Abstrak

Intrusion detection system (IDS) merupakan sistem yang dapat mendeteksi adanya intrusi atau gangguan pada suatu jaringan atau sistem informasi. Salah satu jenis IDS adalah anomaly detection dimana suatu data trafik jaringan akan dikatakan intrusi apabila mempunyai karakteristik yang berbeda dari kebanyakan data lainnya. Pada anomaly detection terdapat pendekatan clustering based dimana data akan dikelompokkan menjadi beberapa cluster. Cluster intrusi adalah cluster dengan jumlah anggota yang sedikit. Algoritma clustering yang cukup dikenal adalah K-Means karena mudah diimplementasikan dengan kompleksitas yang rendah. Akan tetapi terdapat beberapa kekurangan pada algoritma tersebut. Algoritma Y-Means adalah algoritma clustering yang dibangun untuk memperbaiki kekurangan K-Means. Data trafik jaringan akan dikelompokkan ke beberapa cluster, lalu dilihat cluster mana yang merupakan cluster intrusi berdasarkan threshold. Pengujian dilakukan dengan beberapa skenario untuk mengetahui akurasi sistem dilihat dari nilai detection rate dan false positive rate, pengaruh besar konstanta merging terhadap jumlah cluster akhir, dan juga pengaruh konstanta merging dan threshold terhadap nilai akurasi. Y-Means dapat mendeteksi intrusi dengan tingkat akurasi yang cukup baik dilihat dari nilai detection rate sebesar 92.46%. Untuk nilai false positive rate Y-Means menunjukkan akurasi yang tidak terlalu buruk yaitu sebesar 9.69%.

.

Kata kunci: intrusi, *clustering*, anomaly detection, Y-Means