

**DETEKSI ANOMALI (SERANGAN DDOS) PADA LALU LINTAS  
JARINGAN MENGGUNAKAN ALGORITMA ISOLATION FOREST DAN  
ONE-CLASS SVM**



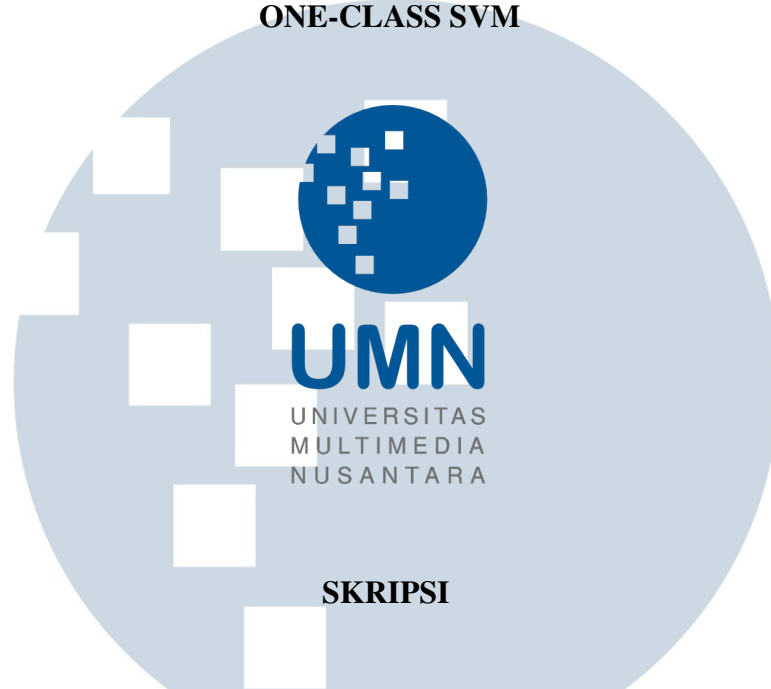
**SKRIPSI**

Diajukan sebagai salah satu syarat untuk memperoleh  
Gelar Sarjana Komputer (S.Kom.)

**Matthew**  
**00000045782**

**PROGRAM STUDI INFORMATIKA  
FAKULTAS TEKNIK DAN INFORMATIKA  
UNIVERSITAS MULTIMEDIA NUSANTARA  
TANGERANG  
2024**

**DETEKSI ANOMALI (SERANGAN DDOS) PADA LALU LINTAS  
JARINGAN MENGGUNAKAN ALGORITMA ISOLATION FOREST DAN  
ONE-CLASS SVM**



**SKRIPSI**

Diajukan sebagai salah satu syarat untuk memperoleh  
Gelar Sarjana Komputer (S.Kom.)

**Matthew  
00000045782**

**UMN**

**UNIVERSITAS  
MULTIMEDIA  
NUSANTARA**

**PROGRAM STUDI INFORMATIKA  
FAKULTAS TEKNIK DAN INFORMATIKA  
UNIVERSITAS MULTIMEDIA NUSANTARA**

**TANGERANG**

**2024**

## HALAMAN PERNYATAAN TIDAK PLAGIAT

Dengan ini saya,

Nama : Matthew  
NIM : 00000045782  
Program studi : Informatika

Menyatakan dengan sesungguhnya bahwa Skripsi saya yang berjudul:  
Deteksi Anomali (Serangan DDoS) pada Lalu Lintas Jaringan  
Menggunakan Algoritma Isolation Forest dan One-Class SVM

merupakan hasil karya saya sendiri, bukan merupakan hasil plagiat, dan tidak pula dituliskan oleh orang lain; Semua sumber, baik yang dikutip maupun dirujuk, telah saya cantumkan dan nyatakan dengan benar pada bagian Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan/penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan karya ilmiah, saya bersedia menerima konsekuensi untuk dinyatakan TIDAK LULUS. Saya juga bersedia menanggung segala konsekuensi hukum yang berkaitan dengan tindak plagiarisme ini sebagai kesalahan saya pribadi dan bukan tanggung jawab Universitas Multimedia Nusantara.

