Bab I

Pendahuluan

1.1 Latar Belakang

Pada kuartal pertama tahun 2019, SYN Flood menduduki peringkat pertama sebagai jenis serangan DDoS yang paling sering terjadi dengan 84,00%, yang dibandingkan dengan kuartal empat pada tahun 2018 terjadi dengan 58,20% [28]. Adanya kenaikan serangan SYN Flood ini menjadikan masalah berbahaya untuk pengguna yang bisa mengganggu rutinitas setiap hari.

Dalam kasus serangan SYN Flood, korban yang telah terkena serangan mempunyai masalah terhadap jaringan. Kondisi ini disebabkan oleh pelaku serangan yang menggunakan IP *address* palsu dengan mengirim SYN paket secara berulang kepada perangkat korban, *server* korban menerima sejumlah besar paket SYN yang mengakibatkan sambungan yang ada memiliki beberapa permintaan dengan paket SYN ACK. *Client* kewalahan sehingga gagal mengirimkan ACK yang diharapkan dan adanya IP *address* yang telah dipalsukan membuat SYN ACK terakhir tidak diterima. Serangan yang masih berjalan membuat *server* menunggu adanya SYN ACK, yang mengakibatkan *server* tidak bisa menutup koneksi yang ada dan membuatnya terbuka. Paket SYN ACK dibutuhkan untuk dapat menyelesaikan *three-way handsake* melalui protocol TCP [17]. Antrian yang berada di *server* yang terbuka menimbulkan masalah sehingga *server* menjadi kewalahan dan mengakibatkan semua permintaan masuk yang dari klien sah dibatalkan. Untuk UDP Lag memiliki cara kerja yang dimana melakukan upaya memecahkan koneksi antara *client* dan *server* dengan *lag switch* maupun program *software* yang terhubung dengan jaringan[36].

Saat ini sudah ada beberapa penelitian terkait deteksi serangan SYN Flood dan UDP Lag menggunakan metode *machine learning*. Metode yang dipakai umumnya menggunakan teknik dari algoritma *supervised learning* dan *unsupervised learning*. Alur yang ada dalam penelitian yang sudah dilakukan dengan pemilihan *dataset* yang ada untuk dijadikan *input* data, lalu dilakukan *training* data dan klasifikasi untuk memudahkan jenis serangan yang terdapat didalam *dataset*. Proses selanjutnya dilakukan uji metrik yang beberapa diantaranya ada *precison, recall* dan *accuracy* untuk mengetahui hasil dari penelitian yang

telah dilakukan.

Beberapa penelitian deteksi serangan SYN Flood dan UDP Lag yang telah ada, salah satunya terdapat penelitian yang dikemukakan oleh oleh Dr. Sumathi dan R. Rajesh pada tahun 2021 yang didalamnya terlalu banyak yang berfokus dengan algoritma *unsupervised learning*. Selain dari teknik algoritma, pembahasan mengenai metrik uji yang didalamnya terkait dengan *accuracy* didalam penelitian tersebut belum ada. Harapan dengan adanya nilai *accuracy* juga dapat menjadi salah satu indikator untuk seberapa akurat penggunaan algoritma dalam mendeteksi serangan SYN Flood dan UDP Lag yang diteliti.

1.2 Perumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah tugas akhir ini adalah sebagai berikut:

1. Bagaimana cara merancang studi literatur terkait serangan SYN Flood dan UDP Lag?
2. Bagaimana melakukan studi algoritma *machine learning* untuk mendeteksi serangan SYN Flood dan UDP Lag?
3. Bagaimana analisa kinerja deteksi serangan SYN Flood dan UDP Lag berdasarkan algoritma *machine learning*?

1.3 Pernyataan Masalah

Berdasarkan latar belakang di atas, dapat disimpulkan terdapat permasalahan pada algoritma *machine learning* dan deteksi yang sudah ada sebagai berikut:

1. Algoritma *machine learning* yang ada masih menghasilkan akurasi deteksi yang rendah.
2. Perbandingan algoritma terhadap hasil deteksi serangan SYN Flood dan UDP Lag masih jarang dilakukan.
3. Performansi dari pengembangan sistem deteksi serangan SYN Flood dan UDP Lag masih rendah.

1.4 Tujuan

1. Melakukan studi literatur terkait serangan SYN Flood dan UDP Lag.
2. Melakukan studi berbasis *ensemble learning* dengan algoritma Random Forest, Adaboost, Stacking.
3. Melakukan analisis kinerja dari algoritma Random Forest, Adaboost, Stacking.

1.5 Batasan Masalah

Berikut adalah ruang lingkup yang ada pada penulisan tugas akhir ini :

1. Jenis serangan yang dideteksi hanya serangan SYN Flood dan UDP Lag yang percobaannya dilakukan secara 1 kali ketika percobaan berjalan.
2. Objek yang digunakan untuk mendeteksi serangan SYN Flood dan UDP Lag diambil dari *dataset*.
3. Metode yang digunakan dalam penelitian akan diimplementasikan menggunakan algoritma *machine learning*.

1.6 Hipotesis

1. Algoritma deteksi serangan SYN Flood dan UDP Lag yang diusulkan dalam penelitian ini menghasilkan akurasi keberhasilan sistem yang dibangun.
2. Performansi algoritma dari sistem yang dikembangkan lebih akurat dibanding yang sudah ada.

1.7 Sistematika Penulisan

Tugas Akhir ini disusun dengan sistematika penulisan sebagai berikut :

- **BAB I Pendahuluan**. Bab ini membahas mengenai latar belakang, pernyataan masalah, batasan masalah, hipotesis dan tujuan pengerjaan Tugas Akhir ini.
- **Bab II Kajian Pustaka**. Bab ini membahas fakta dan teori yang berkaitan dengan penelitian sistem deteksi serangan SYN Flood dan UDP Lag untuk mendirikan landasan berfikir serta acuan dalam melakukan pengerjaan.
- **BAB III Metodologi dan Desain Sistem**. Bab ini menjelaskan metode penelitian, rancangan sistem, kebutuhan sistem, data dan metrik uji yang dilakukan dalam penelitian sistem deteksi serangan SYN Flood dan UDP Lag.
- **BAB IV Hasil dan Pembahasan**. Bab ini membahas hasil serta melakukan uji metrik dalam penelitian sistem deteksi serangan SYN Flood dan UDP Lag.
- **BAB V Kesimpulan dan Saran**. Bab ini merupakan kesimpulan dalam penelitian sistem deteksi serangan SYN Flood dan UDP Lag serta saran untuk penelitian yang akan mendatang.