Abstract
Intrusion Detection System (IDS) acts as a detector of various types of attacks on computer networks. IDS identifies attacks based on network data classification. Nowadays, some IDS classification methods still have their respective deficiencies and advantages. One of the problems in the IDS is the level of performance accuracy is still low. Some of the factors that affect IDS accuracy performance include the training of outdated datasets, imbalance of training data and the selection of classification methods becomes a challenge for this research. By conducting a literature study on non-IDS classification, a method that has good classification performance, AdaBoost. Meanwhile, to handle the imbalance of data, Synthetic Minority Oversampling Technique (SMOTE) becomes one way to handle the problems. Principal Component Analysis (PCA) and Ensemble Feature Selection (EFS) can be applied as feature selection on the IDS dataset. So these methods researchable for performance in IDS data classification. Therefore, in this final project we propose several schemes to improve IDS performance on CIC 2017 dataset. The empirical results show that the AdaBoost classification using PCA and SMOTE yields AUC 92% and the AdaBoost classification using EFS and SMOTE produces an accuracy of 81.83 %, precision 81.83%, 100% recall, and F1 Score 90.01% higher than the AdaBoost classification in the previous study only had 77% precision value, 84% recall and 77% F1 Score.

***Keyword: Intrusion Detection System*, DDoS, AdaBoost, SMOTE, PCA.**