Tangerang, 22/05/2024



(Matthew)

UNIVERSITAS  
MULTIMEDIA  
NUSANTARA

HALAMAN PENGESAHAN

Skripsi dengan judul

**DETEKSI ANOMALI (SERANGAN DDOS) PADA LALU LINTAS  
JARINGAN MENGGUNAKAN ALGORITMA ISOLATION FOREST DAN  
ONE-CLASS SVM**

oleh

Nama : Matthew  
NIM : 00000045782  
Program Studi : Informatika  
Fakultas : Fakultas Teknik dan Informatika

Telah diujikan pada hari Kamis, 6 Juni 2024


Pukul 15.00 s/s 17.00 dan dinyatakan

LULUS

Dengan susunan penguji sebagai berikut

Ketua Sidang

Penguji

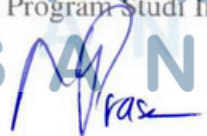
  
(Sy Yuliani Yakub, S.Kom., M.T. PhD)  
NIDN: 0411037904

  
(Yaman Khaeruzaman, M.Sc.)  
NIDN: 0413057104

Pembimbing

  
(Suwito Pomalingo, S.Kom., M.Kom.)  
NIDN: 0911098201

Ketua Program Studi Informatika,

  
(Dr. Eng. Niki Prastomo, S.T., M.Sc.)  
NIDN: 0419128203

## KATA PENGANTAR

Puji Syukur atas berkat dan rahmat kepada Tuhan Yang Maha Esa, atas selesainya penulisan laporan Skripsi ini dengan judul: Deteksi Anomali (Serangan DDoS) pada Lalu Lintas Jaringan Menggunakan Algoritma Isolation Forest dan One-Class SVM dilakukan untuk memenuhi salah satu syarat untuk mencapai gelar Sarjana Komputer Jurusan Informatika Pada Fakultas Teknik dan Informatika Universitas Multimedia Nusantara. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi saya untuk menyelesaikan skripsi ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

1. Bapak Dr. Ninok Leksono, selaku Rektor Universitas Multimedia Nusantara.
2. Bapak Dr. Eng. Niki Prastomo, S.T., M.Sc., selaku Dekan Fakultas Teknik dan Informatika Universitas Multimedia Nusantara.
3. Bapak Dr. Eng. Niki Prastomo, S.T., M.Sc., selaku Ketua Program Studi Informatika Universitas Multimedia Nusantara.
4. Bapak Suwito Pomalingo, S.Kom., M.Kom., sebagai Pembimbing pertama yang telah banyak meluangkan waktu untuk memberikan bimbingan, arahan dan motivasi atas terselesainya skripsi ini.
5. Orang Tua, keluarga, dan teman saya yang telah memberikan bantuan dukungan material dan moral, sehingga penulis dapat menyelesaikan skripsi ini.

Semoga skripsi ini bermanfaat, baik sebagai sumber informasi maupun sumber inspirasi, bagi para pembaca.

Tangerang, 22 Mei 2024

  
Matthew

**DETEKSI ANOMALI (SERANGAN DDOS) PADA LALU LINTAS  
JARINGAN MENGGUNAKAN ALGORITMA ISOLATION FOREST DAN  
ONE-CLASS SVM**

Matthew

**ABSTRAK**

Serangan DDoS merupakan ancaman serius dalam dunia siber yang dapat menyebabkan kerugian besar bagi organisasi dan infrastruktur sehingga terdapat berbagai pendekatan untuk menghindari serta mendeteksi serangan DDos seperti Deteksi Berbasis Tanda Tangan (Signature-Based Detection), Sistem *Intrusion Prevention System* (IPS), serta Pemodelan dan Pembelajaran Mesin. Dua algoritma yang sering digunakan untuk deteksi anomali adalah *Support Vector Machines* (SVM) dan *Isolation Forest*. Menggunakan dua algoritma tersebut, dilakukan pembangunan model untuk deteksi anomali dan dibandingkan. Pembangunan model menggunakan beberapa metode seperti *Synthetic Minority Over-sampling Technique* (SMOTE) dan *hyperparameter tuning* menggunakan *RandomizedSearchCV*. Hasil penelitian menunjukkan kinerja kedua model kurang efektif dalam menghadapi data yang kompleks.

