BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam beberapa tahun terakhir *interconnection network* atau internet mengalami perkembangan yang pesat. Internet adalah jaringan yang terdiri dari milyaran komputer yang ada di seluruh dunia, dengan menggunakan internet semua orang dapat mengakses banyak informasi yang telah disediakan. Oleh karena itu terjadi trafik yang tinggi di dalam suatu jaringan komputer. Trafik yang tinggi dapat disebabkan oleh suatu serangan. Jenis serangan yang umum dilakukan adalah *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS) [1].

Denial of Service (Dos) merupakan suatu bentuk serangan *flooding* yang bertujuan membuat suatu sumber (*resource)* yang dimiliki suatu komputer target habis dan tidak dapat memberikan layanan kepada pengguna yang sah. *Distributed Denial of Service* (DDoS) adalah salah satu jenis serangan DoS yang menggunakan banyak *host* penyerang baik itu menggunakan komputer yang di dedikasikan untuk melakukan penyerangan atau komputer yang "dipaksa" menjadi zombie untuk menyerang sebuah *host* target dalam sebuah jaringan. Target serangan dalam DoS dan DDoS adalah *bandwidth*, dimana *bandwidth* dalam sebuah jaringan tersebut akan dibuat penuh dan sumber daya komputasi pada server maupun node jaringan habis dan akhirnya *crash* atau *down* sehingga tidak dapat lagi memberikan *service* jaringan.

Oleh sebab itu, diperlukan suatu sistem untuk mendeteksi *(Intrussion Detection System)* anomali trafik di jaringan komputer. Salah satu teknik yang dapat digunakan untuk mendeteksi anomali trafik yaitu *clustering based*. Pada Tugas Akhir ini, algoritma *clustering Denstream* yang merupakan pengembangan

dari algoritma DBSCAN digunakan untuk melakukan proses deteksi. Kemudian, dilakukan proses penganalisaan data ke dalam struktur kelompok-kelompok data yang memiliki kesamaan dengan algortima *Denstream* modifikasi yang digunakan.

1.2 Perumusan Masalah

Clustering adalah metode penganalisaan data, yang sering dimasukan sebagai salah satu Metode *Data Mining*, sebuah proses untuk mengelompokan data ke dalam beberapa *cluster* atau kelompok sehingga data dalam satu *cluster* memiliki tingkat kemiripan yang maksimum. Implementasi *clustering* dapat diterapkan di berbagai bidang.

Salah satu metode *clustering* adalah *density-based clustering*. *Density-based clustering* merupakan algoritma yang berdasarkan kerapatan suatu data dan mengelompokannya menjadi beberapa *cluster*. *Density-based clustering* diciptakan untuk menemukan *Cluster* yang berbentuk acak dan terdapat banyak *noise* didalamnya. Beberapa algoritma yang termasuk *Density-based clustering : DBSCAN (Density-based Spatial Clustering of Application with Noise) , OPTICS(Ordering Point to Identify the Clustering Structure), DENCLUE(Density-based Clustering).* Namun masih terdapat kekurangan pada *density-based clustering* yaitu ketika jenis data yang akan dilakukan *clustering* merupakan jenis data stream maka *density-based clustering* akan sulit dalam penentuan *cluster* karena sifat ketidakpastian dari data stream yang menyebabkan sulitnya penentuan kerapatan pada suatu *cluster.*

Dalam penelitian ini kami akan menggunakan algoritma pengembangan dari *density-based* DBSCAN yang disebut algoritma *Denstream*. Algoritma *Denstream* sendiri menggunakan teknik *micro-cluster* yang digunakan untuk mengindentifikasi *cluster* beserta atribut didalamnya dan memproses banyak *outlier* dalam sebuah *data stream.*

Akan tetapi, dalam penelitian ini algoritma *Denstream* memiliki beberapa kekurangan. *Denstream* memiliki keterbatasan dalam memproses *data stream* yang memiliki ukuran besar.

Penelitian Tugas Akhir ini menggunakan algoritma *Denstream* untuk melakukan proses deteksi *(Intrussion Detection System)* terhadap anomali trafik pada jaringan komputer. Fokus penelitian ini yaitu memodifikasi pada proses *generating cluster*. Pada penelitian ini proses *generating cluster* dilakukan dalam periode tertentu hal ini akan menyebabkan sistem menjadi lebih stabil dan dapat mengatasi *data stream*.

