UNIVERSITAS
GADJAH MADA
Metode Deteksi Malware Menggunakan Support Vector Machine (SVM) dan Artificial Neural Network (ANN)
Rahma Maesarah, Dr. Sri Suning Kusumawardani, S.T., M.T. ; Widyawan, S.T., M.Sc., Ph.D.
Universitas Gadjah Mada, 2023 | Diunduh dari http://etd.repository.ugm.ac.id/

INTISARI

Malware merupakan kepanjangan dari *malicious software* atau perangkat lunak yang berbahaya, serta dapat juga diartikan sebagai kode berbahaya atau *malicious code*. Pada dasarnya malware merupakan program yang berisikan kode baik itu kode yang ditambahkan, diubah maupun yang dihapus dari sistem perangkat lunak untuk secara sengaja menyebabkan kerusakan maupun disfungsi dari sistem, sehingga sistem tidak dapat berfungsi sebagaimana mestinya. Malware, dapat menimbulkan dampak buruk serta kerugian bagi sistem dan penggunanya, oleh karena itu, perlu dilakukan pencegahan dari serangan malware, salah satunya adalah dengan melakukan deteksi malware. Terdapat dua metode deteksi, yakni Signature based detection dan Non-signature based detection (Behaviour-based). Penelitian ini menggunakan metode Behavior-based Detection, di mana pada prosesnya menggunakan teknik klasifikasi *machine learning*, sehingga proses deteksi ini membutuhkan dataset. Algoritma yang digunakan pada deteksi ini adalah algoritma machine learning yakni SVM dan deep learning ANN. Penelitian ini bertujuan untuk menganalisis teknik dari deteksi yang dilakukan dengan dua metode tersebut. Dataset yang digunakan adalah CLaMP oleh Ajit Kumar tahun 2020. Kesimpulan dari penelitian ini menghasilkan nilai akurasi sebesar 95,9% untuk metode SVM Linear, 98,1% untuk metode SVM Polynomial, 94,4% untuk SVM Sigmoid, dan 89,4% untuk ANN.

Kata kunci : Malware, *Machine Learning*, ANN, SVM

UNIVERSITAS
GADJAH MADA
Metode Deteksi Malware Menggunakan Support Vector Machine (SVM) dan Artificial Neural Network (ANN)
Rahma Maesarah, Dr. Sri Suning Kusumawardani, S.T., M.T. ; Widyawan, S.T., M.Sc., Ph.D.
Universitas Gadjah Mada, 2023 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

Malware stands for malicious software or malicious software, and can also be interpreted as malicious code or malicious code. Basically, malware is a program that contains code, be it code that is added, changed or deleted from a software system to intentionally cause damage or dysfunction of the system, so that the system cannot function as it should. Malware, can cause adverse effects and losses for the system and its users, therefore, it is necessary to prevent malware attacks, one of which is to perform malware detection. There are two detection methods, namely Signature based detection and Non-signature based detection (Behavior-based). This study uses the Behavior-based Detection method, in which the process uses the machine learning classification technique, so this detection process requires a dataset. The algorithms used in this detection are machine learning algorithms namely SVM and deep learning ANN. This study aims to analyze the techniques of detection carried out by these two methods. The dataset used is CLaMP by Ajit Kumar in 2020. The conclusion of this study resulted in an accuracy value of 95.9% for the Linear SVM method, 98.1% for the Polynomial SVM method, 94.4% for Sigmoid SVM, and 89 .4% for ANNs.

Keywords : Malware, *Machine Learning*, ANN, SVM