BAB I
PENDAHULUAN

1.1 Latar Belakang

Penggunaan Internet of Things (IoT) adalah sebuah komunikasi antara mesin ke mesin melalui internet, protokol yang banyak digunakan digunakan untuk IoT adalah *Message Queue Telemetry Transport* (MQTT) karena mengirimkan dengan paket data yang kecil dibandingkan dengan (HTTP) *Hypertext Transfer Protocol* akan tetapi masalah keamanan pada MQTT kurang terjamin yaitu data yang dikirimkan tidak dirahasiakan dapat membuat dapat melihat pesan atau data yang dikirimkan dan dapat terjadi pengintaian terhadap pesan yang dikirimkan atau *Man in the midle attack* (MITM)[26], pada protokol MQTT juga terdapat sebuah keamanan yaitu (TLS) *Transport Layer Security*. akan tetapi pada penggunaan TLS dapat menggunakan konsumsi memori cukup banyak [1,3] dengan penggunaan daya memori yang kecil serta penggunaan (CPU) *Central Processing Unit* maka dibutuhkan sebuah sistem keamanan dalam hal ini MQTT dapat menggunakan protokol keamanan pada proses pengiriman data yang dilakukan oleh MQTT akan tetapi menurut analisa yang dilakukan oleh perusahaan hiveMQ pada pengiriman data menggunakan TLS menggunakan banyak proses komputasi dan memori sehingga dibutuhkan sebuah alternatif lain untuk mengurangi penggunaan proses komputasi[2], maka diperlukan sebuah metode kriptografi untuk mengamankan data yang efisien dan tidak memerlukan banyak proses komputasi dan memerlukan penggunaan memori yang banyak yaitu dengan menggunakan kunci yang digunakan menggunakan *Advanced Encryption Standard* [29]. penggunaan kriptografi AES tersebut memiliki kekurangan yaitu kunci yang digunakan untuk kriptografi menggunkanan kunci simetris[27], untuk mendapatkan kunci tersebut untuk kriptografi maka

dibutuhkan sebuah pertukaran kunci yang dapat digunakan, dalam penelitian ini penggunaan *Elliptic Curve Diffie Hellman* dikarenakan mekanisme pertukaran kunci untuk kriptografi tidak menggunakan banyak proses komputasi [31] dan penggunaan memori untuk proses pertukaran kunci dibandingkan dengan mekanisme kunci publik RSA [5,28,29]

Mekanisme untuk pengamanan pada otorisasi untuk menjamin bahwa data yang dikirim bersumber dari publisher dan sesuai dengan maka penggunaan username dan password dapat dilakukan sebagai otorisasi dari publisher yang benar, sementara untuk mekanisme enkripsi penggunaan metode enkrispsi yang digunakan adalah *client to broker*, dimana pada saat *publisher* akan mengirim data maka akan dilakukan enkrispi untuk menjamin kerahasiaan data yaitu username dan password untuk otentikasi dan *payload*, sementara apabila pada saat pengiriman data tidak sesuai dengan ketentuan yang dibuat maka publisher akan dicabut otenktikasinya serta menghapus data dari *database* yang tersimpan di broker setelah itu akan merestart *broker* tersebut untuk mencegah terjadinya serangan

Berdasarkan masalah yang telah dipaparkan sebelumnya, maka dapat disimpulkan perlunya sebuah sistem protokol komunikasi yang ringan serta dengan kerahasiaan atau keamanan yang dapat mengamankan data pengiriman tersebut. Oleh karena itu dibangunlah sebuah sistem yang diharapkan mampu menjembatani permasalahan tersebut yaitu "SISTEM KEAMANAN DATA PADA PROTOKOL MESSAGE QUEUING TELEMETRY TRANSPORT MENGGUNAKAN ELLIPTIC CURVE DIFFIE HIELMAN DAN ADVANCED ENCRYPTION STANDARD"

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah dipaparkan sebelumnya, maka permasalahan yang dihadapi adalah sebagai berikut :

1. proses pengiriman data pada protokol mqtt yang tidak rahasia menyebabkan data yang dikirim tidak menjadi rahasia

1.3 Maksud dan Tujuan

Maksud dari penelitian ini untuk membuat sebuah sistem monitorng yang akan dipasang di lahan agribisnis untuk memudahkan proses pemantauan tumbuhan pada lahan yang akan di tinjau oleh siswa

Berdasarkan identifikasi masalah yang telah dipaparkan sebelumnya, maka tujuannya adalah sebagai berikut :

1. Membuat sebuah mekanisme untuk mengamankan pengiriman data dan autentikasi pada protokol MQTT dengan enkripsi AES & ECDH

