

**ANALISIS KECERDASAN BUATAN UNTUK DETEKSI DAN
MITIGASI SERANGAN MALWARE TERBARU PADA
JARINGAN 5G**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh

Dimas Pandit Romada

17.83.0067

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2024

**ANALISIS KECERDASAN BUATAN UNTUK DETEKSI DAN
MITIGASI SERANGAN MALWARE TERBARU PADA
JARINGAN 5G**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh

Dimas Pandit Romada

17.83.0067

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2024

HALAMAN PERSETUJUAN

SKRIPSI

**ANALISIS KECERDASAN BUATAN UNTUK DETEKSI DAN MITIGASI
SERANGAN MALWARE TERBARU PADA JARINGAN 5G**

yang disusun dan diajukan oleh

Dimas Pandit Romada

17.83.0067

telah disetujui oleh di depan Dewan Penguji
pada tanggal 27 Februari 2024

Dosen Pembimbing,



Banu Santoso, S.T., M.Eng

NIK. 190302327

HALAMAN PENGESAHAN

SKRIPSI

**ANALISIS KECERDASAN BUATAN UNTUK DETEKSI DAN MITIGASI
SERANGAN MALWARE TERBARU PADA JARINGAN 5G**

yang disusun dan diajukan oleh

Dimas Pandit Romada

17.83.0067

Telah dipertahankan di depan Dewan Penguji
pada tanggal 27 Februari 2024

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Dwi Nurani, M.Kom
NIK. 190302236

M. Rudyanto Arief, S.T, M.T
NIK. 190302098

Banu Santoso, S.T., M.Eng
NIK. 190302327



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 27 Februari 2024

DEKAN FAKULTAS ILMU KOMPUTER



Hanif Al Fatta, S.Kom., M.Kom., Ph.D.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : **DIMAS PANDIT ROMADA**
NIM : **17.83.0067**

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS KECERDASAN BUATAN UNTUK DETEKSI DAN MITIGASI SERANGAN MALWARE TERBARU PADA JARINGAN 5G

Dosen Pembimbing : **Banu Santoso, S.T., M.Eng**

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, 27 Februari 2024

Yang Menyatakan,



DIMAS PANDIT ROMADA

HALAMAN PERSEMBAHAN

Skripsi ini saya persembahkan untuk saya diri sendiri yang sudah menempuh sebuah proses perjalanan hidup yang penuh lika-liku sampai di titik ini. Tentunya tidak lupa saya persembahkan kepada keluarga saya khususnya kedua orang tua yang secara langsung memberikan dukungan dari awal sampai saat ini. Dengan doa dan usaha saya sendiri serta dukungan dari orang di sekeliling saya, saya bisa menyelesaikan skripsi ini dengan lancar.



KATA PENGANTAR

Puji Syukur, Alhamdulillah atas kehadiran Allah SWT yang telah memberikan rahmat dan karuniaNya kepada kita semua sehingga kami dapat menyelesaikan skripsi yang diajukan sebagai salah satu syarat untuk menyelesaikan program strata satu (S1) di program studi Teknik Komputer Universitas Amikom Yogyakarta.

Adapun penyusunan skripsi ini digunakan sebagai bukti bahwa penyusun telah melaksanakan dan menyelesaikan penelitian Skripsi. Dalam proses penyusunan laporan ini penyusun mendapatkan banyak bantuan dari berbagai pihak. Oleh karena itu kami mengucapkan terima kasih kepada :

1. Prof. Dr. M. Suyanto, M.M. Selaku (Rektor Universitas Amikom Yogyakarta).
2. Hanif Al-Fatah, M.Kom. Selaku Dekan Fakultas Ilmu Komputer.
3. Dony Ariyus, M.Kom. Selaku Ketua Program Studi Teknik Komputer Universitas Amikom Yogyakarta.
4. Banu Santoso, S.T., M.Eng. Selaku Dosen Pembimbing yang telah memberi arahan dalam proses penulisan skripsi ini.
5. Seluruh jajaran dosen dan staff pengajar serta staff administrasi di Program Studi Teknik Komputer.

