

**KLASIFIKASI SERANGAN *DISTRIBUTED DENIAL OF SERVICE*  
MENGUNAKAN ALGORITMA *DECISION TREE***

**SKRIPSI**

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana  
Teknik Komputer



disusun oleh

**MUHAMMAD ZAKI AFLAHDİYAG**

**18.83.0333**

Kepada

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2023**

**KLASIFIKASI SERANGAN *DISTRIBUTED DENIAL OF SERVICE*  
MENGUNAKAN ALGORITMA *DECISION TREE***

**SKRIPSI**

untuk memenuhi salah satu syarat mencapai derajat Sarjana  
Teknik Komputer



disusun oleh

**MUHAMMAD ZAKI AFLAHDYAG**

**18.83.0333**

Kepada

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA  
2023**

**HALAMAN PERSETUJUAN**

**SKRIPSI**

**KLASIFIKASI SERANGAN *DISTRIBUTED DENIAL OF SERVICE*  
MENGUNAKAN ALGORITMA *DECISION TREE***

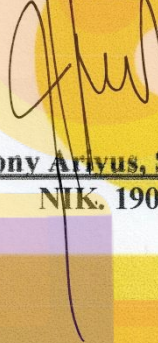
yang disusun dan diajukan oleh

**Muhammad Zaki Aflahdiyag**

**18.83.0333**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 26 Januari 2023

Dosen Pembimbing,



**Dony Ariyus, S.S., M.Kom**

**NIK. 190302128**

HALAMAN PENGESAHAN

SKRIPSI

**KLASIFIKASI SERANGAN *DISTRIBUTED DENIAL OF SERVICE*  
MENGUNAKAN ALGORITMA *DECISION TREE***

yang disusun dan diajukan oleh

**Muhammad Zaki Aflahdiyag**

**18.83.0333**

Telah dipertahankan di depan Dewan Penguji  
pada tanggal 26 Januari 2023

**Susunan Dewan Penguji**

**Nama Penguji**

**Tanda Tangan**

**Rini Indrayani, ST, M.Eng**  
NIK. 190302417

**Joko Dwi Santoso, M.Kom**  
NIK. 190302181

**Dony Arivus, S.S., M.Kom**  
NIK. 190302128



Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 26 Januari 2023

**DEKAN FAKULTAS ILMU KOMPUTER**



**Hanif Al Fatta, S.Kom., M.Kom.**  
NIK. 190302096

## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : **Muhammad Zaki Aflahdiyag**  
NIM : **18.83.0333**

Menyatakan bahwa Skripsi dengan judul berikut:

**Klasifikasi Serangan *Distributed Denial of Service* Menggunakan Algoritma *Decision Tree***

Dosen Pembimbing : **Dony Ariyus, M.Kom**

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, 26 Januari 2023

Yang Menyatakan,



Muhammad Zaki Aflahdiyag

## HALAMAN PERSEMBAHAN

Puji Syukur kehadirat Allah SWT, dengan telah diselesaikannya skripsi ini. Oleh karena itu dengan rasa syukur dan bangga penulis ucapkan terima kasih kepada:

1. Dosen pembimbing penulis, Bapak Dony Ariyus, M.Kom yang telah memberikan bimbingan, arahan, dan dukungan selama proses penulisan skripsi.
2. Keluarga yang selalu mendukung serta mendoakan penulis selama proses penyelesaian skripsi.
3. Rekan – rekan yang telah memberikan masukan, saran, dan kritik yang membangun.
4. Teman – teman yang senantiasa mengingatkan penulis untuk segera menyelesaikan skripsi ini.
5. Semua pihak yang telah membantu dalam penyelesaian skripsi ini.
6. Penyelesaian skripsi ini tidak akan mungkin tanpa bantuan dan dukungan dari semua pihak yang telah disebutkan.

## KATA PENGANTAR

Dengan penuh rasa syukur, saya ucapkan terima kasih kepada Allah karena telah memperbolehkan saya menyelesaikan skripsi ini. Judul skripsi ini adalah "klasifikasi serangan *distributed denial of service* menggunakan algoritma *decision tree*". Skripsi ini diajukan untuk memenuhi syarat kelulusan program studi Ilmu Komputer di Universitas AMIKOM Yogyakarta.

