ABSTRAK

Ancaman siber yang banyak muncul dengan bertambahnya pengguna internet membuat keamanan siber menjadi hal yang penting untuk dimiliki oleh penyedia layanan. Karena ancaman siber tidak hanya merusak sistem penyedia layanan, tapi juga dapat mengambil data yang dimiliki oleh penyedia layanan tersebut. Bila hal ini terjadi dapat merugikan pihak penyedia layanan itu sendiri dan juga pengguna layanan tersebut. Dengan *Intrusion Detection System* yang dapat mendeteksi serangan siber secara otomatis dapat membantu dalam mengurangi serangan yang dapat masuk kedalam sistem.

Didalam Tugas Akhir ini, didesain pendeteksi serangan menggunakan klasifier *Decision Tree*, *Random Forest*, dan *AdaBoost* dan dianalisa klasifier manakah yang paling efisien dalam hal waktu dan performa dari ketiga klasifier yang digunakan. Perbandingan klasifier ini dilakukan dengan cara mendapatkan dataset, *preprocessing* dataset, pemilihan fitur yang digunakan, *training* klasifier, *testing* klasifier, lalu yang terakhir mengevaluasi hasil klasifier. Dataset yang digunakan adalah dataset KDDcup99 dan dataset manual. Dan fitur yang digunakan berjumlah 14 dari total 41 fitur dalam KDDcup99.

Hasil yang didapatkan adalah klasifier *Decision Tree* menjadi klasifier yang paling efisien dalam hal waktu dan performa. Dengan hasil: lama melatih klasifier 9,35 detik, memprediksi serangan 1,42 detik, *Precision* 96,41%, *Recall* 100%, dan *Accuracy* 97,05%. *Random Forest* merupakan klasifier kedua yang efisien untuk mendeteksi serangan karena dibandingkan *Decision Tree*, *Random Forest* memiliki hasil yang fluktuatif pada performanya. *AdaBoost* kurang efisien untuk mendeteksi serangan dikarenakan waktu yang dibutuhkan untuk melatih klasifier (178.64 detik) dan memprediksi serangan (21.56 detik) terlalu lama.

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