

TUGAS AKHIR

***DASHBOARD MONITORING DAN PERTAHANAN SERANGAN SIBER
OTOMATIS DENGAN VISUALISASI REALTIME***



ANDI ATILA BACHRI

NPM 22120012

DOSEN PEMBIMBING

Dr. NIA SAURINA, S.ST., M.Kom.

TEGUH PRIBADI IKHSAN, S.Kom., M.Kom

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS WIJAYA KUSUMA SURABAYA

2026

TUGAS AKHIR

***DASHBOARD MONITORING DAN PERTAHANAN SERANGAN SIBER
OTOMATIS DENGAN VISUALISASI REALTIME***



ANDI ATILA BACHRI

NPM 22120012

DOSEN PEMBIMBING

Dr. NIA SAURINA, S.ST., M.Kom.

TEGUH PRIBADI IKHSAN, S.Kom., M.kom

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS WIJAYA KUSUMA SURABAYA

2026

LEMBAR PENGESAHAN

Tugas Akhir Disusun Untuk Memenuhi Salah Satu
Syarat Memperoleh Gelar
Sarjana Komputer (S.kom)

Di
Universitas Wijaya Kusuma Surabaya

Oleh :

ANDI ATILA BACHRI
22120012

Hari / Tanggal Sidang : Senin, 13 Juli 2026

Menyetujui :

Dosen Pembimbing I

Dosen Pembimbing II


Dr. Nia Saurina, S.ST., M.Kom.
NIK 10423-ET


Teguh Priadi Khisan, S.Kom., M.Kom
NIK 12526-ET

Ketua Program Studi
Informatika


Nonot Wisnu Karyanto, ST., M.Kom.
NIK 11563-ET

Dekan
Fakultas Teknik


Dr. Ir. Anang Kukuh Adisusilo, ST., MT.
NIP 197802152015041001



LEMBAR PENGESAHAN REVISI

Judul : *DASHBOARD MONITORING DAN PERTAHANAN SERANGAN SIBER
OTOMATIS DENGAN VISUALISASI REALTIME*

Nama : Andi Attila Bachri
NPM : 22120012

Telah Diuji Pada :

Hari : Rabu
Tanggal : 15 Juli 2026
Tempat : R. Asistensi (F207)

Disetujui Oleh,

Dosen Penguji I



Nonot Wisnu Karyanto, ST., M.Kom.
NIK 11563-ET

Dosen Penguji II



Ir. FX Wisnu Yudo Untoro, M.Kom.
NIK 12574-ET

Mengetahui,

Dosen Pembimbing I



Dr. Nia Saurina, S.ST., M.Kom.
NIK 10423-ET

Dosen Pembimbing II



Teguh Pribadi Mhsan, S.Kom., M.Kom
NIK 12526-ET

PERNYATAAN KEASLIAN TULISAN

Yang bertanda tangan dibawah ini saya :

Nama : Andi Attila Bachri

NPM 22120012

Program Studi : Informatika

Fakultas Teknik Universitas Wijaya Kusuma Surabaya

Menyatakan dengan sebenarnya bahwa Skripsi Tugas Akhir yang saya tulis dengan judul “Dashboard Monitoring dan Pertahanan Serangan Siber Otomatis dengan Visualisasi Realtime”, Benar-benar hasil karya saya sendiri, Bukan merupakan pengambilan tulisan atau pikiran orang lain yang saya akui sebagai tulisan atau pikiran saya sendiri. Apabila di kemudian hari dapat dibuktikan bahwa Skripsi Tugas Akhir ini adalah hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Surabaya, 21 Juli 2026

Yang membuat pernyataan,



Andi Attila Bachri

DASHBOARD MONITORING DAN PERTAHANAN SERANGAN SIBER OTOMATIS DENGAN VISUALISASI *REALTIME*

Andi Attila Bachri

Program Studi Informatika Fakultas Teknik

Universitas Wijaya Kusuma Surabaya

attila.bachri@gmail.com

ABSTRAK

Perkembangan teknologi informasi yang pesat telah meningkatkan kompleksitas ancaman siber pada berbagai sektor, termasuk institusi pendidikan. Serangan seperti *brute force*, *SQL injection*, *web defacement*, dan request *flooding* semakin sulit dideteksi apabila hanya menggunakan metode konvensional. Kondisi ini menuntut adanya sistem pertahanan siber yang mampu melakukan deteksi dan *respons* otomatis secara *real-time*. Penelitian ini bertujuan merancang dan mengembangkan *dashboard monitoring* serta sistem pertahanan serangan siber dengan visualisasi keamanan jaringan secara interaktif yang berfungsi secara operasional. Metode penelitian yang digunakan adalah *Research and Development (R&D)*, meliputi tahapan analisis serangan, pengolahan log, pengembangan modul *AI Brain*, pembangunan *security agent*, dan integrasi sistem. *AI Brain* dilatih menggunakan model *machine learning* untuk mendeteksi anomali serta mengklasifikasikan aktivitas mencurigakan, sementara *security agent* berfungsi mengeksekusi tindakan pertahanan otomatis seperti pemblokiran *IP* dan pemulihan *file* akibat serangan

