BAB I
PENDAHULUAN

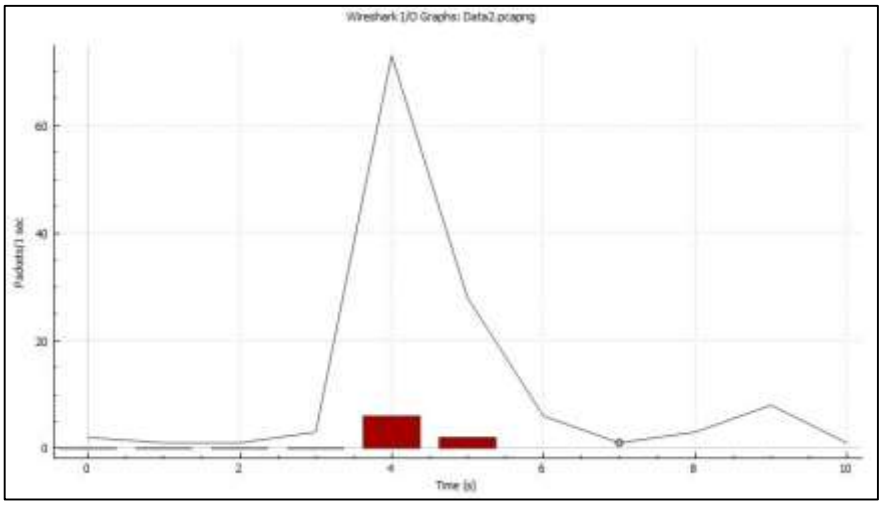
1.1 Latar Belakang

Internet merupakan sebuah teknologi yang banyak digunakan hingga saat ini, salah satunya adalah dapat mencari informasi melalui *website*. *Website* merupakan sebuah sistem yang di dalamnya terdapat informasi baik berupa teks, gambar, maupun suara yang ditulis menggunakan format HTML. Di saat penggunakan melakukan *request* terhadapat *website* memerlukan respon dari server agar *website* dapat di akses, inilah yang biasa di sebut *web server* [1].

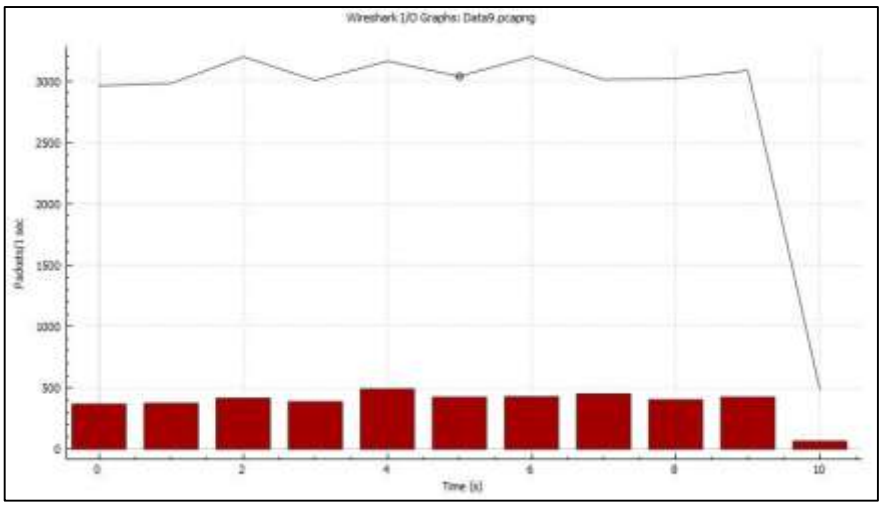
Dengan berkembangnya teknologi, berkembang pula kejahatan yang terjadi melalui teknologi *internet*. Pelaku kejahatan (*attacker*) membanjiri *web server* dengan banyak data sehingga lalu lintas jaringan tidak dapat berjalan dengan normal, ini yang disebut dengan serangan DDoS (*Distributed Denial of Service*). Serangan ini mengakibatkan *server down* karena terlalu banyak menerima *request* dalam waktu yang singkat [1].