**Kata kunci:** DDoS, *F1-Score*, *Hyperparameter tuning*, *Intrusion Prevention System*, *Isolation Forest*, *RandomizedSearchCV*, *Support Vector Machines*, *Synthetic Minority Over-sampling Technique*



## **Anomaly Detection (DDoS Attack) on Network Traffic Using the Isolation Forest and One-Class SVM Algorithm**

Matthew

### **ABSTRACT**

**Kata kunci:** DDoS, *F1-Score*, *Hyperparameter tuning*, *Intrusion Prevention System*, *Isolation Forest*, *RandomizedSearchCV*, *Support Vector Machines*, *Synthetic Minority Over-sampling Technique* DDoS attacks are a serious threat in the cyber world that can cause major losses to organizations and infrastructure so there are various approaches to avoid and detect DDoS attacks such as *Signature-Based Detection*, *Intrusion Prevention System (IPS)* , and *Modeling and Machine Learning*. Two algorithms that are often used for anomaly detection are *Support Vector Machines (SVM)* and *Isolation Forest*. Using these two algorithms, a model was built for anomaly detection and compared. Model construction uses several methods such as *Synthetic Minority Over-sampling Technique (SMOTE)* and *hyperparameter tuning using RandomizedSearchCV*. The research results show that the performance of the two models is less effective in dealing with complex data.

**Kata kunci:** DDoS, *F1-Score*, *Hyperparameter tuning*, *Intrusion Prevention System*, *Isolation Forest*, *RandomizedSearchCV*, *Support Vector Machines*, *Synthetic Minority Over-sampling Technique*

