

**OPTIMASI KEAMANAN JARINGAN KOMPUTER  
BERBASIS LIVE ANALYSIS DAN ALGORITMA  
*MACHINE LEARNING* PADA *INTRUSION  
DETECTION SYSTEM (IDS)*  
STUDI KASUS POLTEKKES KARTINI BALI**

**TESIS**

**OLEH  
I PUTU YESHA AGUS ARIWANTA  
NIM 2229101064**



**PROGRAM STUDI ILMU KOMPUTER  
PROGRAM PASCASARJANA  
UNIVERSITAS PENDIDIKAN GANESHA  
2024**

**OPTIMASI KEAMANAN JARINGAN KOMPUTER  
BERBASIS LIVE ANALYSIS DAN ALGORITMA  
*MACHINE LEARNING* PADA *INTRUSION  
DETECTION SYSTEM (IDS)*  
STUDI KASUS POLTEKKES KARTINI BALI**

**TESIS**

**Diajukan kepada  
Universitas Pendidikan Ganesha  
untuk Memenuhi Sebagian Persyaratan  
Memperoleh Gelar Magister Komputer  
Program Studi Ilmu Komputer**

**OLEH  
I PUTU YESHA AGUS ARIWANTA  
NIM 2229101064**



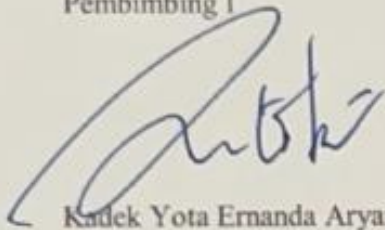
**PROGRAM STUDI ILMU KOMPUTER  
PROGRAM PASCASARJANA  
UNIVERSITAS PENDIDIKAN GANESHA  
2024**

## LEMBAR PERSETUJUAN

Tesis oleh I Putu Yesha Agus Ariwanta ini telah diperiksa dan disetujui untuk mengikuti Ujian Tesis

Singaraja, 21 Mei 2024

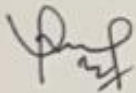
Pembimbing I



Kadek Yota Ernanda Aryanto, S.Kom., M.T., Ph.D.

NIP. 197803242005011001

Pembimbing II



Dr. I Gede Aris Gunadi, S.Si. M.Kom.

NIP. 197703182008121004

## LEMBAR PENGESAHAN

Tesis oleh I Putu Yesha Agus Ariwanta ini telah dipertahankan di depan tim penguji dan dinyatakan diterima sebagai salah satu persyaratan untuk memperoleh gelar Magister Komputer di Program Studi Ilmu Komputer, Program Pascasarjana, Universitas Pendidikan Ganesha.

Disetujui pada tanggal: Juli 2024

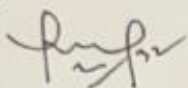
oleh  
Tim Penguji



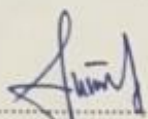
Ketua (Dr. I Made Gede Sunarya, S.Kom., M.Cs.)  
NIP 198307252008011008



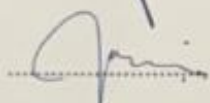
Anggota (Kadek Yota Ernanda Aryanto, S.Kom., M.T., Ph.D.)  
NIP 197803242005011001



Anggota (Dr. I Gede Aris Gunadi, S.Si. M.Kom.)  
NIP 197703182008121004



Anggota (Dr. I Made Gede Sunarya, S.Kom., M.Cs.)  
NIP 198307252008011008



Anggota (Dr. Luh Joni Erawati Dewi, S.T., M.Pd.)  
NIP 197606252001122001



Mengetahui Direktur  
Program Pascasarjana Undiksha,

Prof. Dr. I Nyoman Jampel, M.Pd.  
NIP 195910101986031003

## LEMBAR PERNYATAAN

Saya menyatakan dengan sesungguhnya bahwa tesis yang saya susun sebagai syarat untuk memperoleh gelar Magister Komputer dari Program Pascasarjana Universitas Pendidikan Ganesha seluruhnya merupakan hasil karya saya sendiri. Bagian-bagian tertentu dalam penulisan tesis yang saya kutip dari hasil karya orang lain telah dituliskan sumbernya secara jelas dan sesuai dengan norma, kaidah, serta etika akademis.

