BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan informasi di era digital bukan lagi sekadar pelengkap, melainkan kebutuhan fundamental. Pertukaran data yang masif dalam jaringan komputer membuka celah bagi berbagai jenis serangan siber yang terus berevolusi. Dalam satu dekade terakhir, volume serangan siber mengalami peningkatan yang signifikan, mendorong kebutuhan akan mekanisme pertahanan yang lebih cerdas dan adaptif [1]. Sistem Deteksi Intrusi atau *Intrusion Detection System* (IDS) hadir sebagai mekanisme pertahanan otomatis untuk memantau lalu lintas jaringan secara terus-menerus.

Dalam implementasinya, terdapat dua kendala utama yang menghambat efektivitas IDS modern. Pertama, dataset keamanan jaringan standar seperti NSL-KDD memiliki dimensi yang tinggi, yaitu 41 fitur nominal yang setelah proses *encoding* menjadi 122 fitur. Penggunaan seluruh fitur ini tanpa seleksi seringkali tidak efisien karena mengandung informasi yang redundan atau tidak relevan (*noise*). Fenomena ini dikenal sebagai *Curse of Dimensionality* yang terbukti menurunkan performa model klasifikasi [2]. Hal ini tidak hanya memperlambat proses komputasi, tetapi juga berpotensi menurunkan akurasi deteksi karena model *overfitting* terhadap data latih.

Kedua, mayoritas model deteksi berbasis kecerdasan buatan (AI) seperti *Neural Network* atau *Random Forest* bekerja layaknya "kotak hitam" (*black-box*). Model-model ini mampu memberikan label "Serangan" atau "Normal" dengan akurasi tinggi, tetapi gagal menjelaskan alasan logis di balik keputusan tersebut. Ketidakmampuan ini menimbulkan *trust issue* bagi administrator jaringan yang membutuhkan bukti logis sebelum mengambil tindakan mitigasi seperti pemblokiran IP. Konsep *Explainable AI* (XAI) hadir sebagai solusi untuk menjawab permasalahan transparansi ini [3].

Berdasarkan kondisi tersebut, diperlukan pendekatan baru yang tidak hanya mengejar akurasi angka, tetapi juga efisiensi komputasi dan transparansi logika. Berbagai penelitian sebelumnya seperti Fatmawati & Windarto [4] dan Al-Yaseen et al. [5] telah membuktikan bahwa seleksi fitur mampu meningkatkan performa IDS secara signifikan. Namun, pendekatan yang menggabungkan seleksi fitur hibrid dengan interpretabilitas model secara bersamaan masih terbatas. Oleh karena itu, penelitian ini mengusulkan integrasi metode *Hybrid Feature Selection* untuk menangani dimensi data, serta pendekatan *Explainable AI* berbasis aturan (*Rule-Based*) menggunakan algoritma *Decision Tree* untuk menjawab kebutuhan transparansi keputusan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana penerapan metode Hybrid Feature Selection yang menggabungkan Random Forest (Filter) dan RFECV (Wrapper) dapat mereduksi dimensi fitur dataset NSL-KDD secara efisien tanpa menurunkan akurasi sistem deteksi intrusi?
2. Bagaimana membangun model deteksi intrusi berbasis Decision Tree yang tidak hanya akurat, tetapi juga mampu menghasilkan aturan logika (Rule Extraction) yang transparan sebagai implementasi Explainable AI (XAI)?
3. Seberapa efektif sistem yang dibangun dalam mendeteksi 40 jenis serangan pada dataset NSL-KDD berdasarkan metrik evaluasi Accuracy, Precision, Recall, dan F1-Score, serta bagaimana karakteristik kesalahan False Positive dan False Negative yang dihasilkan?

1.3 Batasan Masalah

Agar penelitian lebih terarah dan terukur, peneliti menetapkan batasan masalah sebagai berikut:

1. Dataset yang digunakan adalah NSL-KDD (KDDTrain+ dan KDDTest+).
2. Proses encoding One-Hot Encoding terhadap tiga fitur kategorikal (Protocol

Type, Service, Flag) menghasilkan total 122 fitur sebagai input seleksi.

