ABSTRAK

Pertumbuhan penggunaan internet yang pesat telah meningkatkan risiko terhadap ancaman siber, termasuk serangan *Distributed Denial of Service* (DDoS) berbasis *DNS Amplification*. Serangan ini mengeksploitasi *open DNS resolver* untuk mengirimkan respons DNS berukuran besar ke target dengan memalsukan alamat IP sumber, sehingga membanjiri infrastruktur jaringan target dan mengganggu performa layanan atau bahkan membuatnya tidak dapat diakses. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem deteksi dan mitigasi serangan *DNS Amplification* secara *real-time* pada *Software-Defined Network* (SDN) dengan metode *Access Control List* (ACL) menggunakan *Ryu Controller*. Pendekatan deteksi yang digunakan mencakup pelatihan model klasifikasi *Support Vector Machine* (SVM) berbasis fitur lalu lintas jaringan yang diekstrak dari paket UDP pada *port* 53. Dataset dibangun melalui simulasi trafik normal dan serangan menggunakan Mininet dan Scapy, kemudian dievaluasi menggunakan *confusion matrix* dan metrik klasifikasi. Hasil pengujian menunjukkan bahwa sistem mampu mendeteksi serangan dengan akurasi 94,69%, dengan kemampuan memblokir 6.584 dari 7.367 paket serangan secara otomatis melalui injeksi *flow rule* ACL. Meskipun masih terdapat *false negative* sebesar 5,31% yang menunjukkan adanya ruang untuk peningkatan sensitivitas model, tingkat keberhasilan mitigasi mencapai 78,97%. Temuan ini menunjukkan bahwa pendekatan SDN berbasis *machine learning* dan mitigasi dinamis yang dikembangkan efektif dalam menangani serangan DDoS, sekaligus menjaga kelangsungan trafik normal.

Kata kunci—***Access Control List,* DDoS*, DNS Amplification*, SDN, SVM*, Ryu Controller***