ABSTRACT

Software Defined Network (SDN) is a term that refers to a new paradigm in designing, managing, and implementing networks, which is software-based. The concept in SDN is the explicit separation between the control and forwarding planes. The controller acts as the brain that regulates packet forwarding in an SDN network, enabling centralized control over a large network through a single controller. However, this controller does not yet have a sufficiently strong security system and is vulnerable to attacks such as Distributed Denial of Service (DDoS). Several DDoS attacks have posed significant challenges to network security systems. In this research, a concept will be developed to detect DDoS attacks that can be implemented using machine learning with the Support Vector Machine (SVM) algorithm. To detect attacks using the SVM machine learning algorithm, it is necessary to evaluate the accuracy, precision, recall, and F1 score. The research shows that the accuracy of the training data against DDoS attacks using the Support Vector Machine algorithm achieves an average accuracy of 97% with K-fold=10 and attack packet sizes of 250, 500, and 1000 packets. The research also demonstrates that the accuracy, precision, recall, and F1-score results have values of 98%.

Keywords— ***Software Defined Network (SDN), Distributed Denial of Service (DDoS), Support Vector Machine (SVM), Controller***