Penulis tidak akan dapat menyelesaikan skripsi ini tanpa kerja keras dan dukungan dari orang-orang di sekitarku. Saya ingin mengucapkan terima kasih kepada:

1. Prof.Dr.M.Suyanto, M.M, Rektor Universitas AMIKOM Yogyakarta.
2. Dony Ariyus, M.Kom dosen pembimbing saya yang memberikan bimbingan selama proses penyusunan skripsi.
3. Semua dosen program studi Ilmu Komputer yang memberikan ilmu yang berguna selama saya menjalani studi.
4. Semua pihak yang telah membantu dan mendukung saya, namun tidak dapat disebutkan satu per satu.

Akhir kata penulis menyadari bahwa skripsi ini tidak sempurna dan mohon maaf atas kesalahan yang mungkin ditemukan. Oleh karena itu, penulis meminta maaf atas kesalahan yang ada dalam skripsi ini.

Penulis berharap skripsi ini dapat bermanfaat bagi pembaca dan dapat dijadikan referensi untuk pengembangan lebih lanjut. Semoga Allah SWT terus memberkahi kita semua

Yogyakarta, 6 Januari 2023

Penulis

## DAFTAR ISI

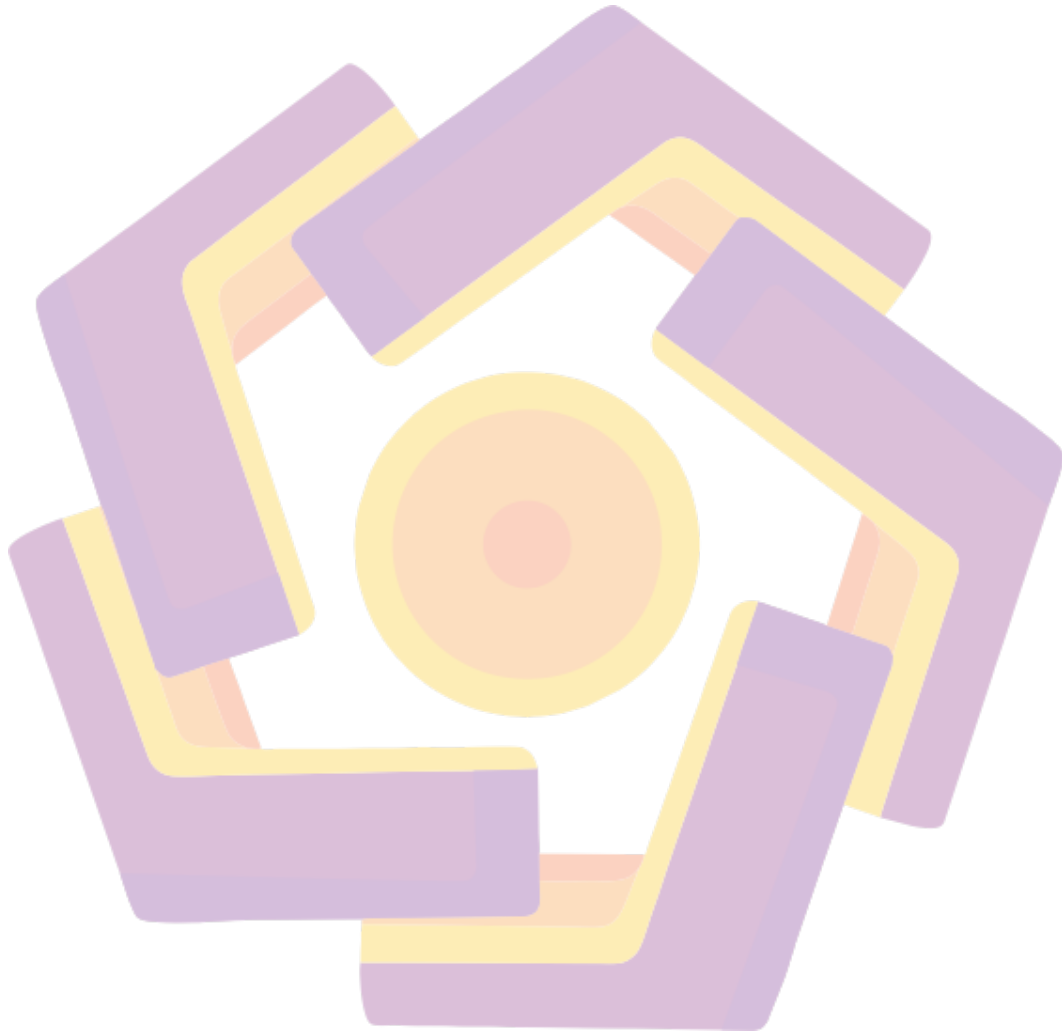
HALAMAN JUDUL .....	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN .....	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI .....	iv
HALAMAN PERSEMBAHAN .....	v
KATA PENGANTAR .....	vi
DAFTAR ISI.....	vii
DAFTAR TABEL.....	ix
DAFTAR GAMBAR.....	x
DAFTAR LAMBANG DAN SINGKATAN .....	xi
DAFTAR ISTILAH .....	xii
INTISARI .....	xiii
ABSTRACT.....	xiv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	4
1.3 Batasan Masalah .....	4
1.4 Tujuan Penelitian .....	4
1.5 Manfaat Penelitian .....	4
BAB II TINJAUAN PUSTAKA .....	5
2.1 Studi Literatur .....	5
2.2 Dasar Teori .....	10
2.2.1 <i>Denial of Service</i> dan <i>Distributed Denial of Services Attack</i> .....	10
2.2.2 <i>Machine Learning</i> .....	10
2.2.2.1 <i>Supervised Learning</i> .....	11
2.2.2.2 <i>Unsupervised Learning</i> .....	12
2.2.2.3 <i>Semi-Supervised Learning</i> .....	12
2.2.2.4 <i>Reinforcement Learning</i> .....	13
2.2.3 <i>Artificial Intelligence</i> .....	13



