

**IMPLEMENTASI NEURAL NETWORK 1-DIMENSI DALAM  
IDENTIFIKASI MALWARE ANDROID**

**SKRIPSI**

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



disusun oleh

**ROFIK HIDAYAT**

**18.83.0165**

Kepada

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

**IMPLEMENTASI NEURAL NETWORK 1-DIMENSI DALAM  
IDENTIFIKASI MALWARE ANDROID**

**SKRIPSI**

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



disusun oleh

**ROFIK HIDAYAT**

**18.83.0165**

Kepada

**FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA**

**YOGYAKARTA**

**2023**

**HALAMAN PERSETUJUAN**

**SKRIPSI**

**IMPLEMENTASI NEURAL NETWORK 1-DIMENSI DALAM  
IDENTIFIKASI MALWARE ANDROID**

yang disusun dan diajukan oleh

**Rofik Hidayat**

**18.83.0165**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 18 Agustus 2023

Dosen Pembimbing,



**Muhammad Kopravi, S.Kom., M.Eng**

**NIK. 190302454**

**HALAMAN PENGESAHAN**  
**SKRIPSI**  
**IMPLEMENTASI NEURAL NETWORK 1-DIMENSI DALAM**  
**IDENTIFIKASI MALWARE ANDROID**

yang disusun dan diajukan oleh

**Rofik Hidayat**

**18.83.0165**

Telah dipertahankan di depan Dewan Penguji  
pada tanggal 18 Agustus 2023

**Susunan Dewan Penguji**

**Nama Penguji**

**Tanda Tangan**

Muhammad Kopravi, S.Kom., M.Eng  
NIK. 190302454

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

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



Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 18 Agustus 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 : Rofik Hidayat  
NIM : 18.83.0165

Menyatakan bahwa Skripsi dengan judul berikut:

### **IMPLEMENTASI NEURAL NETWORK 1-DIMENSI DALAM IDENTIFIKASI MALWARE ANDROID**

Dosen Pembimbing : Muhammad Kopravi, S.Kom., 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, 18 Agustus 2023

Yang Menyatakan,



Rofik Hidayat

## HALAMAN PERSEMBAHAN

Dengan di iringi dengan rasa syukur kepada Tuhan Yang Maha Esa,  
Penelitian ini dipersembahkan kepada:

1. Allah SWT Tuhan Yang Maha Esa
2. Kedua Orang Tua
3. Dosen pembimbing
4. Seluruh Dosen Teknik Komputer
5. Team Freedom Union
6. Seluruh teman-teman mahasiswa Jurusan Teknik Komputer 2018



## KATA PENGANTAR

Alhamdulillahirail'aalamiin puji syukur ke hadirat Allah SWT yang telah melimpahkan rahmat petunjuk dan kemudahan sehingga atas ridho nya, Tugas Akhir ini dapat terselesaikan. Shalawat serta salam tercurah kepada junjungan kita Nabi Muhammad SAW beserta keluarga dan para pengikut-pengikutnya sampai akhir zaman. Dalam menyelesaikan tugas akhir yang berjudul "IMPLEMENTASI NEURAL NETWORK 1-DIMENSI DALAM IDENTIFIKASI MALWARE ANDROID" disusun sebagai hasil proses pembelajaran yang telah peneliti dapatkan selama melakukan proses pembelajaran di Jurusan Teknik Komputer Fakultas ilmu komputer Universitas AMIKOM Yogyakarta. Selama proses menyusun Tugas Akhir ini peneliti telah banyak mendapatkan bantuan dari berbagai pihak. Untuk itu pada kesempatan ini peneliti bermaksud menyampaikan ucapan terima kasih kepada :

1. Prof. Dr. M. Suyanto, MM., selaku Rektor Universitas AMIKOM Yogyakarta
2. Hanif Al Fatta, S.Kom., M.Kom, selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
3. Dony Ariyus, M.Kom. selaku Ketua Program Studi Fakultas Teknik Komputer.
4. Muhammad Kopravi, S.Kom., M.Eng, selaku dosen pembimbing yang telah meluangkan waktu untuk membimbing.
5. Kedua Orang Tua yang selalu memberikan dukungan, doa dan motivasi dalam penyusunan tugas akhir ini.

