BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Kemajuan teknologi dalam industri saat ini mulai berkembang cepat dan mulai memasuki revolusi industri 4.0. Dengan revolusi industri 4.0 menjadikan *Internet of Things* (IoT) sebagai salah satu elemen dasar didalamnya. IoT memanfaatkan jaringan internet untuk melakukan komunikasi antar perangkat yang terhubung. Untuk memantau dan mengkontrol keadaan sekitar manusia [2]. IoT merupakan sebuah konsep komunikasi yang dapat menghubungkan apa saja dengan siapa saja, dengan tidak dibatasi jarak dan waktu. Perkembangan IoT yang semakin massif dan heterogen yang membuat IoT menjadi riskan pada sisi keamanannya [3]. Pada penelitian yang dilakukan pada penelitian [4] serangan yang dapat terjadi pada IoT adalah *Denial of Service* (DoS) yang menyerang *availability*, serangan atau ancaman tersebut terjadi karena masalah pada skalabilitas dan *heterogeneity* dari IoT [4]. IoT memiliki tiga *layer*, yaitu *Preception layer*, *Network layer* dan *Application layer*, serangan DoS yang terjadi pada jaringan IoT dapat terjadi pada *layer network* [5].

Software Defined Network (SDN) adalah sebuah konsep dalam jaringan yang melakukan pemisahan antara *control plane* dan *data plane* dengan menggunakan protokol *OpenFlow*, konsep tersebut mendukung inovasi untuk operator jaringan dapat membangun bentuk arsitektur sesuai dengan sumber daya dan kebutuhan yang ada, dengan SDN pemrograman pada jaringan dapat dilakukan [1]. Pada penelitian [6] salah satu acaman yang sering dan dapat terjadi adalah DoS pada perangkat *forwading* atau yang biasa di sebut *data plane*, DoS yang terjadi menyerang *availability* pada jaringan SDN. Pada penelitian [7] melakukan riset mengenai pengamanan jaringan IoT menggunakan SDN dengan menggunakan *Network Intrusion Detection System* (NIDS) yang melakukan pemantauan *traffic* IoT dengan melihat *anomaly detection*. Implementasi SDN pada jaringan IoT diharapkan dapat memberikan solusi kelemahan dari jaringan IoT yang sudah ada. Penelitian tentang serangan *Distributed Denial of Service* (DDoS) pada jaringan SDN yang dijelaskan pada [8]. DoS melakukan serangan tidak hanya pada *host* target namun juga *link network* pada jaringan tersebut. Sehingga jaringan tidak dapat memberikan layanan kepada pengguna. Terdapat beberapa cara yang dapat digunakan untuk mengatasi DDoS maupun *Denial of Service* (DoS) seperti pada penelitian [9] dan [10] dengan menggunakan *snort* yang berbasis *Intrusion Prevention System* (IPS) dan *Intrusion Detection System* (IDS) yang diaplikasikan pada jaringan SDN. Pada penelitian [7] dilakukan riset mengenai penggunaan algoritma *fuzzy* dan IDS untuk melakukan pengamanan pada jaringan, hasil yang didapatkan penggunaan algoritma *fuzzy* memberikan effisiensi pada pengurangan 20% hingga 30% baris kode dibandingkan dengan menggunakan keamanan SDN konvensional [7].

Pada Tugas Akhir sebelumnya berjudul "Implementasi Pengontrolan Terpusat *Gateway Long Range* (LORA) *Internet of Things* berbasis *Software Defined Network*" berfokus pada penggunaan jaringan SDN untuk traffic IoT. Dalam penelitian lanjutan ini penulis berfokus pada pencegahan DoS dengan melakukan blokir pada *host* penyerang dengan jenis serangan DoS yaitu *synchronization Attack* (SYN *Attack*), namun kekurangan dari *snort* IPS adalah waktu blokir yang statis tidak mempedulikan frekuensi serangan dari suatu *node* pada jaringan, sehingga akan digunakan logika *fuzzy* seperti pada penelitian [11] dan [12] dengan melakukan pengambilan data *log* dari *snort* IDS lalu data akan diteruskan pada sistem *fuzzy* yang akan menentukan waktu *blokir* dan akan di *block* dari jaringan SDN oleh *controller*.

