1. Pendahuluan

1.1. Latar Belakang

Seiring dengan pesatnya perkembangan teknologi dan informasi beberapa tahun ini menyebabkan munculnya suatu konsep bernama Internet of Things (IoT). Konsep IoT diperkenalkan sejak tahun 1999 oleh Kevin Ashton [1]. Manfaat dari adanya IoT membuat manusia dapat mengoptimalkan penggunaan konektivitas internet yang selalu ada terus menerus untuk menghubungkan beberapa perangkat fisik dan virtual agar dapat saling berkomunikasi dan manusia dapat mengontrol dari jarak jauh [2]. Perkembangan IoT belakangan ini sudah semakin pesat di berbagai aspek kehidupan manusia, tidak hanya untuk mengontrol peralatan rumah tangga, namun juga dapat digunakan di bidang kesehatan, pertanian, maupun mendeteksi bencana.

Namun, keamanan data dalam sistem IoT juga menjadi hal yang sangat penting untuk dijaga, terutama ketika data yang dikirim dan diterima melalui jaringan internet [3]. Pada penelitian ini penulis menerapkan suatu sistem keamanan kriptografi dengan algoritma AES untuk mengamankan data yang dikirim. AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit [4].

Algoritma AES sendiri telah digunakan pada berbagai perangkat IoT, salah satunya pada modul ESP32 [5]. ESP32 adalah modul mikrokontroler yang menggunakan daya kecil. Algoritma AES dapat digunakan untuk menambah keamanan pada modul ESP32 dengan konsumsi daya yang kecil [6].

Untuk mengirimkan data dari perangkat IoT ke internet, salah satu protokol yang sering digunakan adalah *Message Queue Telemetry Transport* (MQTT) [7][8][9]. MQTT adalah sebuah protokol komunikasi data *machine to machine* (M2M) yang berada pada layer aplikasi [10].

Di penelitian ini, penulis mengambil data kelembaban dan suhu melalui sensor-sensor yang terpasang pada modul ESP32. Data kemudian dikirimkan secara *real-time* melalui jaringan MQTT. Selain itu, untuk meningkatkan keamanan data sistem ini menerapkan enkripsi AES sebelum data dikirimkan melalui jaringan agar data tetap aman dari ancaman pihak yang tidak berwenang. Penelitian ini bertujuan untuk dan membandingkan AES dengan kunci 128 dan 256 bit dengan parameter waktu enkripsi.

1.2. Topik dan Batasannya

Berdasarkan latar belakang yang telah dijelaskan, batasan masalah yang dapat dijabarkan dalam penelitian ini adalah:

1. Pada algoritma enkripsi AES menggunakan panjang kunci 128 bit dan 256 bit
2. Perangkat IoT yang digunakan adalah sensor *Soil Moisture* dan ESP32
3. Protokol komunikasi yang digunakan berbasis MQTT
4. Database yang digunakan adalah MySQL

1.3. Tujuan

Adapun tujuan dari tugas akhir ini adalah

1. Menerapkan enkripsi AES pada perangkat ESP32
2. Menghitung performansi algoritma AES dengan panjang kunci 128 bit dan 256 bit pada ESP32
3. Melakukan analisis performansi algoritma AES 128 bit dan 256 bit pada ESP32

1.4. Organisasi Tulisan

Penulisan tugas akhir ini dibagi menjadi 5 bagian, yaitu:

1. Bagian 1 membahas mengenai masalah yang terjadi pada penelitian ini, tujuan dari penelitian ini, serta batasan masalahnya.
2. Bagian 2 dibahas mengenai studi terkait yang digunakan sebagai bahan informasi dan referensi pada penelitian ini.
3. Bagian 3 dibahas mengenai sistem yang akan dibangun pada penelitian ini.
4. Bab 4 dibahas mengenai hasil pengujian sistem yang sudah dibangun beserta analisis terkait hasil yang sudah ada.
5. Bagian 5 dijelaskan kesimpulan dari seluruh bagian penelitian yang sudah dilakukan menurut hasil dan analisis yang didapat. Terdapat saran untuk mengembangkan sistem ini untuk kedepannya.