Abstract

In Information Security, intrusion detection is the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource. One of the primary challenges to intrusion detection is the problem of misjudgment, misdetection and lack of real time response to the attack. Various data mining techniques such as clustering, classification and association rule discovery are being used for intrusion detection. The proposed hybrid technique combines data mining approaches like K Means clustering algorithm and Support Vector Machine classification module. The main purpose of proposed technique is to decrease the number of attributes associated with each data point. So that, the proposed technique can perform better in terms of Detection Rate and Accuracy when applied to KDD’99 Data Set.

References

- Z. Muda, W. Yassin, M.N. Sulaiman, N.I. Udzir, “Intrusion Detection based on K-Means Clustering and Naïve Bayes Classification”, 2011 7th International Conference on IT in Asia
Attribute Reduction based Hybrid Anomaly Intrusion Detection using K-Means and SVM Classifier

(CITA).

- Hari Om, Aritra Kundu, “A Hybrid System for Reducing the False Alarm Rate of Anomaly Intrusion Detection System”, 1st Int’l Conf. on Recent Advances in Information Technology (RAIT) 2012 IEEE.

Index Terms

Computer Science

Security
**Keywords**

Intrusion detection system, K Means clustering, Support Vector Machine, KDD'99 Data Set.