World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:8, No:09, 2014

Feature Based Unsupervised Intrusion Detection

Authors : Deeman Yousif Mahmood, Mohammed Abdullah Hussein

Abstract : The goal of a network-based intrusion detection system is to classify activities of network traffics into two major categories: normal and attack (intrusive) activities. Nowadays, data mining and machine learning plays an important role in many sciences; including intrusion detection system (IDS) using both supervised and unsupervised techniques. However, one of the essential steps of data mining is feature selection that helps in improving the efficiency, performance and prediction rate of proposed approach. This paper applies unsupervised K-means clustering algorithm with information gain (IG) for feature selection and reduction to build a network intrusion detection system. For our experimental analysis, we have used the new NSL-KDD dataset, which is a modified dataset for KDDCup 1999 intrusion detection benchmark dataset. With a split of 60.0% for the training set and the remainder for the testing set, a 2 class classifications have been implemented (Normal, Attack). Weka framework which is a java based open source software consists of a collection of machine learning algorithms for data mining tasks has been used in the testing process. The experimental results show that the proposed approach is very accurate with low false positive rate and high true positive rate and it takes less learning time in comparison with using the full features of the dataset with the same algorithm.

Keywords : information gain (IG), intrusion detection system (IDS), k-means clustering, Weka
Conference Title : ICCCISE 2014 : International Conference on Computer, Communication and Information Sciences, and Engineering
Conference Location : Paris, France
Conference Dates : September 22-23, 2014