ABSTRACT

At this time the network has become a very important infrastructure for businesses, offices and campuses. Therefore, it is very important to have a network infrastructure system that is easy to manage but has optimal workability and is also flexible. Software Defined Network (SDN) is a new technology in network concept, where SDN separates the control plane and data plane. The controller as the brain that regulates packet forwarding from an SDN network, so that it can perform centralized control on multiple networks in a controller. The controller does not yet have a security system that is good enough to protect against attacks. There are several cases of attacks such as Distributed Denial of Service (DDoS) which is a serious problem in network security. To be able to support increasingly advanced technology, it is necessary to apply the concept of an adequate network as well. In this study, we will build a concept of an SDN network and develop a controller by applying machine learning K-Nearest Neighbors (KNN). The function of the KNN machine learning itself is to be able to classify the traffic that is run. The traffic that is executed will have attack traffic that can be detected and mitigated by the controller that has been developed. The controller used in this study is the ryu controller. The purpose of this research is to build a DDoS attack detection and mitigation system using machine learning model KNN algorithm. In this study it is proven that the performance of the KNN machine learning developed on the controller can detect and mitigate DDoS attacks. In testing the accuracy measurement, it gets a value of 82% using the value of K = 5 and the test data used is 30%.

Keywords: ***Software Defined Network (SDN), Distributed Denial of Service (DDoS), K-Nearest Neighbors (KNN), Controller.***