ABSTRAK

Software-Defined Networking (SDN) adalah pendekatan baru dalam pengelolaan jaringan yang memisahkan antara *control plane* dan *data plane*. Dengan arsitektur ini, pengaturan jaringan dapat dilakukan secara lebih fleksibel melalui perangkat lunak seperti *controller Ryu*. Namun, SDN juga memiliki tantangan serius dalam hal keamanan, salah satunya adalah serangan *Distributed Denial of Service* (DDoS) berbasis *HTTP Flood* yang dapat menyebabkan gangguan layanan. Penelitian ini bertujuan untuk menerapkan dan menganalisis teknik rate limiting pada *controller Ryu* sebagai upaya mitigasi terhadap serangan *HTTP Flood*. Pengujian dilakukan dalam tiga skenario: lalu lintas normal, serangan tanpa mitigasi, dan serangan dengan mitigasi. Data lalu lintas dianalisis menggunakan algoritma *Support Vector Machine* (SVM) untuk mengklasifikasikan antara trafik normal dan serangan. Evaluasi difokuskan pada parameter *Round Trip Time* (RTT) dan *confusion matrix*. Hasil pengujian menunjukkan bahwa penerapan mitigasi mampu menurunkan nilai RTT maksimum secara signifikan. Pada skenario dua host penyerang, nilai RTT maksimum turun dari 707.569 ms menjadi 100.681 ms setelah penerapan *Rate Limiting*. Selain itu berdasarkan evaluasi dengan *confusion matrix*, sistem klasifikasi yang dikembangkan mencapai akurasi sebesar 94% - 96%, menunjukkan kinerja cukup baik. Penelitian ini menyimpulkan bahwa integrasi antara *rate limiting* dan SVM dapat menjadi pendekatan yang efisien dalam deteksi serta mitigasi serangan DDoS pada SDN. Saran untuk penelitian berikutnya adalah memperluas cakupan jenis serangan dan mengembangkan pendekatan yang lebih adaptif dan real-time.

Kata Kunci: *Software Defined Networking*, *HTTP Flood*, *Rate Limiting*, *Ryu Controller, Support Vector Machine*, Mitigasi Serangan, RTT