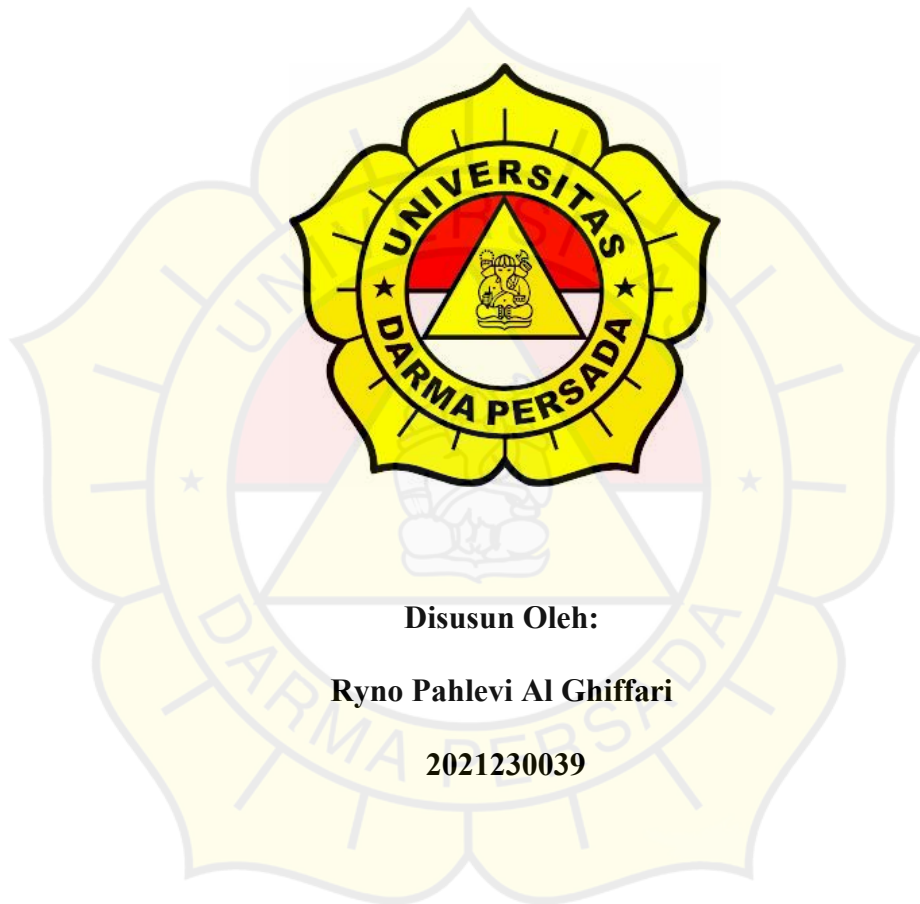


LAPORAN SKRIPSI

DETEKSI ANOMALI AKSES PADA SISTEM LOG FORTIGATE

FIREWALL MENGGUNAKAN AUTOENCODER DAN ONE-CLASS SVM

UNTUK ANALISIS SISTEM LOG FORTIGATE DI PT. XYZ



Disusun Oleh:

Ryno Pahlevi Al Ghiffari

2021230039

PROGRAM STUDI TEKNOLOGI INFORMASI

FAKULTAS TEKNIK

UNIVERSITAS DARMA PERSADA

JAKARTA TIMUR

2025

LEMBAR MONITORING BIMBINGAN



UNIVERSITAS DARMA PERSADA

Jl. Taman Malaka Selatan, Pondok Kelapa, Jakarta Timur, Indonesia 13450
Telp. (021) 8649051, 8649053, 8649057 Fax. (021) 8649052
E-mail : humas@unsada.ac.id Home page : <http://www.unsada.ac.id>

Instrumen Monitoring Bimbingan Skripsi Program Studi Teknologi Informasi

Tahun Akademik : 2024/2025 Genap

NIM>Nama Mhs : 1021230039 / RYNO RAHLEVI AL GHAFFARI
 Judul Skripsi : Deteksi Anomali Akses pada Sistem Log ~~Port~~ Fortigate Firewall
Menggunakan Autoencoder dan One-Class SVM untuk Analisis Sistem Log Fortigate di PFXYZ
 Dosen Pembimbing : Harianto S.Pd., M.T.

