BAB 1 PENDAHULUAN

1.1 Latar belakang

Pada era sekarang teknologi merupakan hal yang tidak bisa dipisahkan dari kebutuhan manusia. Teknologi ini yang memberikan kemudahan dalam melakukan aktivitas. *Internet of things* (IoT) adalah salah satu teknologi masa depan yang mengalami perkembangan pesat. IoT adalah sebuah komputer yang tahu segalanya tentang "sesuatu" dan menggunakan data yang telah dikumpulkan tanpa bantuan dari manusia yang kemudian saling berhubungan satu sama lain dengan internet. IoT mengacu interkonetivitas diantara perangkat elektronik yang sering digunakan bersama dengan kemampuan *sensing* dan kesadaran kontekstual (Aismaschana, 2016).

Pada penelitian sebelumnya telah dikembangkan sebuah *middleware*. *Middleware* dengan pendekatan *event-drivent* tersebut mendukung interoperabilitas untuk perangkat dan sensor yang bermacam-macam (Anwari, 2017). *Middleware* tersebut menyediakan *gateway* berupa protokol MQTT dan CoAP untuk berkomunikasi dengan sensor dan menggunakan websocket untuk berkomunikasi dengan aplikasi lain. server middleware adalah raspberry pi yang juga sebagai broker. Node sensor yang digunakan adalah nodeMcu yang bertugas sebagai *publisher* dengan mengirim data *humidity* dan *temperature* ke *middleware*. NodeMcu mempunyai spesifikasi sebagai berikut: sistem operasi XTOS CPU ESP8266 (LX106) *Memory* 128 *kBytes Storage* 4 *Mbytes Power* USB. Sensor nodemcu tersebut berkomunikasi dengan middleware menggunakan protokol komunikasi MQTT dan CoAP. MQTT dan CoAP adalah sebuah protokol standar yang digunakan pada IoT. Message Query Telemetry Transport (MQTT) terdiri dari satu broker server dan dua jenis klien yang disebut Publisher (Publish Client) dan Subscriber (Subscribe Client). Server broker bertindak sebagai perantara pesan yang dikirim antara publisher dan subscriber untuk topik yang menarik. Ketika publisher mengeluarkan topik dan mengirimkan pesan ke server broker, subscriber akan memilih topik mana yang menarik untuk berlangganan (Shinho, 2013). Dan Constrained Application Protocol (CoAP) adalah protokol yang dikembangkan khusus untuk web transfer. CoAP adalah versi HTTP yang dibuat ulang agar cocok dengan kebutuhan IoT yang low overhead dan multi-cast support (Reem abdul, 2016).

Namun pada komunikasi pertukaran data pada jaringan internet selalu ada kelemahan. Kerantanan pada jaringan komputer adalah kelemahan yang memungkinkan penyerang untuk melewati sistem atau keamanan jaringan. Ini yang memberikan penyerang akses ke informasi penting dari komputer sasaran (Badea, 2015). Salah satu serangan paling sukses adalah *Man-In-The-Middle* (MITM). MITM adalah sebuah jenis serangan dimana pihak ketiga yang berbahaya diam-diam mengambil alih kendali saluran komunikasi antara dua atau lebih *endpoints*. Penyerang MITM bisa mencegat, memodifikasi, mengubah atau mengganti sasaran lalu lintas komunikasi korban (Conti, 2016). Pada skema *middleware* tersebut masih terdapat celah keamanan dimana fitur keamanan belum diterapkan, baik pada transmisi data ataupun validasi data sehingga dibutuhkan metode untuk mengatasi celah keamanan tersebut atau bisa disebut *end-to-end security*.

Untuk mengatasi celah keamanan transmisi data dan validasi data terdapat mekanisme keamanan yang dikenal dengan *end-to-end security.* End-to-end (E2E) security adalah sebuah protokol dan mekanisme yang fokus untuk melindungi titik akhir dari koneksi. *Endpoints* atau titik akhir koneksi ini biasa disebut sebagai klien atau server. TLS dan IPsec adalah dua metode

utama yang digunakan pada E2E *security* (www.cisco.com, 2009). *Transport Layer Security* (TLS) atau biasa disebut *Secure Sockets Layer* (SSL) adalah Protokol yang memungkinkan klien/server aplikasi untuk berkomunikasi dengan cara yang dirancang untuk mencegah penyadapan, gangguan atau pemalsuan pesan. Menurut pengembang protokol ini, tujuan dari Protokol TLS adalah keamanan kriptografi, interoperabilitas, ekstensibiliti, dan efisiensi relatif. Dan IPSec adalah kerangka standar terbuka yang menyediakan kerahasiaan data, integritas data, dan otentikasi data antara rekan-rekan yang berpartisipasi di lapisan IP. IPSec dapat digunakan untuk melindungi satu atau beberapa arus data antara rekan IPSec (www.ciscopress.com, 2002).

Berdasarkan penelitian yang telah dilakukan, ditemukan sebuah solusi untuk masalah keamanan yang terjadi pada MQTT dan CoAP. Pada CoAP yang berjalan pada UDP bisa menggunakan *Datagram Transport Layer Security* (DTLS), versi UDP dari TLS yang lebih ringan. Sedangkan MQTT yang berjalan pada TCP bisa diatasi dengan TLS/SSL dan IPsec (Aimaschana, 2016).

