

KLASIFIKASI INTRUSI JARINGAN MENGGUNAKAN ALGORITMA *DEEP LEARNING*

Tugas Akhir

**Diajukan untuk Memenuhi Salah Satu Persyaratan Mencapai Derajat
Sarjana Komputer**



Dibuat Oleh:

VALENTINUS WILBERT SOEDJITO

210711340

**PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ATMA JAYA YOGYAKARTA
2025**

HALAMAN PENGESAHAN

Tugas Akhir Berjudul

KLASIFIKASI INTRUSI JARINGAN MENGGUNAKAN ALGORITMA DEEP LEARNING

yang disusun oleh

Valentinus Wilbert Soedjito

210711340

dinyatakan telah memenuhi syarat pada tanggal 28 Juli 2025

		Keterangan
Dosen Pembimbing 1	: Y. Sigit Purnomo WP., S.T.,M.Kom., Ph.D.	Telah Menyetujui
Dosen Pembimbing 2	: Wilfridus Bambang Triadi H, ST., M.Cs	Telah Menyetujui
Tim Penguji		
Penguji 1	: Y. Sigit Purnomo WP., S.T.,M.Kom., Ph.D.	Telah Menyetujui
Penguji 2	: Eddy Julianto, S.T.,M.T.	Telah Menyetujui
Penguji 3	: Prof. Ir. A. Djoko Budiyanto, M.Eng., Ph.D.	Telah Menyetujui

Yogyakarta, 28 Juli 2025

Universitas Atma Jaya Yogyakarta

Teknologi Industri

Dekan

ttd.

Dr. Ir. Parama Kartika Dewa SP., S.T., M.T.

Dokumen ini merupakan dokumen resmi UAJY yang tidak memerlukan tanda tangan karena dihasilkan secara elektronik oleh Sistem Bimbingan UAJY. UAJY bertanggung jawab penuh atas informasi yang tertera di dalam dokumen ini

PERNYATAAN ORISINALITAS & PUBLIKASI ILMIAH

Saya yang bertanda tangan di bawah ini:

Nama Lengkap : Valentinus Wilbert Soedjito
NPM : 210711340
Program Studi : Informatika
Fakultas : Teknologi Industri
Judul Penelitian : Klasifikasi Intrusi Jaringan Menggunakan
Algoritma Deep Learning

Menyatakan dengan ini:

1. Tugas Akhir ini adalah benar tidak merupakan salinan sebagian atau keseluruhan dari karya penelitian lain.
2. Memberikan kepada Universitas Atma Jaya Yogyakarta atas penelitian ini, berupa Hak untuk menyimpan, mengelola, mendistribusikan, dan menampilkan hasil penelitian selama tetap mencantumkan nama penulis.
3. Bersedia menanggung secara pribadi segala bentuk tuntutan hukum atas pelanggaran Hak Cipta dalam pembuatan Tugas Akhir ini.

Demikianlah pernyataan ini dibuat dan dapat dipergunakan sebagaimana mestinya.

Yogyakarta, Juli 2025

Yang menyatakan,

Valentinus Wilbert Soedjito

210711340

HALAMAN PERSEMBAHAN

Terima kasih buat diriku, yang sudah berjuang. Bahkan sampai detik ini, kamu masih belum menyerah.

KATA PENGANTAR

Puji dan syukur penulis haturkan kepada Tuhan Yang Maha Esa karena berkat rahmat dan karunia-Nya, penulis dapat menyelesaikan pembuatan tugas akhir yang berjudul “Deteksi Intrusi Jaringan menggunakan Algoritma *Deep Learning* pada Sistem Keamanan Jaringan” ini dengan baik. Penulisan tugas akhir ini bertujuan untuk memenuhi salah satu syarat dalam mencapai sarjana komputer dari Program Studi Informatika, Fakultas Teknologi Industri di Universitas Atma Jaya Yogyakarta.

Penulis menyadari bahwa dalam pembuatan tugas akhir ini penulis telah mendapatkan bantuan, bimbingan, dan dorongan dari banyak pihak. Untuk itu, pada kesempatan ini penulis ingin mengucapkan terima kasih kepada:

1. Tuhan Yesus Kristus selalu membimbing dalam iman-Nya, memberikan berkat-Nya, dan menyertai penulis selalu.
2. Bapak Dr. Ir. Parama Kartika Dewa SP., S.T., M.T. IPU selaku Dekan Fakultas Teknologi Industri, Universitas Atma Jaya Yogyakarta.
3. Bapak Y. Sigit Purnomo WP., S.T., M.Kom. selaku dosen pembimbing I dan Bapak Wilfridus Bambang Triadi H., S.T., M.Cs. selaku dosen pembimbing II yang telah membimbing dan memberikan masukan serta motivasi kepada penulis untuk menyelesaikan tugas akhir ini.
4. Keluarga dan teman-teman penulis yang memberikan semangat dan motivasi kepada penulis untuk menyelesaikan tugas akhir ini.
5. Semua pihak yang tidak bisa disebutkan satu per satu yang sudah membantu penulis menyelesaikan tugas akhir ini.