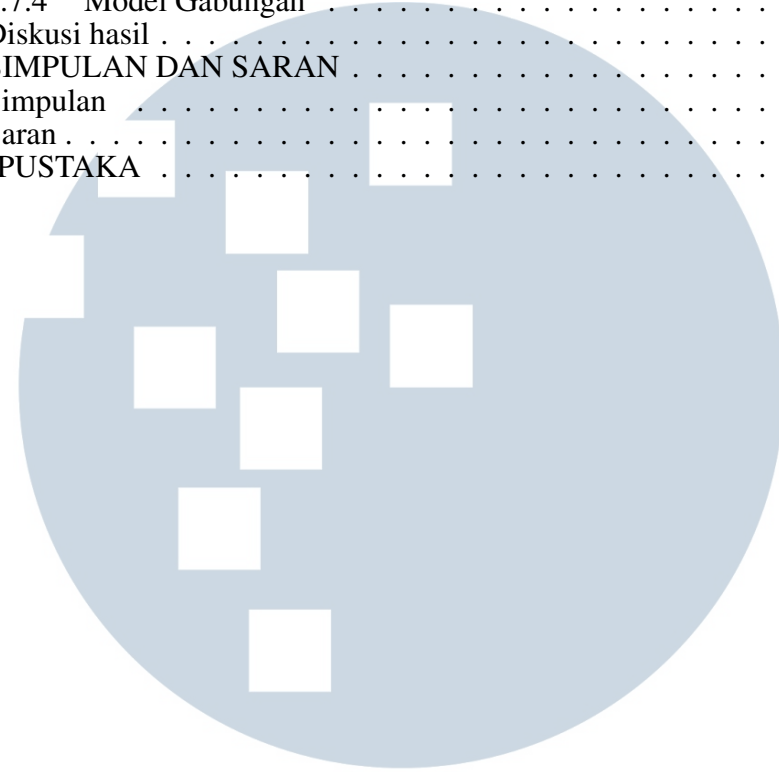


## DAFTAR ISI

HALAMAN JUDUL . . . . .	i
PERNYATAAN TIDAK MELAKUKAN PLAGIAT . . . . .	ii
HALAMAN PENGESAHAN . . . . .	iii
HALAMAN PERSETUJUAN PUBLIKASI ILMIAH . . . . .	iv
HALAMAN PERSEMBAHAN/MOTO . . . . .	v
KATA PENGANTAR . . . . .	vi
ABSTRAK . . . . .	vii
ABSTRACT . . . . .	viii
DAFTAR ISI . . . . .	ix
DAFTAR GAMBAR . . . . .	xi
DAFTAR TABEL . . . . .	xii
DAFTAR KODE . . . . .	xiii
DAFTAR LAMPIRAN . . . . .	xiv
BAB 1 PENDAHULUAN . . . . .	1
1.1 Latar Belakang Masalah . . . . .	1
1.2 Rumusan Masalah . . . . .	3
1.3 Batasan Permasalahan . . . . .	3
1.4 Tujuan Penelitian . . . . .	3
1.5 Manfaat Penelitian . . . . .	4
1.6 Sistematika Penulisan . . . . .	4
BAB 2 LANDASAN TEORI . . . . .	6
2.1 <i>Distributed Denial of Service (DDoS)</i> . . . . .	6
2.2 Anomali . . . . .	6
2.3 <i>Machine Learning</i> . . . . .	6
2.4 <i>Supervised vs Unsupervised Machine Learning</i> . . . . .	7
2.5 <i>Isolation Forest</i> . . . . .	7
2.6 <i>One-Class Support Vector Machine</i> . . . . .	7
2.7 <i>Confusion Matrix</i> . . . . .	8
BAB 3 METODOLOGI PENELITIAN . . . . .	10
3.1 Studi Literatur . . . . .	10
3.2 Pemilihan Dataset . . . . .	12
3.3 Visualisasi Data . . . . .	13
3.4 <i>Splitting Data</i> . . . . .	13
3.5 Implementasi Algoritma . . . . .	14
3.5.1 <i>Isolation Forest</i> . . . . .	14
3.5.2 <i>One-Class SVM</i> . . . . .	16
3.6 Pengujian dan Evaluasi Model . . . . .	16
BAB 4 HASIL DAN DISKUSI . . . . .	17
4.1 Spesifikasi Sistem . . . . .	17
4.2 Implementasi Sistem . . . . .	17
4.3 Persiapan Dataset . . . . .	18
4.4 Visualisasi Data . . . . .	20
4.5 <i>Splitting Data</i> . . . . .	22
4.6 Implementasi Algoritma . . . . .	22
4.6.1 <i>Isolation Forest</i> . . . . .	23
4.6.2 <i>One-Class SVM</i> . . . . .	26
4.7 Pengujian Model . . . . .	30
4.7.1 Model Awal . . . . .	31



4.7.2	Model Setelah <i>Balancing Data</i> . . . . .	33
4.7.3	Model Setelah <i>Hyperparameter Tuning</i> . . . . .	35
4.7.4	Model Gabungan . . . . .	37
4.8	Diskusi hasil . . . . .	39
BAB 5	SIMPULAN DAN SARAN . . . . .	41
5.1	Simpulan . . . . .	41
5.2	Saran . . . . .	42
DAFTAR PUSTAKA	. . . . .	43



UMMN  
 UNIVERSITAS  
 MULTIMEDIA  
 NUSANTARA

## DAFTAR GAMBAR

Gambar 3.1	Bagan Metodologi Penelitian . . . . .	10
Gambar 3.2	Topologi Jaringan . . . . .	12
Gambar 3.3	Proses implementasi SMOTE . . . . .	14
Gambar 3.4	Proses implementasi <i>RandomizedSearchCV</i> . . . . .	15
Gambar 4.1	Proses persiapan dataset . . . . .	18
Gambar 4.2	<i>Output function data.info()</i> . . . . .	18
Gambar 4.3	Bentuk data awal dan data yang sudah dibersihkan . . . . .	20
Gambar 4.4	Diagram batang isi dataset . . . . .	21
Gambar 4.5	Jumlah row dan kolom data . . . . .	22
Gambar 4.6	<i>Output SMOTE</i> . . . . .	24
Gambar 4.7	Parameter yang dihasilkan dari proses <i>hyperparameter tuning Isolation Forest</i> . . . . .	25
Gambar 4.8	Ukuran sampel data . . . . .	26
Gambar 4.9	<i>Output SMOTE OCSVM</i> . . . . .	28
Gambar 4.10	Parameter yang dihasilkan dari proses <i>hyperparameter tuning algoritma OCSVM</i> . . . . .	30
Gambar 4.11	<i>Confusion matrix</i> algoritma tanpa <i>balancing data</i> dan <i>hyperparameter tuning</i> . . . . .	33
Gambar 4.12	<i>Confusion matrix</i> algoritma setelah SMOTE . . . . .	35
Gambar 4.13	<i>Confusion matrix</i> algoritma setelah <i>hyperparameter tuning</i> . . . . .	37
Gambar 4.14	<i>Confusion matrix</i> algoritma setelah <i>balancing data</i> dan <i>hyperparameter tuning</i> . . . . .	39



## DAFTAR TABEL

Tabel 2.1	Tabel Confusion Matrix . . . . .	8
Tabel 3.1	Tabel Studi Literatur . . . . .	11
Tabel 4.1	Tabel <i>Output data.head()</i> . . . . .	19
Tabel 4.2	Tabel <i>Output print(missing_values)</i> . . . . .	20
Tabel 4.3	Tabel perbandingan algoritma tanpa <i>balancing data</i> dan <i>hyperparameter tuning</i> . . . . .	32
Tabel 4.4	Tabel perbandingan algoritma setelah SMOTE . . . . .	34
Tabel 4.5	Tabel perbandingan algoritma setelah <i>hyperparameter</i> <i>tuning</i> . . . . .	36
Tabel 4.6	Tabel perbandingan algoritma setelah <i>balancing data</i> dan <i>hyperparameter tuning</i> . . . . .	38
Tabel 4.7	Tabel <i>F1-Score</i> . . . . .	40
Tabel 5.1	Tabel Hasil Model <i>Isolation Forest</i> . . . . .	41
Tabel 5.2	Tabel Hasil Model <i>One-Class SVM</i> . . . . .	42



