ABSTRAK

Chandra, S. D., Oktavianto, H., & Wardoyo, A. E. (2024). Klasifikasi Malware Menggunakan Metode *Convolutional Neural Network* (CNN) Berbasis Website. Jurnal Penelitian Teknologi Informasi dan Sains, 2(2), 84-99.

Pembimbing: (1) Hardian Oktavianto, S.Si., M.Kom.; (2) Ari Eko Wardoyo, S.T., M.Kom.

Malware adalah perangkat lunak yang diciptakan dengan tujuan tertentu, dimana penyerang mencari celah keamanan dalam sistem. Dampak buruk dari *Malware* dapat dirasakan pada komputer atau pengguna, karena penyerang dapat mencuri informasi atau data pribadi seseorang. Penelitian ini bertujuan untuk mengembangkan sistem deteksi *malware* berbasis web menggunakan *Convolutional Neural Network* (CNN) dengan memanfaatkan dataset IoT23. *Malware* merupakan perangkat lunak berbahaya yang dapat mengeksploitasi celah keamanan pada sistem komputer, mencuri data, dan menurunkan kinerja. Implementasi sistem deteksi ini melibatkan CNN yang mampu mengekstraksi fitur penting dari data visual maupun tekstual, diaplikasikan pada klasifikasi *malware*. Dataset IoT23 terdiri dari 23 skenario lalu lintas jaringan IoT, termasuk lalu lintas dari perangkat terinfeksi *malware*. Hasil penelitian menunjukkan bahwa aplikasi web yang dikembangkan mampu mendeteksi serangan *malware* dengan akurasi, presisi, *recall*, dan *f1-score* masing-masing sebesar 99% pada skenario data terpisah. Sistem deteksi berbasis CNN ini terbukti efektif dalam mengidentifikasi dan mengklasifikasikan serangan *malware*, berkontribusi pada peningkatan keamanan jaringan dan perangkat.

Kata Kunci: *Malware*, *Convolutional Neural Network* (CNN), IoT23 dataset, deteksi *malware* berbasis web, *deep learning*.

ABSTRACK

Chandra, S. D., Oktavianto, H., & Wardoyo, A. E. (2024). Malware Classification Using Website-Based Convolutional Neural Network (CNN) Method. Journal of Information Technology and Science Research, 2(2), 84-99.

Advisor: (1) Hardian Oktavianto, S.Si., M.Kom.; (2) Ari Eko Wardoyo, S.T., M.Kom.

Malware is software that is created with a specific purpose, where the attacker looks for security holes in the system. The adverse impact of Malware can be felt on a computer or user, because the attacker can steal someone's personal information or data. This research aims to develop a web-based malware detection system using Convolutional Neural Network (CNN) by utilizing the IoT23 dataset. Malware is malicious software that can exploit security holes in computer systems, steal data, and degrade performance. The implementation of this detection system involves CNN which is capable of extracting important features from visual and textual data, applied to malware classification. The IoT23 dataset consists of 23 IoT network traffic scenarios, including traffic from malware-infected devices. The results show that the developed web application is able to detect malware attacks with accuracy, precision, recall, and f1-score of 99% each on separate data scenarios. This CNN-based detection system proved effective in identifying and classifying malware attacks, contributing to improved network and device security.

Keywords: *Malware, Convolutional Neural Network (CNN), IoT23 dataset, web-based malware detection, deep learning.*