# ALGORITMA KLASIFIKASI SUPPORT VECTOR MACHINE DALAM MENDETEKSI SERANGAN DDOS PADA TRAFFIC JARINGAN

**SKRIPSI NON REGULER - SCIENTIST**

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer


disusun oleh

**YOKI IRAWAN**

**21.83.0665**


Kepada


**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS AMIKOM YOGYAKARTA**

**YOGYAKARTA**


**2025**

# ALGORITMA KLASIFIKASI SUPPORT VECTOR MACHINE DALAM MENDETEKSI SERANGAN DDOS PADA TRAFFIC JARINGAN

**SKRIPSI NON REGULER - SCIENTIST**

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer


disusun oleh

**YOKI IRAWAN**

**21.83.0665**


Kepada


**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS AMIKOM YOGYAKARTA**

**YOGYAKARTA**


**2025**

## HALAMAN PERSETUJUAN

**SKRIPSI NON REGULER – SCIENTIST**

**ALGORITMA KLASIFIKASI SUPPORT VECTOR MACHINE DALAM MENDETEKSI SERANGAN DDOS PADA TRAFFIC JARINGAN**

yang disusun dan diajukan oleh

**YOKI IRAWAN**

**21.83.0665**

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 11 Agustus 2025

**Dosen Pembimbing,**

**Rina Pramitasari, S.Si., M.Cs.**
**NIK. 190302335**

**HALAMAN PENGESAHAN**

**SKRIPSI NON REGULER - SCIENTIST**

**ALGORITMA KLASIFIKASI SUPPORT VECTOR MACHINE DALAM MENDETEKSI SERANGAN DDOS PADA TRAFFIC JARINGAN**

yang disusun dan diajukan oleh

**Yoki Irawan**

**21.83.0665**

Telah dipertahankan di depan Dewan Penguji
pada tanggal 11 Agustus 2025

**Susunan Dewan Penguji**

| Nama Penguji | Tanda Tangan |
|---|---|
| **Senie Destya, S.T., M.Kom.**<br>**NIK. 190302312** | |
| **Melwin Syafrizal, S.Kom., M.Eng., Ph.D.**<br>**NIK. 190302105** | |
| **Jeki Kuswanto, S.Kom., M.Kom.**<br>**NIK. 190302456** | |

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 11 Agustus 2025

**DEKAN FAKULTAS ILMU KOMPUTER**

**Prof. Dr. Kusrini, M.Kom.**
**NIK. 190302106**

## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

**Nama mahasiswa : Yoki Irawan**
**NIM : 21.83.0665**

Menyatakan bahwa Skripsi dengan judul berikut:

**Algoritma Klasifikasi Support Vector Machine Dalam Mendeteksi Serangan Ddos Pada Traffic Jaringan**

Dosen Pembimbing : Rina Pramitasari, S.Si., M.Cs.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 11 Agustus 2025

Yang Menyatakan,


Yoki Irawan

## HALAMAN PERSEMBAHAN

Dengan penuh rasa syukur ke hadirat Allah Subhanahu wa Ta'ala atas limpahan rahmat, karunia, serta kekuatan yang telah diberikan selama proses penulisan skripsi ini, izinkan penulis mempersembahkan karya sederhana ini kepada:

- Kedua orang tua tercinta, yang senantiasa menjadi sumber semangat dalam setiap langkah perjalanan penulis. Terima kasih atas kasih sayang, kesabaran, doa yang tiada henti, serta dukungan moral maupun materiil yang telah mengiringi setiap proses yang penulis jalani. Tanpa kalian, pencapaian ini tidak akan mungkin terwujud.
- Keluarga besar, yang selalu memberikan semangat, kepercayaan, dan doa terbaiknya. Kehadiran kalian menjadi motivasi tersendiri bagi penulis untuk terus melangkah maju dan menyelesaikan tanggung jawab akademik ini hingga tuntas.
- Rekan-rekan seperjuangan dan sahabat terbaik, yang telah memberikan warna dalam setiap perjalanan selama masa kuliah. Terima kasih atas kebersamaan, bantuan, dukungan, serta semangat yang kalian tularkan saat proses penyusunan skripsi ini berlangsung.
- Seluruh pihak yang secara langsung maupun tidak langsung telah membantu penulis dalam menyelesaikan studi dan penulisan skripsi ini, baik melalui bimbingan, motivasi, maupun dukungan lainnya.