3. Metode seleksi fitur yang digunakan adalah gabungan Random Forest Importance (Filter) dan RFECV (Wrapper), dengan target reduksi ke subset fitur optimal (hasil eksperimen menunjukkan 23 fitur).
4. Metode ekstraksi aturan (rule extraction) menggunakan algoritma Decision Tree.
5. Fokus penelitian adalah pada klasifikasi jenis serangan (multiclass classification) dan analisis logika deteksi, bukan pada implementasi perangkat keras firewall fisik.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah ditetapkan, tujuan penelitian ini adalah sebagai berikut:

1. Mengimplementasikan dan mengevaluasi efektivitas metode Hybrid Feature Selection (Random Forest + RFECV) dalam mereduksi 122 fitur hasil encoding menjadi subset fitur yang paling optimal untuk sistem deteksi intrusi berbasis dataset NSL-KDD.
2. Membangun mekanisme transparansi keputusan dengan mengekstraksi aturan logika (Rule Extraction) menggunakan algoritma Decision Tree, sehingga setiap deteksi serangan dapat dijelaskan secara logis kepada administrator jaringan dalam format aturan JIKA-MAKA (IF-THEN Rules).
3. Melakukan validasi komprehensif terhadap keandalan model yang dihasilkan melalui pengukuran metrik Accuracy, Precision, Recall, dan F1-Score, serta analisis mendalam terhadap tingkat kesalahan False Positive dan False Negative untuk memastikan efektivitas sistem.

1.5 Manfaat Penelitian

Dari hasil penelitian ini diharapkan mampu memberikan beberapa manfaat diantaranya sebagai berikut:

1. Manfaat Teoritis

Penelitian ini memberikan kontribusi ilmiah berupa kajian empiris mengenai efektivitas integrasi metode Hybrid Feature Selection (RF-RFECV) dan penerapan konsep Explainable AI dalam domain keamanan siber. Temuan penelitian diharapkan dapat memperkaya khazanah literatur tentang optimasi sistem deteksi intrusi dan menjadi referensi bagi peneliti selanjutnya yang mengembangkan model IDS yang efisien sekaligus interpretabel.

2. Manfaat Praktis

Hasil penelitian berupa aturan logika serangan (IF-THEN Rules) dapat dimanfaatkan secara langsung oleh administrator jaringan sebagai referensi untuk menyusun aturan firewall yang lebih presisi dan berbasis bukti. Selain itu, aturan tersebut dapat mempercepat proses forensik jaringan dengan memberikan alasan deteksi yang jelas, sehingga mengurangi waktu respons insiden keamanan.

1.6 Sistematika Penulisan

Sistematika penulisan skripsi ini disusun untuk memberikan gambaran umum mengenai urutan dan isi dari tiap bab yang dibahas:

BAB I PENDAHULUAN, berisi latar belakang permasalahan dimensi tinggi dan black-box AI, rumusan masalah, batasan, tujuan, manfaat, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA, memuat studi literatur dari penelitian terdahulu yang relevan serta dasar teori mengenai IDS, NSL-KDD, Random Forest, RFECV, Decision Tree, Confusion Matrix, One-Hot Encoding, dan metrik evaluasi.

BAB III METODE PENELITIAN, menjelaskan objek penelitian, alur penelitian, alat dan bahan, serta tahapan penyiapan data termasuk proses split data dan hyperparameter yang digunakan.

BAB IV HASIL DAN PEMBAHASAN, menyajikan hasil reduksi fitur, performa model pada data uji, analisis kesalahan (error analysis), dan pembahasan mengenai logika aturan serangan yang ditemukan.

BAB V PENUTUP, berisi kesimpulan dari seluruh rangkaian penelitian dan saran untuk pengembangan selanjutnya.