

**OPTIMASI DAN DETEKSI INTRUSI MENGGUNAKAN
HYBRID FEATURE SELECTION DAN DECISION TREE
RULE-BASED PADA DATA NSLKDD**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh

RIKI NUR INDRA PUTRA

22.83.0875

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2026**

**OPTIMASI DAN DETEKSI INTRUSI MENGGUNAKAN
HYBRID FEATURE SELECTION DAN DECISION TREE
RULE-BASED PADA DATA NSLKDD**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh

RIKI NUR INDRA PUTRA

22.83.0875

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2026

HALAMAN PERSETUJUAN

SKRIPSI

**OPTIMASI DAN DETEKSI INTRUSI MENGGUNAKAN HYBRID
FEATURE SELECTION DAN DECISION TREE RULE-BASED PADA
DATA NSLKDD**

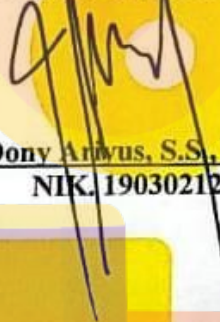
yang disusun dan diajukan oleh

RIKI NUR INDRA PUTRA

22.83.0875

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 28 Januari 2026

Dosen Pembimbing,



Dr. Dony Arivus, S.S., M. Kom.

NIK. 190302128

HALAMAN PENGESAHAN
SKRIPSI
OPTIMASI DAN DETEKSI INTRUSI MENGGUNAKAN HYBRID
FEATURE SELECTION DAN DECISION TREE RULE-BASED PADA
DATA NSLKDD

yang disusun dan diajukan oleh

Riki Nur Indra Putra

22.83.0875

Telah dipertahankan di depan Dewan Penguji
pada tanggal 25 Februari 2026

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Wahid Miftahul Ashari, S.Kom., M.T.
NIK. 190302452

Andika Agus Slameto, S.Kom., M.Kom
NIK. 190302109

Dr. Dony Ariyus, S.S., M. Kom.
NIK. 190302128



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 2 Maret 2026

DEKAN FAKULTAS ILMU KOMPUTER



Prof. Dr. Kusriani, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Riki Nur Indra Putra
NIM : 22.83.0875

Menyatakan bahwa Skripsi dengan judul berikut:

OPTIMASI DAN DETEKSI INTRUSI MENGGUNAKAN HYBRID FEATURE SELECTION DAN DECISION TREE RULE-BASED PADA DATA NSLKDD
Dosen Pembimbing : Dr. Doni Ariyus, S.S., M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 25 Februari 2026

Yang Menyatakan,



Riki Nur Indra Putra

HALAMAN PERSEMBAHAN

Puji dan syukur kepada Allah SWT, karena atas rahmat dan karunia-Nya, penulis berhasil menyelesaikan skripsi ini, dan dengan tulus penulis ingin mempersembahkannya kepada:

1. Prof. Dr. M. Suyanto., M.M selaku Rektor Universitas Amikom Yogyakarta.
2. Bapak Dr. Dony Ariyus, S.S., M.Kom sebagai dosen pembimbing yang telah memberikan bimbingan dan bantuan kepada penulis.
3. Bapak Dr. Dony Ariyus, S.S., M.Kom selaku kaprodi dan Bapak Jeki Kuswanto, M.Kom selaku sekprodi dari Program Studi Teknik Komputer, telah berperan penting dalam meningkatkan kualitas Prodi Teknik Komputer menjadi lebih baik.
4. Bapak Huri dan Ibu Isti Isvantini, selaku ayah dan ibu penulis yang telah memberikan dukungan dan doa kepada penulis dengan tulus.
5. Rahmat Fachrurrozzi selaku CEO Skillupkids.id bos tempat kerja yang telah memberikan bantuan saat mengerjakan skripsi ataupun bantuan saat menjalani kuliah.
6. Teman-teman markas PT. Anak Hebat Nusantara yang tidak bisa saya sebutkan semuanya yang telah memberikan bantuan selama masa perkuliahan.
7. Teman-teman Universitas Amikom Yogyakarta yang telah memberikan bantuan selama masa perkuliahan.
8. Neinsa Mervia selaku support sistem yang senantiasa menemani, memberikan dukungan dan motivasi selama proses penyusunan skripsi ini.

