

**Klasifikasi Serangan DDoS Menggunakan Metode Hybrid  
Penggabungan *Support Vector Machine* (SVM) dengan *Gaussian  
Naive Bayes***

**Laporan Tugas Akhir**

Diajukan Untuk Memenuhi  
Persyaratan Guna Meraih Gelar Sarjana  
Informatika Universitas Muhammadiyah Malang



MUHAMAD RIZQI ZUL ATSARI

201710370311267

**Bidang Minat**

Jaringan

**PROGRAM STUDI INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS MUHAMMADIYAH MALANG  
2023**

## LEMBAR PERSETUJUAN

### **Klasifikasi Serangan DDoS Menggunakan Metode Hybrid Penggabungan Support Vector Machine (SVM) dengan Gaussian Naive Bayes**

#### **TUGAS AKHIR**

**Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1  
Informatika Universitas Muhammadiyah Malang**

Menyetujui,

Malang, *1 November 2023*

Dosen Pembimbing 1

Dosen Pembimbing 2



**Zamah Sari ST., MT.**  
NIP. 10814100555PNS.

**Didih Rizki Chandranegara S.kom.,**  
**M.Kom**  
NIP. 180302101992PNS.

## LEMBAR PENGESAHAN

**Klasifikasi Serangan DDoS Menggunakan Metode Hybrid  
Penggabungan Support Vector Machine (SVM) dengan Gaussian  
Naive Bayes**

### TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1  
Informatika Universitas Muhammadiyah Malang

Disusun Oleh :

**Muhamad Rizqi Zul Atsari**

**201710370311267**

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji  
pada tanggal 1 November 2023

Menyetujui,

Dosen Penguji 1



Christian Sri Kusuma Aditya S.Kom.,

M.Kom

NIP. 180327021991PNS.

Dosen Penguji 2



Harivady S.Kom, MT.

NIP. 10816120588PNS.

Mengetahui,  
Ketua Jurusan Informatika



Ir. Galih Wasis Wicaksono S.kom. M.Cs.

NIP. 10814100541PNS.

## LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

**NAMA** : **Muhamad Rizqi Zul Atsari**

**NIM** : **201710370311267**

**FAK./JUR.** : **Informatika**

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul **“Klasifikasi Serangan DDoS Menggunakan Metode Hybrid Penggabungan Support Vector Machine (SVM) dengan Gaussian Naive Bayes”** beserta seluruh isinya adalah karya saya sendiri dan bukan merupakan karya tulis orang lain, baik sebagian maupun seluruhnya, kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini, atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka saya siap menanggung segala bentuk resiko/sanksi yang berlaku.

Mengetahui,  
Dosen Pembimbing



Zamah Sari ST., MT.