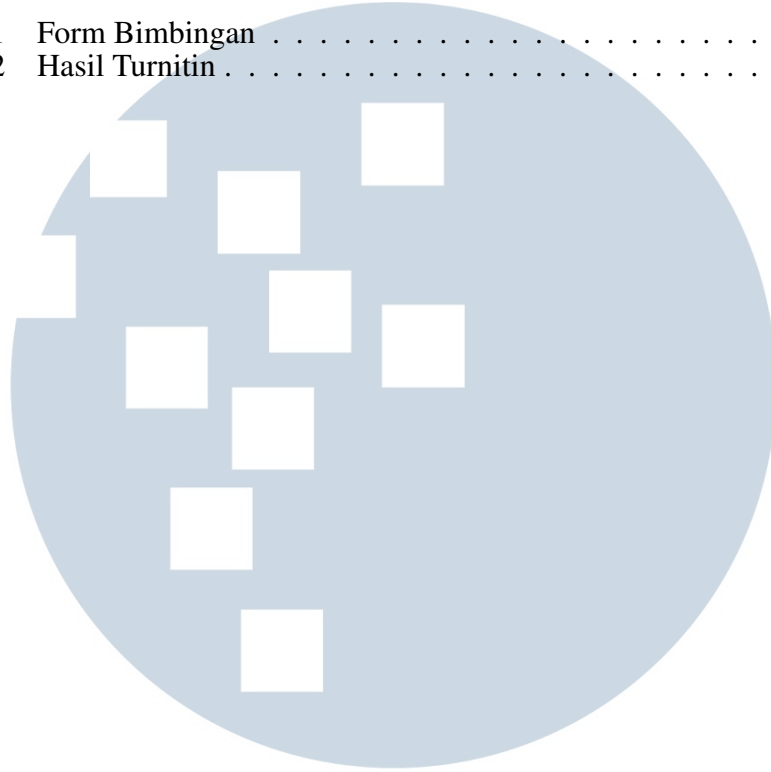
## DAFTAR KODE

4.1	Script Persiapan Dataset	18
4.2	<i>Script</i> penghapusan kolom index	19
4.3	<i>Script cleaning data</i>	19
4.4	<i>Script</i> visualisasi data	20
4.5	<i>Script</i> visualisasi data	21
4.6	<i>Script splitting data</i>	22
4.7	<i>Script</i> model <i>Isolation Forest</i>	23
4.8	<i>Script</i> implementasi SMOTE	23
4.9	<i>Script</i> model <i>Isolation Forest</i> setelah SMOTE	24
4.10	<i>Script hyperparameter tuning Isolation Forest</i>	24
4.11	<i>Script</i> pembuatan model <i>Isolation Forest</i> setelah <i>tuning</i>	25
4.12	<i>Script</i> pelatihan model <i>Isolation Forest</i> gabungan	26
4.13	<i>Script</i> pengambil sampel data	26
4.14	<i>Script</i> pembagian data untuk OCSVM	27
4.15	<i>Script</i> pelatihan model OCSVM	27
4.16	<i>Script balancing sample data</i>	27
4.17	<i>Script</i> pelatihan model OCSVM setelah <i>balancing sample data</i>	28
4.18	<i>Script hyperparameter tuning</i> untuk model OCSVM	29
4.19	<i>Script</i> pembuatan model OCSVM setelah <i>tuning</i>	29
4.20	<i>Script</i> pelatihan model OCSVM gabungan	30
4.21	<i>Script</i> pengujian model	30
4.22	<i>Script confusion matrix</i>	31

UMN  
UNIVERSITAS  
MULTIMEDIA  
NUSANTARA

## DAFTAR LAMPIRAN

Lampiran 1	Form Bimbingan . . . . .	46
Lampiran 2	Hasil Turnitin . . . . .	47



**UMMN**  
UNIVERSITAS  
MULTIMEDIA  
NUSANTARA