ABSTRACT

Internet is one of many technologies that has the most users and is still increasing. With vast increase number of users that has access on internet, it will trigger some irresponsible users to an act of intrusion inside other users through network. The consequence of that action is quite harmful for example; forging an identity, data stealing, server down and many other.

From those negative outcome, it is important to create a system for detecting an intrusion by analyzing network traffic. This research creates an intrusion detecting system in traffic network using clustering methods with Incremental K-means algorithm. Different from the past research that exclusively discussed about detection algorithm, in this research system could detect anomaly packets directly/online.

Output from this research is a system that could cluster data or clustering packet data in stream and save the dataset which is a result from clustering. Those packets of data is first extracted to get some specified data for example; Source IP address, destination IP address, port, total number of packets and many other that are used as feature for detecting intrusion in traffic network. The success parameter of this research is a system could detect anomaly packets and also could save those anomaly packet's attributes.Accuracy obtained in this research was 98.98% with 0% false positive rate and 100% detection rate.

Keywords: *Network Security, clustering, data stream, Incremental K-means, Anomaly Detection*