Malang, 1 November 2023  
Yang Membuat Pernyataan



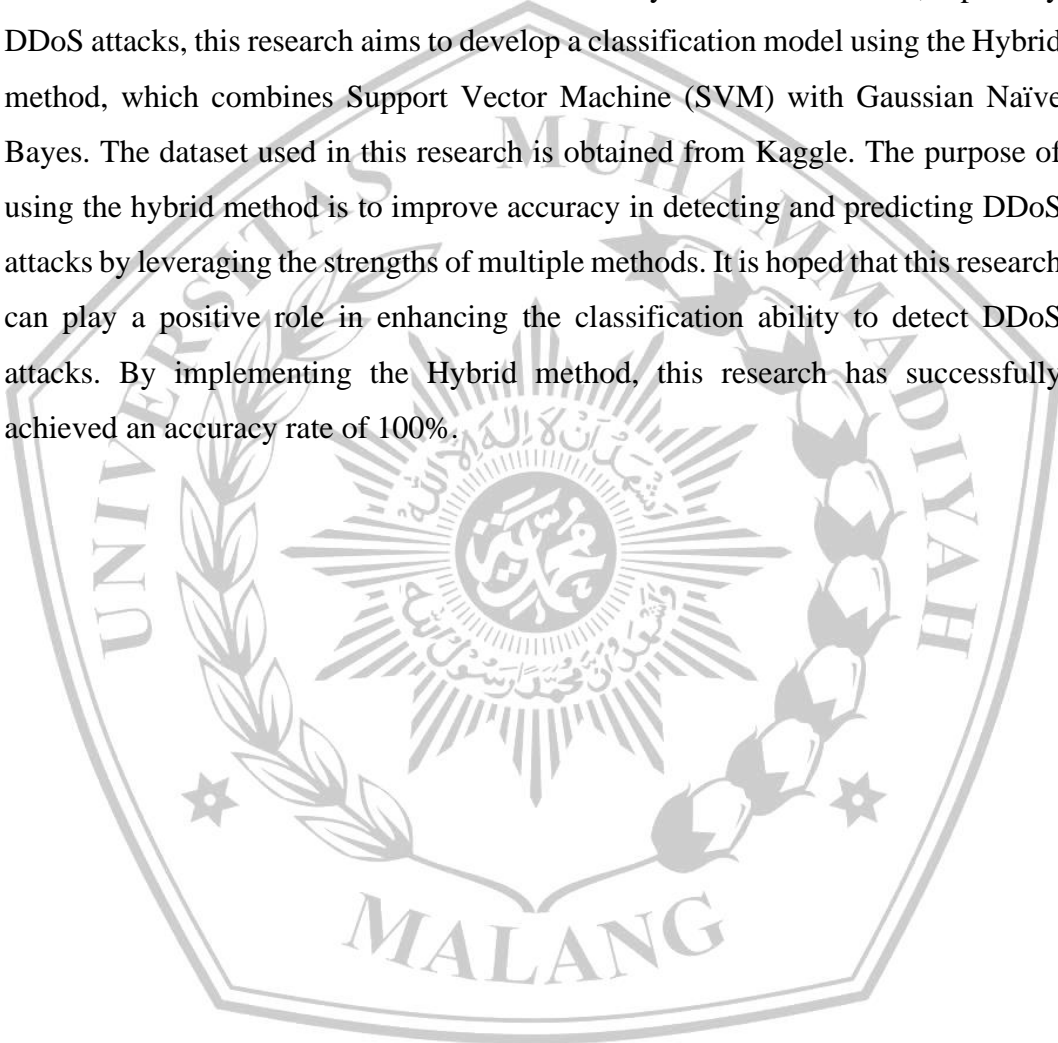
Muhamad Rizqi Zul Atsari

## ABSTRAK

Dengan semakin berkembangnya ketergantungan masyarakat terhadap sistem komputer, keamanan internet menjadi sangat penting. Salah satu ancaman utama yang sering terjadi adalah serangan DDoS (Distributed Denial of Service). Penelitian sebelumnya telah menunjukkan bahwa serangan ini dapat merusak infrastruktur internet dengan cara membanjiri server atau jaringan target dengan lalu lintas internet palsu. Dalam upaya meningkatkan deteksi serangan cyber terutama serangan DDoS, penelitian ini bertujuan untuk mengembangkan sebuah model klasifikasi menggunakan metode Hybrid penggabungan Support Vector Machine (SVM) dengan Gaussian Naïve Bayes. Dataset yang digunakan dalam penelitian ini berasal dari Kaggle. Tujuan penggunaan metode hybrid adalah untuk meningkatkan akurasi dalam mendeteksi dan memprediksi serangan DdoS dengan menggabungkan keunggulan dari beberapa metode. Harapannya, penelitian ini dapat berperan positif dalam meningkatkan kemampuan klasifikasi untuk mendeteksi serangan DDoS. Dengan mengimplementasikan metode Hybrid, hasil penelitian ini berhasil mencapai tingkat akurasi sebesar 100%.

## ABSTRACT

With the increasing dependence of society on computer systems, internet security has become crucial. One of the major threats that often occurs is DDoS (Distributed Denial of Service) attacks. Previous research has shown that these attacks can disrupt internet infrastructure by flooding the target server or network with fake internet traffic. In an effort to enhance cyber attack detection, especially DDoS attacks, this research aims to develop a classification model using the Hybrid method, which combines Support Vector Machine (SVM) with Gaussian Naïve Bayes. The dataset used in this research is obtained from Kaggle. The purpose of using the hybrid method is to improve accuracy in detecting and predicting DDoS attacks by leveraging the strengths of multiple methods. It is hoped that this research can play a positive role in enhancing the classification ability to detect DDoS attacks. By implementing the Hybrid method, this research has successfully achieved an accuracy rate of 100%.