Penulis menyadari masih banyak kekurangan dalam penulisan skripsi ini. Untuk itu, penulis sangat mengharapkan saran yang membangun agar tulisan ini dapat berguna untuk perkembangan ilmu pengetahuankedepannya. Dan penulis berharap semoga skripsi ini dapat bermanfaat bagi sebagian pihak yang berkaitan dalam penulisan ini.

Yogyakarta, 4 September 2023

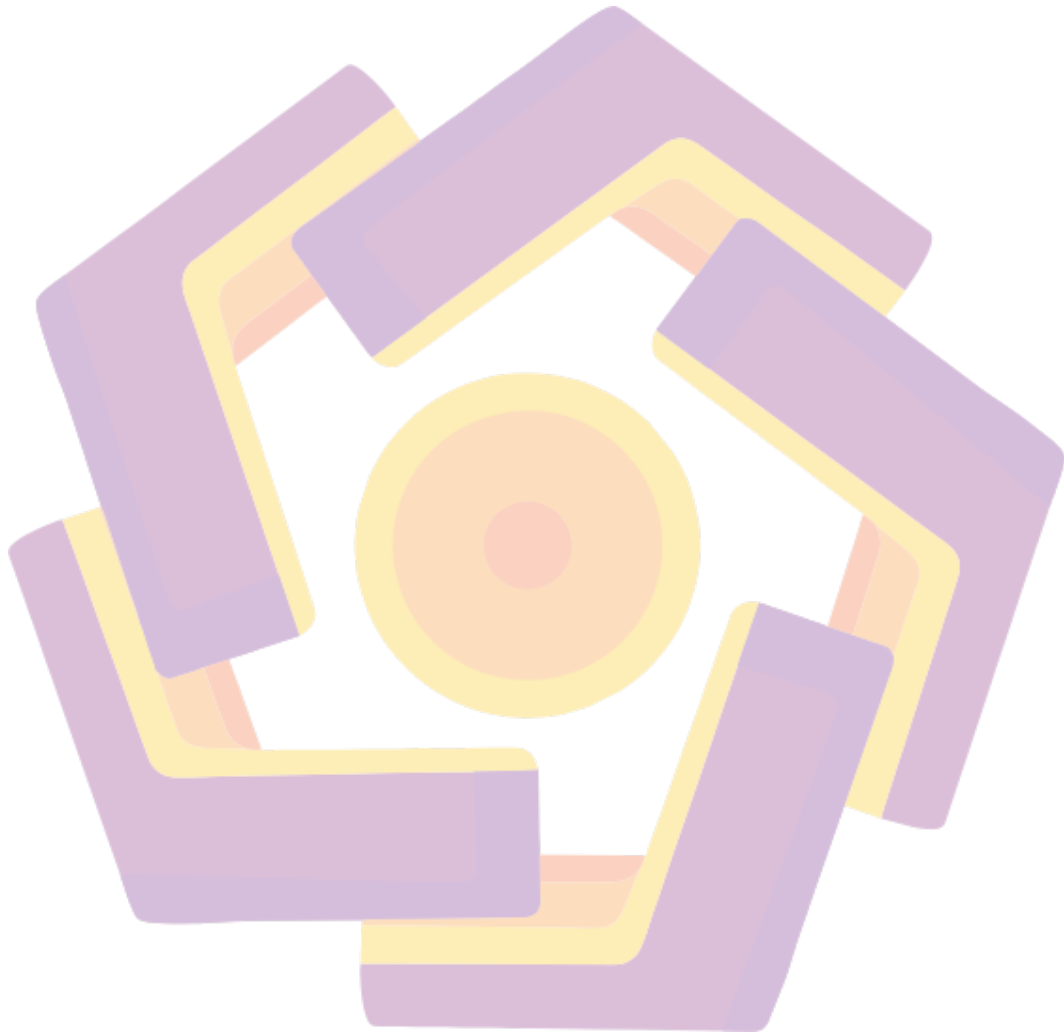
Penulis

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.....	x
DAFTAR GAMBAR	xi
INTISARI.....	xiii
<i>ABSTRACT</i>	xiv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian.....	5
1.5 Manfaat Penelitian.....	6
1.6 Sistematika Penulisan.....	7
BAB II TINJAUAN PUSTAKA.....	9
2.1 Studi Literatur.....	9
2.2 Dasar Teori	17
2.2.1 Jaringan 5G.....	17

