Abstract

Intrusion Detection System (IDS) are said to be more effective when it has both high intrusion detection (true positive) rate and low false alarm (false positive). But current IDS when implemented using data mining approach like clustering, classification alone are unable to give 100% detection rate hence lack effectiveness. In order to overcome these difficulties of the existing systems, many researchers implemented intrusion detection systems by integrating clustering and classification approach like k-means and Fuzzy logic, K-means and genetic algorithm, some of the researcher also tried use of Decision tree and Neural Network to detect unknown attacks. In this paper analysis of such Hybrid systems which are implemented by using the benchmark dataset compiled for the 1999 KDD intrusion detection contest, by MIT Lincoln Labs.

References

1. Myung-Sup Kim, Hun-Jeong Kang, Seong-Cheol Hong, Seung-Hwa Chung, and James
Performance Analysis of Intrusion Detection Systems Implemented using Hybrid Machine Learning Techniques

3. Drew Dean, Matt Franklin, and Adam Stubblefield
15. Preeti Aggarwal, Sudhir Kumar Sharma, 2015 "Analysis of KDD Dataset Attributes-class wise For Intrusion Detection", Procedia Computer Science, Elsevier


Index Terms

Computer Science  System Architecture

Keywords

Intrusion detection system (IDS), Detection rate in IDS, False alarm Rate, Classification, Prediction, MIT KDD’99 dataset.