

PENERAPAN ALGORITMA DECISION TREE DALAM ANALISIS LOG SISTEM ROUTER UNTUK PENGKLASIFIKASIAN SERANGAN DDOS

SKRIPSI

**Oleh
Farras Fatihatul Kautsar
202110715220**



**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BHAYANGKARA JAKARTA RAYA
2025**

LEMBAR PERSETUJUAN PEMBIMBING

Judul Skripsi : Penerapan Algoritma *Decision Tree* Dalam Analisis Log Sistem Router Untuk Pengklasifikasian Serangan DDoS

Nama Mahasiswa : Farras Fatihatul Kautsar

Nomor Pokok Mahasiswa : 202110715220

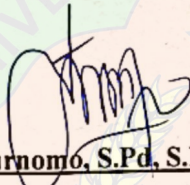
Program Studi/Fakultas : Informatika/Illmu Komputer

Tanggal Lulus Ujian Skripsi : 24 Juli 2025

Jakarta, 31/Juli/2025

MENYETUJUI,

Pembimbing I



(Rakhmat Purnomo, S.Pd, S.Kom, M.Kom.)

NIDN : 0322108201

Pembimbing II



(Muhammad Yasir, S.Si, M.Kom.)

NIDN : 0317129002

Ketua Program Studi



(Ahmad Fathurrozi, S.E., M.M.S.I.)

NIP : 2012486

PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BHAYANGKARA JAKARTA RAYA
2025

LEMBAR PENGESAHAN

Judul Skripsi : Penerapan Algoritma *Decision Tree* Dalam Analisis Log Sistem Router Untuk Pengklasifikasian Serangan DDoS
Nama Mahasiswa : Farras Fatihatul Kautsar
Nomor Pokok Mahasiswa : 202110715220
Program Studi/Fakultas : Informatika/Illmu Komputer
Tanggal Lulus Ujian Tugas
Akhir : 24 Juli 2025

Jakarta, 31/Juli/2025

MENGESAHKAN,

Ketua Tim Penguji : Ir. Muhammad Khaerudin, M.Kom

NIDN : 0413066604

Penguji I : Khairunnisa Fadhillah Ramdhania, S.Si, M.Si

NIDN : 0328039201

Penguji II : Rakhmat Purnomo, S.Pd, S.Kom, M.Kom

NIDN : 0322108201

MENGETAHUI,

Ketua

Program Studi Informatika



Ahmad Fathurrozi, S.E., M.M.S.I
NIP. 2012486

Dekan

Fakultas Ilmu Komputer



Dr. Robertus Suraji, S.S, M.A
NIP. 1904406



UNIVERSITAS BHAYANGKARA JAKARTA RAYA
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI INFORMATIKA

LEMBAR PERNYATAAN BUKAN PLAGIASI

Yang bertanda tangan dibawah ini :

Nama : Farras Fatihatul Kautsar
NPM : 202110715220
Program Studi : Informatika
Fakultas : Ilmu Komputer
Judul Tugas Akhir : Penerapan Algoritma *Decision Tree* Dalam Analisis Log
Sistem Router Untuk Pengklasifikasian Serangan DDoS

Dengan ini menyatakan bahwa hasil penulisan skripsi yang telah saya buat ini merupakan **hasil karya saya sendiri dan benar keasliannya**. Apabila dikemudian hari penulisan skripsi ini merupakan plagiat atau penjiplakan terhadap karya orang lain, maka saya bersedia mempertanggungjawabkan sekaligus bersedia menerima sanksi berdasarkan tata tertib di Universitas Bhayangkara Jakarta Raya.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan dari pihak manapun.

Jakarta, 31 Juli 2025

Penulis



Farras Fatihatul Kautsar
202110715220

ABSTRAK

Farras Fatihatul Kautsar. 202110715220. 2025. PENERAPAN ALGORITMA *DECISION TREE* DALAM ANALISIS LOG SISTEM ROUTER UNTUK PENGKLASIFIKASIAN SERANGAN DDoS

