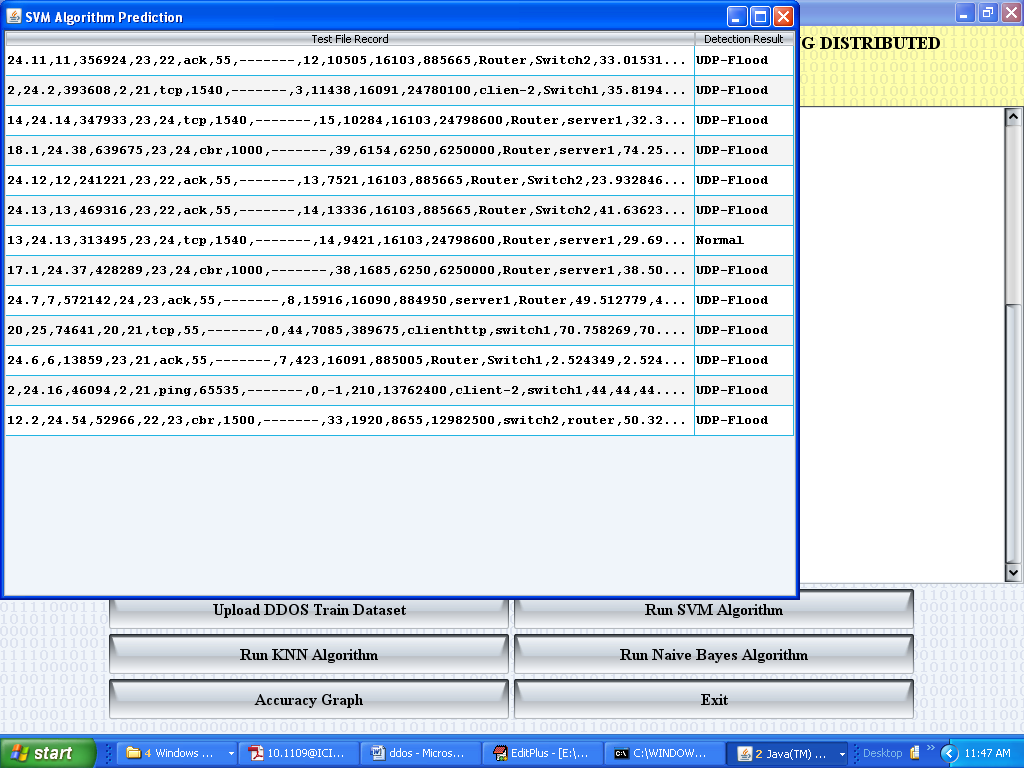




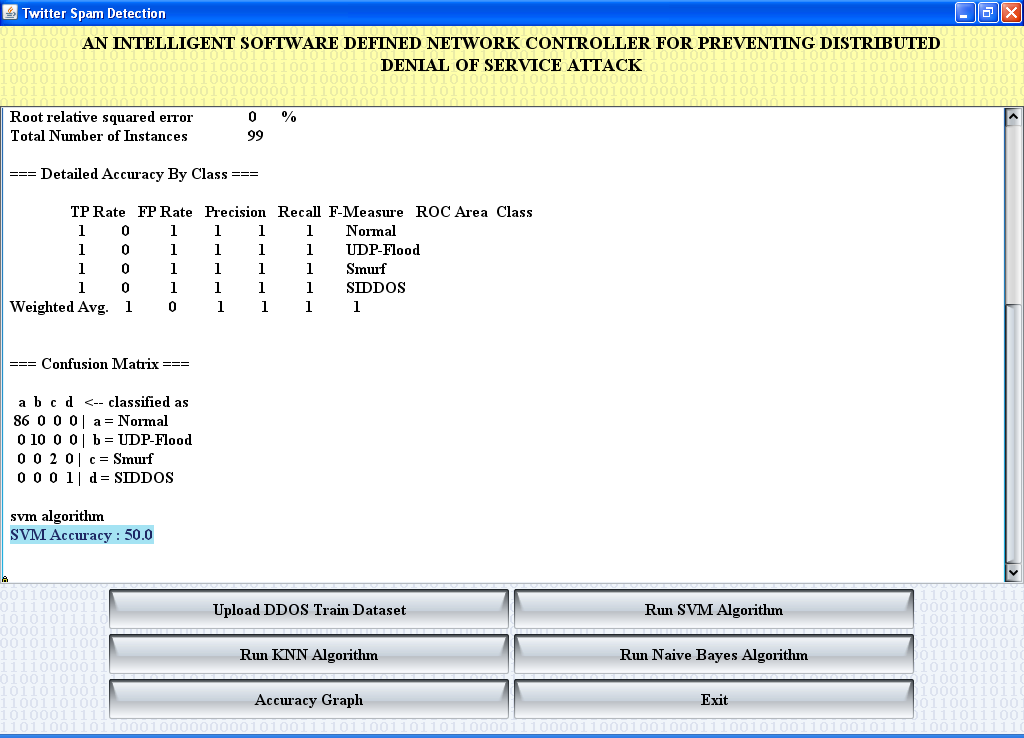
Now click on ‘Run SVM Algorithm’ button and upload test file