Apabila di kemudian hari ditemukan seluruh atau sebagian tesis ini bukan hasil karya saya sendiri atau adanya plagiat dalam bagian-bagian tertentu, saya bersedia menerima sanksi pencabutan gelar akademik yang saya sandang dan sanksi-sanksi lainnya sesuai dengan peraturan perundang-undangan yang berlaku di wilayah Negara Kesatuan Republik Indonesia.

Singaraja, 8 Juli 2024

Yang memberi pernyataan,



(I Putu Yesha Agus Ariwanta)

## PRAKATA

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas anugrahNya, sehingga tesis yang berjudul: “Optimasi Keamanan Jaringan Komputer Berbasis Live Analysis dan Algoritma *Machine Learning* Pada *Intrusion Detection System* (IDS) Studi Kasus Poltekkes Kartini Bali”, dapat diselesaikan sesuai dengan yang direncanakan.

Tesis ini ditulis untuk memenuhi salah satu persyaratan untuk memperoleh gelar Magister Komputer Pascasarjana Universitas Pendidikan Ganesha pada Program Studi Ilmu Komputer. terselesaikannya tesis ini telah banyak memperoleh uluran tangan dari berbagai pihak. Untuk itu, ijin penulis menyampaikan terima kasih dan penghargaan kepada pihak-pihak berikut.

1. Bapak Kadek Yota Ernanda Aryanto, S.Kom., M.T., Ph.D., sebagai pembimbing I yang telah dengan sabar membimbing, mengarahkan, dan memberikan motivasi yang demikian bermakna, sehingga penulis mampu melewati berbagai hambatan dalam perjalanan studi dan penyelesaian tesis ini;
2. Bapak Dr. I Gede Aris Gunadi, S.Si. M.Kom., sebagai pembimbing II, yang dengan gaya dan pola komunikasi yang khas, telah melecut semangat, motivasi, dan harapan penulis selama penelitian dan penulisan naskah laporan tesis ini, sehingga tesis ini dapat terwujud dengan baik sesuai harapan;
3. Kepala Unit IT yang telah memberikan izin kepada penulis untuk melakukan penelitian di Politeknik Kesehatan Kartini Bali;
4. Kepala Program Studi D4 Manajemen Informasi Kesehatan yang telah memberikan izin dan bantuan administratif sehingga penulis memperoleh kesempatan melanjutkan studi dan menyelesaikan tesis ini;
5. Koordinator Program Studi Ilmu Komputer dan staf dosen pengajar yang telah banyak membantu dan memotivasi penulis selama penyusunan tesis ini;
6. Direktur Pascasarjana Undiksha dan staf, yang telah banyak membantu selama penulis menyelesaikan tesis ini;
7. Rektor Universitas Pendidikan Ganesha, yang telah memberikan bantuan

secara moral dan memfasilitasi berbagai kepentingan penulis dalam menyelesaikan tesis ini;

8. Rekan-rekan seangkatan di Program Studi Ilmu Komputer yang dengan karakternya masing-masing telah banyak berkontribusi membentuk kedirian penulis selama menjalani studi dan penyelesaian tesis ini;
9. Bapak I Komang Parwanta dan Ibu Ni Nyoman Karini selaku orang tua penulis, keluarga besar penulis dan pasangan penulis yang telah banyak membantu secara material dan moral selama penyelesaian tesis ini.

Semoga semua bantuan yang telah mereka berikan dalam menyelesaikan studi ini, mereka diberkati imbalan yang sepadan oleh Tuhan Yang Maha Esa, kesehatan, dan keharmonian dalam menjalani kehidupan.

