Abstrak

Internet sekarang sudah menjadi kebutuhan bagi sebagian besar orang. Hal ini didasari oleh kebutuhan informasi yang meningkat. Guna memudahkan orang-orang untuk mendapatkan informasi, dibangulah *server-server web* untuk menyediakan berbagai informasi yang dibutuhkan. Kemudahan mendapatkan akses internet ini menimbulkan pihak-pihak yang tidak bertanggung jawab yang ingin mengacaukan kerja *web server*. Cara paling mudah untuk mengacaukan kerja *web server* adalah dengan menggunakan *ping flood*. *Ping flood* adalah salah satu cara untuk melakukan *Distributed Denial of Service(DDoS)*.

Salah satu metode untuk mengetahui adanya serangan *DDoS* adalah dengan menggunakan *K-means Clustering* pada data *log web server*. *K-means Clustering* akan mengelompokan data *log traffic* kedalam dua kelompok, yaitu *traffic* yang berupa serangan dan *traffic* yang berupa *traffic* normal.

Untuk mengevaluasi akurasi dari proses *clustering* ini, harus dilakukan pelabelan pada *log traffic* awal untuk menentukan data yang berupa serangan dan data yang berupa data normal. Setelah dilakukan pelabelan, data *log traffic* dikelompokan menggunakan *K-means Clustering*. Hasil dari pengelompokan ini kemudian dibandingkan dengan data awal. Hasilnya, akurasi yang didapat selalu diatas 90%.

Kelemahan metode ini, *K-means Clustering* hanya mengelompokan menjadi dua kelompok. Jadi bila data yang dimasukkan hanya berupa data *traffic* normal, maka akan terjadi kesalahan karena data tersebut dipaksa untuk dikelompokan menjadi data serangan dan data normal, walau pada kenyataannya tidak ada data serangan dalam *log traffic* tersebut.

Kata kunci: K-Means Clustering, Distributed Denial of Service, Ping Flood.