BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian dan percobaan yang telah dilakukan dalam pengembangan sistem deteksi serangan DDoS, beberapa kesimpulan utama dapat diambil:

1. Model deteksi yang dibangun mampu mengenali serangan DDoS dengan tingkat akurasi yang sangat baik. Penggunaan dataset terbaru serta pemilihan fitur yang tepat memainkan peran penting dalam peningkatan performa model.
2. Pemilihan delapan fitur terbaik berdasarkan algoritma Random Forest Importance memberikan dampak signifikan terhadap peningkatan kinerja model. Fitur-fitur ini memungkinkan model untuk lebih fokus pada karakteristik yang paling relevan dalam mendeteksi serangan DDoS, sehingga meningkatkan akurasi dan kecepatan prediksi.
3. Naive Bayes, KNN, dan Random Forest masing-masing memiliki kelebihan dan kekurangan terkait waktu komputasi dan kompleksitas. Naive Bayes unggul dalam kecepatan komputasi tetapi memiliki akurasi yang lebih rendah. KNN menunjukkan performa baik pada data non-linear, namun memerlukan waktu komputasi yang lebih lama. Random Forest memberikan akurasi tertinggi, tetapi dengan biaya waktu komputasi yang lebih besar. Oleh karena itu, pemilihan algoritma harus disesuaikan dengan kebutuhan spesifik dan sumber daya yang tersedia.

5.2 Saran

Berdasarkan hasil penelitian dan kesimpulan yang telah diperoleh, berikut adalah beberapa saran yang dapat dijadikan pertimbangan untuk penelitian selanjutnya:

1. Untuk meningkatkan kemampuan generalisasi model, disarankan untuk menggunakan dataset yang lebih beragam dan mencakup berbagai variasi serangan DDoS. Ini akan membantu model mengenali pola serangan yang lebih kompleks.
2. Sebaiknya penamaan fitur diseragamkan untuk memastikan konsistensi dan kemudahan dalam pengelolaan data. Konsistensi dalam penamaan fitur akan memudahkan proses analisis, pemahaman, dan kolaborasi di antara anggota tim. Selain itu, penyeragaman penamaan fitur juga dapat mengurangi risiko kesalahan dan meningkatkan efisiensi dalam pengembangan model
3. Dalam implementasi nyata, penting untuk mempertimbangkan skalabilitas sistem deteksi. Penggunaan teknologi yang dapat menangani volume data yang besar dan pemrosesan paralel dapat membantu dalam menangani serangan dalam skala yang lebih besar.machine learning.