# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Teknologi pada era sekarang sudah berkembang dengan pesat, terutama penggunaan internet. Dengan maraknya internet tidak sedikit pengguna internet melakukan serangan ke pengguna lain untuk kepentingan pribadi. Serangan tersebut mulai dari yang sederhana seperti percobaan membobol *password* hingga serangan *ping* untuk membanjiri *server* sampai *server* tersebut down.

Banyak solusi yang ada untuk menyelesaikan masalah-masalah tersebut. Salah satunya adalah menggunakan *Firewall*. Penggunaan *firewall* didefinisikan secara sederhana adalah memblok paket masuk yang tidak teridentifikasi oleh pengguna. Kelemahannya adalah pengguna harus dapat membedakan sendiri trafik jaringan mana yang bebas dari serangan.

Pada penelitian ini mengembangkan metode pada *Firewall* dengan menambahkan beberapa fitur dan automasi sistem. Dua fitur utama yaitu mendeteksi dan mengklasifikasikan tipe serangan yang ada pada trafik jaringan. Tahap mengatasi serangan tersebut dilakukan secara otomatis menggunakan *remote router.*

Penelitian ini hanya mendeteksi apakah ada serangan pada trafik jaringan. Dengan menggunakan beberapa fitur berdasarkan *dataset* KDDCUP 1999, dilakukan identifikasi paket anomali pada trafik jaringan. Metode yang diguakan untuk mendeteksinya adalah dengan *clustering*. Data yang dikelompokkan diambil secara *stream* yang merupakan data yang datang secara terus-menerus pada trafik jaringan. Algoritma yang digunakan untuk *clustering* adalah *Incremental K-means*.

## 1.2 Perumusan Masalah

Banyak penelitian tenetang deteksi anomali telah dilakukan dan menghasilkan hasil yang akurat [1] [2] [3]. Pada penelitian sebelumnya *dataset* yang digunakan berupa *dataset* yang sudah ada atau *dataset* hasil *monitoring* jaringan pada jangka waktu yang telah ditentukan. Data tersebut kemudian diproses menggunakan berbagai metode dan hasil data tersebut dianalisa. Dari penelitian tesebut dapat dilakukan modifikasi untuk mendeteksi anomali secara *real-time* dan mengimplementasikan *machine-learning* untuk otomasi sehingga hasil deteksi dapat langsung ditanggulangi. Berikut adalah rincian dari rumusan masalah pada penelitian ini:

1. Melakukan pengambilan paket secara langsung/*online*
2. Mengkonversikan raw data menjadi fitur-fitur secara langsung/*online*
3. Mengimplementasikan algoritma Incremental K-means untuk mendeteksi paket-paket anomali
4. Menyimpan fitur-fitur milik paket-paket yang telah terdeteksi sebagai anomali

## 1.3 Tujuan

Tujuan yang dihasilkan dari penelitian ini adalah sebuah sistem yang dapat mendeteksi anomali pada *stream* trafik jaringan menggunakan beberapa fitur acuan dengan metode *clustering data* algoritma *Incremental K-means* dan menyimpan *dataset* yang telah terdeteksi tersebut. Adapun rincian tujuan dari penelitian ini sebagai berikut:

1. Melakukan pengambilan paket secara langsung/*online*
2. Mengkonversikan *raw data* menjadi fitur-fitur secara langsung/*online*
3. Mengimplementasikan algoritma *Incremental K-means* untuk mendeteksi paket-paket anomali
4. Menyimpan fitur-fitur milik paket-paket yang telah terdeteksi sebagai anomali

## 1.4 Batasan Masalah

Pada penelitian ini terdapat batasan masalah sebagai berikut:

1. *Clustering* dilakukan pada data yang diekstrak dari paket data yang telah dikonversi menjadi data numerik.
2. Paket-paket yang diambil merupakan paket-paket data yang masuk atau keluar dari PC.
3. Pemrograman dilakukan dengan bahasa *Java* dan *IDE NetBeans* sebagai *compiler*.
4. Paket di-*capture* menggunakan JPCap, seubah *library* pada *Java*.
5. Menggunakan *training data* KDDCUP 1999 sebagai parameter acuan.
6. Program tidak mendefinisikan jenis anomali.
7. Pengujian menggunakan trafik normal, trafik yang diserang *syn flood* dan *ping flood.*

## 1.5 Metodologi Penyelesian Masalah

1. Studi Literatur

   Melakukan pencarian referensi dan materi yang berkaitan dengan penelitian seperti dasar teori, penelitian sebelumnya, dan algoritma.
2. Analisis dan Perancangan Kebutuhan Sistem

   Melakukan perancangan sistem untuk *clustering* dan *preprocessing* yang dilakukan secara *online*.
3. Implementasi Sistem

   Mennyatukan sistem *preprocessing* yang dilakukan secara *online* dengan proses *clustering* untuk mendeteksi paket anomali.
4. Pengujian Sistem

   Hal-hal yang diuji pada sistem adalah berhasil atau tidaknya mendeteksi serangan.
5. Analisis hasil pengujian

   Tahap ini dilakukan analisis dari hasil pengujian tentang hal-hal yang mempengaruhi hasil deteksi dan kemampuan deteksi *online* sistem.
6. Penyusunan Laporan Tugas Akhir

Tahap ini dilakukan penyusunan laporan tugas akhir. Adapun penyusunan laporan ini mengikuti *format* atau sistematika penulisan dan kaidah yang sesuai yang telah ditetapkan oleh institusi.

BAB I PENDAHULUAN

Pada bab ini membahas tentang hal-hal yang mendasari dilakukannya penelitian serta mengidentifikasi masalah penelitian. Bagian-bagian yang terdapat pada bab ini adalah latar belakang masalah, rumusan masalah, tujuan, batasan masalah, metodologi penyelesaian masalah, dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab landasan teori, diuraikan tentang teori – teori penunjang penelitian seperti prinsip dasar *clustering,* algoritma yang digunakan dan istilah –istilah yang dianggap penting terkait dengan judul.

BAB III DESAIN DAN PERANCANGAN

Bab perancangan dan metodologi penelitian menjelaskan desain dan perancangan dalam menerapkan sistem deteksi pada *host*. Bagian dari bab ini adalah Perancangan sistem dan Impelementasi dan penjelasan mulai dari input sampai output sistem.

BAB IV PENGUJIAN DAN ANALISIS

Bab ini menjelaskan tentang pengujian dan memaparkan analisis dari hasil pengujian. Adapun analisis percobaan yang diharapkan adalah secara kualitatif dan kuantitatif. Pengamatan dan analisis dilakukan terhadap parameter kemampuan sistem mendeteksi paket anomali.

# BAB V KESIMPULAN

Bab ini berisi tentang kesimpulan hasil penelitian baik perancangan maupun analisa yang diperoleh dan juga saran serta harapan untuk pengembangan selanjutnya.