ABSTRAK

Perkembangan pesat teknologi dan informasi khusunya internet sekarang ini memicu munculnya fenomena-fenomena anomali trafik (serangan) atapun ancaman terhadap sebuah komputer atau *server*. *Flash crowd* merupakan fenomena peningkatan akses / trafik secara tinggi ke suatu *server* karena suatu kejadian tertentu. Serangan *Denial of Service (DoS)* dan *Distributed Denial of Service (DDoS)* merupakan serangan yang terjadi dengan membanjiri lalu lintas jaringan dengan banyak data (*traffic flooding*) atau membanjiri jaringan dengan banyak *request* terhadap sebuah *host* atau *service* (*request flooding*) sehingga tidak dapat diakses oleh *user* yang terdaftar / berhak *(legitimate user)*. Oleh karena itu, perlu adanya suatu sistem deteksi dengan melakukan pengelompokan pada anomali trafik

Pada penelitian Tugas Akhir ini digunakan salah satu teknik dalam deteksi anomali trafik yaitu *clustering based*. Algoritma CURE merupakan salah satu algoritma *clustering* berbasis *hierarchical* yang memiliki prestasi dapat mengatasi *outlier* Kemudian, fokus penelitian Tugas Akhir ini adalah dalam hal menangani titik *outlier* dari dataset yang digunakan. *Outlier* dieliminasi dengan menghapus titik yang dianggap sebagai *outlier* dengan teknik *outlier removal clustering (ORC)*.

Hasil dari penelitian ini, algoritma CURE memiliki perfomansi yang baik dalam mendeteksi anomali trafik. Hal itu dapat ditunjukkan dengan pengujian yang dilakukan dengan dataset DARPA 1998, dimana nilai rata-rata *detection rate* sebesar 98.4588 %, *false positive rate* 0.2325 % , dan *accuracy* 94.7323 %. Hasil pengujian eliminasi *outlier* dengan threshold 0.1 – 1, teknik ORC berhasil menemukan dan menghapus titik yang dianggap sebagai *outlier*.

Kata Kunci : anomali trafik, ddos, *flash crowd*, *preprocessing*, *clustering*, algoritma cure