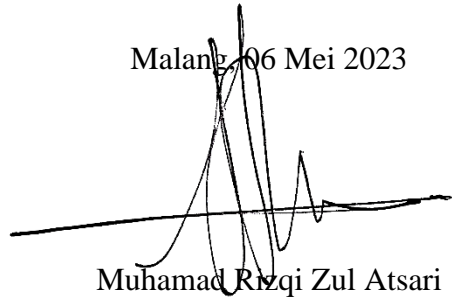
## LEMBAR PERSEMBAHAN

Puji syukur kepada Allah SWT atas rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini. Penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Kedua orangtua, adik beserta keluarga saya yang selalu memberikan do'a dan support sehingga saya dapat menyelesaikan tugas akhir ini sampai selesai.
2. Bapak Zamah Sari, ST., MT. selaku dosen pembimbing I yang telah memberikan bimbingan, arahan, serta saran kepada penulis dalam penelitian tugas akhir.
3. Bapak Didih Rizki Chandranegara, S.Kom., M.Kom. selaku dosen pembimbing II yang telah memberikan bimbingan, arahan, serta saran kepada penulis dalam penelitian tugas akhir.
4. Bapak Drs. H. Fauzan, M.Pd selaku Rektor Universitas Muhammadiyah Malang.
5. Bapak Dr. Ahmad Mubin, S.T., M.T. selaku Dekan Fakultas Teknik Universitas Muhammadiyah Malang.
6. Ibu Gita Indah Marthasari, S.T., M.Kom. selaku Ketua Program Studi Teknik Informatika Universitas Muhammadiyah Malang.
7. Teman-teman seperjuangan yang telah menemani proses belajar dalam perkuliahan serta selalu memberikan dukungan, motivasi dan saran kepada penulis. Terkhusus untuk : M. Fauzi Rais, M. Fikri Azhar, Denny Risky, Andre yang selalu mau direpotkan agar tugas akhir ini bisa selesai.
8. Anas Misbahul Ulum dan Okky Teguh prakoso selaku sahabat serta keluarga ke dua saya yang selalu memberikan semangat dan dukungan dan menemani saya dalam pengerjaan tugas akhir.

Akhir kata penulis mengucapkan rasa hormat dan terima kasih bagi semua pihak atas segala dukungan dan do'anya semoga Allah SWT membalas semua kebaikan yang telah mereka berikan kepada penulis, Aamiin.

Malang, 06 Mei 2023



Muhamad Rizqi Zul Atsari





## KATA PENGANTAR

Dengan memanjatkan puji dan syukur atas kehadiran Allah SWT, karena berkat Rahmat dan hidayah-Nya penyusunan tugas akhir yang berjudul:

**“Klasifikasi Serangan DDoS Menggunakan Metode Hybrid Penggabungan  
*Support Vector Machine (SVM) dengan Gaussian Naive Bayes*”**

Didalam penulisan ini dipaparkan beberapa pokok bahasan meliputi bahasan tentang konsep DDOS, Algoritma Support Vector Machine (SVM), Gaussian Naive Bayes, selain itu juga menjelaskan tentang klasifikasi penggunaan algoritma SVM, Gaussian Naive Bayes serta metode hybrid penggabungan metode SVM dengan Gaussian Naive Bayes untuk mengklasifikasikan serangan DDOS pada dataset yang telah tersedia.

Penulis menyadari bahwa tugas akhir ini masih jauh dari kata sempurna. Oleh sebab itu, penulis berharap dapat belajar lebih banyak lagi dalam implementasikan ilmu yang didapatkan dan mengharapkan saran maupun masukan yang membangun agar tulisan ini dapat bermanfaat bagi kita semua.

