BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan komputer saat ini mulai banyak diminati oleh banyak kalangan. Jika dilihat dari segi negatifnya, maka akan semakin banyak jenis penyusupan ataupun serangan yang dapat dilakukan dalam suatu jaringan melihat perkembangan teknologi yang semakin canggih dan modern. Untuk itu suatu sistem keamanan jaringan harus dapat melindungi data terhadap serangan atau penyusup di jaringan oleh pihak yang tidak berwenang.

Bentuk serangan dari luar jaringan dapat bersifat merugikan seperti pengambilan data/informasi tanpa izin. Jenis serangan juga dapat berkembang semakin luas seiring dengan perkembangan teknologi. Contoh jenis serangan yang merugikan pada jaringan antara lain: *DOS attack, CGI attacks, SMB probes, OS fingerprinting*, dll. Serangan-serangan tersebut tentu sangat merugikan jika tidak dapat terdeteksi oleh jaringan komputer yang sedang digunakan. Pihak luar akan mengambil keuntungan tanpa jejak pada suatu jaringan.

Dalam *survey* [1] sistem deteksi anomali trafik, dilakukan suatu pendekatan ke masalah deteksi serangan pada jaringan komputer atau dikenal sebagai *Intrusion Detection System* (*IDS*). Penerapan *IDS* sebagai *security tools* yang akan mendeteksi intrusi-intrusi, pemindaian, penyerangan ataupun penyusupan serta berbagai ancaman lain pada lalu lintas jaringan seperti anomali trafik. Kekurangan dari penelitian yang sudah ada, deteksi anomali trafik masih dilakukan secara *offline*. Dibutuhkan sistem deteksi secara *real-time*, sehingga saat terdapat aktifitas yang mencurigakan pada jaringan akan langsung di-*generate* oleh sistem.

Oleh karena itu dibutuhkan suatu sistem untuk menganalisa adanya anomali trafik pada suatu jaringan secara *real-time*. Hasil akhir sistem deteksi ini berupa pengelompokan data trafik normal dan trafik anomali.

1.2 Rumusan Masalah

Masalah aliran data telah banyak diteliti dalam beberapa tahun terakhir dengan menggunakan sejumlah aplikasi yang relevan [4,5,6,7,8]. Penelitian tentang *data stream clustering* dengan menggunakan berbagai algoritma yang berbeda, misalnya [4] menganggap bahwa pengelompokan harus dihitung atas seluruh aliran data. Metode tersebut hanya melihat masalah pengelompokan aliran data sebagai varian dari algoritma pengelompokan satu masukan.

Dalam penelitian ini akan dibentuk perancangan sistem untuk deteksi anomali trafik dengan algoritma *clustream* dengan parameter berdasarkan waktu per-2 detik di mana proses *clustering* dibagi menjadi dua tahap yakni *micro-clustering* dan selanjutnya akan diolah kembali melalui tahap *macro-clustering*.

1.3 Tujuan

Dengan merujuk pada rumusan masalah di atas, maka tujuan yang dibahas pada penelitian ini adalah untuk mengimplementasikan algoritma *clustream* berdasarkan waktu untuk mendeteksi anomali trafik serta dapat mengelompokan trafik normal dan trafik anomali dengan nilai akurasi, *detection rate* tinggi (>90%) dan *false positive rendah* (0%).

1.4 Batasan Masalah

Adapun batasan masalah pada tugas akhir ini, yaitu:

a. Menggunakan sistem operasi Linux Ubuntu
b. Menggunakan Python *IDS Tools*
c. Pengelompokan berdasarkan waktu per-2 detik
d. Pengujian menggunakan *ping* normal dan *ping flood*
e. Menggunakan enam fitur (*packet_size, time_interval, counter_paket, count_tcp, count_udp, count_icmp*) sebagai masukan pada sistem deteksi
f. Menggunakan algoritma *clustream* dalam proses *clustering*
g. Hasil keluaran hanya dapat mengelompokan trafik normal dan trafik anomali, tidak mengklasifikasikan jenis anomali dan tidak berupa pencegahan.
h. Ruang lingkup jaringan yang dideteksi adalah *LAN (Local Area Network)*

1.5 Metodologi Penyelesaian Masalah

Pada penelitian yang telah dilaksanakan ini, terdapat beberapa tahapan hingga didapatkan hasil akhir yang diinginkan. Berikut tahapan-tahapan tersebut:

1.5.1 Studi Literatur

Tahap mencari materi dan referensi pendukung untuk pembuatan tugas akhir, seperti mencari jurnal terkait algoritma clustream, mempelajari penggunaan *IDS Tools* serta membaca dan mereview jurnal internasional yang berkaitan dengan topik tugas akhir.

1.5.2 Pengumpulan Data

Pengumpulan data dilakukan dengan men-*generate* trafik jaringan agar didapat data trafik yang akan diolah oleh algoritma clustream.

1.5.3 Perancangan Sistem

Merancang sistem deteksi yang akan dibuat seperti *flowchart* sistem deteksi, *flowchart* algoritma clustream tahapan dari awal trafik masuk hingga diolah menjadi kelompok trafik normal dan trafik anomali.

1.5.4 Pengujian Sistem

Pada tahap ini dilakukan pengujian terhadap sistem deteksi yang telah dibuat. Pengujian berupa penghitungan nilai akurasi dari hasil deteksi *stream traffic*.

1.5.5 Analisis Pengujian

Dari tahap pengujian yang telah dilakukan sebelumnya, dilakukan analisis terhadap keakuratan dari sistem dalam mendeteksi *stream traffic*.

1.5.6 Penyusunan Laporan

Pada tahap ini dilakukan penyusunan laporan akhir dan pengumpulan dokumentasi yang diperlukan dengan mengikuti format laporan yang telah ditetapkan oleh universitas.

1.6 Sistematika Penulisan

Sistematika dalam penulisan tugas akhir ini dibagi menjadi beberapa bagian. Tiap-tiap bagian menjelaskan langkah demi langkah dalam pengerjaan tugas akhir ini. Berikut adalah bagian tersebut:

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang dari pembuatan sistem, rumusan masalah, tujuan dan batasan masalah dari judul tugas akhir ini. Serta metodologi penelitian dan sistematika penulisan yang digunakan dalam tugas akhir ini.

BAB II TINJAUAN PUSTAKA

Bab ini berisi tentang penjelasan teori-teori terkait yang digunakan dalam perancangan sistem yang dibuat untuk tugas akhir ini. Teori-teori tersebut bersumber dari jurnal, buku, maupun artikel resmi dari internet.

BAB III PERANCANGAN SISTEM

Bab ini membahas mengenai semua hal yang berkaitan dengan proses pemodelan, perancangan sistem, pengerjaan dan penyelesaian sistem, serta alur dari algoritma yang digunakan untuk sistem yang dibuat.

BAB IV PENGUJIAN DAN ANALISIS

Bab ini menjelaskan tentang kinerja sistem dan pengujian-pengujian yang dilakukan pada sistem. Dari setiap hasil pengujian akan dilakukan analisis dan menarik kesimpulan dari hasil analisis tersebut.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan akhir dari perancangan, pengujian dan analisis yang telah dilakukan serta saran dan harapan untuk pengembangan lebih lanjut.