

ABSTRAKSI

Intrusi adalah semua tindakan yang mengancam ketersediaan, integritas, dan kerahasiaan sumber daya jaringan, seperti *user account*, *file system*, *system kernel*, dan sebagainya. Untuk mencegah terjadinya intrusi pada jaringan, dibangunlah *intrusion detection system* (IDS), sebuah sistem yang berfungsi untuk mengamati dan menganalisis sebuah *event* yang terjadi pada komputer, apakah *event* tersebut merupakan *intrusion* atau bukan. Salah satu kategori IDS adalah *anomaly detection*. *Anomaly detection* mendeteksi *intrusion event* berdasarkan profil data. Data yang dianggap intrusi adalah data yang mempunyai karakteristik yang berbeda dari profil data secara umum. *Clustering* adalah salah satu cara untuk mengetahui profil data tersebut. Ada banyak algoritma *clustering* yang telah diusulkan untuk *anomaly detection* pada IDS, salah satunya adalah *CLIQUE Partitioning* (CP). CP merupakan gabungan dari teknik *grid-based clustering* dan *density-based clustering*. CP membagi *dataspace* ke dalam *subspace* dan mencari *cluster* pada masing-masing *subspace* tersebut. Pengujian dilakukan untuk melihat performansi IDS dari segi *computational time*, *completeness*, dan *false alarm rate*. Algoritma CP mampu menghasilkan performansi yang bagus dari *completeness* (94.59%) dan *false alarm rate* (2.54%). Dari segi *computational time*, CP mampu menghasilkan performansi yang bagus apabila dilihat dari banyaknya *tuple* (peningkatan banyaknya *tuple* berbanding linier dengan peningkatan *computational time*), namun kurang bagus dari segi banyaknya atribut (peningkatan banyaknya *tuple* berbanding eksponensial dengan peningkatan *computational time*).

Kata kunci : anomaly detection, IDS, CLIQUE Partitioning, subspace, cluster