ANALISA PERBANDINGAN ALGORITMA SVM, NAIVE BAYES, DAN POHON KEPUTUSAN DALAM MENGKLASIFIKASIKAN SERANGAN PADA SISTEM PENDETEKSI INTRUSI

Dwi Widiastuti Prihandoko

Program Studi Sistem Informasi
Fakultas IlKom dan Tek. Informasi
Universitas Gunadarma
Jl. Margonda Raya 100 Depok

September 2008

ABSTRAK

Prediksi serangan merupakan tindakan yang diperlukan oleh sebuah sistem pendeteksi intrusi sebagai langkah awal atau antisipasi jika terjadi serangan. Banyak metode yang bisa dilakukan untuk prediksi jenis serangan. Salah satu metode yang digunakan adalah teknik data mining. Tapi tidak semua algoritma data mining memiliki kinerja yang baik dalam mengklasifikasi jenis serangan. Oleh karena itu penelitian ini akan mencoba membandingkan beberapa algoritma.

Ada 41 atribut/variabel yang digunakan untuk mengklasifikasikan jenis serangan. Dari sekian banyak jenis serangan yang terjadi, maka dikelompokkan kedalam empat kelas, yang dikategorikan berdasarkan tujuan akhir yang dicapai oleh suatu serangan. Kategori tersebut antara lain *Probe, DoS, U2R,* dan *R2L*. Data set yang dipakai adalah data set dari KDD Cup 1999, dimana data set ini merupakan data yang direferensikan untuk penelitian kasus IDS.

Perbandingan algoritma dilihat berdasarkan nilai *correctly classified instance, incorrectly classified, kappa statistic, true positif, false positif,* dan *confusion matrix*. Dengan menggunakan alat bantu Waikato Environment for Knowledge Analysis (WEKA) versi 3.4.13, dapat disimpulkan algoritma yang memiliki kinerja yang lebih unggul adalah pohon keputusan.

Kata kunci : *serangan, pohon keputusan, IDS, Klasifikasi, Naive Bayes*