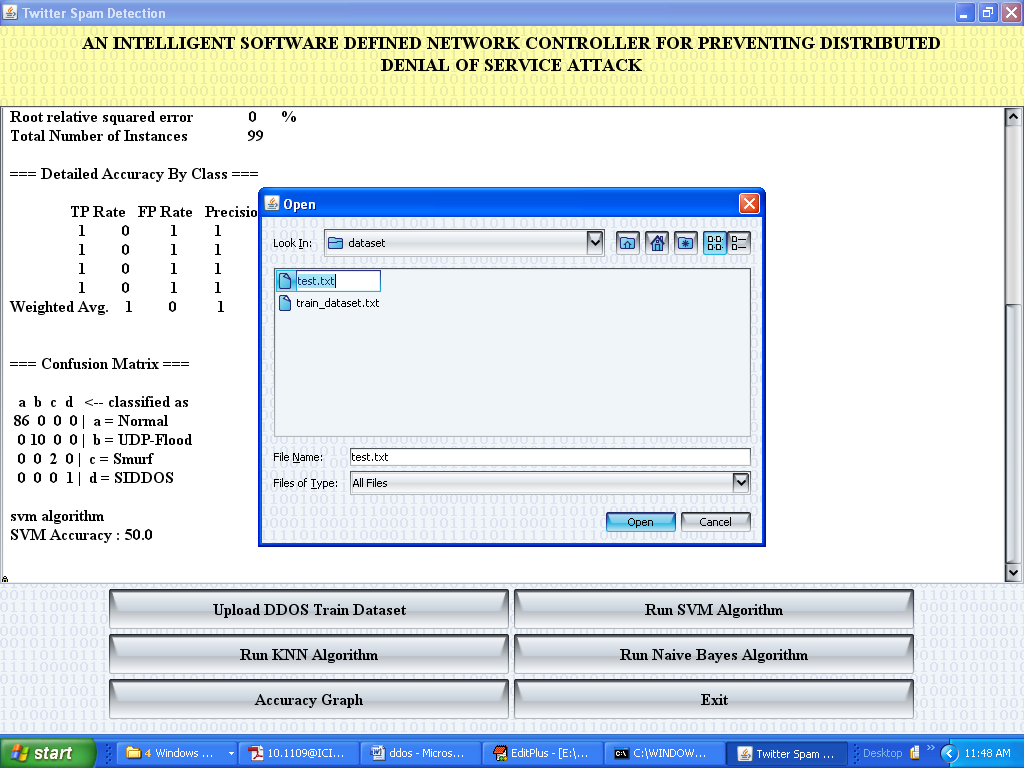
Below is the prediction for test dataset

