ABSTRAK

Internet merupakan salah satu teknologi yang paling banyak penggunanya dan terus meningkat. Dengan jumlah peningkatan pengguna yang mengakses internet akan memicu oknum-oknum untuk melakukan intrusi ke pengguna melalui jaringan. Dampak dari intrusi-intrusi tersebut sangatlah buruk, mulai dari pemalsuan identitas, pencurian data, *down* sebuah *server*, dan lain-lain.

Dari dampak negatif tersebut, sangat penting dibuat suatu sistem untuk mendeteksi intrusi dengan menganalisa trafik pada jaringan. Pada penelitian ini dibuat sebuah sistem deteksi seragan pada trafik menggunakan metode *clustering* dengan algoritma *Incremental K-means.* Berbeda dari penelitian-penelitian sebelumnya yang hanya melakukan analisa mengenai algoritma deteksi anomali, pada penelitian ini sistem dirancang untuk mendeteksi paket-paket anomali secara langsung/*online*.

Keluaran dari penelitian ini adalah sebuah sistem yang dapat melakukan pengelompokkan data atau *clustering* paket data secara *stream* dan menyimpan *dataset* hasil dari *clustering*. Paket data tersebut terlebih dahulu diekstrak untuk diambil data-data tertentu seperti *source IP address, destination IP address, port*, jumlah paket, dan lain-lain yang digunakan sebagai fitur untuk mendeteksi serangan pada trafik jaringan. Parameter keberhasilan dari penelitian ini adalah sebuah system yang dapat mendeteksi paket-paket anomali dan juga dapat menyimpan attribute-attribut yang ada dalam paket anomali tersebut. Akurasi yang diapatkan dari penelitian ini adalah 98.98% dengan *false positive rate* 0% dan *detection rate* 100%.

Kata kunci: *Network Security, clustering, data stream, Incremental K-means, Anomaly Detection*