IMPLEMENTASI CONVOLUTIONAL NEURAL NETWORK UNTUK MENDETEKSI MALWARE PACKER

SKRIPSI

Diajukan oleh

SINDRI FERA KUSUMA

18.83.0300

Kepada

PROGRAM SARJANA

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

IMPLEMENTASI CONVOLUTIONAL NEURAL NETWORK UNTUK MENDETEKSI MALWARE PACKER

SKRIPSI

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

Diajukan oleh

SINDRI FERA KUSUMA

18.83.0300

Kepada

PROGRAM SARJANA

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2020

HALAMAN PERSETUJUAN

SKRIPSI

IMPLEMENTASI CONVOLUTIONAL NEURAL NETWORK UNTUK MENDETEKSI MALWARE PACKER

Yang disusun dan diajukan oleh

Sindri Fera Kusuma

18.83.0300

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 21 Juli 2022

Dosen Pembimbing,

iii

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

HALAMAN PENGESAHAN

SKRIPSI

IMPLEMENTASI CONVOLUTIONAL NEURAL NETWORK UNTUK MENDETEKSI MALWARE PACKER

Yang disusun dan diajukan oleh

Sindri Fera Kusuma

18.83.0300

Telah dipertahankan di depan Dewan Penguji
pada tanggal 21 Juli 2022

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Joko Dwi Santoso, M.Kom **NIK. 190302181**	_____
Nila Feby Puspitasari, S.Kom, M.Cs **NIK. 190302161**	_____
Banu Santoso, S.T., M.Eng **NIK. 190302327**	_____

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 21 Juli 2022

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom.
NIK. 19030209

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Sindri Fera Kusuma
NIM : 18.83.0300

Menyatakan bahwa Skripsi dengan judul berikut:

IMPLEMENTASI CONVOLUTIONAL NEURAL NETWORK UNTUK MENDETEKSI MALWARE PACKER

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, 21 Juli 2022

Yang Menyatakan,

Sindri Fera Kusuma

HALAMAN PERSEMBAHAN

Penulisan laporan tugas akhir ini tak luput dari doa dan dukungan dari keluarga, sahabat dan rekan rekan yang selalu sedia membantu dan menyemangati, hanya Allah SWT yang mampu membalas semua kebaikan yang telah dicurahkan. Oleh sebab itu penulis banyak mengucapkan terima kasih kepada :

1. Allah SWT dan Nabi Muhammad SAW.
2. Keluarga dan Saudara yang saya cintai serta saya sayangi Sandra Novie Kustuma.
3. Bapak Banu Santoso, S.T, M.Eng selaku Pembimbing Tugas Akhir
4. Bapak Joko Dwi Santoso, M.Kom dan Ibu Nila Feby Puspitasari, S.Kom, M.Cs. selaku dosen penguji.
5. Bapak serta Ibu Dosen prodi Teknik Komputer
6. Winda Hariana Arta selaku sahabat yang selalu mendukung saya
7. Sahabat yang senantiasa memberikan dorongan: Ardiana Ratna Mardani dan Alma Dewi Ananda.
8. Teman kelas Teknik Komputer-03 khususnya Nur Dian Yustikarini, Diah Pingkan Sari dan Intan Nurrohma yang telah berjuang bersama serta banyak membantu saya sejak awal semester.
9. Teman seperjuangan Teknik Komputer angkatan 2018
10. Diri saya sendiri, terima kasih untuk tidak menyerah.

KATA PENGANTAR

Alhamdulillah puji syukur penulis panjatkan kehadirat ALLAH SWT atas banyak rahmat dan karuniaNya yeng telah senantiasa membimbing memudahakan jalan pada penulis dalam menyelesaikan penulisan tugas akhir ini yang berjudul Implementasi Convolutional Neural Network untuk Mendeteksi Malware Packer, tak lupa penulis ucapkan terima kasih kepada Dosen Pembimbing saya Bapak Banu Santoso S.T, M.Eng, Tim Dosen Penguji yaitu Bapak Joko Dwi Santoso, M.Kom dan Ibu Nila Feby Puspitasari, S.Kom, M.Cs serta semua pihak yang terkait dalam penyelesaian tugas akhir termasuk Keluarga, Sahabat dan Teman-teman.

