Saat ini terdapat banyak perangkat yang sudah terhubung dengan internet menggunakan konsep IoT untuk mempermudah dalam mendapatkan informasi dari perangkat sebuah. Terdapat beberapa protokol yang digunakan agar perangkat IoT dapat terhubung dengen internet yaitu MQTT,CoAP,dan sebagainya. Diantara protokol tersebut, MQTT merupakan salah satu protokol yang umum digunakan karena ringan dan fleksibilitas dalam penerapannya. Dalam sebuah layanan, server memegang peranan penting karena server bertugas mengatur alur berkomunikasi dari tiap perangkat yang terhubung dengan server. Dalam protokol MQTT, broker merupakan komponen penting karena berperan sebagai server yang mengatur alur komunikasi antar perangkat. Saat ini, terdapat beberapa pihak yang melakukan serangan siber yang bertujuan untuk melumpuhkan sebuah layanan. Terdapat beberapa eksploit yang dapat melumpuhkan layanan seperti serangan DoS. Serangan DoS merupakan serangan tipe flood yang dilakukan dengan tujuan membuat resource layanan menjadi lumpuh atau membanjiri bandwidth dari sebua layanan. Agar serangan siber dapat terdeteksi dapat menerapkan IDS yang merupakan sebuah sistem yang dapat diterapkan sebagai langkah mitigasi dalam mendeteksi sebuah serangan. Pada penelitian ini berfokus untuk membangun IDS dengan menerapkan algoritma klasifikasi untuk melakukan analisa terhadap trafik jaringan. Penelitian ini menerapkan metode SVM sebagai metode klasifikasi. Hasil model yang diperoleh adalah akurasi 98.865% dan akurasi 99.4601 % berdasarkan pada metode serangan DoS yang berbeda.

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