1.4 Batasan Masalah

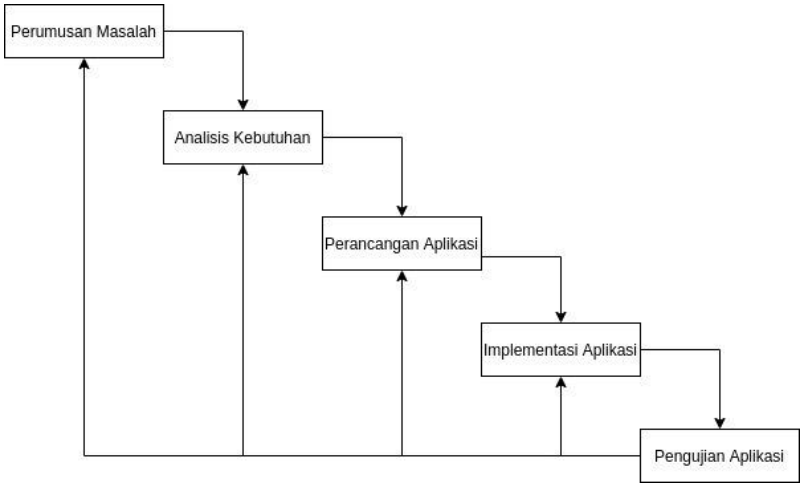
Adapun batasan masalah yang dibuat untuk membatasi dalam pengembangan sistem yaitu :

1. Pembuatan aplikasi ini menggunakan bahasa pemrograman Javascript dan environment Node js dikarenakan broker yang digunakan menggunakan library Aedes berbasis Node js
2. Penggunaan enkripsi menggunakan algoritma AES-256
3. Pertukaran Kunci menggunakan algoritma ECDH (*Elliptic Curve Diffie Hielman*) dikarenakan adanya pertukarana antara 2 node yaitu *client* dan *broker*

4. Microcontroller yang digunakan adalan Raspberry Pi 4 B berfungsi untuk mengirimkan data yang telah diolah serta menerima data sensor dari arduino UNO dan berfungsi untuk autentikasi pengirim
5. Data yang di ambil berasal dari hidrponik adalah kadar PH dan Ketinggian Air Penampung, air penampung diambil menggunakan sensor PH4502C dan ketinggian air diambil menggunakan sensor ultra sonic
6. Penggunaan Arduino uno digunakan untuk mengambil data dari sensor PH yaitu PH4502C karena *output* atau nilai keluaran dari sensor PH adalah analog maka dari Arduino UNO mengirikan data sensor PH melalui *Serial Communication* dan Arduino berfungsi untuk menyalakan mini waterpump karena voltase yang digunakan untuk menyalakan waterpump tersebut adalah 3 – 5 voltase
7. Perancangan kebutuhan perangkat lunak menggunakan *Use Case Diagram.*
8. Sistem yang dibangun untuk melihat monitoring berbasis website.
9. Database yang digunakan menggunakan mysql.

1.5 Metodologi Penelitian

Metodologi merupakan kerangka dasar dari tahapan penyelesaian tugas akhir. Metodologi penulisan pada tugas ini menggunakan *Waterfall*. Berikut ini merupakan metodologi penelitian, dapat dilihat pada gambar 1 di bawah ini



Gambar 1.1 Metodologi Penelitian

Berikut merupakan rincian dari metodologi tugas akhir ini, diantaranya adalah :

1. Perumusan Masalah

Pada tahap ini dilakukan mengidentifikasi masalah. Mengkaji aktivitas sebenarnya serta memutuskan dengan pasti masalah yang akan disederhanakan dalam bentuk aplikasi.

2. Analisis Kebutuhan Aplikasi

Pada tahap ini dilakukan untuk menentukan requirement yang dibutuhkan terhadap aplikasi.

3. Perancangan Aplikasi

Pada tahap ini dilakukan perancangan aplikasi berdasarkan dengan analisis kebutuhan.

4. Implementasi Aplikasi

Pada tahap ini dilakukan implementasi dari hasil perancangan yang sebelumnya telah dibuat.

5. Pengujian

Pada tahap ini dilakukan pengujian sistem serta feedback yang diberikan oleh pihak yang bersangkutan terhadap aplikasi yang telah dibuat

1.6 Sistematika Penulisan

Untuk memudahkan serta mengarahkan dalam penulisan, maka dibuat sistematika penulisan laporan kerja praktek ini sebagai berikut :

Bab I PENDAHULUAN

Bab ini berisi tentang Latar Belakang, Identifikasi Masalah, Maksud dan Tujuan, Manfaat, Batasan Masalah, Metodologi Penelitian dan Sistematika Penulisan.

Bab II TINJAUAN PUSTAKA

Bab ini berisi tentang Profil Tempat Penelitian dan Landasan Teori.

Bab III ANALISIS DAN PERANCANGAN

Bab ini berisi tentang analisis sistem yang dibuat dan perancangan sistem

Bab IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini berisi tentang Implementasi Sistem yang telah dibuat kemudian diuji

Bab V KESIMPULAN DAN SARAN

Bab ini berisi tentang keismpulan dan saran dari penilitan yang telah dilakukan