

Abstrak

DoS atau Denial of Service adalah serangan yang menyebabkan komputer atau device mengalami gangguan sehingga jaringan pada komputer terganggu. Serangan DoS ini bisa dideteksi dengan melakukan metode IDS atau Intrusion Detection System yang dapat mendeteksi serangan tersebut. IDS bekerja dengan cara mengklasifikasi data-data pada suatu jaringan. Untuk membantu metode tersebut, untuk penelitian ini digunakan algoritma Relevance Vector Machine untuk mendapatkan nilai akurasi pada serangan DoS dengan menggunakan metode Feature Selection, One-hot Encoding, dan Feature Scaling. Dataset yang digunakan adalah dataset NSL-KDD. Dataset NSL-KDD merupakan dataset yang telah dikembangkan dari dataset pendahulunya yaitu dataset KDDCUP'99 . Berdasarkan hasil penelitian, didapat nilai akurasi sebesar 93.27% ketika menggunakan 9 fitur dan 89.08% untuk 41 fitur.

Kata kunci : DoS, Denial of Service, Intrusion Detection System, Relevance Vector Machine, Feature Selection, One-hot Encoding, Feature Scaling, NSL-KDD, akurasi