ABSTRAK

Perkembangan jaringan teknologi internet sudah semakin pesat, keamanan jaringan menjadi fokus penting dalam melindungi serangan terhadap suatu data di jaringan. Saat ini begitu banyak jenis penyusupan atau serangan terhadap suatu jaringan komputer. Keamanan jaringan komputer sangatlah penting untuk menjaga integritas data. IDS (*Intrusion Detection System*) merupakan sistem komputer yang digunakan untuk mengidentifikasi jika terdapat aktivitas yang mencurigakan pada lalu lintas suatu jaringan.

Sistem deteksi anomali trafik ini mempunyai kemampuan untuk mendeteksi anomali yang terjadi dan mengenali setiap serangan sehingga dapat dikelompokkan berdasarkan waktu serangan dan kelompok serangan. Waktu serangan dan kelompok serangan adalah parameter untuk meningkatkan akurasi deteksi. Dan pada penelitian ini dibangun sebuah metode IDS yang menggunakan algoritma Clustream.

Hasil dari penelitian ini sistem yang dibangun dapat bekerja dengan baik dalam deteksi dan membedakan antara trafik normal dan anomali trafik. Setiap serangan telah di analisis dengan algoritma Clustream berdasarkan waktu serangan dan kelompok serangan. Dimana algoritma Clustream terbagi menjadi *online* (mikro-Clustering) dan *offline* (makro-Clustering). Pada *online* komponen menyimpan statistik *summary* secara periodik tentang *stream* data sedangkan untuk *offline* komponen berdasarkan pada statistik *summary* yang tersimpan.

Kata Kunci: IDS (*Instrusion Detection System*), anomali trafik, algoritma clustream.