Peningkatan penggunaan jaringan komputer di lingkungan pendidikan memberikan kemudahan akses informasi, namun juga menimbulkan ancaman keamanan, salah satunya adalah serangan Distributed Denial of Service (DDoS) yang dapat menyebabkan gangguan serius pada ketersediaan layanan jaringan. Permasalahan utama dalam penelitian ini adalah belum adanya sistem deteksi dini yang mampu mengklasifikasikan lalu lintas jaringan normal dan lalu lintas mencurigakan secara otomatis berdasarkan data log sistem dari router Mikrotik. Penelitian ini bertujuan untuk menerapkan algoritma Decision Tree dalam menganalisis log sistem router Mikrotik guna mengklasifikasikan serangan DDoS di SMKN 2 Cikarang Barat. Metode yang digunakan mengikuti pendekatan CRISP-DM dengan tahapan business understanding, data understanding, data preparation, modeling, evaluation, dan deployment. Evaluasi model dilakukan menggunakan confusion matrix dan pengukuran metrik seperti akurasi, presisi, recall, serta f1-score. Hasil penelitian menunjukkan bahwa model klasifikasi dengan Decision Tree mencapai akurasi 98%, presisi 98%, recall 98%, dan f1-score tinggi pada kedua kelas. Kesimpulannya, algoritma Decision Tree efektif dalam membedakan pola lalu lintas normal dan serangan DDoS berdasarkan data log, dan dapat dijadikan dasar dalam pengembangan sistem deteksi dini serangan di lingkungan pendidikan.

Kata Kunci: *Decision Tree*, Router Mikrotik, Log Sistem, DDoS, Keamanan Jaringan.

ABSTRACT

Farras Fatihatul Kautsar. 202110715220. 2025. *APPLICATION OF DECISION TREE ALGORITHM IN ROUTER SYSTEM LOG ANALYSIS FOR CLASSIFICATION OF DDOS ATTACKS*

The increasing use of computer networks in educational environments provides easy access to information, but also poses security threats, one of which is a Distributed Denial of Service (DDoS) attack that can cause serious disruption to the availability of network services. The main problem in this study is the absence of an early detection system that is able to classify normal network traffic and suspicious traffic automatically based on system log data from Mikrotik routers. This study aims to apply the Decision Tree algorithm in analyzing Mikrotik router system logs to classify DDoS attacks at SMKN 2 Cikarang Barat. The method used follows the CRISP-DM approach with the stages of business understanding, data understanding, data preparation, modeling, evaluation, and deployment. Model evaluation is carried out using a confusion matrix and measuring metrics such as accuracy, precision, recall, and f1-score. The results show that the classification model with Decision Tree achieves 98% accuracy, 98% precision, 98% recall, and high f1-score in both classes. In conclusion, the Decision Tree algorithm is effective in distinguishing normal traffic patterns and DDoS attacks based on log data, and can be used as a basis for developing an early detection system for attacks in educational environments.

Keywords: *Decision Tree, Mikrotik Router, Log System, DDoS, Network Security.*

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIK

Sebagai sivitas akademik Universitas Bhayangkara Jakarta Raya saya yang bertanda tangan dibawah ini :

Nama : Farras Fatihatul Kautsar
NPM : 202110715220
Program Studi : Informatika
Fakultas : Ilmu Komputer
Jenis Karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Bhayangkara Jakarta Raya **Hak Bebas Royalti Non-Eksklusif (Non-Exclusive Royalty-Free Right)**, atas karya ilmiah saya yang berjudul :

Penerapan Algoritma *Decision Tree* Dalam Analisis Log Sistem Router Untuk Pengklasifikasian Serangan DDoS.

Beserta perangkat yang ada (bila diperlukan). Dengan hak bebas royalti non-eksklusif ini, Universitas Bhayangkara Jakarta Raya berhak menyimpan, mengalihmediakan, mengelolanya, dalam bentuk pangkalan data (database), mendistribusikannya dan mempublikasikannya di Internet atau media lain untuk kepentingan akademis tanpa perlu meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik hak cipta.

Segala bentuk tuntutan hukum yang timbul atas pelanggaran hak cipta dalam karya ilmiah ini menjadi tanggung jawab saya pribadi.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal : 31 Juli 2025

Yang menyatakan



KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT, karena dengan rahmat, petunjuk dan karunia-Nya penulis dapat menyelesaikan penyusunan skripsi yang berjudul “Penerapan Algoritma *Decision Tree* Dalam Analisis Log Sistem Router Untuk Pengklasifikasian Serangan DDoS”. Skripsi ini disusun sebagai salah satu syarat untuk menyelesaikan jenjang pendidikan Strata Satu (S1) pada Program Studi Informatika. Tidak lupa juga penulis mengucapkan banyak terimakasih sebesar-besarnya kepada semua pihak yang secara langsung maupun tidak langsung dalam membantu penulisan skripsi ini. Oleh karena itu, penulis ingin menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Bapak Irjen. Pol. (Purn) Prof. Dr. Drs. Bambang Karsono, S.H., M.M., Ph.D., D.Crim. (HC) selaku Rektor Universitas Bhayangkara Jakarta Raya.
2. Bapak Dr. Robertus Suraji, M.A. selaku Dekan Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.
3. Bapak Ahmad Fathurrozi, S.E., M.M.S.I selaku Ketua Program studi Informatika Universitas Bhayangkara Jakarta Raya.
4. Bapak Rakhmat Purnomo, S.Pd, S.Kom, M.Kom selaku Dosen Pembimbing I yang telah membantu menyelesaikan dalam penulisan Skripsi.
5. Bapak Muhammad Yasir, S.Si, M.Kom selaku Dosen Pembimbing II yang telah membantu menyelesaikan dalam penulisan Skripsi.
6. Bapak dan Ibu Dosen Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya yang selama ini telah memberikan ilmu dalam menempuh jenjang S1.

