ABSTRAK

Pada era digital yang semakin kompleks, serangan siber jenis Distributed Denial of Service (DDoS) telah menjadi ancaman serius bagi keamanan jaringan, karena mampu melumpuhkan sistem dan layanan dengan membanjiri target menggunakan lalu lintas data yang berlebihan. Penelitian ini mengusulkan sistem deteksi serangan DDoS inovatif yang menggabungkan kekuatan jaringan yang terdefinisi perangkat lunak (Software-Defined Network/SDN) dengan algoritma pembelajaran mesin Random Forest. Data lalu lintas dianalisis untuk menghasilkan fitur-fitur seperti jumlah paket, waktu antar paket, dan ukuran rata-rata paket. Fitur-fitur ini digunakan karena dikenal memiliki kemampuan diskriminatif tinggi dalam mendeteksi pola anomali. Selanjutnya, model yang telah dilatih diintegrasikan ke dalam kontroler SDN, seperti Ryu Controller, sehingga mampu mendeteksi pola lalu lintas mencurigakan secara cepat dan akurat. sistem ini menunjukkan efektivitasnya dengan tingkat akurasi deteksi sebesar 88%. Hasil ini menunjukkan bahwa kombinasi teknologi SDN dan Random Forest memberikan solusi yang andal dalam melindungi infrastruktur digital dari serangan DDoS, sehingga dapat mencegah kerusakan signifikan pada sistem jaringan.

Kata kunci — ***Software Defined Network (SDN), Distributed Denial of Service (DDoS), Random Forest***