ABSTRAK

Pada perkembangan teknologi jaringan internet sekarang ini banyak membahas tentang fenomena-fenomena serangan atapun ancaman terhadap sebuah komputer atau *server*. Banyak sekali macam-macam tipe ancaman pada komputer dalam sebuah jaringan internet seperti *DoS (Denial of Service)*, *DDoS (Distributed Denial of Service)*, *flash-crowd*, dan sebagainya. Oleh karena itu, untuk memudahkan dalam pengambilan informasi agar sesuai dengan keinginan, perlu adanya pengelompokan dalam anomali trafik tersebut untuk mengenali tipe-tipe serangan yang baru.

Dari permasalahan tersebut perlu suatu sistem deteksi anomali trafik yang mempunyai kemampuan untuk mendeteksi anomali dan mengenali setiap serangan yang datang dengan dilakukan pengelompokkan berdasarkan waktu dan grup. Waktu dan grup adalah parameter untuk meningkatkan akurasi deteksi algoritma. Pada penelitian ini dibangun sebuah metode *IDS* yang menggunakan algoritma *clustream*.

Hasil dari penelitian ini, sistem yang dibangun secara *real-time* dapat bekerja dengan baik dalam deteksi dan membedakan antara trafik normal dan anomali trafik. Pengelompokan trafik dilakukan per-2 detik, setelah itu akan dianalisis dengan algoritma *clustream*. Algoritma ini terbagi menjadi *online (micro-clustering)* dan *offline (macro-clustering)*. Di mana *macro-clustering* akan menggunakan data hasil dari *micro-clustering.*

Kata Kunci : anomali trafik, *clustering*, algoritma *clustream*, *stream traffic*