2.2.4 Klasifikasi .....	14
2.2.5 <i>Decision Tree</i> .....	15
2.2.6 Naïve Bayes .....	16
2.2.7 Support Vector Machine .....	17
2.2.8 Evaluasi .....	18
2.2.9.1 Akurasi .....	18
2.2.9.2 Presisi .....	19
2.2.9.3 Recall .....	19
2.2.9.4 <i>F1 Score</i> .....	19
<b>BAB III METODE PENELITIAN</b> .....	<b>20</b>
3.1 Kebutuhan Alat dan Bahan .....	20
3.2 Alur Penelitian .....	20
3.2.1 <i>Data Acquisition</i> .....	21
3.2.2 <i>Preprocessing</i> .....	24
3.2.3 Klasifikasi .....	25
3.2.4 Evaluasi .....	26
<b>BAB IV HASIL DAN PEMBAHASAN</b> .....	<b>27</b>
4.1 Implementasi .....	27
4.1 Pengujian .....	31
<b>BAB V PENUTUP</b> .....	<b>37</b>
5.1 Kesimpulan .....	37
5.2 Saran .....	37
<b>REFERENSI</b> .....	<b>38</b>

## DAFTAR TABEL

Tabel 2.1. Referensi Penelitian	5
Tabel 3.1. Jumlah sampel dataset NSL-KDD	21
Tabel 3.2. Deskripsi fitur yang ada pada dataset NSL-KDD	22
Tabel 3.2. Hasil Evaluasi Model	36

