ABSTRACT

A computer network attack is an activity that threatens network security by attacking all or part of a particular area of network resources. In order to detect or prevent various potential attacks, an Intrusion Detection System (IDS) has been developed where this IDS has two methods of detection, namely Rule Based (Signature Based) and Behavior Based. In this study we use the methods of behavior based where in the process of its works require a dataset and methods. The non-machine learning Intrusion Detection System (IDS) method is currently not very accurate, therefore an IDS method with more accurate machine learning is needed to detect attacks. To address this problem, the study compares the K-Nearest Neighbor and Support Vector Machine methods to optimally detect the intrusion. In this study, implementations used KNN, SVM Polynomial and SVM Sigmoid methods in detecting HTTPDoS attacks using ISCX 2012 testbed June 14 datasets with 157,867 packets and 19 features. This study performs a comparative analysis of the methods resulting from the classification process in the form of a confusion matrix and ROC curve. From the study is proven that method of K-Nearest Neighbor with the percentage of 99,994% has a very excellent quality to classify network intrusion.

Keywords—**IDS, KNN, SVM *Polynomial*, SVM *Sigmoid***