1. Pendahuluan

Latar Belakang

Internet of Things (IoT) adalah komunikasi antar mesin melalui Internet, konsepnya adalah bahwa setiap perangkat dapat berkomunikasi melalui akses Internet [1]. Protokol komunikasi yang banyak digunakan di IoT adalah *Message Queue Telemetry Transport* (MQTT) [2]. Protokol ini banyak digunakan IoT karena menggunakan *bandwidth* yang kecil dan ringan, sehingga baik diterapkan pada IoT [3].

Penggunaan protokol MQTT telah banyak diterapkan. Ada beberapa sistem yang menggunakan MQTT untuk mengirimkan data rahasia dan sensitif seperti *Internet of Things for Health* [4], *GPS Tracking* [5] dan *Automated Home Automation* [6]. Tetapi begitu IoT juga memiliki kelemahan, itu mengacu pada *Open Web Application Security Project* (OWASP) bahwa IoT memiliki serangan yang ada pada perangkat layanan jaringan yang memiliki kurangnya verifikasi payload dan pemeriksaan integritas dalam pesan. Terkadang perangkat IoT ingin mengirim pesan rahasia yang hanya dapat diakses oleh perangkat resmi [1].

Protokol MQTT tidak memiliki proses enkripsi pada *payload* yang menimbulkan masalah keamanan dan integritas pada data *payload*, yang memungkinkan penyerang untuk mengetahui konten yang dikirim[1].

Berdasarkan masalah di atas untuk menangani masalah keamanan dan integritas data dapat menggunakan *digital signature*. *Digital signature* bertujuan untuk otentikasi data *payload* dan untuk memastikan bahwa informasi tidak diperbarui selama transmisi [8]. *Digital signature* akan memberi kepercayaan kepada penerima bahwa informasi yang dikirimkan adalah benar dari *publisher* yang berwenang. *Digital signature* juga digunakan untuk mengidentifikasi apakah pesan pengirim memenuhi persyaratan untuk diterima dan dibaca oleh penerima atau tidak. *Digital signature* bisa dilakukan untuk mengamankan data sensitif [9].

Digital Signature mendukung enkripsi *shared secret key* untuk mengirimnya dengan aman melalui Internet [10]. Aplikasi *digital signature* dalam penelitian ini mengimplementasikan algoritma AES dan SHA. Penggunaan enkripsi AES dalam penelitian ini karena ringan dan efisien digunakan dalam perangkat lunak dan keras [11] juga dapat digunakan untuk *digital signature* [12] dan SHA untuk membuat *digest* untuk mendeteksi modifikasi ilegal oleh entitas yang tidak terpercaya [9].

Penambahan mekanisme keamanan tentu akan menghasilkan *overhead* komputasi pada sistem [13]. Analisis *overhead* digunakan untuk mengukur berapa banyak sumber daya tambahan yang dibutuhkan dalam mekanisme keamanan yang diterapkan [14]. Analisis *overhead* di MQTT dapat dilakukan dengan melihat beberapa aspek yang meningkat dengan penambahan mekanisme seperti pada proses enkripsi, waktu pengiriman latensi, beban CPU [13], konsumsi memori, proses keamanan [14].

Pennelitian ini menganalisis *overhead* menggunakan *digital signature* pada protokol MQTT. Penggunaan mekanisme *digital signature* ini memiliki *overhead* karena adanya penambahan mekanisme keamanan yang menghasilkan peningkatan dalam beberapa aspek. Oleh karena itu analisis *overhead* dilakukan untuk mengetahui berapa banyak *overhead* yang dihasilkan pada sistem yang diusulkan.

Topik dan Batasannya

Berdasaran latar belakang yang telah dijelaskan, permasalahan yang diteliti adalah menganalisis *overhead* dari penggunaan *digital signature* pada MQTT. Skema *digital signature* ini menerapkan algortima AES dan SHA. *Overhead* yang dilakukan adalah dengan mengukur ukuran *payload*, lama pengiriman *payload* dari *publisher* ke *subscriber*, waktu penggunaan skema *digital signature* terhadap *payload* yang dikirimkan, konsumsi memori dari *device* yang menjalankan program, dan penggunaan CPU saat menggunakan program ini. Pengetasan dilakukan dengan penetrasi *testing* untuk meyakinkan bahwa program dapat mengamankan *payload* yang dikirim. Penetrasi menggunakan *man-in-the-middle* untuk *sniffing* komunikasi antara dua buah entitas yaitu *publisher* dan *subscriber*. Program yang dibuat adalah program *publish*/*subscribe* middleware yang dibuat oleh *python* yang mengimplementasikan protokol MQTT didalamnya dengan menambahkan skema *digital signature*, tipe data yang dikirimkan adalah tipe data *string*, penelitian ini tidak menggunakan *microcontroller* dalam proses menjalankan program tetapi dengan menggunakan *microprocessor* (Raspberry Pi 3).

Tujuan

Tujuan dari penelitian tugas akhir ini adalah menganalisis *overhead* pada penggunaan *digital signature* pada *publish/subscribe middleware* dengan menggunakan enkripsi simetrik AES dan SHA untuk mengetahui nilai *overhead* dari masing-masing versi dari AES dan SHA agar mengetahui mana yang sedikit dan banyak menggunakan *resource* dari device IoT (Raspberry Pi). *Publish/subscribe middleware* ini bertujuan untuk mengamankan *payload* yang dikirimkan oleh protokol MQTT untuk mencegah penyalahgunaan *payload* yang dikirimkan oleh protokol MQTT.

Organisasi Tulisan

Pada penulisan tugas akhir ini disusun dalam 5 Bab bagian yaitu Bab 1 – Pendahuluan yang berisikan latar belakang, rumusan masalah, batasan masalah, dan tujuan. Bab 2 – Studi terkait menjelaskan tentang literatur apa saja yang telah diteliti sebelumnya sebagai acuan untuk peneliti an ini. Bab 3 – Perancangan Sistem yaitu menjelaskan alur sistem yang dibuat. Bab 4 – Implementasi dan Evaluasi menjelaskan tentang pengimplementasian sistem dan analisis dari program yang telah dibuat. Bab 5 – Penutup yang berisi kesimpulan dari hasil analisis dan saran.