BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada perkembangan teknologi komputer seperti internet sekarang, keamanan merupakan aspek penting dari suatu sistem. Saat ini hampir seluruh kalangan masyarakat dapat menggunakannya untuk mendapatkan informasi yang luas dan beragam dari seluruh dunia. Banyak kalangan sering kali tidak bertanggung jawab dalam menggunakan teknologi internet saat ini, yang sering kali menyebabkan kerugian. Hal ini pula yang menyebabkan munculnya serangan-serangan di dalam suatu jaringan komputer yang tentunya merugikan. Serangan yang terjadi ini bisa disebut sebagai anomali trafik dimana dapat terjadi *flash-crowd* atau karena serangan *flooding* trafik seperti *Denial of Service* (Dos) dan *Distributed Denial of Service* (DDoS).

Denial of Service (DoS) dan *Disributed Denial of Service* (DDoS) merupakan bentuk serangan *flooding* yang berusaha membuat suatu *host* atau *service* menjadi tak dapat diakses oleh user yang berhak. Sasaran serangan oleh DoS/DDoS adalah *link/bandwidth* untuk membuat sumber daya bandwidth penuh dan sumber daya komputasi pada server agar sistem pengolah kehabisan sumber daya yang berujung oleh jaringan *down* atau *crash* [2]. Sedangkan *flashcrowd* adalah kejadian yang tidak dapat diprediksi tetapi akan terjadi peningkatan akses secara dramatis/tinggi ke suatu server karena suatu kejadian seperti bencana alam, peluncuran produk, *breaking news*, dll. Metode deteksi menggunakan anomali trafik dikembangkan karena dapat mendeteksi serangan baru yang tidak sama dengan pola normal.

Dalam mendeteksi dan mengatasi serangan di jaringan komputer, dikenal dengan istilah *Intrusion Detection System (IDS).* Pada *Intrusion Detection System (IDS)* dikenal 2 metode yang sering digunakan yaitu *intrusion signature* dan *traffic anomaly based* yang berfungsi untuk mengenali serangan yang terjadi [3]. Pada

Tugas Akhir ini penulis menggunakan *traffic anomaly based* untuk mendeteksi serangan dimana keunggulannya tidak memerlukan *database* serangan. Kekurangan dari *traffic anomaly based* ini terletak pada tingkat kesalahan (*false positive rate)* tinggi jika tidak dibuat dengan baik, maka untuk mengatasi kekurangan tersebut kami menggunakan data mining teknik statistik [4].

Dalam pengembangannya sistem deteksi anomali banyak pendekatan untuk mengetahui pola trafik normal sebagai acuan deteksi anomali trafik. Penelitian Tugas Akhir ini menggunakan teknik statistik *covariance matrix* yang tidak mengabaikan hubungan dan ketergantungan antar fitur yang dapat menyebabkan kesalahan deteksi. Deteksi anomali trafik menggunakan *covariance matrix* menggunakan metode *landmark window* bertujuan untuk memperoleh nilai *detection rate* yang tinggi dan *false positive rate* yang rendah.

1.2 Tujuan

Tujuan dari Tugas akhir ini pada poin-poin berikut:

a. Menghasilkan metode sistem deteksi anomaly trafik dengan metode statistik *Covariance Matrix* menggunakan *Support Vector Machine* (SVM) untuk proses klasifikasi.
b. Mengukur tingkat keakuratan metode yang digunakan untuk parameter nilai *Detection Rate* (DR) dan *False Positive Rate* (FPR).
c. Membandingkan tingkat keakuratan dan kompleksitas sistem deteksi menggunakan data homogen dan heterogen.

1.3 Rumusan Masalah

Rumusan masalah dalam pembuatan Tugas Akhir ini adalah seperti yang dijelaskan dibawah ini:

1. Bagaimana menghasilkan metode sistem deteksi anomali trafik dengan metode statistik *Covariance Matrix* menggunakan *Support Vector Machine* (SVM) umtuk proses klasifikasi.
2. Bagaimana mengukur tingkat keakuratan metode yang digunakan untuk parameter nilai *Detection Rate* (DR) dan *False Positive Rate* (FPR).

