Abstract

Distributed Denial-of-Service (DDoS) is an attack launched over a computer network to make the server unable to provide services to users. DDoS is also effectively used to stop services on Internet of Things systems based on the message Queuing Telemetry Transport (MQTT) protocol. In the system, attackers usually attack brokers who are used to manage data traffic between the issuer and the customer. Several research projects have been undertaken to detect DDoS in the Internet of Things (IoT) using machine learning. However, existing research projects still generally have low detection accuracy in predicting DDoS. This study provides a solution to the above problems by proposing the development of a machine learning model based on Neural Network (NN) to detect DDoS. Furthermore, this study also compared the results of NN predictions with K-Nearest Neighbor (KNN). The methods used in this study are as follows: 1. Conducting literature studies. 2. Develop both machine learning models. 3. Conduct analysis. Rigorous experiments have been carried out using dataset derived from research [1] and dataset generated through DDOS simulations in IoT environments. By using the dataset generated through simulation, the results obtained showed that the accuracy of NN is better than KNN, which is 99.99% and 99.82%, respectively.

Keywords: DDoS, NN, KNN