ABSTRAK

Software Defined Network (SDN) merupakan arsitektur jaringan modern yang memisahkan control plane dan data plane, dengan kontroler sebagai pusat pengendali. Meskipun menawarkan efisiensi dan fleksibilitas, arsitektur ini menjadikan kontroler sebagai titik yang rawan diserang. Serangan *Distributed Denial of Service* (DDoS) jenis SYN Flood yang ditujukan ke kontroler dapat membanjiri sistem dengan permintaan koneksi palsu, menyebabkan konsumsi sumber daya secara berlebihan, dan membuat kontroler gagal memproses paket normal, sehingga layanan tidak dapat diakses oleh pengguna.

Penelitian ini mengembangkan sistem deteksi dan mitigasi serangan *SYN Flood* berbasis *Support Vector Machine* (SVM) dan mekanisme *rate limiting* menggunakan algoritma *token bucket*. Model SVM dilatih menggunakan dataset lalu lintas jaringan dari internet. Proses pelatihan dilakukan dengan pembagian data (*train-validation-test*) dan optimasi *hyperparameter* menggunakan Optuna, menghasilkan akurasi sebesar 96.64% yang mencerminkan kemampuan model dalam membedakan paket normal dan paket serangan.

Model kemudian diintegrasikan ke dalam Ryu Controller dan diuji melalui 23 skenario serangan, masing-masing diulang 4 kali, dengan variasi sumber IP statis, acak, dan kombinasi. Hasil pengujian menunjukkan *false negative* rata-rata hanya 1,2–1,5 paket per *trial*, dan tingkat mitigasi terhadap paket serangan mencapai 98–99%. Sistem juga mampu menjaga *packet loss* pada paket normal tetap mendekati 0% di 83 dari 92 *trial*. Pada sisa 9 *trial* dengan serangan intensif, *packet loss* tercatat sangat rendah (hanya 0,83%).

Sistem dilengkapi dengan monitoring real-time menggunakan Prometheus dan Grafana, serta notifikasi otomatis melalui Telegram bot, sehingga administrator dapat memantau kondisi kontroler secara pasif. Hasil ini membuktikan sistem mampu mempertahankan layanan SDN secara otomatis, efisien, dan adaptif saat terjadi serangan *SYN Flood*.

Kata kunci — ***Software Defined Network, SYN Flood, Rate Limiting, Support Vector Machine, Network*** **Monitoring**