Nowadays there are many devices that are already connected to the internet using the concept of IoT to make it easier to get information from a device. There are several protocols used so that IoT devices can connect with the internet namely MQTT, CoAP, and so on. Among these protocols, MQTT is one of the protocols commonly used because of its lightness and flexibility in its implementation. In a service, the server plays an important role because the server is tasked with managing the communication flow of each device connected to the server. In the MQTT protocol, brokers are an important component because they act as servers that regulate the flow of communication between devices. Currently, there are some who carry out cyberattacks aimed at crippling a service. There are some exploits that can cripple services such as DoS attacks. A DoS attack is a flood-type attack that is carried out with the aim of making service resources crash or flood the bandwidth of a service. In order for cyberattacks to be detected can implement IDS which is a system that can be applied as a mitigation step in detecting an attack. The study focused on building IDS by implementing classification algorithms to analyze network traffic. This research applies the SVM method as a classification method. The results of the model obtained are 98.865% accuracy and 99.4601% accuracy based on different DoS attack methods.

Keywords: Intrusion Detection System (IDS), Support Vector Machine (SVM), Internet of Things (IoT), Message Query Telementry Transport(MQTT), Denial of Service (DoS)