Kata Kunci: *Artificial Intelligence, Cyber Defense, Machine Learning, Security Agent, IDS*

KATA PENGANTAR

Puji Syukur ke pada Tuhan Yang Maha Esa atas segala karunia nya sehingga penulis dapat menyelesaikan penulisan laporan tugas akhir yang berjudul “*DASHBOARD MONITORING DAN PERTAHANAN SERANGAN SIBER OTOMATIS DENGAN VISUALISASI REALTIME*”

Laporan Tugas Akhir ini dilaksanakan dengan baik di kampus Universitas Wijaya Kusuma Surabaya. Laporan Tugas Akhir ini merupakan tugas yang harus di selesaikan oleh mahasiswa jurusan informatika program S1 di Universitas Wijaya Kusuma Surabaya. Tujuan utama dari pembuatan Laporan tugas akhir ini untuk memantapkan teori dan praktek yang telah dipelajari di kampus dan dapat diselesaikan dengan serta diaplikasikan di lapangan. Oleh karena itu perkenankanlah penulis mengucapkan terimakasih yang sebesar-besarnya dan penghargaan yang setinggi-tingginya kepada :

1. Orang tua dan keluarga penulis yang selalu memberikan doa terbaiknya dan dukungan kepada penulis
2. Ibu Dewi Fitria Sukmawati Sebagai Ibu dari penulis, karena segala perjuangannya menghantarkan penulis Menjadi Seorang Sarjana.
3. Bapak Dr.Ir.Anang Kukuh Adisusilo, ST., MT. Sebagai Dekan Fakultas Teknik
4. Bapak Nonot Wisnu Karyanto, ST., M.Kom Sebagai Kaprodi Informatika
5. Dosen Pembimbing Ibu Dr. Nia Saurina, S.ST., M.Kom.
6. Dosen Pembimbing Bapak Teguh Pribadi Ikhsan, S.Kom., M.Kom.
7. Segenap Dosen Program Studi Informatika Universitas Wijaya Kusuma Surabaya yang telah memberikan ilmunya kepada saya selama masa perkuliahan
8. Teman teman Fakultas Teknik saya yang selalu memberikan semangat dalam penulisan Laporan tugas akhir ini

Ucapan terima kasih juga penulis sampaikan kepada pihak-pihak lain yang tidak dapat disebutkan satu per satu atas kontribusi dan dukungannya. Penulis menyadari sepenuhnya bahwa Laporan Tugas Akhir ini masih memiliki kekurangan, sehingga kritik dan saran yang membangun dari semua pihak sangat penulis harapkan demi perbaikan lebih lanjut

Surabaya, 15 Juli 2026

Andi Attila Bachri

DAFTAR ISI

HALAMAN JUDUL	i
ABSTRAK	v
KATA PENGANTAR	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL	xii
BAB I.....	1
PENDAHULUAN	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah	2
1.3. Tujuan Penelitian	3
1.4. Manfaat Penelitian.....	3
1.5. Batasan Masalah	3
1.6. Sistematika Penulisan	4
BAB II	6
TINJAUAN PUSTAKA	6
2.1. Penelitian Terdahulu	6
2.2. Keamanan Jaringan.....	7
2.3. <i>Cybersecurity</i> dan Perkembangannya	7
2.4. <i>Ransomware</i> (Penyanderaan Data).....	9
2.5. <i>DDoS (Distributed Denial of Service)</i>	9
2.6. <i>SQL Injection</i>	10
2.7. <i>Malware (Malicious Software)</i>	10
2.8. <i>Brute Force Attack</i>	11
2.9. <i>Web Defacement</i>	11
2.10. <i>XSS (Cross Site Scripting)</i>	12
2.11. <i>Man In The Middle Attack</i>	13
2.12. <i>Artificial Intelligence</i>	13
2.13. <i>Machine Learning</i> untuk keamanan	14
2.14. <i>Random Forest</i>	15
2.15. <i>Isolation Forest</i>	15
2.16. <i>Python</i>	15

