BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam pesatnya perkembangan Internet terdapat salah satu pemanfaatan dari berkembangnya internet yaitu munculnya konsep *Internet of Things* (IoT). Dalam penerapan konsep IoT ini ternyata banyak kasus yang ditemukan pada perangkat IoT yaitu menjadi target kejahatan siber, dengan terhubungnya perangkat kedalam jaringan internet maka disitu akan timbul kerentanan dalam jaringan IoT, maka dari itu disitulah menjadi tantangan terbesar untuk IoT ini[1]. Salah satu jenis serangan yang dilancarkan dapat berupa *Denial of Service*(DoS).

DoS adalah salah satu serangan yang mempunyai tujuan utama untuk menghentikan pengguna sah agar tidak dapat mengakses sumber daya yang tersedia[2]. Serangan ini akan membanjiri atau membebani target hingga nantinya target tidak lagi dapat melayani permintaan dalam beberapa waktu tertentu. Tentunya dalam berkembangannya perangkat IoT ancaman seperti ini harus dihindari, menjadikan aspek keamanan di sisi jaringan dan perangkat IoT menjadi salah satu yang harus diperhatikan.

Oleh karena itu dalam Tugas Akhir ini, penulis merancang sebuah sistem keamanan yang dapat diterapkan di dalam platform IoT. Pada platform IoT itu terdiri dari komponen *web service* yang berfungsi untuk menerima data dari perangkat IoT lalu menyimpan di database dan *website* untuk menampilkan data yang telah diterima di database. Pada penelitian lainnya juga telah dirancang sebuah sistem keamanan dan peratahanan dengan cara mengontentikasi trafik yang masuk ke dalam jaringan dan mengamamankan data yang dikirimkan menggunakan enkripsi-dekripsi gerbang XOR[3]. Pada penelitian kali ini penulis mengusulkan sistem keamanan dan pertahanan dengan menerapkan sistem keamanan yang mengadopsi algoritma Advanced Encryption Standard (AES) dan fungsi hasing berupa Message Digest 5 (MD5)[6]. Rancangan sistem keamanan ini meliputi 2 titik yaitu pada *server* dan perangkat IoT. Pada rancangannya perangkat dan server ditetapakan sebuah *password*, hal ini bertujuan sebagai tanda pengenal setiap perangkat yang ingin terhubung. Ketika perangkat ingin mengubungkan ke server,

maka perangkat akan mengirimkan trafik atau tanda pengenal *password* yang telah melalui proses hashing menggunakan metode MD5 yang diubah menjadi sebuah *nilai hash* yang nantinya akan diteruskan dengan proses enkripsi menggunakan algoritma AES, setelah melakukan serangkaian proses tersebut maka dikirimkan ke *server* untuk diperiksa keaslian data yang dikirim. Sistem keamanan dan pertahan ini diuji dengan serangan DoS dan tanpa serangan DoS untuk dapat diketahuai nilai QoS yang di dapat. Selain itu juga kedua hasil pengujian itu akan dibandingkan dengan nilai QoS tanpa sistem keamanan, tujuannya agar mengetahui perbandingan nilai QoS yang di uji[11].

1.2 Tujuan dan Manfaat

1.2.1 Tujuan Penelitian

Adapun tujuan dari Tugas Akhir ini adalah untuk merancang sistem keamanan pada jaringan IoT, dengan menerapkan proses enkripsi-dekripsi menggunakan Algoritma AES yang bertujuan untuk mengamankan data yang dikrim dan proses *hasihing* MD5 yang bertujuan menjaga keabsahannya. Selain itu juga dapat performasi dari *server* yang dirancang terhadap serangan DoS.

1.2.2 Manfaat Penelitian

Manfaat dari penelitian ini adalah manambahkan kemampuan untuk pertahanan pada platform IoT dan kemampuan untuk menjaga kerahasiaan data yang dikirim dari perangkat IoT ke server yang tersedia.

