BAB 1

PENDAHULUAN

1.1 Latar Belakang Masalah

PT. ARTRISTIK STUDIO BANDUNG memiliki sistem monitoring berbasis *Internet of Things* yang digunakan untuk melihat kondisi arus listrik yang mengalir pada stasiun pengisian kendaraan listrik umum (SPKLU) milik pelaku usaha yang telah menjalin kerjasama. Cara kerja sistem tersebut yaitu dengan mengirimkan data dari hasil pengukuran sensor arus listrik kemudian diteruskan oleh perangkat IoT menuju basis data yang disediakan oleh *cloud server* secara *online*. Berdasarkan hasil pengujian akurasi terhadap sensor yang digunakan pada sistem monitoring berbasis IoT dibuktikan pada Lampiran A-1 yang dapat disimpulkan bahwa penggunaan sistem tersebut menghasilkan data yang akurat sesuai dengan yang terjadi dilapangan.

Namun, penggunaan perangkat IoT sebagai instrumen dalam sistem monitoring ini dapat menimbulkan sebuah ancaman, berdasarkan penelitian Laayu, dkk [1] menjelaskan bahwa transmisi data yang dilakukan perangkat IoT rentan terhadap penyadapan dengan teknik *man-in-the-middle*, istilah ini muncul ketika penyerang berada pada posisi sudah memasuki ruang lingkup jaringan yang sama dengan perangkat IoT, kemudian melakukan pemantauan dan menangkap atau mengubah data hasil pengukuran sensor yang sedang ditransmisikan pada jaringan tersebut. Contoh dari kegiatan tersebut merujuk pada penelitian Zubaidi, dkk [2] yang dimana terjadi penggunaan aplikasi wireshark pada jaringan IoT dan merujuk pada penelitian Najib dan Sulistyo [3] juga menceritakan terdapat informasi yang bersifat privasi dihasilkan dari analisis data perangkat IoT yang tidak dilengkapi pengamanan mengakibatkan penyalahgunaan pada data tersebut.

Melihat dari permasalahan tersebut, maka dilakukan penerapan kriptografi menggunakan algoritma AES yang berfungsi untuk melakukan pengacakan data

sehingga data sulit untuk dibaca. Berdasarkan penelitian [1], [2], [4], [5], [6] menjelaskan bahwa, algoritma AES dapat digunakan sebagai salah satu pengamanan pada perangkat IoT dan sesuai dengan daya komputasi yang dimilikinya. Dalam hal ini menjadi sebuah alasan mengapa penerapan keamanan pada perangkat IoT harus dilakukan untuk menjaga kerahasiaan data hasil pengukuran sensor sehingga data tersebut aman sampai dilakukan analisis pada sistem monitoring dan pengambilan keputusan.

1.2 Identifikasi Masalah

Permasalahan penelitian yang penulis ajukan dapat diidentifikasi permasalahannya sebagai berikut:

1. Adanya potensi pencurian data yang bersifat privasi ketika data sedang ditransmisikan pada lingkungan IoT sehingga mudah terbaca dan dapat disalahgunakan.
2. Adanya potensi data dari hasil pengukuran sensor yang ditransmisikan perangkat IoT dimanipulasi oleh pihak yang tidak berwenang.

1.3 Maksud dan Tujuan

Maksud:

Mengamankan data perangkat IoT menggunakan kriptografi AES agar terjaga kerahasiaan data pada saat melakukan transmisi.

Tujuan:

1. Menerapkan keamanan pada data hasil pengukuran sensor yang akan ditransmisikan oleh perangkat IoT.
2. Menerapkan sistem yang hanya dapat menerima data dalam bentuk enkripsi dan berasal dari perangkat IoT.