Serangan DDoS yang terjadi sering kali tidak dapat disadari oleh korban dikarenakan DDoS mengalami perkembangan yang mutakhir. Salah satunya adalah dengan *SYN Flood* yang mana paket *SYN* merupakan paket yang bersifat legal sehingga sulit untuk di deteksi sebagai aktivitas yang mencurigakan [2]. *Fuzzy logic* merupakan sebuah teknik *soft computing* yang dapat digunakan untuk mendeteksi serangan DDoS yang rumit [3].

DDoS biasanya dapat dibedakan berdasarkan lalu lintas jaringan yang terjadi. Pelonjakan *request* data yang besar secara cepat adalah salah satu cara mengetahui bahwa sedang terjadi ketidak normalan lalu lintas jaringan. Gambar 1.1 menjelaskan bagaimana pola lalu lintas normal dengan jumlah paket 60 paket/*sec* dan Gambar 1.2 menjelaskan lalu lintas menjadi padat setelah di serang menggunakan DDoS hingga lebih dari 3000 paket/*sec.*



Gambar 1.1 Lalu Lintas Jaringan Normal



Gambar 1.2 Lalu Lintas Jaringan Serangan DDoS

Untuk itu, dalam penelitian ini penulis mencoba menerapkan konsep *fuzzy logic sugeno* dalam upaya mendeteksi serangan DDoS. *Fuzzy logic* akan bekerja untuk melakukan filterisasi terhadap log aktivitas yang terjadi dalam jaringan sehingga dapat membedakan mana yang lalu lintas normal dan lalu lintas yang dibuat untuk melakukan serangan DDoS.

1.2 Rumusan Masalah

Rumusan masalah pada penilitian ini adalah, bagaimana sistem dapat mendeteksi serangan DDoS *(Distributed Denial of Service)* menggunakan *fuzzy logic* sugeno *secara* akurat.

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah diatas, maka tujuan dari penelitian yang penulis lakukan adalah:

1. Melakukan identifikasi terhadap lalu lintas jaringan berdasarkan jumlah *user*, panjang paket, *rate* dan jumlah paket**.**
2. Mendeteksi serangan *Distributed Denial of Service* (DDoS) menggunakan pendekatan *fuzzy logic sugeno*.

1.4 Batasan Masalah

Batasan masalah yang perlu diperhatikan pada penilitian ini adalah, sebagai berikut:

1. Penelitian ini hanya difokuskan pada serangan DDoS saja, tidak untuk serangan jenis lain nya.
2. Penilitan ini difokuskan untuk mengetahui pola lalu lintas jaringan yang tidak normal sebagai acuan mengetahui serangan DDoS atau bukan.

1.5 Manfaat Penelitian

Penulis menjabarkan beberapa manfaat dari penelitian yang dilakukan antara lain:

1. Penelitian ini di harapkan mampu menghasilkan presentase akurasi yang tinggi untuk mendeteksi serangan DDoS yang dalam jaringan dengan menggunakan *fuzzy logic*.
2. Penelitian ini dapat dijadikan dasar untuk melakukan tindakan terhadap *web server* yang di serang menggunakan DDoS.

1.6 Sistematika Penulisan

Untuk mempermudah dalam memahami permasalahan dan pembahasan, maka sistematika penulisan penelitian ini dibuat sebagai berikut:

Bab I **Pendahuluan**

Bab I akan membahas latar belakang melakukan penelitian, perumusan masalah, tujuan penelitian, batasan masalah dan manfaat yang didapat dari penelitian.

Bab II **Landasan Teori**

Bab II akan menjelaskan dasar – dasar teori yang menyangkut dalam penelitian ini seperti DDoS, *Fuzzy Logic*, dan *Web Server* serta mebahas peneltian – penelitian terkait yang sudah ada.

Bab III **Metodologi**

Bab III akan membahas tentang metode yang digunakan pada penelitian ini, serta tahap – tahap apa yang akan dilakukan dalam penelitian.

Bab IV **Hasil Dan Pembahasan**

Bab IV akan menjelaskan semua hasil yang telah dilakukan dalam penelitian baik dari data yang diolah serta hasil identifikasi DDoS menggunakan *fuzzy logic* berdasarkan data tersebut.

Bab V **Penutup**

Bab V akan menjelaskan uraian yang telah dijabarkan pada bab – bab sebelumnya, sehingga mendapatkan kesimpulan dari penelitian yang telah dilakukan serta saran ataupun rekomendasi yang nantinya dapat digunakan untuk pengembangan berikutnya.