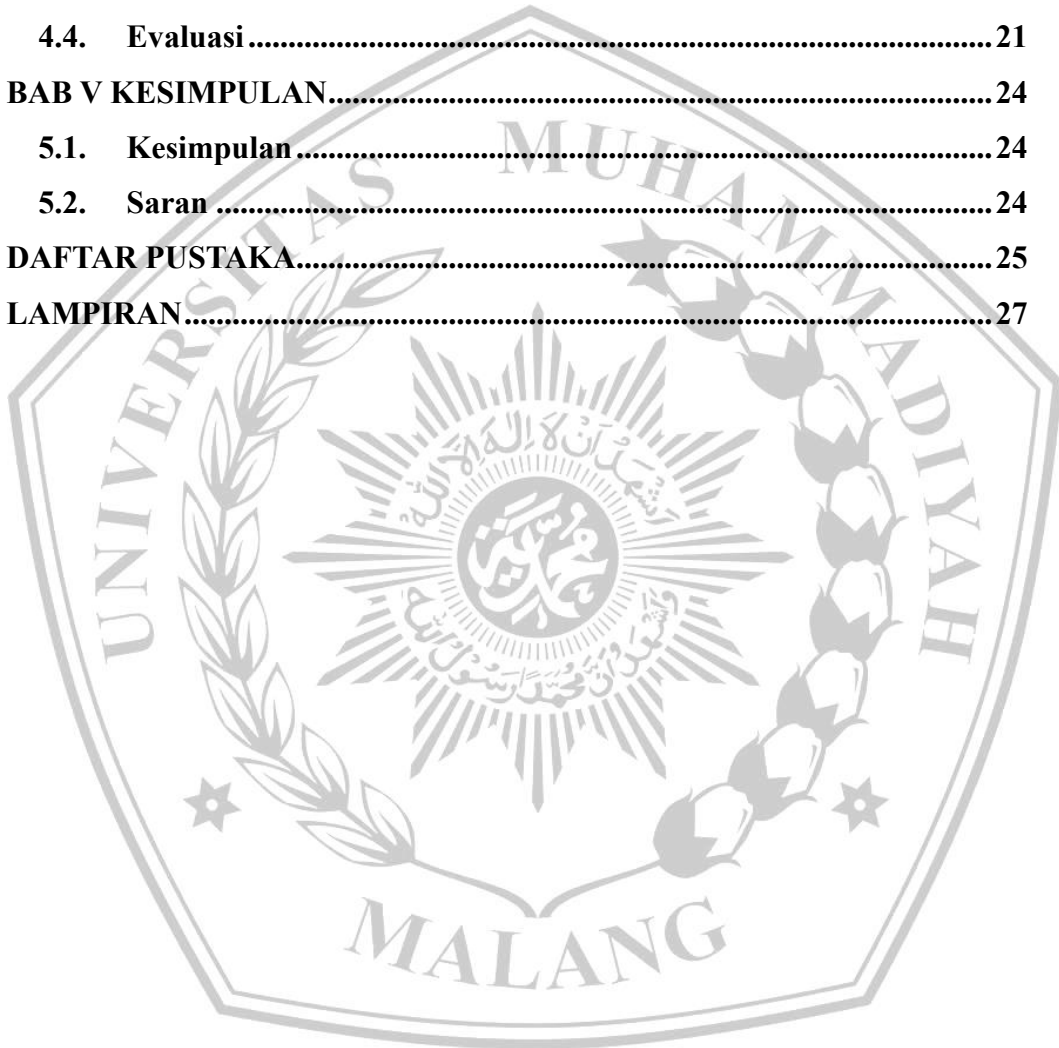
Malang, 06 Mei 2023

  
Muhamad Rizqi Zul Atsari

## DAFTAR ISI

LEMBAR PERSETUJUAN .....	ii
LEMBAR PENGESAHAN .....	iii
LEMBAR PERNYATAAN .....	iv
ABSTRAK .....	v
ABSTRACT .....	vi
LEMBAR PERSEMBAHAN .....	vii
KATA PENGANTAR.....	ix
DAFTAR ISI.....	x
DAFTAR GAMBAR .....	xii
DAFTAR TABEL .....	xiii
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah.....	3
1.3. Tujuan Penelitian .....	3
1.4. Batasan Masalah .....	4
BAB II TINJAUAN PUSTAKA.....	5
2.1. Penelitian Terdahulu.....	5
2.2. Dasar Teori.....	6
2.2.1 Data Mining .....	6
2.2.2 Information Gain .....	6
2.2.3 Standar Scaler .....	8
2.2.4 Support Vector Machine (SVM) .....	8
2.2.5 Gaussian Naïve Bayes .....	8
2.2.6 MetodeHybrid .....	10
BAB III METODOLOGI PENELITIAN .....	12
3.1. Alur Penelitian.....	12
3.2. Dataset.....	13
3.3. Preprocessing Data.....	13
3.4. Data Splitting.....	14
3.5. Building Model SVM .....	14
3.6. Building Model Gaussian Naïve Bayes.....	14