1.3 Rumusan Masalah

Rumusan masalah yang terdapat pada tugas akhir ini adalah:

1. Dapat melakukan proses hashing menggunakan metoda MD5, kemudian dilakukan proses enkripsi menggunakan algoritma AES.
2. Menerapkan sistem keamanan di sisi *server* dan keamanan data saat melakukan pengiriman data dari perangkat ke *server*.
3. Pengujian sistem keamanan yang diterapkan pada perangkat IoT dan enkripsi-deskripsi data dari perangkat ke server dengan menghitung QoS.

1.4 Batasan Masalah

Dalam pengerjaan Tugas Akhir terdapat batasan masalah sebegai berikut:

1. Perangkat IoT yang digunakan menggunakan Raspberry Pi.
2. Penerapan sistem dilakukan pada *web server* (Apache).
3. Pengujian dilkakukan dengan jenis serangan DoS dengan protocol HTTP.
4. Pengujian dilakukan untuk menghitung nilai QoS sistem.

1.5 Metode Penelitian

Dalam penyelesaian penelitian tugas akhir ini dilakukan beberapa metode yang digunakan, yaitu:

1. Studi Literatur

Mempelajari teori dan konsep tentang IoT, mencari informasi mengenai masalah yang dihadapi IoT, mengkaji sumber-sumber berupa *paper*, jurnal, dan buku referensi untuk membantu proses perancangan sistem keamanan pada platform IoT.

2. Flow Chart

Membuat alur secara sistematis langkah-langkah proses peertahanan dalam sistem yang diterapkan.

3. Perancangan Sistem

Melakukan perancangan sistem keamanan mengikuti flow chart yang sudah dibuat sebelumnya, kemudian melakukan analisa kembali apakah rancangan sudah tepat atau belum.

4. Implementasi Sistem

Melakukan implementasi terhadap konsep yang sudah dibuat sebelumnya ke dalam *server* dan perangkat IoT, kemudian melakukan pengecekan sistem berhasil diterapkan tanpa ada *bug* atau *error*.

5. Pengujian dan Analisis

Melakukan pengujian terhadap perangkat IoT dengan melakukan serangan terhadap sistem keamanan dan pertahanan. Setelah melakukan pengujuan terahadap sistem kemudian dilakukan analisis berdasarkan hasil yang telah di dapat.

6. Kesimpulan

Melakukan penarikan kesimpulan terhadap setiap tahap yang telah dilakukan dan analisis serangan terhadap sistem yang telah dirancang.

1.6 Sistematika Penulisan

Pada penulisan Tugas Akhir ini terdiri lima BAB pembahasan sebagai berikut,

BAB I PENDAHULUAN

Pada BAB ini membahas tentang latar belakang mengapa diadakannya penelitian, perumusan masalah, tujuan, manfaat, batasan masalah, metodologi penelitian dan sistematika penulisan.

BAB II TINJUAN PUSTAKA

Pada BAB ini membahas teori pendukung penyususan tugas akhir. Teori pendukung meliputi konsep dan teori dasar antara lain seperti *Internet of Things* (IoT), *Denial of Service* (DoS), Algoritma Advanced Encryption Standard (AES) dan metode hashing MD5.

BAB III PERANCANGAN SISTEM

Pada BAB ini diuraikan mengenai diagram alir sistem, bagaimana penerapan metode hash MD5 dan Algoritma AES saat berada di perangkat melakukan proses enkripsi dan *server* melakukan proses dekripsi.

BAB IV PENGUJIAN DAN ANALISIS SISTEM

Pada BAB ini menjelaskan hasil dan analisis dari rancangan sistem beserta keluaran yang didapat berdasarkan nilai dari parameter yang telah ditetapkan

BAB V KESIMPULAN DAN SARAN

Pada BAB ini membahas kesimpulan menurut hasil dan analisis yang telah didapat, selain itu juga berisikan saran untuk memberikan gambaran pada penelitian selanjutnya