Demikian laporan tugas akhir ini dibuat, dan penulis mengucapkan terima kasih kepada semua pihak. Semoga laporan ini dapat bermanfaat bagi pembaca.

Yogyakarta, Juli 2025

Penulis

DAFTAR ISI

PERNYATAAN ORISINALITAS & PUBLIKASI ILMIAH	ii
HALAMAN PERSEMBAHAN	iii
KATA PENGANTAR.....	iv
DAFTAR ISI	v
DAFTAR GAMBAR	vii
DAFTAR TABEL.....	ix
INSTISARI	x
BAB I. PENDAHULUAN	1
A. Latar Belakang	1
B. Rumusan Masalah	3
C. Batasan Penelitian	3
D. Tujuan Penelitian.....	3
E. Metode Penelitian.....	4
1. Pendekatan Penelitian	4
2. Tahapan Penelitian	4
3. Alat.....	9
F. Sistematika Penulisan	10
BAB II. TINJAUAN PUSTAKA	13
BAB III. LANDASAN TEORI.....	22
A. Serangan Siber	22
B. <i>Intrusion Detection System (IDS)</i>	25
C. <i>Deep Learning</i>	26
BAB IV. PENGUMPULAN DATASET	29
A. Deskripsi <i>Problem</i>	29
B. Pengumpulan Rekaman Lalu Lintas Jaringan.....	30
C. Pembersihan Data dan Normalisasi	43
D. Ekstraksi File Rekaman Lalu Lintas Jaringan.....	43
F. Karakteristik Dataset.....	53

BAB V. PENGEMBANGAN MODEL	55
A. <i>Data Loading</i>	60
B. <i>Data Preparation</i>	62
C. <i>Model Configuration</i>	64
D. <i>Model Tranning and Validation</i>	67
E. <i>Model Evaluation</i>	74
BAB VI. IMPLEMENTASI MODEL.....	87
A. Pengaplikasian Model	87
B. Implementasi Sistem	88
C. Pengujian Sistem.....	90
BAB VII. PENUTUP	95
A. Kesimpulan	95
B. Saran.....	95
DAFTAR PUSTAKA	97

DAFTAR GAMBAR

Gambar 3.1. Alur Sistem Deteksi Intrusi	26
Gambar 4.1. Diagram Alur Pengumpulan Dataset.....	31
Gambar 4.2. Contoh File PCAP Rekaman Lalu Lintas Jaringan Serangan DoS Menggunakan Wireshark	33
Gambar 4.3. Contoh File PCAP Rekaman Lalu Lintas Jaringan Serangan Brute Force Menggunakan Wireshark	34
Gambar 4.4. Contoh File PCAP Rekaman Lalu Lintas Jaringan Serangan Pemindaian Nmap Menggunakan Wireshark.....	36
Gambar 4.5. Contoh File PCAP Rekaman Lalu Lintas Jaringan Serangan Spoofing Menggunakan Wireshark	38
Gambar 4.6. Contoh File .csv Mentah	44
Gambar 4.7. Antarmuka Aplikasi CICFlowMeter	46
Gambar 4.8. Hasil dari Konversi menggunakan CICFlowMeter.....	47
Gambar 4.9. Contoh File CSV yang Sudah Diekstraksi Menggunakan CICFlowMeter	47
Gambar 4.10. Script untuk Pelabelan Data	48
Gambar 4.11. Script untuk Menggabungkan Dataset	50
Gambar 4.12. Tampilan Dataset Hasil Penggabungan dan Pelabelan dalam Format CSV	52
 Gambar 5.1. Konfigurasi Alokator Memori GPU	 58
Gambar 5.2. <i>Import Library</i>	59
Gambar 5.3. Pemanggilan Dataset	60
Gambar 5.4. Pembagian Data Menjadi Data Latih dan Data Uji.....	61
Gambar 5.5. Penerapan <i>Preprocessing</i>	62
Gambar 5.6. Tahap <i>Preprocessing</i> Data.....	63
Gambar 5.7. Fungsi untuk Melatih Model DNN	67
Gambar 5.8. Fungsi untuk Melatih Model LSTM	68
Gambar 5.9. Fungsi untuk Melatih Model BiGRU.....	68
Gambar 5.10. Grafik Model <i>Deep Neural Network</i> (DNN) dengan: (a) Akurasi Model DNN dan (b) Loss Model DNN	69

