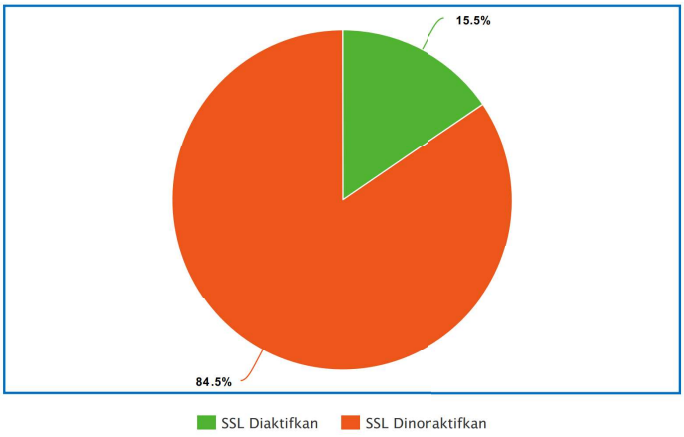
BAB I

PENDAHULUAN

1.1 Latar Belakang

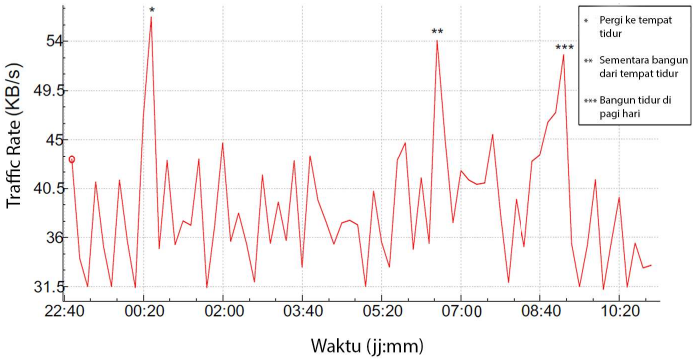
Di era modern sekarang ini manajemen energi memegang peran penting dalam sektor kehidupan, baik dalam skala besar seperti sektor publik dan organisasi pemerintahan, ataupun dalam skala kecil seperti rumah pribadi. Ide dasar pentingnya sebuah manajemen energi adalah pemakaian listrik yang efisien. Penggunaan listrik yang tidak efisien pada sebuah bangunan ditentukan dengan menganalisis pola dari sejumlah data yang terbentuk dari aktifitas pemantauan dan pengukuran listrik. Pendekatan modern untuk memperoleh data konsumsi daya listrik yaitu dengan menggunakan bantuan instrumen teknologi *Internet of Things* (IoT).

Modul ESP8266 merupakan platform populer dalam pembuatan proyek IoT karena harganya yang relatif murah dan kepraktisan yang ditawarkan, namun statistik menunjukkan dalam implementasiannya aspek keamanan masih tergolong rendah[1].



Gambar 1.1. Dalam periode april-mei 2020 terdapat 7.190 *firmware* khusus yang dibuat untuk platform ESP8266. Dari jumlah tersebut, hanya 15,5% yang memiliki dukungan keamanan enkripsi berupa *Secure Socket Layer* (SSL)[1].

Penggunaan sensor yang selalu aktif pada perangkat IoT menciptakan masalah privasi tersendiri bagi konsumen. Informasi yang direkam terkadang bersifat sensitif, seperti pola tidur[4], rutinitas olahraga[5], perilaku anak[6], dan informasi medis[7].



Gambar 1.2. Tingkat lalu lintas/*Traffic Rate* pada sensor pola tidur selama 12 jam[2]. Jika informasi dicuri, pengamat jaringan dapat dengan mudah menganalisis kebiasaan tidur konsumen IoT.

Lalu lintas jaringan IoT rentan terhadap ancaman penyadapan dengan teknik serangan *man-in-the-middle* oleh pihak-pihak yang tidak diinginkan. Aktifitas penyadapan pada lalu lintas jaringan yang tidak diproteksi dapat mengarah pada pencurian data sensitif yang berujung pada penyalahgunaan data. Perlu adanya sistem yang menjamin keamanan lalu lintas data konsumen sehingga lalu lintas jaringan IoT tidak mudah disadap.