3.7. Building Model Hybrid.....	15
3.8. Uji Deteksi.....	15
3.9. Skenario Pengujian .....	16
<b>BAB IV HASIL DAN PEMBAHASAN.....</b>	<b>18</b>
4.1. Import Dataset.....	18
4.2. Preprocessing Data.....	19
4.3. Pembentukan Model .....	21
4.4. Evaluasi.....	21
<b>BAB V KESIMPULAN.....</b>	<b>24</b>
5.1. Kesimpulan.....	24
5.2. Saran .....	24
<b>DAFTAR PUSTAKA.....</b>	<b>25</b>
<b>LAMPIRAN.....</b>	<b>27</b>



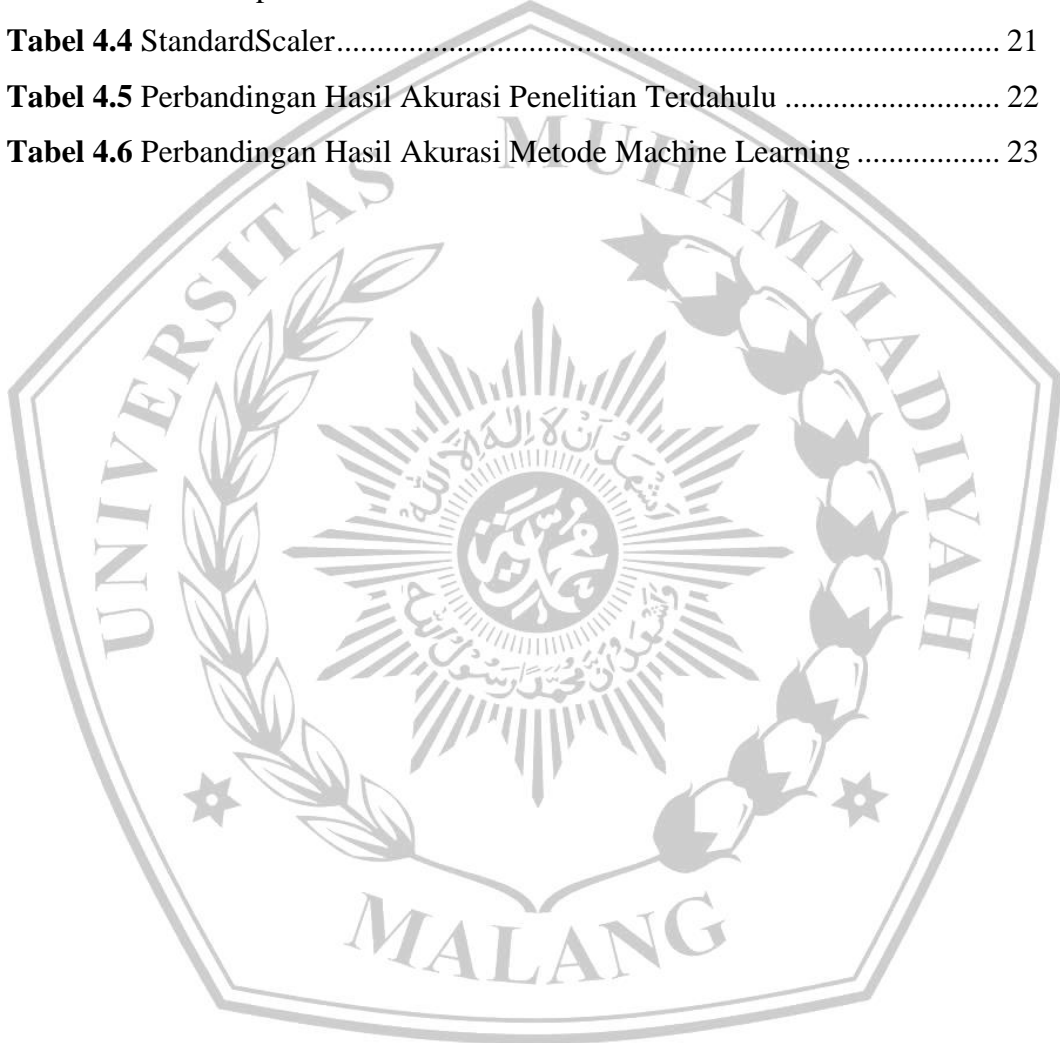
## DAFTAR GAMBAR

<b>Gambar 3.1</b> Alur Penelitian .....	12
<b>Gambar 3.2</b> Sampel Dataset .....	13
<b>Gambar 4.1</b> Classification Report metode hybrid .....	22



