ABSTRAK

Ketertarikan masyarakat terhadap berbagai informasi yang mudah didapat menyebabkan meningkatnya penggunaan internet. Seiring banyaknya masyarakat yang mengakses internet menyebabkan adanya fenomena anomali trafik. Fenomena anomali trafik ini dapat berupa serangan DDoS dan *flash crowd*. Fenomena anomali ini dapat menyebabkan suatu komputer atau server tidak berfungsi dengan baik. Pada penelitian sebelumnya dalam mendeteksi anomali trafik menggunakan metode *Data Mining* dengan algoritma *K-means*, dikatakan berhasil dalam membedakan trafik normal dengan trafik anomali. Namun, algoritma *K-means masih* sangat sensitif terhadap adanya outlier dan cluster yang dihasilkan cenderung berbentuk oval.

Dalam kelemahan tersebut, pada penelitian tugas akhir ini dibuat sebuah metode *Intrussion Detection System* (IDS) dengan teknik *unsupervised learning clustering* yang menggunakan algoritma ISODATA clustering dengan penambahan metode pengukuran jarak *Manhattan Distance* dan metode *Dunn Index* untuk menghitung kualitas cluster yang dihasilkan. Hasil dari penelitian ini berupa *False Positive rate*, *Detection rate*, *Accuracy* dan waktu proses yang diperlukan pada *Manhattan Distance*.

Hasil dari sistem deteksi anomali trafik menggunakan algoritma ISODATA menunjukan performansi yang baik. Sistem sudah mampu membedakan trafik anomali dengan trafik normal. Hal itu dapat diperlihatkan pada pengujian yang sudah dilakukan dengan menggunakan dataset DARPA 1998 dimana mendapatkan nilai rata – rata *Detection Rate* sebesar 95,4317 %, *False Positive Rate* sebesar 1,29264 %, *Accuracy* sebesar 95,3361 % dan waktu proses pada metode *Manhattan Distance* lebih cepat disbandingkan dari metode *Euclidean Distance.*

Kata Kunci : Anomali Trafik, DOS/DDOS, *Flash Crowd*, *Clustering*, ISODATA, *Manhattan Distance*