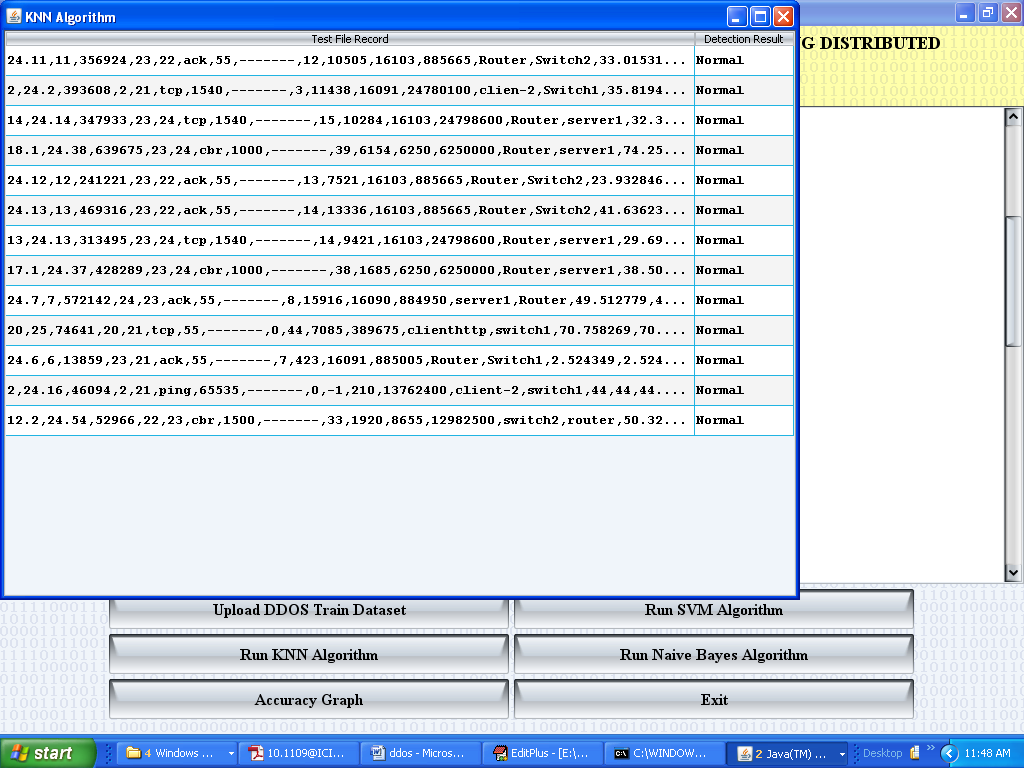


Below is SVM accuracy

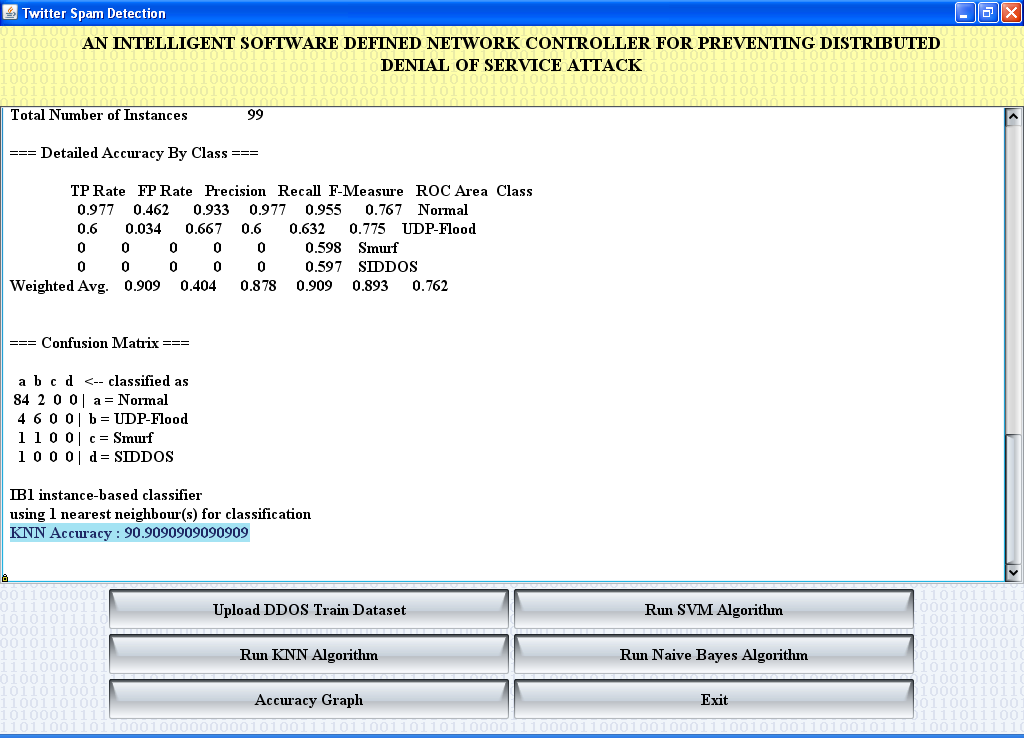


Now run KNN

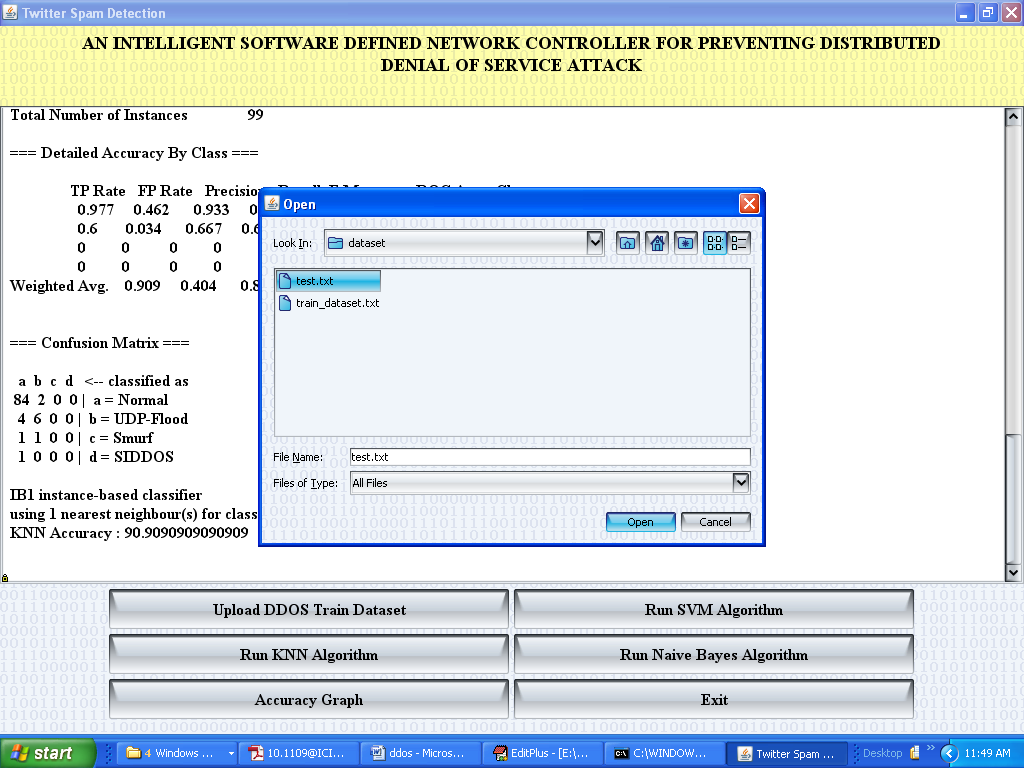