## DAFTAR TABEL

<b>Tabel 2.1</b> Information Gain .....	7
<b>Tabel 3.1</b> Jenis Data .....	13
<b>Tabel 4.1</b> Import Dataset .....	18
<b>Tabel 4.2</b> Label Encoder.....	19
<b>Tabel 4.3</b> Oversample.....	20
<b>Tabel 4.4</b> StandardScaler.....	21
<b>Tabel 4.5</b> Perbandingan Hasil Akurasi Penelitian Terdahulu .....	22
<b>Tabel 4.6</b> Perbandingan Hasil Akurasi Metode Machine Learning .....	23



## DAFTAR PUSTAKA

- [1] Kurniabudi, K., Harris, A., & Rahim, A. (2020). Seleksi Fitur Dengan Information Gain Untuk Meningkatkan Deteksi Serangan DDoS menggunakan Random Forest. *Techno.Com*, 19(1), 56–66. <https://doi.org/10.33633/tc.v19i1.2860>
- [2] Riadi, I., Umar, R., & Aini, F. D. (2019). Analisis Perbandingan Detection Traffic Anomaly Dengan Metode Naive Bayes Dan Support Vector Machine (Svm). *ILKOM Jurnal Ilmiah*, 11(1), 17–24. <https://doi.org/10.33096/ilkom.v11i1.361.17-24>
- [3] <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>
- [4] <https://inet.detik.com/security/d-4656851/serangan-ddos-meningkat-hingga-18-dibandingkan-tahun-lalu>
- [5] Netscout. (2019). NETSCOUT's 14th Annual Worldwide Infrastructure Security Report. *Netscout*, 69. <https://www.netscout.com/press-releases/netscout-releases-14th-annual-worldwide-infrastructure--->
- [6] [https://www.kominfo.go.id/index.php/content/detail/14959/indonesia-negara-ketiga-paling-sering-terkena-serangan-siber/0/sorotan\\_media](https://www.kominfo.go.id/index.php/content/detail/14959/indonesia-negara-ketiga-paling-sering-terkena-serangan-siber/0/sorotan_media)
- [7] Chris, J., Sihombing, J., Kartikasari, D. P., & Bhawiyuga, A. (2019). Implementasi Sistem Deteksi dan Mitigasi Serangan Distributed Denial of Service ( DDoS ) menggunakan SVM Classifier pada Arsitektur Software-Defined Network ( SDN ). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, 3(10), 9608–9613.
- [8] Zidane, M. (2021). KLASIFIKASI SERANGAN DISTRIBUTED DENIAL-OF-SERVICE ( DDOS ) MENGGUNAKAN METODE DATA MINING NAÏVE BAYES memperoleh gelar Sarjana Komputer Disusun oleh : *Universitas Brawijaya*, 6(1), 63.
- [9] Ridho, M. A., & Arman, M. (2020). Analisis Serangan DDoS Menggunakan Metode Jaringan Saraf Tiruan. *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, 9(3), 373–379. <https://doi.org/10.32736/sisfokom.v9i3.945>
- [10] Li, D., Yu, C., Zhou, Q., & Yu, J. (2018). Using SVM to Detect DDoS Attack in SDN Network. *IOP Conference Series: Materials Science and Engineering*, 466(1). <https://doi.org/10.1088/1757-899X/466/1/012003>

