BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil implementasi, pengujian, dan analisis yang telah dilakukan terhadap sistem deteksi intrusi menggunakan dataset NSL-KDD, dapat ditarik beberapa kesimpulan sebagai jawaban atas rumusan masalah penelitian:

1. Penerapan metode Hybrid Feature Selection yang menggabungkan Random Forest Importance (Filter) dan Recursive Feature Elimination with Cross-Validation (Wrapper) terbukti efektif dalam mereduksi dimensi data secara signifikan. Dari total 122 fitur hasil encoding One-Hot, sistem berhasil mengidentifikasi subset optimal sebanyak 23 fitur yang paling relevan (reduksi sebesar 81,1%). Reduksi ini mampu meringankan beban komputasi secara signifikan tanpa mengorbankan kinerja sistem.

2. Penggunaan algoritma Decision Tree Classifier berhasil menjawab tantangan black-box pada sistem keamanan berbasis AI. Model ini menghasilkan struktur pohon keputusan yang dapat diekstraksi menjadi aturan logika JIKA-MAKA (IF-THEN Rules) untuk 40 jenis serangan. Aturan ini memungkinkan administrator jaringan melacak alasan spesifik di balik setiap keputusan deteksi—misalnya melihat parameter Flag_S0 pada serangan DoS Neptune atau indikator Urgent Pointer pada serangan Rootkit—sehingga sistem menjadi transparan dan dapat dipercaya.

3. Sistem yang dibangun mencapai Accuracy sebesar 99,92% pada data uji KDDTest+ (22.544 rekaman) yang terpisah sepenuhnya dari proses pelatihan, membuktikan kemampuan generalisasi model yang baik. Analisis kesalahan menunjukkan 135 False Negative dan 139 False Positive (total 1,22% dari data uji), di mana dominasi kesalahan terjadi pada kategori R2L yang memiliki karakteristik mimicry attack—suatu tantangan klasik dalam sistem IDS berbasis fitur statistik. Tingkat kesalahan ini tergolong sangat rendah dan dapat diterima untuk implementasi sistem keamanan jaringan.

5.2 Saran

Penelitian ini masih memiliki ruang untuk pengembangan lebih lanjut. Penulis mengajukan beberapa saran sebagai berikut:

1. Pengujian pada Dataset Terbaru: Penelitian ini menggunakan dataset NSL-KDD yang merupakan standar benchmark klasik. Untuk penelitian selanjutnya, disarankan menguji model pada dataset yang lebih modern seperti CIC-IDS2017 atau UNSW-NB15 guna memastikan ketangguhan model dalam menghadapi pola serangan siber generasi terbaru.
2. Implementasi pada Lingkungan Real-Time: Sistem saat ini diuji menggunakan simulasi data statis (offline). Pengembangan selanjutnya dapat diarahkan pada implementasi real-time dengan menghubungkan model langsung ke antarmuka jaringan fisik atau menggunakan teknologi Software Defined Network (SDN.
3. Eksplorasi Algoritma Explainable Lainnya: Selain Decision Tree, penelitian mendatang dapat membandingkan algoritma lain yang mendukung interpretabilitas seperti RuleFit atau Logistic Regression, atau menerapkan teknik LIME dan SHAP pada model Deep Learning untuk mendapatkan keseimbangan yang lebih baik antara akurasi dan transparansi model.
4. Penanganan Class Imbalance: Untuk meningkatkan akurasi deteksi pada kategori R2L dan U2R yang memiliki sampel sangat sedikit, dapat diterapkan teknik oversampling seperti SMOTE (Synthetic Minority Oversampling Technique) pada tahap pra-pemrosesan data.