Abstract

This paper introduces Big data security analysis with the help of different techniques used in network intrusion detection system. The topic of how big data affects any intrusion detection system being used and how huge volume of the dataset, its specialized features that are heterogeneous in nature and what will happen if big data is processed at real time. Different attacks and intrusion detection methods such as intrusion detection and prevention systems (IDPS), signature-based detection (SD) and anomaly-based detection (AD) has been done. Challenges faced by intrusion detection systems (IDS), how they can be prevented and how machine learning, data mining techniques could be used in any general intrusion detection-based system has also been discussed. Also, how all the problem faced by IDPS can be solved by network simulator named NS-3.0. Its objectives, advantages, comparison with other networks and limitation have also been to be discussed. The recommendation is also given to improve faults. Also, results obtained after using NS-3 based svm classifier using KDD Cup 99 Dataset showed the accuracy of 99 percent.
References


Index Terms

Computer Science Security

Keywords

anomaly-based detection, big data security analysis, challenges, data mining, intrusion detection and prevention systems (IDPS) machine learning, network security, NS-3, signature-based detection, svm.