Abstract

Intrusion detection is a detection of encroachment on the personal network or the private network to breach the security systems. This system provides analytical measures to gather information from various networks or computers to identify the cracks in the security systems caused by intruders. The sudden tremendous growth in the amount of internet users network intrusion detection has gained a huge amount of attention/need towards the research of network. Today, cyber-attacks have become a vital issue for any organization or individual in the network against preserving significant data and information in their personal computers connected to a network. In this paper, a comparative study was done on two different data mining techniques: decision tree and support vector machine algorithms. These techniques are implemented on the dataset for the experiment, since decision tree C5.0 technique and support vector machine (SVM) in general widely used in intrusion experiment data i.e. KDD CUP99 data set downloaded from UCI repository site. The better performance of C5.0 algorithm in terms of accuracy, sensitivity and specificity error measures are to be proved in this paper.
References

11. Shi Jnn Horng, "A Novel Intrusion Detection System Based On Hierarchical Clustering And Support Vector Machines" 2010
17. Wenyiing Feng, Qinglei Zhang, Gongzhu Hu, Jimmy Xiangji, Hwang, "Mining Network Data For Intrusion Through Combining Svms With Ant Colony Networks", Future Generation Computer Systems, 2013

Index Terms
Keywords

Support Vector Machine (SVM), Decision Tree Technique, NSL-KDD Data.