

Implementasi Metode Whale Optimization Algorithm-Support Vector Machine dalam Klasifikasi Serangan Siber pada Jaringan Internet of Things = Implementation of Whale Optimization Algorithm-Support Vector Machine Method in Cyber Attack Classification on Internet of Things Networks

Rafa Elmira Afiani, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=9999920564285&lokasi=lokal>

Abstrak

Internet of Things (IoT) merupakan sebuah teknologi yang memungkinkan perangkat untuk berkomunikasi dan mengirimkan data melalui jaringan tanpa campur tangan manusia. Kompleksitas pada jaringan IoT menyebabkan sistem mengalami kesulitan dalam mendeteksi properti serangan dan memaksa sistem untuk memperkuat keamanannya. Salah satu upaya yang paling sering digunakan untuk pertahanan jaringan IoT adalah Intrusion Detection System (IDS). Penggunaan IDS dapat memberikan peringatan dini dan mampu melakukan pencegahan terhadap potensi serangan pada jaringan. Penelitian ini menggunakan dataset Aegean WIFI Intrusion Dataset (AWID2) yang berisikan lalu lintas trafik internet pada jaringan WIFI. Data AWID2 berisi 2,3 juta records dan dikelompokkan ke dalam empat kelas yaitu normal, impersonation, injection, dan flooding. Penelitian ini dilakukan untuk melakukan klasifikasi jenis serangan siber pada jaringan IoT melalui penerapan teknik machine learning dengan metode Whale Optimization Algorithm – Support Vector Machine (WOA-SVM) dengan kernel RBF dan pendekatan One vs Rest, dimana Whale Optimization Algorithm (WOA) digunakan sebagai optimasi parameter yang digunakan pada metode Support Vector Machine (SVM). Untuk mengatasi permasalahan dimensi data yang tinggi pada dataset yang digunakan, dilakukan seleksi fitur untuk reduksi dimensi data dengan menggunakan metode seleksi fitur filter Information Gain. Kinerja model dievaluasi berdasarkan nilai metrik accuracy, precision, recall, dan F1 Score dengan memperhatikan waktu klasifikasi dan proporsi train-test split berkisar dari 50%-90%. Hasil penelitian menunjukkan bahwa model WOA-SVM memperoleh kinerja terbaik dengan menggunakan 40 fitur terbaik dari hasil seleksi fitur Information Gain menghasilkan tingkat accuracy sebesar 99,5951%, precision sebesar 96,3928%, recall sebesar 99,8888%, F1 Score sebesar 98,0662%, dan waktu klasifikasi selama 16,831 detik. Hasil kinerja model WOA-SVM tersebut lebih baik jika dibandingkan dengan tanpa menggunakan seleksi fitur dan SVM tanpa optimasi parameter WOA.

.....The Internet of Things (IoT) is a technology that enables devices to communicate and transmit data over a network without human intervention. The complexity of IoT networks poses challenges in detecting attack properties and necessitates enhanced security measures. One of the most commonly employed defenses for IoT networks is the Intrusion Detection System (IDS). The use of IDS provides early warnings and can prevent potential attacks on the network. This study utilizes the Aegean Wi-Fi Intrusion Dataset (AWID2), which contains internet traffic data on Wi-Fi networks. The AWID2 dataset comprises 2 million records categorized into four classes: normal, impersonation, injection, and flooding. This research aims to classify types of cyber-attacks on IoT networks by applying machine learning techniques using the Whale Optimization Algorithm - Support Vector Machine (WOA-SVM) method with an RBF kernel and a One vs. Rest approach. The Whale Optimization Algorithm (WOA) is used to optimize the parameters employed in the Support Vector Machine (SVM) method. To address the high-dimensional data issue in the dataset,

feature selection is performed to reduce data dimensions using the Information Gain filter method. The model's performance is evaluated based on the metrics of accuracy, precision, recall, and F1 Score, considering computation time and train-test split proportions ranging from 50% to 90%. The results indicate that the WOA-SVM model achieves the best performance by using the top 40 features from the Information Gain feature selection, yielding an accuracy of 99.5951%, precision of 96.3928%, recall of 99.8888%, F1 Score of 98.0662%, and a computation time of 16.831 seconds. The performance of the WOA-SVM model is superior compared to models without feature selection and SVM without WOA parameter optimization.