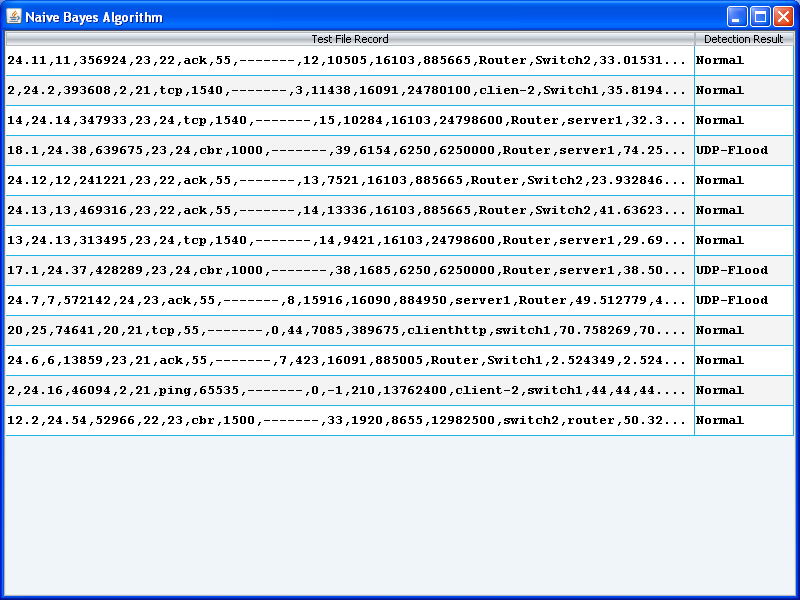
Below is KNN Accuracy



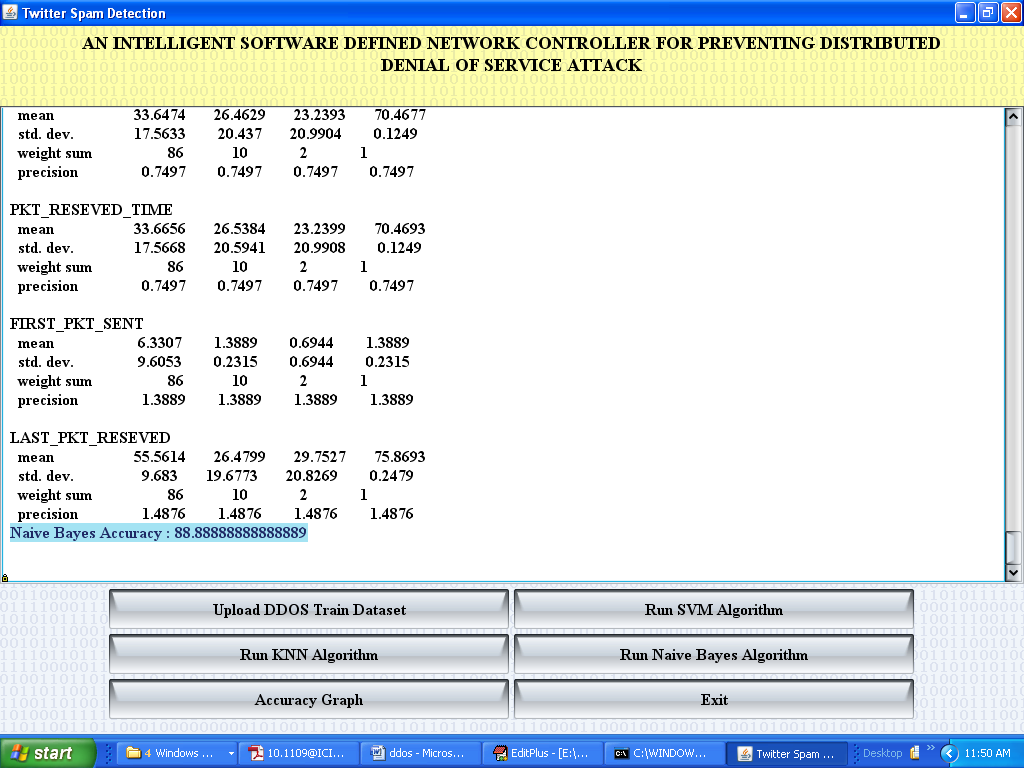
Now run naiye bayes



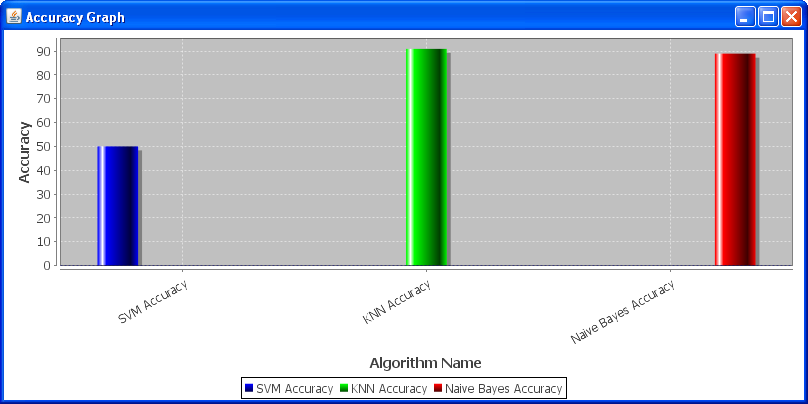
Below is naiye bayes prediction



Below is naïve bayes accuracy



Click on Accuracy graph button



In above graph x-axis represents algorithm name and y-axis represents accuracy