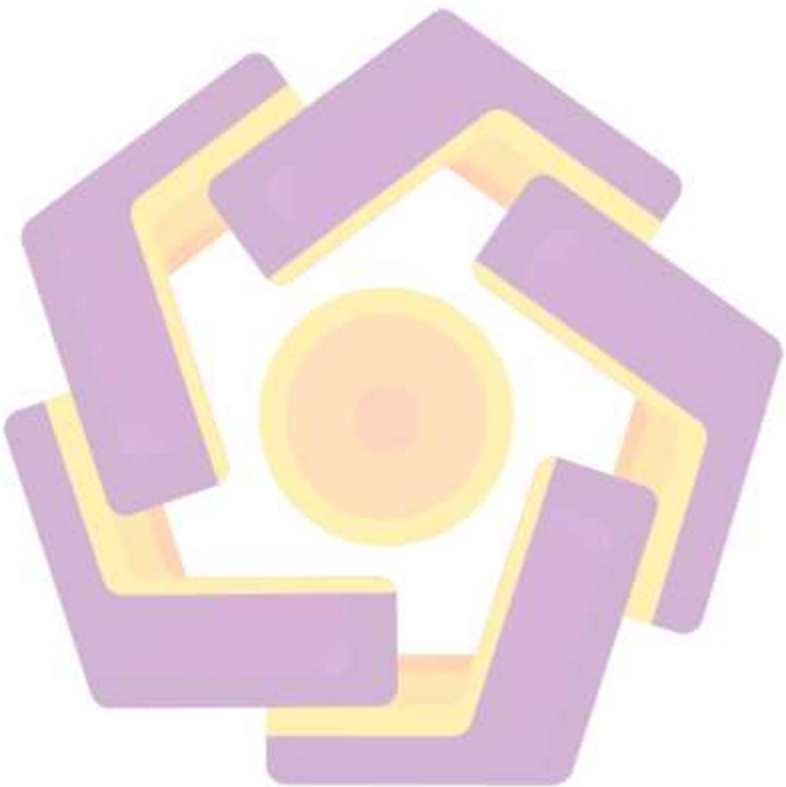
Penulis berharap dengan adanya Penulisan laporan tugas akhir ini dapat memberikan manfaat ataupun referensi bagi siapapun yang memiliki minat dibidang keamanan informasi serta bisa dijadikan pengetahuan yang berguna dalam penerapan keamanan pada computer dari ancaman berbahaya seperti serangan malware.

Yogyakarta, 21 Juli 2022

Penulis

DAFTAR ISI

DAFTAR TABEL



DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR LAMBANG DAN SINGKATAN

$\sum$	Sigma
CNN	Connvolutional Neural Network
Malware	Malicious Software
ReLU	Rectified Linear Unit
API	Application Programming Interface
NN	Neural Network
PE	Portable Execute
RNN	Recurrent Neural Networks