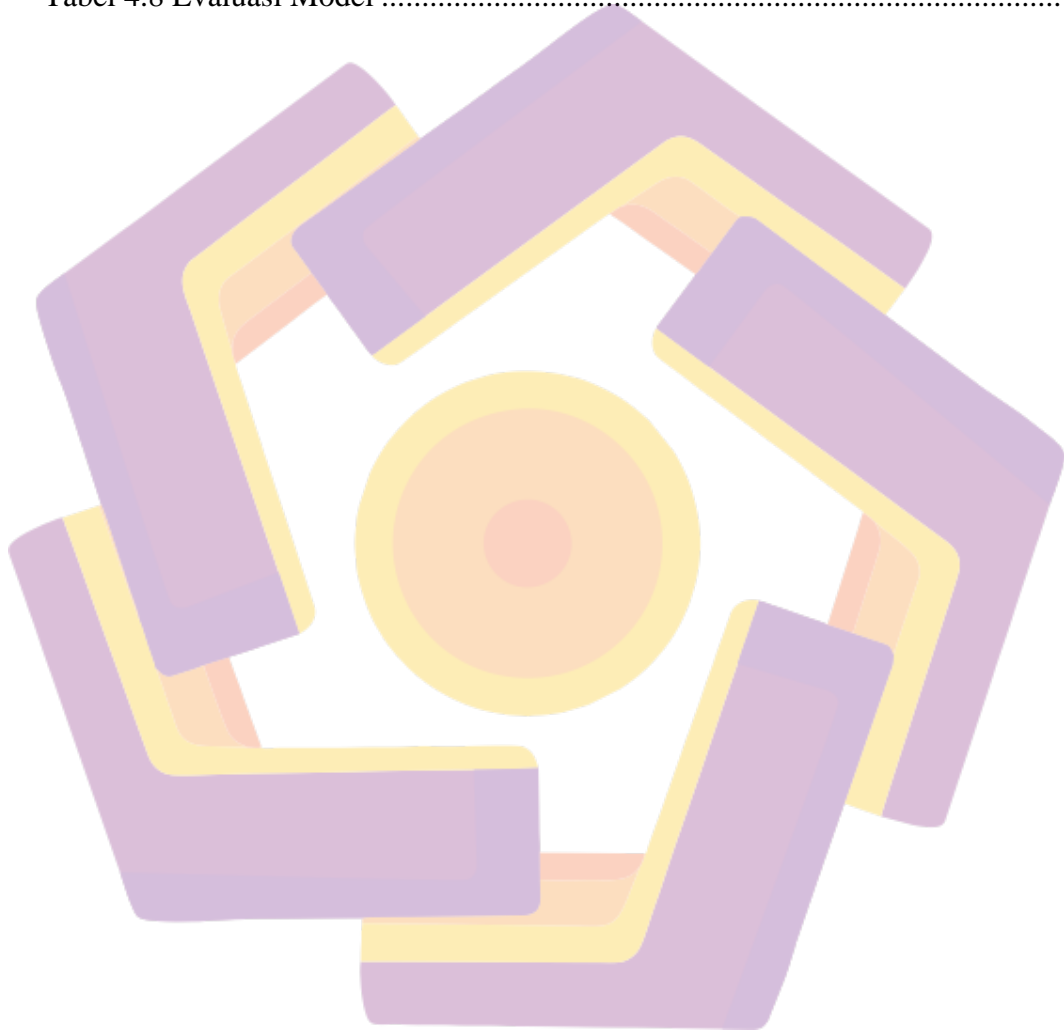
2.2.2	Malware	21
2.2.3	Keamanan Jaringan	25
2.2.4	Kecerdasan Buatan	28
2.2.5	Deteksi dan Mitigasi	31
2.2.6	<i>Support Vector Machine (SVM)</i>	34
BAB III METODE PENELITIAN.....		38
3.1	Objek Penelitian	38
3.2	Alur Penelitian.....	39
3.3	Alat dan Bahan	41
3.3.1	Data Penelitian	41
3.3.2	Alat Dan Instrumen.....	41
BAB IV HASIL DAN PEMBAHASAN		43
4.1	Analisis Masalah	43
4.2	Model Pembelajaran Mesin.....	43
4.2.1	Supervised Learning	43
4.2.2	Analisis Heuristic.....	44
4.2.3	Deteksi Anomali	45
4.2.4	Analisis Big Data.....	45
4.3	Scenario Uji Coba	45
4.4	Split Data	48
4.5	Memproses Data.....	50
4.6	Metode SVM	54
4.7	Hasil Uji Coba	62
4.8	Evaluasi Model.....	63

