Analisis dan Implementasi DL4MD: *Deep Learning Framework for Intelligent Malware Detection*

Mentari Puspa Adriyani[1], Parman Sukarno[2], Erwid Musthofa Jadied[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]mentaripuspaa@student.telkomuniversity.ac.id, [2]psukarno@telkomuniversity.ac.id,
[3]jadied@telkomuniversity.ac.id

Abstrak

Dalam beberapa tahun ini, *malware* menimbulkan ancaman yang sangat serius dan terus berkembang membuat deteksi *malware* menjadi perhatian utama. Pencegahan dan penanggulangan *malware* dapat dilakukan melalui deteksi *signature* dan perilaku *malware* tersebut. *Malware* yang semakin berevolusi dapat menghindari proses pencocokan *signature* dengan memodifikasi dirinya secara dinamis, sehingga sulit bagi system untuk mempertahankan diri dari infeksi *malware.* Dengan mengamati perilaku *malware* ada beberapa informasi yang didapat salah satunya berupa fitur API *call* yang dapat merepresentasikan tujuan dari *malware*. Beberapa penelitian terkait telah dilakukan untuk mendeteksi serangan *malware*, dan memiliki akurasi yang bagus. Namun, kebanyakan penerapan deteksi tersebut dibangun diatas arsitektur pembelajaran yang dangkal. Diantara metode *deep learning* yang digunakan, *Autoencoder* merupakan metode yang sangat jarang digunakan. *Autoencoder* merupakan salah satu arsitektur dalam *deep learning* yang digunakan untuk mereduksi data. Oleh karena itu, pada tugas akhir ini, Convolutional Neural Network Autoencoder (CNN-AE) digunakan sebagai metode pembelajaran deteksi *malware.* Akurasi deteksi yang berhasil dicapai oleh model CNN-AE adalah 97.14 %.

Kata kunci : deep learning, malware, api call, autoencoder, convolutional neural network

Abstract

In recent years, malware has issued a very serious threat and continues to make malware detection a major concern. Prevention and prevention of malware can be done through detection of signatures and protection of these malware. Malicious software that can be used for the signature matching process using dynamic software, making it difficult for the system to defend itself against malware. By being able to restore malware, there is some information obtained, one of which is the API call feature. Several related studies have been conducted to deal with malware attacks, and have good accuracy. However, the evaluation is broader than the evaluation of superficial architecture. The deep learning method used, Autoencoder is a method that is very rarely used. Autoencoder is an architecture in deep learning that is used to reduce data. Therefore, in this final project, Convolutional Neural Network Autoencoder (CNN-AE) is used as a malware detection learning method. The detection accuracy that was achieved by the CNN-AE model was 97.14%.

Keywords: deep learning, malware, API call, autoencoder, convolutional neural network