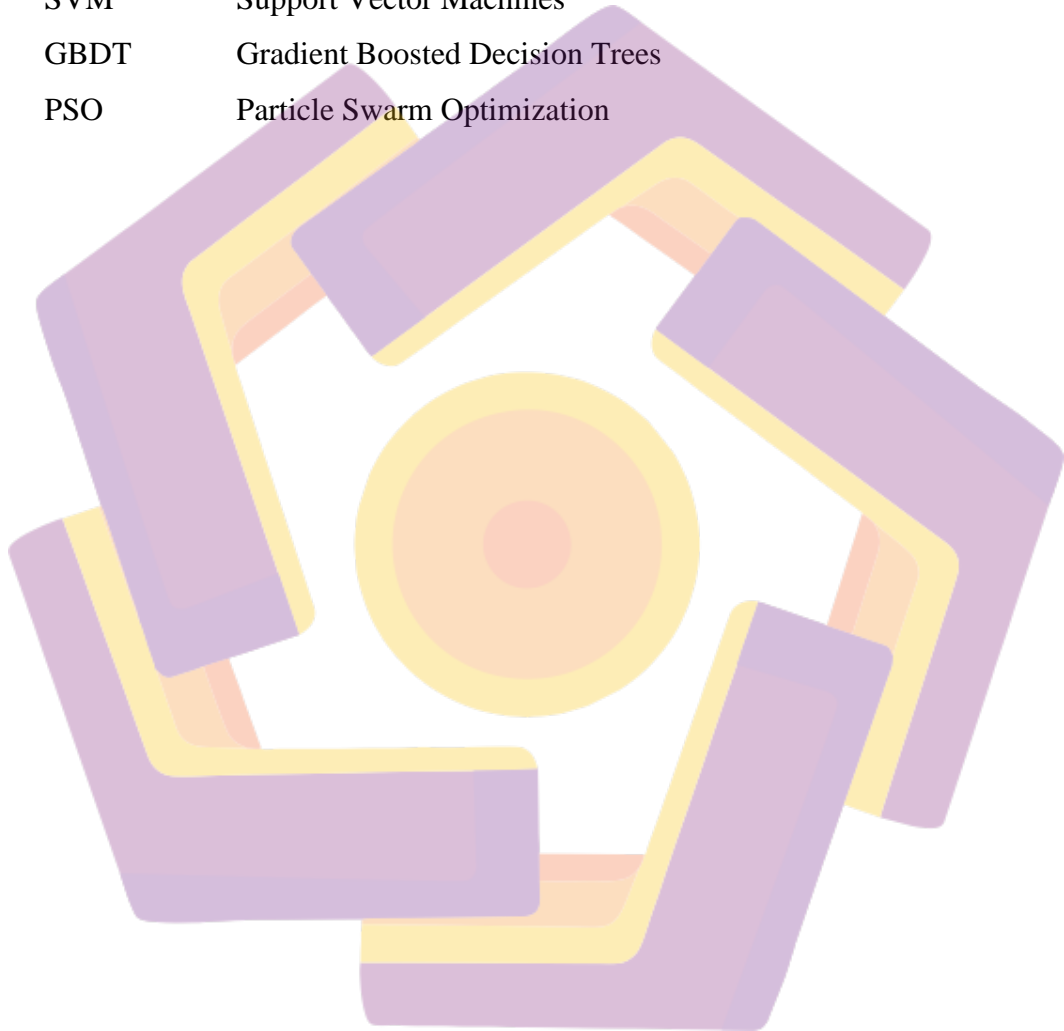


## DAFTAR GAMBAR

Gambar 2.1. Jenis Machine Learning	11
Gambar 2.2. Interaksi antara agen dengan lingkungan dalam reinforcement learning	13
Gambar 2.3. Binary Classification	14
Gambar 2.4. Multiclass Classification	15
Gambar 2.5. Struktur Algoritma Decision Tree	16
Gambar 2.6. Confusion Matrix	18
Gambar 3.1. Alur Penelitian	20
Gambar 4.1. NSL-KDD Dataset	26
Gambar 4.2. Indeks Pertama NSL-KDD Dataset	27
Gambar 4.3. Preprocessing menggunakan LabelEncoder	28
Gambar 4.4. Hasil setelah menambahkan prefix	28
Gambar 4.5. Preprocessing menggunakan LabelEncoder	29
Gambar 4.6. Fitur yang ditambahkan ke data test	29
Gambar 4.7. Ukuran dataset selama proses penggabungan	30
Gambar 4.8. Confusion Matrix Model Decision Tree	31
Gambar 4.9. Hasil Evaluasi Model Decision Tree	32
Gambar 4.10. Hasil model decision tree	32
Gambar 4.11. Confusion Matrix Model Naïve Bayes	33
Gambar 4.12. Hasil Evaluasi Model Naïve Bayes	33
Gambar 4.13. Confusion Matrix Model SVM	34
Gambar 4.14. Hasil Evaluasi Model SVM	34

