BAB 1
PENDAHULUAN

1.1 Latar Belakang

IoT adalah sebuah konsep atau skenario dimana suatu objek yang memiliki kemampuan untuk mentransfer data melalui jaringan tanpa memerlukan interaksi manusia ke manusia atau manusia ke komputer. Objek-objek dalam IoT dapat menggunakan maupun menghasilkan layanan-layanan yang bisa digunakan dalam kebutuhan sehari-hari, contoh penggunaan IoT yang sering digunakan adalah sebuah sistem yang dirancang menggunakan protokol MQTT. (Muktiawan & Nurfiana, 2018)

Message Queuing Telemetry Transport *(MQTT)* protokol merupakan sebuah protokol yang berjalan diatas stack TCP/IP dan dirancang khusus untuk machine to machine yang tidak memiliki alamat khusus. Dengan kata lain MQTT adalah protokol yang tidak memiliki arduino, raspi atau device yang memiliki alamat khusus. Sistem kerja MQTT adalah menerapkan Publish dan Subscribe dengan menggunakan topik tertentu yang mengharuskan untuk terhubung dengan sebuah Broker. Broker pada MQTT berfungsi untuk Menghandle dan mengirimkan data dari berbagai device, Broker sama fungsinya seperti sebuah server yang memiliki IP khusus. Meski tidak memiliki alamat khusus, MQTT berpotensi mendapatkan serangan dari pihak yang berusaha merusak penyimpanan yang dimiliki. Jenis serangan yang dapat merusak penyimpanan dengan cara mengirimkan data sebanyak-banyaknya adalah DDOS.(Susanto et al., 2018)

Serangan Distributed Denial Of Service *(DDOS)* merupakan serangan yang kerap terjadi atau sering dilakukan untuk menyerang layanan yang menggunakan jalur yang terkoneksi dengan jaringan. Serangan DDOS terus berkembang sampai saat ini secara dinamis, Semakin tinggi kemampuan komputasi suatu komputer penyerang, serangan DoS yang dapat dihasilkan juga semakin membahayakan. Serangan ini dapat mengakibatkan ketidakmampuan server untuk melayani service request dikarenakan daya tampung dari serangan yang dikirimkan dapat menghabiskan memori penyimpanan. Mengingat resiko

besar yang diakibatkan serangan DDoS ini, banyak peneliti yang terdorong untuk merancang mekanisme pengamanan sumber daya jaringan yang dapat berfungsi untuk mendeteksi jika terjadi serangan atau keanehan pada pengiriman data dari Publisher ke Subscriber pada MQTT. Jenis mekanisme pengamanan yang digunakan untuk mendeteksi berbagai serangan adalah Intrusion Detection System atau dikenal dengan IDS. (Geges & Wibisono, 2015)

Intrusion Detection System merupakan fungsi yang dimiliki atau kemampuan untuk mencari dan menganalisa, mendeteksi suatu aktivitas yang dicurigai pada jaringan komputer pada umumnya. Kemampuan IDS dalam mendeteksi seluruh aktivitas port scanning adalah karena IDS ditempatkan pada komputer yang menjadi gateway dan sekaligus difungsikan sebagai firewall. Penempatan IDS pada server gateway ini akan melindungi data yang ada di server gateway dari serangan. Selain itu, IDS juga dapat ditempatkan pada host tertentu yang penting untuk dilindungi, misalnya web server atau FTP server, agar dapat melindungi data pada host tersebut jika serangan yang dilancarkan lolos dari pengawasan IDS yang ditempatkan pada server gateway. (Niko Suwaryo[1], Ismasari Nawangsih[2], 2021)

Intrusion Prevention System (IPS) merupakan sebuah perangkat yang berfungsi untuk mendeteksi, mengidentifikasi dan mencegah masuknya serangan ke sebuah Jalur layanan yang digunakan. Intrusion Prevention System mampu melakukan keamanan Jalur layanan selama 24 Jam nonstop guna mencegah terjadinya serangan seperti DDOS dan lainnya. Snort merupakan sebuah software yang berfungsi layaknya IPS guna juga mencegah dan mendeteksi jika terjadi gangguan atau penyerangan pada Jalur layanan. (Muhaimi et al., 2019)

Pengembangan ilmu pengetahuan bagi seorang Muslim, termasuk teknologi di dalamnya, merupakan bagian dari ketaatan kepada perintah Allah SWT. Ilmu pengetahuan dikembangkan oleh umat Islam untuk kebaikan umat manusia. Sebagaimana ayat-ayat naqliyyah yang memiliki berbagai lapisan makna serta tafsir, dari mulai yang paling harfiyyah (lahir) maupun sampai ke dalam lapisan terdalam dari ayat itu (makna batin). Pun demikian dengan alam semesta. Ia menyimpan hierarki makna yang terbentang dari apa yang nampak sampai ke

makna yang paling tersembunyi.5 Itulah alasan yang melandasi bahwa ilmu pengetahuan di dalam Islam memiliki makna yang juga bertingkat-tingkat. Allah berfirman dalam Surat Ali ‘Imran (QS: 190 – 191). (Rukmana, 2019)

Berdasarkan Uraian di atas maka penelitian yang berjudul “Intrusion Prevention System Menggunakan Snort Pada MQTT Broker Untuk Menangkal Serangan DDoS” ini dibuat agar dapat merancang suatu sistem keamanan bagi jalur pelayanan MQTT Broker guna menangkal serangan DDOS yang sering dilakukan untuk merusak Software ataupun Hardware.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang tertera di atas, permasalahan yang muncul pada penilitan ini adalah :

1. Bagaimana cara agar IDS dan IPS membedakan bahwa serangan Flood yang dilakukan bukan oleh publisher melainkan DDOS
2. Apa yang terjadi pada server MQTT Broker jika selain serangan DDOS yang dilancarkan pada jalur layanan?

1.3 Tujuan Penelitian

Tujuan penelitian ini adalah untuk mendeteksi dan menangkal serangan DDOS ke jalur layanan yang disediakan oleh MQTT Broker menggunakan Intrusion Detection System dan Intrustion Prevention System.

1.4 Manfaat Penelitian

Manfaat penelitian ini adalah guna mencegah serangan yang terjadi pada jalur layanan yang dapat menyebabkan kerugian bagi penyedia layanan maupun konsumen. Selain mencegah kerugian bagi kedua pihak, manfaat penelitian ini juga berfokus agar mengurangi serangan yang dilakukan oleh pihak yang tidak bertanggung jawab.

1.5 Batasan Penelitian

Berdasarkan latar belakang yang tertera di atas, batasan masalah yang muncul pada penelitian ini adalah :

1. Sistem ini hanya mengimplementasikan deteksi dan pencegahan untuk serangan DDOS
2. Versi Rapsberry Pi yang masih tidak compatible dengan Mqtt
3. Zombies yang dibuat untuk melancarkan Flood ke server masih dalam tahap pengembangan