

BAB V

PENUTUP

5.1. Kesimpulan

Berdasarkan hasil eksperimen yang telah dibahas sebelumnya, berikut ini adalah kesimpulan yang telah didapat sebagai berikut:

1. Dalam penelitian ini, model *Multilayer Perceptron* (MLP) telah berhasil dilatih dan dikembangkan untuk deteksi dan klasifikasi serangan DDoS pada jaringan SDN. Model MLP dengan akurasi sebesar 71.17% menunjukkan efisiensi dan kecepatan tinggi dalam mendeteksi serangan DDoS sehingga menunjukkan potensi besar dalam meningkatkan keamanan jaringan melalui metode *deep learning*.
2. Proses pengembangan model MLP melibatkan pemilihan dan persiapan dataset yang relevan dan representatif untuk serangan DDoS. Dataset diambil dari hasil pengumpulan data menggunakan tabel sFlow dengan *hping3*, menghasilkan 2 juta paket data yang terdiri dari lalu lintas normal dan lalu lintas DDoS. Data tersebut kemudian diratakan agar seimbang untuk menghindari bias. Hasilnya, model yang dibentuk menggunakan algoritma *RandomSearchCV* menunjukkan akurasi 71.17% dalam mengklasifikasikan serangan DDoS, memastikan efektivitas model dalam mendeteksi dan mengklasifikasikan serangan.
3. Persiapan *environment* yang tepat untuk pelatihan dan pengujian model sangat penting. Dalam penelitian ini, *environment* telah disiapkan dengan hati-hati menggunakan Ubuntu 22.04 sebagai sistem operasi, Mininet sebagai emulator jaringan, Ryu *controller* untuk pengendalian jaringan, dan Python sebagai bahasa pemrograman. Hasilnya, proses pelatihan dan pengujian dapat berjalan dengan lancar dan efisien, mendukung pengembangan dan evaluasi model MLP dengan optimal.
4. Hasil mitigasi serangan DDoS menunjukkan perbaikan signifikan dalam analisis jaringan. Berdasarkan pengukuran *jitter*, *delay*, *throughput*, *packet loss*, dan *resource utilization*, tindakan mitigasi terbukti efektif. Meskipun *packet loss* belum sepenuhnya pulih dan masih berada dalam kategori "buruk" menurut standar TIPHON, mitigasi berhasil mengurangi dampak serangan DDoS secara

keseluruhan dan memulihkan performa jaringan ke kategori "bagus" hingga "sangat bagus" pada metrik lainnya. Ini menandakan bahwa langkah-langkah mitigasi yang diterapkan berhasil meningkatkan kualitas layanan jaringan sesuai dengan standar yang diterima.

5.2. Saran

Berdasarkan temuan-temuan ini, peneliti merekomendasikan adanya upaya lanjutan dalam pengembangan model deteksi serangan DDoS.

1. Dalam penelitian mendatang, dapat dilakukan penelitian lebih lanjut terhadap teknik *deep learning* lainnya, seperti *Convolutional Neural Network* (CNN) atau *Recurrent Neural Network* (RNN), untuk membandingkan kinerja dan efektivitasnya dalam penanganan paket DDoS.
2. Mengumpulkan dataset yang lebih besar dan lebih beragam untuk melatih model. Dataset yang mencakup berbagai jenis serangan DDoS dan pola lalu lintas jaringan dapat meningkatkan kemampuan model dalam mendeteksi dan mengklasifikasikan serangan dengan lebih akurat.
3. Melakukan pengujian dan evaluasi model pada lingkungan jaringan nyata untuk menilai kinerja dan efektivitas model dalam kondisi dunia nyata. Hal ini penting untuk memastikan bahwa model dapat diandalkan dalam situasi sebenarnya.