2.17.	<i>Teori R&d</i>	16
2.18.	Arsitektur Sistem Keamanan Siber Terintegrasi.....	17
BAB III		19
METODOLOGI PENELITIAN		19
3.1.	Jenis penelitian	19
3.2.	Pendekatan dan Metode Pengembangan	22
3.3	Lingkungan Penelitian.....	22
3.4	Instrumen Penelitian	23
3.5	Arsitektur Pengembangan <i>AI Brain</i> dan <i>Security Agent</i>	23
3.6	Teknik Pengumpulan Data.....	25
3.7	Validasi Desain	26
3.8	Rumus Evaluasi dan Deteksi	26
3.8.1.	Rumus <i>Confusion Matrix</i>	26
3.8.2.	Rumus <i>Accuracy</i> (Akurasi)	26
3.8.3.	Rumus <i>Precision</i> (Presisi)	27
3.8.4.	Rumus <i>Recall</i> (<i>Recall / Sensitivity</i>)	27
3.8.5.	Rumus <i>F1 Score</i>	28
3.8.6.	Rumus <i>Weighted Average</i> (Untuk <i>Multi-Class</i>)	28
3.8.7.	Rumus <i>ROC-AUC</i> (<i>Area Under ROC Curve</i>)	28
3.8.8.	Rumus <i>Cross-Validation</i> (<i>CV Score</i>)	29
3.8.9.	Rumus <i>OOB Score</i> (<i>Out-of-Bag Score</i>)	29
3.8.10.	Rumus <i>Isolation Forest</i> (<i>Anomaly Detection</i>)	29
3.8.11.	Rumus <i>Feature Extraction</i> (30 Fitur)	30
3.8.12.	Rumus <i>Decision Engine</i> (3-Layer <i>Detection</i>)	31
3.8.13.	<i>Final Decision Confidence</i>	32
3.8.14.	<i>Response Time</i>	32
3.8.15.	<i>Feature Normalization</i> (<i>StandartdScaler</i>)	32
3.9	Teknik Pengujian Sistem	33
3.10	<i>Flowchart AI Brain</i>	34
3.11	<i>Flowchart Security Agent</i>	35
3.12	<i>Flowchart Dashboard</i>	36
3.13	<i>Rule Based Detection Engine</i> (32 Rules).....	37
3.14	Desain <i>UI/UX</i>	40
3.14.1	Desain Halaman <i>Overview</i>	40

3.14.2	Desain Halaman Monitoring	41
3.14.3	Desain Halaman <i>Attack Intelligence</i>	42
3.14.4	Halaman <i>AI Analysis</i>	42
3.14.5	Desain Halaman <i>Auto Defense</i>	44
3.14.6	Desain Halaman <i>Logs</i>	45
HASIL DAN PEMBAHASAN		46
4.1	Hasil dan Implementasi Sistem	46
4.1.1	Arsitektur dan Implementasi Sistem.....	48
4.1.2	Alur Komunikasi Antar Komponen.....	49
4.2	Implementasi Antarmuka Sistem (<i>Dashboard</i>)	50
4.2.1	Halaman <i>Overview</i>	50
4.2.2	Halaman Monitoring	51
4.2.3	Halaman <i>Attack Intelligence</i>	52
4.2.4	Halaman <i>AI Analysis</i>	53
4.2.5	Halaman <i>Auto Defense</i>	55
4.2.6	Halaman <i>logs</i>	55
4.3	Hasil Pengujian Deteksi Serangan.....	56
4.3.1	Pengujian <i>SQL Injection</i>	57
4.3.2	Pengujian <i>XSS (Cross-Site Scripting)</i>	58
4.3.3	Pengujian <i>Bruteforce Attack</i>	59
4.3.4	Pengujian <i>Web Defacement</i>	60
4.3.5	Pengujian <i>DDoS/Request Flood</i>	61
4.3.6	Pengujian <i>Ransomware</i>	62
4.3.7	Pengujian <i>MITM (Man in The Middle)</i>	62
4.3.8	Pengujian <i>Malware Injection</i>	63
4.4	Hasil Pengujian <i>Model Machine Learning</i>	64
4.4.1	<i>Dataset Training</i>	64
4.4.2	Hasil Evaluasi <i>Random Forest</i>	65
4.4.3	Hasil Evaluasi <i>Isolation Forest</i>	65
4.4.4	<i>Classification Report (Per Class)</i>	66
4.4.5	<i>Feature Importance (Top 10)</i>	67
4.5	Hasil Pengujian <i>Auto Defense Response</i>	67
4.5.1	<i>Response Time Analysis</i>	67
4.5.2	<i>Defense Action Succes Rate</i>	68