No	BAB Utama Skripsi dan BATAS WAKTU Bimbingan	Materi Yang dibahas saat Konsultasi	Tanggal Bimbingan	TTD Dosen
1		- Penulisan awal bab di Bold - awal paragraf menyerek ke dalam - tidak ada spasi antar numbered list	06 Mei 2025	
2	BAB I PENDAHULUAN			
3	Paling lama upload: 9 Mei 2025			
		Tanggal BAB I di ACC pembimbing =>	9/5	
4	BAB II LANDASAN TEORI	- penulisan awal bab di Bold - tambahkan referensi yg esensial	9/5/25	
5				
6	Paling lama upload: 9 Mei 2025			
		Tanggal BAB II di ACC pembimbing =>	9/5/25	
7	BAB III METODOLOGI	Flow diagram tnr 12 Paragraf menyerek Tambah chart tambah tahun, tambah VAT	9/5/25	
8		Line spacing double website tambah login	9/5/25	
9	Paling lama upload : 16 Mei 2025			
		Tanggal BAB III di ACC pembimbing =>	16-5-25	



UNIVERSITAS DARMA PERSADA

Jl. Taman Malaka Selatan, Pondok Kelapa, Jakarta Timur, Indonesia 13450

Telp. (021) 8649051, 8649053, 8649057 Fax. (021) 8649052

E-mail : humas@unsada.ac.id Home page : <http://www.unsada.ac.id>

10				
11	Percobaan/Demo Aplikasi atau Sistem			
12				
13				
			Tanggal Aplikasi/Sistem ACC pembimbing =>	
14	BAB IV HASIL DAN PEMBAHASAN	Perbaiki format penulisan, paragraf	4/6	
15		Perbaiki evaluasi maknitas	12/6	
16	Paling lama upload : 13 Juni 2025			
			Tanggal BAB IV di ACC pembimbing =>	
17	BAB V PENUTUP	- kesimpulan harus sesuai dgn rumusan masalah	12/6	
18			26/6	
			Tanggal BAB V di ACC pembimbing =>	
			26/6	

Catatan :

- Mahasiswa harus konsultasi jauh-jauh hari sebelum batas akhir tanggal per BAB nya.
- Tanggal Bimbingan dan ACC per BAB **HARUS** sebelum batas tanggal maksimum, tetapi boleh sebelum tanggalnya jika bisa lebih cepat
- Dokumen ini **WAJIB** diupload ke gform yang ditentukan pada range tanggal setiap BAB
- Ujian Seminar ISI akan diadakan pada range tanggal : 21 s.d 27 Juni 2025

ACC Mengikuti Seminar dari Pembimbing :

Jenis ACC	Tanggal	TTD Pembimbing
ACC Mendaftar Seminar Judul	26/6	
ACC Mendaftar Sidang Skripsi	25/07	

LEMBAR PERBAIKAN REVISI



UNIVERSITAS DARMA PERSADA

Jl. Taman Mahkota Selatan, Porolok Kelapa, Jakarta Timur, Indonesia 13450
Telp. (021) 8649051, 8649053, 8649057 Fax. (021) 8649052
E-mail: persada@persada.ac.id | www.persada.ac.id

LEMBAR REVISI - SIDANG SKRIPSI

NIM>Nama : 2021230039 - RYNO PAHLIVI AL GHIFFARI
Fakultas/Prodi : Teknik / Teknologi Informasi

No.	Keterangan Revisi	Dosen
1.	seuslta beapa sum leah jend dkonding ncthon aslar. jeculen jela beth 5 dng per mngkut dai pabul jromel	J. Bji F. H. H. H. H. H. G. H. H. H. H. O. H. H. H. H.

Mengetahui,
Ka Prodi Teknologi Informasi
Herianto, S.Pd., MT.