DAFTAR ISTILAH

Akurasi	Tingkat tertinggi dari hasil pengukuran terhadap nilai sebenarnya
Batch	Set data yang dimasukkan dalam satu iterasi training model
Batch Normalization	Normalisasi masukan atau keluaran dari aktivasi fungsi dalam lapisan tersembunyi yang memiliki fungsi untuk membuat jaringan saraf lebih stabil dan melindunginya dari bobot outlier
Class/Label	Label atau keterangan yang digunakan dalam penelitian dataset
Epoch	Putaran dari data yang telah melewati proses training
Batch Size	ukuran data sampel yang disebarkan ke jaringan neural yang dimasukkan dalam proses
Feeding	Memasukkan data dengan Tensorflow Record (TFRecord) kepada API Tensorflow
Framework	Sebuah frame yang dapat memudahkan dalam membuat sebuah aplikasi atau sistem tertentu agar terbentuk dan terstruktur secara rapi
Stride	Parameter yang menentukan jumlah pergeseran filter/kernel
Padding	Indikator yang menentukan jumlah pixel yang berisi nilai 0 yang akan ditambahkan disetiap sisi masukan
Dropout	Teknik regulasi neural network dimana beberapa jaringan akan dipilih secara acak untuk tidak dipakai selama proses training
Step	Langkah yang didefinisikan pada konfigurasi pipeline untuk proses training yang menentukan tingkat keberhasilan pelatihan jaringan saraf
Filter/Kernel	Matriks untuk menghitung dan mendeteki suatu ciri atau pola yang digunakan untuk perhitungan konvulasi

Neuron	Dikenali juga sebagai node/unit yaitu simpul dalam jaringan saraf yang biasanya menggunakan beberapa nilai masukan dan menghasilkan satu nilai keluaran
Model	Bentuk dari apa yang telah dipelajari oleh sistem dari data training
Parameter	Indikator dalam model yang dilatih oleh sistem.
Pipeline	Susunan yang berkaitan dengan algoritma meliputi proses pengumpulan data, input data kedalam data training, melatih satu atau beberapa model, dan mengekspor model
Loss	Ukuran seberapa jauh prediksi model tidak sesuai dengan label yang sebenarnya atau dengan kata lain ukuran seberapa buruk model

INTISARI

File Portable Execute merupakan file dengan ekstensi yang banyak dicari dan digunakan namun semakin berkembangnya internet ada saja varian dari file tersebut yang tak sesuai dengan fungsinya, bagi orang awam yang menggunakan file ekstensi tersebut tidak terlalu memperhatikan akan adanya bahaya dari file yang diinstallnya jika tidak hati-hati dan sekarang perkembangan virus, Trojan, worm dan malware lainnya tidak bisa dicegah.

Semakin banyak variasi dari malware yang menyebar di dunia internet dan mengancam keamanan dari sistem komputer yang awalnya hanya file PE biasa bisa dijadikan sarang malware dengan cara di packed. Banyak cara bisa dilakukan untuk menangatasi masalah tersebut salah satunya dari bidang Machine Learning yaitu Neural Network.

Neural Network ada berbagai jenis namun untuk mengatasi masalah ini hanya beberapa metode yang bisa dipakai. Convolutional Neural Network adalah salah satu metode learning yang cukup populer untuk mendeteksi malware berbasis image, dimana jika menggunakan model ini maka malware tersebut akan di olah menjadi image terlebih dahulu sebelum akhirnya dideteksi, dan pada penelitian ini model CNN digunakan untuk mendeteksi malware dengan tingkat akurasi diatas 95%.

Kata kunci: CNN, Malware, Akurai, Deteksi, FastAPI

Abstract

Portable Execute files are files with extensions that are widely sought after and used but as the internet develops there are variants of these files that are not in accordance with their functions, for ordinary people who use the extension files do not pay much attention to the dangers of the files they install if they are not careful and now the development of viruses, Trojans, worms and other malware cannot be prevented.

More and more variations of malware are spreading in the internet world and threatening the security of computer systems that were originally just ordinary PE files can be used as a hotbed of malware by being packed. There are many ways that can be done to overcome these problems, one of which is from the field of Machine Learning, namely Neural Networks.

Neural Networks there are various types but to overcome this problem only a few methods can be used. Convolutional Neural Network is one of the learning methods that is quite popular for detecting image-based malware, where if you use this model, the malware will be processed into an image first before finally being detected, and in this study the CNN model was used to detect malware with an accuracy level above 95%.

Keyword: *CNN, Malware, Accuracy, Detection, FastAPI*