

ABSTRAK

Perkembangan *Software Defined Network* meningkatkan fleksibilitas pengelolaan jaringan dengan memisahkan control plane dan data plane, namun rentan terhadap serangan *Distributed Denial of Service* berbasis *SNMP Amplification* yang membanjiri port SNMP (161) dengan paket UDP. Penelitian ini mengembangkan sistem deteksi dan mitigasi menggunakan *Support Vector Machine* untuk deteksi dan *Access Control List* untuk mitigasi pada SDN. Simulasi dilakukan dengan Mininet dan Ryu Controller pada topologi dua switch dan sepuluh host IP 10.0.0.1–10.0.0.10. Data lalu lintas diambil via *Traffic_Logger.py*, menghasilkan fitur seperti *packet count*, *packet rate*, dan *packet size average*, diolah dengan Pandas dan NumPy. Model *Support Vector Machine* dengan kernel RBF dilatih 70% pelatihan, 30% pengujian, mendeteksi serangan berdasarkan ambang batas fitur. ACL diterapkan dinamis via Ryu Controller dan iptables. Pengujian meliputi skenario normal, serangan, dan mitigasi. Hasil menunjukkan akurasi SVM >90% dan mitigasi *Access Control List* efektif memulihkan performa jaringan. Hasil juga menunjukkan penurunan *packet loss* dari 20% menjadi 2% setelah dilakukan mitigasi, menandakan bahwa ACL efektif dalam memitigasi serangan *SNMP Amplification*. Visualisasi real-time via Matplotlib mempermudah pemantauan. Penelitian ini berkontribusi pada keamanan *Software Defined Network*, meski terbatas pada simulasi.

Kata kunci—***Software Defined Network, Distributed Denial of Service, SNMP Amplification, Support Vector Machine, Access Control List, Mininet, Ryu Controller.***