# ABSTRAK

SDN merupakan arsitektur jaringan yang memisahkan fungsi kontrol dan pengiriman data, sehingga memungkinkan pengelolaan lalu lintas dilakukan secara terpusat melalui *controller*. Meskipun fleksibel, pendekatan ini rentan terhadap serangan DDoS, termasuk *DNS Amplification*. Serangan ini memanfaatkan *server* DNS terbuka untuk mengirimkan respons dalam volume besar ke target melalui teknik IP *spoofing*, dengan ukuran rata-rata paket sebesar 72 *byte*. Jika tidak dikendalikan, lalu lintas ini dapat membanjiri *controller* dan menurunkan kinerja jaringan. Penelitian ini mengimplementasikan teknik mitigasi *rate limiting* yang dikendalikan oleh *controller*, dengan ambang batas sebesar 20 permintaan DNS dari satu alamat IP dalam interval 10 detik. Ketika ambang tersebut tercapai, permintaan dari IP terkait dibatasi agar tidak menghasilkan respons dari *server* DNS. Pengujian dilakukan dalam tiga skenario, yaitu kondisi normal, kondisi serangan tanpa mitigasi, dan kondisi serangan dengan mitigasi. Pada pengujian dengan enam *host* penyerang, nilai rata-rata RTT tanpa mitigasi mencapai 32.458 ms, sedangkan dengan mitigasi menurun menjadi 14.860 ms. Jumlah *False Positive* (FP) meningkat dari 428 menjadi 2.219, dan *False Negative* (FN) dari 116 menjadi 563 pada kondisi tanpa mitigasi. Namun, pada skenario mitigasi, *True Positive* (TP) tercatat sebesar 21.781 dan *True Negative* (TN) sebesar 6.003. Akurasi model turun dari 94,70% (2 *host*) menjadi 90,90% (6 *host*), dan berada dalam kisaran 90,88% sampai 94,55% setelah mitigasi diterapkan. Hasil ini menunjukkan bahwa penerapan *rate limiting* dengan *threshold* yang telah ditentukan dapat membatasi lalu lintas berbahaya dan mempertahankan stabilitas SDN saat terjadi serangan.

**Kata kunci: SDN, *DNS Amplification*, *Rate Limiting*, *Confusion Matrix***