BERKUALITAS - BERKEMAJUAN - BERKONTRIBUSI



Jember, 10 Januari
2023



LEMBAR PERNYATAAN ORISINALITAS SKRIPSI

Saya yang bertanda tangan dibawah ini :

Nama : Ryno Pahlevi Al Ghiffari

NIM : 2021230039

Fakultas : Teknik

Jurusan : Teknologi Informasi

Dengan ini menyatakan bahwa skripsi dengan judul "**Deteksi Anomali Akses pada Sistem Log Fortigate Firewall Menggunakan Autoencoder dan One-Class SVM untuk Analisis Sistem Log Fortigate di PT. XYZ**" adalah benar hasil karya Penulis sendiri.

Penulis tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika keilmuan yang berlaku, serta tidak menggunakan karya orang lain tanpa mencantumkan sumbernya.

Apabila di kemudian hari terbukti pernyataan ini tidak benar, Penulis bersedia menerima sanksi akademik sesuai dengan peraturan yang berlaku di institusi.

Jakarta, 15 Oktober 2025



Ryno Pahlevi Al Ghiffari

LEMBAR PENGUJI SKRIPSI

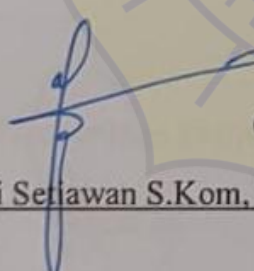
Skripsi yang berjudul:

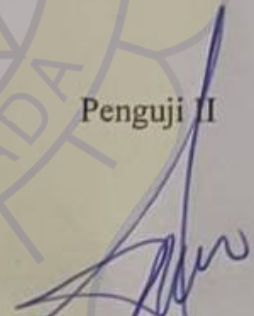
“DETEKSI ANOMALI AKSES PADA SISTEM LOG FORTIGATE
FIREWALL MENGGUNAKAN AUTOENCODER DAN ONE-CLASS SVM
UNTUK ANALISIS SISTEM LOG FORTIGATE DI PT. XYZ” ini telah diujikan
pada tanggal

“06 Agustus 2025”