Penulis menyadari bahwa tesis ini belum sempurna. Namun, kehadirannya dalam konstelasi masyarakat akademis akan menambah perbendaharaan ilmu dalam perkembangan ilmu pengetahuan. Semoga tesis ini bermanfaat bagi masyarakat akademis, terutama mereka yang menyatakan diri bernaung di bawah kebesaran panji-panji pendidikan.

Singaraja, 8 Juli 2024

Penulis

## DAFTAR ISI

(Halaman)

TESIS .....	i
LEMBAR PERSETUJUAN .....	iii
LEMBAR PENGESAHAN .....	iv
LEMBAR PERNYATAAN.....	v
PRAKATA.....	vi
ABSTRAK.....	viii
ABSTRACT .....	ix
DAFTAR ISI .....	x
DAFTAR TABEL .....	xiii
DAFTAR GAMBAR .....	xiv
DAFTAR LAMPIRAN.....	xvi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah .....	1
1.2 Identifikasi Masalah.....	4
1.3 Batasan Masalah.....	4
1.4 Rumusan Masalah .....	5
1.5 Tujuan Penelitian .....	5
1.6 Manfaat Penelitian .....	6
1.7 Rencana Publikasi .....	6
BAB II KAJIAN PUSTAKA .....	8
2.1 <i>State of Art</i> .....	8
2.2 Kajian Teori.....	10
2.2.1 Jaringan komputer .....	10
2.2.2 Topologi jaringan komputer .....	11
2.2.3 <i>Client dan server</i> .....	11
2.2.4 Keamanan Jaringan Komputer .....	12
2.2.5 Aspek Keamanan Informasi.....	12
2.2.6 <i>Framework Streamlit</i> .....	13
2.2.7 <i>Support Vector Machine (SVM)</i> .....	13



2.2.8	<i>One-Class Support Vector Machine (OCSVM)</i> .....	14
2.2.9	<i>Intrusion Detection System</i> .....	15
2.2.11	Suricata.....	16
2.3	Kerangka Berpikir.....	16
BAB III METODE PENELITIAN.....		18
3.1	Tahapan Penelitian.....	18
3.2	Sumber dan Karakteristik Data .....	18
3.3	Metode Pengumpulan Data .....	20
3.4	Populasi dan Sampel Penelitian.....	22
3.5	Variabel Penelitian.....	23
3.6	Waktu dan Tempat Penelitian .....	23
3.7	Metode Pengembangan Sistem .....	24
3.7.1	Identifikasi .....	25
3.7.2	Analisis.....	25
3.7.3	Desain.....	27
3.7.4	Implementasi.....	30
3.7.5	Pengujian.....	30
3.7.6	Evaluasi .....	32
3.8	Pengambilan Data .....	32
3.9	Pengujian dan Evaluasi.....	33
3.10	Teknik Analisis Data.....	34
BAB IV HASIL PENELITIAN DAN PEMBAHASAN.....		36
4.1	Implementasi Sistem .....	36
4.1.1	Implementasi Topologi Jaringan .....	37
4.1.2	Implementasi dan Konfigurasi <i>Intrusion Detection System (IDS)</i> ..	39
4.1.3	Implementasi dan Konfigurasi <i>Framework Streamlit</i> .....	42
4.2	Pengujian Sistem.....	45
4.2.1	Skenario Pengujian <i>Intrusion Detection System (IDS)</i> Suricata ....	45
4.2.2	Pengujian <i>Intrusion Detection System (IDS)</i> Suricata .....	47
4.2.3	Hasil Pengujian <i>Intrusion Detection System (IDS)</i> Suricata .....	55
4.2.4	Skenario Pengujian Sistem <i>Live Analysis Framework Streamlit</i> ....	56