Berdasarkan uraian diatas, keamanan pada jaringan merupakan hal yang penting untuk melindungi data dari serangan. maka dalam penelitian ini akan dilakukan analisis kinerja dua metode umum dalam E2E pada komunikasi dengan protokol MQTT dan CoAP pada IoT *middleware* yang telah dikembangkan di penelitan sebelumnya. Sehingga komunikasi dan transmisi data aman dari serangan seperti MITM yang bisa menyadap informasi pada komunikasi antara node sensor dengan middleware. Melihat minimnya spesifikasi pada nodeMcu muncul pertanyaan mekanisme keamanan apa saja yang dapat diterapkan antara nodeMcu dengan IoT *middleware*. Ada dua mekanisme keamanan yang bisa diterapkan pada NodeMcu berdasarkan modul yang tersedia, yaitu TLS dan crypto. Selain menerapkan mekanisme keamanan, pada penelitian ini diharapkan ada rekomendasi dari kedua mekanisme ini yang manakah yang paling sesuai, aman dan efisien serta tidak mengurangi *Quality of Service* (QoS) pengiriman data dari sistem sebelumnya.

1.2 Rumusan masalah

Berdasarkan permasalahan yang diuraikan sebelumnya, maka rumusan masalah:

1. Bagaimana implementasi mekanisme *end-to-end security* pada komunikasi antara *node* sensor dengan IoT *middleware*?
2. Bagaimana kinerja mekanisme *end-to-end security* pada komunikasi antara *node* sensor dengan IoT *middleware*?
3. Bagaimana pengaruh mekanisme *end-to-end security* pada komunikasi antara *node* sensor dengan IoT *middleware* terhadap *Quality of Service* (QoS) pengiriman?

1.3 Tujuan

Berdasarkan rumusan masalah yang diuraikan diatas, tujuan yang ingin dicapai dari penulisan skripsi ini adalah:

1. Mengimplementasikan mekanisme *end-to-end security* pada komunikasi antara *node* sensor dengan IoT *middleware*
2. Menganalisis kinerja mekanisme *end-to-end security* pada komunikasi antara *node* sensor dengan IoT *middleware*
3. Menganalisis pengaruh mekanisme *end-to-end security* pada komunikasi antara *node* sensor dengan IoT *middleware* terhadap Quality of Service (QoS) pengiriman?

1.4 Manfaat

Manfaat dari penelitian skripsi ini untuk beberapa pihak, diantaranya sebagai berikut:

Untuk Penulis:

1. Dapat menerapkan ilmu yang telah dipelajari selama perkuliahan
2. Dapat menambah keilmuan tentang jaringan komputer dan keamanan pada jaringan

Untuk Fakultas Ilmu Komputer:

1. Memberikan inspirasi sebagai pemicu untuk penelitian dan pengembangan tentang jaringan dan keamanan jaringan

Untuk Masyarakat:

1. Menmberikanpengetahuan tentang mekanisme *end-to-end security* komunikasi antara *node* sensor dengan IoT *middleware*

1.5 Batasan masalah

Batasan masalah dalam penelitian ini sehingga lebih fokus adalah:

1. NodeMcu mempunyai mempunyai spesifikasi sebagai berikut: sistem operasi XTOS CPU ESP8266 (LX106) *Memory* 128 kBytes *Storage* 4 Mbytes *Power* USB
2. Protokol yang akan digunakan adalah MQTT dan CoAP
3. Mekanisme yang akan diterapkan pada *end-to-end security* menggunakan modul dari nodeMcu yaitu TLS dan *crypto*

1.6 Sistematika Penulisan

Sistematika penulisan ditujukan sebagai petunjuk tentang gambaran penulisan skripsi ini yang terdiri dari beberapa bab berikut:

BAB 1 PENDAHULUAN

Pada bab satu berisi tentang latar belakang dari penelitian, rumusan masalah yang terjadi, tujuan yang ingin dicapai, manfaat dari penelitian, batasan masalah penelitian ini, dan sistematika penulisan skripsi

BAB 2 LANDASAN KEPUSTAKAAN

Pada bab dua berisi tentang pembahasan dan uraian dari dasar teori yang digunakan pada penelitian ini yang berkaitan dengan masalah atau pertanyaan untuk penelitian sebagai referensi

BAB 3 METODOLOGI

Pada bab tiga berisi tentang metodelogi yaitu tahap-tahap penelitian mulai dari identifikasi masalah sampai dengan kesimpulan yang digunakan pada penelitian ini.

BAB 4 PEGUJIAN DAN PENGOLAHAN DATA

Pada bab empat ini berisi tentang skenario-skenario pengujian dari sistem yang telah dibuat dan pengolahan data dari hasil pengujian sistem.

BAB 5 ANALISIS DAN PEMBAHASAN

Pada bab lima ini berisi tentang hasil analisis dari pengujian dan pengolahan data sehingga kemudian dilakukan pembahasan.

BAB 6 PENUTUP

Pada bab enam ini berisi kesimpulan dan saran yang diambil dari hasil penelitian ini berdasarkan tahap yang telah dilakukan.