- [11] M. Sholeh, E. K. Nurnawati, and U. Lestari, "Penerapan Data Mining dengan Metode Regresi Linear untuk Memprediksi Data Nilai Hasil Ujian Menggunakan RapidMiner," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 8, no. 1, pp. 10–21, 2023, doi: 10.14421/jiska.2023.8.1.10-21.
- [12] <https://www.digitalocean.com/community/tutorials/standardscaler-function-in-python>
- [13] Reynaldhi, M. A. R., & Sibaroni, Y. (2021). Analisis Sentimen Review Film pada Twitter menggunakan Metode Klasifikasi Hybrid Naïve Bayes dan Decision Tree. *E-Proceeding of Engineering*, 8(5), 10127–10137.
- [14] Harto, M. K., & Basuki, A. (2021). *Deteksi Serangan DDoS Pada Jaringan Berbasis SDN Dengan Klasifikasi Random Forest*. 5(4), 1329–1333.
- [15] Sugianti, N., Galuh, Y., Fatia, S., & Holle, K. F. H. (2020). Deteksi Serangan Distributed Denial of Services (DDoS) Berbasis HTTP Menggunakan Metode Fuzzy Sugeno. *JISKA (Jurnal Informatika Sunan Kalijaga)*, 4(3), 18. <https://doi.org/10.14421/jiska.2020.43-03>
- [16] Risyad, E., Data, M., & Pramukantoro, E. S. (2018). Perbandingan Performa Intrusion Detection System (IDS) Snort Dan Suricata Dalam Mendeteksi Serangan TCP SYN Flood. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, 2(9), 2615–2624.
- [17] [learningbox.coffeecup.com](http://learningbox.coffeecup.com). (2018, 28 Juli). Algoritma Random Forest. Diakses pada 20 November 2022, dari [http://learningbox.coffeecup.com/05\\_2\\_randomforest.html](http://learningbox.coffeecup.com/05_2_randomforest.html)
- [18] Azhar, M. F. (2022). *LOW RATE ATTACK DETECTION ON SD-WSN USING SVM*.
- [19] Al Azhima, S. A. T., Darmawan, D., Arief Hakim, N. F., Kustiawan, I., Al Qibtiya, M., & Syafei, N. S. (2022). Hybrid Machine Learning Model untuk memprediksi Penyakit Jantung dengan Metode Logistic Regression dan Random Forest. *Jurnal Teknologi Terpadu*, 8(1), 40–46. <https://doi.org/10.54914/jtt.v8i1.539>
- [20] <https://www.projectpro.io/article/predictive-modelling-techniques/598>

# LAMPIRAN



UNIVERSITAS  
MUHAMMADIYAH  
MALANG



## FAKULTAS TEKNIK

### INFORMATIKA

informatika.umm.ac.id | informatika@umm.ac.id

### FORM CEK PLAGIARISME LAPORAN TUGAS AKHIR

Nama Mahasiswa : Muhamad Rizqi Zul Atsari  
NIM : 201710370311267  
Judul TA : Klasifikasi Serangan DDoS Menggunakan Metode Hybrid  
Penggabungan Support Vector Machine (SVM) dengan Gaussian  
Naïve Bayes

#### Hasil Cek Plagiarisme dengan Turnitin

No.	Komponen Pengecekan	Nilai Maksimal Plagiarisme (%)	Hasil Cek Plagiarisme (%) *
1.	Bab 1 – Pendahuluan	10 %	9 %
2.	Bab 2 – Daftar Pustaka	25 %	20 %
3.	Bab 3 – Analisis dan Perancangan	25 %	14 %
4.	Bab 4 – Implementasi dan Pengujian	15 %	10%
5.	Bab 5 – Kesimpulan dan Saran	5 %	0 %
6.	Makalah Tugas Akhir	20%	15 %

\*) Hasil cek plagiarism diisi oleh pemeriksa (staf TU)

\*) Maksimal 5 kali (4 Kali sebelum ujian, 1 kali sesudah ujian)

Mengetahui,

Pemeriksa (Staff TU)

(.....)



Kampus I  
Jl. Blandung 1 Malang Jawa Timur  
P. +62 341 551 253 (Hunting)  
F. +62 341 460 435

Kampus II  
Jl. Bendungan Sulam No 100 Malang, Jawa Timur  
P. +62 341 551 140 (Hunting)  
F. +62 341 582 080

Kampus III  
Jl. Raya Tlogomas No 246 Malang, Jawa Timur  
P. +62 341 464 318 (Hunting)  
F. +62 341 460 435  
E. webmaster@umm.ac.id