In today era modern infrastructures and technologies are more prone to various types of accesses. A method that is commonly used for launching these types of attack is popularly known as malware i.e. viruses, Trojan horses and worms, which, when propagate can cause a great damage to commercial companies, private users and governments. The another reason that enhance malware to infect and spread very rapidly is high-speed Internet connections as it has become more popular now a days, therefore it is very important to eradicate and detect new (benign) malware in a prompt manner. Hence in this work, proposing three data mining algorithms to produce new classifiers with separate features: RIPPER, Naïve Bayes and a Multi Classifier system along with hybrid of clustering techniques and the comparison between these methods to predict which provides better results.
Detection of Malicious Data using hybrid of Classification and Clustering Algorithms under Data Mining


Dr. R. Geetha Ramani, Suresh Kumar. S, Shomona Gracia Jacob, "Rootkit (Malicious Code) Prediction through Data Mining Methods and Techniques"; 978-1-4799-1597-2/13/$31.00 ©2013 IEEE.

Guillermo Suarez-Tangle, "Evolution, Detection and Analysis of Malware for Smart Devices"; IEEE communications surveys & tutorials, accepted for publication, 2013, pp. 1-27.


Index Terms

Computer Science

Data Mining

Keywords

Malicious Code Detection; Data Mining; Computer Security; Prediction