BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil analisis dan pembahasan yang telah dilakukan dalam penelitian ini, dapat disimpulkan beberapa poin penting yang menjawab rumusan masalah dan mencapai tujuan penelitian sebagai berikut :

a. Berdasarkan hasil penelitian dan pengujian yang telah dilakukan, dapat disimpulkan bahwa algoritma Random Forest menunjukkan performa yang sangat baik dalam mengklasifikasikan berbagai jenis serangan jaringan pada dataset CIC-IDS2017. Model ini mampu mencapai tingkat akurasi sebesar 98,3%, serta menghasilkan nilai precision, recall, dan F1-score yang tinggi pada hampir seluruh kelas serangan, termasuk serangan seperti DDoS, DoS Hulk, Botnet, dan PortScan. Evaluasi menggunakan confusion matrix juga menunjukkan bahwa prediksi model terhadap kelas-kelas serangan sangat presisi, dengan tingkat kesalahan yang sangat rendah. Keberhasilan ini didukung oleh kekuatan algoritma Random Forest dalam menangani data berdimensi tinggi serta kemampuannya dalam melakukan generalisasi melalui pendekatan ensemble learning. Model ini terbukti efisien dalam mengenali pola lalu lintas jaringan dan mendeteksi intrusi secara otomatis, menjadikannya algoritma yang sangat cocok untuk diimplementasikan dalam sistem deteksi intrusi (IDS) berbasis machine learning.

b. Berdasarkan hasil pengujian yang dilakukan terhadap dataset CIC-IDS2017 menggunakan algoritma Random Forest, diperoleh hasil bahwa model mampu mengklasifikasikan jenis-jenis serangan jaringan seperti DoS, DDoS, Port Scan, Brute Force, dan Web Attack dengan tingkat akurasi yang sangat baik, yaitu sebesar 98,3%. Evaluasi menggunakan confusion matrix menunjukkan bahwa sebagian besar prediksi berada pada diagonal utama, menandakan bahwa Random Forest efektif dalam membedakan lalu lintas jaringan yang normal (BENIGN) dan yang

berbahaya (anomali). Hasil ini menunjukkan bahwa algoritma Random Forest sangat tepat diterapkan untuk klasifikasi multi-kelas dalam sistem deteksi intrusi jaringan (IDS).

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan dengan algoritma Random Forest untuk mendeteksi berbagai jenis serangan jaringan, terdapat beberapa hal yang dapat dijadikan bahan pengembangan lebih lanjut. Pertama, perlu dilakukan eksperimen lanjutan dengan algoritma lain seperti XGBoost atau metode deep learning untuk mengetahui perbandingan performa yang lebih komprehensif.

Selanjutnya, disarankan untuk menambahkan fitur baru atau melakukan rekayasa fitur lanjutan guna meningkatkan akurasi klasifikasi. Evaluasi model juga sebaiknya dilakukan dalam lingkungan real-time untuk melihat kemampuan model dalam menghadapi data yang terus mengalir. Selain itu, pada dataset yang tidak seimbang, penting untuk menerapkan teknik penyeimbangan data agar model tidak bias terhadap kelas tertentu. Terakhir, hasil dari penelitian ini dapat dikembangkan lebih lanjut untuk diterapkan sebagai bagian dari sistem deteksi intrusi (IDS) di lingkungan nyata sebagai bentuk sistem keamanan jaringan berbasis machine learning.