BAB V PENUTUP.....	69
5.1 Kesimpulan.....	69
5.2 Saran.....	70
REFERENSI	71



DAFTAR TABEL

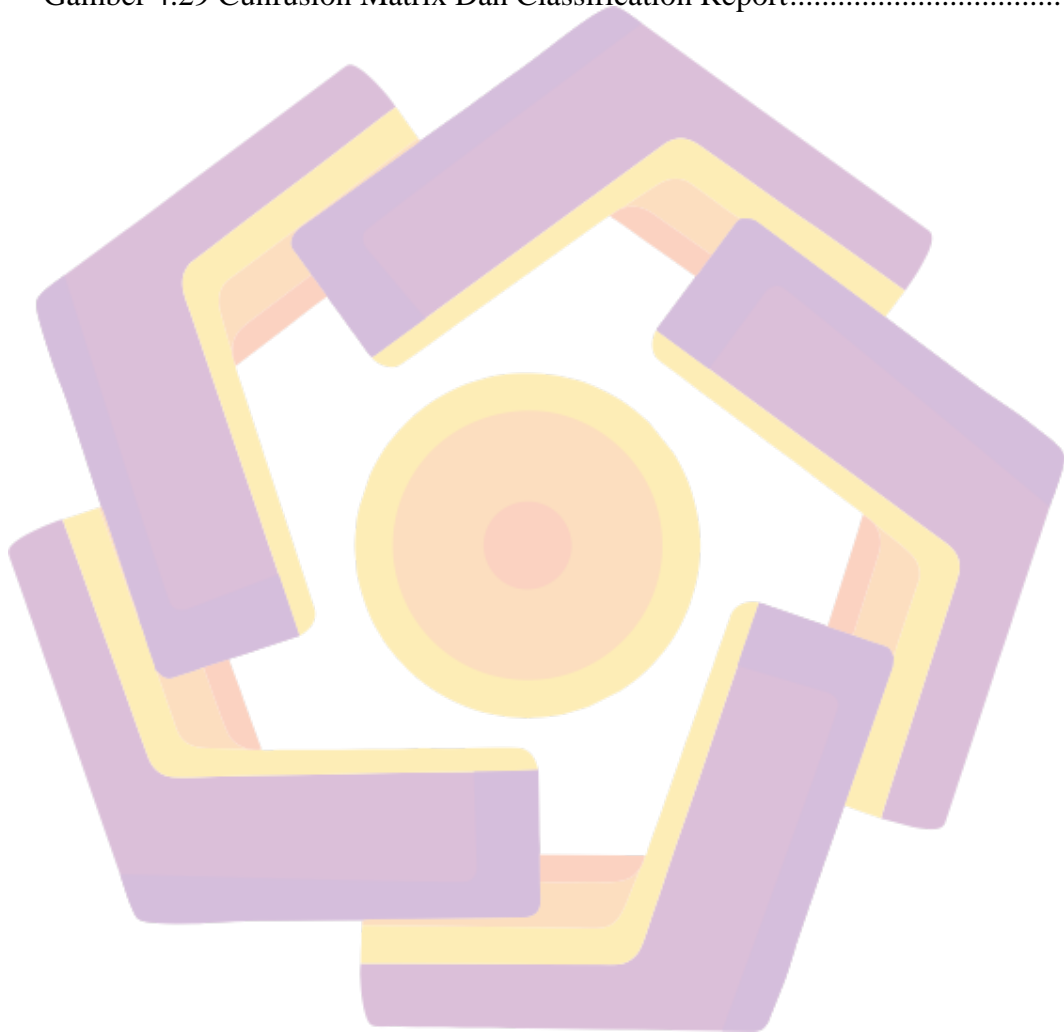
Tabel 2.1 Keaslian Penelitian.....	13
Tabel 4.3 Scenario Uji Coba	46
Tabel 4.6 Metode SVM.....	59
Tabel 4.8 Evaluasi Model	64