1.2 Rumusan Masalah

Pada Penelitian Tugas Akhir ini dapat dirumuskan beberapa permasalahan, yaitu bagaimana menghubungkan fungsi IDS *snort*, *Controller* SDN dan fungsi *Fuzzy* untuk dapat meningkatkan keamanan suatu jaringan SDN untuk IoT, bagaimana merancang sistem *fuzzy* untuk menentukan *block* waktu yang dapat beradaptasi dari banyaknya frekuensi serangan dan jenis serangan yang diberikan, dan arsitektur jaringan seperti apa yang dapat digunakan untuk membuat sistem dapat berjalan dengan efektif dan efisien serta mengetahui *Quality of Service* yang didapatkan dalam pengimplementasian sistem yang digunakan.

1.3 Tujuan dan Manfaat

Tujuan dari Tugas Akhir ini adalah mengimplementasikan, menganalisis arsitektur jaringan SDN untuk IoT dan memastikan terhubungnya antara sistem kerja *snort* IDS dengan algoritma *fuzzy* dan *Controller* SDN untuk meningkatkan keamanan jaringan SDN dengan memblokir suatu *host* penyerang dengan waktu blokir yang dapat menyesuaikan dari jenis serangan DoS dan frekuensi blokirnya.

1.4 Batasan Masalah

Adapun batasan-batasan masalah pada penelitian ini adalah sebagai berikut :

1. Pengontrolan terpusat menggunakan fitur "*Firewall"* pada aplikasi *controller* Ryu.
2. Topologi yang dirancang menggunakan 3 *Personal Computer* (PC) sebagai *Gateway* IoT, *Database*, *OpenVswitch* dan *Controller* dan 1 *mini* PC sebagai *Attacker*.
3. *Control Plane* yang digunakan adalah *controller* Ryu versi 4.34 *OpenFlow* versi 2.5.5
4. *Controller* Ryu dipasang pada satu PC yang sama dengan OVS, berfungsi sebagai pemisah antara *control plane* dan *data plane*, serta sebagai pusat pengontrollan *traffic* dan aturan pada jaringan SDN.
5. *Gateway* IoT yang digunakan adalah MQTT dengan menggunakan *Personal Computer* (PC) , yang kemudian dipisahkan antara *Control Plane* dan *Data Plane* pada PC untuk pengontrolan secara terpusat pada arsitektur SDN.
6. *Database* IoT menggunakan InfluxDB yang dipasang pada PC untuk menerimat data IoT dari *Gateway* IoT dan menampilkan data dengan menggunakan Grafana.
7. *Constraint device* mengunakan data *dummy,* berisi data kelembapan dan suhu dengan mengikuti standart besaran data dari sensor DHT 11 dan Node MCU ESP 8266.

8. Menggunakan RYU sebagai SDN *Controller*.
9. Menggunakan *Snort* sebagai IDS.
10. Metode IDS yang digunakan adalah signature-based
11. Diutamakan untuk serangan DoS.
12. Serangan DoS hanya menggunakan SYN *Attack*.

1.5 Metode Penelitian

Beberapa metode penelitian yang digunakan adalah sebagai berikut:

1. Studi Literatur

Studi literature adalah proses pembelajaran teori dan konsep tentang IoT, SDN, kemanan jaringan IDS serta alogirtma *Fuzzy*, dan pengumpulan literatur berupa buku referensi, artikel – artikel serta jurnal tentang teknik kemanan yang mendukung dalam penyusunan penelitian ini.

2. Perancangan Sistem

Perancangan sistem yang akan di uji dari instalasi *OpenFlow* versi 2.2.5 dan *Controller* RYU versi 4.34 Pengecekan konektivtas jaringan dilakukan denganperintah *ping* antar *host*. Jika konfigurasi sudah berjalan, maka ditentukanskenario pengambilan data, implementasi arsitektur SDN dan spesifikasi sistem.

3. Implementasi Sistem

Pengujian Kemanan jaringan IoT berbasis SDN yang sudah di bangun dengan menggunakan serangan teknik serangan DoS, lalu dilakukan skenario pengambilan data.

4. Pengujian Sistem

Pengujian dan Analisis, dilakukan uji coba untuk menguji hasil penerapan pada jaringan IoT berbasis SDN, dan menganalisis dengan pengambilan data terhadap perameter yang sudah di tentukan.

5. Penyusunan Laporan

Setelah dilakukan analisis, langkah selanjutnya membuat kesimpulan dari penelitian yang telah dilakukan serta saran-saran untuk penelitian selanjutnya dan membuat laporan penelitian yang sudah dilakukan dari awal sampai akhir.