7. Staf Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya atas bantuannya dalam administrasi.
8. Bapak Muhammad Fariz Al Fatah, S. Kom., M.M. yang telah mengizinkan serta memberikan waktu dan tempat serta bantuan dalam melaksanakan penelitian di SMK N 2 Cikarang Barat.
9. Keluarga tercinta yang selalu memberikan doa, dukungan moril maupun materil, serta semangat yang tiada henti kepada penulis.
10. Rekan-rekan seperjuangan mahasiswa angkatan 2021 dari Program Studi Informatika Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya atas dukungan dan kerjasamanya dalam penyelesaian skripsi ini.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun demi perbaikan di masa mendatang. Semoga skripsi ini dapat memberikan manfaat, baik bagi pembaca maupun bagi perkembangan ilmu pengetahuan, khususnya dalam bidang keamanan jaringan dan penerapan algoritma machine learning.

Jakarta, 31 Juli 2025



Farras Fatihatul Kautsar

202110715220

DAFTAR ISI

LEMBAR PERSETUJUAN PEMBIMBING	i
LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN BUKAN PLAGIASI	iii
ABSTRAK	iv
ABSTRACT	v
LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR TABEL	xiii
DAFTAR GAMBAR	xiv
DAFTAR LAMPIRAN	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Identifikasi Masalah	5
1.3 Rumusan Masalah	5
1.4 Batasan Masalah	6
1.5 Tujuan Penelitian	6
1.6 Manfaat Penelitian	7

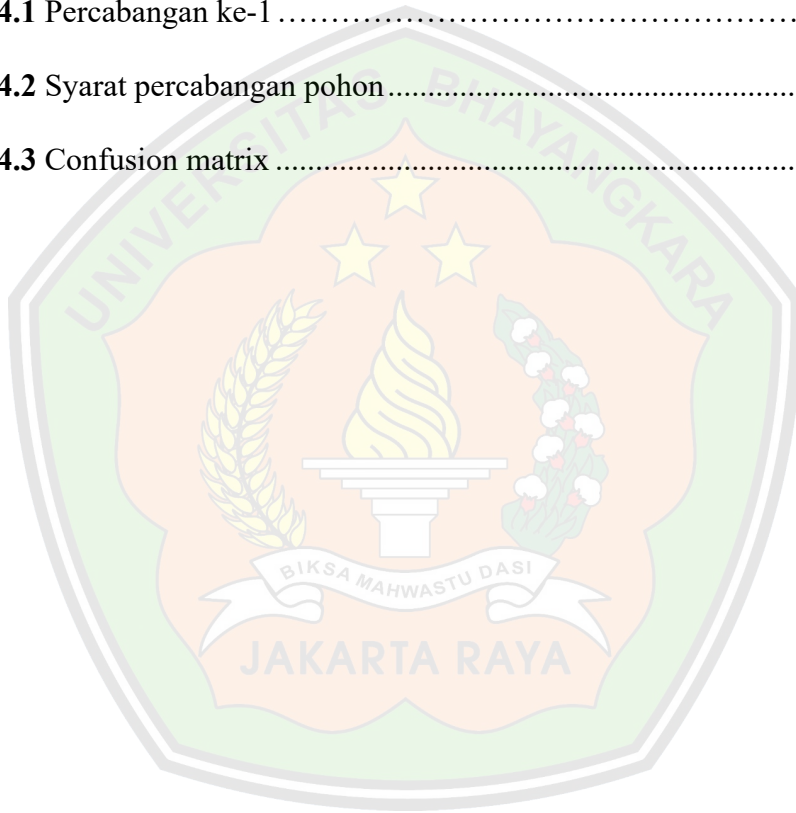
1.7 Sistematika Penulisan	7
BAB II TINJAUAN PUSTAKA	9
2.1 Penelitian Terdahulu.....	9
2.2 Landasan Teori	10
2.2.1 Jaringan Komputer	10
2.2.2 Protokol Jaringan	12
2.2.3 <i>Distributed Denial of Service (DDOS)</i>	14
2.2.4 CRISP-DM.....	16
2.2.5 Flowchart	19
2.2.6 Konsep Klasifikasi	21
2.2.7 Model Klasifikasi	21
2.2.8 <i>Decision Tree</i>	23
2.2.9 <i>Confusion Matrix</i>	24
BAB III METODOLOGI PENELITIAN	27
3.1 Objek dan Tempat Penelitian	27
3.2 Kerangka Penelitian	27
3.3 Metode Pengumpulan Data	29
3.3.1 Observasi.....	30
3.3.2 Wawancara	32
3.3.3 Log Mikrotik	32
3.4 CRISP DM	33