## DAFTAR LAMBANG DAN SINGKATAN

PCA	Principal Component Analysis
GMM	Gaussian Mixture Model
IP	Internet Protocol
SVM	Support Vector Machines
GBDT	Gradient Boosted Decision Trees
PSO	Particle Swarm Optimization



## DAFTAR ISTILAH

Noise	data yang salah atau pencilan.
Overfitting	Kondisi dimana pohon keputusan menjadi terlalu kompleks yang dapat menangani training data dengan baik namun tidak dapat menangani data yang baru yang berarti model akan membuat prediksi yang buruk pada data yang tidak terlihat.
Leaf Node	Kemungkinan hasil dari setiap tindakan dalam decision tree
Hyperplane	Sebuah garis yang digunakan dalam algoritma SVM untuk memisahkan dua kelas dalam suatu dataset.
Multiclass	Klasifikasi yang memiliki lebih dari dua kelas.
Missing Values	nilai yang tidak ada atau tidak diketahui dari suatu atribut pada data yang digunakan.

## INTISARI

Meningkatnya pengguna dunia maya, semakin banyak jenis kejahatan siber yang muncul. Salah satunya adalah serangan *Distributed Denial of Services* (DDoS). Serangan ini dilakukan dengan mengirim paket sebanyak mungkin ke sistem yang akan membebani server dan memperlambat kinerja server atau bahkan menyebabkan deadlock. Serangan ini mengakibatkan kerugian finansial atau bahkan hilangnya data penting. Maka dari itu diperlukan algoritma *machine learning* yang dapat secara otomatis melakukan klasifikasi serangan DDoS.

Salah satu algoritma klasifikasi yang populer adalah *decision tree*. Algoritma ini dapat menangani kumpulan data besar dengan dimensi yang lebih tinggi dan dapat menangani tugas *multiclass*. Disisi lain, algoritma *decision tree* memiliki kemungkinan mengalami *overfitting* yang mengakibatkan algoritma membuat prediksi yang kurang tepat pada *unseen* data. Maka dari itu perlu dilakukan *pruning* yaitu dengan memberikan batasan baik kedalaman pohon atau batasan jumlah maksimal *nodes*.

Dataset yang digunakan adalah NSL-KDD, dataset ini merupakan pengembangan dari dataset KDD Cup 1999. Setelah dilakukan uji coba menggunakan algoritma *decision tree*, SVM, dan *naïve bayes* diperoleh hasil akurasi untuk *decision tree* 83,61%, SVM 75,58%, dan *naïve bayes* 51,17%. Akurasi ini menunjukkan bahwa algoritma *decision tree* berhasil memprediksi 83,71% benar dari keseluruhan dataset.

**Kata kunci:** *decision tree*, *machine learning*, DDoS, klasifikasi, *entropy*

## ABSTRACT

The development of cyberspace users, Then more types of crimes appear. One of them is a Distributed Denial of Services (DDoS) attack. This attack is carried out by sending as many packets as possible to the system which will overload the server and slow down server performance or even cause deadlocks. These attacks result in financial loss or even loss of important data. Therefore, a machine learning algorithm is needed that can automatically classify DDoS attacks.

One of the popular classification algorithms is the decision tree. This algorithm can handle large data sets with higher dimensions and can handle multi class tasks. On the other hand, the decision tree algorithm has the possibility of experiencing overfitting which causes the algorithm to make inaccurate predictions on unseen data. Therefore it is necessary to do pruning, namely by providing a limit to either the depth of the tree or the maximum number of nodes.

The dataset used is NSL-KDD, this dataset is an development from KDD Cup 1999. After testing using decision tree algorithm, SVM, and naive bayes, the accuracy results obtained are 83.61% for decision tree, 75.58% for SVM, and 51.17% for naive bayes. These accuracies indicate that the decision tree algorithm successfully predicted 83.71% of the dataset correctly.

**Keyword:** decision tree, machine learning, DDoS, classification, entropy

