ABSTRACT

In the development of Internet network technology today, there are many discussionsl about the phenomena of attacks or threats to a computer or server. There are so many kinds of types of threats on a computer in an internet network such as DoS (Denial of Service), DDoS (Distributed Denial of Service), flash-crowd, etc. Therefore, to facilitate the retrieval of information in order to conform with the desire, the need for the grouping in the traffic anomalies to identify the types of new attacks.

Of these problems, it is necessary to provide a traffic anomaly detection system that has the ability to detect anomalies and identify any attack that comes by grouping based on time and group. Time and groups are the parameters to improve the accuracy of detectiing algorithms. In this study it was built a method of IDS that uses an algorithm clustream.

The results of this study, the system built in real-time can work well in detecting and distinguishing normal traffic and traffic anomalies. Grouping traffic is done per 2 seconds, after which it will be analyzed by the algorithm clustream. This algorithm is divided into online (micro-*clustering*) dan offline (macro-*clustering*). Where macro-*clustering* will use the data of results from the micro-*clustering*.

Keywords: traffic anomalies, clustering, algorithm clustream, stream traffic