

Pengujian terhadap sistem *anomaly detection* ini menunjukkan hasil akhir bahwa hasil pendeteksian anomali sangat bergantung pada tiga hal hal, yaitu tergantung pada pemilihan data yang digunakan untuk dianalisis (*dataset*), jarak maksimal yang diijinkan dari titik pusat *cluster* atau *center* ke setiap data yang menjadi anggota dari *cluster* tersebut atau biasa disebut jari jari *cluster*, dan perbandingan jumlah data *instrusion* dengan data normal pada *dataset*.

Kata kunci :*Intrusion Detection System(IDS), clustering, anomaly detection, outlier detection scheme.*

ABSTRACT

Intrusion Detection System (IDS) is a group of techniques and methods for detecting activities that hapenned in network and host level. IDS has two approaches : signature-based intrusion detection system and anomaly detection system. First approach has any weakness, the detection can only done if the intrusion had been definded. Therefore except using the data which had been definded, we can also analyze anomaly patterns from the packets , but if we take the wrong parameter this method could eventually be a false alarm.

Analyze anomaly detection in network data packets can be handled by outlier detection scheme method. With this method we can build the analysis with some algorithms, one of the algorithms is clustering. Clustering algorithm clustered the data and mark the smallest cluster with assumption that smallest cluster as an anomaly.

This final Project will build an implementation of intrusion detection system in computer or network system using anomaly detection method with cluster-based outlier detection algorithm. The process is to clustering data connection record. Implementation use HTML programming language, PHP script, and MySQL DBMS.

Anomaly detection system evaluation shows that the results are depend on three things, data which have been analyzed or data set given and the maximum distance between center to each data point that included in that cluster, or cluster radius values and ratio between normal data and instrusion data

Keywords :Intrusion Detection System(IDS), clustering, anomaly detection, outlier detection scheme.