KATA PENGANTAR

Puji syukur kehadiran Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul **“Optimasi Dan Interpretasi Deteksi Intrusi Menggunakan Hybrid Feature Selection Dan Decision Tree Rule-Based Pada Data NSLKDD”** ini dengan baik. Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana pada Program Studi Teknik Komputer, Universitas Amikom Yogyakarta.

Penulisan skripsi ini tentu tidak lepas dari bantuan, dukungan, serta bimbingan dari berbagai pihak. Oleh karena itu, pada kesempatan ini, penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

1. Bapak Huri dan Ibu Isti Isvantini, selaku ayah dan ibu penulis yang telah memberikan dukungan dan doa kepada penulis dengan tulus.
2. Bapak Dr. Dony Ariyus, S.S., M.Kom sebagai dosen pembimbing yang telah memberikan bimbingan dan bantuan kepada penulis.
3. Bapak Anggit Ferdita Nugraha, S.T., M.Eng. selaku dosen yang telah memberikan wawasan serta dorongan dalam perjalanan akademik saya.
4. Teman-teman Prodi Teknik Komputer yang selalu memberikan semangat, bantuan, serta kebersamaan dalam menghadapi tantangan akademik.
5. Rahmat Fachrurrozzi selaku CEO Skillupkids.id bos tempat kerja yang telah memberikan bantuan saat mengerjakan skripsi ataupun bantuan saat menjalani kuliah.
6. Teman-teman markas PT. Anak Hebat Nusantara yang tidak bisa saya sebutkan semuanya yang telah memberikan bantuan selama masa perkuliahan.
7. Neinsa Mervia selaku support system yang senantiasa menemani, memberikan dukungan dan motivasi selama proses penyusunan skripsi ini.

Yogyakarta, 28 Januari 2025

Penulis

Riki Nur Indra Putra

DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....	iv
HALAMAN PERSEMBAHAN.....	v
KATA PENGANTAR.....	vi
DAFTAR ISI.....	vii
DAFTAR TABEL.....	x
DAFTAR GAMBAR.....	xi
DAFTAR ISTILAH	xii
INTISARI.....	xiii
ABSTRACT.....	xiv
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3
1.6 Sistematika Penulisan.....	4
BAB II TINJAUAN PUSTAKA.....	5
2.1 Studi Literatur	5
2.2 Dasar Teori.....	11
2.2.1 Sistem Deteksi Intrusi (Intrusion Detection System).....	11
2.2.2 Dataset NSL-KDD	11
2.2.3 One Hot Encoding.....	12

