BAB I

PENDAHULUAN

1.1 Latar Belakang

Intrusion Detection adalah sebuah gangguan atau ancaman yang berpotensi melakukan usaha yang disengaja untuk mengakses informasi, memanipulasi informasi, atau membuat sistem menjadi rusak dan tidak dapat digunakan [2]. Untuk menangani hal tersebut, maka dikenalkan *Intrusion Detection System* atau bisa disingkat IDS adalah sebuah sistem yang digunakan untuk mengecek dan mengklasifikasikan jaringan computer melalui *dataset* yang ada untuk mengetahui bahwa aktivitas yang ada termasuk normal atau instrusi [8].

Ada beberapa pendekatan dalam pendeteksian intrusi yaitu *misuse detection* dan *anomaly detection*. *Misuse detection* dikenal juga sebagai *signature-based atau knowledge-based systems*. Pendekatan tersebut memiliki prinsip yang sama dengan kebanyakan *anti-virus software*, dimana *misuse detection* mengenali pola serangan yang telah dikenali sebelumnya, jika ada pola yang terdeksi maka alarm akan langsung berbunyi. *Anomaly detection*, dikenal juga dengan *behaviours-based systems.* Pada pendekatan ini mampu mendeteksi intrusi tanpa harus mengenal pola ancaman terlebih dahulu, jadi ketika ada sedikit saja pola yang tidak normal, maka akan dianggap sebagai ancaman. Pendeteksian ini dapat mengenali instrusi tanpa mempelajarinya terlebih dahulu. Tingkat *false Alarms* nya juga sangat tinggi apabila dibandingkan dengan *misuse detection* [1]. Salah satu metode yang digunakan dalam deteksi anomali dalam IDS adalah dengan menggabungkan metode *rough set* dan Algoritma Genetik [3]. Dalam penelitian ini, *dataset* yang digunakan adalah KDD CUP 1999 dengan banyak data 10%.

Fokus penelitian ini adalah pendeteksian intrusi dengan pendekatan *misuse* dan menggunakan cara klasifikasi untuk mengetahui intrusi. *Misuse* perlu mempelajari pola yang sudah ada, jadi mudah untuk mengenali serangan. Keuntungan utamanya adalah *misuse detection* dapat mengenali langsung ancaman yang diketahui dan tingkat *false Alarms* yang sangat rendah [1]. Untuk mengani masalah klasifikasi tersebut diperlukan metode yang tepat dalam menangani hal tersebut. Metode yang dipilih adalah dengan *Support Vector Machines*. SVM terkenal dengan dapat menangani *2-class question*. Dikarenakan hanya bisa menangani dua kelas, maka diterapkan juga metode *multiclass* SVM. Sebagai solusi untuk menangani kelas yang lebih dari dua jumlahnya. SVM juga relatif tidak sensitif pada jumlah data serta kompleksitas dari klasifikasi tidak bergantung pada dimensi dari ruang. Oleh karena itu SVM memiliki potensi untuk mempelajari pola yang besar [10].

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka perumusan masalah pada penelitian ini adalah:

a. Bagaimana mengimplementasikan metode *Support Vector Machines* untuk deteksi *misuse* pada IDS?
b. Bagaimana analisa performansi dari *Support Vector Machines* untuk kasus *misuse detection* pada IDS berdasarkan DR, TNR, dan Akurasi

1.3 Batasan Masalah

a. Pendekatan yang diterapkan pada penilitian ini adalah *misuse detection*.
b. Pada tugas akhir ini tidak membahas lebih dalam mengenai optimasi koefisien *langrange* (*Sequence Minimal Optimization*).
c. *Dataset* yang digunakan adalah data KDD Cup 1999 10%
d. Sistem yang dibangun bersifat simulasi, menggunakan matlab.
e. Analisa performansi adalah menghitung nilai *Detection Rate*, *True Negative Rate* dan Akurasi.

1.4 Tujuan

a. Mengimplementasikan metode *Support Vector Machines* untuk deteksi *misuse* pada IDS.
b. Menganalisa performansi dari metode *Support Vector Machines* untuk *misuse* detection pada IDS dan variable-variabel yang mempengaruhinya.

1.5 Metodologi Penyelesaian Masalah

1. Studi Literatur
   Mencari sumber referensi mengenai data mining, *genetic algorithm*, *support vector machines* dan kombinasi dari kedua metode tersebut dan segala hal berhubungan dengan masalah performansi IDS.
2. Pengumpulan Data
   Data yang digunakan adalah dataset KDD Cup 1999 10%.
3. Perancangan Sistem
   Pemaparan secara detil mulai dari perancangan sistem, proses kerja sistem, input-output, dan batasan angka performansi.
4. Implementasi
   Mengimplementasikan sistem berdasarkan perancangan sistem yang telah dibuat sebelumnya menggunakan matlab.
5. Pengujian Sistem
   Melakukan analisis performansi dari hasil pengujian simulasi.
6. Analisa performansi dan Pengambilan Kesimpulan
   Menganalisa performansi berdasarkan hasil implementasi serta menarik kesimpulan.
7. Penyusunan Laporan Tugas Akhir
   Menyusun laporan tugas akhir berdasarkan pada hasil penelitian.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN
Bab ini berisi latar belakang, rumusan masalah, tujuan, batasan masalah, metodologi penelitian, sistematika penulisan, dan jadwal penelitian

BAB II LANDASAN TEORI
Bab ini berisi teori-teori yang mendukung pengembangan sistem
BAB III ANALISA KEBUTUHAN DAN PERANCANGAN SISTEM
Bab ini berisi analisa kebutuhan dari sistem serta perancangan sistem sesuai dengan kebutuhan yang sudah dianalisa
BAB IV IMPLEMENTASI DAN ANALISA HASIL PENGUJIAN
Bab ini berisi implementasi dari sistem yang telah dibuat serta hasil analisa dari pengujian
BAB V KESIMPULAN DAN SARAN
Bab ini berisi kesimpulan mengenai penelitian serta saran pengembangan penelitian di masa yang akan datang