ABSTRACT

With increasing usage of internet, the cyber threat will also increasing which makes cyber security become something that must have for every service provider. Because cyber threat not only can damage service provider's system but also can steal user's personal data that use service from service provider. If this happen not only loss on service provider but also on users. That's where Intrusion Detection System comes in. IDS can detect cyber attack automatically and can help reduce attack that comes to system.

In this Final Assignment was designed Decision Tree, Random Forest, and AdaBoost classfier to detecting attack and would be analyzed which more efficient based on time and performance from those three classifiers. This comparative classifier was done by getting datasets, preprocessing datasets, features selection, training classifiers, testing classifiers, and evaluating classifiers result. Datasets used were KDDcup99 dataset and manual dataset. From 41 features in KDDcup99, chosen 14 features to be used in this Final Assignment.

The results are Decision Tree classifier is the most efficient classifier based on time and performance with the outcome in training time 9.35 second and predict time 1.42 second. The performance from classifier are Precision 96.41%, Recall 100%, and Accuracy 97.05%. Random Forest is the second most effient because compared with Decision Tree, Random Forest performance is fluctuative. On the other hand, AdaBoost is not very efficient to detecting attack because time needed for AdaBoost to train classifier (178.64 second) and predict attack (21.56 second) are too long.

Keywords: *Decision Tree, Random Forest, AdaBoost, Intrusion Detection System, Classifier, Confusion Matrix, KDDcup99*