Penguji I

Penguji II


Dr. Aji Setiawan S.Kom, MMSI


Andi Susilo S.Kom., M.T.I

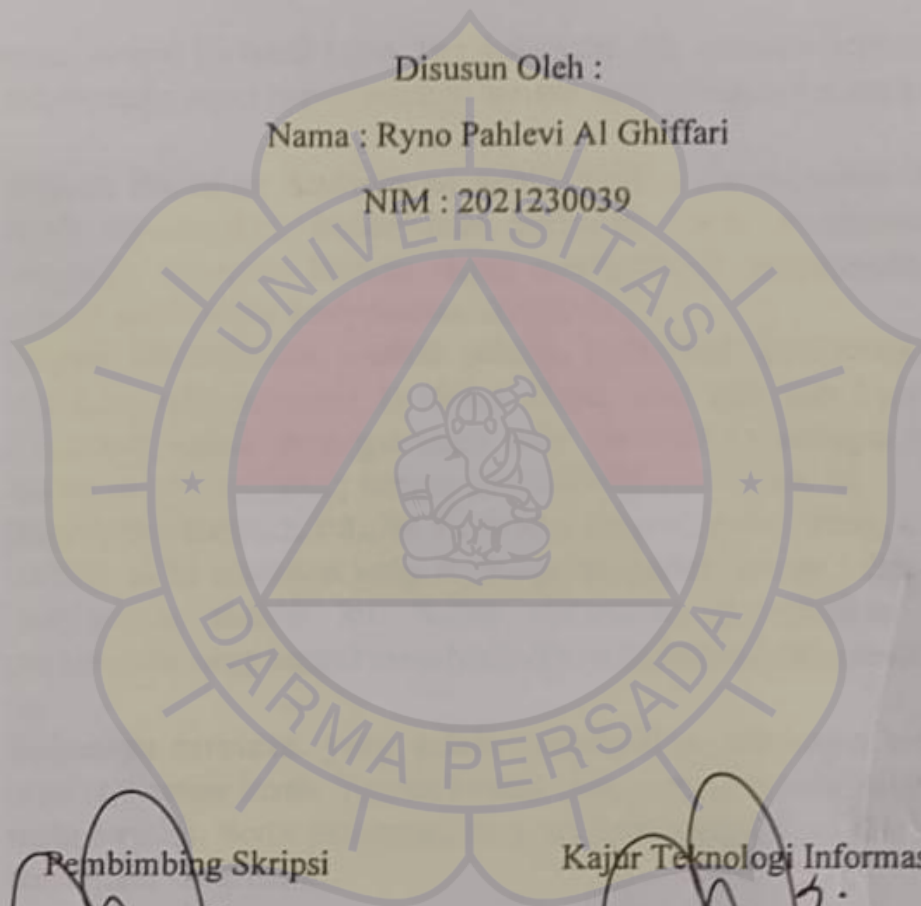
LEMBAR PENGESAHAN

DETEKSI ANOMALI AKSES PADA SISTEM LOG FORTIGATE FIREWALL
MENGUNAKAN AUTOENCODER DAN ONE-CLASS SVM UNTUK
ANALISIS SISTEM LOG FORTIGATE DI PT. XYZ

Disusun Oleh :

Nama : Ryno Pahlevi Al Ghiffari

NIM : 2021230039



Pembimbing Skripsi

Kajur Teknologi Informasi

Herianto, S.Pd., M.T

Herianto, S.Pd., M.T

KATA PENGANTAR

Puji syukur kehadirat Allah Subhanahu Wa Ta'ala atas segala rahmat dan karunia-Nya, sehingga skripsi berjudul "Deteksi Anomali Akses pada Sistem Log Fortigate Firewall Menggunakan Autoencoder dan One-Class SVM untuk Analisis Sistem Log Fortigate di PT. XYZ" ini dapat terselesaikan dengan baik. Skripsi ini merupakan salah satu syarat untuk memperoleh gelar sarjana di Universitas Darma Persada.

Penyusunan skripsi ini tidak lepas dari dukungan dan bantuan berbagai pihak. Oleh karena itu, Penulis ingin mengucapkan terima kasih yang tulus kepada:

1. **Bapak Ramdan Andriawan** selaku Office Management Manager, yang telah memberikan kesempatan berharga untuk melaksanakan program magang, sehingga Penulis dapat memperoleh pengalaman praktis yang sangat menunjang penyusunan skripsi ini.
2. **Bapak Miftahudin Luthfi** selaku CyberSec Technology Services & Business Development Division Head, atas izin dan kepercayaan yang diberikan untuk menggunakan data perusahaan sebagai bahan analisis dalam skripsi ini, yang sangat esensial bagi penelitian ini.
3. **Bapak Herianto, S.Pd., M.T.**, selaku Dosen Pembimbing, atas bimbingan, arahan, serta masukan yang berharga dan tidak pernah lelah selama proses penyusunan skripsi ini. Beliau senantiasa memberikan motivasi dan pencerahan yang sangat membantu Penulis dalam menyelesaikan penelitian ini.
4. **Keluarga tercinta**, yang selalu memberikan dukungan moral, doa, dan motivasi tanpa henti. Teman-teman, atas semangat dan kebersamaan yang telah terjalin. Serta pasangan, atas support, pengertian, dan motivasi yang senantiasa diberikan.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang membangun sangat Penulis harapkan demi penyempurnaan di masa mendatang. Semoga skripsi ini dapat memberikan manfaat bagi perkembangan ilmu pengetahuan, khususnya di bidang keamanan siber.

Bekasi, 15 Oktober 2025

Ryno Pahlevi Al Ghiffari

ABSTRAK

Analisis manual volume data log Fortigate yang besar di PT. XYZ memakan waktu dan rentan terhadap kesalahan, sehingga menyulitkan deteksi aktivitas mencurigakan. Penelitian ini mengatasi masalah tersebut dengan merancang dan mengimplementasikan sistem deteksi anomali otomatis menggunakan model *unsupervised machine learning*, yaitu Autoencoder dan One-Class SVM, yang dilatih hanya pada data log normal. Prosesnya dimulai dari pra-pemrosesan data dengan *parsing* dan rekayasa fitur untuk memilih 23 atribut informatif. Berdasarkan evaluasi kuantitatif, model Autoencoder menunjukkan performa superior dengan akurasi 95.53%, Recall 1.0000, Precision 0.7918, dan F1-Score 0.8838. Sebagai perbandingan, model One-Class SVM menghasilkan akurasi 88.74% dengan F1-Score 0.7507 (Precision: 0.6018, Recall: 0.9973). Sistem ini diwujudkan dalam aplikasi web interaktif berbasis Streamlit. Dengan demikian, pendekatan *unsupervised learning* menggunakan Autoencoder terbukti menjadi metode yang efektif dan andal untuk mengotomatisasi deteksi anomali pada log Fortigate, sekaligus meningkatkan efisiensi dan akurasi analisis keamanan jaringan di PT. XYZ.

