BAB I
PENDAHULUAN

1.1 Latar Belakang

Paradigma *Internet of Things* (IoT) mengacu pada jaringan objek fisik atau "benda" yang disematkan dengan elektronik, perangkat lunak, sensor, dan konektivitas untuk memungkinkan objek bertukar data dengan server, sistem terpusat, dan/atau perangkat terhubung lainnya berdasarkan ragam infrastruktur komunikasi [1]. Dalam siaran pers November 2014, Gartner, Inc. memperkirakan bahwa pada 2015 akan ada 4,9 miliar perangkat IoT yang digunakan di seluruh dunia tumbuh menjadi 25 miliar perangkat pada tahun 2020 [2]. *Internet of Everything* (IoE) tidak terhubung untuk menciptakan nilai bisnis misalnya, orang, data, proses, dan lainnya [3]. Perangkat fisik dan hal-hal yang terhubung ke Internet dan satu sama lain untuk pengambilan keputusan yang cerdas juga disebut IoT. Jadi, IoT mengubah data menjadi pengalaman, yaitu informasi data penting melalui jaringan publik, data besar, dan lain-lain. Dalam IoT, keamanan informasi data melalui Internet harus ditangani dengan hati-hati karena saat ini terdapat sekitar 50 miliar objek pintar yang telah terhubung [4].

Penerapan sistem IoT digunakan untuk memberikan solusi pada berbagai macam masalah. Keamanan data dan privasi tentunya merupakan salah satu permasalahan utama yang dihadapi oleh semua organisasi dan perusahaan yang terhubung ke internet. Meskipun IoT memiliki begitu banyak potensi bagi perkembangan dunia digital, tetapi dalam penerapannya, sistem IoT masih memiliki beberapa masalah utama seperti heterogenitas perangkat, identitas perangkat, manajemen perangkat, dan pengamanan komunikasi perangkat. Kemungkinan terjadinya kejahatan siber pada perangkat IoT dimungkinkan karena banyaknya data pribadi dan penting yang dikumpulkan pada perangkat IoT yang bisa dimanfaatkan untuk tujuan jahat. Oleh karena itu, memfasilitasi sistem dan protokol komunikasi yang aman bagi konsumen menjadi tanggung jawab bagi vendor-vendor perangkat sistem IoT.

Untuk membuat suatu sistem IoT dibutuhkan sensor, perangkat mikrokontroler, server, dan jaringan nirkabel yang menggunakan protokol komunikasi berbeda. Dalam tujuh protokol *stack* interkoneksi TCP/IP terdapat protokol komunikasi yang berbeda untuk tiap lapisan. Melihat hasil penelitian-penelitian terdahulu yang berkaitan dengan protokol komunikasi pada IoT, terdapat lima protokol yang paling banyak digunakan yaitu HTTP [5], XMPP [6], MQTT [7], AMQP [8], dan CoAP [9]. Diantara protokol tersebut, MQTT merupakan protokol paling umum yang digunakan sebagai standar protokol komunikasi untuk sistem IoT karena dengan menggunakan protokol MQTT tidak diperlukan banyak protokol tambahan dan kemampuannya untuk melakukan pengiriman data dengan cepat [10].

Dimulai dengan pengembangan protokol MQTT yang dilakukan oleh [10], penelitian ini menunjukkan bahwa celah keamanan yang membolehkan penyerang untuk melakukan pencurian informasi dari perangkat IoT dapat memberikan dampak yang serius. Alasan tersebut membawa penelitian ini dengan tujuan untuk mengoptimalkan penerapan protokol MQTT pada lingkungan IoT tanpa mengorbankan banyak sumber daya. Dengan mengunakan topologi ini peneliti menerapkan sistem pengamanan data yang dikirim oleh perangkat IoT ke server atau data *center*.

Pada tahun 2001, NIST (*National Institute of Standard and Technology*) mempublikasikan algoritma enkripsi data baru untuk menggantikan algoritma DES (*Data Encryption Standard*) yang memiliki beberapa kelemahan. Algorima baru ini dinamakan AES (*Advanced Encryption Standard*) atau Rijndael [19]. Saat ini, AES merupakan algoritma *cipher* yang cukup aman untuk melindungi data atau informasi yang bersifat rahasia. Algoritma AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit [18].

1.2 Rumusan Masalah

1. Bagaimana merancang sistem pengiriman data IoT melalui protokol MQTT dengan perangkat Arduino Uno?
2. Bagaimana cara melakukan pengiriman pesan terenkripsi AES melalui protokol MQTT pada perangkat Arduino Uno?

1.3 Tujuan

1. Merealisasikan rancangan sistem pengiriman data IoT melalui protokol MQTT dengan perangkat Arduino Uno.
2. Menerapkan pengiriman pesan yang akan dienkripsi AES melalui protokol MQTT pada perangkat Arduino Uno.

1.4 Batasan Masalah yang Dihadapi

1. Broker dan server yang akan diuji dijalankan pada Arduino Uno.

1.5 Metode Penelitian

Pekerjaan penelitian ini dilakukan dengan pendekatan: studi teoritis/studi literatur, pengukuran empirik, analisis statistik, simulasi, perancangan, dan implementasi.

1. Studi Literatur

   Studi literatur dilakukan dengan mempelajari teori dasar mengenai sistem enkripsi AES, komunikasi nirkabel antara perangkat IoT menggunakan MQTT, serta mikrokontroler yang bersumber dari *textbook*, jurnal, buku tugas akhir, dan sumber-sumber referensi lainnya.
2. Analisis Masalah

   Setelah melakukan studi literatur, selanjutnya menganalisis permasalahan pada keamanan data yang dikirim melalui protokol MQTT yang terdiri dari bagian *software* dan *hardware* agar sistem bekerja dengan baik.
3. Perancangan dan Realisasi

   Setelah analisis masalah, selanjutnya merancang pengamanan data yang dikirim melalui protokol MQTT, yang bersumber dari studi literatur dan analisis masalah.

4. Pengujian

   Setelah selesai tahap perancangan dan realisasi, pengamanan data yang dikirim melalui protokol MQTT yang sudah dibuat akan diuji coba untuk mengetahui kinerja sistem.

5. Analisis dan Evaluasi

   Hasil dari pengujian sistem dianalisis kembali untuk dilihat masalah yang ada dan kebutuhan untuk perbaikan alat.