3. Bagaimana membandingkan tingkat keakuratan metode klasifikasi yang digunakan menggunakan data homogen dan heterogen dengan *noise*.

1.4 Batasan Masalah

Tugas akhir ini mempunyai batasan masalah yaitu :

1. Menggunakan metode statistik *Covariance Matrix*.
2. Menggunakan teknik *Support Vector Machine* (SVM) untuk proses klasifikasi.
3. Analisis dilakukan dengan menggunakan tools / software Matlab.
4. Menggunakan dataset KDD Cup 99 *real time* yang sudah terekam (ter-*capture*) berupa *network log connection* untuk trafik normal dan serangan DDoS, sedangkan untuk trafik *flash-crowd* menggunakan dataset *worldcup 98.*
5. Tidak membahas mengenai pencegahan *(prevention)* terhadap serangan yang ada pada jaringan.

1.5 Metodologi Penyelesaian Masalah

Penelitian Tugas Akhir ini dilakukan dengan metodologi sebagai berikut:

1. Studi Literatur

   Studi Literatur ini dimaksudkan untuk memahami dan mempelajari konsep dan teori yang berkaitan dengan *covariance matrix* menggunakan landmark untuk deteksi anomali trafik yang hasilnya digunakan dalam acuan dasar teori dalam pembuatan tugas akhir ini.
2. Pengumpulan data

   Pengumpulan data yang digunakan adalah pengumpulan berbagai dataset real traffic yang digunakan untuk mendeteksi serangan anomali trafik seperti *worldcup98* dan *KDDCUP 99*. Dataset tersebut merupakan lingkungan implementasi sistem deteksi yang berupa data *non-realtime (captured).*
3. Perancangan

Setelah mengumpulkan data-data yang diperlukan, maka akan dilakukan perancangan proses dalam deteksi anomali trafik yang dapat dilakukan dalam tahap penelitian dan membuat data training dan data test.

4. Preprocessing

   Data *preprocessing* merupakan strategi agar data cocok digunakan untuk proses pengujian. *Preprocessing* dari pengujian ini yaitu mengambil pola data normal yang terjadi pada trafik jaringan. Deteksi anomali based memiliki kelebihan yaitu tidak perlu database serangan untuk deteksi serangan baru, namun akan menjadi kelemahan jika proses *preprocessing* ini tidak di buat dengan benar yang akan mengakibatkan *false positive rate* yang tinggi bila pola normal tidak di deteksi secara akurat. Maka dari itu dibuatlah karakteristik fitur-fitur agar dapat menjadi acuan dalam mendeteksi serangan yang terjadi.

5. Pengujian Sistem

   Pengujian dilakukan dengan mengukur tingkat keakuratan yang dihasilkan oleh sistem deteksi dibandingkan dengan karakter normal dalam mendapatkan hasil *detection rate* dan *false positive rate*. Melalui pengujian dapat dilihat metode yang digunakan efektif atau tidak.

6. Analisis hasil pengujian

   Dari tahap pengujian sistem yang dilakukan sebelumnya, dilakukan analisis terhadap faktor – faktor yang mempengaruhi kinerja.

7. Penyusunan Laporan Tugas Akhir

   Pada tahap ini dilakukan penyusunan laporan akhir dan pengumpulan dokumentasi yang diperlukan, format laporan mengikuti kaidah penulisan yang benar dan yang sesuai dengan ketentuan – ketentuan yang telah ditetapkan oleh institusi.

1.6 Sistematika Penulisan TA

Penelitian ini secara keseluruhan dapat disusun secara struktural sebagai berikut:

BAB I PENDAHULUAN

Bab ini membahas latar belakang, tujuan, manfaat, rumusan masalah, batasan masalah, metode penyelesaian masalah, dan sistematika penulisan.

BAB II DASAR TEORI

Bab ini membahas teori-teori pendukung yang berkaitan dengan penelitian ini.

BAB III PERANCANGAN

Bab ini membahas tentang proses yang akan digunakan pada sistem ini.

BAB IV PENGUJIAN DAN ANALISIS

Bab ini berisi pengujian dari rancangan terhadap metode yang di purpose yang telah di buat sebelumnya.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari hasil penelitian dan saran-saran berupa tindak lanjut yang bisa dilakukan pada pengembangan selanjutnya