Berdasarkan uraian diatas, maka masalah yang akan dibahas pada penelitian Tugas Akhir ini, sebagai berikut :

1. Perancangan sistem deteksi anomali trafik menggunakan algoritma *clustering Denstream*.
2. Penerapan generating cluster secara periodik dalam algoritma *clustering Denstream.*
3. Proses *Prepocessing* untuk mendapatkan fitur dari dataset yang digunakan untuk kemudian diolah dalam sistem deteksi anomali trafik menggunakan algoritma *Denstream*.
4. Analisis dan performansi algoritma Denstream dalam proses deteksi anomali trafik.

1.3 Tujuan

Tugas Akhir mengenai penyesuaian proses generating cluster secara periodik pada algoritma Denstream untuk analisis sistem deteksi anomali trafik memiliki beberapa tujuan, yaitu :

1. Merancang sistem deteksi anomali trafik menggunakan algoritma *clustering Denstream.*

2. Proses preprocessing untuk mendapatkan fitur dari dataset yang digunakan kemudian diolah dalam sistem deteksi anomali trafik menggunakan algoritma Denstream.
3. Menerapkan metode penyesuain proses generating cluster secara periodik dalam algoritma *Clustering Denstream.*
4. Analisis metode penyesuaian proses *generating cluster* secara periodik serta performansi algoritma denstrean dalam proses deteksi anomali trafik dengan parameter uji *Purity*.

1.4 Batasan Masalah

Berikut merupakan hal-hal yang dibatasi dalam penelitian Tugas Akhir ini :

1. Membahas tentang sistem deteksi anomali trafik *(Intrussion Detection System)*
2. Membahas tentang metode yang digunakan untuk melakukan proses deteksi anomali trafik.
3. Metode yang digunakan yang adalah algortima clustering *Denstream*
4. Menggunakan teknik pengembangan dari algoritma *Denstream* pada proses generating cluster.
5. Analisis dilakukan dengan menggunakan tools / software berbasis java (javascript programming).
6. Menggunakan dataset (DARPA 1998) *real time* yang sudah terekam (ter-*capture*) berupa *network log connection* untuk trafik normal dan serangan DDoS.
7. Tidak membahas mengenai pencegahan *(prevention)* terhadap serangan yang terdapat pada jaringan.

1.5 Metodologi Penyelesaian Masalah

Metodologi penelitian yang digunakan adalah:

a. Studi literatur, yaitu mempelajari literatur dan teori yang ada sesuai dengan permasalahan yang akan dibahas meliputi, konsep deteksi anomali trafik *(Intrussion Detection System)*, teori serangan *DDoS*, konsep algoritma *clustering Denstream,* dan teori mengenai uji performansi menggunakan parameter *Purity*.

b. Analisis terhadap kebutuhan dan pemodelan sistem untuk proses deteksi anomali trafik.

c. Perancangan dan analisis menggunakan tools untuk sistem deteksi anomali trafik.

d. Uji performansi dan analisis hasil penelitian.

e. Pembuatan laporan dari hasil penelitian.

1.6 Sistematika Penulisan TA

Adapun sistematika penulisan pada Tugas Akhir ini adalah :

BAB I PENDAHULUAN

Berisi tentang latar belakang penelitian, rumusan masalah, batasan masalah, tujuan penelitian, metodologi penelitian, dan sistematika penelitian.

BAB II TINJAUAN PUSTAKA

Berisi tentang penjelasan mengenai deteksi anomali trafik *(Intrussion Detection System)*, penjelasan mengenai serangan DDoS, penjelasan mengenai konsep algoritma *clustering Denstream*, penjelasan mengenai parameter uji.

BAB III PERANCANGAN SISTEM

Berisi tentang perancangan sistem yang akan dibangun.

BAB IV PENGUJIAN DAN ANALISIS

Berisi tentang pengujian performansi dan analisis hasil penelitian.

BAB V KESIMPULAN DAN SARAN

Berisi kesimpulan dari hasil penelitain yang dilakukan dan rekomendasi untuk penelitian berikutnya.