Yogyakarta, 18 Agustus 2023

Penulis

## DAFTAR ISI

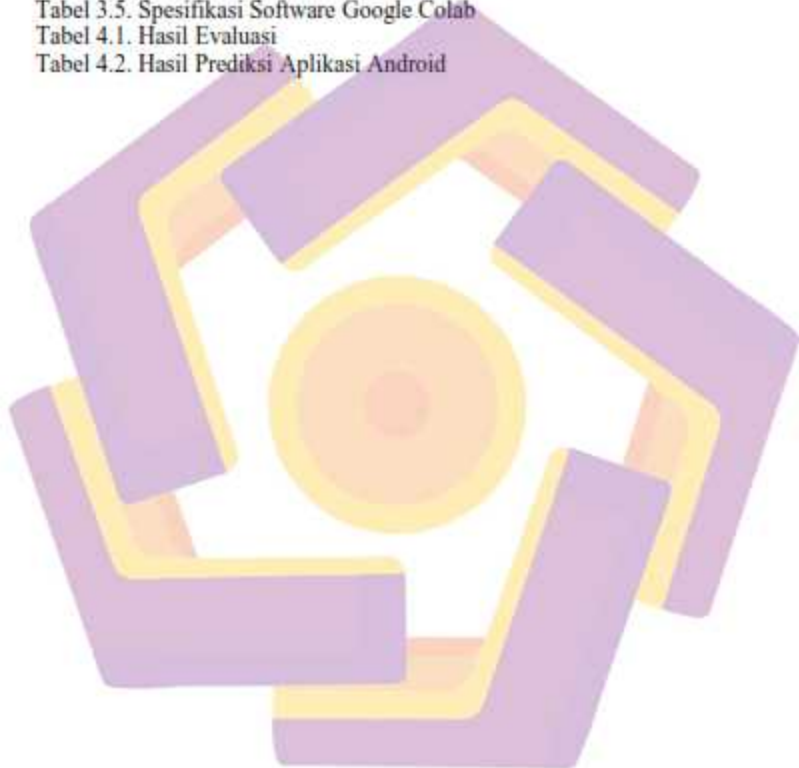
HALAMAN JUDUL .....	i
HALAMAN PERSETUJUAN .....	ii
HALAMAN PENGESAHAN .....	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI .....	iv
HALAMAN PERSEMBAHAN .....	v
KATA PENGANTAR .....	vi
DAFTAR ISI .....	vii
DAFTAR TABEL .....	ix
DAFTAR GAMBAR .....	x
DAFTAR LAMPIRAN .....	xi
DAFTAR LAMBANG DAN SINGKATAN .....	xii
DAFTAR ISTILAH .....	xiii
INTISARI .....	xiv
ABSTRACT .....	xv
<b>BAB I PENDAHULUAN</b> .....	<b>1</b>
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	2
1.3 Batasan Masalah .....	2
1.4 Tujuan Penelitian .....	3
1.5 Manfaat Penelitian .....	3
1.5.1 Manfaat Teoritis .....	3
1.5.2 Manfaat Praktisi .....	3
1.6 Sistematika Penulisan .....	4
<b>BAB II TINJAUAN PUSTAKA</b> .....	<b>5</b>
2.1 Studi Literatur .....	5
2.2 Dasar Teori .....	9
2.2.1 Android .....	9
2.2.2 Android Permission .....	9
2.2.3 Malware .....	9
2.2.4 Machine Learning .....	10
2.2.5 Deep Learning .....	10
2.2.6 Convolutional Neural Network 1-Dimensi .....	10
2.2.7 Adam Optimizer .....	12



2.2.8	Python .....	12
2.2.9	JDAX .....	12
2.2.10	Confusion Matrix .....	12
2.2.11	TensorFlow .....	13
2.2.12	Binary Cross Entropy .....	13
2.2.13	Selenium Webdriver .....	14
<b>BAB III METODE PENELITIAN .....</b>		<b>15</b>
3.1	Populasi dan Sample .....	15
3.2	Variable Penelitian .....	15
3.3	Alat dan Bahan .....	16
3.3.1	Perangkat Keras .....	16
3.3.2	Perangkat Lunak .....	16
3.4	Metode Penelitian .....	17
3.4.1	Metode Pengumpulan Data .....	17
3.4.2	Metode Analisis .....	17
3.4.3	Tahapan Penelitian .....	17
<b>BAB IV HASIL DAN PEMBAHASAN .....</b>		<b>21</b>
4.1	Pengumpulan Dataset .....	21
4.2	<i>Preprocessing</i> Data .....	30
4.3	Pembuatan Arsitektur .....	32
4.4	Pelatihan Model .....	35
4.5	Evaluasi Model dan Hasil .....	36
4.6	Implementasi Program .....	38
<b>BAB V PENUTUP .....</b>		<b>41</b>
5.1	Kesimpulan .....	41
5.2	Saran .....	41
<b>REFERENSI .....</b>		<b>42</b>
<b>LAMPIRAN .....</b>		<b>45</b>

