ABSTRACT

The development of Internet technology network has been growing rapidly, network security becomes an important focus in protecting the attacks on a data network. We have so many kinds of intrusion or attack against a computer network. Network security is extremely important to maintain the integrity of the data. IDS (Intrusion Detection System) is a computer system that is used to identify if there is suspicious activity on the traffic network.

This traffic anomaly detection system has the ability to detect anomalies and identify any attacks that can be grouped based on the time of the attack and the raid group. Time attack and raid groups are the parameters to improve detection accuracy. And in this study constructed a method that uses an algorithm Clustream IDS.

The results of this research system built to work well in the detection and distinguish between normal traffic and traffic anomaly. Any attack will be analyzed with Clustream algorithm based on the time of attack and group attack. Where Clustream algorithm is divided into online (micro-clustering) and offline (macro-Clustering). In the online component store periodic statistical summary of the data stream while the offline component is based on a statistical summary stored.

Keywords: IDS (Instrusion Detection System), traffic anomaly, the algorithm clustream.