4.5.3	<i>Blocked IP Management</i>	68
4.6	Hasil Pengujian <i>Dashboard</i> dan Visualisasi.....	69
4.6.1	<i>Dashboard Performance</i>	69
4.6.2	<i>Realtime Attack Graph</i>	69
4.7	Analisis <i>3-Layer Detections</i>	69
4.7.1	<i>Layer Contribution</i>	69
4.7.2	<i>Layer Performance by Attack Type</i>	70
4.8	Analisis Kelebihan dan Kekurangan Sistem	70
4.8.1	Kelebihan Sistem.....	70
4.8.2	Kekurangan Sistem.....	70
4.9	Pembahasan	71
BAB V		74
KESIMPULAN DAN SARAN		74
5.1	Kesimpulan.....	74
5.2	Saran	74
DAFTAR PUSTAKA		75
LAMPIRAN		78

DAFTAR GAMBAR

Gambar 3. 1 Metode <i>R&D</i> Sistem <i>AI Cyber Defense</i>	19
Gambar 3. 2 Desain Arsitektur Sistem	25
Gambar 3. 3 <i>Flowchart AI Brain</i>	34
Gambar 3. 4 <i>Flowchart Security Agent</i>	35
Gambar 3. 5 <i>Flowchart Dashboard</i>	37
Gambar 3. 6 Desain Halaman <i>Overview</i>	41
Gambar 3. 7 Desain Halaman <i>Monitoring</i>	41
Gambar 3. 8 Desain Halaman <i>Attack Intelligence</i>	42
Gambar 3. 9 Desain Halaman <i>AI Analysis</i>	43
Gambar 3. 10 Desain Halaman <i>Auto Defense</i>	44
Gambar 3. 11 Desain Halaman <i>Logs</i>	45
Gambar 4. 1 Tampilan Halaman <i>Overview</i>	51
Gambar 4. 2 Tampilan Halaman <i>Monitoring</i>	52
Gambar 4. 3 Tampilan Halaman <i>Attack Intelligence</i>	53
Gambar 4. 4 Halaman <i>AI Analysis</i>	54
Gambar 4. 5 Tampilan Halaman <i>Auto Defense</i>	55
Gambar 4. 6 Tampilan Halaman <i>Logs</i>	56
Gambar 4. 7 <i>Blocked IP Management</i>	68

DAFTAR TABEL

Tabel 3. 1 Interpretasi <i>Anomaly Score</i>	29
Tabel 3. 2 <i>Decision Rules</i>	32
Tabel 4. 1 Serangan <i>SQL Injection</i>	57
Tabel 4. 2 Hasil Deteksi <i>SQL Injection</i>	57
Tabel 4. 3 Serangan <i>XSS</i>	58
Tabel 4. 4 Hasil Deteksi <i>XSS</i>	59
Tabel 4. 5 Serangan <i>Bruteforce</i>	59
Tabel 4. 6 Hasil Deteksi <i>Bruteforce</i>	60
Tabel 4. 7 Serangan <i>Defacement</i>	60
Tabel 4. 8 Hasil Deteksi <i>Defacement</i>	60
Tabel 4. 9 Serangan <i>DDoS/Request Flood</i>	61
Tabel 4. 10 Hasil Deteksi <i>DDoS</i>	61
Tabel 4. 11 Serangan <i>Ransomware</i>	62
Tabel 4. 12 Hasil Deteksi <i>Ransomware</i>	62
Tabel 4. 13 Serangan <i>MITM</i>	62
Tabel 4. 14 Hasil Deteksi <i>MITM</i>	62
Tabel 4. 15 Serangan <i>Malware</i>	63
Tabel 4. 16 Hasil Deteksi <i>Malware</i>	63
Tabel 4. 17 Dataset <i>Training</i>	64
Tabel 4. 18 Evaluai <i>Random Forest</i>	65
Tabel 4. 19 Evaluasi <i>Isolation Forest</i>	65
Tabel 4. 20 <i>Clasification Report</i>	66
Tabel 4. 21 <i>Feature Importance</i>	67
Tabel 4. 22 Respon <i>Time Analysis</i>	67
Tabel 4. 23 Defense Action <i>Succes Rate</i>	68
Tabel 4. 24 Dashboard <i>Performance</i>	69
Tabel 4. 25 <i>Layer Contribution</i>	69
Tabel 4. 26 <i>Performance by Attack Type</i>	70