Performance Analysis of Intrusion Detection Systems Implemented using Hybrid Machine Learning Techniques

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


Drew Dean, Matt Franklin, and Adam Stubblefield


15. [K. M. Faraoun and A. Boukelif, 2005 “Neural Networks Learning Improvement using the K-Means Clustering Algorithm to Detect Network Intrusions” International Journal of Computational Intelligence" Vol. 3 .


20. Jiawei Han and Mitcheline Kamber 2006, "Data Mining Concepts and approaches", 2e, Elsevier.
21. Hai Nguyen, Katrin Franke and Slobodan Petrovic 2010, "Improving Effectiveness of Intrusion Detection by Correlation Feature Selection", IEEE.

Index Terms

Computer Science System Architecture

Keywords

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