## DAFTAR TABEL

Tabel 2.1. Keaslian Penelitian	7
Tabel 3.1. Permission Android	15
Tabel 3.2. Spesifikasi Hardware Laptop	16
Tabel 3.3. Spesifikasi Hardware Google Colab	16
Tabel 3.4. Spesifikasi Software Laptop	16
Tabel 3.5. Spesifikasi Software Google Colab	16
Tabel 4.1. Hasil Evaluasi	38
Tabel 4.2. Hasil Prediksi Aplikasi Android	39

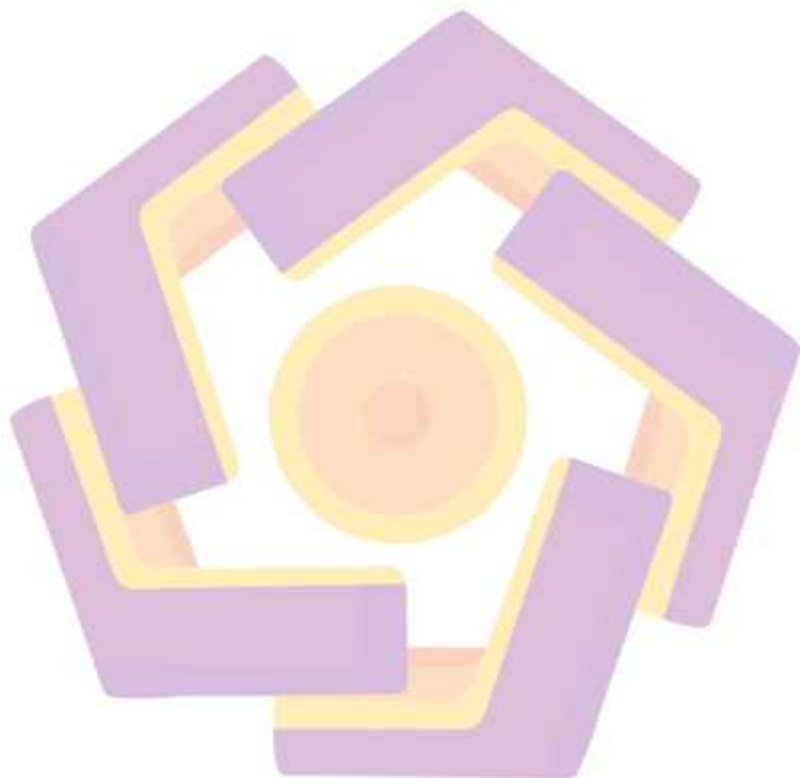


## DAFTAR GAMBAR

Gambar 2.1. Struktur Dasar CNN 1 Dimensi	11
Gambar 2.2. Contoh CNN 1 Dimensi	12
Gambar 3.1. Flowchart Alur Penelitian	18
Gambar 3.2. Flowchart Identifikasi Malware	18
Gambar 4.1. Proses Mengunduh Dataset 1	21
Gambar 4.2. Mengambil Hash SHA256 Malware	22
Gambar 4.3. Mengubah Format Hash	23
Gambar 4.4. Mengunduh Malware	23
Gambar 4.5. Ekstrak File Kompresi Malware	24
Gambar 4.6. Contoh Nama Apk Package	25
Gambar 4.7. Proses Mengunduh Apk dari ApkPure	25
Gambar 4.8. Apk yang telah diunduh	26
Gambar 4.9. Mengunduh APK dari Playstore	26
Gambar 4.10. Apk yang telah di export	27
Gambar 4.11. Folder yang berisi file apk	27
Gambar 4.12. Kode untuk Decompile apk	28
Gambar 4.13. Proses Dekompilasi untuk mendapatkan permission	29
Gambar 4.14. Kode untuk membuat dataset	29
Gambar 4.15. Proses Pelabelan Data	29
Gambar 4.16. Dataset 2	30
Gambar 4.17. Cleaning Dataset	31
Gambar 4.18. Jumlah Malware dan Aplikasi Jinak	31
Gambar 4.19. Dataset Splitting	32
Gambar 4.20. Rancangan Arsitektur CNN 1D	33
Gambar 4.21. Membangun Model CNN 1D	35
Gambar 4.22. Proses Training	36
Gambar 4.23. Grafik Loss dan Akurasi Proses Training	36
Gambar 4.24. Confusion Matrix	37
Gambar 4.25. Tampilan Program output identifikasi malware android	39