DAFTAR ISI

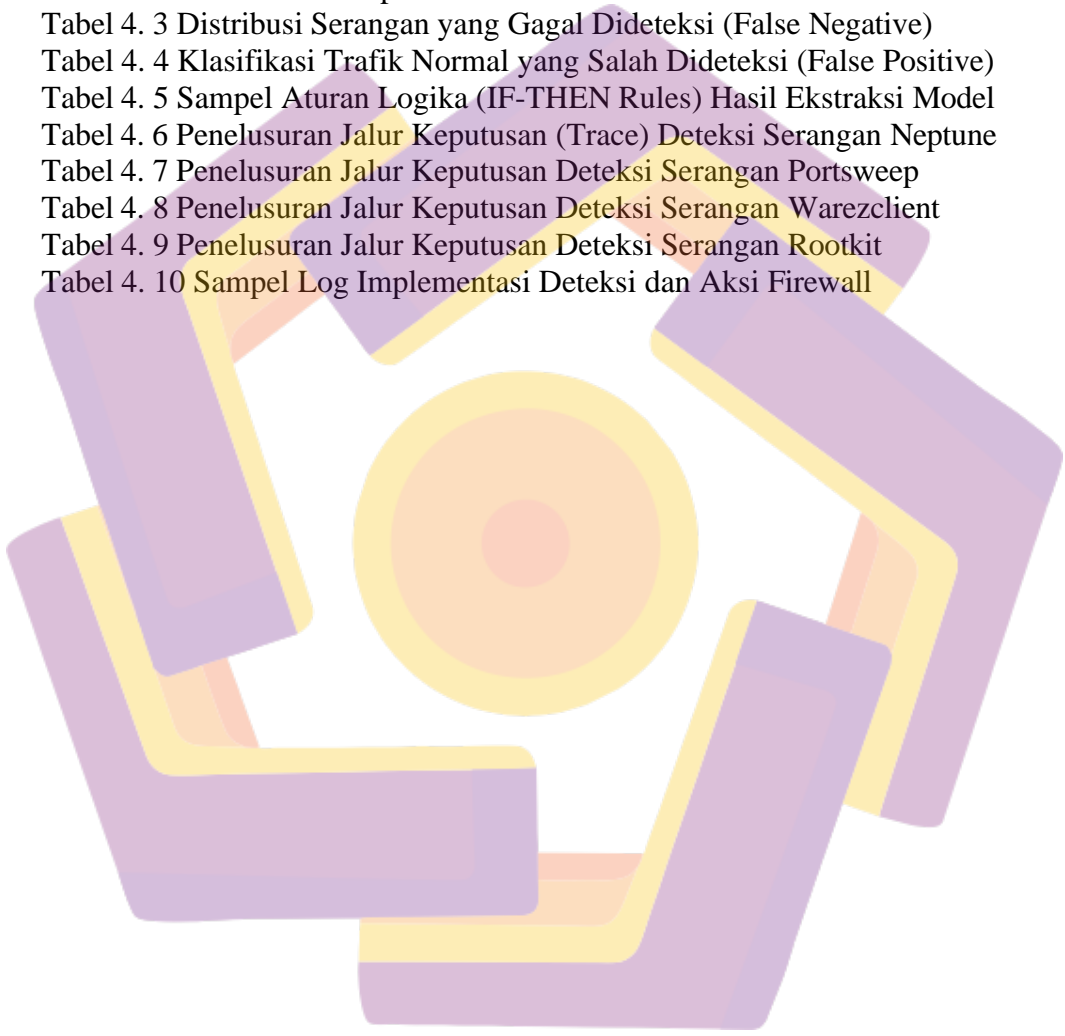
2.2.4	Konsep Seleksi Fitur Hybrid (Hybrid Feature Selection)	12
2.2.5	Algoritma Random Forest.....	13
2.2.6	Recursive Feature Elimination with Cross-Validation (RFECV)	14
2.2.7	Decision Tree dan Explainable AI (XAI).....	16
2.2.8	Confusion Matrix	17
2.2.9	Metrik Evaluasi Model.....	17
BAB III METODE PENELITIAN.....		20
3.1	Objek Penelitian	20
3.2	Alur Penelitian.....	21
3.3	Alat dan Bahan	24
3.3.1	Perangkat Keras (<i>Hardware</i>).....	25
3.3.2	Perangkat Lunak (<i>Software</i>).....	25
3.3.3	Bahan Penelitian.....	27
3.4	Tahap Penyiapan Data (Data Preparatian).....	27
3.4.1	Pembersihan Data (Data Cleaning)	27
3.4.2	Transformasi Data (Encoding)	27
3.4.3	Pembagian Data (Data Splitting).....	28
3.4.3	Hyperparameter Penelitian	28
BAB IV HASIL DAN PEMBAHASAN.....		30
4.1	Hasil Optimasi Fitur	30
4.2	Hasil Implementasi dan Validasi Akurasi	34
4.2.1	Skenario Pengujian.....	34
4.2.2	Analisis Confusion Matrix	34
4.2.3	Performa Akurasi Keseluruhan	35
4.3	Analisis Kesalahan (False Positive & False Negative)	36
4.4	Visualisasi Pohon Keputusan (<i>Decision Tree</i>).....	38

DAFTAR ISI

4.5	Interpretasi Aturan Serangan (Logika AI).....	38
4.5.1	Mekanisme Ekstraksi Aturan	39
4.5.2	Sampel Logika Deteksi Serangan	39
4.5.3	Analisis Pola Keputusan.....	40
4.5.4	Verifikasi Jalur Keputusan (<i>Decision Traceability</i>).....	41
4.6	Simulasi Log Deteksi dan Respon Sistem.....	43
4.6.1	Statistik Distribusi Tindakan.....	44
4.6.2	Komponen Log Sistem.....	45
4.6.3	Mekanisme Mitigasi Otomatis	45
4.6.4	Analisis Statistik Distribusi Tindakan.....	46
BAB V PENUTUP.....		47
5.1	Kesimpulan.....	47
5.2	Saran.....	48
REFERENSI		49

