BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Menyalurkan listrik dari pembangkit sampai dengan ke pelanggan banyak terjadi penyusutan daya. Pada saat pengiriman energi dari pembangkit listrik, lalu mengirimkannya melalui media transmisi daya dan sampai ke Gardu Induk (GI) PT. PLN (Persero.) Sudah dapat diketahui angka penyusutan daya, karena pengukuran dan pemantauan berjalan dengan baik. Namun pada saat distribusi dari GI sampai ke pelanggan rugi tidak dapat diketahui. Tapi ketika mendistribusikan energi, rugi dari penyusutan daya sulit diketahui besarannya, selain itu ditemukan kejadian penambahan daya listrik ilegal disekitar wilayah Jakarta dalam kejadian tersebut terjadi perbedaan kapasitas listrik seperti yang terdapat di daerah Johar Baru, dalam kapasitas resmi yang seharusnya tertera 450 *Voltampere(VA)* tetapi kenyataannya saat petugas PT. PLN(Persero) melakukan inspeksi dadakan, pemilik rumah menambahkan kapasitas daya menjadi 2200 *VA* tanpa sepengetahuanpihak PT. PLN(Persero) [7]. Setiap daya yang keluar dari GI ini dilengkapi dengan alat ukur, begitu pula pada sisi primer trafo tenaganya. Selepas ini tidak terdapat lagi alat pengukuran kecuali pada meteran pelanggan yang diperiksa oleh petugas.

Kemajuan teknologi dibidang telekomunikasi khususnya internet oleh masyarakat sangat meningkat dan hampir dibutuhkan setiap saat. Sekarang banyak perangkat teknologi yang dapat terkoneksi dengan internet [6]. Menurut paper yang diterbitkan oleh *Electrical Engineering Department, UND, USA.* Meskipun *smart grid* mengatasi beberapa masalah jaringan tradisional, *smart grid* dapat menghadapi sejumlah tantangan dalam keamanan jaringan. Dikarenakan komunikasi telah dimasukan kedalam daya listrik dengan kelemahan bawaannya, sehingga memiliki banyak risiko [3]. Dalam tugas akhir ini dirancang suatu keamanan danpertahanan jaringan pada sistem yang akan bekerja pada jaringan tenaga listrik pintar dirumah. Dalam penelitian ini, akan diimplementasikan keamanan jaringan pada *server smart kwh meter*. Implementasi ini diharapkan dapat dijadikan sebuah solusi untuk melindungi *server* dari serangan *DOS attack* (*smurfing attack*) dan *Sniffing attack.*

1.2. Rumusan Masalah

Berdasarkan latar belakang diatas permasalahan yang dapat diangkat adalah sebagai berikut:

1 Bagaimana menerapkan sistem keamanan jaringan pada perangkat *Smart KWH Meter* di rumah.

2 Bagaiamana hasil serangan *DOS attack (Smurfing attack)* dan *Sniffing attack* pada *firebase server* yang disimulasikan pada sistem keamanan jaringan pada *Smart KWH Meter.*

3 Apakah sistem keamanan jaringan yang dirancang dapat mengatasi serangan terhadap sistem jaringan pada *Smart KWH Meter.*

1.3. Tujuan Penelitian

Tujuan dari penelitian Tugas Akhir ini adalah sebagai berikut:

1. Merancang desain sistem keamanan jaringan pada perangkat *Smart KWH Meter di rumah.*

2. Menganalisis hasil simulasi untuk jenis serangan jaringan *DOS attack* dan *Sniffing Attack* pada *server Smart KWH Meter*.

3. Mengamankan Jaringan yang telah di rancang dan mengatasi serangan terhadap desain jaringan pada *Smart KWH Meter*.

1.4. Batasan Masalah

Untuk membatasi cakupan pembahasan masalah pada Tugas Akhir ini, maka diberikan batasan-batasan sebagai berikut :

1 Perangkat *IoT* yang digunakan berbasis *NodeMcu ESP8266*.

2 Server *IoT* yang digunakan adalah *Firebase*.

3 Jenis serangan yang disimulasikan *DOS attack (Smurfing attack)* dan *Sniffing attack* pada *http server.*

4 Simulasi menggunakan jaringan *WLAN.*

1.5. Metode Penelitian

Metode penelitian yang digunakan pada Tugas Akhir ini adalah sebagai berikut:

1. Studi Literatur

   Dalam Studi Literatur dilakukan dengan mempelajari beberapa referensi yang nantinya mampu menunjang untuk melakukan penelitian dan pengerjaan Tugas Akhir. Referensi yang dapat digunakan adalah bersumber dari buku – buku, paper, *white paper*, jurnal, serta sumber – sumber lain yang berhubungan dengan penelitian dan pengerjaan Tugas Akhir

2. Perancangan Sistem

   Tahap Perancangan sistem dilakukan perancangan sistem keamanan jaringan yang akan dibuat, seperti menyiapkan *config* pada *server* dan intalasi tambahan sesuai yang dibutuhkan

3. Implementasi dan Pengujian

   Meimplementasikan rancangan sistem yang telah dibuat. Membuat sistem keamanan jaringan sesuai simulasi yang akan dilakukan

4. Pengambilan Data

   Pengambilan data bertujuan untuk mengetahui ketepatan data yang diambil ketika implementasi. Pengambilan data dapat menentukan kelayakan metode dan sistem yang penulis terapkan ketika melakukan pengerjaan tugas akhir ini.

5. Analisa Sistem

   Sitem yang telah diimplementasi dan dilakukan pengujian akan dianalisi perfomansinya berdasarkan hasil yang dilakukan saat simulasi serangan

1.6. Sistematika Penulisan

Sistematika penulisan yang digunakan pada Tugas Akhir ini adalah sebagai berikut:

1. BAB I PENDAHULUAN

   Pada bab ini akan dibahas mengenai latar belakang, tujuan, perumusan masalah, batasan masalah, metodologi penelitian, dan sistematika dalam penulisan Tugas Akhir.

2. BAB II TINJAUAN PUSTAKA

   Pada bab ini akan dibahas mengenai teori-teori dasar yang mendukung realisasi sistam dan juga mengenai dasar-dasar dari perangkat yang digunakan sebagai penunjang Tugas Akhir ini. Hal ini dapat mendukung dalam pemecahan masalah, baik yang berhubungan sistem maupun perangkat.

3. BAB III PERANCANGAN SISTEM

   Pada bab ini akan dibahas mengenai perancangan dan realisasi dari Analisis Keamanan Jaringan Pada *Smart Kwh Meter* Berbasis *Internet of Things (IoT).*

4. BAB IV ANALISIS DAN PEMBAHASAN HASIL PENELITIAN

   Pada bab ini akan dibahas mengenai rincian dari hasil analisa serta pembahasannya dari Keamanan Jaringan Pada *Smart Kwh Meter* Berbasis *Internet of Things (IoT)* sesuai dengan tujuan Tugas Akhir ini.

5. BAB V KESIMPULAN DAN SARAN

   Pada bab ini akan dibahas mengenai kesimpulan atas hasil kerja yang telah dilakukan serta akan diberikan rekomendasi dan saran untuk pengembangan dan perbaikan selanjutnya.