ISBN: 978-81-949112-9-6

Chapter 6 Intrusion Detection System Using Soft Computing Techniques

Manoj Kumar Behera and S. Chakravarty

Dept. of CSE, Centurion University of Technology and Management, Odisha, India

Abstract

Intrusion Detection System (IDS) defined as a software application which monitors the network or system activities and finds if there is any malicious activity occur. Through malicious actions, hackers can have unauthorized access that compromises the integrity, confidentiality, and the availability of resources or services. Intrusion detection systems (IDSs) have been developed to monitor and filter network activities by identifying attacks and alerting network administrators. Different IDS approaches have been emerged using data mining, machine learning, statistical analysis, and soft computing techniques such as Genetic Algorithms, Artificial Neural Networks, Fuzzy Logic, Swarm Intelligence, etc. However, higher-quality training data is an essential determinant that could improve detection performance. The experiment will be conducted on the NSL KDD dataset consists of a 20% training dataset, which is an advanced version of the KDDCUP99 dataset. In this paper, the work is based on developing a binary classification of Anomaly Based Intrusion Detection System with the help of Machine Learning techniques. The uses of PSO with NB return an RMSE of 0.0128 as compared to only Naïve Bayes which is 0.3271. The NB classifier combined with the Hybrid PSO Feature Selection method proves to be the best feature selection capability without degrading the classification