ABSTRAK

Serangan denial of service yang mengirimkan permintaan massal hingga server tidak mampu beroperasi dengan baik, salah satu teknik dalam membedakan permintaan normal dan dicurigai adanya serangan adalah dengan teknik clustering yang bertujuan memisahkan data log dengan jarak tertentu untuk dikelompokan pada cluster tertentu.

Algoritma K-means sebagai teknik clustering dalam mengelompokkan data bekerja berdasarkan perhitungan jarak tertentu. Fungsi Sum of Square Within cluster ditambahkan dalam algoritma K-means untuk mengetahui densitas data pada cluster. Usulan dalam pembelajaran ini adalah menerapkan clustering Density K-means dalam mengelompokkan data log dengan input algoritma ini berupa total frekuensi atribut length & tcplength per jam dengan parameter centroid adalah nilai terkecil, nilai tengah dan nilai terbesar dari dataset total frekuensi length & tcplength sebagai indikator tingkat bahaya yang dikelompokan menjadi tingkat bahaya rendah, sedang & tinggi

Hasil clustering dengan algoritma density k-means mengenali cluster dengan tingkat bahaya sedang & tinggi, serta nilai DBI sebesar 0.082 yang menunjukan jumlah cluster yang optimal. Hasil percobaan pengelompokkan dengan algoritma ini menghasilkan cluster bahaya sedang & tinggi, tapi tidak dapat mengenali bahaya rendah. Hal ini disebabkan karena penentuan centroid diawal proses clustering.

Kata kunci: denial of service, k-means, density, log, analisys