3.4.1 Business Understanding	33
3.4.2 Data Understanding.....	33
3.4.3 Data Preparation.....	34
3.4.4 Modeling	34
3.4.5 Evaluation	36
3.4.6 Deployment.....	36
3.5 Metode Analisis.....	37
3.5.1 Analisis Sistem Berjalan	37
3.5.2 Analisis sistem usulan	39
3.5.3 Analisis Permasalahan.....	40
3.6 Alat dan Software Pendukung.....	42
3.6.1 Alat Pendukung Penelitian :	42
3.6.2 Software Pendukung Penelitian :	42
BAB IV HASIL DAN PEMBAHASAN.....	43
4.1 <i>Busines Understanding</i>	43
4.2 <i>Data Understanding</i>	44
4.2.1 Akses Router MikroTik.....	44
4.2.2 Eksplorasi dan Karakteristik Data.....	45
4.3 <i>Data Preparation</i>	46
4.3.1 Transformasi Data	46
4.3.2 Pembuatan Kolom Baru	47

4.4 Modelling	49
4.4.1 Labeling Data	50
4.4.2 Pembentukan Pohon Keputusan (<i>Decision Tree</i>).....	50
4.5 Evaluation	60
4.5.1 Confusion Matrix	61
4.5.2 Perhitungan Manual Evaluasi Model	62
4.6 Deployment	66
BAB V PENUTUP	67
5.1 Kesimpulan	67
5.2 Saran.....	68
DAFTAR PUSTAKA.....	69
LAMPIRAN.....	69

DAFTAR TABEL

Tabel 2.1 Penelitian terdahulu yang relevan.....	9
Tabel 2.2 Simbol Flowchart.....	20
Tabel 2.3 Confusion Matrix.....	25
Tabel 3.1 Alat pendukung penelitian.....	42
Tabel 3.2 Software pendukung penelitian	42
Tabel 4.1 Percabangan ke-1	56
Tabel 4.2 Syarat percabangan pohon.....	60
Tabel 4.3 Confusion matrix	61



DAFTAR GAMBAR

Gambar 2.1 CRISP-DM	17
Gambar 2.2 Proses Klasifikasi.....	22
Gambar 3.1 Lokasi SMK N 2 Cikarang Barat.....	27
Gambar 3.2 Tahapan Penelitian	28
Gambar 3.3 Diagram proses pengumpulan data.....	30
Gambar 3.4 Server.....	31
Gambar 3.5 Digram ekspor log mikrotik.....	32
Gambar 3.6 Topologi yang sedang berjalan	38
Gambar 4.1 Menu pada mikrotik.....	44
Gambar 4.2 Ekstrak log.....	45
Gambar 4.3 Data sebelum ditransformasi	46
Gambar 4.4 Data setelah di transformasi.....	47
Gambar 4.5 Fitur frequency.....	48
Gambar 4.6 Fitur packet size	48
Gambar 4.7 Fitur protocol	49
Gambar 4.8 Pengkodean labeling pada data.....	50
Gambar 4.9 Visualisasi split data.....	61
Gambar 4.10 Visualisasi Confusion Matrix.....	62
Gambar 4.11 Visualisasi precision.....	64
Gambar 4.12 Visualisasi hasil recall per-class.....	65
Gambar 4.13 Visualisasi hasil f1-score	66

DAFTAR LAMPIRAN

Lampiran 1. Dosen Pembimbing 1	72
Lampiran 2. Dosen Pembimbing 2	73
Lampiran 3. Dataset	70
Lampiran 4. Upload data pada google colab.....	70
Lampiran 5. Split data	71
Lampiran 6. Algoritma <i>Decision Tree</i> dan evaluasi dengan hyperparameter tuning	71
Lampiran 7. Evaluasi per class.....	72
Lampiran 8. Hasil cek turnitin	76
Lampiran 9. Kesimpulan	77