Gambar 5.11. Grafik Model <i>Long Short-Term Memory</i> (LSTM) dengan: (a) Akurasi Model LSTM dan (b) Loss Model LSTM	71
Gambar 5.12. Grafik Model <i>Bidirectional Gated Recurrent Unit</i> (BiGRU) dengan: (a) Akurasi Model BiGRU dan (b) Loss Model BiGRU .	73
Gambar 5.13. Confusion Matrix untuk Model <i>Deep Neural Network</i> (DNN)	75
Gambar 5.14. Laporan Klasifikasi Model DNN	77
Gambar 5.15. <i>Confusion Matrix</i> untuk Model <i>Long Short-Term Memory</i> (LSTM)	78
Gambar 5. 16 Laporan Klasifikasi Model LSTM	80
Gambar 5.17. <i>Confusion Matrix</i> untuk Model <i>Bidirectional Gated Recurrent Unit</i> (BiGRU)	82
Gambar 5.18. Laporan Klasifikasi Model BiGRU	84
Gambar 6.1. Import Model Deteksi Intrusi pada Sistem Website.....	88
Gambar 6.2. Tampilan Awal Web Aplikasi	89
Gambar 6.3. Tampilan <i>Browse File</i>	89
Gambar 6.4. Tampilan Ketika Sudah Berhasil Mengunggah File.....	89

DAFTAR TABEL

Tabel 2.1. Perbandingan dari Penelitian Terdahulu Mengenai <i>Intrusion Detection System</i> Berbasis <i>Deep Learning</i>	15
Tabel 4.1. Perbedaan File Rekaman Jaringan antara .pcap dan .csv	41
Tabel 4.2. Ringkasan Deskripsi untuk Lalu Lintas Jaringan Normal dan Beberapa Jenis Serangan Umum	48
Tabel 4.3. Distribusi Jenis Serangan	53
Tabel 5.1. Konfigurasi Setiap Algoritma.....	66
Tabel 6.1. Pengujian Deteksi Intrusi Jaringan.....	91

INTISARI

KLASIFIKASI INTRUSI JARINGAN MENGGUNAKAN ALGORITMA *DEEP LEARNING*

Intisari

Valentinus Wilbert Soedjito

210711340

Penelitian ini bertujuan mengembangkan dan membandingkan algoritma *deep learning* untuk mengklasifikasi intrusi jaringan guna mengatasi keterbatasan *Intrusion Detection System* (IDS) konvensional dalam menghadapi serangan siber yang kian kompleks, termasuk *zero-day attack*. Dataset dibuat secara mandiri melalui simulasi serangan (DoS, Port Scanning, Brute Force, Spoofing) pada lingkungan virtual menggunakan Kali Linux dan Server Ubuntu, direkam dengan Wireshark, lalu diolah menjadi fitur aliran menggunakan CICFlowMeter dan digabungkan menjadi satu dataset berlabel.

Tiga model *deep learning* utama—*Deep Neural Network* (DNN), *Long Short-Term Memory* (LSTM), dan *Bidirectional Gated Recurrent Unit* (BiGRU) diimplementasikan dan dievaluasi. Hasil evaluasi menunjukkan ketiga model memiliki akurasi pelatihan dan validasi tinggi. Namun, analisis *Confusion Matrix* memperlihatkan DNN lebih praktis karena kemampuannya mendeteksi lalu lintas Normal (192 *True Positive*), sementara LSTM dan BiGRU gagal mendeteksi kelas Normal (*True Positive* = 0). Model yang dipilih kemudian diimplementasikan ke dalam IDS berbasis web menggunakan *framework* Streamlit, memungkinkan pengguna mengunggah file CSV untuk deteksi.

Kata Kunci: *Intrusion Detection System* (IDS), Serangan Siber, *Deep Learning*, CICFlowMeter, Wireshark

Dosen Pembimbing I: Y. Sigit Purnomo WP., S.T., M.Kom., Ph.D.

Dosen Pembimbing II: Wilfridus Bambang Triadi H., S.T., M.Cs.