

INTISARI

PROYEK AKHIR

ANALISIS PERBANDINGAN KINERJA ALGORITMA METAHEURISTIK PADA SISTEM DETEKSI MALWARE

Tasya Widiyarsari
19/441183/SV/16535

Keamanan siber merupakan isu utama dalam era teknologi informasi yang semakin maju. Ancaman *malware*, seperti perangkat lunak berbahaya yang kompleks dan dapat menyebar melalui jaringan, semakin meningkat. Dalam upaya mengatasi masalah ini, algoritma *Machine Learning* telah menjadi solusi yang menjanjikan untuk mendeteksi *malware*. Namun, salah satu tantangan utama adalah dimensi fitur yang besar pada kumpulan data *malware* yang tidak terstruktur. Untuk mengatasi hal tersebut, para peneliti menggunakan teknik *Feature Selection* (FS) untuk mengurangi dimensi fitur dan memilih subset optimal. Dalam konteks deteksi *malware*, terdapat dua pendekatan yang umum digunakan, yaitu pendekatan *signature-based* dan pendekatan berbasis anomali. Namun, karena *malware* terus mengubah perilakunya, metode deteksi berbasis *signature-based* tidak lagi efektif. Untuk mengatasi masalah tersebut, penelitian ini mengusulkan penggunaan metode seleksi fitur berbasis algoritma metaheuristik *Marine Predator* untuk deteksi *malware* pada lalu lintas jaringan. Hasil penelitian menunjukkan bahwa implementasi sistem deteksi *malware* menggunakan teknik seleksi fitur berbasis algoritma *Marine Predator* dapat menghasilkan akurasi yang baik yaitu sebesar 99,74%. Dengan demikian, penelitian ini dapat menjadi solusi untuk mengatasi permasalahan dalam mengidentifikasi dan melindungi sistem dari ancaman *malware* yang semakin berkembang dan kompleks.

Kata kunci : *Machine Learning, Algorithm, Metaheuristik, Malware, Marine Predator*

ABSTRACT

Cyber security is a major issue in the era of increasingly advanced information technology. Malware threats, such as complex malicious software that can spread through networks, are increasing. In an effort to solve this problem, Machine Learning algorithms have become a promising solution for detecting malware. However, one of the main challenges is the large feature dimensions of the unstructured malware data set. To overcome this, the researchers used the Feature Selection (FS) technique to reduce the feature dimensions and select the optimal subset. In the context of malware detection, there are two commonly used approaches, namely the signature-based approach and anomaly-based approach. However, as malware continues to change its behavior, signature-based detection methods are no longer effective. To overcome this problem, this study proposes the use of a feature search method based on the Marine Predator metaheuristic algorithm for cross-network malware detection. The results of the study show that the implementation of a malware detection system using a feature selection technique based on the Marine Predator algorithm can produce a good accuracy of 99,74%. Thus, this research can be a solution to overcome problems in identifying and protecting systems from increasingly growing and complex malware threats.

Keywords: Machine Learning, Algorithm, Metaheuristics, Malware, Marine Predator