BAB I
PENDAHULUAN

1.1. Latar Belakang

Istilah revolusi industri 4.0 sudah terdengar tidak asing lagi, dimana istilah ini sering disebut-sebut oleh para tokoh nasional maupun internasional. Revolusi industri 4.0 memiliki unsur utama yaitu *Internet of Things* (IoT). IoT merupakan unsur utama dalam revolusi ini dengan memanfaatkan jaringan internet. Dengan adanya IoT, manusia akan merasa terbantu untuk mengontrol maupun memantau keadaan sekitarnya tanpa harus mengeluarkan lebih banyak tenaga.

IoT adalah suatu konsep dimana perangkat yang ada disekitar dapat terhubung ke internet dan dapat berkomunikasi satu sama lain. Dengan adanya IoT, manusia akan dimudahkan untuk mengontrol dan memantau perangkat dimana saja dan kapan saja. IoT memberikan segala kemudahan bagi manusia, namun hal ini tentu tidak serta merta baik, disisi lain justru perangkat IoT ini merupakan salah satu target dari serangan siber anatara lain *Modification Attack*, *Drop Packet* dan *DoS* [1].

Penelitian ini berfokus pada kerentanan perangkat IoT terhadap serangan DoS. DoS atau sering dikenal sebagai *Denial of Service* adalah salah satu jenis serangan siber terhadap jaringan yang bertujuan untuk meniadakan layanan terhadap pengguna. Pengguna-pengguna yang seharusnya berhak dalam menikmati layanan tersebut akan merasa terganggu apabila layanan tersebut hilang yang diakibatkan serangan DoS dan biasanya layanan akan mengalami *crash*, *not responding* atau pun *shutdown* [2]. Maka dari itu dibutuhkan sebuah sistem yang mampu memfilter data tersebut agar tidak serta-marta masuk kedalam *server* sehingga menimbulkan hal yang tidak diinginkan.

Berdasarkan pecobaan yang sudah ada sebelumnya yaitu sebuah sistem didesain dengan cara meng-otentikasi paket-paket data yang diterima oleh *server* dengan metode *Trafic Authentication* [3]. Penelitian ini merupakan inovasi dari penelitian sebelumnya dengan mengadopsi cara kerja dari jaringan Blockchain dimana sistem akan bekerja mulai dari penerimaan data sensor yang kemudian akan

diubah menjadi *hash value* untuk dikirimkan ke *gateway* yang berguna untuk pembuatan *block* baru. *Block* ini nantinya akan divalidasi oleh *server* dengan mencocokan *hash value* yang sudah dibentuk kemudian akan disimpan ke dalam *database server*. Apabila *hash value* tidak sesuai maka data akan diabaikan oleh *server* dan alamat IP dari pengirim data akan diblok oleh *server*. *Block-block* ini nantinya akan di-distribusi ke *gateway-gateway* yang akan berguna untuk menyimpan Salinan *block* serta pembentukan *block* baru dari data yang baru.

1.2. Tujuan dan Manfaat Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Merancang sistem keamanan terhadap perangkat IoT terutama dari serangan DoS dengan menggunakan teknologi Blockchain.
2. Mengimplementasikan sistem keamanan berbasis Blockchain terhadap perangkat IoT.

Manfaat dari penelitian ini diharapkan para pengguna perangkat IoT memiliki rasa aman terhadap perangkat IoT yang dimiliki dan memberikan integritas data yang tinggi.

1.3. Rumusan Masalah

Penelitian Tugas Akhir ini berfokus pada mengimplementasikan sistem keamanan yang berbasis jaringan Blockchain terhadap serangan DoS pada perangkat IoT, maka masalah dapat dirumuskan sebagai berikut:

1. Bagaimana keamanan data terhadap sistem yang sudah dirancang.
2. Bagaimana mengimplementasikan cara kerja jaringan Blockchain terhadap perangkat IoT.
3. Bagaimana performansi perangkat IoT terhadap sistem yang sudah dirancang.
4. Bagaimana performansi *server* terhadap sistem yang sudah dirancang.

1.4. Batasan Masalah

Batasan masalah dalam Tugas Akhir ini meliputi sebagai berikut:

1. Metode *hashing* yang digunakan dalam sistem ini berbasis algoritma MD5.
2. Proses pengiriman data dalam sistem ini menggunakan protokol HTTP.

3. Perangkat IoT yang digunakan adalah perangkat dengan model ESP8266.
4. Sensor yang digunakan dalam sistem yaitu sensor LDR.
5. Pengujian serangan berbasis HTTP.
6. Sistem menggunakan alamat IP statis.
7. Mengabaikan UI/UX dalam menyajikan data.
8. Mengabaikan keamanan pada *interface* pengguna.

1.5. Metode Penelitian

Metode penelitian yang digunakan dalam meyelesaikan Tugas Akhir ini meliputi beberapa bagian, yaitu:

1. Studi Literatur

   Memahami konsep dan teori tentang IoT, memahami konsep dan teori tentang teknik keamanan, mempelajari konsep dan cara kerja dari blockchain, dan memahami meteri lain yang membantu penyelesaian permasalahan ini.
2. Perancangan Sistem

   Perancangan sistem yang diadopsi dari cara kerja blockchain serta berkonsultasi dengan pembimbing.
3. Implementasi Sistem

   Mengimplementasikan sistem yang sudah dirancang untuk meneyelesaikan permasalahan ini.
4. Pengujian Sistem

   Pengujian sistem yang sudah diimplemntasikan dengan Teknik penyerangan yang sudah didefinisikan.
5. Analisis Kinerja Sistem dan Penarikan Kesimpulan

   Analisis hasil keluaran dari sistem yang diujikan berdasarkan parameter-parameter yang sudah ditetapkan serta penarikan kesimpulan dari sistem yang sudah dirancang.

1.6. Sistematika Penulisan

Sistematika dalam penulisan Tugas Akhir ini terdiri dari beberapa BAB, yaitu sebagai berikut:

BAB I PENDAHULUAN

Membahas tentang latar belakang,tujuan,rumusan masalah,batasan masalah dan sistematika terkait sistem yang akan dirancang.

BAB II DASAR TEORI

Membahas tentang teori-teori penunjang untuk merancang sistem yang ingin dibentuk.

BAB III PERANCANGAN DAN REALISASI SISTEM

Membahas tentang cara kerja sistem yang sudah dirancang dengan menggunakan metode yang sudah didefinisikan.

BAB IV PENGUJIAN SISTEM DAN ANALISIS

Membahas tentang pengujian terhadap sistem yang sudah dirancang dan analisi terkait performa dari sistem tersebut.

BAB V PENUTUP

Membahas tentang kesimpulan terhadap sistem yang dirancang serta saran yang membangun terhadap sistem terkait.