

BAB I

PENDAHULUAN

1.1 Latar Belakang

Internet adalah sebuah sistem dari seluruh jaringan komputer yang saling terhubung. Internet telah mengalami banyak sekali perkembangan dan telah menjadi salah satu kebutuhan bagi masyarakat. Dalam sebuah survey yang dimuat dalam [1] terkait penggunaan internet di masyarakat menunjukkan bahwa pengguna internet di dunia telah mencapai 1,5 Milyar jiwa atau sekitar 20% dari 6,5 Milyar penduduk bumi.

Seiring dengan perkembangan internet yang semakin pesat, berdampak pula pada tipe serangan yang semakin beragam. Namun dengan adanya suatu sistem keamanan pada jaringan, salah satunya Firewall yang dapat mendeteksi dan mengklasifikasi tipe serangan tersebut sehingga dapat memudahkan untuk menentukan solusi yang paling tepat mengatasi tiap tipe serangan.

Pada penelitian ini lebih memfokuskan pada pendeteksian dan pengklasifikasian tipe serangan pada trafik jaringan. Metode yang digunakan dapat membedakan antara trafik normal dan trafik serangan serta mengklasifikasikan tipe dari serangan tersebut. Fitur yang dijadikan acuan dari penelitian ini adalah fitur pada KDDCUP 1999 yang telah sering digunakan dalam berbagai penelitian. Metode yang digunakan untuk pendeteksian adalah clustering, sedangkan metode untuk menentukan tipe serangan adalah classification. Algoritma yang digunakan untuk clustering adalah Minkowski Weighted K-Means, sedangkan algoritma untuk classification adalah Decision Tree.

1.2 Perumusan Masalah

Fokus pada tugas akhir ini adalah metode yang digunakan dalam melakukan *clustering* menggunakan Algoritma *Minkowski Weighted K-means* dan pelabelan data menggunakan metode *Decision Tree*. Sehingga dapat dirumuskan masalah sebagai berikut:

1. Bagaimana cara menghasilkan *datastream* menggunakan NS3.
2. Bagaimana cara melakukan *clustering* sehingga data dapat dikelompokkan.
3. Bagaimana cara memberikan label pada masing – masing data.
4. Bagaimana membentuk suatu sistem deteksi tipe serangan dengan menggunakan metode *clustering* dan *classification*.

1.3 Tujuan

Tujuan yang ingin dicapai dari penelitian tugas akhir ini antara lain:

1. Membuat sebuah sistem deteksi tipe serangan dengan menggunakan NS3 sebagai sumber trafik.
2. Membuat sebuah sistem deteksi tipe serangan dengan menggunakan algoritma *Minkowski Weighted K-means* dan *Decision Tree* untuk membentuk *cluster* dan memberikan label pada masing – masing data.
3. Menguji keakuratan dari algoritma berdasarkan output label masing – masing data yang dihasilkan.

1.4 Batasan Masalah

Hal-hal yang dibatasi dalam penelitian Tugas akhir ini adalah :

1. Menggunakan *raw data* hasil dari NS3
2. Menggunakan Algoritma *Minkowski Weighted K-means* dan *Decision Tree* dalam proses *clustering* dan *classification* data.
3. Menggunakan fitur data berdasarkan *dataset* KDDCUP 1999.
4. Hasil keluaran berupa label masing – masing data.

1.5 Metodologi Penyelesaian Masalah

Metodologi penelitian yang digunakan adalah:

1. STUDI LITERATUR

Melakukan pencarian referensi dan materi yang berkaitan dengan pengelompokan data dan klasifikasi serangan pada jaringan. Selain itu juga melakukan pencarian materi dan referensi yang berkaitan dengan network simulator 3, pemrograman python, dan algoritma yang digunakan yaitu minkowski weighted k-means dan decision tree.

2. PENGUMPULAN DATA

Pada tahap ini melakukan pengumpulan dan analisis dataset yang akan diolah sistem deteksi. Analisis yang dilakukan berupa pengecekan apakah dataset sudah sesuai dengan kebutuhan sistem deteksi yang dibuat. Dataset yang digunakan diantaranya dataset hasil dari PCA dan sampling, dataset hasil clustering dan KDDCup 1999.

3. PERANCANGAN KEBUTUHAN SISTEM

Melakukan perancangan sistem deteksi yang dapat mengelompokkan data dan mengklasifikasikannya serta dapat diintegrasikan dengan Network Simulator 3

4. PENGUJIAN SISTEM

Pada tahap ini sistem yang telah dibangun akan diuji menggunakan dataset yang telah disiapkan pada tahap sebelumnya. Hasil dari pengujian diantaranya kemampuan sistem untuk mendeteksi dan mengklasifikasi serangan pada dataset yang diujikan.

5. ANALISIS HASIL PENGUJIAN

Pada tahap ini akan dilakukan analisa terhadap parameter yang mempengaruhi hasil dari pengujian diantaranya *detection rate* dan *accuracy*.

6. PENYUSUNAN LAPORAN TUGAS AKHIR

Pada tahap ini semua data dan hasil dari penelitian akan dibuat menjadi sebuah laporan dengan sistematika penulisan yang sesuai dengan ketentuan institusi.

1.6 Sistematika Penulisan TA

Adapun sistematika penulisan pada Tugas Akhir ini adalah:

BAB I PENDAHULUAN

Pada bab ini membahas tentang alasan dilakukannya penelitian serta identifikasi masalah pada penelitian. Bagian - bagian yang dibahas pada bab ini adalah latar belakang masalah, rumusan masalah, tujuan, batasan masalah, metodologi penyelesaian masalah, dan sistematika penulisan.

BAB II KAJIAN PUSTAKA

Pada bab ini berisi penjelasan tentang teori – teori yang berkaitan dengan penelitian seperti konsep dasar clustering, algoritma Minkowski Weighted K-Means, algoritma Decision Tree serta istilah – istilah yang berkaitan dengan topik penelitian.

BAB III PERANCANGAN DAN SIMULASI SISTEM

Pada bab ini berisi tentang penjelasan sistem dan komponen – komponen yang diperlukan pada pengujian.

BAB IV PENGUJIAN DAN ANALISIS

Pada bab ini berisi tentang pengujian accuracy dari sistem yang dibuat dan analisis terhadap hasil dari pengujian.

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan dari penelitian yang dilakukan berdasarkan hasil dari pengujian dan analisis serta rekomendasi untuk penelitian selanjutnya.