BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi dunia terlebih di Indonesia semakin hari sangatlah berkembang dengan pesat. Semakin banyak teknologi yang bermunculan salah satunya adalah Iot. Iot memiliki kemampuan untuk mengontrol sensor atau alat electronika lainnya dari jarak jauh dengan bantuan internet. Iot muncul sebagai isu besar di internet. Diharapkan bahwa miliaran fisik atau benda akan dilengkapi dengan berbagai jenis sensor terhubung ke internet melalui jaringan serta dukungan teknologi seperti *embedded sensor and actuator*, frekuensi radio Identifikasi (RFID), jaringan sensor nirkabel, *real-time* dan layanan web, Iot sebenarnya cyber fisik sistem atau jaringan dari jaringan.[1]

Iot memiliki konsep dimana suatu sensor atau objek yang mampu mentransfer data melalui jaringan tanpa melalui intreaksi dari manusia secara *realtime*. Iot banyak diterapkan pada pengiriman data sensor secara *realtime*. Hingga saat ini sangat beragam sekali protokol yang digunakan untuk perangkat Iot. Beberapa pertimbangan ketika memilih protokol yang akan digunakan diantaranya adalah perangkat Iot yang memiliki keterbatasan (seperti kemampuan menghitung, memiliki daya yang terbatas, dan lainnya). Ada beberapa protokol Iot yang digunakan saat ini, diantaranya adalah *Hypertext Transfer Protocol* (HTTP), *Extensible Messaging and Presence Protocol* (XMPP), *Constrained Application Protocol* (CoAP), *Advanced Message Queuing Protocol* (AMQP), dan *Message Queuing Telemetry Transport* (MQTT)[2].

Protokol MQTT (*Message Queuing Telemetry Transport*) didesain oleh IBM merupakann sebuah protokol yang berjalan pada stack TCP/IP dan memiliki paket data yang ringan sehingga akan berpengaruh pada penggunaan daya[3]. Protokol MQTT memiliki tiga komponen utama yaitu topik, broker dan juga klien. Menggunakan MQTT, klien tidak berkomunikasi langsung dengan titik akhir. publish – mekanisme berlangganan memisahkan klien (penerbit) yang mengirim

pesan dan klien lain (pelanggan) yang menerima pesan[4]. Topik pada protokol MQTT memiliki peran yang sangat krusial dikarenakan pada aplikasi point to point data akan didistribusikan berdasarkan topik. Dalam melakukan komunikasi pada web browser yang berarti HTTP atau HTTPS MQTT menyediakan websocket sebagai perantara Untuk menampilkan data pada web browser. Websocket memberikan browser membangun komunikasi duplex penuh.

Websocket adalah protokol pesan dua arah dengan latensi rendah yang memungkinkan koneksi persisten melalui koneksi TCP/IP tunggal. Websocket dirancang untuk digunakan dalam aplikasi web yang membutuhkan koneksi persisten waktu nyata, seperti obrolan langsung, konferensi video, dll[4]. MQTT melalui websocket merupakann alternative ketika data MQTT akan ditampilkan pada web browser. MQTT melalui Websocket memungkinkan setiap browser menjadi klien MQTT. Saat menggunakan MQTT melalui websocket koneksi websocket akan bertindak sebagai tabung external untuk protokol MQTT. MQTT melalui websocket merupakann metode transformasi yang baik untuk MQTT karena menyediakan komunikasi dua arah.

Salah satu aspek yang terpenting yang harus diperhatikan dalam sistem komunikasi pada protokol MQTT adalah Integritas data yang diterima dari hasil pembacaan sensor oleh *publisher*. Untuk mengirimkan data pada web browser dibutuhkan internet publik untuk transportasi data yang dikirimkan oleh klien *publisher*. Dengan internet publik yang bisa diakses oleh siapapun maka setiap orang yang terhubung akan memiliki potensi mengakses data yang diterima oleh *publisher* dari *subscriber*. Oleh karena itu diperlukan suatu mekanisme keamanan yang dapat menjaga integritas data yang diterima dan di publish oleh klien agar tidak ada pihak yang dapat melihat ataupun mengubah data yang dikirimkan tersebut. Maka dari itu, pada tugas akhir ini akan dilakukan *"implementasi dan analisis fitur keamanan protokol MQTT pada sistem monitoring suhu dan kelembapan berbasis Iot"* dengan memanfaatkan fitur keamanan TLS pada port MQTT websocket sebagai keamanan data sensor yang akan diterima dan ditampilkan oleh *subscriber*.

1.2 Rumusan Masalah

1. Bagaimana kerahasiaan data protokol MQTT Websocket pada Platform Iot dan MQTT websocket klien?
2. Bagaimana mengukur selisih paket data protokol MQTT Websocket pada Platform Iot dan MQTT websocket klien?
3. Bagaimana menghitung besar delay transmisi data protokol MQTT websocket pada Platform Iot dan MQTT websocket klien?

1.3 Tujuan

Tujuan dari penelitian yang dilakukan dari permasalah yang telah dikemukakan di atas yaitu

1. Dapat membandingkan tingkat keamanan data protokol MQTT Websocket dalam mengamankan data pada Platform Iot dan MQTT websocket klien.
2. Dapat membandingkan selisih besar paket data yang diterima oleh Platform Iot dan MQTT websocket.
3. Dapat menghitung rata-rata delay transmisi paket yang dikirim dan diterima menggunakan protokol MQTT Websocket.

1.4 Batasan Masalah

Batasan masalah dalam penelitian ini adalah :

1. Menggunakan Platform Iot *dashboard* dari Nusabot.
2. menggunakan MQTT websocket klien dari EMQX.
3. Menggunakan dua broker publik yaitu broker EMQX dan Eclipse.
4. Menggunakan data sensor DHT11

1.5 Manfaat

Manfaat yang akan diperoleh dari penelitian ini yaitu penelitian ini diharapkan menjadi salah satu rujukan keamanan dengan memanfaatkan fitur keamanan protokol MQTT melalui websocket pada Platform Iot yang memiliki protokol web HTTPS dan MQTT websocket klien yang memiliki protokol HTTP.