DAFTAR TABEL

Tabel 2. 1 Keaslian Penelitian	7
Tabel 2. 2 Metrik Evaluasi Model Klasifikasi	18
Tabel 3. 1 Perangkat Lunak dan Pustaka (library) yang Digunakan	26
Tabel 3. 2 Hyperparameter yang Digunakan	28
Tabel 4. 1 Distribusi Fitur Flag Status Koneksi pada NSL-KDD	31
Tabel 4. 2 Daftar Fitur Terpilih	33
Tabel 4. 3 Distribusi Serangan yang Gagal Dideteksi (False Negative)	36
Tabel 4. 4 Klasifikasi Trafik Normal yang Salah Dideteksi (False Positive)	37
Tabel 4. 5 Sampel Aturan Logika (IF-THEN Rules) Hasil Ekstraksi Model	39
Tabel 4. 6 Penelusuran Jalur Keputusan (Trace) Deteksi Serangan Neptune	41
Tabel 4. 7 Penelusuran Jalur Keputusan Deteksi Serangan Portsweep	42
Tabel 4. 8 Penelusuran Jalur Keputusan Deteksi Serangan Warezclient	42
Tabel 4. 9 Penelusuran Jalur Keputusan Deteksi Serangan Rootkit	43
Tabel 4. 10 Sampel Log Implementasi Deteksi dan Aksi Firewall	45