Kata Kunci: Deteksi Anomali, *Unsupervised Learning*, *Autoencoder*, *One-Class SVM*, Log Fortigate, Keamanan Jaringan.

ABSTRACT

Manual analysis of large volumes of Fortigate log data at PT. XYZ is time-consuming and error-prone, hindering the timely detection of suspicious activities. This research addresses this issue by designing and implementing an automated anomaly detection system using two unsupervised machine learning models, Autoencoder and One-Class SVM, trained exclusively on normal log data. The process begins with data preprocessing, involving parsing and feature engineering to select 23 informative attributes. Quantitative evaluation reveals the Autoencoder model's superior performance, achieving an accuracy of 95.53%, a Recall of 1.0000, a Precision of 0.7918, and an F1-Score of 0.8838. In comparison, the One-Class SVM model yielded a lower accuracy of 88.74% and an F1-Score of 0.7507 (Precision: 0.6018, Recall: 0.9973). This system is implemented as an interactive web application built with Streamlit. Consequently, the unsupervised learning approach using an Autoencoder with meticulous feature engineering proves to be an effective and reliable method for automating anomaly detection in Fortigate logs, thereby enhancing the efficiency and accuracy of network security analysis at PT. XYZ.

Keywords: Anomaly Detection, Unsupervised Learning, Autoencoder, One-Class SVM, Fortigate Logs, Network Security.

DAFTAR ISI

LEMBAR MONITORING BIMBINGAN	i
LEMBAR PERBAIKAN REVISI	iii
LEMBAR PERNYATAAN ORISINALITAS SKRIPSI	iv
LEMBAR PENGUJI SKRIPSI	v
LEMBAR PENGESAHAN	vi
KATA PENGANTAR	vii
ABSTRAK	viii
DAFTAR ISI	x
DAFTAR TABEL	xiii
DAFTAR GAMBAR	xiv
DAFTAR LAMPIRAN	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Identifikasi Masalah	3
1.3 Rumusan Masalah	3
1.4 Batasan Masalah	4
1.5 Tujuan Penelitian	4
1.6 Manfaat Penelitian	4
1.7 Metode Penelitian	5
1.7.1 Metode Pengumpulan Data	5
1.8 Sistematika Penulisan Laporan Skripsi	5
1.8.1 Komponen Awal Laporan	6
1.8.2 Bagian Pendahuluan dan Abstrak	6
1.8.3 Struktur Isi Laporan	6
BAB II LANDASAN TEORI	8
2.1 Landasan Teori	8
2.1.1 Konsep Dasar <i>Machine Learning</i> dan <i>Deep Learning</i>	9
2.1.2 Metodologi CRISP-DM	12
2.1.3 Pemodelan Sistem Menggunakan UML	16
2.1.4 Bahasa Pemrograman Python dan Library Terkait	18

