BAB V
PENUTUP

5.1 Kesimpulan

Implementasi sistem deteksi intrusi siber menggunakan algoritma Random Forest telah berhasil dilakukan melalui serangkaian tahap penelitian yang terstruktur. Berdasarkan hasil penelitian, implementasi, dan pengujian yang telah dipaparkan pada bab-bab sebelumnya, maka dapat ditarik beberapa kesimpulan utama sebagai berikut:

1. Hasil pengujian menunjukkan bahwa performa algoritma Ensemble Random Forest sangat efektif dalam mengklasifikasikan aktivitas jaringan ke dalam kategori normal dan intrusi dengan tingkat akurasi mencapai 89,68%. Model ini juga memiliki tingkat kepercayaan yang tinggi pada kelas intrusi dengan nilai Precision sebesar 1,00, yang membuktikan bahwa sistem mampu bekerja tanpa menghasilkan kesalahan deteksi pada trafik normal (Zero False Positives). Namun, hasil evaluasi juga menunjukkan nilai *Recall* sebesar 0,77, yang mengindikasikan adanya 197 data serangan yang belum teridentifikasi (*False Negative*). Hal ini menunjukkan bahwa meskipun model sangat akurat dalam pelabelan aktivitas normal, diperlukan pengembangan lebih lanjut untuk meningkatkan sensitivitas deteksi terhadap variasi serangan yang luput.
2. Identifikasi fitur-fitur berpengaruh mengungkap bahwa variabel failed_logins dan ip_reputation_score memiliki kontribusi yang paling signifikan dalam membentuk pola perilaku anomali pada dataset yang digunakan. Tingginya skor kepentingan pada fitur kegagalan login membuktikan secara ilmiah bahwa upaya masuk paksa (brute force) merupakan karakteristik serangan yang paling dominan. Temuan ini memberikan dasar bagi administrator jaringan untuk memprioritaskan pengawasan pada parameter-parameter kunci tersebut guna mempercepat proses identifikasi ancaman di masa depan.

5.2 Saran

Penelitian ini telah mencapai hasil yang memuaskan dalam lingkup deteksi intrusi berbasis data historis. Beberapa rekomendasi dapat dikembangkan untuk penelitian selanjutnya guna meningkatkan kualitas dan cakupan sistem deteksi sebagai berikut:

1. Peningkatan nilai Recall disarankan menjadi fokus utama melalui eksplorasi teknik penanganan data yang lebih kompleks atau penggunaan algoritma Boosting seperti XGBoost atau LightGBM. Upaya ini penting dilakukan untuk menekan jumlah serangan yang saat ini masih mungkin luput dari deteksi (False Negatives), sehingga sistem perlindungan menjadi semakin menyeluruh.
2. Pengujian model pada dataset yang lebih bervariasi dengan cakupan jenis serangan yang lebih luas sangat direkomendasikan untuk pengembangan ke depan. Penambahan variasi data seperti serangan DDoS atau SQL Injection akan sangat membantu dalam menguji tingkat generalisasi model di berbagai skenario ancaman siber yang terus berkembang di lingkungan nyata.
3. Eksperimen di masa mendatang dapat diarahkan pada pengembangan sistem deteksi yang bekerja secara real-time di lingkungan jaringan aktif. Langkah ini diperlukan untuk mengevaluasi performa kecepatan inferensi model dalam menangani lalu lintas data yang sesungguhnya serta memastikan efisiensi sumber daya sistem saat dijalankan pada infrastruktur jaringan yang kompleks.