BAB I

PENDAHULUAN

1.1 Latar Belakang

Seiring berjalan waktu *Internet of Things* (IoT) banyak digunakan dan dikembangkan dengan pesat, dengan semakin mudah nya seseorang untuk memperoleh informasi dari berbagai sumber. Proses *transfer* data dan proses penyimpanan data di dalam *database* juga semakin berkembang. Semakin maju teknologi dalam mengakses informasi kerap disalahgunakan oleh berbagai pihak yang tidak bertanggung jawab [1].Informasi tersebutlah yang harus diberikan keamanan karena tidak menutup kemungkinan informasi tersebut dapat diakses oleh pihak yang tidak bertanggung jawab dan menyebabkan kerugian bagi instansi tertentu. Oleh sebab itu penulis merancang sistem keamanan agar informasi tersebut tidak disalahgunakan.

Dengan latar belakang ketakutan tindakan pencurian data pada saat pengiriman dan didalam *database*,penulis merancang sebuah sistem yang dapat menghindari manipulasi dokumen yang dapat disalah gunakan untuk kepentingan tertentu. Terdapat beberapa cara pengamanan melalui proses autentifikasi dengan dukungan kriptografi yang diantaranya adalah penggunaan algoritma Hash dan pengunaan *Cipher* Simetrik dan Asimetrik. Algoritma hash sangat berguna jika user ingin melakukan pengamanan pesan secara *irreversible* (satu arah). Sedangakan metode *Cipher* simetrik dan asimetrik berguna untuk pengaman yang bersifat *reversible* (dua arah) [6].

Ada berbagai macam pengamanan bersifat *reversible,* salah satunya algoritma RSA. RSA merupakan proses pengkodean kunci asimetris. Proses

perumusan RSA didasarkan pada Teorema Euler, yang menghasilkan kunci publik dan kunci privat yang saling terkait [3]. Sekalipun dua kunci yang berbeda digunakan dalam proses enkripsi dan dekripsi, hasilnya benar. Kunci publik dan pribadi yang digunakan adalah bilangan prima, dan bilangan prima yang besar direkomendasikan untuk mencegah upaya *cracking* karena semakin besar bilangan prima yang digunakan sebagai kunci, semakin sulit menemukan bilangan besar sebagai faktor.

Data di kirimkan melalui protokol *Message Queue Telemetry Transport* (MQTT). *Message Queuing Telemetry Transport* (MQTT) protokol merupakan sebuah protokol yang berjalan diatas *stack* TCP/IP dan dirancang khusus untuk *machine to machine* yang tidak memiliki alamat khusus. Maksud dari kata tidak memiliki alamat khusus ini seperti halnya sebuah arduino, raspi atau *device* lain yang tidak memiliki alamat khusus. Sistem kerja MQTT menerapkan *Publish* dan *Subscribe* data. Dan pada penerapannya, *device* akan terhubung pada sebuah *Broker* dan mempunyai suatu *Topic* tertentu [5].

Data yang dikirimkan melalui protokol MQTT kemudian di teruskan ke dalam *database* menggunakan MySQL. MySQL adalah *tool* yang digunakan khusus untuk mengolah *Structured Query Language* (SQL). SQL sendiri merupakan sebuah bahasa yang digunakan untuk mengakses baris data relasi. Mudahnya adalah untuk mengakses bahasa dalam komputer. Data yang telah masuk di dalam *database* MySQL merupakan data *chipertext* sehingga kerahasiaannya terjamin.

1.2 Rumusan Masalah

Dalam penelitian ini dirumuskan beberapa masalah sebagai berikut :

1. Bagaimana cara menerapkan sistem enkripsi dan dekripsi pada pengiriman data melalui MQTT ke *database* ?
2. Bagaimana tingkat kecepatan pengaman data menggunakan algoritma RSA dalam sistem ?
3. Bagaimana bentuk data yang terkirim melalui MQTT ke *database* ?
4. Bagaimana hasil pengukuran *Quality Of Services* (QoS) pada sistem yang dibuat ?

1.3 Tujuan dan Manfaat

Tujuan dari Tugas Akhir ini adalah :

1. Dapat menerapkan sistem enkripsi dan dekripsi pada pengiriman data melalui MQTT ke *database*.
2. Mengetahui tingkat kecepatan pengamanan data menggunakan algoritma RSA dalam sistem.
3. Mengetahui bentuk data yang terkirim melalui MQTT ke *database*.
4. Mengetahui dan mendapatkan hasil pengukuran *Quality Of Services* (QoS) pada sistem yang dibuat.

Adapun manfaat dari penelitian ini adalah :

1. Mencegah adanya pencurian data.
2. Menambahkan kemampuan untuk pertahanan pada *platform* IoT kemampuan untuk menjaga kerahasiaan data yang dikirim dari perangkat IoT ke *server* yang tersedia.

1.4 Batasan Masalah

Penelitian ini memiliki batasan masalah sebagai berikut :

1. Penerapan sistem menggunakan protokol MQTT.
2. Database yang digunakan menggunakan MySQL.
3. Enkripsi yang digunakan dalam penelitian ini adalah RSA.
4. Dekripsi dilakukan secara otomatis didalam database MySQL.
5. Bahasa pemrogaman yang digunakan adalah *python.*
6. Tidak dilakukan penyerangan dalam penelitian ini.
7. Data yang digunakan menggunakan sensor ultrasonik HC-SR04 dan mikrokomputer Raspberry pi.
8. Proses pertukaran dan pembentukan kunci tidak ditampilkan.

1.5 Metode Penelitian

Metodologi Penulisan yang akan penulis lakukan dalam proses menyelesaikan proyek Tugas Akhir ini terdapat beberapa tahapan, yaitu:

1. Studi Literatur

   Studi literatur ini dimaksudkan untuk memahami dan mempelajari konsep dan teori yang berkaitan dengan perancangan dan implementasi yang digunakan dalam membuat implementasi pengamanan data ini.

2. Analisis Masalah

   Digunakan untuk menganalisis semua permasalahan berdasarkan sumber - sumber dan pengamatan terhadap permasalahan yang telah di kemukakan da-lam batasan masalah.

3. Perancangan

   Merancang sistem yang difokuskan pada proses keamanan data yang dikirimkan ke protokol MQTT menggunakan RSA. Berupa enkripsi dan dekripsi.

4. Pengujian sistem dan analisis

   Tahap ini dilakukan pengujian terhadap keamanan sistem yang telah dibangun.

5. Penyusunan Laporan Tugas Akhir

   Pada tahap ini, dilakukan penyusunan laporan akhir dan pengumpulan dokumentasi yang diperlukan, format laporan mengikuti kaidah penulisan yangbenar dan sesuai dengan ketentuan-ketentuan yang telah ditetapkan oleh institusi.

1.6 Sistematika Penulisan

Sistematika penulisan laporan adalah sebagai berikut:

1. Bab 1 PENDAHULUAN

   Bab ini berisi latar belakang, permasalahan, tujuan, metode penelitian, dan sistematika penulisan.

2. Bab 2 DASAR TEORI

   Bab ini berisi penjelasan teori, sistem, dan perlengkapan yang digunakan.

3. Bab 3 PERANCANGAN

   Bab ini berisi alur kerja dan alur perancangan sistem.