

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan tentang penggunaan algoritma *Decision Tree* dalam menganalisis log sistem router Mikrotik untuk mengklasifikasikan serangan DDoS, dapat ditarik beberapa kesimpulan sebagai berikut:

1. Model klasifikasi berhasil mencapai akurasi sebesar 98%, yang menunjukkan bahwa 98% dari total klasifikasi (baik serangan DDoS maupun lalu lintas normal) dilakukan dengan benar oleh algoritma *Decision Tree*.
2. Dengan presisi sebesar 98% (minim false positive), recall 98% (mampu mendeteksi sebagian besar serangan yang terjadi), dan F1-Score 98% yang mencerminkan keseimbangan antara akurasi dan sensitivitas.
3. Hasil klasifikasi menunjukkan bahwa 98% dari prediksi serangan DDoS memang benar-benar serangan, sehingga administrator dapat mempercayai hasil deteksi tanpa khawatir terhadap banyaknya false alarm.
4. Administrator dapat menggunakan hasil klasifikasi sebagai dasar pengambilan keputusan, dalam melakukan *blocking* IP sumber serangan atau membatasi trafik tertentu yang terindikasi serangan.

5.2 Saran

Berdasarkan hasil penelitian dan evaluasi yang telah dilakukan, penulis memberikan beberapa saran berikut agar penelitian ini dapat dikembangkan lebih lanjut, khususnya di lingkungan pendidikan:

1. Implementasi sistem deteksi secara real-time perlu dikembangkan, agar model klasifikasi yang telah dibangun dapat langsung digunakan untuk mendeteksi serangan DDoS secara otomatis.
2. Penambahan atribut fitur dari log sistem perangkat jaringan lainnya, seperti log dari perangkat access point, firewall eksternal, dan statistik bandwidth, untuk memperkaya informasi yang dianalisis.
3. Peningkatan literasi dan pelatihan bagi administrator jaringan sekolah tentang penggunaan machine learning untuk keamanan jaringan perlu dilakukan.