Di Tugas Akhir ini penulis mengusulkan sistem enkripsi pada lalu lintas jaringan IoT menggunakan algoritma *Advanced Encryption Standard* (AES) yang diterapkan dalam sistem pemantauan konsumsi daya listrik. Diharapkan dengan penggunaan enkripsi pada lalu lintas jaringan IoT tercipta suatu sistem yang bisa dibilang aman dan meningkatkan aspek keamanan informasi berupa *Confidentiality* dan *Integrity* bagi konsumen IoT.

1.2 Rumusan Masalah

Dari latar belakang yang sudah dijelaskan sebelumnya, adapun rumusan masalah dari Tugas Akhir ini adalah sebagai berikut:

1. Bagaimana desain dan implementasi enkripsi AES pada lalu lintas sistem pemantauan konsumsi daya listrik?
2. Enkripsi AES dengan mode operasi apa yang digunakan untuk mengamankan lalu lintas data pada sistem pemantauan konsumsi daya listrik?
3. Bagaimana kinerja dan keamanan algoritma AES berdasarkan ukuran kunci dalam implementasi enkripsi pada sistem pemantauan konsumsi daya listrik?
4. Bagaimana pengaruh dari implementasi enkripsi AES terhadap performansi sistem pemantauan konsumsi daya listrik?

1.3 Tujuan dan Manfaat

Berdasarkan permasalahan yang telah dijelaskan, maka tujuan dari Tugas Akhir ini adalah sebagai berikut:

1. Merancang dan mengimplementasikan algoritma enkripsi AES pada sistem pemantauan konsumsi daya listrik.
2. Mengetahui kinerja sistem enkripsi AES berdasarkan ukuran kunci pada sistem pemantauan konsumsi daya listrik.
3. Mengetahui performansi sistem yang dibuat dengan melakukan pengukuran konsumsi daya, penggunaan memori, kecepatan proses, dan *Quality of Service* (QoS) berupa *Delay* dan *Throughput*.

Adapun manfaat penelitian Tugas Akhir ini adalah sebagai berikut :

1. Meningkatkan aspek keamanan IoT pada sistem pemantauan konsumsi daya listrik.
2. Membuat referensi kepada pengembang lain mengenai implementasi enkripsi AES dalam teknologi IoT.

1.4 Batasan Masalah

Dalam penelitian Tugas Akhir ini terdapat beberapa hal yang harus dibatasi untuk memberi fokus kepada objek yang dikerjakan, diantaranya:

1. Sistem menggunakan sensor SCT-013-000 sebagai sensor arus listrik.
2. Algoritma enkripsi AES menggunakan mode operasi *Cipher Block Chaining* (CBC).
3. Algoritma enkripsi menggunakan AES dengan ukuran kunci masing-masing 128, 192, dan 256 bit.
4. Mikrokontroler yang digunakan adalah Wemos D1 ESP8266 yang diprogram menggunakan aplikasi konsol PlatformIO.
5. Sistem menggunakan layanan *Amazon Elastic Compute Cloud* (Amazon EC2).
6. Sistem menyajikan data berupa besar daya dan arus listrik.
7. Sistem menggunakan aplikasi Node.js dan ReactJS sebagai *back-end* dan *front-end* pada *cloud server*.
8. Protokol yang digunakan sistem adalah HTTP dan WebSocket.
9. Proses *encoding* dan *decoding* data menggunakan Base64.
10. Data ditampilkan pada *liquid crystal display* (LCD) secara *real-time* dan halaman web.
11. Analisa *avalanche effect* berdasarkan panjang kunci dilakukan untuk mengukur kinerja dan keamanan algoritma AES.
12. Uji performansi sistem dilakukan dengan pengukuran konsumsi daya, penggunaan memori, kecepatan proses dan QoS berupa *Delay* dan *Throughput*.

1.5 Metode Penelitian

Metodologi yang digunakan untuk menyelesaikan penulisan Tugas Akhir ini adalah sebagai berikut:

1. Studi Literatur

   Tahap ini merupakan tahap pengumpulan referensi dan dasar teori sebagai pendukung dalam menganalisis permasalahan yang akan dibahas dengan sumber berupa artikel, jurnal, *textbook* dan *paper* terkait penelitian.

2. Analisis Perancangan

   Pada tahap ini dilakukan perancangan sistem alur, sistem kendali, dan menganalisis permasalahan berdasarkan sumber.

3. Implementasi

   Pada tahap ini perangkat yang telah dibuat sebelumnya kemudian diimplementasikan pada objek yang akan diuji.

4. Pengujian Sistem

   Pada tahap ini dilakukan pengujian terhadap sistem dan melakukan analisis terhadap hasil yang di dapat.