

ABSTRAK

Dalam beberapa tahun terakhir, fenomena anomali trafik pada lalu lintas jaringan komputer menarik banyak perhatian para peneliti. Menurut [1] serangan *Distributed Denial of Service* (DDoS) adalah jenis serangan yang dapat merugikan trafik jaringan yang sedang digunakan, baik terhadap target serangan maupun seluruh pengguna. Sedangkan peristiwa *flashcrowd* adalah sebuah lonjakan besar pada lalu lintas jaringan internet karena jumlah *user* yang mengakses server naik secara signifikan dan menempatkan tekanan berat pada link jaringan yang mengarah ke server.

Pada tugas akhir ini digunakan teknik statistik *covariance matrix* yang tidak mengabaikan fitur satu dengan fitur lainnya, dapat dibuat sistem deteksi anomali dengan mengubah data asli ke ruang fitur *covariance*. Serangan yang ada ini dapat diklasifikasi dengan menggunakan SVM. *Accuracy*, *detection rate* dan *false positive rate* adalah parameter pengujian yang digunakan dalam penelitian.

Hasil dari penelitian ini, algoritma SVM memiliki performansi nilai rata-rata *detection rate* dalam mengklasifikasikan data homogen sebesar 99% pada dataset KDDCUP 99 dan akurasi sebesar 90,5%. Untuk data heterogen performansi menurun dengan meningkatnya nilai FPR pada data yg di uji dengan rata-rata 22,6% karena data diberi *noise* serangan pada proses preprocessing.

Kata kunci : DdoS, SVM, *flashcrowd*, *covariance matrix*, *Landmark Window*, *detection rate*, *false positive rate*.