BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan seluruh rangkaian penelitian yang telah dilakukan mulai dari penggabungan dataset, preprocessing, normalisasi, pelatihan model, hingga evaluasi performa algoritma *Random Forest* dan *Support Vector Machine (SVM)*, diperoleh beberapa kesimpulan utama sebagai berikut:

1. **Proses deteksi serangan *DoS/DDoS* pada dataset CICIDS2017 dapat dilakukan secara efektif setelah melalui tahapan preprocessing dan normalisasi data.** Tahapan ini berperan penting dalam mempersiapkan data agar lebih representatif, terutama melalui penghapusan nilai kosong, penggabungan label serangan menjadi kategori *Attack*, serta normalisasi fitur numerik menggunakan *StandardScaler*. Seluruh tahap tersebut terbukti meningkatkan kualitas data sehingga model dapat mempelajari pola trafik jaringan dengan lebih akurat.
2. **Algoritma *Random Forest* menunjukkan performa paling optimal dibandingkan *SVM* dalam mendeteksi serangan *DoS/DDoS*.** *Random Forest* mampu mencapai akurasi **99.96%**, serta memperoleh nilai *precision*, *recall*, dan *F1-score* sempurna (1.00) pada seluruh kelas. Hasil ini menunjukkan bahwa *RF* mampu mengidentifikasi seluruh serangan tanpa kesalahan, sekaligus mempertahankan tingkat *false positive* dan *false negative* yang sangat rendah. Performa tinggi ini dipengaruhi oleh sifat model *ensemble* yang stabil untuk dataset besar dan *imbalanced*.
3. **Algoritma *SVM* memiliki performa yang baik namun tidak mampu menyaingi *Random Forest*.** *SVM* menghasilkan akurasi **95.4%** dengan *precision* tinggi, namun nilai *recall* yang rendah pada kelas Attack (0.83) menunjukkan bahwa sebagian serangan tidak terdeteksi. Hal ini disebabkan oleh sifat *SVM* yang sensitif terhadap dataset tidak seimbang dan penggunaan subset data 30.000 record sehingga variasi pola serangan tidak sepenuhnya terwakili.

Secara keseluruhan, ***Random Forest* merupakan algoritma yang paling direkomendasikan untuk implementasi deteksi serangan *DoS/DDoS* pada dataset CICIDS2017**, karena lebih stabil, akurat, dan memiliki kemampuan generalisasi yang lebih baik.

5.2 Saran

Berdasarkan hasil penelitian dan keterbatasan yang ditemui selama proses pengerjaan, beberapa saran yang dapat diberikan adalah sebagai berikut:

1. Pengembangan penelitian dengan algoritma tambahan.

   Untuk penelitian selanjutnya, disarankan menambahkan algoritma lain seperti *XGBoost, LightGBM*, atau *Deep Learning (CNN/LSTM)* untuk membandingkan performa model pada kondisi dan arsitektur yang berbeda. Hal ini dapat memberikan gambaran lebih komprehensif terhadap efektivitas setiap pendekatan.

2. Mengatasi ketidakseimbangan data menggunakan Teknik *Oversampling* atau *Undersampling* .

   Teknik seperti *SMOTE, ADASYN*, atau *Random Undersampling* dapat membantu meningkatkan performa algoritma yang sensitif terhadap distribusi kelas, seperti *SVM*. Penanganan *imbalance* ini berpotensi meningkatkan nilai recall terutama pada kelas *Attack*.

3. Menggunakan jumlah data yang lebih besar untuk pelatihan *SVM*.

   Penggunaan subset 30.000 data untuk *SVM* menyebabkan variasi fitur serangan tidak sepenuhnya tercakup. Dengan memanfaatkan teknik reduksi dimensi seperti *PCA, SVM* dapat dilatih dengan dataset yang lebih besar tanpa mengorbankan waktu komputasi.

4. Implementasi *system IDS* secara real-time.

   Penelitian ini masih terbatas pada data statis (offline). Pengembangan selanjutnya dapat diarahkan pada implementasi sistem deteksi real-time menggunakan paket jaringan aktual, sehingga performa model dapat diuji pada kondisi sistem yang lebih nyata.

5. Optimasi parameter menggunakan Teknik *Hyperparameter Tuning*.

   Baik Random Forest maupun SVM dapat ditingkatkan performanya dengan melakukan pencarian parameter terbaik menggunakan GridSearchCV ataupun RandomSearchCV untuk menemukan konfigurasi yang paling optimal.

Dengan adanya saran-saran tersebut, diharapkan penelitian selanjutnya dapat mengembangkan sistem deteksi serangan yang lebih akurat, adaptif, dan sesuai untuk implementasi pada lingkungan jaringan modern.