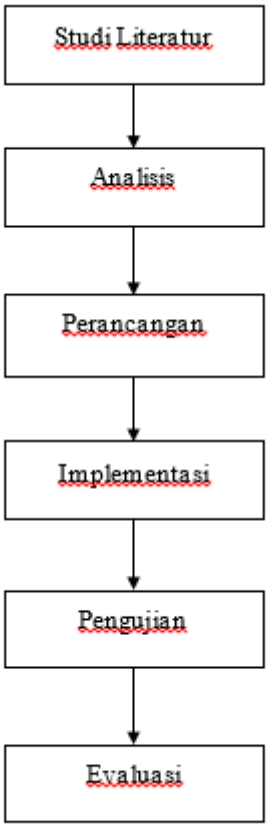
1.4 Batasan Masalah

Adapun batasan-batasan masalah yang ada di dalam penelitian ini meliputi:

1. Metode enkripsi menggunakan algoritma AES.
2. Pengamanan terjadi pada saat sebelum data akan ditransmisikan.
3. Hanya berfokus pada proses pengiriman data dari perangkat IoT.
4. Pembahasan tidak mengenai pengambilan nilai dari sensor, melainkan hanya membahas pemrosesan data.
5. Data yang diamankan merupakan data hasil pengukuran sensor perangkat IoT.
6. Data yang akan dilakukan proses enkripsi berupa teks.
7. Mekanisme kunci yang digunakan adalah hasil dari pembangkitan acak dan tiap perangkat akan memiliki kunci yang berbeda.
8. Penerapan keamanan dilakukan dengan mengembangkan koding *backend* pada perangkat IoT dan *cloud server*.
9. Pembangkitan kunci dilakukan oleh pelaku usaha guna meningkatkan kepercayaan terhadap pemegang kunci.

1.5 Metodologi Penelitian

Metodologi penelitian merupakan suatu proses untuk memecahkan sebuah permasalahan secara logis, dimana memerlukan data-data yang mendukung untuk terlaksananya suatu penelitian. Pada penelitian ini menggunakan metode eksperimental dengan melakukan percobaan dengan data yang sebenarnya terjadi, penelitian ini memiliki 5 tahapan yaitu:



Gambar 1. 1. Metode Penelitian

1. Studi Literatur

   Melakukan studi literatur yang berkaitan dengan pentingnya sebuah keamanan pada perangkat IoT, penggunaan algoritma AES sebagai keamanan data untuk perangkat IoT.

2. Analisis

   Melakukan analisis terkait dengan sistem yang berjalan seperti proses bisnis yang dilakukan, alur proses monitoring yang berjalan, analisis perangkat keras, analisis masalah.

3. Perancangan

   Melakukan perancangan keamanan data yang berdasar dari studi literatur dan analisis yang sudah dilakukan untuk mengamankan data pada perangkat IoT agar pada tahapan transmisi data menjadi aman.

4. Implementasi

Melakukan implementasi hasil perancangan yang sudah dilakukan pada perangkat IoT.

5. Pengujian

   Melakukan pengujian terhadap hasil implementasi rancangan yang sudah dilakukan kemudian memastikan alur sistem berjalan dengan baik dan tidak mengalami masalah.

6. Evaluasi

   Melakukan evaluasi terhadap hasil pengujian yang telah dilakukan.

1.6 Sistematika Penulisan

Sebagai acuan bagi penulis agar penulisan skripsi ini dapat terarah dan tersusun sesuai dengan yang penulis harapkan, maka akan disusun sistematika penulisan sebagai berikut:

BAB 1 PENDAHULUAN

Pada bab ini berisi uraian latar belakang masalah, identifikasi masalah, maksud dan tujuan, batasan masalah, metodologi penelitian, dan sistematika penulisan.

BAB 2 TINJAUAN PUSTAKA

Pada bab ini akan membahas berbagai konsep dasar dan teori-teori pendukung yang berhubungan serta studi literatur terkait pentingnya keamanan data pada perangkat IoT dan penggunaan AES pada perangkat IoT.

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

Pada bab ini akan membahas tentang analisis proses bisnis, deskripsi sistem secara umum, perangkat keras yang digunakan, analisis sistem yang berjalan, analisis masalah serta perancangan sistem.

BAB 4 IMPLEMENTASI DAN PENGUJIAN SISTEM

Pada bab ini berisi hasil implementasi dari hasil analisis dan perancangan yang sudah dilakukan pada BAB 3, kemudian pengujian terhadap hasil implementasi

sistem yang sudah dilakukan untuk memastikan implementasi berjalan dengan baik.

BAB 5 KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan yang diperoleh dari hasil implementasi dan pengujian yang telah dilakukan, serta saran untuk penelitian selanjutnya terkait penggunaan kriptografi sebagai keamanan data pada perangkat IoT.