4.2.5	Pengujian Sistem <i>Live Analysis Framework Streamlit</i> .....	57
4.2.6	Hasil Pengujian Sistem <i>Live Analysis Framework Streamlit</i> .....	63
4.3	Analisis Dataset.....	64
4.4	Analisis dan Hasil Parsing Data dan <i>Preprocessing Dataset</i> .....	65
4.3.1	Analisis dan Hasil <i>Handling Outlier</i> .....	68
4.3.2	Analisis dan Hasil <i>Correlation</i> .....	69
4.5	Analisis dan Hasil Pengujian <i>One-Class Support Vector Machine</i> .....	70
4.4.1	Analisis dengan <i>One-Class Support Vector Machine</i> .....	71
4.4.2	Hasil Pengujian Model <i>One-Class Support Vector Machine</i> .....	72
4.4.3	Hasil Pengujian Model Deteksi <i>DDoS Attack</i> .....	76
4.4.4	Hasil Pengujian Model Deteksi <i>Brute Force Attack</i> .....	78
4.4.5	Hasil Pengujian Model Deteksi <i>Port Scanning</i> .....	80
4.6	Hasil Pengujian Akurasi Sistem.....	82
4.7	Hasil Rekomendasi Penggunaan <i>Hardware</i> dan <i>Software</i> .....	84
4.8	Hasil <i>Interface</i> Aplikasi <i>Live Analysis</i> .....	85
BAB V SIMPULAN DAN SARAN .....		88
5.1	Simpulan .....	88
5.2	Saran .....	89
DAFTAR PUSTAKA .....		91
LAMPIRAN .....		94

## DAFTAR TABEL

Tabel 3.1 Atribut Data File Log Eve.Json .....	19
Tabel 3.2 Atribut atau <i>Features</i> Data .....	21
Tabel 3.3 Variabel dalam Penelitian .....	23
Tabel 3.4 Pengujian Snort.....	27
Tabel 3.5 Spesifikasi Kebutuhan Sistem <i>Hardware</i> dan <i>Software</i> .....	29
Tabel 3.6 Pengujian Suricata .....	31
Tabel 4.1 Rubrik Pengujian <i>Intrusion Detection System (IDS)</i> Suricata.....	46
Tabel 4.2 Rubrik Pengujian Sistem <i>Live Analysis Framework Streamlit</i> .....	56
Tabel 4.3 Atribut Dataset.....	64
Tabel 4.4 Nilai Koefisien Korelasi.....	69
Tabel 4.5 Hasil <i>Hyperparameter Tuning</i> .....	71
Tabel 4.6 Hasil Pengujian Akurasi Sistem .....	82
Tabel 4.7 Rekomendasi Biaya Investasi <i>Hardware</i> .....	84
Tabel 4.8 Rekomendasi Penggunaan <i>Hardware</i> dan <i>Software</i> .....	85



## DAFTAR GAMBAR

Gambar 2.1 Klasifikasi SVM .....	14
Gambar 2.2 <i>One-Class Support Vector Machine (OCSVM)</i> .....	15
Gambar 2.3 Diagram Alir Kerangka Berpikir .....	17
Gambar 3.1 Struktur Data Format File Log Json .....	19
Gambar 3.2 Topologi Jaringan Komputer Poltekkes Kartini Bali .....	22
Gambar 3.3 Bagan Metode Pengembangan SPDLC.....	24
Gambar 3.4 Snort .....	25
Gambar 3.5 Percobaan Serangan di Poltekkes Kartini Bali .....	26
Gambar 3.6 Topologi Jaringan Komputer Politeknik Kesehatan Kartini Bali .....	28
Gambar 3.7 Alur Sistem Keamanan Jaringan Komputer.....	29
Gambar 3.8 Proses Pengambilan Data .....	33
Gambar 4.1 Alur Sistem Keamanan Jaringan Komputer Baru .....	36
Gambar 4.2 Alur Machine Learning Process .....	37
Gambar 4.3 Topologi Sistem Keamanan Jaringan Komputer Baru .....	38
Gambar 4.4 Tahap Awal Instalasi <i>Intrusion Detection System (IDS)</i> Suricata.....	39
Gambar 4.5 Tahap Awal Konfigurasi <i>Intrusion Detection System</i> Suricata.....	40
Gambar 4.6 Konfigurasi <i>Network Address</i> Suricata .....	40
Gambar 4.7 Konfigurasi <i>Output Log</i> Suricata.....	41
Gambar 4.8 Konfigurasi File Rules Suricata .....	41
Gambar 4.9 Instalasi Npcap.....	42
Gambar 4.10 Instalasi <i>Software Anaconda</i> .....	43
Gambar 4.11 Instalasi Streamlit .....	43
Gambar 4.12 Pengujian Instalasi Streamlit .....	44
Gambar 4.13 Tampilan Interface Demo Streamlit .....	44
Gambar 4.14 <i>Directory</i> Suricata.....	47
Gambar 4.15 Pengujian Fungsionalitas Suricata .....	48
Gambar 4.16 <i>Eve.json Log</i> Suricata.....	49
Gambar 4.17 Pengujian Port Scanning .....	50

