BAB V PENUTUP

5.1 Kesimpulan

Dari hasil penelitian ini, dapat ditarik beberapa kesimpulan sebagai berikut:

1. Optimalisasi Algoritma Decision Tree dengan Seleksi Fitur Penelitian ini berhasil mengimplementasikan dan mengoptimalkan algoritma Decision Tree melalui teknik seleksi fitur pada dataset CIC-DDoS2019. Proses pra-pemrosesan data, yang meliputi pembersihan, normalisasi, dan seleksi fitur, terbukti meningkatkan kualitas data dan memberikan kontribusi signifikan terhadap peningkatan akurasi model dalam mendeteksi serangan DDoS.

2. Deteksi Serangan DDoS secara Efektif Dengan penerapan metode machine learning, sistem yang dikembangkan mampu membedakan antara aktivitas jaringan normal dan aktivitas mencurigakan dengan tingkat false positive yang rendah. Evaluasi performa menunjukkan bahwa penggunaan algoritma Decision Tree yang dioptimalkan memberikan hasil yang memuaskan dari segi akurasi, presisi, dan recall dalam mendeteksi pola serangan DDoS.

3. Integrasi sistem notifikasi real-time menggunakan bot Telegram memberikan nilai tambah pada penelitian ini. Mekanisme notifikasi ini memungkinkan tim keamanan untuk segera mendapatkan informasi terkait deteksi serangan, sehingga respons terhadap ancaman dapat dilakukan dengan cepat dan tepat.

4. Penelitian ini tidak hanya meningkatkan efisiensi deteksi serangan DDoS, namun juga memberikan kontribusi dalam pengembangan sistem deteksi intrusi berbasis machine learning sebagai solusi untuk memperkuat pertahanan jaringan di lingkungan yang rentan terhadap serangan siber.

5.2 Saran

Berdasarkan temuan dan analisis yang diperoleh dalam penelitian ini, saran-saran untuk pengembangan selanjutnya adalah sebagai berikut:

1. Disarankan agar penelitian selanjutnya melakukan perbandingan performa antara algoritma Decision Tree dengan algoritma machine learning lain seperti Random Forest, Support Vector Machine (SVM), atau bahkan algoritma deep learning. Hal ini dapat memberikan gambaran lebih

komprehensif mengenai metode yang paling optimal untuk deteksi serangan DDoS.

2. Mengingat penelitian ini dibatasi oleh penggunaan satu dataset (CIC-DDoS2019), disarankan untuk menguji sistem dengan dataset lain yang bersifat lebih heterogen. Hal ini penting untuk menguji kemampuan generalisasi model dalam menghadapi variasi serangan yang lebih luas di lingkungan dunia nyata.

3. Untuk meningkatkan respons dan fleksibilitas sistem deteksi, pengintegrasian notifikasi tidak hanya terbatas pada bot Telegram, tetapi juga dapat dikembangkan untuk mendukung platform notifikasi lain (seperti email, SMS, atau aplikasi mobile) agar dapat menjangkau lebih banyak pengguna dan mempercepat penanganan insiden.