Evaluasi Kinerja Sistem Deteksi Serangan Denial of Service (DoS) Berbasis Convolution Neural Network (CNN) 1 Dimensi = Performance Evaluation of Denial of Service (DoS) Attacks Detection System Based on 1 Dimension Convolution Neural Network (1D CNN)

Bayu Ardianto, author

Abstrak

Dalam rangka meningkatkan kemampuan Intrusion Detection System (IDS) dalam mendeteksi serangan, beberapa penelitian melakukan penerapan teknik deep learning. Penelitian ini menggunakan salah satu teknik deep learning yaitu Convolutional Neural Network (CNN) dengan algoritma Convolution 1 Dimension (Conv1D) dan dataset Communications Security Establishment and Canadian Institute of Cybersecurity Intrusion Detection System (CSE-CIC-IDS) 2017 dan CSE-CIC-IDS 2018 untuk deteksi serangan DoS-Hulk, DoS-SlowHTTPTest, DoS-GoldenEye, dan DoS-Slowloris. Selain itu, dilakukan penggabungan kedua dataset tersebut untuk meningkatkan kinerja deteksi. Kontribusi dari penelitian ini adalah penerapan teknik resampling sebelum data mengalami proses pembelajaran. Selain itu, dilakukan penambahan fungsi dropout untuk mencegah terjadinya overfitting. Berdasarkan hasil penelitian diperoleh bahwa model CNN yang dibangun dengan dataset CSE-CIC-IDS 2018 memiliki kinerja yang lebih tinggi dalam deteksi serangan DoS dibanding model CNN yang dibangun dengan dataset CSE-CIC-IDS 2017 yaitu akurasi 99,57%, precision 99,58%, recall 99,43% dan f1-score 99,50%.

.....To improve the ability of Intrusion Detection System (IDS) to detect attacks, several studies have implemented deep learning techniques. Our study uses one of the deep learning techniques, namely Convolutional Neural Network (CNN) with Conv1D algorithm and dataset Communications Security Establishment and Canadian Institute of Cybersecurity Intrusion Detection System (CSE-CIC-IDS) 2017 and CSE-CIC-IDS 2018 for detection of DoS attacks-Hulk, DoS attacks-SlowHTTPTest, DoS attacks-GoldenEye, and DoS attacks-Slowloris. In addition, the two datasets were combined to improve detection performance. The contribution of our study is the application of resampling techniques before the data undergoes the learning process. In addition, a dropout function was added to prevent overfitting. Based on the results of the study, it was found that the CNN model built with the CSE-CIC-IDS dataset 2018 had a higher performance in detecting DoS attacks than the CNN model built with the CSE-CIC-IDS 2017 dataset, such as accuracy 99,57% precision 99,58% recall 99,43% dan f1-score 99,50%.