2.1.5 Sistem Log Keamanan Jaringan	20
2.1.6 Wazuh	22
2.1.7 Fortigate dan Format Syslog.....	23
2.1.8 Deteksi Anomali	25
2.1.9 Autoencoder.....	26
2.1.10 One-Class SVM	28
2.1.11 Evaluasi Model	32
2.1.12 <i>Tools Website</i> dan Sistem Integrasi	35
2.2 Kajian Penelitian Terdahulu	37
2.2.1 Paper 1: <i>Syscall Security Components</i> , HP Léo, dipublikasikan di Repositorio Aberto, University of Porto, 2024. Klasifikasi jurnal: Repositori akademik terakreditasi universitas Eropa.	38
2.2.2 Paper 2: <i>Anomaly Detection Through User Behaviour Analysis</i> , V. Dumitrasc, dipublikasikan di Universitat Politècnica de Catalunya (UPC), 2023. Klasifikasi jurnal: Repositori TFM terakreditasi EHEA (European Higher Education Area).	39
2.2.3 Paper 3: <i>Survey on Unified Threat Management (UTM) Systems for Home Networks</i> , Siddiqui et al., dipublikasikan di IEEE Communications Surveys & Tutorials, 2024. Klasifikasi jurnal: Q1 (Scopus), IEEE.	40
2.2.4 Paper 4: <i>Deteksi Anomali Jaringan Menggunakan Isolation Forest pada Log Wazuh dengan Pemberitahuan WhatsApp di PT XYZ</i> , R.P. Dewa & W. Windarto, dipublikasikan di KRESNA: Jurnal Riset dan Inovasi Teknik Informatika, Universitas Budi Luhur, 2024. Klasifikasi jurnal: SINTA 5 (Indonesia).	41
2.2.5 Paper 5: <i>ML-Driven Log Analysis for Real-Time Cyber Threat Detection in Security Operation Centers</i> , S.A. Chamkar et al., dipublikasikan di <i>Preprints</i> , 2025. Klasifikasi: Pra-cetak akademik dari penelitian Universitas Maroko.....	42
BAB III METODOLOGI PENELITIAN.....	44
3.1 Rancangan Dasar Penelitian	44
3.2 Kerangka Kerja Metodologi CRISP-DM	47
3.3 Alur Kerja Model Deteksi Anomali.....	53
3.4 Perancangan Sistem dan Antarmuka	62
BAB IV HASIL DAN PEMBAHASAN	77
4.1 Hasil Penelitian	77
4.2 Analisa Hasil.....	93

BAB V KESIMPULAN DAN SARAN.....	98
DAFTAR PUSTAKA	104
LAMPIRAN.....	109



DAFTAR TABEL

Tabel 3.1 Gantt Chart Jadwal Penelitian	73
Tabel 3.2 Struktur Atribut Dataset Penelitian	95
Tabel 4.1. Hasil tes evaluasi model	120



DAFTAR GAMBAR

Gambar 2. 1 Arsitektur Autoencoder(Jimenez et al., 2020)	27
Gambar 2. 2 Arsitektur One-Class SVM (Liang, et al, 2018)	30
Gambar 3. 1 Alur CRISP-DM.....	47
Gambar 3. 2 Diagram Pra-Pemrosesan Data.....	54
Gambar 3. 3 Flowchart Training Model	56
Gambar 3. 4 Flowchart Arsitektur Autoencoder.....	58
Gambar 3. 5 Flowchart Arsitektur OC-SVM.....	60
<i>Gambar 3. 6 Usecase Website Deteksi Anomali</i>	<i>63</i>
<i>Gambar 3. 10 Mockup halaman website unggah file</i>	<i>72</i>
<i>Gambar 3. 11 Mockup halaman website Error file tidak valid</i>	<i>73</i>
<i>Gambar 3. 12 Mockup halaman website Log berhasil di proses.....</i>	<i>73</i>
<i>Gambar 3. 13 Mockup halaman website Log sudah ready pilih model.....</i>	<i>74</i>
<i>Gambar 3. 14 Mockup Halaman Website Deteksi Selesai dan Download File....</i>	<i>75</i>
Gambar 3. 15 Mockup Web Dashboard History.....	75
Gambar 4. 1 Halaman Login Web	79
Gambar 4. 2 Tampilan Page Home	79
Gambar 4. 3 Tampilan Dashboard Deteksi Anomali	80
Gambar 4. 4 Tampilan Unggah File.....	80
Gambar 4. 5 Ringkasan Hasil Deteksi	81
Gambar 4. 6 Hasil Deteksi Anomali	82
Gambar 4. 7 Hasil Excel Deteksi Anomali	82
Gambar 4. 8 Dashboard History Bulanan	83
Gambar 4. 9 Confusion Matrix Autoencoder.....	90
Gambar 4. 10 Confusion Matrix One-Class SVM.....	91

DAFTAR LAMPIRAN

Lampiran 1 Surat Keterangan Bebas Plagiat	108
Lampiran 2 <i>Originality Report</i>	109
Lampiran 3 Source Code.....	119