DAFTAR GAMBAR

Gambar 2.1 Kecepatan Unduh Maksimal	19
Gambar 2.2 Kecepatan Unggah Maksimal	19
Gambar 2.3 Latensi Jaringan 4G Dan 5G	20
Gambar 2.4 Macam-Macam Machine Learning	30
Gambar 2.5 Alur Pada ML Dan Deep Learning	30
Gambar 2.6 Hyperplane Pada SVM.....	34
Gambar 3.1 Alur Penelitian.....	39
Gambar 4.2 Model Unsupervised	44
Gambar 4.3 Pola Machine Learning	44
Gambar 4.4 Analisis Big Data	46
Gambar 4.5 Deskripsi Dataset 5 Fitur.....	47
Gambar 4.6 Deskripsi Dataset 6 Fitur.....	47
Gambar 4.7 Implementasi Split Data	48
Gambar 4.8 Rincian Data X_Train	49
Gambar 4.9 Rincian Data X_Test	49
Gambar 4.10 Rincian Data Y_Train	49
Gambar 4.11 Rincian Data Y_Test	50
Gambar 4.12 Keluaran Pembersih Data X_Train	51
Gambar 4.13 Hasil Pembersih DataX_Train	51
Gambar 4.14 Hasil Pembersih Data Y_Train	51
Gambar 4.15 Hasil Pembersih Data Y_Test	51
Gambar 4.16 Proses Standarisasi Atribut.....	53
Gambar 4.17 Standarisasi Atribut X_Train	53
Gambar 4.18 Standar Atribut X_Test	53
Gambar 4.19 Model SVM.....	54
Gambar 4.20 Algoritma 1	54
Gambar 4.21 Algoritma 2	55
Gambar 4.22 Modeling SVM.....	58
Gambar 4.23 Algoritma 3	60

Gambar 4.24 Scoring	62
Gambar 4.25 Data Uji Coba.....	62
Gambar 4.26 Data Normal Pada Uji Coba.....	63
Gambar 4.27 Hasil Evaluasi Penggunaan RAM Saat Running Code.....	66
Gambar 4.28 Hasil Evaluasi Lama Waktu Running Code.....	66
Gambar 4.29 Confusion Matrix Dan Classification Report.....	66



INTISARI

Jaringan 5G pada saat ini sangat canggih dan pintar membawa manfaat dalam konektivitas dan kinerja, tetapi tidak menutup kemungkinan memiliki sisi negatif. Pada dunia teknologi pada masa sekarang kecerdasan buatan menjadi peran penting untuk mendeteksi serangan malware pada jaringan 5G. Model kecerdasan buatan ini (AI) Artificial intelligence kemudian akan diimplementasikan dalam sistem deteksi real time yang dapat memantau lalu lintas jaringan dan mengenali pelaku yang mencurigakan. Dengan menerapkan AI secara efektif, jaringan 5G dapat memperkuat pertahanannya terhadap serangan malware terbaru yang semakin canggih, menjaga keamanan, dan menjaga integritas operasionalnya. Namun perlu diingat bahwa upaya berkelanjutan yang memerlukan investasi sumber daya yang substansial dan pemeliharaan yang terus menerus untuk tetap efektif dalam menghadapi ancaman keamanan yang terus berkembang. Penelitian ini sangat relatif diimplementasikan sehingga dapat mengamankan lebih banyak data.

Kata kunci: Kecerdasan buatan, malware, jaringan 5G, efektif, keamanan.

ABSTRACT

5G networks are currently very sophisticated and smart bringing benefits in connectivity and performance, but it does not rule out the possibility of having a negative side. In today's technological world, artificial intelligence plays an important role in detecting malware attacks on 5G networks. This artificial intelligence (AI) model will then be implemented in a real time detection system that can monitor network traffic and recognize suspicious actors. By effectively implementing AI, 5G networks can strengthen their defenses against the latest, increasingly sophisticated malware attacks, maintain security, and preserve operational integrity. But keep in mind that this is an ongoing effort that requires substantial resource investment and continuous maintenance to remain effective in the face of evolving security threats. This research is highly relative to implementation so as to secure more data.

Keyword: Artificial intelligence, malware, 5G network, effective, security.