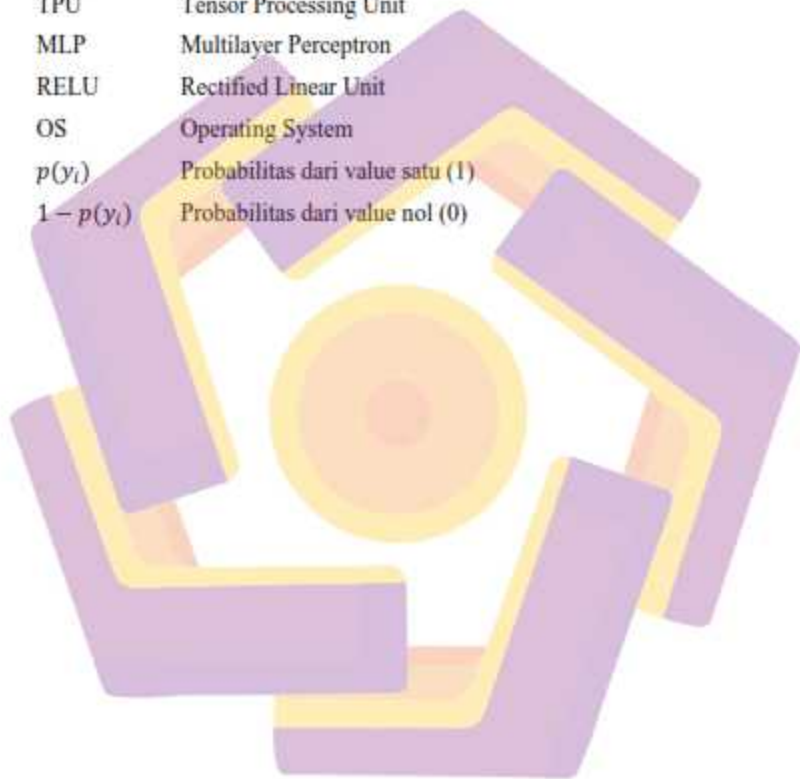
## DAFTAR LAMPIRAN

Lampiran 1. Souce Code Training	45
Lampiran 2. Source Code Testing	45
Lampiran 3. Source Code Prototype Program Identifikasi malware	46



