ABSTRAK

Software Defined Networking (SDN) memperkenalkan cara yang lebih fleksibel untuk mengelola dan mengontrol lalu lintas jaringan. SDN memiliki arsitektur pemisahan antara control plane dan data plane yang bertujuan untuk memprogram perangkat secara terpusat. Namun, karena terpusatnya kontrol terhadap jaringan ini SDN menjadi rentan terhadap serangan Denial Of Service (DoS) yang memungkinkan penyerang melumpuhkan *controller* dan berakibat fatal. Jika SDN *controller* tidak dapat diakses oleh perangkat jaringan lain, maka keseluruhan jaringan akan mengalami kegagalan. Untuk dapat menemukan dan mengidentifikasi serangan tersebut, dibutuhkan proses penangkapan, pencatatan, dan analisis *traffic* yang disimpan dalam sebuah file log yang memiliki format data tertentu. Namun, karena data tersebut berjumlah sangat banyak dan relative besar, maka akan sangat sulit jika dilakukan analisis secara manual. Teknik clustering adalah salah satu metode yang bisa digunakan untuk memudahkan proses tersebut. Metode clustering yang dipilih adalah K-Means Clustering yang bisa mengelompokkan data dalam jumlah yang cukup besar dengan waktu yang cepat dan efisien. Hasil akhir dari penelitian ini adalah bahwa dengan metode K-Means Clustering, bisa dilakukan analisis pendeteksian serangan terbukti dengan akurasi adalah 91,41%.

Kata kunci : Software Defined Network, Log Analisis, Clustering, K-Means, DoS