BAB V

PENUTUP

5.1 KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan mengenai perbandingan visualisasi data deteksi serangan DDoS menggunakan algoritma Gaussian Naive Bayes dan K-Nearest Neighbor (K-NEAREST NEIGHBOR), dapat disimpulkan beberapa hal sebagai berikut:

1. Performa Algoritma Dalam Deteksi Serangan Ddos Hasil Analisis menunjukkan bahwa algoritma K-Nearest Neighbor (K-NEAREST NEIGHBOR) memiliki tingkat akurasi yang lebih tinggi dibandingkan dengan Gaussian Naive Bayes (GNB). K-NEAREST NEIGHBOR mencapai akurasi 63.75% pada data training dan 55% pada data testing, sementara GNB hanya mencapai 61.25% pada data training dan 40% pada data testing. Hasil ini menunjukkan bahwa K-NEAREST NEIGHBOR lebih efektif dalam melakukan klasifikasi dan mendeteksi serangan DDoS berdasarkan pola yang ada dalam dataset.
2. Efektivitas Visualisasi Data Dalam Penelitian ini, teknik visualisasi data seperti heatmap, pie chart, dan confusion matrix sangat membantu dalam memahami distribusi serangan DDoS serta pola klasifikasi yang dihasilkan oleh masing-masing algoritma. Visualisasi ini memberikan gambaran yang lebih jelas mengenai hubungan antar variabel dalam dataset serta efektivitas algoritma dalam mendeteksi serangan.

5.2 SARAN

Adapun beberapa saran yang dapat diberikan untuk penelitian selanjutnya guna meningkatkan efektivitas deteksi serangan DDoS:

1. Penggunaan Algoritma Lain penelitian ini hanya menggunakan algoritma Gaussian Naïve Bayes (GNB) dan K-Nearest Neighbors (K-NEAREST NEIGHBOR). Oleh karena itu, disarankan untuk mencoba algoritma lain seperti Random Forest, Support Vector Machine (SVM), atau Deep Learning agar diperoleh hasil yang lebih optimal dalam klasifikasi dan deteksi serangan DDoS.
2. Optimasi Parameter dan Teknik Feature Engineering penelitian ini belum melakukan optimasi parameter pada algoritma yang digunakan. Untuk meningkatkan akurasi, penelitian selanjutnya dapat menerapkan teknik hyperparameter tuning seperti Grid Search atau Random Search. Selain itu, penerapan teknik feature selection juga disarankan untuk mengidentifikasi fitur-fitur yang paling berpengaruh dalam mendeteksi serangan, sehingga model yang digunakan dapat bekerja lebih efisien dan akurat