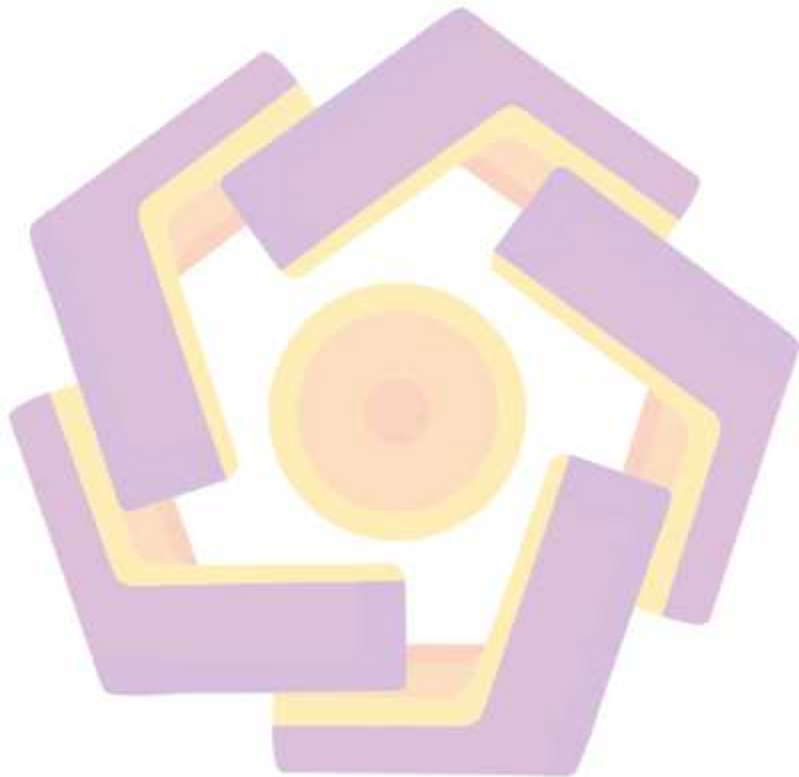
## DAFTAR LAMBANG DAN SINGKATAN

CNN	Convolutional Neural Network
CPU	Central Processing Unit
GPU	Graphic Processing Unit
TPU	Tensor Processing Unit
MLP	Multilayer Perceptron
RELU	Rectified Linear Unit
OS	Operating System
$p(y_i)$	Probabilitas dari value satu (1)
$1 - p(y_i)$	Probabilitas dari value nol (0)



## DAFTAR ISTILAH

Vektor	besaran yang mempunyai arah
Dekompilasi	proses merubah Bahasa komputer menjadi kode sumber



## INTISARI

Permasalahan Malware tiap tahunnya menjadi ancaman serius dalam teknologi informasi dari segi keamanan sehingga perlu adanya penanganan masalah tersebut. Dengan meningkatnya penggunaan perangkat mobile ponsel pintar android menjadikannya target yang rentan terkena serangan Malware. Untuk mencegah terjadinya serangan Malware maka perlu adanya deteksi dini aplikasi yang berpotensi malware. Tiap aplikasi android memiliki permission untuk membuka hak akses agar aplikasi tersebut dapat mengakses informasi pada perangkat android, begitu juga dengan Malware yang juga mempunyai permission tersebut. Teknologi *Machine Learning* dapat menyelesaikan masalah masalah yang rumit dengan meniru kecerdasan pada manusia. Salah satu teknologi tersebut adalah *Neural Network* yang merupakan Teknik *Machine learning* dengan strukturnya meniru cara kerja otak manusia, *Neural Network* memiliki banyak jenis algoritma diantaranya adalah *Convolutional Neural Network* 1-Dimensi. Dengan bantuan algoritma *Convolutional Neural Network* 1-Dimensi dapat dilakukan pengklasifikasi Malware atau Aplikasi jinak berdasarkan permissionnya. Model *Convolutional Neural Network* 1-Dimensi yang digunakan pada penelitian ini akan mengubah data permission menjadi urutan data dan akan mengidentifikasi malware menggunakan *binary classification* dengan fungsi *sigmoid* yang memiliki range (0,1) dimana akan menghasilkan output 1 yang menandakan Malware dan juga 0 yang menandakan aplikasi yang jinak. Dengan menggunakan dataset sebanyak 510 aplikasi, metode yang diusulkan mampu mendapatkan 92.1% untuk tingkat akurasi, 93.4% untuk *recall* dan 89.5% untuk *precision*, dapat dikatakan model yang didapat sudah cukup baik dalam mengidentifikasi malware berdasarkan permissionnya.

**Kata kunci:** Neural Network, Android Permission, Klasifikasi, Malware.

## ABSTRACT

Malware issues annually become a serious threat in information technology from a security perspective, so it is necessary to address this problem. With the increasing use of mobile devices, Android smartphones make them vulnerable targets for malware attacks. To prevent malware attacks, it is necessary to have early detection of potential malware applications. Each Android application has permission to open access rights so that the application can access information on the Android device, as well as Malware which also has this permission. Machine Learning technology can solve complex problems by imitating human intelligence. One of these technologies is a Neural Network which is a machine learning technique with a structure that mimics how the human brain works. Neural Networks have many types of algorithms, including a 1-Dimensional Convolutional Neural Network. With the help of the 1-Dimensional Convolutional Neural Network algorithm, it is possible to classify malware or benign applications based on their permissions. The 1-Dimensional Convolutional Neural Network model used in this study will convert data permissions into data sequences and will identify malware using a binary classification with a sigmoid function that has a range  $(0,1)$  which will produce output 1 indicating Malware and also 0 indicating A benign application. By using a dataset of 510 applications, the proposed method is able to get 92.1% for accuracy, 93.4% for recall and 89.5% for precision, it can be said that the model obtained is good enough in identifying malware based on its permissions.

**Keyword:** Neural Network, Android Permission, Classification, Malware.