ABSTRAK

Serangan *User Datagram Protocol (UDP) Flood* merupakan salah satu bentuk *Distributed Denial of Service (DDoS)* yang dapat mengganggu ketersediaan layanan jaringan dengan membanjiri target menggunakan paket UDP dalam jumlah besar. Dalam arsitektur *Software Defined Network (SDN)*, fungsi pengambilan keputusan terpusat berada pada *controller*. Meskipun menawarkan fleksibilitas dan kemudahan manajemen lalu lintas, sifat terpusat ini menjadikan controller sebagai *single point of failure* yang sangat krusial—jika controller diserang atau kelebihan beban akibat lalu lintas berbahaya, maka seluruh jaringan dapat lumpuh karena semua switch bergantung padanya untuk instruksi pengambilan keputusan.

Penelitian ini bertujuan untuk mengatasi kerentanan tersebut dengan mengembangkan sistem deteksi dan mitigasi serangan UDP Flood berbasis *machine learning* pada jaringan SDN menggunakan POX Controller. Algoritma *Support Vector Machine (SVM)* digunakan untuk mengklasifikasikan lalu lintas sebagai normal atau serangan berdasarkan fitur-fitur seperti *packet rate* dan *destination port*. Setelah serangan terdeteksi, teknik mitigasi *traffic shaping* diterapkan secara otomatis untuk membatasi lalu lintas dari sumber serangan tanpa mengganggu trafik normal.

Simulasi dilakukan menggunakan emulator Mininet dengan topologi *tree* yang terdiri dari lima switch dan 20 host, sedangkan serangan diujikan dengan *hping3* pada lingkungan Ubuntu virtual. Hasil pengujian menunjukkan bahwa sistem deteksi berbasis SVM mampu mencapai akurasi di atas 95%, dan mitigasi traffic shaping mampu memulihkan jaringan dalam waktu rata-rata 40–52 detik setelah serangan berlangsung. Penelitian ini menunjukkan bahwa integrasi deteksi adaptif berbasis SVM dan mitigasi otomatis melalui traffic shaping pada *POX Controller* mampu menjaga stabilitas jaringan SDN secara efektif, serta memberikan waktu pemulihan yang responsif dalam menghadapi serangan *UDP Flood*.

Kata kunci — *Software Defined Network, UDP Flood, POX Controller, Support Vector Machine, Traffic sha*ping*, Mitigasi DDoS, Quality of Service (QoS).*