

TELKOM UNIVERSITY

Abstract

School of Computing

The Graduate School

Master of Engineering

Semi – supervised Method for Anomaly Intrusion Detection System

by Sofy Fitriani

Saat ini, jumlah serangan terhadap jaringan komputer meningkat yang membuat keamanan menjadi isu penting dalam sistem ini. Karena itu, sistem perlu menjaga keamanan jaringan komputer. Salah satunya adalah dengan menggunakan Intrusion Detection System (IDS). Jenis serangan biasanya memiliki ritme yang berbeda dengan lalu lintas normal. Oleh karena itu, penelitian yang dilakukan adalah pendeteksian intrusi berbasis anomali. Penelitian ini menggunakan metode machine learning, yaitu semi-supervised. Metode ini merupakan kombinasi dari metode supervised dan unsupervised. Biasanya, teknik deteksi biasanya menggunakan satu classifier seperti supervised dan unsupervised saja. Namun, kelemahan supervised adalah metode ini tidak bekerja dengan baik pada serangan tidak diketahui dan memakan waktu untuk mengenali serangan. Akurasi deteksi menjadi lebih buruk ketika menghadapi serangan yang tidak diketahui. Metode unsupervised menunjukkan tidak ada perbedaan yang signifikan dengan metode diawasi dalam akurasi deteksi dan memiliki false positif yang tinggi. Dalam Semi-supervised IDS (SS-IDS) ini menggunakan metode seleksi fitur baru, kemudian dibantu dengan menggunakan penyaringan multikolinearitas pada preprocessing untuk mendapatkan fase training yang lebih baik. Hasil penelitian menunjukkan bahwa metode yang diusulkan menghasilkan false positif rendah yaitu 18,75% dan akurasi tinggi 89,02%.

Keywords : Computer Network, Intrusion Detection System, Semi-supervised, Machine Learning, Network Security