Abstrak

SYN Flood adalah salah satu jenis serangan DDoS yang paling sering terjadi, serangan ini memanfaatkan TCP *three – way handsake* untuk membuat koneksi dengan *server* yang memiliki tujuan untuk mengganggu dan menolak paket pengguna dengan memenuhi permintaan target yang sangat besar. Sedangkan UDP Lag tersendiri yaitu sebuah upaya memecahkan koneksi antara *client* dan *server*. Dalam beberapa tahun terakhir, penelitian terkait menggunakan algoritma *machine learning* untuk mendeteksi serangan DDoS dengan metode yang berbeda-beda.Tahapan yang dilakukan mendeteksi serangan SYN Flood dan UDP Lag yaitu perancangan sistem, pengumpulan data, pengembangan algoritma, identifikasi dan analisa data. Penelitian yang dilakukan sangat berkaitan dengan metrik uji seperti *precision, recall,* dan *accuracy*. Perolehan nilai dari *precision, recall,* dan *accuracy* sangat dipengaruhi dengan pemilihan algoritma *machine learning* yang digunakan saat mendeteksi serangan. Beberapa literature deteksi serangan SYN Flood dan UDP Lag memiliki nilai akurasi yang rendah dengan pemilihan algoritma yang digunakan. Dengan adanya masalah yang ada, penelitian yang dilakukan penulis dalam deteksi serangan SYN Flood dan UDP Lag dengan merancang dan membangun sistem dengan menggunakan 3 pilihan algoritma machine learning yang meliputi *ensemble learning, logistic regression,* dan *decision tree* dengan tujuan dapat meningkatkan efektivitas deteksi, dapat mengatasi masalah yang timbul dalam deteksi serangan SYN Flood dan UDP Lag dalam penelitian yang dijalankan dengan harapan penelitian ini memiliki capaian 100% *precision*, 100% *recall*, dan 100% *accuracy*.

Kata Kunci: SYN Flood, UDP Lag, machine learning, DDoS.