Skripsi ini adalah wujud kecil dari perjuangan panjang yang penuh proses, doa, dan pengorbanan. Semoga karya ini dapat menjadi bentuk balas budi yang membawa manfaat dan menjadi pijakan awal untuk langkah selanjutnya.

## KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah Subhanahu wa Ta'ala atas segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul "Algoritma Klasifikasi Support Vector Machine Dalam Mendeteksi Serangan Ddos Pada Traffic Jaringan" ini dengan baik dan tepat waktu.

Skripsi ini merupakan hasil dari proses pembelajaran, dedikasi, dan kerja keras penulis selama menempuh pendidikan di Program Studi Keamanan Siber, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta. Selain sebagai syarat akademik untuk memperoleh gelar Sarjana Komputer, skripsi ini juga menjadi bentuk kontribusi penulis dalam bidang keamanan jaringan.

Penulis menyadari bahwa pencapaian ini tidak mungkin diraih tanpa bantuan, doa, dan dukungan dari berbagai pihak. Oleh karena itu, dengan segala kerendahan hati, penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

- Kedua orang tua dan keluarga tercinta atas kasih sayang, dukungan moral dan spiritual, serta semangat yang tiada henti.
- Dosen pembimbing atas bimbingan, arahan, serta masukan berharga selama proses penyusunan skripsi.
- Seluruh dosen dan staf akademik di lingkungan Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta, atas ilmu dan fasilitas yang telah diberikan.
- Teman-teman dan rekan seperjuangan yang telah memberikan semangat dan bantuan selama proses penyusunan skripsi ini.

Penulis menyadari bahwa skripsi ini masih memiliki keterbatasan. Oleh karena itu, penulis membuka diri terhadap kritik dan saran yang membangun demi perbaikan ke depan. Semoga skripsi ini dapat memberikan manfaat bagi pengembangan ilmu pengetahuan, khususnya dalam bidang keamanan siber.

Yogyakarta, 11 Agustus 2025

Penulis

**DAFTAR ISI**

## DAFTAR TABEL

## DAFTAR GAMBAR

## DAFTAR LAMPIRAN

## DAFTAR LAMBANG DAN SINGKATAN

| | |
|---|---|
| DDoS | Distributed Denial of Service |
| DoS | Denial of Service |
| SVM | Support Vector Machine |
| CICIDS2017 | Canadian Institute for Cybersecurity Intrusion Detection System 2017 (nama dataset) |
| RBF | Radial Basis Function (jenis kernel pada SVM) |
| ROC | Receiver Operating Characteristic |
| AUC | Area Under Curve |
| TP | True Positive (benar diklasifikasikan sebagai serangan) |
| TN | True Negative (benar diklasifikasikan sebagai normal) |
| FP | False Positive (salah diklasifikasikan sebagai serangan) |
| FN | False Negative (salah diklasifikasikan sebagai normal) |
| PCA | Principal Component Analysis (metode reduksi dimensi) |
| CNN | Convolutional Neural Networks |
| GANFS | Generative Adversarial Networks for Feature Selection |
| IDS | Intrusion Detection System |
| SMOTE | Synthetic Minority Over-sampling Technique |
| ADASYN | Adaptive Synthetic Sampling |
| API | Application Programming Interface |
| REST API | Representational State Transfer Application Programming Interface |
| SDN | Software Defined Networking |

## DAFTAR ISTILAH

| | |
|---|---|
| Hyperparameter Tuning | Proses pengaturan parameter model untuk meningkatkan kinerjanya. |
| Kernel Trick | Teknik dalam SVM untuk mengubah ruang input menjadi ruang berdimensi lebih tinggi. |
| Feature Selection | Pemilihan fitur paling relevan untuk meningkatkan kinerja model. |
| Chi-Square ($\chi^2$) | Teknik statistik untuk mengukur ketergantungan antara fitur dan label target. |
| Min-Max Scaling | Teknik normalisasi data ke dalam rentang [0, 1]. |
| GridSearchCV | Teknik pencarian parameter terbaik menggunakan pencarian grid dan cross-validation. |
| Confusion Matrix | Tabel evaluasi yang menunjukkan prediksi benar dan salah dari model klasifikasi. |
| Precision | Proporsi prediksi positif yang benar dari seluruh prediksi positif. |
| Recall (Sensitivity) | Proporsi kasus positif yang berhasil dikenali oleh model. |
| F1-Score | Rata-rata harmonis antara precision dan recall. |
| ROC Curve | Grafik hubungan antara TPR dan FPR untuk berbagai ambang klasifikasi. |
| Classification Report | Ringkasan metrik evaluasi seperti precision, recall, dan F1-score. |
| Train-Test Split | Pembagian dataset menjadi data latih dan uji. |
| Stratification | Teknik pembagian data untuk menjaga proporsi label tetap sama di data latih dan uji. |
| Inference Time | Waktu yang dibutuhkan model untuk membuat prediksi setelah pelatihan. |
| Overfitting | Ketika model terlalu cocok pada data latih dan tidak bekerja baik pada data baru. |
| Payload | Data aktual yang dikirim melalui jaringan. |
| N-Gram | Teknik ekstraksi fitur dari teks atau data sekuensial berdasarkan urutan n-kata/karakter. |
| Histogram | Representasi grafis distribusi frekuensi dari data. |

