ABSTRACT

Software Defined Networking (SDN) introduces a more flexible way to manage and control network traffic. SDN has a separation architecture between the control plane and data plane which aims to centrally program the device. However, due to centralized control over this network, SDNs are vulnerable to Denial Of Service (DoS) attacks that allow attackers to disable the controller and have fatal consequences. If the SDN controller cannot be accessed by other network devices, the whole network will fail. To be able to find and identify these attacks, it takes a process of capturing, recording, and analyzing traffic which is stored in a log file that has a specific data format. However, because the data is very large and relatively large, it will be very difficult to do the analysis manually. The clustering technique is one method that can be used to facilitate the process. The clustering method chosen is K-Means Clustering, which can classify large amounts of data in a fast and efficient manner. The final result of this research is that with the K-Means Clustering method, it can be done a proven attack detection analysis with an accuracy of 91.41%.

Keywords: Software Defined Network, Log Analysis, Clustering, K-Means, Denial of Service