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 Koprawi, 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 Koprawi, 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 Koprawi, 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 Fakutas Teknik Komputer.
4. Muhammad Koprawi, 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

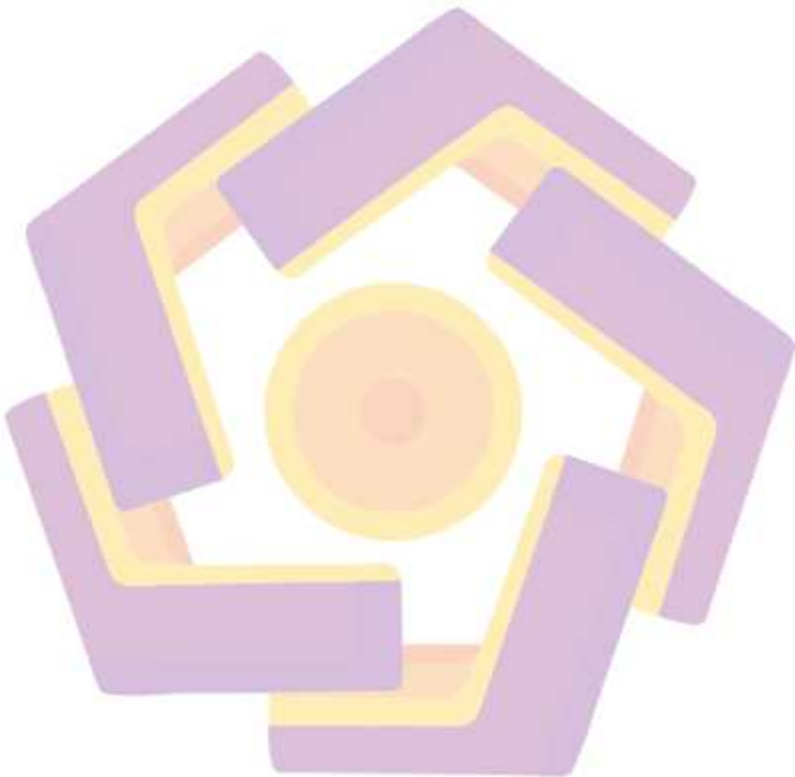
Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

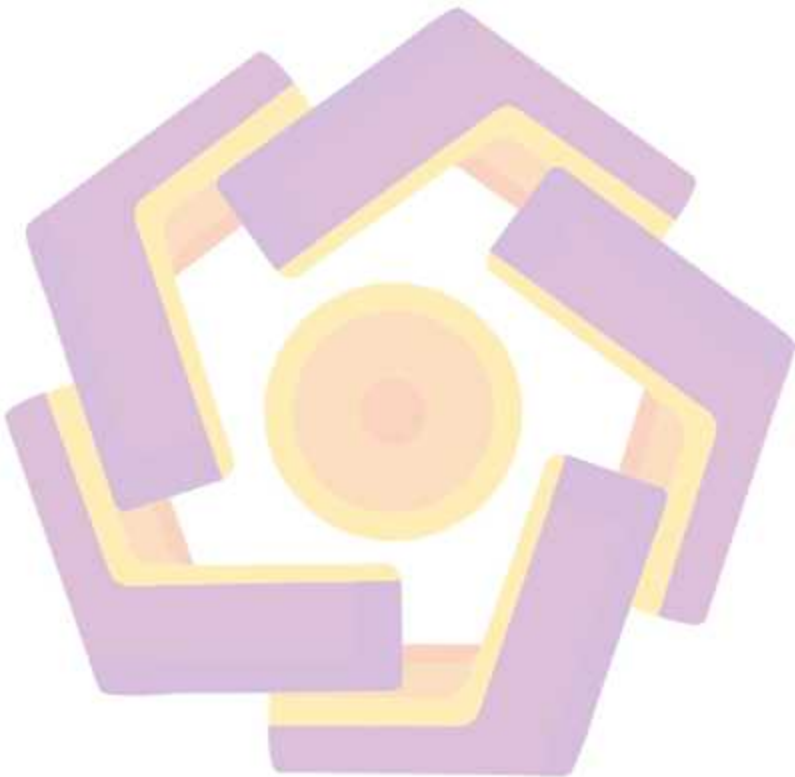


DAFTAR LAMBANG DAN SINGKATAN

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 sumbers



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.