Gambar 4.18 <i>Rules Suricata Port Scanning</i> .....	50
Gambar 4.19 <i>Log Port Scanning Suricata</i> .....	51
Gambar 4.20 Pengujian <i>Brute Force Attack</i> .....	52
Gambar 4.21 <i>Rules Suricata Brute Force Attack</i> .....	52
Gambar 4.22 <i>Log Brute Force Attack Suricata</i> .....	53
Gambar 4.23 Pengujian <i>Ddos Attack</i> .....	53
Gambar 4.24 <i>Rules Suricata Ddos Attack</i> .....	54
Gambar 4.25 <i>Log Ddos Attack Suricata</i> .....	55
Gambar 4.26 Halaman Utama Sistem <i>Live Analysis</i> .....	58
Gambar 4.27 Pengujian Halaman Login.....	58
Gambar 4.28 Halaman Monitoring Anomali.....	59
Gambar 4.29 Pengujian <i>Button Logout</i> .....	59
Gambar 4.30 Pengujian <i>Responsive</i> .....	60
Gambar 4.31 Penggunaan CPU dan Memory Halaman Login Sistem.....	61
Gambar 4.32 Penggunaan CPU dan Memory Halaman Utama Sistem.....	61
Gambar 4.33 <i>Tools Locust</i> .....	62
Gambar 4.34 <i>Locust Test Report</i> .....	62
Gambar 4.35 Kode Python untuk Proses Parsing Data.....	65
Gambar 4.36 Kode Python Preprocessing dan Pelabelan Data .....	66
Gambar 4.37 Perbandingan Jumlah Rekaman.....	67
Gambar 4.38 Hasil <i>Filter Data Outlier</i> .....	69
Gambar 4.39 Visualisasi <i>Correlation</i> .....	70
Gambar 4.40 Hasil <i>Confusion Matrix</i> .....	72
Gambar 4.41 Hasil <i>Confusion Matrix</i> Deteksi <i>DDos Attack</i> .....	77
Gambar 4.42 Hasil <i>Confusion Matrix</i> Deteksi <i>Brute Force Attack</i> .....	79
Gambar 4.43 Hasil <i>Confusion Matrix</i> Deteksi <i>Port Scanning</i> .....	81
Gambar 4.44 Halaman Login Sistem <i>Live Analysis</i> .....	86
Gambar 4.45 Halaman Home Sistem <i>Live Analysis</i> .....	86
Gambar 4.46 Halaman Anomali Detection.....	87

## DAFTAR LAMPIRAN

Lampiran 1. Format Data File Log eve.json .....	94
Lampiran 2. Sintaks Kode Parsing Data Json ke CSV .....	95
Lampiran 3. Sintaks Kode Grid Search Cross Validation .....	97
Lampiran 4. Sintaks Kode Pelatihan dan Pengujian Model .....	99
Lampiran 5. Sintaks Kode Evaluasi Model .....	101
Lampiran 6. Sintaks Kode Program Live Analysis .....	102

