# ABSTRACT

Along with the development of technology at this point, needs of Internet access service as a medium of communication is increasing. This increase led to anomalies in network traffic. These anomalies, can occur because of a Distributed Denial of Service (DDoS) that deliberately or *Flashcrowd*, a large spike in network traffic because of the number of Internet *user*s who access the *server* rose significantly at a time. The impact of an anomaly is to make the *user* can not access the internet service.

If left alone, these anomalies can be detrimental to a lot of parties, both in terms of *user*s and providers of internet access services. Therefore, further research is needed to detect anomalies. Anomalies can be detected by using a *Covariance Matrix*. The amount of data that is tested by *Covariance Matrix* is often a bottleneck in time, to the use of *Sliding window* to be able to cope with the large number of data. Upon obtainment *Covariance Matrix*, then the next step for anomaly detection method is to use *decision tree* to determine the types of anomalies.

The test results obtained from the used anomaly detection method is the obtainment of output types of anomalies, and the output can be calculated from the value of the *accuracy* in detecting (*Detection rate*) and the value of detection errors (*False positive rate*). A great anomaly detection method is able to detect anomalies with parameter values with a high *Detection rate False positive rate* low.

Keywords : anomaly detection, *Covariance Matrix, Sliding Window*, *Decision tree*, *Detection rate*, *False positive rate*