An Intrusion detection system is a machine or software that monitors the traffic in a network and on detection of a malicious packet, informs the user or a specific acting unit which can take further action and avoid the malicious packet from entering the network. This paper discusses a way to implement an intelligent IDS which classifies the normal traffic in a network with abnormal or attacked ones. This paper explains the method used to generate such a system and the various classifiers used in the generation process.

The proposed system of Intrusion Detection, classifies data with three different classifiers and an Ensemble technique which selects the majority of the three classifiers to assign the packet in the network as anomaly or normal. The dataset used to train the classifiers is the NSL – KDD dataset. The IDS proposed serves many applications in the field of Military Systems, Banks and Social Networking websites where data is very sensitive. The paper also explains related work done in this field and briefly explains every classifier, the network attacks and the dataset.
References


Index Terms

Computer Science

Artificial Intelligence

Keywords

IDS, Intrusion Detection System, Artificial Intelligence, AI, Majority Voting, Ensemble Learning, Random Forest, SVM