ABSTRAK

Serangan jaringan komputer adalah aktivitas yang mengancam keamanan jaringan dengan menyerang seluruh atau sebagian di area tertentu sumber daya jaringan. Untuk mendeteksi atau mencegah berbagai potensi serangan telah dikembangkan *Intrusion Detection System* (IDS) dimana IDS ini mempunyai dua metode dalam melakukan pendeteksian yaitu *Rule Based (Signature Based)* dan *Behavior Based*. Metode *Intrusion Detection System* (IDS) *non-machine learnin*g untuk sekarang keakuratannya tidak terlalu baik, karena itu dibutuhkan metode IDS dengan *machine learning* yang lebih akurat untuk mendeteksi serangan. Untuk mengatasi permasalahan ini, penelitian ini membandingkan metode *Support Vector Machine* dan *K-Nearest Neighbor* untuk mendeteksi serangan jaringan komputer secara optimal. Di penelitian ini, implementasi menggunakan metode KNN, SVM Polynomial dan SVM Sigmoid dalam mendeteksi serangan HTTPDoS menggunakan ISCX 2012 dataset testbed 14 Juni yang terdiri dari 157.867 paket dengan 19 fitur. Penelitian ini melakukan analisis perbandingan metode yang dihasilkan dari proses klasifikasi berupa *confusion matrix* dan kurva ROC. Hasil yang diperoleh dari penelitian ini adalah metode KNN dengan persentase 99,994% memiliki kualitas klasifikasi data yang sangat baik dibandingkan dengan SVM Polynomial dan SVM Sigmoid.

Kata kunci—**IDS, KNN, SVM Polynomial, SVM Sigmoid**