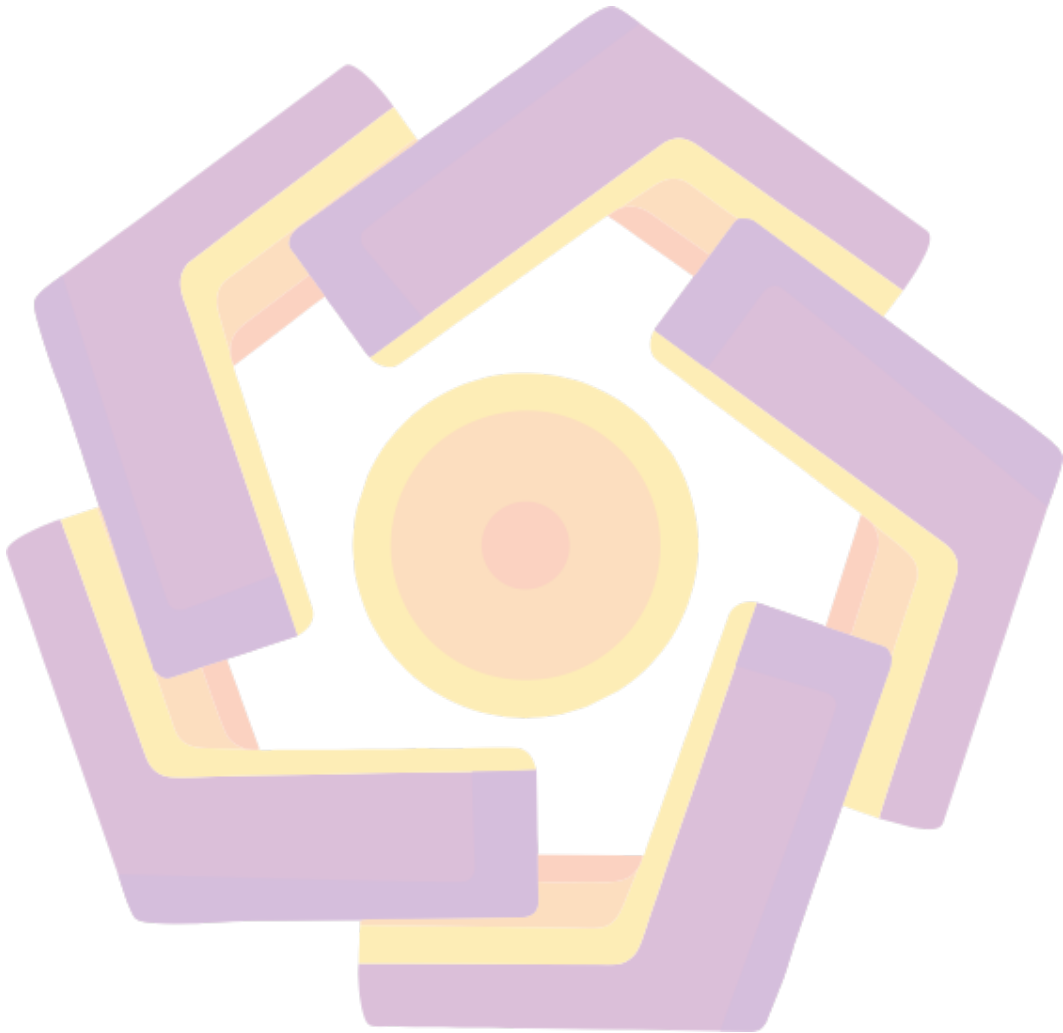
DAFTAR GAMBAR

Gambar 2. 1 Random Forest dan Majority Voting	13
Gambar 2. 2 Proses Seleksi Fitur RFECV	15
Gambar 2. 3 Struktur Decision Tree dan Mekanisme Ekstraksi Aturan Logika	16
Gambar 3. 1 Alur Penelitian	22
Gambar 4. 1 Grafik bobot kepentingan fitur berdasarkan Random Forest	31
Gambar 4. 2 Kurva Performa RFECV: Akurasi vs. Jumlah Fitur	32
Gambar 4. 3 Confusion Matrix hasil klasifikasi data implementasi.	34
Gambar 4. 4 Metrik Evaluasi (KDDTest+)	35
Gambar 4. 5 Visualisasi Root Node dan cabang utama Decision Tree	38
Gambar 4. 6 Persentase tindakan pemblokiran serangan vs koneksi normal	44



DAFTAR ISTILAH

Vektor	besaran yang mempunyai arah
Eigen Value	akar akar persamaan



INTISARI

Keamanan jaringan komputer menghadapi tantangan besar akibat meningkatnya volume lalu lintas data dan kecanggihan serangan siber. Penggunaan Intrusion Detection System (IDS) berbasis Machine Learning menjadi solusi vital, namun sering terkendala oleh dimensi data yang tinggi (seperti 41 fitur pada dataset NSL-KDD) yang membebani komputasi, serta sifat black-box dari model AI yang sulit divalidasi logikanya oleh manusia. Masalah ini menyebabkan ketidakefisienan sistem dan keraguan administrator terhadap keputusan blokir yang diambil oleh IDS. Penelitian ini bertujuan untuk mengoptimalkan kinerja IDS sekaligus memberikan transparansi keputusan. Metode yang digunakan adalah Hybrid Feature Selection yang menggabungkan kecepatan Random Forest (Filter) dan ketelitian Recursive Feature Elimination with Cross-Validation (Wrapper) untuk menyeleksi fitur terbaik. Selanjutnya, algoritma Decision Tree digunakan untuk mengekstraksi aturan logika (Rule Extraction) dari setiap serangan. Hasil penelitian menunjukkan bahwa sistem mampu mereduksi 41 fitur menjadi 23 fitur optimal dengan mempertahankan akurasi validasi sebesar 99,73%. Sistem juga berhasil menghasilkan "kamus aturan" yang transparan untuk 40 jenis serangan berbeda, sehingga dapat dimanfaatkan oleh praktisi keamanan jaringan untuk memvalidasi insiden keamanan secara cepat dan akurat.

Kata kunci: Intrusion Detection System, Hybrid Feature Selection, RFECV, Decision Tree, Explainable AI.

ABSTRACT

Computer network security faces significant challenges due to the increasing volume of data traffic and the sophistication of cyber attacks. The use of Machine Learning-based Intrusion Detection Systems (IDS) has become a vital solution but is often hindered by high data dimensionality (such as 41 features in the NSL-KDD dataset) which burdens computation, as well as the black-box nature of AI models whose logic is difficult for humans to validate. These problems lead to system inefficiency and administrator skepticism regarding blocking decisions made by IDS. This research aims to optimize IDS performance while providing decision transparency. The method used is Hybrid Feature Selection, combining the speed of Random Forest (Filter) and the precision of Recursive Feature Elimination with Cross-Validation (Wrapper) to select the best features. Furthermore, the Decision Tree algorithm is used to extract logic rules (Rule Extraction) from each attack. The research results show that the system is capable of reducing 41 features to 23 optimal features while maintaining a validation accuracy of 99.73%. The system also successfully generated a transparent "rule dictionary" for 40 different types of attacks, which can be utilized by network security practitioners to validate security incidents quickly and accurately.

Keywords: *Intrusion Detection System, Hybrid Feature Selection, RFECV, Decision Tree, Explainable AI.*