BAB V
SIMPULAN, IMPLIKASI, DAN REKOMENDASI

5.1 Simpulan

Berdasarkan penelitian yang telah dilakukan dengan judul **"Perancangan Model Deteksi DDoS Menggunakan Algoritma Random Forest Dengan Pemberitahuan Cepat Melalui Telegram"**, dapat ditarik beberapa simpulan sebagai berikut:

1. Berhasil merancang model *Random Forest*
2. Performa Model Deteksi DDoS berbasis Random Forest menunjukkan performa kuat dengan akurasi, presisi, recall, dan F1-score masing-masing 93%. Hasil ini menunjukkan kemampuan model dalam mengidentifikasi ancaman DDoS
3. Dapat di integrasi dengan *Telegram* menggunakan bahasa pemograman *python*
4. Dari hasil pengujian pada tiga jenis jaringan yang berbeda (*Wifi*, 4G, dan *Ethernet* LAN), total rata-rata waktu deteksi keseluruhan adalah 0,0174 detik.

5.2 Implikasi

Dalam penelitian ini, perancangan model deteksi DDoS menggunakan algoritma *Random Forest* dengan pemberitahuan cepat melalui *Telegram* memiliki beberapa implikasi penting yang dapat mempengaruhi berbagai aspek keamanan *cyber*, operasional jaringan, dan respons terhadap insiden. Berikut adalah beberapa implikasi yang diidentifikasi:

1. Peningkatan Keamanan Jaringan

Model deteksi DDoS yang dirancang dalam penelitian ini mampu secara efektif mengidentifikasi serangan DDoS, bahkan dalam skenario lalu lintas tinggi dan kompleks. Dengan demikian, penerapan model ini dapat secara signifikan meningkatkan kemampuan deteksi dini terhadap serangan DDoS, yang pada akhirnya membantu dalam melindungi infrastruktur jaringan dari potensi kerusakan atau gangguan operasional.

2. Respon Cepat terhadap Insiden Keamanan

Implementasi pemberitahuan cepat melalui *Telegram* memungkinkan tim keamanan untuk menerima peringatan secara *real-time* saat serangan DDoS terdeteksi. Hal ini memungkinkan respons yang lebih cepat dan efektif, mengurangi waktu deteksi dan reaksi terhadap insiden, serta membantu dalam mengurangi dampak dari serangan tersebut.

3. Efisiensi Operasional

Penggunaan sistem otomatisasi untuk deteksi dan pemberitahuan serangan dapat mengurangi beban kerja manual tim keamanan. Dengan adanya sistem ini, tim dapat lebih fokus pada analisis dan mitigasi serangan yang lebih kompleks, serta meningkatkan efisiensi dalam penanganan insiden keamanan.

4. Keandalan dan Skalabilitas Deteksi

Algoritma *Random Forest*, yang digunakan dalam model ini, terbukti mampu menangani volume data yang besar dan beragam jenis serangan. Ini menunjukkan bahwa sistem dapat diandalkan dalam berbagai skenario serangan dan dapat diskalakan untuk menangani jaringan dengan berbagai ukuran dan kompleksitas.

5.3 Rekomendasi

Berdasarkan temuan dan simpulan penelitian ini, beberapa rekomendasi untuk pengembangan lebih lanjut adalah sebagai berikut:

1. Peningkatan Dataset dan Pelatihan Model

Untuk meningkatkan akurasi dan kemampuan deteksi model, disarankan untuk memperluas dataset dengan menambahkan lebih banyak contoh serangan DDoS yang berbeda, serta mempertimbangkan berbagai jenis lalu lintas jaringan. Hal ini akan membuat model lebih robust dan mampu mendeteksi berbagai variasi serangan yang mungkin terjadi.

2. Penambahan Fitur Pendeteksian Lainnya

Penggunaan algoritma lain atau *ensemble learning* bisa diimplementasikan untuk membandingkan performa dengan *Random F*orest. Kombinasi beberapa model dapat membantu meningkatkan akurasi dan reliabilitas sistem deteksi.

3. Pengembangan Sistem Pemberitahuan yang Lebih Canggih

Selain pemberitahuan melalui *Telegram*, disarankan untuk mengembangkan sistem pemberitahuan yang lebih canggih, seperti dashboard *monitoring* berbasis

web atau integrasi dengan sistem manajemen insiden. Ini akan memberikan lebih banyak opsi bagi administrator dalam mengelola dan merespons insiden keamanan.

4. Pengujian di Lingkungan Produksi

Untuk memastikan kesiapan dan keandalan sistem deteksi ini, disarankan untuk melakukan uji coba di lingkungan produksi nyata. Pengujian ini akan membantu dalam mengidentifikasi kelemahan sistem dan melakukan penyesuaian yang diperlukan sebelum implementasi penuh.