# INTISARI

Serangan Distributed Denial of Service (DDoS) merupakan ancaman serius dalam keamanan jaringan karena dapat menyebabkan gangguan layanan yang luas. Seiring dengan semakin miripnya pola serangan ini dengan lalu lintas normal, diperlukan sistem deteksi yang cerdas dan efektif. Penelitian ini bertujuan untuk mengevaluasi efektivitas algoritma klasifikasi Support Vector Machine (SVM) dalam mengidentifikasi serangan DDoS pada lalu lintas jaringan. Data yang digunakan berasal dari dataset CICIDS2017, dengan fokus pada subset Friday-WorkingHours-Afternoon-DDos.pcap_ISCX.csv yang memuat lalu lintas normal serta serangan DDoS seperti DoS-Hulk, DoS-GoldenEye, dan DDoS. Tahapan praproses mencakup penghapusan duplikat dan entri kosong, encoding label biner, normalisasi dengan Min-Max Scaler, serta seleksi fitur menggunakan teknik Chi-Square. Data dibagi menjadi 80% untuk pelatihan dan 20% untuk pengujian. Model SVM dilatih menggunakan kernel Radial Basis Function (RBF), dan penyetelan hiperparameter dilakukan dengan GridSearchCV. Evaluasi performa model dilakukan menggunakan metrik akurasi, presisi, recall, F1-score, confusion matrix, serta visualisasi melalui kurva ROC dan Precision-Recall Curve. Hasil penelitian menunjukkan bahwa sebelum penyetelan, model mencapai akurasi sebesar 97%, yang meningkat menjadi 99% setelah penyetelan, dengan nilai F1-score sebesar 0,99. Hal ini menunjukkan bahwa algoritma SVM, ketika dipadukan dengan praproses dan optimasi yang tepat, sangat efektif dalam mendeteksi serangan DDoS pada lalu lintas jaringan.

**Kata kunci:** DDoS, Support Vector Machine, Deteksi Serangan, CICIDS2017, Trafik Jaringan.

## *ABSTRACT*

*Distributed Denial of Service (DDoS) attacks represent a significant danger in network security because they can lead to extensive service interruptions. With these attacks increasingly mirroring regular traffic, smart and effective detection systems are essential. This research seeks to assess the efficacy of the Support Vector Machine (SVM) classification algorithm in identifying DDoS attacks in network traffic. The data utilized is CICIDS2017, focusing on the subset Friday-WorkingHours-Afternoon-DDos.pcap_ISCX.csv, which contains both legitimate traffic and DDoS attacks like DoS-Hulk, DoS-GoldenEye, and DDoS. The preprocessing stage included eliminating duplicates and null entries, label binary encoding, normalization through Min-Max Scaler, and feature selection applying the Chi-Square technique. The data was divided into 80% for training and 20% for testing purposes. The Radial Basis Function (RBF) kernel was utilized to train the SVM model, and hyperparameter optimization was performed with GridSearchCV. The evaluation of the model's performance was conducted through accuracy, precision, recall, F1-score, confusion matrix, and visual representations including ROC and Precision-Recall Curves. The findings indicate that prior to tuning, the model reached an accuracy of 97%, which increased to 99% post-tuning, accompanied by an F1-score of 0.99. This shows that the SVM algorithm, when paired with appropriate preprocessing and optimization, is very efficient in identifying DDoS attacks within network traffic.*



**Keyword:** *DDoS, Support Vector Machine, Attack Detection, CICIDS2017, Network Traffic.*